Московский физико-технический институт
Физтех-школа прикладной математики и информатики

АЛГЕБРА И ГЕОМЕТРИЯ

I СЕМЕСТР

Лектор: *Богданов Илья Игоревич*

h\nu

Автор: *Даниил Дрябин*
Проект на Github

осень 2019

Содержание

1 Матрицы и векторы

1.1 Матрицы

Определение 1.1. *Матрицей размера* $n \times k$ называется таблица из n строк и k столбцов, заполненная числами (или другими элементами):

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix} = (a_{ij})$$

Обозначение множества числовых матриц данного размера — $M_{n\times k}$, множества квадратных числовых матриц размера $n \times n$ — M_n

Определение 1.2. *Строкой длины* k называется матрица размера $1 \times k$, *столбцом высоты* n — матрица размера $n \times 1$. Если $A = (a_{ij}) \in M_{n\times k}$, то строка матрицы A с номером d обозначается через a_{d*}, столбец с номером d — через a_{*d}.

Определение 1.3. *Подматрицей* матрицы $A \in M_{n\times k}$ называется матрица, полученная из A удалением некоторых ее строк или столбцов.

Определение 1.4. Ниже перечислены основные операции над матрицами:

1. Пусть $A = (a_{ij}), B = (b_{ij}) \in M_{n\times k}$. *Суммой матриц A и B* называется матрица $A + B \in M_{n\times k}$ следующего вида:

$$A + B := (a_{ij} + b_{ij})$$

2. Пусть $A = (a_{ij}) \in M_{n\times k}$, A, $\lambda \in \mathbb{R}$. Матрицей, полученной из A *умножением на скаляр* λ, называется матрица $\lambda A \in M_{n\times k}$ следующего вида:

$$\lambda A := (\lambda a_{ij})$$

3. Пусть $A = (a_{ij}) \in M_{n\times k}$. Матрицей, полученной из A *транспонированием*, называется матрица $A^T \in M_{k\times n}$ следующего вида:

$$A^T := \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1k} & a_{2k} & \dots & a_{nk} \end{pmatrix} = (a_{ji})$$

4. Пусть $a_{1*} \in M_{1\times n}$ — строка длины n, $b_{*1} \in M_{n\times 1}$ — столбец высоты n. *Произведением строки A и столбца B* называется следующая величина:

$$a_{1*}b_{*1} := \sum_{i=1}^{n} a_{1i}b_{i1}$$

Величину AB можно считать как числом, так и матрицей размера 1×1.

5. Пусть $A = (a_{ij}) \in M_{n\times k}$, $B = (b_{ij}) \in M_{k\times m}$. *Произведением матриц* A *и* B называется матрица $AB \in M_{n\times m}$ следующего вида:

$$AB := (a_{i*}b_{*j}) = \left(\sum_{t=1}^{k} a_{it}b_{tj}\right)$$

Утверждение 1.1. *Сложение матриц обладают следующими свойствами:*

- ▷ $\forall A, B \in M_{n\times k} : A + B = B + A$ *(коммутативность)*
- ▷ $\forall A, B, C \in M_{n\times k} : (A + B) + C = A + (B + C)$ *(ассоциативность)*
- ▷ $\exists 0 \in M_{n\times k} : \forall A \in M_{n\times k} : A + 0 = A$ *(существование нейтрального элемента)*
- ▷ $\forall A \in M_{n\times k} : \exists(-A) \in M_{n\times k} : A+(-A) = 0$ *(существование противоположного элемента)*

Доказательство. Доказательство производится непосредственной проверкой. Отметим только, что $0 \in M_{n\times k}$ — это матрица из нулей, а $(-A) \in M_{n\times k}$ — матрица, каждый элемент которой является противоположным соответствующему элементу A. □

Утверждение 1.2. *Умножение матрицы на число обладает следующими свойствами:*

- ▷ $\forall \lambda \in \mathbb{R} : \forall A, B \in M_{n\times k} : \lambda(A + B) = \lambda A + \lambda B$ *(дистрибутивность умножения матрицы на число относительно сложения)*
- ▷ $\forall \lambda, \mu \in \mathbb{R} : \forall A \in M_{n\times k} : (\lambda+\mu)A = \lambda A+\mu A$ *(дистрибутивность умножения матриц относительно сложения)*
- ▷ $\forall \lambda, \mu \in \mathbb{R} : \forall A \in M_{n\times k} : (\lambda\mu)A = \lambda(\mu A)$
- ▷ $\forall A \in M_{n\times k} : 1A = A$

Доказательство. Доказательство производится непосредственной проверкой. □

Утверждение 1.3. *Транспонирование обладает следующими свойствами:*

- ▷ $\forall A, B \in M_{n\times k} : (A + B)^T = A^T + B^T$ *(дистрибутивность транспонирования относительно сложения матриц)*
- ▷ $\forall \lambda \in \mathbb{R} : \forall A \in M_{n\times k} : (\lambda A)^T = \lambda A^T$
- ▷ $\forall A \in M_{n\times k} : (A^T)^T = A$
- ▷ $\forall A, B \in M_{n\times k} : (AB)^T = B^T A^T$

Доказательство. Доказательство производится непосредственной проверкой. □

Утверждение 1.4. *Умножение матриц обладает следующими свойствами:*

- ▷ $\forall A \in M_{n\times k} : \forall B \in M_{k\times m} : \forall C \in M_{m\times l} : (AB)C = A(BC)$ *(ассоциативность)*

- ▷ $\exists E_n \in M_n : \exists E_k \in M_k : \forall A \in M_{n\times k} : E_nA = AE_k = A$ *(существование нейтрального элемента)*
- ▷ $\forall A, B \in M_{n\times k} : \forall C \in M_{k\times m} : \forall D \in M_{m\times n} : (A+B)C = AC + BC$ *и* $D(A+B) = = DA + DB$ *(дистрибутивность относительно сложения матриц)*
- ▷ $\forall \lambda \in \mathbb{R} : \forall A \in M_{n\times k} : \forall B \in M_{k\times m} : \lambda(AB) = (\lambda A)B = A(\lambda B)$

Доказательство. Доказательство производится непосредственной проверкой. Отметим только, что матрица $E_m \in M_m$ имеет следующий вид:

$$E_m := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Определенная таким образом единичная матрица произвольного размера удовлетворяет условию. □

Определение 1.5. *Линейной комбинацией* элементов $v_1, \dots, v_n$ (для которых определено сложение и умножение на числа) с коэффициентами $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ называется следующая величина:

$$\sum_{i=1}^{n} \alpha_i v_i = \alpha_1 v_1 + \dots + \alpha_n v_n$$

Утверждение 1.5. *Пусть* $A \in M_{n\times k}$, $B \in M_{k\times m}$, $C := AB \in M_{n\times m}$. *Тогда:*

- ▷ *Столбцы матрицы C являются линейными комбинациями столбцов матрицы A*
- ▷ *Строки матрицы C являются линейными комбинациями строк матрицы B*

Доказательство. Докажем первую часть утверждения, поскольку вторая доказывается аналогично. Представим A в виде $(a_{*1} \dots a_{*k})$, тогда столбцы C имеют следующий вид:

$$c_{*i} = \sum_{t=1}^{k} a_{*t} b_{ti}$$

Каждый столбец c_{*i} матрицы C является линейной комбинацией столбцов $a_{*1}, \dots, a_{*k}$ с коэффициентами $b_{1i}, \dots, b_{ki}$, что и требовалось. □

1.2 Векторы и линейная зависимость

Определение 1.6. *Направленным отрезком* называется отрезок (на прямой, на плоскости или в пространстве), концы которого упорядоченны. Обозначение — $\overline{AB}$. Направленные отрезки $\overline{AB}$ и $\overline{CD}$ называются *равными*, если они сонаправленны и их длины равны.

Замечание. Равенство является отношением эквивалентности на множестве всех направленных отрезков на прямой, на плоскости или в пространстве.

Определение 1.7. *Вектором* называется класс эквивалентности направленных отрезков. Формально, если $\overline{AB}$ — представитель класса $\overline{v}$, то $\overline{AB} \in \overline{v}$, но в дальнейшем это будет обозначаться как $\overline{AB} = \overline{v}$.

Определение 1.8. Ниже перечислены обозначения множеств векторов и точек:

- V_0 — *нулевое пространство*, состоящее только из нулевого вектора $\overline{0}$
- V_1, P_1 — множества всех векторов и всех точек *на прямой*
- V_2, P_3 — множества всех векторов и всех точек *на плоскости*
- V_3, P_3 — множества всех векторов и всех точек *в пространстве*

Всегда можно считать, что $V_0 \subset V_1 \subset V_2 \subset V_3$ и $P_1 \subset P_2 \subset P_3$.

Замечание. Вектор отличается от направленного отрезка тем, что его можно отложить от заданной точки: для любой точки $A \in P_n$ и вектора $\overline{v} \in V_n$ существует единственная точка $B \in P_n$ такая, что $\overline{AB} = \overline{v}$.

Определение 1.9. Основные операции с векторами:

1. Пусть $\overline{u}, \overline{v} \in V_n$. Отложим вектор $\overline{u}$ от некоторой точки $A \in P_n$, получим $\overline{AB} = \overline{u}$. Теперь отложим $\overline{v}$ от точки $B \in P_n$, получим $\overline{BC}$. *Суммой векторов* $\overline{u}$ *и* $\overline{v}$ называется такой класс $\overline{u} + \overline{v}$ с представителем $\overline{AC}$.

2. Пусть $\overline{u} \in V_n$. Отложим вектор $\overline{u}$ от некоторой точки $A \in P_n$, получим $\overline{AB} = \overline{v}$. Вектором, полученным из $\overline{u}$ *умножением на скаляр* λ, называется следующий класс эквивалентности $\lambda\overline{u}$:
   - Если $\lambda = 0$, то $\lambda\overline{u} = \overline{0}$
   - Если $\lambda > 0$, то $\lambda\overline{u}$ — это класс с представителем $\overline{AC}$ таким, что $AC = \lambda AB$ и $\overline{AC} \uparrow\uparrow \overline{AB}$
   - Если $\lambda < 0$, то $\lambda\overline{u}$ — это класс с представителем $\overline{AC}$ таким, что $AC = |\lambda| AB$ и $\overline{AC} \uparrow\downarrow \overline{AB}$

Утверждение 1.6. *Операции с векторами обладают следующими свойствами:*

- $\forall \overline{u}, \overline{v} \in V_n : \overline{u} + \overline{v} = \overline{v} + \overline{u}$
- $\forall \overline{u}, \overline{v}, \overline{w} \in V_n : (\overline{u} + \overline{v}) + \overline{w} = \overline{u} + (\overline{v} + \overline{w})$
- $\exists \overline{0} \in V_n : \forall \overline{u} \in V_n : \overline{u} + \overline{0} = \overline{u}$
- $\forall \overline{u} \in V_n : \exists (-\overline{u}) \in V_n : \overline{u} + (-\overline{u}) = \overline{0}$
- $\forall \lambda, \mu \in \mathbb{R} : \forall \overline{u} \in V_n : (\lambda + \mu)\overline{u} = \lambda\overline{u} + \mu\overline{u}$
- $\forall \lambda \in \mathbb{R} : \forall \overline{u}, \overline{v} \in V_n : \lambda(\overline{u} + \overline{v}) = \lambda\overline{u} + \lambda\overline{v}$
- $\forall \lambda, \mu \in \mathbb{R} : \forall \overline{u} \in V_n : (\lambda\mu)\overline{u} = \lambda(\mu\overline{u})$
- $\forall \overline{u} \in V_n : 1\overline{u} = \overline{u}$

Доказательство. Доказательство производится непосредственной проверкой. Приведем указания к доказательству некоторых из свойств:

- Первое свойство сводится к использованию свойств параллелограмма.

- ▷ Для доказательства второго свойства достаточно показать, что оба случая представляют собой последовательное откладывание следующего вектора от конца предыдущего.

- ▷ Свойства, связанные с умножением на число, требуют рассмотрения всех случаев выбора знаков у чисел и во всех случаях очевидно выполняются. □

Замечание. Используя свойства операций с векторами как аксиомы, можно показать, что $0\overline{u} = \overline{0}$ для любого $\overline{u} \in V_n$, не требуя этого равенства по определению:

$$0\overline{u} + 0\overline{u} = (0+0)\overline{u} = 0\overline{u} \Rightarrow 0\overline{u} + 0\overline{u} + (-0\overline{u}) = 0\overline{u} + (-0\overline{u}) \Rightarrow 0\overline{u} = \overline{0}$$

Определение 1.10. Система $(\overline{v_1}, \ldots, \overline{v_n})$ векторов из V_n называется *линейно независимой*, если для любых $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ выполнено следующее условие:

$$\sum_{i=1}^{n} \alpha_i \overline{v_i} = \overline{0} \Leftrightarrow \alpha_1 = \cdots = \alpha_n = 0$$

Замечание. Условие выше эквивалентно тому, что любая ее *нетривиальная* (имеющая ненулевой коэффициент) линейная комбинация отлична от нулевого вектора.

Определение 1.11. Система $(\overline{v_1}, \ldots, \overline{v_n})$ векторов из V_n называется *линейно зависимой*, если существует ее нетривиальная линейная комбинация, равная $\overline{0}$.

Утверждение 1.7.

1. *Если система линейно независима, то любая ее подсистема тоже линейно независима.*

2. *Если система линейно зависима, то любая ее надсистема тоже линейно зависима.*

Доказательство.

1. Пусть без ограничения общности у линейно независимой системы $(\overline{v_1}, \ldots, \overline{v_n})$ есть линейно зависимая подсистема $(\overline{v_1}, \ldots, \overline{v_k})$. Тогда существует нетривиальная линейная комбинация $\alpha_1\overline{v_1} + \cdots + \alpha_k\overline{v_k}$. Но если эту линейную комбинацию дополнить линейной комбинацией $0\overline{v_{k+1}} + \cdots + 0\overline{v_n}$, то получится нетривиальная линейная комбинация векторов $(\overline{v_1}, \ldots, \overline{v_n})$, равная $\overline{0}$ — противоречие.

2. Если система $(\overline{v_1}, \ldots, \overline{v_n})$ линейно зависима, то ее нетривиальную линейную комбинацию, равную $\overline{0}$, можно аналогично дополнить до нетривиальной линейной комбинации любой ее надсистемы. □

Определение 1.12. Пусть $\overline{u} \in V_n$, $(\overline{v_1}, \ldots, \overline{v_n})$ — система векторов из V_n. Вектор $\overline{u}$ *выражается через* $(\overline{v_1}, \ldots, \overline{v_n})$, если $\overline{u}$ является линейной комбинацией этой системы.

Утверждение 1.8. *Система* $(\overline{v_1}, \ldots, \overline{v_n})$ *линейно зависима* $\Leftrightarrow$ *один из ее векторов выражается через остальные.*

Доказательство.

- $\Leftarrow$ Пусть без ограничения общности $\overline{v_n}$ выражается через остальные векторы системы, тогда существуют коэффициенты $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{R}$ такие, что:

$$\overline{v_n} = \sum_{i=1}^{n-1} \alpha_i \overline{v_i}$$

Преобразуем это равенство:

$$\sum_{i=1}^{n-1} \alpha_i \overline{v_i} + (-1)\overline{v_n} = \overline{0}$$

Значит, система $(\overline{v_1}, \dots, \overline{v_n})$ линейно зависима.

$\Rightarrow$ Пусть без ограничения общности в нетривиальной линейной комбинации, равной $\overline{0}$, коэффициент α_n отличен от нуля. Тогда:

$$\sum_{i=1}^{n-1} \alpha_i \overline{v_i} + \alpha_n \overline{v_n} = \overline{0} \Rightarrow \overline{v_n} = \sum_{i=1}^{n-1} \left(-\frac{\alpha_i}{\alpha_n}\right) \overline{v_i}$$

Таким образом, вектор $\overline{v_n}$ выражается через остальные векторы системы. □

Утверждение 1.9. *Пусть система $(\overline{v_1}, \dots, \overline{v_n})$ векторов из V_n линейно независима, а система $(\overline{v_1}, \dots, \overline{v_{n+1}})$ — линейно зависима. Тогда вектор $\overline{v_{n+1}}$ выражается через $(\overline{v_1}, \dots, \overline{v_n})$.*

Доказательство. Так как система $(\overline{v_1}, \dots, \overline{v_{n+1}})$ линейно зависима, то существует нетривиальная линейная комбинация, равная $\overline{0}$, то есть существуют коэффициенты $\alpha_1, \dots, \alpha_{n+1} \in \mathbb{R}$ такие, что:

$$\sum_{i=1}^{n+1} \alpha_i \overline{v_i} = \overline{0}$$

Если $\alpha_{n+1} = 0$, то у $(\overline{v_1}, \dots, \overline{v_n})$ также существует равная $\overline{0}$ нетривиальная линейная комбинация, что противоречит условию линейной независимости. Значит, $\alpha_{n+1} \neq 0$, тогда:

$$\overline{v_{n+1}} = \sum_{i=1}^{n} \left(-\frac{\alpha_i}{\alpha_{n+1}}\right) \overline{v_i}$$ □

Определение 1.13. Система векторов из V_n называется:

- ▷ *Коллинеарной*, если все ее векторы параллельны одной прямой
- ▷ *Компланарной*, если все ее векторы параллельны одной плоскости

Векторы, образующие коллинеарную или компланарную систему, тоже называются *коллинеарными* или *компланарными* соответственно.

Утверждение 1.10. *Пусть $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in V_n$. Выполнены следующие свойства:*

1. *Если $\overline{a} \neq \overline{0}$ и вектор $\overline{b}$ коллинеарен вектору $\overline{a}$, то $\overline{b}$ выражается через $\overline{a}$*
2. *Если $\overline{a}, \overline{b}$ — неколлинеарные векторы и вектор $\overline{c}$ компланарен системе $(\overline{a}, \overline{b})$, то $\overline{c}$ выражается через $\overline{a}, \overline{b}$.*
3. *Если $\overline{a}, \overline{b}, \overline{c}$ — некомпланарные векторы, то $\overline{d}$ выражается через $\overline{a}, \overline{b}, \overline{c}$.*

Доказательство. Отложим векторы $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ от точки $O \in P_n$ и получим направленные отрезки $\overline{OA}, \overline{OB}, \overline{OC}, \overline{OD}$. Произведем следующие построения:

1. Если $\overline{a} \uparrow\uparrow \overline{b}$, то домножим $\overline{OA}$ на $\frac{|\overline{b}|}{|\overline{a}|}$, иначе — на $\left(-\frac{|\overline{b}|}{|\overline{a}|}\right)$, и получим $\overline{OB}$.

2. Проведем через C прямую l, параллельную $\overline{b}$. Пусть эта прямая пересекает OA в точке X. Тогда $\overline{OC} = \overline{OX} + \overline{XC}$, и по пункту (1) имеем, что $\overline{OX}$ выражается через $\overline{a}$, а $\overline{XC}$ — через $\overline{b}$.

3. Проведем через D плоскость α, параллельную $(\overline{a}, \overline{b})$. Пусть эта плоскость пересекает OC в точке X. Тогда $\overline{OD} = \overline{OX} + \overline{XD}$, и по пунктам (1) и (2) имеем, что $\overline{OX}$ выражается через $\overline{c}$, а $\overline{XD}$ — через $\overline{a}, \overline{b}$. □

Теорема 1.1. *Пусть $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in V_n$. Выполнены следующие свойства:*

1. Система $(\overline{a})$ линейно независима $\Leftrightarrow \overline{a} \neq \overline{0}$

2. Система $(\overline{a}, \overline{b})$ линейно независима $\Leftrightarrow$ она неколлинеарна

3. Система $(\overline{a}, \overline{b}, \overline{c})$ линейно независима $\Leftrightarrow$ она некомпланарна

4. Система $(\overline{a}, \overline{b}, \overline{c}, \overline{d})$ всегда линейно зависима

Доказательство.

1. $\Rightarrow$ Пусть $\overline{a} = \overline{0}$, тогда $1\overline{a} = \overline{0}$, и система $(\overline{a})$ линейно зависима.

   $\Leftarrow$ Если $\overline{a} \neq \overline{0}$, то при умножении этого вектора на любое число $\alpha \neq 0$ снова получится ненулевой вектор, то есть система $(\overline{a})$ линейно независима.

2. $\Rightarrow$ Пусть система $(\overline{a}, \overline{b})$ коллинеарна. Если $\overline{a} = \overline{0}$, то вся система линейно зависима по пункту (1), иначе — $\overline{b}$ выражается через $\overline{a}$, тогда система тоже линейно зависима.

   $\Leftarrow$ Пусть система $(\overline{a}, \overline{b})$ линейно зависима, тогда без ограничения общности $\overline{b}$ выражается через $\overline{a}$, то есть эти векторы коллинеарны.

3. $\Rightarrow$ Пусть система $(\overline{a}, \overline{b}, \overline{c})$ компланарна. Если система $(\overline{a}, \overline{b})$ коллинеарна, то вся система линейно зависима по пункту (2), иначе — $\overline{c}$ выражается через $\overline{a}, \overline{b}$, тогда система тоже линейно зависима.

   $\Leftarrow$ Пусть система $(\overline{a}, \overline{b}, \overline{c})$ линейно зависима, тогда без ограничения общности $\overline{c}$ выражается через $\overline{a}, \overline{b}$, то есть эти векторы компланарны. □

4. Если система $(\overline{a}, \overline{b}, \overline{c})$ компланарна, то вся система линейно зависима по пункту (3), иначе — $\overline{d}$ выражается через $\overline{a}, \overline{b}, \overline{c}$, тогда система тоже линейно зависима.

1.3 Базисы и координаты

Определение 1.14. *Базисом* в V_n называется линейно независимая система векторов, через которую выражаются все векторы V_n.

Утверждение 1.11. *Пусть $e = (\overline{e_1}, \ldots, \overline{e_n})$ — базис в V_n. Тогда для любого вектора $\overline{v} \in V_n$ существует единственный столбец коэффициентов α такой, что $\overline{v} = e\alpha$.*

Доказательство. По определению базиса, такой столбец α существует. Если также существует столбец $\alpha' \neq \alpha$, удовлетворяющий условию, то:

$$\overline{v} = e\alpha = e\alpha' \Rightarrow e(\alpha - \alpha') = \overline{0}$$

Так как e — линейно независимая система, то линейная комбинация $e(\alpha - \alpha')$ должна быть тривиальной, откуда $\alpha = \alpha'$. $\square$

Определение 1.15. Пусть e — базис в V_n, $\overline{v} = \alpha e \in V_n$. Столбец коэффициентов α называется *координатным столбцом* вектора $\overline{v}$ в базисе e. Обозначение — $\overline{v} \leftrightarrow_e \alpha$.

Утверждение 1.12 (линейность сопоставления координат)**.** *Для любых $\overline{u}, \overline{v} \in V_n$ таких, что $\overline{u} \leftrightarrow_e \alpha$, $\overline{v} \leftrightarrow_e \beta$, выполнено следующее:*

1. $\overline{u} + \overline{v} \leftrightarrow_e \alpha + \beta$
2. $\forall \lambda \in \mathbb{R} : \lambda\overline{u} \leftrightarrow_e \lambda\alpha$

Доказательство.

1. $\overline{u} + \overline{v} = e\alpha + e\beta = e(\alpha + \beta)$.
2. $\lambda\overline{u} = \lambda e\alpha = e(\lambda\alpha)$. $\square$

Теорема 1.2.

1. *Базис в V_0 не существует.*
2. *Базис в V_1 — это система из одного ненулевого вектора.*
3. *Базис в V_2 — это система из двух неколлинеарных векторов.*
4. *Базис в V_3 — это система из трех некомпланарных векторов.*

Доказательство.

1. Единственный вектор в V_0 — это $\overline{0}$, и он образует линейно зависимую систему.
2. В V_1 любая система из $\geqslant 2$ векторов коллинеарна и потому линейно зависима. При этом вектор $\overline{a} \neq \overline{0}$ образует линейно независимую систему, и через него выражаются все векторы V_1. Если же $\overline{a} = \overline{0}$, то он образует линейно зависимую систему.
3. В V_2 любая система из $\geqslant 3$ векторов компланарна и потому линейно зависима, а система из одного вектора коллинеарна и потому выражает не все векторы из V_2. При этом неколлинеарная система $(\overline{a}, \overline{b})$ линейно независима, и через нее выражаются все векторы из V_2. Если же система $(\overline{a}, \overline{b})$ коллинеарна, то она линейно зависима.
4. В V_3 любая система из $\geqslant 4$ векторов линейно зависима, а система из $\leqslant 2$ векторов компланарна и потому выражает не все векторы из V_3. При этом некомпланарная система $(\overline{a}, \overline{b}, \overline{c})$ линейно независима, и через нее выражаются все векторы из V_3. Если же система $(\overline{a}, \overline{b}, \overline{c})$ компланарна, то она линейно зависима. $\square$

Замечание. Из теоремы выше, в частности, следует, что базис в V_n состоит ровно из n векторов при $n \in \{1, 2, 3\}$.

Определение 1.16. Пусть e, e' — базисы в V_n. Тогда каждый вектор из e' раскладывается по базису e, то есть имеет место представление $e' = eS$ для некоторой матрицы $S \in M_i$. Матрица S называется *матрицей перехода* от базиса e к базису e'.

Теорема 1.3. *Пусть e, e' — базисы в V_n, $e' = eS$, и пусть $\overline{v} \in V_n$, $\overline{v} \leftrightarrow_e \alpha$, $\overline{v} \leftrightarrow_{e'} \alpha'$. Тогда:*

$$\alpha = S\alpha'$$

Доказательство. Заметим, что выполнены равенства $\overline{v} = e\alpha = e'\alpha' = eS\alpha'$. Значит, вектор $\overline{v}$ имеет в базисе e координатные столбцы α и $S\alpha'$, но разложение вектора по базису единственно, поэтому $\alpha = S\alpha'$. □

Утверждение 1.13. *Пусть e, e' и e'' — базисы в V_n, а матрицы перехода S_1, S_2 и S_3 таковы, что $e' = eS_1$, $e'' = e'S_2$, $e'' = eS_3$. Тогда:*

$$S_3 = S_1 S_2$$

Доказательство. Выполнены равенства $e'' = e'S_2 = eS_1S_2$, и при этом $e'' = eS_3$, но каждый из координатных столбцов векторов $\overline{e''_1}, \ldots, \overline{e''_i}$ в базисе e единственен, поэтому $S_1S_2 = S_3$. □

Определение 1.17. Базис в V_n называется:

- ▷ *Ортогональным*, если его векторы попарно ортогональны
- ▷ *Ортонормированным*, если он ортогонален и все его векторы имеют длину 1

Определение 1.18. *Декартовой системой координат* в P_n называется набор (O, e), где $O \in P_n$ — *начало системы координат*, e — базис в V_n. Точка $A \in P_n$ имеет координатный столбец α в данной системе координат, если $\overline{OA} \leftrightarrow_e \alpha$. Обозначение — $A \leftrightarrow_{(O,e)} \alpha$. Декартова система координат называется *прямоугольной*, если базис e — ортонормированный.

Утверждение 1.14. *Пусть $A \leftrightarrow_{(O,e)} \alpha$, $B \leftrightarrow_{(O,e)} \beta$. Тогда:*

$$\overline{AB} \leftrightarrow_e \beta - \alpha$$

Доказательство. Выполнены равенства $\overline{AB} = \overline{OB} - \overline{OA} = e\beta - e\alpha = e(\beta - \alpha)$. □

Утверждение 1.15. *Пусть $A \leftrightarrow_{(O,e)} \alpha$, $B \leftrightarrow_{(O,e)} \beta$, и $C \in AB$ — такая точка на отрезке AB, что $AC : BC = \lambda : (1 - \lambda)$ для некоторого $\lambda \in (0, 1)$. Тогда:*

$$C \leftrightarrow_{(O,e)} (1 - \lambda)\alpha + \lambda\beta$$

Доказательство. По условию, $\overline{AC} = \lambda\overline{AB}$, тогда:

$$\overline{OC} = \overline{OA} + \overline{AC} = \overline{OA} + \lambda\overline{AB} = e\alpha + \lambda e(\beta - \alpha) = e((1 - \lambda)\alpha + \lambda\beta)$$ □

Теорема 1.4. *Пусть (O, e), (O', e') — декартовы системы координат в P_n такие, что $e' = eS$ и $O' \leftrightarrow_{(O,e)} \gamma$. Тогда, если $A \leftrightarrow_{(O,e)} \alpha$ и $A \leftrightarrow_{(O',e')} \alpha'$, то:*

$$\alpha = S\alpha' + \gamma$$

Доказательство. Выполнены равенства $\overline{OA} = e\alpha = \overline{OO'} + \overline{O'A} = e\gamma + e'\alpha' = e\gamma + eS\alpha'$. Тогда, в силу единственности координатного столбца вектора $\overline{OA}$ в базисе e, получим, что $\alpha = S\alpha' + \gamma$. □

2 Произведения векторов

2.1 Скалярное произведение

Определение 2.1. *Скалярным произведением* ненулевых векторов $\overline{a}, \overline{b} \in V_n$ называется следующая величина:

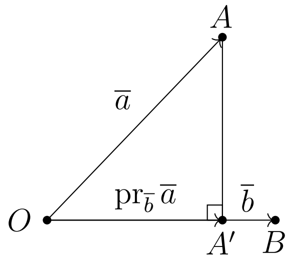
$$(\overline{a}, \overline{b}) := |\overline{a}||\overline{b}| \cos \angle(\overline{a}, \overline{b})$$

Если один из векторов $\overline{a}, \overline{b}$ — нулевой, то скалярное произведение $(\overline{a}, \overline{b})$ считается равным 0. Другое обозначение скалярного произведения — $\overline{a} \cdot \overline{b}$.

Определение 2.2. Векторы $\overline{a}, \overline{b} \in V_n$ называются *перпендикулярными*, если $(\overline{a}, \overline{b}) = 0$. Обозначение — $\overline{a} \perp \overline{b}$.

Замечание. Векторы $\overline{a}, \overline{b} \in V_n$ перпендикулярны $\Leftrightarrow$ либо один из векторов — нулевой, либо $\angle(\overline{a}, \overline{b}) = \frac{\pi}{2}$. Кроме того, $\forall \overline{a} \in V_n : (\overline{a},\overline{a}) = |\overline{a}|^2$.

Определение 2.3. Пусть $\overline{a}, \overline{b} \in V_n$, $\overline{b} \neq \overline{0}$, от точки $O \in P_n$ отложены направленные отрезки $\overline{OA} = \overline{a}$ и $\overline{OB} = \overline{b}$. *Проекцией вектора $\overline{a}$ на вектор $\overline{b}$* называется такой класс эквивалентности, представителем которого является вектор $\overline{OA'}$, где A' — ортогональная проекция точки A на прямую OB.



Обозначение — $\mathrm{pr}_{\overline{b}}\,\overline{a}$.

Утверждение 2.1 (линейность проекции)**.** *Для любых $\overline{a}, \overline{b} \in V_n$, $\overline{b} \neq \overline{0}$, выполнено следующее:*

1. $\mathrm{pr}_{\overline{b}}(\overline{a_1} + \overline{a_2}) = \mathrm{pr}_{\overline{b}}\,\overline{a_1} + \mathrm{pr}_{\overline{b}}\,\overline{a_2}$
2. $\forall \lambda \in \mathbb{R} : \mathrm{pr}_{\overline{b}}(\lambda\overline{a}) = \lambda\,\mathrm{pr}_{\overline{b}}\,\overline{a}$

Доказательство.

1. Пусть $\overline{OA_1} = \overline{a_1}$, $\overline{A_1A_2} = \overline{a_2}$, $\overline{OB} = \overline{b}$. Проведем через A_1 прямую l, параллельную отрезку OB. Пусть A_1' — ортогональная проекция точки A_1 на OB, A_2' — ортогональная проекция точки A_2 на l, A_2'' — ортогональная проекция точки A_2' на OB. Тогда $l \perp (A_2A_2'A_2'')$, и, следовательно, $OB \perp A_2A_2''$. Значит, $\overline{OA_2''} = \mathrm{pr}_{\overline{b}}(\overline{a_1} + \overline{a_2})$, при этом $\overline{OA_2''} = \overline{OA_1} + \overline{A_1A_2''} = \overline{OA_1'} + \overline{A_1A_2'} = \mathrm{pr}_{\overline{b}}\,\overline{a_1} + \mathrm{pr}_{\overline{b}}\,\overline{a_2}$.

2. Если $\lambda = 0$, то утверждение, очевидно, верно. Пусть теперь $\lambda \neq 0$, тогда рассмотрим направленные отрезки $\overline{OA_1} = \overline{a}$, $\overline{OA_2} = \lambda\overline{a}$, $\overline{OB} = \overline{b}$. Пусть A_1' — ортогональная проекция точки A_1 на OB, A_2' — ортогональная проекция точки A_2 на OB. По определению умножения вектора на скаляр, $\triangle A_1OA_1' \sim \triangle A_2OA_2'$, причем коэффициент подобия равен $|\lambda|$, откуда $\overline{OA_2'} = \lambda\overline{OA_1'}$, то есть $\mathrm{pr}_{\overline{b}}(\lambda\overline{a}) = \lambda\,\mathrm{pr}_{\overline{b}}\,\overline{a}$. □

Замечание. Для любых $\overline{a}, \overline{b} \in V_n$, $\overline{b} \neq \overline{0}$, выполнены следующие равенства:

$$(\overline{a}, \overline{b}) = |\overline{a}||\overline{b}| \cos \angle(\overline{a}, \overline{b}) = \begin{cases} |\overline{b}|| \operatorname{pr}_{\overline{b}} \overline{a}|, & \text{если } \angle(\overline{a}, \overline{b}) < \frac{\pi}{2} \\ 0, & \text{если } \angle(\overline{a}, \overline{b}) = \frac{\pi}{2} \\ -|\overline{b}|| \operatorname{pr}_{\overline{b}} \overline{a}|, & \text{если } \angle(\overline{a}, \overline{b}) > \frac{\pi}{2} \end{cases}$$

В каждом из случаев выполнено равенство $(\overline{a}, \overline{b}) = (\operatorname{pr}_{\overline{b}} \overline{a}, \overline{b})$.

Утверждение 2.2. *Для любых $\overline{a}, \overline{b} \in V_n$, $\overline{b} \neq \overline{0}$, выполнено следующее равенство:*

$$\operatorname{pr}_{\overline{b}} \overline{a} = \frac{(\overline{a}, \overline{b})}{|\overline{b}|^2} \overline{b}$$

Доказательство. Поскольку $\operatorname{pr}_{\overline{b}} \overline{a} \parallel \overline{b}$, то $\operatorname{pr}_{\overline{b}} \overline{a}$ выражается через $\overline{b}$, то есть $\operatorname{pr}_{\overline{b}} \overline{a} = \lambda \overline{b}$ для некоторого $\lambda \in \mathbb{R}$. Тогда:

$$(\overline{a}, \overline{b}) = (\operatorname{pr}_{\overline{b}} \overline{a}, \overline{b}) = (\lambda \overline{b}, \overline{b}) = \lambda |\overline{b}|^2 \Rightarrow \lambda = \frac{(\overline{a}, \overline{b})}{|\overline{b}|^2}$$

Таким образом, $\operatorname{pr}_{\overline{b}} \overline{a} = \lambda \overline{b} = \frac{(\overline{a}, \overline{b})}{|\overline{b}|^2} \overline{b}$. □

Теорема 2.1. *Скалярное произведение обладает следующими свойствами:*

1. $\forall \overline{a} \in V_n : \overline{a} \neq \overline{0} \Leftrightarrow (\overline{a}, \overline{a}) > 0$
2. $\forall \overline{a}, \overline{b} \in V_n : (\overline{a}, \overline{b}) = (\overline{b}, \overline{a})$ *(симметричность)*
3. $\forall \overline{a_1}, \overline{a_2}, \overline{b} \in V_n : (\overline{a_1} + \overline{a_2}, \overline{b}) = (\overline{a_1}, \overline{b}) + (\overline{a_2}, \overline{b})$
   $\forall \lambda \in \mathbb{R} : \forall \overline{a}, \overline{b} \in V_n : (\lambda \overline{a}, \overline{b}) = \lambda (\overline{a}, \overline{b})$ *(линейность по первому аргументу)*

Доказательство.

1. $\overline{a} \neq \overline{0} \Leftrightarrow |\overline{a}| > 0 \Leftrightarrow (\overline{a}, \overline{a}) = |\overline{a}|^2 > 0$
2. $(\overline{a}, \overline{b}) = |\overline{a}||\overline{b}| \cos \angle(\overline{a}, \overline{b}) = (\overline{b}, \overline{a})$
3. Для случаев, когда $\overline{b} = \overline{0}$ или $\overline{a_1} \parallel \overline{a_2} \parallel \overline{b}$, утверждение, очевидно, верно. В других случаях воспользуемся следующими равенствами:

   $$(\overline{a_1} + \overline{a_2}, \overline{b}) = (\operatorname{pr}_{\overline{b}}(\overline{a_1} + \overline{a_2}), \overline{b}) = (\operatorname{pr}_{\overline{b}} \overline{a_1} + \operatorname{pr}_{\overline{b}} \overline{a_2}, \overline{b})$$

   Так как $\operatorname{pr}_{\overline{b}} \overline{a_1} \parallel \operatorname{pr}_{\overline{b}} \overline{a_2} \parallel \overline{b}$, то:

   $$(\operatorname{pr}_{\overline{b}} \overline{a_1} + \operatorname{pr}_{\overline{b}} \overline{a_2}, \overline{b}) = (\operatorname{pr}_{\overline{b}} \overline{a_1}, \overline{b}) + (\operatorname{pr}_{\overline{b}} \overline{a_2}, \overline{b}) = (\overline{a_1}, \overline{b}) + (\overline{a_2}, \overline{b})$$

   Доказательство второй части свойства аналогично. □

Замечание. Линейность скалярного произведения относительно второго аргумента также верна в силу симметричности.

Утверждение 2.3. *Пусть e — ортонормированный базис в V_n, $\overline{v} \in V_n$, $\overline{v} \leftrightarrow_e \alpha$. Тогда для любого $i \in \{1, \ldots, n\}$ выполнено равенство $\alpha_i = (\overline{e_i}, \overline{v})$.*

Доказательство. В силу линейности скалярного произведения, имеем:

$$(\overline{e_i}, \overline{v}) = \left(\overline{e_i}, \sum_{j=1}^{n} \alpha_j \overline{e_j}\right) = \sum_{j=1}^{n} \alpha_j (\overline{e_i}, \overline{e_j})$$

Так как для любых $i, j \in \{1, \ldots, n\}$ верно, что $(\overline{e_i}, \overline{e_j}) = 0$ при $i \neq j$ и $(\overline{e_i}, \overline{e_j}) = 1$ при $i = j$, то выполнены следующие равенства:

$$(\overline{e_i}, \overline{v}) = \sum_{j=1}^{n} \alpha_j (\overline{e_i}, \overline{e_j}) = \alpha_i$$

Получено требуемое. $\square$

Утверждение 2.4. *Пусть e — ортонормированный базис в V_n, $\overline{a}, \overline{b} \in V_n$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$. Тогда выполнены следующие равенства:*

$$(\overline{a}, \overline{b}) = \alpha^T \beta = \sum_{i=1}^{n} \alpha_i \beta_i$$

Доказательство. Аналогично предыдущему утверждению, выполнено следующее:

$$(\overline{a}, \overline{b}) = \left(\sum_{i=1}^{n} \alpha_i \overline{e_i}, \sum_{j=1}^{n} \beta_j \overline{e_j}\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j (\overline{e_i}, \overline{e_j}) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j (\overline{e_i}, \overline{e_j}) = \sum_{i=1}^{n} \alpha_i \beta_i$$

Получено требуемое. $\square$

Определение 2.4. Пусть $e = (\overline{e_1}, \ldots, \overline{e_n})$ — базис в V_n. *Матрицей Грама* называется следующая матрица:

$$\Gamma := ((\overline{e_i}, \overline{e_j})) = \begin{pmatrix} (\overline{e_1}, \overline{e_1}) & (\overline{e_1}, \overline{e_2}) & \ldots & (\overline{e_1}, \overline{e_n}) \\ (\overline{e_2}, \overline{e_1}) & (\overline{e_2}, \overline{e_2}) & \ldots & (\overline{e_2}, \overline{e_n}) \\ \vdots & \vdots & \ddots & \vdots \\ (\overline{e_n}, \overline{e_1}) & (\overline{e_n}, \overline{e_2}) & \ldots & (\overline{e_n}, \overline{e_n}) \end{pmatrix}$$

Утверждение 2.5. *Пусть e — базис в V_n, $\overline{a}, \overline{b} \in V_n$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$. Тогда выполнены следующие равенства:*

$$(\overline{a}, \overline{b}) = \alpha^T \Gamma \beta$$

Доказательство. Выполнены следующие равенства:

$$\alpha^T(\Gamma\beta) = \alpha^T \begin{pmatrix} \sum_{j=1}^{n} \beta_j (\overline{e_1}, \overline{e_j}) \\ \sum_{j=1}^{n} \beta_j (\overline{e_2}, \overline{e_j}) \\ \vdots \\ \sum_{j=1}^{n} \beta_j (\overline{e_n}, \overline{e_j}) \end{pmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j (\overline{e_i}, \overline{e_j}) = \left(\sum_{i=1}^{n} \alpha_i \overline{e_i}, \sum_{j=1}^{n} \beta_j \overline{e_j}\right) = (\overline{a}, \overline{b})$$

Получено требуемое. $\square$

Утверждение 2.6. *Пусть e — ортонормированный базис в V_n, $\overline{a}, \overline{b} \in V_n$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$. Тогда выполнены следующие равенства:*

1. $|\overline{a}| = \sqrt{\alpha^T \alpha}$
2. *Если* $\overline{a}, \overline{b} \neq \overline{0}$, *то* $\cos\angle(\overline{a}, \overline{b}) = \frac{\alpha^T \beta}{|\overline{a}||\overline{b}|}$

Доказательство.

1. $|\overline{a}|^2 = (\overline{a}, \overline{a}) \Rightarrow |\overline{a}| = \sqrt{(\overline{a}, \overline{a})} = \sqrt{\alpha^T \alpha}$
2. $(\overline{a}, \overline{b}) = |\overline{a}||\overline{b}| \cos\angle(\overline{a}, \overline{b}) \Rightarrow \cos\angle(\overline{a}, \overline{b}) = \frac{(\overline{a}, \overline{b})}{|\overline{a}||\overline{b}|} = \frac{\alpha^T \beta}{|\overline{a}||\overline{b}|}$ □

Утверждение 2.7. *Пусть (O, e) — прямоугольная декартова система координат в P_n, $A, B \in P_n$, $A \leftrightarrow_{(O,e)} \alpha$, $B \leftrightarrow_{(O,e)} \beta$. Тогда:*

$$AB = \sqrt{(\beta - \alpha)^T (\beta - \alpha)}$$

Доказательство. Заметим, что $\overline{AB} \leftrightarrow_e \beta - \alpha$, тогда:

$$AB = \sqrt{(\overline{AB}, \overline{AB})} = \sqrt{(\beta - \alpha)^T (\beta - \alpha)}$$ □

Определение 2.5. Матрица $S \in M_n$ называется *ортогональной*, если $S^T S = E$.

Утверждение 2.8. *Пусть e — ортонормированный базис в V_n, e' — произвольный базис в V_n, $e' = eS$. Тогда базис e' — ортонормированный $\Leftrightarrow$ матрица S — ортогональная.*

Доказательство. Столбцы S — это координатные столбцы векторов e' в базисе e. Так как e — ортонормированный, то $S^T S$ — это матрица Грама для e'. Значит, e' — ортонормированный $\Leftrightarrow \Gamma = S^T S = E \Leftrightarrow S$ — ортогональная. □

2.2 Ориентированные площадь и объем

Определение 2.6. Пусть плоскость P_2 вложена в пространство P_3, и выделено одно из полупространств в P_3 относительно этой плоскости. Базис $(\overline{a}, \overline{b})$ в V_2 называется *положительно ориентированным*, если поворот на кратчайший угол, который переводит вектор $\overline{a}$ в вектор $\overline{a'} \parallel \overline{b}$, происходит против часовой стрелки при взгляде из выделенного полупространства. В противном случае базис называется *отрицательно ориентированным.*

Замечание. Базисы $(\overline{a}, \overline{b})$ и $(\overline{b}, \overline{a})$ всегда ориентированы по-разному.

Определение 2.7. Базис $(\overline{a}, \overline{b}, \overline{c})$ в V_3 называется *правой тройкой*, если базис $(\overline{a}, \overline{b})$ в плоскости V_2, содержащей эти два вектора, ориентирован положительно относительно полупространства, содержащего вектор $\overline{c}$, отложенный от точки в P_2. В противном случае базис называется *левой тройкой.*

Утверждение 2.9.

1. *Базисы $(\overline{a}, \overline{b}, \overline{c})$ и $(\overline{b}, \overline{a}, \overline{c})$ в V_3 всегда ориентированы по-разному.*
2. *Базисы $(\overline{a}, \overline{b}, \overline{c})$ и $(\overline{a}, \overline{c}, \overline{b})$ в V_3 всегда ориентированы по-разному.*

Доказательство.

1. Так как базисы $(\overline{a}, \overline{b})$ и $(\overline{b}, \overline{a})$ ориентированы по-разному, то базисы $(\overline{a}, \overline{b}, \overline{c})$ и $(\overline{b}, \overline{a}, \overline{c})$ тоже ориентированы по-разному.

2. Пусть $\overline{OA} = \overline{a}$, $\overline{OB} = \overline{b}$, $\overline{OC} = \overline{c}$. Будем поворачивать направленный отрезок $\overline{OC}$ в плоскости (BOC), пока он не перейдет в такой направленный отрезок $\overline{OC'}$, что C и C' лежат по разные стороны от OB. Ориентация базиса $(\overline{a}, \overline{b}, \overline{c'})$ противоположна ориентации $(\overline{a}, \overline{b}, \overline{c})$, но совпадает с ориентацией $(\overline{a}, \overline{c}, \overline{b})$. □

Замечание. В силу утверждения выше, всевозможные перестановки базиса $(\overline{a}, \overline{b}, \overline{c})$ делятся на два класса противоположной ориентации:

▷ $(\overline{a}, \overline{b}, \overline{c})$, $(\overline{c}, \overline{a}, \overline{b})$ и $(\overline{b}, \overline{c}, \overline{a})$

▷ $(\overline{b}, \overline{a}, \overline{c})$, $(\overline{c}, \overline{b}, \overline{a})$ и $(\overline{a}, \overline{c}, \overline{b})$

Определение 2.8. Пусть $\overline{a}, \overline{b} \in V_2$, и в плоскости V_2 задана ориентация. *Ориентированной площадью* $S(\overline{a}, \overline{b})$ называется площадь параллелограмма, построенного на этих векторах, взятая со знаком, соответствующим ориентации $(\overline{a}, \overline{b})$.

Определение 2.9. Пусть $\overline{a}, \overline{b}, \overline{c} \in V_3$. *Ориентированным объемом* $V(\overline{a}, \overline{b}, \overline{c})$ называется объем параллелепипеда, построенного на этих векторах, взятая со знаком, соответствующим ориентации $(\overline{a}, \overline{b}, \overline{c})$. Эта величина также называется *смешанным произведением* векторов $\overline{a}, \overline{b}, \overline{c}$ и обозначается через $(\overline{a}, \overline{b}, \overline{c})$.

Замечание. Определения выше корректны, поскольку в них не требуется определять ориентацию набора векторов, не являющегося базисом:

1. $S(\overline{a}, \overline{b}) = 0 \Leftrightarrow \overline{a}$ и $\overline{b}$ коллинеарны.
2. $V(\overline{a}, \overline{b}, \overline{c}) = 0 \Leftrightarrow \overline{a}$, $\overline{b}$ и $\overline{c}$ компланарны.

Утверждение 2.10.

1. *Если базис $e = (\overline{e_1}, \overline{e_2})$ в V_2 — ортонормированный, то $S(\overline{e_1}, \overline{e_2}) = \pm 1$.*
2. *Если базис $e = (\overline{e_1}, \overline{e_2}, \overline{e_3})$ в V_3 — ортонормированный, то $V(\overline{e_1}, \overline{e_2}, \overline{e_3}) = \pm 1$.*

Доказательство.

1. Параллелограмм, образованный векторами $\overline{e_1}$ и $\overline{e_2}$, — это квадрат со стороной 1, поэтому $|S(\overline{e_1}, \overline{e_2})| = 1$.
2. Параллелепипед, образованный векторами $\overline{e_1}$, $\overline{e_2}$ и $\overline{e_3}$, — это куб со стороной 1, поэтому $|V(\overline{e_1}, \overline{e_2}, \overline{e_3})| = 1$. □

Теорема 2.2. *Ориентированный объем обладает следующими свойствами:*

1. $\forall \overline{a}, \overline{b}, \overline{c} \in V_n : V(\overline{a}, \overline{b}, \overline{c}) = -V(\overline{b}, \overline{a}, \overline{c}) = -V(\overline{a}, \overline{c}, \overline{b})$ *(кососимметричность)*
2. $\forall \overline{a_1}, \overline{a_2}, \overline{b}, \overline{c} \in V_n : V(\overline{a}, \overline{b}, \overline{c_1} + \overline{c_2}) = V(\overline{a}, \overline{b}, \overline{c_1}) + V(\overline{a}, \overline{b}, \overline{c_2})$
   $\forall \lambda \in \mathbb{R} : \forall \overline{a}, \overline{b}, \overline{c} \in V_n : V(\overline{a}, \overline{b}, \lambda\overline{c}) = \lambda V(\overline{a}, \overline{b}, \overline{c})$ *(линейность по третьему аргументу)*

Доказательство.

1. Если $\overline{a}$, $\overline{b}$ и $\overline{c}$ компланарны, то утверждение очевидно. Иначе — объем параллепипеда при перестановке векторов базиса не меняется по модулю, но меняет знак при смене ориентации.

2. Если $\overline{a}$ и $\overline{b}$ коллинеарны, то утверждение очевидно. Пусть теперь это не так, тогда рассмотрим направленные отрезки $\overline{OA} = \overline{a}$, $\overline{OB} = \overline{b}$, $\overline{OC} = \overline{c}$. Обозначим через $\overline{d}$ вектор такой, что $|\overline{d}| = 1$, $\overline{d} \perp (AOB)$ и $(\overline{a}, \overline{b}, \overline{d})$ — правая тройка, и пусть $\overline{OD} = \overline{d}$.

   Заметим теперь, что $\forall \overline{c} \in V_n : V(\overline{a}, \overline{b}, \overline{c}) = |S(\overline{a}, \overline{b})|(\overline{c}, \overline{d})$, поскольку выполнены равенства $(\overline{c}, \overline{d}) = (\operatorname{pr}_{\overline{d}} \overline{c}, \overline{d}) = \pm|\operatorname{pr}_{\overline{d}} \overline{c}| = \pm h$, где h — высота параллелепипеда, а знак соответствует ориентации базиса $(\overline{a}, \overline{b}, \overline{c})$. Тогда линейность ориентированного объема следует из линейности скалярного произведения. □

Замечание. Линейность ориентированного объема по первому и второму аргументам также верна в силу кососимметричности. Кроме того, как было отмечено в доказательстве, свойство кососимметричности можно записать следующим образом: при любой перестановке тройки векторов ее ориентированный объем сохраняется по модулю, но меняет знак при смене ориентации.

Замечание. Аналогичным образом доказываются свойства кососимметричности и линейности ориентированной площади.

Определение 2.10. Пусть $A = (a_{ij}) \in M_n$, $n \in \{1, 2, 3\}$. *Определителем*, или *детерминантом*, матрицы A называется следующая величина:

- ▷ $\det A := a_{11}$ при $n = 1$
- ▷ $\det A := a_{11}a_{22} - a_{12}a_{21}$ при $n = 2$
- ▷ $\det A := a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$ при $n = 3$

Другое обозначение для определителя имеет следующий вид:

$$\det A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Замечание. Более общее определение определителя для произвольного $n \in \mathbb{N}$ будет дано далее в курсе.

Теорема 2.3. *Пусть $e = (\overline{e_1}, \overline{e_2})$ — базис в V_2, $\overline{a}, \overline{b} \in V_2$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$. Тогда верно следующее равенство:*

$$S(\overline{a}, \overline{b}) = \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{vmatrix} S(\overline{e_1}, \overline{e_2})$$

Доказательство. В силу линейности ориентированной площади, имеем:

$$S(\overline{a}, \overline{b}) = S\left(\sum_{i=1}^{2} \alpha_i \overline{e_i}, \sum_{j=1}^{2} \beta_j \overline{e_j}\right) = \sum_{i=1}^{2} \sum_{j=1}^{2} \alpha_i \beta_j S(\overline{e_i}, \overline{e_j})$$

Поскольку для любого $i \in \{1, 2\}$ выполнено $S(\overline{e_i}, \overline{e_i}) = 0$, то:

$$S(\overline{a}, \overline{b}) = \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{vmatrix} S(\overline{e_1}, \overline{e_2})$$

Получено требуемое. □

Теорема 2.4. *Пусть* $e = (\overline{e_1}, \overline{e_2}, \overline{e_3})$ — *базис в* V_3, $\overline{a}, \overline{b}, \overline{c} \in V_3$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$, $\overline{c} \leftrightarrow_e \gamma$. *Тогда верно следующее равенство:*

$$V(\overline{a}, \overline{b}, \overline{c}) = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix} V(\overline{e_1}, \overline{e_2}, \overline{e_3})$$

Доказательство. В силу линейности ориентированного объема, имеем:

$$V(\overline{a}, \overline{b}, \overline{c}) = V\left(\sum_{i=1}^{3} \alpha_i \overline{e_i}, \sum_{j=1}^{3} \beta_j \overline{e_j}, \sum_{k=1}^{3} \gamma_k \overline{e_k}\right) = \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} \alpha_i \beta_j \gamma_k V(\overline{e_i}, \overline{e_j}, \overline{e_k})$$

Поскольку для любых $i, j, k \in \{1, 2, 3\}$ таких, что $i = j$, $i = k$ или $j = k$, выполнено $V(\overline{e_i}, \overline{e_j}, \overline{e_k}) = 0$, то:

$$V(\overline{a}, \overline{b}, \overline{c}) = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix} V(\overline{e_1}, \overline{e_2}, \overline{e_3})$$

Получено требуемое. □

Замечание. Из теорем выше следуют, в частности, такие свойства:

- ▷ Если e — положительно ориентированный ортонормированный базис в V_2, то для любых $\overline{a}, \overline{b} \in V_2$ таких, что $\overline{a} \leftrightarrow_e \alpha$ и $\overline{b} \leftrightarrow_e \beta$, верно равенство $S(\overline{a}, \overline{b}) = |\alpha\beta|$.
- ▷ Если e — правый ортонормированный базис в V_3, то для любых $\overline{a}, \overline{b}, \overline{c} \in V_3$ таких, что $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$ и $\overline{c} \leftrightarrow_e \gamma$, верно равенство $V(\overline{a}, \overline{b}, \overline{c}) = |\alpha\beta\gamma|$.
- ▷ Если e — базис в V_2, $\overline{a}, \overline{b} \in V_2$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$, то векторы $\overline{a}$ и $\overline{b}$ коллинеарны $\Leftrightarrow$ $|\alpha\beta| = 0$.
- ▷ Если e — базис в V_3, $\overline{a}, \overline{b}, \overline{c} \in V_3$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$, $\overline{c} \leftrightarrow_e \gamma$, то векторы $\overline{a}$, $\overline{b}$ и $\overline{c}$ компланарны $\Leftrightarrow$ $|\alpha\beta\gamma| = 0$.

Определение 2.11. Пусть $A = (a_{ij}) \in M_3$, $b = (b_i) \in M_{3\times 1}$. *Системой линейных уравнений* $Ax = b$ называется следующая система:

$$\begin{cases} a_{11}x + a_{12}y + a_{13}z = b_1 \\ a_{21}x + a_{22}y + a_{23}z = b_2 \\ a_{31}x + a_{32}y + a_{33}z = b_3 \end{cases}$$

Теорема 2.5 (правило Крамера). *Пусть* $A \in M_3$, *причем* $\Delta := \det A \neq 0$. *Обозначим через* $\Delta_x, \Delta_y, \Delta_z$ *определители матриц, полученных заменой столбца коэффициентов при соответствующей переменной на столбец* b. *Тогда система* $Ax = b$ *имеет единственное решение* (x, y, z), *и это решение имеет следующий вид:*

$$(x, y, z) := \left(\frac{\Delta_x}{\Delta}, \frac{\Delta_y}{\Delta}, \frac{\Delta_z}{\Delta}\right)$$

Доказательство. Пусть e — правый ортонормированный базис в V_3. Рассмотрим векторы $\overline{v_1}, \overline{v_2}, \overline{v_2}, \overline{u} \in V_3$ такие, что для каждого $i \in \{1, 2, 3\}$ выполнено $\overline{v_i} \leftrightarrow_e a_{*i}$, и $\overline{u} \leftrightarrow_e b$. Тогда

$Ax = b \Leftrightarrow x\overline{v_1} + y\overline{v_2} + z\overline{v_3} = \overline{u}$. Поскольку $\Delta \neq 0$, то векторы $\overline{v_1}$, $\overline{v_2}$ и $\overline{v_3}$ некомпланарны и потому образуют базис в V_3. Значит, существует единственное решение (x, y, z) уравнения $x\overline{v_1} + y\overline{v_2} + z\overline{v_3} = \overline{u}$, и это решение имеет следующий вид:

$$\begin{aligned}
\Delta_x &= V(\overline{u}, \overline{v_2}, \overline{v_3}) = V(x\overline{v_1} + y\overline{v_2} + z\overline{v_3}, \overline{v_2}, \overline{v_3}) = xV(\overline{v_1}, \overline{v_2}, \overline{v_3})\\
\Delta_y &= V(\overline{v_1}, \overline{u}, \overline{v_3}) = V(\overline{v_1}, x\overline{v_1} + y\overline{v_2} + z\overline{v_3}, \overline{v_3}) = yV(\overline{v_1}, \overline{v_2}, \overline{v_3})\\
\Delta_z &= V(\overline{v_1}, \overline{v_2}, \overline{u}) = V(\overline{v_1}, \overline{v_2}, x\overline{v_1} + y\overline{v_2} + z\overline{v_3}) = zV(\overline{v_1}, \overline{v_2}, \overline{v_3})
\end{aligned}$$

Следовательно, $x = \frac{\Delta_x}{\Delta}$, $y = \frac{\Delta_y}{\Delta}$ и $z = \frac{\Delta_z}{\Delta}$. □

Замечание. Аналогичное правило для произвольного $n \in \mathbb{N}$ будет сформулировано далее в курсе. Отметим также, что если $\det A = 0$, то система $(\overline{v_1}, \overline{v_2}, \overline{v_3})$ из доказательства выше линейно зависима, тогда решений либо нет, либо их бесконечно много.

2.3 Векторное произведение

Определение 2.12. Пусть $\overline{a}, \overline{b} \in V_3$. *векторным произведением* векторов $\overline{a}$ и $\overline{b}$ называется единственный вектор $\overline{c} := [\overline{a}, \overline{b}]$ такой, что выполнены следующие условия:

1. $\overline{c} \perp \overline{a}$, $\overline{c} \perp \overline{b}$
2. $|\overline{c}| = |S(\overline{a}, \overline{b})|$
3. $(\overline{a}, \overline{b}, \overline{c})$ — правая тройка

Другое обозначение — $\overline{a} \times \overline{b}$.

Замечание. Выполнены следующие равносильности:

$$\overline{a} \parallel \overline{b} \Leftrightarrow S(\overline{a}, \overline{b}) = 0 \Leftrightarrow |[\overline{a}, \overline{b}]| = 0 \Leftrightarrow [\overline{a}, \overline{b}] = \overline{0}$$

Теорема 2.6. *Для любых $\overline{a}, \overline{b}, \overline{c} \in V_3$ выполнены равенства $(\overline{a}, \overline{b}, \overline{c}) = ([\overline{a}, \overline{b}], \overline{c}) = (\overline{a}, [\overline{b}, \overline{c}])$.*

Доказательство. Докажем первое равенство. Если $\overline{a} \parallel \overline{b}$, то $(\overline{a}, \overline{b}, \overline{c}) = ([\overline{a}, \overline{b}], \overline{c}) = 0$. Если же $\overline{a} \nparallel \overline{b}$, то выберем такой вектор $\overline{d}$, что $[\overline{a}, \overline{b}] = |S(\overline{a}, \overline{b})|\overline{d}$. Тогда, как уже доказывалось, $(\overline{a}, \overline{b}, \overline{c}) = |S(\overline{a}, \overline{b})|(\overline{c}, \overline{d})$, откуда:

$$(\overline{a}, \overline{b}, \overline{c}) = (|S(\overline{a}, \overline{b})|\overline{d}, \overline{c}) = ([\overline{a}, \overline{b}], \overline{c})$$

Для доказательства второго равенства заметим следующее:

$$(\overline{a}, [\overline{b}, \overline{c}]) = ([\overline{b}, \overline{c}], \overline{a}) = (\overline{b}, \overline{c}, \overline{a}) = (\overline{a}, \overline{b}, \overline{c})$$

Получено требуемое. □

Утверждение 2.11. *Пусть $\overline{x}, \overline{y} \in V_3$ — векторы такие, что для любого вектора $\overline{c} \in V_3$ выполнено $(\overline{x}, \overline{c}) = (\overline{y}, \overline{c})$. Тогда $\overline{x} = \overline{y}$.*

Доказательство. Для любого $\overline{c} \in V_3$ выполнено, что $(\overline{x}, \overline{c}) = (\overline{y}, \overline{c}) \Leftrightarrow (\overline{x} - \overline{y}, \overline{c}) = 0$. В частности, это верно для вектора $\overline{c} := \overline{x} - \overline{y}$, тогда $(\overline{x} - \overline{y}, \overline{x} - \overline{y}) = 0 \Leftrightarrow \overline{x} - \overline{y} = \overline{0} \Leftrightarrow \overline{x} = \overline{y}$. □

Замечание. Пусть $\overline{a}, \overline{b}, \overline{v} \in V_3$. Утверждение выше гарантирует, что если для некоторого вектора $\overline{v} \in V_3$ и всех $\overline{c} \in V_3$ выполнено равенство $(\overline{a}, \overline{b}, \overline{c}) = (\overline{v}, \overline{c})$, то $\overline{v} = [\overline{a}, \overline{b}]$.

Теорема 2.7. *Векторное произведение обладает следующими свойствами:*

1. $\forall \overline{a}, \overline{b} \in V_3 : [\overline{a}, \overline{b}] = -[\overline{b}, \overline{a}]$ *(кососимметричность)*

2. $\forall \overline{a_1}, \overline{a_2}, \overline{b}, \overline{c} \in V_3 : [\overline{a_1} + \overline{a_2}, \overline{b}] = [\overline{a_1}, \overline{b}] + [\overline{a_2}, \overline{b}]$
   $\forall \lambda \in \mathbb{R} : \forall \overline{a}, \overline{b}, \overline{c} \in V_3 : [\lambda\overline{a}, \overline{b}] = \lambda[\overline{a}, \overline{b}]$ *(линейность по первому аргументу)*

Доказательство.

1. Это свойство следует из определения векторного произведения.

2. Для доказательства первого равенства достаточно проверить, что для любого $\overline{c} \in V_3$ выполнено $([\overline{a_1} + \overline{a_2}, \overline{b}], \overline{c}) = ([\overline{a_1}, \overline{b}], \overline{c}) + ([\overline{a_2}, \overline{b}], \overline{c})$:

$$([\overline{a_1} + \overline{a_2}, \overline{b}], \overline{c}) = (\overline{a_1} + \overline{a_2}, \overline{b}, \overline{c}) = (\overline{a_1}, \overline{b}, \overline{c}) + (\overline{a_2}, \overline{b}, \overline{c}) = ([\overline{a_1}, \overline{b}], \overline{c}) + ([\overline{a_2}, \overline{b}], \overline{c})$$

   Для доказательства второго равенства достаточно проверить, что для любого $\overline{c} \in V_3$ выполнено $([\lambda\overline{a}, \overline{b}], \overline{c}) = (\lambda[\overline{a}, \overline{b}], \overline{c})$:

$$([\lambda\overline{a}, \overline{b}], \overline{c}) = (\lambda\overline{a}, \overline{b}, \overline{c}) = \lambda(\overline{a}, \overline{b}, \overline{c}) = \lambda([\overline{a}, \overline{b}], \overline{c}) = (\lambda[\overline{a}, \overline{b}], \overline{c})$$ □

Замечание. Линейность векторного произведения по второму аргументу также верна в силу кососимметричности.

Теорема 2.8. *Пусть* $e = (\overline{e_1}, \overline{e_2}, \overline{e_3})$ — *базис в* V_3, $\overline{a}, \overline{b} \in V_3$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$. *Тогда верно следующее равенство:*

$$[\overline{a}, \overline{b}] = \begin{vmatrix} [\overline{e_2}, \overline{e_3}] & [\overline{e_3}, \overline{e_1}] & [\overline{e_1}, \overline{e_2}] \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = \begin{vmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{vmatrix} [\overline{e_2}, \overline{e_3}] + \begin{vmatrix} \alpha_3 & \alpha_1 \\ \beta_3 & \beta_1 \end{vmatrix} [\overline{e_3}, \overline{e_1}] + \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix} [\overline{e_1}, \overline{e_2}]$$

Доказательство. В силу линейности векторного произведения, имеем:

$$[\overline{a}, \overline{b}] = \left[\sum_{i=1}^{3} \alpha_i \overline{e_i}, \sum_{j=1}^{3} \beta_j \overline{e_j}\right] = \sum_{i=1}^{3} \sum_{j=1}^{3} \alpha_i \beta_j [\overline{e_i}, \overline{e_j}]$$

Поскольку для любого $i \in \{1, 2, 3\}$ выполнено $[\overline{e_i}, \overline{e_i}] = \overline{0}$, то:

$$[\overline{a}, \overline{b}] = \begin{vmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{vmatrix} [\overline{e_2}, \overline{e_3}] + \begin{vmatrix} \alpha_3 & \alpha_1 \\ \beta_3 & \beta_1 \end{vmatrix} [\overline{e_3}, \overline{e_1}] + \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix} [\overline{e_1}, \overline{e_2}]$$

Получено требуемое. □

Замечание. Если $e = (\overline{e_1}, \overline{e_2}, \overline{e_3})$ — правый ортонормированный базис в V_3, то выполнены равенства $[\overline{e_1}, \overline{e_2}] = \overline{e_3}$, $[\overline{e_2}, \overline{e_3}] = \overline{e_1}$, $[\overline{e_3}, \overline{e_1}] = \overline{e_2}$. Значит, в таком базисе для любых $\overline{a}, \overline{b} \in V_3$, $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$, верно следующее равенство:

$$[\overline{a}, \overline{b}] = \begin{vmatrix} \overline{e_1} & \overline{e_2} & \overline{e_3} \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix}$$

Теорема 2.9. *Для любых* $\overline{a}, \overline{b}, \overline{c} \in V_3$ *верно следующее равенство:*

$$[\overline{a}, [\overline{b}, \overline{c}]] = \overline{b}(\overline{a}, \overline{c}) - \overline{c}(\overline{a}, \overline{b})$$

Доказательство. Для упрощения проверки выберем такой правый ортонормированный базис $e = (\overline{e_1}, \overline{e_2}, \overline{e_3})$ в V_3, что $\overline{e_1} \parallel \overline{a}$, а векторы $\overline{b}$, $\overline{e_1}$ и $\overline{e_2}$ компланарны. Тогда координатные столбцы векторов $\overline{a}, \overline{b}, \overline{c}$ имеют вид $(\alpha, 0, 0)^T$, $(\beta_1, \beta_2, 0)^T$, $(\gamma_1, \gamma_2, \gamma_3)^T$. Найдем координатный столбец вектора $[\overline{b}, \overline{c}]$:

$$[\overline{b}, \overline{c}] = \begin{vmatrix} \overline{e_1} & \overline{e_2} & \overline{e_3} \\ \beta_1 & \beta_2 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} = (\beta_2\gamma_3)\overline{e_1} + (-\beta_1\gamma_3)\overline{e_2} + (\beta_1\gamma_2 - \beta_2\gamma_1)\overline{e_3} \leftrightarrow_e \begin{pmatrix} \beta_2\gamma_3 \\ -\beta_1\gamma_3 \\ \beta_1\gamma_2 - \beta_2\gamma_1 \end{pmatrix}$$

Положим $\delta_1 := \beta_2\gamma_3$, $\delta_2 := -\beta_1\gamma_3$, $\delta_3 := \beta_1\gamma_2 - \beta_2\gamma_1$, тогда:

$$[\overline{a}, [\overline{b}, \overline{c}]] = \begin{vmatrix} \overline{e_1} & \overline{e_2} & \overline{e_3} \\ \alpha & 0 & 0 \\ \delta_1 & \delta_2 & \delta_3 \end{vmatrix} = 0\overline{e_1} + (-\alpha\delta_3)\overline{e_2} + (\alpha\delta_2)\overline{e_3} \leftrightarrow_e \begin{pmatrix} 0 \\ -\alpha\delta_3 \\ \alpha\delta_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha(\beta_2\gamma_1 - \beta_1\gamma_2) \\ -\alpha\beta_1\gamma_3 \end{pmatrix}$$

С другой стороны:

$$\overline{b}(\overline{a}, \overline{c}) - \overline{c}(\overline{a}, \overline{b}) \leftrightarrow_e \begin{pmatrix} \alpha\beta_1\gamma_1 \\ \alpha\beta_2\gamma_1 \\ 0 \end{pmatrix} - \begin{pmatrix} \alpha\beta_1\gamma_1 \\ \alpha\beta_1\gamma_2 \\ \alpha\beta_1\gamma_3 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha(\beta_2\gamma_1 - \beta_1\gamma_2) \\ -\alpha\beta_1\gamma_3 \end{pmatrix}$$

Таким образом, $[\overline{a}, [\overline{b}, \overline{c}]] = \overline{b}(\overline{a}, \overline{c}) - \overline{c}(\overline{a}, \overline{b})$. □

3 Уравнения прямых и плоскостей

3.1 Прямая в плоскости

Определение 3.1. *Направляющим вектором* прямой $l \subset P_3$ называется вектор $\overline{a} \in V_3$, $\overline{a} \neq \overline{0}$, представителем которого является направленный отрезок, лежащий в l.

Определение 3.2. Пусть $l \subset P_2$ — прямая с направляющим вектором $\overline{a} \in V_2$, $M \in l$, и в декартовой системе координат (O, e) в P_2 выполнены соотношения $\overline{a} \leftrightarrow_e (\alpha_1, \alpha_2)^T$, $M \leftrightarrow_{(O,e)} (x_0, y_0)^T$, $\overline{r_0} := \overline{OM}$.

- ▷ *Векторно-параметрическим уравнением прямой* называется следующее семейство уравнений:
$$\overline{r} = \overline{r_0} + t\overline{a},\ t \in \mathbb{R}$$
- ▷ *Параметрическим уравнением прямой* называется следующее семейство систем:
$$\begin{cases} x = x_0 + t\alpha_1 \\ y = y_0 + t\alpha_2 \end{cases},\ t \in \mathbb{R}$$
- ▷ *Каноническим уравнением прямой* называется следующее уравнение:
$$\frac{x - x_0}{\alpha_1} = \frac{y - y_0}{\alpha_2}$$

Замечание. Множество точек $X \in P_2$ таких, что $X \leftrightarrow_{(O,e)} (x, y)^T$, $\overline{r} := \overline{OX}$, являющихся решениями любого из уравнений прямой выше, совпадает с прямой l. Действительно, $X \in l \Leftrightarrow MX \parallel l \Leftrightarrow \overline{MX} \parallel \overline{a}$.

Замечание. В случае канонического уравнения прямой, если без ограничения общности $\alpha_1 = 0$, то тогда $\alpha_2 \neq 0$, и следует считать, что исходное уравнение эквивалентно условию $x = x_0$. Отметим также, что каноническое уравнение прямой эквивалентно следующему такому уравнению:

$$\alpha_2 x - \alpha_1 y + (\alpha_1 y_0 - \alpha_2 x_0) = 0$$

Определение 3.3. Пусть $A, B, C \in \mathbb{R}$, $A^2 + B^2 \neq 0$. *Общим уравнением прямой* называется следующее уравнение:

$$Ax + By + C = 0$$

Утверждение 3.1. *Пусть прямая l задана в декартовой системе координат (O, e) в P_2 общим уравнением прямой $Ax + By + C = 0$, $\overline{b} \in V_2$, $\overline{b} \leftrightarrow_e \beta$. Тогда выполнена равносильность $\overline{b} \parallel l \Leftrightarrow A\beta_1 + B\beta_2 = 0$.*

Доказательство. Пусть $M \in l$, точка $N \in P_2$ такова, что $\overline{MN} = \overline{b}$, и $M \leftrightarrow_{(O,e)} (x_0, y_0)^T$, тогда $N \leftrightarrow_{(O,e)} (x_0 + \beta_1, y_0 + \beta_2)^T$. Поскольку $M \in l$, выполнены следующие эквивалентности:

$$\overline{b} \parallel l \Leftrightarrow N \in l \Leftrightarrow A(x_0 + \beta_1) + B(y_0 + \beta_2) + C = 0 \Leftrightarrow A\beta_1 + B\beta_2 = 0 \qquad \square$$

Следствие. Пусть прямая $l \subset P_2$ задана в декартовой системе координат (O, e) общим уравнением прямой $Ax + By + C = 0$, $\overline{b} \in V_2$, $\overline{b} \leftrightarrow_e \beta$. Тогда направляющим вектором прямой l является вектор $\overline{a} \in V_2$ такой, что $\overline{a} \leftrightarrow_e (-B, A)^T$.

Определение 3.4. *Вектором нормали* прямой $l \subset P_3$ называется вектор $\overline{n} \in V_3$, $\overline{n} \neq \overline{0}$, представителем которого является направленный отрезок, ортогональный прямой l.

Следствие. Пусть прямая $l \subset P_2$ задана в декартовой системе координат (O, e) общим уравнением прямой $Ax + By + C = 0$, $\overline{b} \in V_2$, $\overline{b} \leftrightarrow_e \beta$. Тогда вектором нормали прямой l является вектор $\overline{n} \in V_2$ такой, что $\overline{n} \leftrightarrow_e (A, B)^T$.

Определение 3.5. Пусть $l \subset P_2$ — прямая с вектором нормали $\overline{n} \in V_2$, и пусть $M \in l$, $\overline{r_0} := \overline{OM}$. *Нормальным уравнением прямой* называется следующее уравнение:

$$(\overline{r} - \overline{r_0}, \overline{n}) = 0$$

Замечание. Множество точек $X \in P_2$, $\overline{r} := \overline{OX}$, являющихся решениями нормального уравнения прямой, совпадает с прямой l. Кроме того, это уравнение можно переписать в следующем виде при $\gamma := (\overline{r_0}, \overline{n})$:

$$(\overline{r}, \overline{n}) = \gamma$$

Замечание. Уравнения различного типа, задающие прямую, эквивалентны: из каждого из них можно получить любое другое.

Замечание. Рассмотренные способы задания прямой позволяют определить *взаимное расположение прямых на плоскости.* Пусть прямые l_1, l_2 заданы векторно-параметрическими уравнениями $\overline{r} = \overline{r_1} + t\overline{a_1}$, $\overline{r} = \overline{r_2} + t\overline{a_2}$. Тогда:

- $l_1 \cap l_2 \neq \varnothing$ и $l_1 \neq l_2 \Leftrightarrow \overline{a_1} \nparallel \overline{a_2}$

- $\triangleright$ $l_1 \parallel l_2$ и $l_1 \neq l_2 \Leftrightarrow \overline{a_1} \parallel \overline{a_2}$ и $(\overline{r_1} - \overline{r_2}) \nparallel \overline{a_1}$
- $\triangleright$ $l_1 = l_2 \Leftrightarrow (\overline{r_1} - \overline{r_2}) \parallel \overline{a_1} \parallel \overline{a_2}$

Замечание. Прямая $l \subset P_2$ в плоскости делит ее на две полуплоскости. Выделим одну из открытых полуплоскостей $S \subset P_2$. Пусть прямая l задана нормальным уравнением $(\overline{r} - \overline{r_0}, \overline{n}) = 0$, причем вектор нормали $\overline{n}$ направлен в полуплоскость S. Тогда точка $X \in P_2$, $\overline{r} := \overline{OX}$, лежит в $S \Leftrightarrow (\overline{r} - \overline{r_0}, \overline{n}) > 0$. Противоположная полуплоскость задается противоположным неравенством.

Определение 3.6. *Пучком прямых* называется либо множество всех прямых в P_2, проходящих через фиксированную точку $P \in P_2$, либо множество всех прямых, параллельных фиксированной прямой $l \subset P_2$.

Замечание. Любые две прямые в P_2 лежат ровно в одном пучке.

Теорема 3.1. *Пусть в декартовой системе координат (O, e) в P_2 различные прямые l_1, l_2 заданы уравнениями $A_1x + B_1y + C_1 = 0$, $A_2x + B_2y + C_2 = 0$. Тогда прямая $l \subset P_2$ лежит в одном пучке с прямыми l_1 и $l_2 \Leftrightarrow$ прямая l задается уравнением следующего вида при некоторых $\alpha_1, \alpha_2 \in \mathbb{R}$:*

$$\alpha_1(A_1x + B_1y + C_1) + \alpha_2(A_2x + B_2y + C_2) = 0$$

Доказательство.

$\Leftarrow$ Возможны два случая:

1. Если $l_1 \cap l_2 = \{P\}$, $P \in P_2$, то координаты точки P удовлетворяют требуемому уравнению, то есть $P \in l$.
2. Если $l_1 \parallel l_2$, то из требуемого уравнения направляющий вектор прямой l параллелен направляющим векторам l_1 и l_2. В этом случае уравнение задает прямую не при всех $\alpha_1, \alpha_2 \in \mathbb{R}$, но если задает, то лежащую в данном пучке.

$\Rightarrow$ Возможны два случая:

1. Если $l \cap l_1 \cap l_2 = \{P\}$, $P \in P_2$, то выберем на l точку $Q \neq P$, $Q \leftrightarrow_{(O,e)} (x_0, y_0)^T$. Тогда Q удовлетворяет уравнению с коэффициентами $\alpha_1 := A_2x_0 + B_2y_0 + C_2$, $\alpha_2 := -(A_1x_0 + B_1y_0 + C_1)$. Хотя бы один из коэффициентов ненулевой, поскольку Q лежит не более, чем на одной из прямых l_1, l_2. Значит, такое уравнение задает l, так как ему удовлетворяют две различных точки этой прямой.
2. Если $l \parallel l_1 \parallel l_2$, то аналогичным образом выберем любую точку $Q \in l$ и соответствующие коэффициенты, тогда полученное уравнение задает l при условии, что оно задает прямую. Но оно всегда задает прямую, поскольку множество его решений непусто и не содержит хотя бы одну из прямых l_1, l_2. $\square$

Утверждение 3.2. *Пусть в прямоугольной декартовой системе координат (O, e) в P_2 прямые l_1, l_2 заданы уравнениями $A_1x + B_1y + C_1 = 0$, $A_2x + B_2y + C_2 = 0$. Тогда угол φ между ними удовлетворяет следующему равенству:*

$$\cos\varphi = \frac{|A_1A_2 + B_1B_2|}{\sqrt{A_1^2 + B_1^2}\sqrt{A_2^2 + B_2^2}}$$

Доказательство. Пусть $\overline{n_1}, \overline{n_2} \in V_2$, $\overline{n_1} \leftrightarrow_e (A_1, B_1)^T$, $\overline{n_2} \leftrightarrow_e (A_2, B_2)^T$, — нормальные векторы прямых l_1, l_2, $\alpha := \angle(\overline{n_1}, \overline{n_2})$. Тогда угол φ равен меньшему из углов α и $\pi - \alpha$. В каждом из случаев выполнено следующее:

$$\cos\varphi = |\cos\alpha| = \frac{|A_1A_2 + B_1B_2|}{\sqrt{A_1^2 + B_1^2}\sqrt{A_2^2 + B_2^2}} \qquad \square$$

Утверждение 3.3. *Пусть в прямоугольной декартовой системе координат (O, e) в P_2 прямая l задана уравнением $Ax+By+C = 0$, $M \in P_2$, $M \leftrightarrow_{(O,e)} (x_0, y_0)^T$. Тогда расстояние ρ от точки M до прямой l равно следующей величине:*

$$\rho = \frac{|Ax_0 + By_0 + C|}{\sqrt{A^2 + B^2}}$$

Доказательство. Пусть $\overline{n} \in V_2$, $\overline{n} \leftrightarrow_e (A, B)^T$ — вектор нормали прямой l, $\overline{r_0} := \overline{OM}$, и пусть $X \in l$, $\overline{r} := \overline{OX}$. Тогда:

$$\rho = |\operatorname{pr}_{\overline{n}}(\overline{r_0} - \overline{r})| = \left|\frac{(\overline{r_0} - \overline{r}, \overline{n})}{|\overline{n}|^2}\overline{n}\right| = \frac{|(\overline{r_0} - \overline{r}, \overline{n})|}{|\overline{n}|} = \frac{|Ax_0 + By_0 + C|}{\sqrt{A^2 + B^2}} \qquad \square$$

3.2 Плоскость в пространстве

Определение 3.7. Пусть $\nu \subset P_3$ — плоскость, $\overline{a}, \overline{b} \in V_3$ — неколлинеарные векторы, представители которых лежат в ν, $M \in l$, и в декартовой системе координат (O, e) в P_3 выполнены соотношения $\overline{a} \leftrightarrow_e \alpha$, $\overline{b} \leftrightarrow_e \beta$, $M \leftrightarrow_{(O,e)} (x_0, y_0, z_0)^T$, $\overline{r_0} := \overline{OM}$.

- ▷ *Векторно-параметрическим уравнением плоскости* называется следующее семейство уравнений:
$$\overline{r} = \overline{r_0} + t\overline{a} + s\overline{b},\ t, s \in \mathbb{R}$$

- ▷ *Параметрическим уравнением плоскости* называется следующее семейство систем:

$$\begin{cases} x = x_0 + t\alpha_1 + s\beta_1 \\ y = y_0 + t\alpha_2 + s\beta_2 \\ z = z_0 + t\alpha_3 + s\beta_3 \end{cases},\ s, t \in \mathbb{R}$$

Замечание. Множество точек $X \in P_3$ таких, что $X \leftrightarrow_{(O,e)} (x, y, z)^T$, $\overline{r} := \overline{OX}$, являющихся решениями любого из уравнений прямой выше, совпадает с плоскостью ν. Действительно, $X \in \nu \Leftrightarrow MX \parallel \nu \Leftrightarrow \overline{MX}$ компланарен системе $(\overline{a}, \overline{b}) \Leftrightarrow \overline{MX}$ выражается через $\overline{a}, \overline{b}$.

Замечание. Векторно-параметрическое уравнение плоскости можно также переписать в следующем виде:

$$(\overline{r} - \overline{r_0}, \overline{a}, \overline{b}) = 0$$

Перепишем это уравнение, положив $\gamma := (\overline{r_0}, \overline{a}, \overline{b})$:

$$(\overline{r}, \overline{a}, \overline{b}) = \gamma$$

Если расписать смешанное произведение $(\overline{r}, \overline{a}, \overline{b})$ как определитель соответствующей матрицы, можно получить еще одно уравнение плоскости, определенное ниже.

Определение 3.8. Пусть $A, B, C, D \in \mathbb{R}$, $A^2+B^2+C^2 \neq 0$. *Общим уравнением плоскости* называется следующее уравнение:

$$Ax + By + Cz + D = 0$$

Утверждение 3.4. *Пусть плоскость ν задана в декартовой системе координат (O, e) в P_3 общим уравнением плоскости $Ax + By + Cz + D = 0$, $\overline{b} \in V_3$, $\overline{b} \leftrightarrow_e \beta$. Тогда выполнена равносильность $\overline{b} \parallel \nu \Leftrightarrow A\beta_1 + B\beta_2 + C\beta_3 = 0$.*

Доказательство. Пусть $M \in \nu$, точка $N \in P_3$ такова, что $\overline{MN} = \overline{b}$, и $M \leftrightarrow_{(O,e)} (x_0, y_0, z_0)^T$, тогда $N \leftrightarrow_{(O,e)} (x_0 + \beta_1, y_0 + \beta_2, z_0 + \beta_3)^T$. Поскольку $M \in \nu$, выполнены следующие эквивалентности:

$$\overline{b} \parallel \nu \Leftrightarrow N \in \nu \Leftrightarrow A(x_0 + \beta_1) + B(y_0 + \beta_2) + C(z_0 + \beta_3) + D = 0 \Leftrightarrow$$
$$\Leftrightarrow A\beta_1 + B\beta_2 + C\beta_3 = 0 \quad \square$$

Утверждение 3.5. *Пусть $A, B, C, D \in \mathbb{R}$, $A^2 + B^2 + C^2 \neq 0$. Тогда общее уравнение плоскости $Ax+By+Cz+D = 0$ действительно задает плоскость в декартовой системе координат (O, e) в P_3.*

Доказательство. Пусть без ограничения общности $A \neq 0$. Зафиксируем векторы $\overline{a}, \overline{b} \in V_3$, $\overline{a} \leftrightarrow_e (-B, A, 0)^T$, $\overline{b} \leftrightarrow_e (-C, 0, A)^T$, и точку $M \in P_3$, $M \leftrightarrow_{(O,e)} \big(-\frac{D}{A}, 0, 0\big)^T$. Векторы $\overline{a}$ и $\overline{b}$ неколлинеарны, поскольку их координаты непропорциональны. Рассмотрим плоскость $\nu \subset P_3$, содержащую точку M и векторы $\overline{a}, \overline{b}$, отложенные от точки M. Тогда для произвольной точки $X \in P_3$, $X \leftrightarrow_{(O,e)} (x, y, z)^T$, $\overline{r} := \overline{OX}$, выполнено $X \in \nu \Leftrightarrow (\overline{r} - \overline{r_0}, \overline{a}, \overline{b}) = 0$. Вычислим смешанное произведение $(\overline{r} - \overline{r_0}, \overline{a}, \overline{b})$:

$$(\overline{r} - \overline{r_0}, \overline{a}, \overline{b}) = \begin{vmatrix} x + \frac{D}{A} & -B & -C \\ y & A & 0 \\ z & 0 & A \end{vmatrix} = \left(x + \frac{D}{A}\right) A^2 - y\,(-B)\,A - z(-C)A =$$
$$= A^2x + ABy + ACz + AD = A(Ax + By + Cz + D)$$

Таким образом, $X \in \nu \Leftrightarrow Ax + By + Cz + D = 0$, что и требовалось. $\square$

Определение 3.9. *Вектором нормали* плоскости $\nu \subset P_3$ называется вектор $\overline{n} \in V_3$, $\overline{n} \neq \overline{0}$, представителем которого является направленный отрезок, ортогональный плоскости ν.

Определение 3.10. Пусть $\nu \subset P_3$ — плоскость с вектором нормали $\overline{n} \in V_3$, и пусть $M \in \nu$, $\overline{r_0} := \overline{OM}$. *Нормальным уравнением плоскости* называется следующее уравнение:

$$(\overline{r} - \overline{r_0}, \overline{n}) = 0$$

Замечание. Множество точек $X \in P_3$, $\overline{r} := \overline{OX}$, являющихся решениями нормального уравнения плоскости, совпадает с плоскостью ν. Кроме того, это уравнение можно переписать в следующем виде при $\gamma := (\overline{r_0}, \overline{n})$:

$$(\overline{r}, \overline{n}) = \gamma$$

Замечание. Уравнения различного типа, задающие плоскость, эквивалентны: из каждого из них можно получить любое другое.

Замечание. В прямоугольной декартовой системе координат (O, e) в P_3 нормальное уравнение плоскости преобразуется к виду $Ax + By + Cz + D = 0$, поэтому вектором нормали этой плоскости является вектор $\overline{n} \in V_3$ такой, что $\overline{n} \leftrightarrow_e (A, B, C)^T$.

Определение 3.11. Пусть в декартовой системе координат (O, e) в P_3 плоскость ν задана уравнением $Ax + By + Cz + D = 0$. *Сопутствующим вектором* плоскости ν в данной системе координат называется вектор $\overline{n} \in V_3$ такой, что $\overline{n} \leftrightarrow_e (A, B, C)^T$.

Утверждение 3.6. *Пусть в декартовой системе координат (O, e) в P_3 плоскости ν_1, ν_2 заданы общими уравнениями $A_1x + B_1y + C_1z + D_1 = 0$, $A_2x + B_2y + C_2z + D_2 = 0$. Тогда:*

- $\nu_1 \cap \nu_2 \neq \varnothing$ *и* $\nu_1 \neq \nu_2 \Leftrightarrow \overline{n_1} \nparallel \overline{n_2}$
- $\nu_1 \parallel \nu_2$ *и* $\nu_1 \neq \nu_2 \Leftrightarrow \overline{n_1} \parallel \overline{n_2}$, *но уравнения плоскостей непропорциональны*
- $\nu_1 = \nu_2 \Leftrightarrow$ *уравнения плоскостей пропорциональны*

Доказательство.

- Пусть $\overline{n_1} \nparallel \overline{n_2}$, тогда без ограничения общности столбцы $(A_1, B_1)^T$ и $(A_2, B_2)^T$ непропорциональны. Рассмотрим следующую систему уравнений относительно x и y:

$$\begin{cases} A_1x + B_1y = -C_1z - D_1 \\ A_2x + B_2y = -C_2z - D_2 \end{cases}$$

  По правилу Крамера, эта система имеет единственное решение при любом $z \in \mathbb{R}$. Значит, плоскости имеют общие точки, но не все их точки общие, и это означает, что они пересекаются.

- Пусть $\overline{n_1} \parallel \overline{n_2}$ и уравнения непропорциональны. Поскольку столбцы $(A_1, B_1, C_1)^T$ и $(A_2, B_2, C_2)^T$ пропорциональны из коллинеарности векторов $\overline{n_1}$ и $\overline{n_2}$, можно без ограничения общности считать, что $A_1 = A_2$, $B_1 = B_2$, $C_1 = C_2$, но $D_1 \neq D_2$. Тогда уравнения плоскостей не имеют общих решений, откуда $\nu_1 \parallel \nu_2$ и $\nu_1 \neq \nu_2$.

- Пусть уравнения плоскостей пропорциональны, тогда можно считать, что они совпадают. Тогда совпадают и множества их решений, то есть $\nu_1 = \nu_2$. $\square$

Утверждение 3.7. *Пусть в декартовой системе координат (O, e) пересекающиеся плоскости ν_1, ν_2 заданы уравнениями $A_1x + B_1y + C_1z + D_1 = 0$, $A_2x + B_2y + C_2z + D_2 = 0$. Тогда направляющим вектором прямой их пересечения является вектор $\overline{v} \in V_3$ такой, что:*

$$\overline{v} \leftrightarrow_e \left(\begin{vmatrix} B_1 & C_1 \\ B_2 & C_2 \end{vmatrix}, \begin{vmatrix} C_1 & A_1 \\ C_2 & A_2 \end{vmatrix}, \begin{vmatrix} A_1 & B_1 \\ A_2 & B_2 \end{vmatrix} \right)^T$$

Доказательство.

1. Поскольку $\nu_1 \nparallel \nu_2$, то хотя бы один из определителей, указанных в координатном столбце вектора $\overline{v}$, ненулевой, откуда $\overline{v} \neq \overline{0}$.

2. Заметим, что выполнено следующее равенство:

$$A_1 \begin{vmatrix} B_1 & C_1 \\ B_2 & C_2 \end{vmatrix} + B_1 \begin{vmatrix} C_1 & A_1 \\ C_2 & A_2 \end{vmatrix} + C_1 \begin{vmatrix} A_1 & B_1 \\ A_2 & B_2 \end{vmatrix} = \begin{vmatrix} A_1 & B_1 & C_1 \\ A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{vmatrix}$$

Поскольку определитель матрицы не меняется при транспонировании, выполнено следующее:

$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{vmatrix} = \begin{vmatrix} A_1 & A_1 & A_2 \\ B_1 & B_1 & B_2 \\ C_1 & C_1 & C_2 \end{vmatrix} = 0$$

Определитель в правой части равенства равен 0, поскольку он соответствует ориентированному объему от тройки векторов, среди которых есть два одинаковых. Получено следующее равенство:

$$A_1 \begin{vmatrix} B_1 & C_1 \\ B_2 & C_2 \end{vmatrix} + B_1 \begin{vmatrix} C_1 & A_1 \\ C_2 & A_2 \end{vmatrix} + C_1 \begin{vmatrix} A_1 & B_1 \\ A_2 & B_2 \end{vmatrix} = 0$$

Значит, по критерию параллельности вектора и плоскости, $\overline{v} \parallel \nu_1$.

3. Аналогично пункту (2), выполнено $\overline{v} \parallel \nu_2$. □

Замечание. Плоскость $\nu \subset P_3$ в пространстве делит его на два полупространства. Выделим одно из открытых полупространств $S \subset P_3$. Пусть плоскость ν задана нормальным уравнением $(\overline{r} - \overline{r_0}, \overline{n}) = 0$, причем вектор нормали $\overline{n}$ направлен в полупространство S. Тогда точка $X \in P_3$, $\overline{r} := \overline{OX}$, лежит в $S \Leftrightarrow (\overline{r} - \overline{r_0}, \overline{n}) > 0$. Противоположное полупространство задается противоположным неравенством.

Определение 3.12. *Пучком плоскостей* называется либо множество всех плоскостей в P_3, проходящих через фиксированную прямую $l \subset P_3$, либо множество всех плоскостей, параллельных фиксированной плоскости $\nu \subset P_3$.

Замечание. Любые две плоскости в P_3 ровно в одном пучке.

Теорема 3.2. *Пусть в декартовой системе координат (O, e) в P_3 различные плоскости ν_1, ν_2 заданы уравнениями $A_1x + B_1y + C_1z + D_1 = 0$, $A_2x + B_2y + C_2z + D_2 = 0$. Тогда плоскость $\nu \subset P_2$ лежит в одном пучке с плоскостями ν_1 и $\nu_2 \Leftrightarrow$ плоскость ν задается уравнением следующего вида при некоторых $\alpha_1, \alpha_2 \in \mathbb{R}$:*

$$\alpha_1(A_1x + B_1y + C_1z + D_1) + \alpha_2(A_2x + B_2y + C_2z + D_2) = 0$$

Доказательство.

$\Leftarrow$ Возможны два случая:

1. Если $\nu_1 \cap \nu_2 = l \subset P_3$, то координаты каждой точки P на прямой l удовлетворяют требуемому уравнению, откуда $l \subset \nu$.
2. Если $\nu_1 \parallel \nu_2$, то из требуемого уравнения сопутствующий вектор плоскости ν параллелен сопутствующим векторам плоскостей ν_1 и ν_2. В этом случае уравнение задает плоскость не при всех $\alpha_1, \alpha_2 \in \mathbb{R}$, но если задает, то лежащую в данном пучке.

$\Rightarrow$ Возможны два случая:

1. Если $\nu \cap \nu_1 \cap \nu_2 = l \subset P_3$, то выберем на ν точку $Q \notin l$, $Q \leftrightarrow_{(O,e)} (x_0, y_0, z_0)^T$. Тогда Q удовлетворяет уравнению с коэффициентами $\alpha_1 := A_2x_0 + B_2y_0 + C_2z_0 + D_2$, $\alpha_2 := -(A_1x_0 + B_1y_0 + C_1z_0 + D_1)$. Хотя бы один из коэффициентов ненулевой,

поскольку Q лежит не более, чем на одной из плоскостей ν_1, ν_2. Значит, такое уравнение задает ν, так как ему удовлетворяют все точки прямой l и точка, не лежащая на l.

2. Если $\nu \parallel \nu_1 \parallel \nu_2$, то аналогичным образом выберем любую точку $Q \in \nu$ и соответствующие коэффициенты, тогда полученное уравнение задает ν при условии, что оно задает плоскость. Но оно всегда задает плоскость, поскольку множество его решений непусто и не содержит хотя бы одну из плоскостей ν_1, ν_2. □

Утверждение 3.8. *Пусть в прямоугольной декартовой системе координат (O, e) в P_3 плоскости ν_1, ν_2 заданы уравнениями $A_1x + B_1y + C_1z + D_1 = 0$, $A_2x + B_2y + C_2z + D_2 = 0$. Тогда угол φ между ними удовлетворяет равенству:*

$$\cos\varphi = \frac{|A_1A_2 + B_1B_2 + C_1C_2|}{\sqrt{A_1^2 + B_1^2 + C_1^2}\sqrt{A_2^2 + B_2^2 + C_2^2}}$$

Доказательство. Пусть $\overline{n_1}, \overline{n_2} \in V_3$, $\overline{n_1} \leftrightarrow_e (A_1, B_1, C_1)^T$, $\overline{n_2} \leftrightarrow_e (A_2, B_2, C_2)^T$, — нормальные векторы плоскостей ν_1, ν_2, $\alpha := \angle(\overline{n_1}, \overline{n_2})$. Тогда угол φ равен меньшему из углов α и $\pi - \alpha$. В каждом из случаев выполнено следующее:

$$\cos\varphi = |\cos\alpha| = \frac{|A_1A_2 + B_1B_2 + C_1C_2|}{\sqrt{A_1^2 + B_1^2 + C_1^2}\sqrt{A_2^2 + B_2^2 + C_2^2}}$$ □

Утверждение 3.9. *Пусть в прямоугольной декартовой системе координат (O, e) в P_3 плоскость ν задана уравнением $Ax + By + Cz + D = 0$, $M \in P_3$, $M \leftrightarrow_{(O,e)} (x_0, y_0, z_0)^T$. Тогда расстояние ρ от точки M до плоскости ν равно следующей величине:*

$$\rho = \frac{|Ax_0 + By_0 + Cz_0 + D|}{\sqrt{A^2 + B^2 + C^2}}$$

Доказательство. Пусть $\overline{n} \in V_3$, $\overline{n} \leftrightarrow_e (A, B, C)^T$ — вектор нормали плоскости ν, $\overline{r_0} := \overline{OM}$, и пусть $X \in \nu$, $\overline{r} := \overline{OX}$. Тогда:

$$\rho = |\operatorname{pr}_{\overline{n}}(\overline{r_0} - \overline{r})| = \left|\frac{(\overline{r_0} - \overline{r}, \overline{n})}{|\overline{n}|^2}\overline{n}\right| = \frac{|(\overline{r_0} - \overline{r}, \overline{n})|}{|\overline{n}|} = \frac{|Ax_0 + By_0 + Cz_0 + D|}{\sqrt{A^2 + B^2 + C^2}}$$ □

Утверждение 3.10. *Пусть в прямоугольной системе координат (O, e) в P_3 параллельные плоскости ν_1, ν_2 заданы уравнениями $Ax + By + Cz + D_1 = 0$, $Ax + By + Cz + D_2 = 0$. Тогда расстояние ρ между ними равно следующей величине:*

$$\rho = \frac{|D_1 - D_2|}{\sqrt{A^2 + B^2 + C^2}}$$

Доказательство. Пусть $M_1 \in \nu_1$, $M_2 \in \nu_2$, $\overline{r_1} := \overline{OM_1}$, $\overline{r_2} := \overline{OM_2}$. Плоскости ν_1, ν_2 имеют общий вектор нормали $\overline{n} \in V_3$, $\overline{n} \leftrightarrow_e (A, B, C)^T$, и выполнены равенства $(\overline{r_1}, \overline{n_1}) = -D_1$, $(\overline{r_2}, \overline{n_2}) = -D_2$, тогда:

$$\rho = |\operatorname{pr}_{\overline{n}}(\overline{r_1} - \overline{r_2})| = \left|\frac{(\overline{r_1}, \overline{n_1}) - (\overline{r_2}, \overline{n_2})}{|\overline{n}|}\right| = \frac{|D_1 - D_2|}{\sqrt{A^2 + B^2 + C^2}}$$ □

3.3 Прямая в пространстве

Определение 3.13. Пусть $l \subset P_3$ — прямая с направляющим вектором $\overline{a} \in V_3$, $M \in l$, и в декартовой системе координат (O, e) в P_3 выполнены соотношения $\overline{a} \leftrightarrow_e \alpha$, $M \leftrightarrow_{(O,e)} (x_0, y_0, z_0)^T$, $\overline{r_0} := \overline{OM}$.

- ▷ *Векторно-параметрическим уравнением прямой* называется следующее семейство уравнений:

$$\overline{r} = \overline{r_0} + t\overline{a},\ t \in \mathbb{R}$$

- ▷ *Параметрическим уравнением прямой* называется следующее семейство систем:

$$\begin{cases} x = x_0 + t\alpha_1 \\ y = y_0 + t\alpha_2 \\ z = z_0 + t\alpha_3 \end{cases},\ t \in \mathbb{R}$$

- ▷ *Каноническим уравнением прямой* называется следующая система уравнений:

$$\frac{x - x_0}{\alpha_1} = \frac{y - y_0}{\alpha_2} = \frac{z - z_0}{\alpha_3}$$

Замечание. Множество точек $X \in P_3$ таких, что $X \leftrightarrow_{(O,e)} (x, y, z)^T$, $\overline{r} := \overline{OX}$, являющихся решениями любого из уравнений прямой выше, совпадает с прямой l. Действительно, $X \in l \Leftrightarrow MX \parallel l \Leftrightarrow \overline{MX} \parallel \overline{a}$.

Замечание. Для канонического уравнения прямой имеют место следующие соглашения:

- ▷ Если без ограничения общности $\alpha_1 = 0$ и $\alpha_2, \alpha_3 \neq 0$, то следует считать, что исходное уравнение эквивалентно системе уравнений $x = x_0$ и $\frac{y-y_0}{\alpha_2} = \frac{z-z_0}{\alpha_3}$.
- ▷ Если без ограничения общности $\alpha_1 = \alpha_2 = 0$, то тогда $\alpha_3 \neq 0$, и следует считать, что исходное уравнение эквивалентно системе уравнений $x = x_0$ и $y = y_0$.

Определение 3.14. Пусть $l \subset P_3$ — прямая с направляющим вектором $\overline{a}$, и пусть $M \in l$, $\overline{r_0} := \overline{OM}$. *Векторным уравнением прямой* называется следующее уравнение:

$$[\overline{r} - \overline{r_0}, \overline{a}] = \overline{0}$$

Замечание. Множество точек $X \in P_3$, $\overline{r} := \overline{OX}$, являющихся решениями векторного уравнения прямой, совпадает с прямой l. Кроме того, это уравнение можно переписать в следующем виде при $\overline{b} := [\overline{r_0}, \overline{a}]$:

$$[\overline{r}, \overline{a}] = \overline{b}$$

Отметим также, что пространстве прямую также можно задать как пересечение двух плоскостей.

Замечание. Рассмотренные способы задания прямой позволяют определить *взаимное расположение прямых в пространстве*. Пусть прямые l_1, l_2 заданы векторно-параметрическими уравнениями $\overline{r} = \overline{r_1} + t\overline{a_1}$, $\overline{r} = \overline{r_2} + t\overline{a_2}$. Тогда:

- ▷ $l_1 \parallel l_2$ и $l_1 \neq l_2 \Leftrightarrow \overline{a_1} \parallel \overline{a_2}$ и $\overline{a_1} \nparallel (\overline{r_2} - \overline{r_1}) \Leftrightarrow [\overline{a_1}, \overline{a_2}] = \overline{0}$ и $[\overline{a_1}, \overline{r_2} - \overline{r_1}] \neq \overline{0}$

▷ $l_1 = l_2 \Leftrightarrow \overline{a_1} \parallel \overline{a_2}$ и $\overline{a_1} \parallel (\overline{r_2} - \overline{r_1}) \Leftrightarrow [\overline{a_1}, \overline{a_2}] = \overline{0}$ и $[\overline{a_1}, \overline{r_2} - \overline{r_1}] = \overline{0}$

▷ $l_1 \cap l_2 \neq \varnothing$ и $l_1 \neq l_2 \Leftrightarrow (\overline{a_1}, \overline{a_2}, \overline{r_2} - \overline{r_1}) = 0$ и $\overline{a_1} \nparallel \overline{a_2} \Leftrightarrow (\overline{a_1}, \overline{a_2}, \overline{r_2} - \overline{r_1}) = 0$ и $[\overline{a_1}, \overline{a_2}] \neq \overline{0}$

▷ l_1, l_2 скрещиваются $\Leftrightarrow (\overline{a_1}, \overline{a_2}, \overline{r_2} - \overline{r_1}) \neq 0$

Замечание. Рассмотренные способы задания прямой и плоскости позволяют определить *взаимное расположение прямой и плоскости в пространстве*. Пусть в декартовой системе координат (O, e) в P_3 плоскость ν задана общим уравнением $Ax + By + Cz + D = 0$, и пусть прямая l задана векторно-параметрическим уравнением $\overline{r} = \overline{r_0} + t\overline{a}$, $\overline{r_0} \leftrightarrow_e (x_0, y_0, z_0)^T$, $\overline{a} \leftrightarrow_e \alpha$. Тогда:

▷ $l \cap \nu \neq \varnothing$ и $l \not\subset \nu \Leftrightarrow \overline{a} \nparallel \nu \Leftrightarrow A\alpha_1 + B\alpha_2 + C\alpha_3 \neq 0$

▷ $l \parallel \nu$ и $l \not\subset \nu \Leftrightarrow \begin{cases} A\alpha_1 + B\alpha_2 + C\alpha_3 = 0 \\ Ax_0 + By_0 + Cz_0 + D \neq 0 \end{cases}$

▷ $l \subset \nu \Leftrightarrow \begin{cases} A\alpha_1 + B\alpha_2 + C\alpha_3 = 0 \\ Ax_0 + By_0 + Cz_0 + D = 0 \end{cases}$

Утверждение 3.11. *Пусть прямая $l \subset P_3$ задана векторно-параметрическим уравнением $\overline{r} = \overline{r_0} + \overline{a}t$, $A \in P_3$, $\overline{r_A} := \overline{OA}$. Тогда расстояние ρ от точки A до прямой l равно следующей величине:*

$$\rho = \frac{|[\overline{r_A} - \overline{r_0}, \overline{a}]|}{|\overline{a}|}$$

Доказательство. Искомое расстояние ρ является длиной высоты параллелограмма, построенного на векторах $\overline{a}$ и $\overline{r_A} - \overline{r_0}$, проведенной к стороне, образованной вектором $\overline{a}$ и имеющей длину $|\overline{a}|$, из чего и следует требуемое. □

Утверждение 3.12. *Пусть скрещивающиеся прямые $l_1, l_2 \subset P_3$ заданы уравнениями $\overline{r} = \overline{r_1} + \overline{a_1}t$, $\overline{r} = \overline{r_2} + \overline{a_2}t$. Тогда расстояние ρ между ними равно следующей величине:*

$$\rho = \frac{|(\overline{a_1}, \overline{a_2}, \overline{r_1} - \overline{r_2})|}{|[\overline{a_1}, \overline{a_2}]|}$$

Доказательство. Искомое расстояние ρ является длиной высоты параллелепипеда, построенного на векторах $\overline{a_1}$, $\overline{a_2}$ и $\overline{r_1} - \overline{r_2}$, проведенной к грани, образованной векторами $\overline{a_1}$, $\overline{a_2}$ и имеющей площадь $|\overline{a_1}||\overline{a_2}| \sin \angle(\overline{a_1}, \overline{a_2}) = |[\overline{a_1}, \overline{a_2}]|$, из чего и следует требуемое. □

4 Алгебраические кривые

4.1 Многочлены

Определение 4.1. *Одночленом*, или *мономом*, от переменных $x_1, \ldots, x_n$ называется выражение вида $\alpha x_1^{k_1} \cdots x_n^{k_n}$, где $\alpha \in \mathbb{R}$, $k_1, \ldots, k_n \in \mathbb{N} \cup \{0\}$. *Многочленом*, или *полиномом*, от переменных $x_1, \ldots, x_n$ называется линейная комбинация одночленов от $x_1, \ldots, x_n$.

Определение 4.2. *Несократимой записью* многочлена $P(x_1, \ldots, x_n)$ называется представление этого многочлена в виде линейной комбинации одночленов $\alpha x_1^{k_1} \cdots x_n^{k_n}$ с ненулевыми коэффициентами α и попарно различными наборами степеней $k_1, \ldots, k_n$.

Утверждение 4.1. *Если несократимая запись многочлена $P(x_1, \ldots, x_n)$ содержит хотя бы один моном, то $P \neq 0$.*

Доказательство. Проведем индукцию по n. База, $n = 1$, тривиальна: ненулевой многочлен $P(x_1)$ имеет лишь конечное число корней. Докажем переход. Для этого сгруппируем в $P(x_1, \ldots, x_n)$ мономы с одинаковой степенью при x_n:

$$P(x_1, \ldots, x_n) = \sum_{j=0}^{d} Q_j(x_1, \ldots, x_{n-1}) x_n^j$$

Хотя бы один многочлен Q_t имеет ненулевую несократимую запись. Тогда, по предположению индукции, существуют $a_1, \ldots, a_{n-1} \in \mathbb{R}$ такие, что $Q_t(a_1, \ldots, a_{n-1}) \neq 0$. Тогда:

$$P(a_1, \ldots, a_{n-1}, x_n) = \sum_{j=0}^{d} Q_j(a_1, \ldots, a_{n-1}) x_n^j$$

Полученное выражение — это многочлен от одной переменной x_n с ненулевой несократимой записью. Он имеет конечное число корней, поэтому существует $a_n \in \mathbb{R}$ такое, что $P(a_1, \ldots, a_{n-1}, a_n) \neq 0$. $\square$

Следствие. Несократимая запись многочлена $P(x_1, \ldots, x_n)$ единственна.

Доказательство. Предположим, что у $P(x_1, \ldots, x_n)$ есть две различных несократимых записи P_1 и P_2. Тогда несократимая запись разности $P_1 - P_2$ содержит хотя бы один моном, но эта же запись должна быть тождественно нулевой, что невозможно по утверждению выше. $\square$

Определение 4.3. *Степенью одночлена $\alpha x_1^{k_1} \cdots x_n^{k_n}$* с ненулевым коэффициентом α называется число $k_1 + \cdots + k_n$. *Степенью многочлена* называется наибольшая из степеней одночленов, входящих в его несократимую запись. Обозначение — $\deg P$. Считается также, что $\deg 0 = -\infty$.

Утверждение 4.2. *Для любых многочленов P, Q выполнено следующее неравенство:*

$$\deg (P + Q) \leqslant \max\{\deg P, \deg Q\}$$

Доказательство. Сложим несократимые записи многочленов P и Q. Приводя подобные слагаемые, получим несократимую запись многочлена $P + Q$. В ней не будет мономов степени, превосходящей $\max\{\deg P, \deg Q\}$. $\square$

Утверждение 4.3. *Для любых многочленов P, Q выполнено следующее равенство:*

$$\deg PQ = \deg P + \deg Q$$

Доказательство. Перемножим несократимые записи многочленов P и Q, получим сумму мономов со степенями, не превосходящими $\deg P + \deg Q$, поэтому $\deg (PQ) \leqslant \deg P + \deg Q$. Далее рассмотрим в несократимой записи P моном $a x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $a \neq 0$, удовлетворяющий следующим условиям:

- ▷ $\alpha_1 + \cdots + \alpha_n = \deg P$, то есть моном имеет наибольшую степень

- ▷ Среди всех мономов, удовлетворяющих предыдущему пункту, показатель степени α_1 у данного монома наибольший
- ▷ Среди всех мономов, удовлетворяющих предыдущему пункту, показатель степени α_2 у данного монома наибольший, и так далее

Аналогичным образом выберем в Q моном $bx_1^{\beta_1}\cdots x_n^{\beta_n}$, $b \neq 0$. Произведение выбранных мономов дает моном $abx_1^{\alpha_1+\beta_1}\ldots x_n^{\alpha_n+\beta_n}$, $ab \neq 0$. Пусть моном с такими же показателями степеней появился как произведение мономов $cx_1^{\gamma_1}\ldots x_n^{\gamma_n}$, $c \neq 0$, из P и $dx_1^{\delta_1}\ldots x_n^{\delta_n}$, $d \neq 0$, из Q, тогда:

- ▷ $\gamma_1+\cdots+\gamma_n \leqslant \alpha_1+\cdots+\alpha_1$ и $\delta_1+\cdots+\delta_n \leqslant \beta_1+\cdots+\beta_1$, поэтому в обоих неравенствах имеет место равенство
- ▷ $\gamma_1 \leqslant \alpha_1$ и $\delta_1 \leqslant \beta_1$, поэтому в обоих неравенствах имеет место равенство
- ▷ $\gamma_2 \leqslant \alpha_2$ и $\delta_2 \leqslant \beta_2$, поэтому в обоих неравенствах имеет место равенство, и так далее

Таким образом, все степени в данных парах мономов совпадают, тогда, в силу несократимости записей, совпадают и эти мономы. Значит, после приведения подобных слагаемых моном $abx_1^{\alpha_1+\beta_1}\ldots x_n^{\alpha_n+\beta_n}$, $ab \neq 0$, степени $\deg P + \deg Q$ сократиться не мог, откуда $\deg(PQ) = \deg P + \deg Q$. □

Теорема 4.1. *Пусть $P(x,y,z)$ — многочлен от координат точки в декартовой системе координат в P_3, и пусть при замене координат в P_3 из функции $P(x,y,z)$ была получена функция $Q(x',y',z')$. Тогда Q — тоже многочлен, причем $\deg Q = \deg P$.*

Доказательство. Формула замены координат имеет вид $(x,y,z)^T = S(x',y',z')^T + \gamma$ для некоторой матрицы $S \in M_3$ и столбца $\gamma \in M_{3\times 1}$. Значит, каждая из переменных x,y,z заменяется на линейную комбинацию выражений $x',y',z',1$. При подстановке этих выражений в $P(x,y,z)$ получится многочлен, причем, очевидно, $\deg Q \leqslant \deg P$. Наконец, поскольку возможен обратный переход к переменным x,y,z, переводящий $Q(x',y',z')$ в $P(x,y,z)$, то $\deg P \leqslant \deg Q$. Значит, $\deg P = \deg Q$. □

Замечание. Аналогичное утверждение верно и для пространства P_2.

Определение 4.4. *Алгебраической кривой* называется множество всех точек в P_2, координаты которых в некоторой декартовой системе координат удовлетворяют уравнению $P(x,y) = 0$, где P — многочлен. *Порядком кривой* называется наименьшая степень многочлена, задающего данную кривую.

Замечание. Порядок алгебраической кривой не зависит от выбора системы координат.

Замечание. Аналогичным образом можно определить *алгебраические поверхности* и их порядок в P_3. Понятно также, что алгебраическая кривая первого порядка — это прямая, а алгебраическая поверхность первого порядка — это плоскость.

Утверждение 4.4. *Объединение и пересечение алгебраических кривых также являются алгебраическими кривыми.*

Доказательство. Пусть две кривые задаются многочленами $P_1(x,y)$ и $P_2(x,y)$ соответственно. Тогда объединение кривых задается следующим уравнением:

$$P_1(x,y)P_2(x,y) = 0$$

Пересечение кривых задается следующим уравнением:

$$(P_1(x,y))^2 + (P_2(x,y))^2 = 0$$

Видно, что оба полученных выражения также являются многочленами. □

Утверждение 4.5. *Сечение алгебраической поверхности плоскостью является алгебраической кривой в этой плоскости.*

Доказательство. Перейдем в такую систему координат в P_3, в которой плоскость будет задаваться уравнением $z = 0$. Пусть алгебраическая поверхность в этой системе задается многочленом $P(x, y, z)$, тогда уравнение сечения имеет вид $P(x, y, 0) = 0$. Значит, сечение является алгебраической кривой. □

4.2 Кривые второго порядка

Определение 4.5. Пусть $A, B, C, D, E, F \in \mathbb{R}$, $A^2 + B^2 + C^2 \neq 0$. *Кривой второго порядка* называется алгебраическая кривая, которая в некоторой прямоугольной декартовой системе координат в P_2 задается следующим уравнением:

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

Теорема 4.2. *Любое уравнение кривой второго порядка в некоторой прямоугольной декартовой системой координат в P_2 имеет один из девяти канонических видов:*

- ▷ *Кривые эллиптического типа:*
  - $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, $a \geqslant b > 0$, — *эллипс*
  - $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0$, $a \geqslant b > 0$, — *точка*
  - $\frac{x^2}{a^2} + \frac{y^2}{b^2} = -1$, $a \geqslant b > 0$, — *мнимый эллипс*
- ▷ *Кривые гиперболического типа:*
  - $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$, $a, b > 0$, — *гипербола*
  - $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$, $a, b > 0$, — *пара пересекающихся прямых*
- ▷ *Кривые параболического типа:*
  - $y^2 = 2px$, $p > 0$, — *парабола*
  - $\frac{y^2}{a^2} = 1$, $a > 0$, — *пара параллельных прямых*
  - $\frac{y^2}{a^2} = 0$, $a > 0$, — *пара совпадающих прямых*
  - $\frac{y^2}{a^2} = -1$, $a > 0$, — *пара мнимых параллельных прямых*

Доказательство. Пусть в исходной прямоугольной декартовой системе координат в P_2 кривая второго порядка задается уравнением $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$. Процесс перехода в искомую систему координат происходит в три этапа:

1. Если $B \neq 0$, избавимся от монома $2Bxy$. Для этого произведем поворот системы координат на угол α против часовой стелки. Матрица перехода S при таком преобразовании имеет следующий вид:

$$S = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Тогда, по свойству замены координат:

$$\begin{cases} x = x'\cos\alpha - y'\sin\alpha \\ y = x'\sin\alpha + y'\cos\alpha \end{cases}$$

Определим значение α, при котором коэффициент при $x'y'$ обращается в 0:

$$-2A\sin\alpha\cos\alpha + 2B(\cos^2\alpha - \sin^2\alpha) + 2C\sin\alpha\cos\alpha = 0 \Rightarrow 2B\cos 2\alpha = (A-C)\sin 2\alpha$$

Если $A = C$, то выберем $\alpha = \frac{\pi}{4}$, иначе — такой α, что $\operatorname{tg} 2\alpha = \frac{2B}{A-C}$. В новой системе координат получим выражение вида $A'x'^2 + C'y'^2 + 2D'x' + 2E'y' + F' = 0$.

2. Если $A' \neq 0$, избавимся от монома $2D'x'$. Для этого произведем следующий сдвиг системы координат:
$$\begin{cases} x' = x'' + \dfrac{D'}{A'} \\ y' = y'' \end{cases}$$
После этого получим выражение $A''x''^2 + C''y''^2 + 2E''y'' + F'' = 0$.

3. Если $C'' \neq 0$, избавимся от монома $2E''y''$, аналогично пункту (2).

Опустим штрихи в записи уравнения в полученной системе координат. После того, как произведены операции выше, могут быть получены три различных результата:

1. Если $AC > 0$, то ни один из мономов x^2, y^2 не сократился, и полученное уравнение имеет вид $Ax^2 + Cy^2 + F = 0$. Если $A, C < 0$, домножим уравнение на -1. Перенесем F в другую часть и, если $F \neq 0$, разделим уравнение на $|F|$. После данных операций получим уравнение следующего вида:
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = \varepsilon,\ a, b > 0,\ \varepsilon \in \{-1, 0, 1\}$$
Если $a < b$, то поменяем координаты местами. Получено уравнение кривой эллиптического типа.

2. Если $AC < 0$, то ни один из мономов x^2, y^2 не сократился, и полученное уравнение имеет вид $Ax^2 + Cy^2 + F = 0$. Аналогичными описанным в предыдущем пункте преобразованиями, получим уравнение следующего вида:
$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = \varepsilon,\ a, b > 0,\ \varepsilon \in \{0, 1\}$$
Получено уравнение кривой гиперболического типа.

3. Если $AC = 0$, то одно из чисел A, C осталось ненулевым, поскольку многочлен в уравнении должен иметь степень 2. Заменой системы координат можно добиться того,

чтобы это было число C. Тогда полученное уравнение имеет вид $Cy^2 + 2Dx + F = 0$. Если $D \neq 0$, то сдвиг системы координат позволяет избавиться от F и получить уравнение следующего вида:

$$y^2 = 2px,\ p > 0$$

Если же $D = 0$, то уравнение можно привести к следующему виду:

$$\frac{y^2}{a^2}\varepsilon,\ a > 0,\ \varepsilon \in \{-1, 0, 1\}$$

Получено уравнение кривой параболического типа. □

Определение 4.6. *Канонической системой координат* для кривой второго порядка называется такая прямоугольная декартова система координат, в которой данная кривая имеет уравнение канонического вида.

Определение 4.7. *Центром многочлена* $P(x, y)$ в декартовой системе координат (O, e) в P_2 называется такая точка $A \in P_2$, $A \leftrightarrow_{(O,e)} \alpha$, что для любых чисел $x, y \in \mathbb{R}$ выполнено равенство $P(\alpha_1 - x, \alpha_1 - y) = P(\alpha_1 + x, \alpha_2 + y)$.

Утверждение 4.6. *Если в декартовой системе координат (O, e) в P_2 точка $A \in P_2$, $A \leftrightarrow_{(O,e)} \alpha$, является центром многочлена $P(x, y)$, то A — центр симметрии кривой, заданной уравнением $P(x, y) = 0$.*

Доказательство. По условию, любые две точки в P_2, симметричные относительно точки A, или одновременно принадлежат кривой, или одновременно не принадлежат ей. □

Замечание. Можно показать, что верно и такое утверждение: если точка $A \in P_2$ является центром симметрии непустой кривой второго порядка, задаваемой многочленом $P(x, y)$, то A также является центром симметрии многочлена $P(x, y)$.

Замечание. Начало координат в канонической системе координат любой кривой второго порядка является ее центром симметрии, если эта кривая имеет хотя бы один центр симметрии.

Утверждение 4.7. *Пусть $A \in P_2$, в декартовой системе координат (O, e) в P_2 выполнено $A \leftrightarrow_{(O,e)} \alpha$, и пусть $P(x, y) = Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F$. Тогда:*

$$A \text{ — \textit{центр многочлена} } P(x, y) \Leftrightarrow \begin{cases} A\alpha + B\beta + D = 0 \\ B\alpha + C\beta + E = 0 \end{cases}$$

Доказательство. Доказательство производится непосредственной проверкой. □

Определение 4.8. Кривая второго порядка называется *центральной*, если у нее существует единственный центр симметрии.

Замечание. Если кривая задана уравнением $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F$, то, согласно правилу Крамера, она центральна $\Leftrightarrow AC \neq B^2$.

Замечание. Из непустых кривых второго порядка центральными являются только кривые эллиптического и гиперболического типа.

4.3 Эллипс, гипербола и парабола

Определение 4.9. *Эллипсом* называется кривая второго порядка, которая в канонической системе координат (O, e) задается следующим уравнением:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,\ a \geqslant b > 0$$

- ▷ *Вершинами* эллипса называются точки с координатами $(\pm a, 0)^T$, $(0, \pm b)^T$ в системе (O, e). Число a называется *длиной большой полуоси* эллипса, число b — *длиной малой полуоси* эллипса.
- ▷ *Фокусным расстоянием* эллипса называется величина $c := \sqrt{a^2 - b^2}$. *Фокусами* эллипса называются точки $F_1, F_2 \in P_2$ такие, что $F_1 \leftrightarrow_{(O,e)} (c, 0)^T$, $F_2 \leftrightarrow_{(O,e)} (-c, 0)^T$.
- ▷ *Эксцентриситетом* эллипса называется величина $\varepsilon := \frac{c}{a} = \frac{\sqrt{a^2-b^2}}{a}$.
- ▷ *Директрисами* эллипса называются прямые d_1, d_2, задаваемые в системе (O, e) уравнениями $x = \pm\frac{a}{\varepsilon}$.

Теорема 4.3. *Пусть эллипс задан в канонической системе координат (O, e), $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$. Тогда точка A лежит на эллипсе $\Leftrightarrow AF_1 = |a - \varepsilon x| \Leftrightarrow AF_2 = |a + \varepsilon x|$.*

Доказательство. Докажем, что A лежит на эллипсе $\Leftrightarrow AF_1 = |a - \varepsilon x|$. Для этого заметим, что выполнены следующие равенства:

$$AF_1^2 - |a - \varepsilon x|^2 = (x - c)^2 + y^2 - |a - \varepsilon x|^2 = b^2 \left(\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 \right)$$

Значит, $AF_1 = |a - \varepsilon x| \Leftrightarrow \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \Leftrightarrow A$ лежит на эллипсе. Аналогично доказывается, что $AF_2 = |a + \varepsilon x| \Leftrightarrow A$ лежит на эллипсе. □

Теорема 4.4. *Пусть эллипс задан в канонической системе координат (O, e). Тогда он является геометрическим местом точек $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$, таких, что выполнены следующие равенства:*

$$\frac{AF_1}{\rho(A, d_1)} = \frac{AF_2}{\rho(A, d_2)} = \varepsilon$$

Доказательство. Заметим, что выполнены следующие равенства:

$$\rho(A, d_1) = \left| x - \frac{a}{\varepsilon} \right| = \frac{1}{\varepsilon}|a - \varepsilon x|$$

Значит, A лежит на эллипсе $\Leftrightarrow |a - \varepsilon x| = AF_1 \Leftrightarrow \varepsilon\rho(A, d_1) = AF_1$. Аналогично доказывается, что A лежит на эллипсе $\Leftrightarrow \varepsilon\rho(A, d_2) = AF_2$. □

Теорема 4.5. *Пусть эллипс задан в канонической системе координат (O, e). Тогда он является геометрическим местом точек $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$, таких, что выполнено равенство $AF_1 + AF_2 = 2a$.*

Доказательство.

$\Rightarrow$ Пусть A лежит на эллипсе, тогда $AF_1 = a - \varepsilon x$ и $AF_2 = a + \varepsilon x$, откуда $AF_1 + AF_2 = 2a$.

$\Leftarrow$ Зафиксируем произвольное число $x_0 \in \mathbb{R}$ и заметим, что при движении точки $X \in P_2$, $X \leftrightarrow_{(O,e)} (x_0, 0)^T$ вдоль прямой $x = x_0$ вверх или вниз величина $XF_1 + XF_2$ строго возрастает. Рассмотрим возможные случаи:

1. Если $|x_0| < a$, то таких точек, что $XF_1 + XF_2 = 2a$, на прямой $x = x_0$ две.
2. Если $|x_0| = a$, то такая точка, что $XF_1 + XF_2 = 2a$, на прямой $x = x_0$ одна.
3. Если $|x_0| > a$, то таких точек, что $XF_1 + XF_2 = 2a$, на прямой $x = x_0$ нет.

Полученное точек совпадает с множеством точек эллипса. $\square$

Определение 4.10. *Гиперболой* называется кривая второго порядка, которая в канонической системе координат (O, e) задается следующим уравнением:

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1,\ a, b > 0$$

- $\triangleright$ *Вершинами* гиперболы называются точки с координатами $(\pm a, 0)^T$ в системе (O, e). Число a называется *длиной действительной полуоси* гиперболы, число b — *длиной мнимой полуоси* гиперболы.
- $\triangleright$ *Фокусным расстоянием* гиперболы называется величина $c := \sqrt{a^2 + b^2}$. *Фокусами* гиперболы называются точки $F_1, F_2 \in P_2$ такие, что $F_1 \leftrightarrow_{(O,e)} (c, 0)^T$, $F_2 \leftrightarrow_{(O,e)} (-c, 0)^T$.
- $\triangleright$ *Эксцентриситетом* гиперболы называется величина $\varepsilon := \frac{c}{a} = \frac{\sqrt{a^2+b^2}}{a}$.
- $\triangleright$ *Директрисами* гиперболы называются прямые d_1, d_2, задаваемые в системе (O, e) уравнениями $x = \pm\frac{a}{\varepsilon}$.

Теорема 4.6. *Пусть гипербола задана в канонической системе координат (O, e), $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$. Тогда точка A лежит на гиперболе $\Leftrightarrow AF_1 = |a - \varepsilon x| \Leftrightarrow AF_2 = |a + \varepsilon x|$.*

Доказательство. Докажем, что A лежит на гиперболе $\Leftrightarrow AF_1 = |a - \varepsilon x|$. Для этого заметим, что выполнены следующие равенства:

$$AF_1^2 - |a - \varepsilon x|^2 = (x - c)^2 + y^2 - |a - \varepsilon x|^2 = b^2 \left(\frac{x^2}{a^2} - \frac{y^2}{b^2} - 1 \right)$$

Значит, $AF_1 = |a - \varepsilon x| \Leftrightarrow \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \Leftrightarrow A$ лежит на гиперболе. Аналогично доказывается, что $AF_2 = |a + \varepsilon x| \Leftrightarrow A$ лежит на гиперболе. $\square$

Теорема 4.7. *Пусть гипербола задана в канонической системе координат (O, e). Тогда она является геометрическим местом точек $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$, таких, что выполнены следующие равенства:*

$$\frac{AF_1}{\rho(A, d_1)} = \frac{AF_2}{\rho(A, d_2)} = \varepsilon$$

Доказательство. Заметим, что выполнены следующие равенства:

$$\rho(A, d_1) = \left| x - \frac{a}{\varepsilon} \right| = \frac{1}{\varepsilon} |a - \varepsilon x|$$

Значит, A лежит на гиперболе $\Leftrightarrow |a - \varepsilon x| = AF_1 \Leftrightarrow \varepsilon\rho(A, d_1) = AF_1$. Аналогично доказывается, что A лежит на эллипсе $\Leftrightarrow \varepsilon\rho(A, d_2) = AF_2$. $\square$

Теорема 4.8. *Пусть гипербола задана в канонической системе координат (O, e). Тогда она является геометрическим местом точек $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$, таких, что выполнено равенство $|AF_1 - AF_2| = 2a$.*

Доказательство.

- $\Rightarrow$ Пусть A лежит на гиперболе. Если без ограничения общности точка A лежит на правой ее ветви, то тогда $AF_1 = \varepsilon x - a$ и $AF_2 = a + \varepsilon x$, тогда $|AF_1 - AF_2| = 2a$.

- $\Leftarrow$ Зафиксируем произвольное число $x_0 \in \mathbb{R}$ и заметим, что при движении точки $X \in P_2$, $X \leftrightarrow_{(O,e)} (x_0, 0)^T$ вдоль прямой $x = x_0$ вверх или вниз величина $|XF_1 - XF_2|$ строго убывает. Рассмотрим возможные случаи:

  1. Если $|x_0| > a$, то таких точек, что $|XF_1 - XF_2| = 2a$, на прямой $x = x_0$ две.
  2. Если $|x_0| = a$, то такая точка, что $|XF_1 - XF_2| = 2a$, на прямой $x = x_0$ одна.
  3. Если $|x_0| < a$, то таких точек, что $|XF_1 - XF_2| = 2a$, на прямой $x = x_0$ нет.

  Полученное точек совпадает с множеством точек гиперболы. □

Определение 4.11. Пусть гипербола задана в канонической системе координат (O, e). *Асимптотами* гиперболы называются прямые l_1, l_2, задаваемые в этой же системе уравнениями $\frac{x}{a} \pm \frac{y}{b} = 0$.

Утверждение 4.8. *Пусть гипербола задана в канонической системе координат (O, e), $A \in P_2$ — точка на гиперболе. Тогда выполнено следующее равенство:*

$$\rho(A, l_1)\rho(A, l_2) = \frac{a^2b^2}{a^2 + b^2}$$

Доказательство. Пусть $A \leftrightarrow_{(O,e)} (x, y)^T$. По формуле расстояния от точки до прямой в плоскости, имеем:

$$\rho(A, l_1)\rho(A, l_2) = \frac{\left|\frac{x}{a} - \frac{y}{b}\right|}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} \frac{\left|\frac{x}{a} + \frac{y}{b}\right|}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} = \frac{b^2x^2 - a^2y^2}{a^2 + b^2} = \frac{a^2b^2\left(\frac{x^2}{a^2} - \frac{y^2}{b^2}\right)}{a^2 + b^2} = \frac{a^2b^2}{a^2 + b^2}$$

Получено требуемое. □

Следствие. Пусть гипербола задана в канонической системе координат (O, e). Если точка $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$, движется по одной полуветви гиперболы так, что $x \to \infty$, то расстояние от A до одной из асимптот стремится к 0.

Доказательство. Пусть без ограничения общности точка A движется так, что $x \to +\infty$ и $y \to +\infty$, тогда $\rho(A, l_2) \to +\infty$. Но величины $\rho(A, l_1)$ и $\rho(A, l_2)$ обратно пропорциональны, поэтому $\rho(A, l_1) \to 0$. □

Определение 4.12. *Параболой* называется кривая второго порядка, которая в канонической системе координат (O, e) задается следующим уравнением:

$$y^2 = 2px,\ p > 0$$

- ▷ *Вершиной* параболы называется точка с координатами $(0, 0)^T$ в системе (O, e).

- *Фокусом* параболы называется точка F такая, что $F \leftrightarrow_{(O,e)} \left(\frac{p}{2}, 0\right)^T$.
- *Эксцентриситетом* параболы называется величина $\varepsilon := 1$.
- *Директрисой* параболы называется прямая d, задаваемая в системе (O, e) уравнением $x = -\frac{p}{2}$.

Теорема 4.9. *Пусть парабола задана в канонической системе координат (O, e), $A \in P_2$, $A \leftrightarrow_{(O,e)} (x, y)^T$. Тогда точка A лежит на параболе $\Leftrightarrow$ $AF = \rho(A, d)$.*

Доказательство. Заметим, что выполнены следующие равенства:

$$AF^2 - \rho^2(A, d) = \left(x - \frac{p}{2}\right)^2 + y^2 - \left(x + \frac{p}{2}\right)^2 = y^2 - 2px$$

Значит, $AF = \rho(A, d) = |x + \frac{p}{2}| \Leftrightarrow y^2 = 2px \Leftrightarrow A$ лежит на параболе. □

4.4 Сопряженные диаметры и касательные

Теорема 4.10. *Пусть C — эллипс, гипербола или парабола, C задана в канонической системе координат (O, e), $\overline{v} \in V_2$, $\overline{v} \neq \overline{0}$ — вектор направления, $\overline{v} \leftrightarrow_e \alpha$. Тогда центры всех хорд кривой C, параллельных вектору $\overline{v}$, лежат на одной прямой.*

Доказательство. Рассмотрим случай, когда C — гипербола, поскольку в остальных случаях доказательство аналогично. Пусть $A \leftrightarrow_{(O,e)} (x_0, y_0)^T$ — середина некоторой хорды, параллельной вектору $\overline{v}$. Точки пересечения прямой, содержащей данную хорду, с гиперболой C удовлетворяет следующему уравнению:

$$\frac{(x_0 + \alpha_1 t)^2}{a^2} - \frac{(y_0 + \alpha_2 t)^2}{b^2} = 1$$

Так как точка A является серединой хорды, то значения параметра t, удовлетворяющие уравнению, должны быть противоположными числами. Приведем данное уравнение к виду квадратного уравнения относительно t, тогда, по теореме Виета, коэффициент при t должен быть равен нулю, то есть:

$$\alpha_1 b^2 x_0 - \alpha_2 a^2 y_0 = 0$$

Таким образом, центры всех хорд, параллельных вектору $\overline{v}$, удовлетворяют следующему уравнению прямой:

$$\frac{\alpha_1 x}{a^2} - \frac{\alpha_2 y}{b^2} = 0$$ □

Определение 4.13. Пусть C — эллипс, гипербола или парабола, $\overline{v} \in V_2$, $\overline{v} \neq \overline{0}$ — вектор направления. *Диаметром, сопряженным к направлению $\overline{v}$ относительно кривой C*, называется прямая, содержащая середины всех хорд C, параллельных вектору $\overline{v}$.

Замечание. Пусть C — эллипс, гипербола или парабола, C задана в канонической системе координат (O, e), $\overline{v} \in V_2$, $\overline{v} \neq \overline{0}$ — вектор направления, $\overline{v} \leftrightarrow_e \alpha$. Тогда уравнения диаметров, сопряженных к направлению $\overline{v}$, имеют следующий вид:

- Если C — эллипс, то прямая задается уравнением $\frac{\alpha_1 x}{a^2} + \frac{\alpha_2 y}{b^2} = 0$ и имеет направляющий вектор $\overline{a} \in V_2$, $\overline{a} \leftrightarrow_e (\frac{\alpha_2}{b^2}, -\frac{\alpha_1}{a^2})^T$

- ▷ Если C — гипербола, то прямая задается уравнением $\frac{\alpha_1 x}{a^2} - \frac{\alpha_2 y}{b^2} = 0$ и имеет направляющий вектор $\overline{a} \in V_2$, $\overline{a} \leftrightarrow_e (\frac{\alpha_2}{b^2}, \frac{\alpha_1}{a^2})^T$
- ▷ Если C — парабола, то прямая задается уравнением $\alpha_2 y = \alpha_1 p$ и имеет направляющий вектор $\overline{a} \in V_2$, $\overline{a} \leftrightarrow_e (1, 0)^T$

Утверждение 4.9. *Пусть C — эллипс или гипербола, $\overline{v} \in V_2$, $\overline{v} \neq \overline{0}$ — вектор направления. Тогда если диаметр, сопряженный к $\overline{v}$, имеет направляющий вектор $\overline{u}$, то диаметр, сопряженный к $\overline{u}$, имеет направляющий вектор $\overline{v}$.*

Доказательство. Рассмотрим случай, когда C — гипербола, поскольку в случае эллипса доказательство аналогично. Пусть C задана в канонической системе координат (O, e), и пусть $\overline{v} \leftrightarrow_e \alpha$. Диаметр, сопряженный к направлению $\overline{v}$, имеет направляющий вектор $\overline{u} \in V_2$, $\overline{u} \leftrightarrow_e (\frac{\alpha_2}{b^2}, \frac{\alpha_1}{a^2})^T$. Диаметр, сопряженный к направлению $\overline{u}$, имеет направляющий вектор $\overline{w} \in V_2$, $\overline{w} \leftrightarrow_e (\frac{\alpha_1}{a^2 b^2}, \frac{\alpha_2}{a^2 b^2})^T$. Остается заметить, что $\overline{w} \parallel \overline{v}$. □

Определение 4.14. *Касательной* к кривой C в точке $A \in C$ называется предельное положение секущей AB, $B \in C$, при $B \to A$.

Утверждение 4.10. *Пусть C — эллипс, гипербола или парабола. Тогда диаметр, сопряженный к направлению касательной к C в точке $A \in C$, проходит через A.*

Доказательство. Пусть кривая C задана в канонической системе координат (O, e), и пусть $A \leftrightarrow_{(O,e)} (x_0, y_0)^T$. Когда точка B на гиперболе стремится к A, середина хорды AB также стремится к A, поэтому диаметр, содержащий середину хорды AB, в предельном случае проходит через A. □

Следствие. Пусть C — эллипс или гипербола, C задана в канонической системе координат (O, e), $A \in C$, $A \leftrightarrow_{(O,e)} (x_0, y_0)^T$. Тогда уравнения касательных к C в точке A имеют следующий вид:

- ▷ Если C — эллипс, то прямая задается уравнением $\frac{x_0 x}{a^2} + \frac{y_0 y}{b^2} = 1$
- ▷ Если C — гипербола, то прямая задается уравнением $\frac{x_0 x}{a^2} - \frac{y_0 y}{b^2} = 1$

Доказательство.

- ▷ Пусть C — эллипс, тогда диаметр, проходящий через точку A, задается уравнением $y_0 x - x_0 y = 0$ и имеет направляющий вектор с координатами $(x_0, y_0)^T$. Тогда сопряженный к нему диаметр и касательная в точке A имеют направляющий вектор с координатами $(\frac{y_0}{b^2}, -\frac{x_0}{a^2})^T$. С учетом того, что касательная проходит через точку A, получаем уравнение прямой $\frac{x_0 x}{a^2} + \frac{y_0 y}{b^2} = 1$.
- ▷ Пусть C — гипербола, тогда диаметр, проходящий через точку A, задается уравнением $y_0 x - x_0 y = 0$ и имеет направляющий вектор с координатами $(x_0, y_0)^T$. Тогда сопряженный к нему диаметр и касательная в точке A имеют направляющий вектор с координатами $(\frac{y_0}{b^2}, \frac{x_0}{a^2})^T$. С учетом того, что касательная проходит через точку A, получаем уравнение прямой $\frac{x_0 x}{a^2} - \frac{y_0 y}{b^2} = 1$. □

Утверждение 4.11. *Пусть C — парабола, заданная в канонической системе координат (O, e), $A \in C$, $A \leftrightarrow_{(O,e)} (x_0, y_0)^T$. Тогда уравнение касательной к C в точке A имеют следующий вид:*

$$y_0 y = p(x_0 + x)$$

Доказательство. Диаметр, проходящий через A, задается уравнением $y = y_0$, и при этом является сопряженным к направлению $\overline{v} \in V_2$, $\overline{v} \leftrightarrow_e \alpha$, касательной в точке A. Тогда имеет место равенство $\alpha_2 y_0 = \alpha_1 p$, поэтому можно считать, что $\alpha = (y_0, p)^T$. Значит, касательная в точке A задается следующим уравнением:

$$\frac{x - x_0}{y_0} = \frac{y - y_0}{p}$$

Преобразуя это уравнение с учетом того, что $y_0^2 = 2px_0$, получим следующее уравнение:

$$y_0 y = p(x_0 + x)$$ □

5 Алгебраические структуры

5.1 Группы

Определение 5.1. *Группой* называется множество G с определенной на нем бинарной операцией *умножения* $\cdot : G \times G \to G$, удовлетворяющей следующим условиям:

- ▷ $\forall a, b, c \in G : (ab)c = a(bc)$ (ассоциативность)
- ▷ $\exists e \in G : \forall a \in G : ae = ea = a$ (существование нейтрального элемента)
- ▷ $\forall a \in G : \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$ (существование обратного элемента)

Утверждение 5.1. *Нейтральный элемент e в группе $(G, \cdot)$ единственен.*

Доказательство. Пусть e и e' — нейтральные элементы в G. Тогда $e = ee' = e'$. □

Утверждение 5.2. *Обратный элемент к каждому элементу группы $(G, \cdot)$ единственен.*

Доказательство. Пусть для некоторых $b, c \in G$ выполнены равенства $ba = ac = e$. Тогда $b = be = b(ac) = (ba)c = ec = c$. □

Утверждение 5.3. *В группе $(G, \cdot)$ можно «сокращать», то есть для любых $a, b, c \in G$ таких, что $ab = ac$, выполнено $b = c$.*

Доказательство. Домножив обе части равенства $ab = ac$ на a^{-1}, получим требуемое. □

Определение 5.2. Группа называется $(G, \cdot)$ *абелевой*, если умножение в ней коммутативно, то есть для любых $a, b \in G$ выполнено $ab = ba$.

Пример. Рассмотрим несколько примеров абелевых групп:

- ▷ $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ являются абелевыми группами, при этом $(\mathbb{N}, +)$ — нет, поскольку в $\mathbb{N}$ нет обратных элементов
- ▷ $(M_{n\times k}, +)$, $(V_i, +)$ являются абелевыми группами
- ▷ $(\mathbb{Q}^*, \cdot) := (\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}^*, \cdot) := (\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}^*, \cdot) := (\mathbb{C}\backslash\{0\}, \cdot)$ являются абелевыми группами

Пример. *Группа перестановок* $(S_n, \circ)$, где $S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} : \sigma — \text{биекция}\}$, является неабелевой при $n \geqslant 3$. Эта группа будет изучена подробнее далее в курсе.

Определение 5.3. *Суммой множеств* A и B называется следующее множество:

$$A + B := \{a + b : a \in A, b \in B\}$$

Определение 5.4. Пусть $n \in \mathbb{N}$, $n \geqslant 2$. Числа $a, b \in \mathbb{Z}$ называются *сравнимыми по модулю* n, если $n \mid (a - b)$. Обозначение — $a \equiv_n b$. Сравнимость является отношением эквивалентности. Множество классов эквивалентности обозначается через $\mathbb{Z}_n$. Класс, которому принадлежит число $a \in \mathbb{Z}$, обозначается через $\overline{a}$.

Замечание. Для любого числа $a \in \mathbb{Z}$ выполнено равенство $\overline{a} = \{a + nk : k \in \mathbb{Z}\}$, поэтому класс $\overline{a}$ также обозначают через $a + n\mathbb{Z}$.

Пример. Для любых классов $\overline{a}, \overline{b} \in \mathbb{Z}_n$ их *сумма* определяется как сумма множеств, то есть $\overline{a} + \overline{b} := \overline{a + b}$. Тогда $(\mathbb{Z}_n, +)$ является абелевой группой. Ассоциативность, коммутативность, существование нейтрального и обратного элементов в $\mathbb{Z}_n$ выполнены как следствия соответствующих свойств сложения в $\mathbb{Z}$.

Определение 5.5. Пусть $(G, \cdot)$ — группа. Ее *подгруппой* называется такое ее непустое подмножество $H \subset G$, что выполнены следующие условия:

- $\forall a, b \in H : ab \in H$
- $\forall a \in H : a^{-1} \in H$

Замечание. Имеет место эквивалентное определение подгруппы, согласно которому подгруппой группы $(G, \cdot)$ называется такое ее непустое подмножество $H \subset G$, что $(H, \cdot)$ тоже является группой.

5.2 Кольца

Определение 5.6. *Кольцом* называется множество R с определенными на нем бинарными операциями *сложения* $+ : R \times R \to R$ и *умножения* $\cdot : R \times R \to R$, удовлетворяющими следующим условиям:

- $(R, +)$ — абелева группа, нейтральный элемент в которой обозначается через 0
- $\forall a, b, c \in R : (ab)c = a(bc)$ (ассоциативность умножения)
- $\forall a, b, c \in R : a(b + c) = ab + ac$ и $(a + b)c = ac + bc$ (дистрибутивность умножения относительно сложения)
- $\exists 1 \in R : \forall a \in R : a1 = 1a = a$ (существование нейтрального элемента относительно умножения)

Определение 5.7. Кольцо называется $(R, +, \cdot)$ *коммутативным*, если умножение в нем коммутативно, то есть для любых $a, b \in R$ выполнено $ab = ba$.

Утверждение 5.4. *Пусть $(K, +, \cdot)$ — кольцо. Тогда для любого $a \in R$ выполнены равенства $a0 = 0a = 0$.*

Доказательство. Докажем, что $a0 = 0$:

$$a0 + a0 = a(0 + 0) = a0 \Rightarrow a0 + a0 + (-a0) = a0 + (-a0) \Rightarrow a0 = 0$$

Аналогично доказывается, что $0a = 0$. □

Пример. Рассмотрим несколько примеров коммутативных колец:

- $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ являются коммутативными кольцами, при этом $(\mathbb{N},+,\cdot)$ — нет
- $(\mathbb{Z}[\sqrt{2}],+,\cdot)$, где $\mathbb{Z}[\sqrt{2}] := \{a+b\sqrt{2} : a,b\in\mathbb{Z}\}$, является коммутативным кольцом
- $(\mathbb{R}[x_1,\ldots,x_n],+,\cdot)$, где $\mathbb{R}[x_1,\ldots,x_n] := \{P : P$ — многочлен от переменных $x_1,\ldots,x_n\}$, является коммутативным кольцом

Пример. Кольцо $(M_n,+,\cdot)$ является некоммутативным кольцом при $n \geqslant 2$. Более того, некоммутативным кольцом также является $(M_n(R),+,\cdot)$, где $M_n(R)$ — множество матриц с элементами из произвольного кольца $(R,+,\cdot)$.

Утверждение 5.5. *Определим для любых классов $\overline{a},\overline{b}\in\mathbb{Z}_n$ их произведение как $\overline{a}\overline{b} := \overline{ab}$. Тогда $(\mathbb{Z}_n,+,\cdot)$ является коммутативным кольцом.*

Доказательство. Проверим, что определение умножения корректно. Пусть $a'\in\overline{a}$, $b'\in\overline{b}$, тогда $a' = a+kn$, $b' = b+ln$ для некоторых $k,l\in\mathbb{Z}$, и, следовательно:

$$a'b' = ab + n(la' + kb' + kln) \Rightarrow a'b' \in \overline{ab}$$

Ассоциативность и коммутативность умножения, дистрибутивность и существование нейтрального элемента относительно умножения в $\mathbb{Z}_n$ выполнены как следствия соответствующих свойств в $\mathbb{Z}$. □

Определение 5.8. *Подкольцом* кольца $(R,+,\cdot)$ называется такое его непустое подмножество $S\subset R$, что выполнены следующие условия:

- $(S,+)$ — подгруппа в $(R,+)$
- $\forall a,b\in S : ab\in S$
- $1\in S$

Замечание. Имеет место эквивалентное определение подкольца, согласно которому подкольцом кольца $(R,+,\cdot)$ называется такое его непустое подмножество $S\subset R$, что $(S,+,\cdot)$ тоже является кольцом.

5.3 Поля

Определение 5.9. Пусть $(R,+,\cdot)$ — кольцо. Элемент $a\in R$ называется *обратимым*, если существует $a^{-1}\in R$ такой, что $aa^{-1} = a^{-1}a = 1$. *Группой обратимых элементов* кольца $(R,+,\cdot)$ называется множество R^* его обратимых элементов.

Утверждение 5.6. *Пусть $(R,+,\cdot)$ — кольцо. Тогда $(R^*,\cdot)$ является группой.*

Доказательство. Множество R^* непусто, поскольку $1\in R^*$. Умножение в R^* определено корректно, поскольку если $a,b\in R^*$, то и $ab\in R^*$, причем обратный к ab элемент имеет вид $(ab)^{-1} = b^{-1}a^{-1}$. Свойства группы, очевидно, выполнены:

- $\forall a,b,c\in R^* : (ab)c = a(bc)$

▷ $\exists 1 \in R^* : \forall a \in R^* : a1 = 1a = a$

▷ $\forall a \in R^* : \exists a^{-1} \in R^* : aa^{-1} = a^{-1}a = 1$ □

Определение 5.10. *Полем* называется такое коммутативное кольцо $(F, +, \cdot)$, для которого выполнено равенство $F^* = F \backslash \{0\}$.

Пример. Рассмотрим несколько примеров полей:

▷ $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ являются полями

▷ $(\mathbb{Q}[\sqrt{2}], +, \cdot)$, где $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, является полем

Утверждение 5.7. *Пусть $n \in \mathbb{N}$, $n \geqslant 2$. Тогда кольцо $(\mathbb{Z}_n, +, \cdot)$ является полем $\Leftrightarrow$ число n является простым.*

Доказательство.

$\Rightarrow$ Предположим, что n — составное число, то есть $n = ab$ для некоторых $a, b \in \mathbb{N}$ таких, что $a, b > 1$. Тогда $\overline{a}, \overline{b} \neq \overline{0}$, при этом $\overline{a}\overline{b} = \overline{0}$. Покажем, что тогда $\overline{a} \notin \mathbb{Z}_n^*$. Пусть это не так, тогда, умножая обе части равенства $\overline{a}\overline{b} = \overline{0}$ на $\overline{a}^{-1}$, получим, что $\overline{b} = \overline{0}$, что неверно. Значит, $\mathbb{Z}_n^*$ не является полем — противоречие.

$\Leftarrow$ Пусть n — простое число. Зафиксируем произвольный класс $\overline{a} \in \mathbb{Z}_n \backslash \{\overline{0}\}$ и рассмотрим числа $a, 2a, \ldots, na$. Покажем, что все они дают разные остатки при делении на n. Действительно, если для некоторых $k, l \in \{1, \ldots, n\}$ выполнено $n|(k - l)a$, то либо $n \mid a$, что неверно, либо $n \mid (k - l)$, откуда $k = l$. Значит, существует $m \in \{1, \ldots, n\}$ такое, что $am \equiv_n 1$, то есть обратным к элементу $\overline{a}$ является элемент $\overline{m}$. □

Определение 5.11. *Подполем* поля $(F, +, \cdot)$ называется такое его непустое подмножество $S \subset F$, что выполнены следующие условия:

▷ $(S, +, \cdot)$ — подкольцо в $(F, +, \cdot)$

▷ $\forall a \in S \backslash \{0\} : a^{-1} \in S$

Замечание. Имеет место эквивалентное определение подполя, согласно которому подполем поля $(F, +, \cdot)$ называется такое его непустое подмножество $S \subset F$, что $(S, +, \cdot)$ тоже является полем.

Замечание. Далее в курсе при рассмотрении групп, колец и полей указание операций в них часто будет опускаться, если выбор операций понятен из контекста.

Определение 5.12. *Изоморфизмом полей* $(F_1, +, \cdot)$ и $(F_2, +, \cdot)$ называется такое биективное отображение $\varphi : F_1 \to F_2$, что для любых элементов $a, b \in F$ выполнены равенства $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$. Поля F_1 и F_2 называются *изоморфными*, если между ними существует изоморфизм. Обозначение — $F_1 \cong F_2$.

Утверждение 5.8. *Изоморфизм полей $\varphi : F_1 \to F_2$ обладает следующими свойствами:*

▷ $\varphi(0) = 0$

▷ $\varphi(1) = 1$

- ▷ $\forall a \in F_1 : \varphi(-a) = -\varphi(a)$
- ▷ $\forall a \in F_1^* : \varphi(a^{-1}) = (\varphi(a))^{-1}$

Доказательство.

- ▷ $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) \Rightarrow \varphi(0) = 0$
- ▷ В силу биективности и предыдущего пункта, $\varphi(1) \neq 0$, то есть элемент $\varphi(1)$ обратим, поэтому $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \Rightarrow \varphi(1) = 1$
- ▷ $\varphi(0) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a) \Rightarrow \varphi(-a) = -\varphi(a)$
- ▷ $\varphi(1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}$ □

Замечание. В любом поле F можно определить целое число n, отличное от 0 и 1:

- ▷ Если $n > 0$, то в поле F число n — это сумма n элементов 1
- ▷ Если $n < 0$, то в поле F число n — это сумма $|n|$ элементов -1

Арифметические операции с целыми числами в F согласованы с обычными арифметическими операциями.

Определение 5.13. Пусть F — поле. Его *характеристикой* называется наименьшее число $k \in \mathbb{N}$ такое, что в поле F выполнено равенство $k = 0$. Если такого k не существует, то характеристика поля считается равной 0. Обозначение — $\operatorname{char} F$.

Утверждение 5.9. *Пусть F — поле. Тогда если $\operatorname{char} F > 0$, то $\operatorname{char} F$ — простое число.*

Доказательство. Пусть $\operatorname{char} F = n$. Если $n = 1$, то элементы 0 и 1 в F совпадают, откуда $F^* = F$, что невозможно. Пусть теперь n — составное число, то есть $n = ab$ для некоторых $a, b \in \mathbb{N}$ таких, что $a, b > 1$. Тогда в поле F числа a, b отличны от нуля, но $ab = 0$. Умножая обе части равенства на a^{-1}, получим, что $b = 0$, — противоречие. Значит, возможен только случай простого числа n. □

Определение 5.14. Поле называется *простым*, если оно не имеет подполей, отличных от него самого.

Теорема 5.1 (о простом подполе)**.** *Пусть F — поле. Тогда:*

1. *Если $\operatorname{char} F = p > 0$, то в F существует подполе, изоморфное $\mathbb{Z}_p$*
2. *Если $\operatorname{char} F = 0$, то в F существует подполе, изоморфное $\mathbb{Q}$*

Доказательство.

1. Пусть $\operatorname{char} F = p$. Определим K как множество всех целых чисел в F, и зададим отображение $\varphi : \mathbb{Z}_p \to K$ как $\varphi(\overline{a}) := a$ для каждого $\overline{a} \in \mathbb{Z}_p$. Покажем, что отображение определено корректно. Пусть $\overline{a} = \overline{a'}$ для некоторых $a, a' \in \mathbb{Z}$, тогда $a' = a + kp$ для некоторого $k \in \mathbb{Z}$, откуда в поле F выполнены равенства $a' = a + kp = a$. Ясно, что определенное таким образом отображение φ сохраняет операции сложения и умножения.

Сюръективность отображения φ очевидна, проверим его инъективность. Пусть для некоторых $\overline{a}, \overline{b} \in Z_p$ выполнено $\varphi(\overline{a}) = \varphi(\overline{b})$. Без ограничения общности можно считать, что $a, b \in \{0, \ldots, p-1\}$ и $a \geqslant b$, тогда $\varphi\big(\overline{a-b}\big) = \varphi(\overline{a}) - \varphi\big(\overline{b}\big) = 0$. Но это возможно только в том случае, когда $p \mid (a-b)$, откуда $a = b$.

Из доказанного также следует, что K — подполе в F. Например, замкнутость относительно взятия обратного элемента по умножению можно показать, используя свойства отображения φ. Пусть $a \in K \backslash \{0\}$, тогда обратным к нему является элемент $\varphi(\overline{a}^{-1})$:

$$\varphi(\overline{a}^{-1})a = \varphi(\overline{a}^{-1})\varphi(\overline{a}) = \varphi(\overline{1}) = 1$$

Проверка остальных свойств подполя позволяет убедиться, что K является полем, тогда отображение φ является изоморфизмом полей.

2. Пусть $\operatorname{char} F = 0$. Определим K как множество всех выражений вида $\frac{a}{b} = ab^{-1}$, где $a, b \in F$ — целые числа в поле F, $b \neq 0$, и зададим $\varphi : \mathbb{Q} \to K$ как $\varphi(\frac{a}{b}) := \frac{a}{b}$ для каждого $\frac{a}{b} \in \mathbb{Q}$. Покажем, что отображение определено корректно. Пусть $\frac{a}{b} = \frac{a'}{b'}$ для некоторых $a, a', b, b' \in \mathbb{Z}$, $b, b' \neq 0$, тогда $a'b = ab'$, откуда в поле F выполнены равенства $ab^{-1} = (aa')(a'b)^{-1} = (aa')(ab')^{-1} = a'b'^{-1}$. Ясно, что определенное таким образом отображение φ сохраняет операции сложения и умножения.

   Сюръективность отображения φ очевидна, проверим его инъективность. Пусть для некоторых $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ выполнено $\varphi(\frac{a}{b}) = \varphi(\frac{c}{d})$, тогда $\varphi(\frac{ad-bc}{bd}) = \varphi(\frac{a}{b}) - \varphi(\frac{c}{d}) = 0$. Но это возможно только в том случае, когда $ad - bc = 0$, откуда $\frac{a}{b} = \frac{c}{d}$.

   Из доказанного также следует, что K — подполе в F. Например, замкнутость относительно взятия обратного элемента по умножению можно показать, используя свойства отображения φ. Пусть $\frac{a}{b} \in K \backslash \{0\}$, тогда $a \neq 0$, и обратным к элементу $\frac{a}{b}$ является элемент $\varphi(\frac{b}{a})$:

$$\frac{a}{b}\,\varphi\left(\frac{b}{a}\right) = \varphi\left(\frac{a}{b}\right)\varphi\left(\frac{b}{a}\right) = \varphi(1) = 1$$

   Проверка остальных свойств подполя позволяет убедиться, что K является полем, тогда отображение φ является изоморфизмом полей. □

6 Линейные пространства

6.1 Пространства и подпространства

Определение 6.1. *Линейным пространством*, или *векторным пространством*, над полем F называется абелева группа $(V, +)$, на которой определено *умножение на элементы поля* $\cdot : F \times V \to V$, удовлетворяющее следующим условиям:

- $\forall \alpha, \beta \in F : \forall \overline{v} \in V : (\alpha + \beta)\overline{v} = \alpha\overline{v} + \beta\overline{v}$
- $\forall \alpha \in F : \forall \overline{u}, \overline{v} \in V : \alpha(\overline{u} + \overline{v}) = \alpha\overline{u} + \alpha\overline{v}$
- $\forall \alpha, \beta \in F : \forall \overline{v} \in V : (\alpha\beta)\overline{v} = \alpha(\beta\overline{v})$
- $\forall \overline{v} \in V : 1\overline{v} = \overline{v}$

Элементы поля F называются *скалярами*, элементы группы V — *векторами*.

Пример. Рассмотрим несколько примеров линейных пространств:

- ▷ V_1, V_2, V_3 являются линейными пространствами над $\mathbb{R}$
- ▷ $F^n := M_{n\times 1}(F)$ является линейным пространством над полем F
- ▷ $M_{n\times k}(F)$ является линейным пространством над полем F
- ▷ $F[x]$ — множество многочленов от переменной x с коэффициентами из F — является линейным пространством над полем F
- ▷ Поле F является линейным пространством над своим подполем K

Утверждение 6.1. *Пусть V — линейное пространство над F. Тогда выполнены следующие свойства:*

- ▷ $\forall \overline{v} \in V : 0\overline{v} = \overline{0}$
- ▷ $\forall \alpha \in F : \alpha\overline{0} = \overline{0}$
- ▷ $\forall \overline{v} \in V : (-1)\overline{v} = -\overline{v}$

Доказательство.

- ▷ $0\overline{v} + 0\overline{v} = (0+0)\overline{v} = 0\overline{v} \Rightarrow 0\overline{v} = \overline{0}$
- ▷ $\alpha\overline{0} + \alpha\overline{0} = \alpha(\overline{0}+\overline{0}) = \alpha\overline{0} \Rightarrow \alpha\overline{0} = \overline{0}$
- ▷ $(-1)\overline{v} + 1\overline{v} = (-1+1)\overline{v} = 0\overline{v} = \overline{0} \Rightarrow (-1)\overline{v} = -1\overline{v} = -\overline{v}$ □

Определение 6.2. *Подпространством* линейного пространства V над полем F называется такое его непустое подмножество $U \subset V$, что выполнены следующие условия:

- ▷ $(U, +)$ — подгруппа в $(V, +)$
- ▷ $\forall \alpha \in F : \forall \overline{u} \in U : \alpha\overline{u} \in U$

Обозначение — $U \leqslant V$.

Замечание. Имеет место эквивалентное определение подпространства, согласно которому подпространством линейного пространства V над полем F называется такое его непустое подмножество $U \subset V$, которое тоже является линейным пространством над F.

Пример. Рассмотрим несколько примеров подпространств в соответствующих линейных пространствах:

- ▷ $U := \left\{(x_1, \ldots, x_n)^T \in F^n : x_1 + \cdots + x_n = 0\right\} \leqslant F^n$
- ▷ $U := \{A = (a_{ij}) \in M_{n\times k} : a_{11} = 0\} \leqslant M_{n\times k}$
- ▷ $U := \{P \in \mathbb{R}[x] : P(0) = 0\} \leqslant \mathbb{R}[x]$

Определение 6.3. Пусть V — линейное пространство над F, $\overline{v_1}, \ldots, \overline{v_k} \in V$. *Линейной оболочкой* векторов $\overline{v_1}, \ldots, \overline{v_k}$ называется множество линейных комбинаций этих векторов:

$$\langle \overline{v_1}, \ldots, \overline{v_k} \rangle := \left\{ \sum_{i=1}^{k} \alpha_i \overline{v_i} : \alpha_1, \ldots, \alpha_k \in F \right\}$$

Замечание. Линейную оболочку можно определить и для бесконечного набора векторов. В этом случае следует брать всевозможные линейные комбинации конечного числа векторов из набора.

Утверждение 6.2. *Пусть V — линейное пространство, $\overline{v_1}, \ldots, \overline{v_k} \in V$, $U := \langle \overline{v_1}, \ldots, \overline{v_k} \rangle$. Тогда $U \leqslant V$, и, более того, U является наименьшим по включению подпространством в V, содержащим все векторы $\overline{v_1}, \ldots, \overline{v_k}$.*

Доказательство. Сначала проверим, что U является линейным пространством:

- ▷ Множество U замкнуто относительно сложения и взятия обратного элемента п осложению, поэтому $(U, +)$ — подгруппа в $(V, +)$
- ▷ U замкнуто относительно умножения на скаляр

Наконец, если $W \leqslant V$ и $\overline{v_1}, \ldots, \overline{v_k} \in W$, то и $U = \langle \overline{v_1}, \ldots, \overline{v_k} \rangle \subset W$. □

6.2 Базисы и изоморфизмы

Определение 6.4. *Базисом* в линейном пространстве V называется такая линейно независимая система $(\overline{v_1}, \ldots, \overline{v_n})$ векторов из V, что $\langle \overline{v_1}, \ldots, \overline{v_n} \rangle = V$.

Замечание. В пространстве $\mathbb{R}[x]$ конечного базиса нет. Действительно, если $(P_1, \ldots, P_n)$ — конечная система многочленов из $\mathbb{R}[x]$, то через нее не выражаются многочлены степени большей, чем $\max\{\deg P_1, \ldots, \deg P_n\}$.

Определение 6.5. Линейное пространство V называется *конечнопорожденным*, если существуют векторы $\overline{v_1}, \ldots, \overline{v_n} \in V$ такие, что $\langle \overline{v_1}, \ldots, \overline{v_n} \rangle = V$.

Утверждение 6.3. *Любое конечнопорожденное пространство V обладает базисом.*

Доказательство. Выберем набор из минимального количества векторов $(\overline{u_1}, \ldots, \overline{u_k})$ такой, что $\langle \overline{u_1}, \ldots, \overline{u_k} \rangle = V$. Предположим, что он линейно зависим. Тогда без ограничения общности можно считать, что вектор $\overline{u_k}$ выражается через остальные векторы набора, то есть $\langle \overline{u_1}, \ldots, \overline{u_k} \rangle \subset \langle \overline{u_1}, \ldots, \overline{u_{k-1}} \rangle$. Тогда $\langle \overline{u_1}, \ldots, \overline{u_{k-1}} \rangle = \langle \overline{u_1}, \ldots, \overline{u_k} \rangle = V$ — противоречие с минимальностью. □

Пример. Базисами в соответствующих линейных пространствах являются:

- ▷ В F^n — $\left\{(1, 0, \ldots, 0)^T, (0, 1, \ldots, 0)^T, \ldots, (0, 0, \ldots, 1)^T\right\}$
- ▷ В $M_{n \times k}$ — $\{E_{ij} : i, j \in \{1, \ldots, n\}\}$, где E_{ij} — матрица из нулей с единственной единицей на позиции (i, j)

Замечание. Пусть e — базис в линейном пространстве V над полем F. Аналогично случаю V_n, для любого вектора $\overline{v} \in V$ определяется его координатный столбец в базисе e: если $\overline{v} = e\alpha$ для некоторого $\alpha \in F^n$, то $\overline{v} \leftrightarrow_e \alpha$. Координатный столбец каждого вектора существует и единственен, а сопоставление координат линейно.

Определение 6.6. *Изоморфизмом линейных пространств* U и V над полем F называется биективное отображение $\varphi : U \to V$, удовлетворяющее следующим условиям:

- ▷ $\forall \overline{u_1}, \overline{u_2} \in U : \varphi(\overline{u_1} + \overline{u_2}) = \varphi(\overline{u_1}) + \varphi(\overline{u_2})$

▷ $\forall \alpha \in F : \forall \overline{u} \in U : \varphi(\alpha\overline{u}) = \alpha\varphi(\overline{u})$

Пространства U и V называются *изоморфными*, если между ними существует изоморфизм. Обозначение — $U \cong V$.

Замечание. Если для некоторых линейных пространств U, V, W над одним выполнены соотношения $U \cong V$ и $V \cong W$, то $U \cong W$.

Утверждение 6.4. *Пусть V — линейное пространство с базисом из n элементов. Тогда $V \cong F^n$.*

Доказательство. Пусть $e = (\overline{e_1}, \ldots, \overline{e_n})$ — базис в пространстве V. Зададим отображение $\varphi : V \to F^n$ как $\varphi(\overline{v}) := \alpha$ для каждого $\overline{v} \in V$, где α — координатный столбец вектора $\overline{v}$ в базисе e. Уже было доказано, что отображение φ линейно. Кроме того, φ инъективно, поскольку разным векторам соответствуют разные координатные столбцы, и сюръективно, поскольку каждый столбец $\alpha \in F^n$ может быть получен как соответствующая линейная комбинация базисных векторов, поэтому φ — биекция. □

Следствие. Пусть V — линейное пространство над полем F, $|F| = k$, и базис в V состоит из n векторов. Тогда $|V| = |F^n| = k^n$.

Следствие. Пусть F — поле, $|F| = k$ и $\operatorname{char} F = p > 0$. Тогда $k = p^d$ для некоторого числа $d \in \mathbb{N}$.

Доказательство. Пусть $K \cong \mathbb{Z}_p$ — простое подполе в F, $|K| = p$, тогда F является линейным пространством над K. Поскольку F конечно, то оно является конечнопорожденным пространством, тогда в нем есть базис из d элементов для некоторого $d \in \mathbb{N}$, откуда $|F| = p^d$. □

6.3 Системы линейных уравнений

Определение 6.7. Пусть $A = (a_{ij}) \in M_{k\times n}(F)$, $b = (b_i) \in F^n$. *Системой линейных уравнений* $Ax = b$ называется следующая система:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \ldots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = b_k \end{cases}$$

Матрица A называется *матрицей системы*, матрица $(A|b)$ — *расширенной матрицей системы*.

Определение 6.8. Система линейных уравнений $Ax = b$ называется:

▷ *Однородной*, если $b = 0$

▷ *Совместной*, если множество ее решений непусто

Утверждение 6.5. *Множество решений однородной системы $Ax = 0$ является линейным пространством.*

Доказательство. Пусть V — множество решений. Оно непусто, поскольку $0 \in V$. Проверим замкнутость относительно сложения, взятия обратного элемента по сложению и умножения на скаляры:

- Если $v_1, v_2 \in V$, то $A(v_1 + v_2) = Av_1 + Av_2 = 0$, то есть $v_1 + v_2 \in V$
- Если $v \in V$, то для любого $\alpha \in F$ выполнено $A(\alpha v) = \alpha Av = 0$, то есть $\alpha v \in V$
- Из предыдущего пункта следует, что если $v \in V$, то $-v = (-1)v \in V$ □

Замечание. Чтобы найти все решения однородной системы линейных уравнений, достаточно найти базис пространства решений.

Утверждение 6.6. *Пусть $Ax = b$ — совместная система, $x_0 \in F^n$ — решение системы, V — пространство решений однородной системы $Ax = 0$. Тогда множество решений системы $Ax = b$ имеет вид $x_0 + V = \{x_0 + v : v \in V\}$.*

Доказательство. Пусть U — множество решений системы $Ax = b$.

- Если $v \in V$, то $A(x_0 + v) = Ax_0 + Av = b$, откуда $x_0 + v \in U$
- Если $u \in U$, то $A(u - x_0) = 0$, откуда $u - x_0 \in V$

Таким образом, $U = x_0 + V$. □

Определение 6.9. Системы $Ax = b$ и $A'x = b'$ называются *эквивалентными*, если множества их решений совпадают.

Определение 6.10. *Элементарными преобразованиями* строк матрицы $A \in M_{n\times k}(F)$ называются следующие операции:

- Прибавление к i-й строке j-й строки, умноженной на скаляр $\alpha \in F$, $i, j \in \{1, \dots, n\}$, $i \neq j$
- Умножение i-й строки на скаляр $\lambda \in F^*$, $i \in \{1, \dots, n\}$
- Перестановка i-й и j-й строк местами, $i, j \in \{1, \dots, n\}$, $i \neq j$

Определение 6.11. *Элементарными матрицами* порядка $n \in \mathbb{N}$ называются матрицы, умножение слева на которые приводит к осуществлению соответствующего элементарного преобразования строк над матрицей с n строками:

- $D_{ij}(\alpha) := E + \alpha E_{ij}$, $i, j \in \{1, \dots, n\}$, $i \neq j$
- $T_i(\lambda) := E + (\lambda - 1)E_{ii}$, $i \in \{1, \dots, n\}$
- $P_{ij} := E - (E_{ii} + E_{jj}) + (E_{ij} + E_{ji})$, $i, j \in \{1, \dots, n\}$, $i \neq j$

Замечание. Аналогично определяются элементарные преобразования столбцов. Они осуществляются умножением на элементарные матрицы справа.

Определение 6.12. Матрица $A \in M_n(F)$ называется *обратимой*, если существует матрица $A^{-1} \in M_n(F)$ такая, что $AA^{-1} = A^{-1}A = E$.

Утверждение 6.7. *Элементарные матрицы любого порядка n обратимы.*

Доказательство. Обратными к данным элементарным матрицам будет такие элементарные матрицы, которым соответствуют преобразования, обратные к данным, то есть такие, которые возвращают матрицу, к которой применено преобразование, в исходный вид:

- ▷ $(D_{ij}(\alpha))^{-1} = D_{ij}(-\alpha)$
- ▷ $(T_i(\lambda))^{-1} = T_i(\lambda^{-1})$
- ▷ $(P_{ij})^{-1} = P_{ij}$ □

Следствие. Рассмотрим расширенную матрицу $(A|b)$ системы $Ax = b$. Тогда элементарные преобразования строк этой матрицы переводят ее в расширенную матрицу эквивалентной системы.

Доказательство. Пусть L — элементарная матрица, тогда $L(A|b) = (LA|Lb)$. Зафиксируем произвольный столбец $x \in F^n$, тогда:

- ▷ Если $Ax = b$, то и $LAx = Lb$
- ▷ Если $LAx = Lb$, то $L^{-1}LAx = L^{-1}Lb \Leftrightarrow Ax = b$ □

Определение 6.13. *Главным* элементом строки называется ее первый ненулевой элемент. Нулевая строка не имеет главного элемента

Определение 6.14. Матрица $A \in M_{n\times k}(F)$ имеет *ступенчатый вид*, если номера главных элементов ее строк строго возрастают. При этом если в матрице есть нулевые строки, то они расположены внизу матрицы.

Теорема 6.1 (метод Гаусса)**.** *Любую матрицу $A \in M_{n\times k}(F)$ элементарными преобразованиями строк можно привести к ступенчатому виду.*

Доказательство. Предъявим алгоритм приведения к ступенчатому виду:

1. Если $A = 0$, то она уже имеет ступенчатый вид, тогда завершим процедуру.
2. Пусть $j \in \{1, \dots, k\}$ — наименьший номер ненулевого столбца. Переставим строки так, чтобы a_{1j} стал ненулевым.
3. Для всех $i \in \{2, \dots, n\}$ к i-й строке прибавим первую, умноженную на $-a_{ij}(a_{1j})^{-1}$. Тогда все элементы $a_{2j}, \dots, a_{nj}$ станут нулевыми.
4. Пусть матрица A была приведена к виду A'. Повторим шаги $(1), \dots, (4)$ для подматрицы B, расположенной на пересечении строк с номерами $2, \dots, n$ и столбцом с номерами $j+1, \dots, k$. Дальнейшие преобразования не изменят элементов за пределами этой подматрицы. □

Определение 6.15. Алгоритм приведения матрицы $A \in M_{n\times k}(F)$ к ступенчатому виду называется *прямым ходом метода Гаусса.*

Определение 6.16. В системе $Ax = b$ переменная x_i называется *главной*, если в матрице $(A|b)$, приведенной к ступенчатому виду, есть строка, где i-й элемент является главным. В противном случае x_i переменная называется *свободной.*

Теорема 6.2. *Пусть $(A|b)$ — расширенная матрица системы $Ax = b$, приведенная к ступенчатому виду. Тогда система совместна $\Leftrightarrow$ в $(A|b)$ нет «ступеньки», начинающейся в столбце b.*

Доказательство.

$\Rightarrow$ Пусть в $(A|b)$ есть ступенька, начинающаяся в b. Тогда она соответствует уравнению $0x_1 + \ldots + 0x_n = b_i \neq 0$, поэтому система несовместна — противоречие.

$\Leftarrow$ Присвоим свободным переменным произвольные значения. Тогда, двигаясь по матрице $(A|b)$ снизу вверх, выразим каждую главную переменную через свободные и предыдущие главные, и получим частное решение системы. $\square$

Замечание. Каждому набору значений свободных переменных в совместной системе соответствует единственное решение, и его можно получить описанным выше способом.

Определение 6.17. Матрица $A \in M_{n\times k}(F)$ имеет *упрощенный вид*, если она является ступенчатой, и всякий ее столбец, содержащий главный элемент, состоит из одной единицы, соответствующей главному элементу, и нулей.

Теорема 6.3. *Любую матрицу $A \in M_{n\times k}(F)$ элементарными преобразованиями строк можно привести к упрощенному виду.*

Доказательство. Сначала приведем матрицу A к ступенчатому виду, затем запустим следующий алгоритм:

- $\triangleright$ Если $A = 0$, она уже имеет упрощенный вид.
- $\triangleright$ Пусть $i \in \{1, \ldots, n\}$ — наибольший номер ненулевой строки, a_{ik} — главный элемент в ней. Умножим i-ю строку на $(a_{ik})^{-1}$, чтобы коэффициент a_{ik} стал равным 1.
- $\triangleright$ Для всех $j \in \{1, \ldots, i-1\}$ к j-й строке прибавим i-ю, умноженную на $-a_{jk}$. Тогда все элементы $a_{1k}, \ldots, a_{(i-1)k}$ станут нулевыми.
- $\triangleright$ Пусть матрица A была приведена к виду A'. Повторим шаги $(1), \ldots, (4)$ для подматрицы B, расположенной на пересечении строк $1, \ldots, i-1$ и столбцов $1, \ldots, k-1$. Дальнейшие преобразования не изменят элементов за пределами этой подматрицы. $\square$

Определение 6.18. Алгоритм приведения ступенчатой матрицы $A \in M_{n\times k}(F)$ к упрощенному виду называется *обратным ходом метода Гаусса.*

Замечание. Перестановка столбцов матрицы системы $Ax = b$ соответствует перестановке переменных. Такой перестановкой из упрощенного вида расширенной матрицы совместной системы $Ax = b$ можно получить следующую матрицу:

$$\left(\begin{array}{c|c|c} E & C & b \\ \hline 0 & 0 & 0 \end{array}\right) = \left(\begin{array}{ccc|ccc|c} 1 & \ldots & 0 & \alpha_1 & \ldots & \xi_1 & b_1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & \alpha_m & \ldots & \xi_m & b_m \\ \hline 0 & \ldots & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 & 0 \end{array}\right)$$

Это позволяет непосредственно выразить главные переменные через свободные. Нулевые строки при этом не влияют на множество решений системы, и их можно отбросить.

Определение 6.19. *Фундаментальной системой решений* однородной системы $Ax = 0$ называется базис пространства ее решений. Матрица, образованная столбцами фундаментальной системы решений, называется *фундаментальной матрицей системы* и обозначается через Φ.

Замечание. В силу уже доказанного, любое решение $v \in F^n$ системы $Ax = b$ может быть представлено в виде $v = x_0 + \Phi\gamma$, где $x_0 \in F^n$ — частное решение системы $Ax = b$, $\Phi \in M_{n\times m}(F)$ — фундаментальная матрица однородной системы $Ax = 0$, $\gamma \in F^m$ — произвольный столбец коэффициентов.

Теорема 6.4. *Пусть расширенная матрица системы $Ax = b$ имеет упрощенный вид $A = (E_k|B|b)$. Тогда фундаментальная матрица Φ однородной системы $Ax = 0$ и частное решение x_0 системы $Ax = b$ имеют следующий вид:*

$$\Phi = \left(\frac{-B}{E_{n-k}}\right), \; x_0 = \left(\frac{b}{0}\right)$$

Доказательство. Покажем сначала, что каждый столбец матрицы Φ является решением системы $Ax = 0$:

$$A\Phi = (E_k|B)\left(\frac{-B}{E_{n-k}}\right) = E_k(-B) + BE_{n-k} = 0$$

Теперь покажем, что столбцы матрицы Φ линейно независимы. Любая их линейная комбинация имеет следующий вид при некотором $\gamma \in F^k$:

$$\Phi\gamma = \left(\frac{-B\gamma}{E_{n-k}\gamma}\right) = \left(\frac{-B\gamma}{\gamma}\right)$$

Значит, что $\Phi\gamma = 0 \Leftrightarrow \gamma = 0$, что и означает требуемое. Наконец, пусть α — решение системы $Ax = 0$. Перепишем его в виде $\alpha = (\beta^T|\gamma^T)^T$, $\beta \in F^k$, $\gamma \in F^{n-k}$, и рассмотрим линейную комбинацию $\Phi\gamma$. Эта комбинация является решением системы $Ax = 0$, причем с теми же значениями свободных переменных, что и в α. Но главные переменные однозначно выражаются через свободные, поэтому $\Phi\gamma = \alpha$. Таким образом, матрица Φ является фундаментальной матрицей системы $Ax = 0$. Остается проверить, что x_0 является частным решением системы $Ax = b$:

$$Ax_0 = (E_k|B)\left(\frac{b}{0}\right) = E_k b + B0 = b$$

□

Замечание. Каждый из столбцов матрицы Φ получается следующим образом: одна из $n - k$ свободных переменных полагается равной единице, остальные — нулю, и главные переменные выражаются через ненулевую свободную.

Замечание. На практике, при решении систем можно предварительно не переставлять столбцы в расширенной матрице упрощенного вида, поскольку перестановке переменных соответствует перестановка строк Φ и x_0.

Утверждение 6.8. *Пусть $Ax = 0$ — однородная система, в которой $A \in M_{k\times n}(F)$, $n > k$. Тогда у этой системы есть нетривиальное решение.*

Доказательство. Приведем A к упрощенному виду A'. Главных переменных в полученной матрице не больше, чем k, значит, есть свободные переменные. Каждому набору свободных переменных соответствует единственное решение, значит, выбирая нетривиальный набор свободных переменных, получим нетривиальное решение. □

6.4 Размерности и ранги

Теорема 6.5 (основная лемма о линейной зависимости)**.** *Пусть V — линейное пространство над полем F, и $V = \langle \overline{v_1}, \ldots, \overline{v_k} \rangle$ для некоторых $\overline{v_1}, \ldots, \overline{v_k} \in V$. Тогда для любых векторов $\overline{u_1}, \ldots, \overline{u_n} \in V$, $n > k$, система $(\overline{u_1}, \ldots, \overline{u_n})$ линейно зависима.*

Доказательство. Векторы $\overline{u_1}, \ldots, \overline{u_n}$ выражаются через $\overline{v_1}, \ldots, \overline{v_k}$, поскольку лежат в их линейной оболочке $\langle \overline{v_1}, \ldots, \overline{v_k} \rangle = V$. Следовательно, $(\overline{u_1}, \ldots, \overline{u_n}) = (\overline{v_1}, \ldots, \overline{v_k})A$ для некоторой матрицы $A \in M_{k\times n}(F)$. Но $n > k$, поэтому существует такой ненулевой столбец $\gamma \in F^n$, что $A\gamma = 0$, тогда $(\overline{u_1}, \ldots, \overline{u_n})\gamma = (\overline{v_1}, \ldots, \overline{v_k})A\gamma = \overline{0}$. Значит, система линейно зависима. □

Следствие. Пусть V — линейное пространство с базисом из n векторов. Тогда любая система из $n+1$ вектора из V линейно зависима.

Доказательство. Пусть $e = (\overline{e_1}, \ldots, \overline{e_n})$ — базис в V, тогда $V = \langle \overline{e_1}, \ldots, \overline{e_n} \rangle$. Поэтому любая система из $n+1$ вектора из V линейно зависима. □

Следствие. Любые два базиса в конечнопорожденном линейном пространстве V равномощны.

Доказательство. Пусть e_1, e_2 — базисы в V. Если без ограничения общности $|e_1| < |e_2|$, то $e_2 \subset \langle e_1 \rangle$ и e_2 состоит из большего числа векторов, чем e_1, поэтому система e_2 линейно зависима — противоречие. □

Замечание. Для пространств, не являющихся конечнопорожденными, утверждение о равномощности базисов также справедливо.

Определение 6.20. Пусть V — конечнопорожденное линейное пространство. Его *размерностью* называется количество векторов в любом его базисе. Обозначение — $\dim V$.

Теорема 6.6. *Пусть U и V — конечнопорожденные линейные пространства над полем F. Тогда $U \cong V \Leftrightarrow \dim U = \dim V$.*

Доказательство.

- $\Rightarrow$ Пусть $(\overline{e_1}, \ldots, \overline{e_n})$ — базис в U. Рассмотрим изоморфизм $\varphi : U \to V$ и покажем, что система $(\varphi(\overline{e_1}), \ldots, \varphi(\overline{e_n}))$ образует базис в V. Проверим, что она линейно независима. Действительно, для любого $\gamma \in F^n$, $\gamma \neq \overline{0}$, выполнено следующее:

$$(\varphi(\overline{e_1}), \ldots, \varphi(\overline{e_n}))\gamma = \varphi((\overline{e_1}, \ldots, \overline{e_n})\gamma) \neq \varphi(\overline{0}) = \overline{0}$$

Кроме того, для любого вектора $\overline{v} \in V$ существует $\overline{u} \in U$ такой, что $\varphi(\overline{u}) = \overline{v}$, и существуют $\alpha_1, \ldots, \alpha_n \in F$ такие, что $\overline{u} = \sum_{i=1}^n \alpha_i \overline{e_i}$, тогда:

$$\overline{v} = \varphi(\overline{u}) = \varphi\left(\sum_{i-1}^{n} \alpha_i \overline{e_i}\right) = \sum_{i=1}^{n} \alpha_i \varphi(\overline{e_i})$$

Таким образом, $(\varphi(\overline{e_1}), \ldots, \varphi(\overline{e_n}))$ — базис в V, поэтому $\dim U = \dim V = n$.

$\Leftarrow$ Пусть $n := \dim U = \dim V$, тогда $U \cong F^n$ и $V \cong F^n$, откуда $U \cong V$. $\square$

Утверждение 6.9. *Пусть V — линейное пространство, $\dim V = n$. Тогда:*

1. *Если $V = \langle \overline{v_1}, \ldots, \overline{v_n} \rangle$, то система $(\overline{v_1}, \ldots, \overline{v_n})$ является базисом*

2. *Если система $(\overline{v_1}, \ldots, \overline{v_n})$ линейно независима, то она является базисом*

Доказательство.

1. Пусть $(\overline{v_1}, \ldots, \overline{v_n})$ не является базисом. Тогда она линейно зависима, и без ограничения общности вектор $\overline{v_n}$ выражается через $(\overline{v_1}, \ldots, \overline{v_{n-1}})$. Значит, $V = \langle \overline{v_1}, \ldots, \overline{v_{n-1}} \rangle$, но тогда в V нет линейно независимых систем из n векторов — противоречие с тем, что $\dim V = n$.

2. Предположим $(\overline{v_1}, \ldots, \overline{v_n})$ не является базисом. Следовательно, она выражает не все векторы пространства V, то есть существует $\overline{v} \in V$ такой, что $\overline{v} \notin \langle \overline{v_1}, \ldots, \overline{v_n} \rangle$. Но тогда система $(\overline{v_1}, \ldots, \overline{v_n}, \overline{v})$ тоже линейно независима — противоречие с тем, что $\dim V = n$. $\square$

Утверждение 6.10. *Пусть V — конечнопорожденное линейное пространство, $U \leqslant V$. Тогда пространство U — тоже конечнопорожденное, причем $\dim U \leqslant \dim V$.*

Доказательство. Будем выбирать из U векторы $\overline{u_1}, \overline{u_2}, \ldots$ так, чтобы система $(\overline{u_1}, \overline{u_2}, \ldots)$ оставалась линейно независимой. Процесс закончится не позднее, чем за $n := \dim V$ шагов, поскольку в V нет линейно независимой системы из $n+1$ вектора. Пусть полученная система — $(\overline{u_1}, \ldots, \overline{u_k})$, $k \leqslant n$. Она линейно независима по построению, и для любого $\overline{u} \in U$ система $(\overline{u_1}, \ldots, \overline{u_k}, \overline{u})$ уже линейно зависима, откуда $U = \langle \overline{u_1}, \ldots, \overline{u_k} \rangle$. Значит, полученная система образует базис в U. $\square$

Замечание. Если в доказательстве выше $k = n$, то $(\overline{u_1}, \ldots, \overline{u_n})$ — линейно независимая система из n векторов в V, поэтому она также является базисом в V, то есть $U = V$. Значит, если $U \neq V$, то $\dim U < \dim V$.

Утверждение 6.11. *Пусть V — конечнопорожденное линейное пространство размерности n, векторы $\overline{v_1}, \ldots, \overline{v_k} \in V$, $k < n$, образуют линейно независимую систему. Тогда систему $(\overline{v_1}, \ldots, \overline{v_k})$ можно дополнить до базиса в V.*

Доказательство. Выберем вектор $\overline{v_{k+1}} \in V$ такой, что $\overline{v_{k+1}} \notin \langle \overline{v_1}, \ldots, \overline{v_k} \rangle$, тогда система $(\overline{v_1}, \ldots, \overline{v_{k+1}})$ остается линейно независимой. Затем аналогично выберем вектор $\overline{v_{k+2}} \in V$ такой, что $\overline{v_{k+2}} \notin \langle \overline{v_1}, \ldots, \overline{v_{k+1}} \rangle$, и так далее. Процесс будет продолжаться, пока не будет получена система $(\overline{v_1}, \ldots, \overline{v_n})$, которая и является базисом. Он не может остановиться раньше, потому что пока в системе менее n векторов, она не выражает все пространство V, и не может продолжиться дольше, потому что в V нет линейно независимой системы из $n+1$ вектора. $\square$

Определение 6.21. Пусть V — конечнопорожденное линейное пространство, $X \subset V$. *Рангом* системы X называется наибольший размер линейно независимой подсистемы в X. Обозначение — $\operatorname{rk} X$.

Утверждение 6.12. *Пусть V — конечнопорожденное линейное пространство, $X \subset V$. Тогда $\operatorname{rk} X = \dim \langle X \rangle$.*

Доказательство. Пусть $k := \operatorname{rk} X$ и $(\overline{v_1}, \ldots, \overline{v_k})$ — линейно независимая система в X. Тогда для любого $\overline{v} \in X$ система $(\overline{v_1}, \ldots, \overline{v_k}, \overline{v})$ линейно зависима, откуда $X \subset \langle \overline{v_1}, \ldots, \overline{v_k} \rangle$. Но тогда $\langle X \rangle \subset \langle \overline{v_1}, \ldots, \overline{v_k} \rangle \subset \langle X \rangle$, откуда $\langle X \rangle = \langle \overline{v_1}, \ldots, \overline{v_k} \rangle$. Значит, $(\overline{v_1}, \ldots, \overline{v_k})$ — базис в $\langle X \rangle$, поэтому $\dim \langle X \rangle = k = \operatorname{rk} X$. □

Замечание. Аналогично случаю V_n, для базисов e и e' векторного пространства V над полем F определяется матрица перехода от e к e', то есть такая матрица $S \in M_n(F)$, что $e' = eS$. Если для некоторого вектора $\overline{v} \in V$ выполнено $\overline{v} \leftrightarrow_e \alpha$ и $\overline{v'} \leftrightarrow_{e'} \alpha'$, то $\alpha = S\alpha'$.

Утверждение 6.13. *Пусть V — линейное пространство над полем F, e, e' — базисы в V. Тогда матрица перехода $S \in M_n(F)$ от e к e' обратима.*

Доказательство. Поскольку возможен также обратный переход от e' к e, то существует матрица $T \in M_n(F)$ такая, что $e = e'T = e(ST)$, откуда $ST = E$ в силу единственности координатных столбцов векторов из в базисе e. Аналогично, $e' = eS = e'(TS)$, откуда $ST = TS = E$. □

Утверждение 6.14. *Пусть V — линейное пространство над полем F, $n := \dim V$, система e — базис в V, $S \in M_n(F)$ — обратимая матрица. Тогда система $e' = eS$ — тоже базис в V.*

Доказательство. $e' = eS \Leftrightarrow e = e'S^{-1}$, поэтому $e \subset \langle e' \rangle$, откуда $V \subset \langle e' \rangle$. Но в системе e' ровно n векторов, поэтому она образует базис в V. □

Определение 6.22. Пусть $A \in M_{n\times k}(F)$.

- ▷ *Строчным рангом* матрицы A называется ранг $\operatorname{rk}_r A$ системы ее строк
- ▷ *Столбцовым рангом* матрицы A называется ранг $\operatorname{rk}_c A$ системы ее столбцов

Утверждение 6.15. *Для любых матриц $A \in M_{n\times k}(F)$ и $B \in M_{k\times m}(F)$ выполнены неравенства $\operatorname{rk}_c AB \leqslant \operatorname{rk}_c A$ и $\operatorname{rk}_r AB \leqslant \operatorname{rk}_r B$.*

Доказательство. Докажем первое неравенство, поскольку второе неравенство доказывается аналогично. Пусть U — линейная оболочка столбцов матрицы A, V — линейная оболочка столбцов матрицы AB. Уже было доказано, что столбцы матрицы AB являются линейными комбинациями столбцов матрицы A, поэтому $V \leqslant U$. Следовательно, $\operatorname{rk}_r(AB) = \dim V \leqslant \dim U = \operatorname{rk}_r A$. □

Теорема 6.7 (о ранге матрицы)**.** *Для любой матрицы $A \in M_{n\times k}(F)$ выполнено следующее равенство:*

$$\operatorname{rk}_r A = \operatorname{rk}_c A$$

Доказательство. Пусть $r := rk_c A$, тогда столбцы матрицы A выражаются через некоторые r столбцов. Составим из этих r столбцов матрицу B, тогда каждый столбец матрицы A имеет вид $B\gamma$ для некоторого $\gamma \in F^r$. Следовательно, A можно представить в виде $B(\gamma_1|\ldots|\gamma_k)$. По уже доказанному, $\operatorname{rk}_r A \leqslant \operatorname{rk}_r(\gamma_1|\ldots|\gamma_k) \leqslant r$, поскольку в матрице $(\gamma_1|\ldots|\gamma_k)$ ровно r строк. Аналогично показывается, что $\operatorname{rk}_c A \leqslant \operatorname{rk}_r A$. Таким образом, $\operatorname{rk}_r A = \operatorname{rk}_c A$. □

Определение 6.23. *Рангом матрицы* $A \in M_{n\times k}(F)$ называется ее строчный или столбцовый ранг. Обозначение — $\operatorname{rk} A$.

Утверждение 6.16. *Пусть* $A \in M_{n\times k}(F)$, $B \in M_{k\times m}(F)$, *причем столбцы матрицы* A *линейно независимы. Тогда* $\operatorname{rk} AB = \operatorname{rk} B$.

Доказательство. Пусть $r := \operatorname{rk} B$, $\gamma_1, \ldots, \gamma_r$ — столбцы матрицы B, образующие линейно независимую систему. Тогда $A\gamma_1, \ldots, A\gamma_r$ — столбцы с теми же номерами в матрице AB. Докажем, что они тоже образуют линейно независимую систему. Действительно, для любого нетривиального набора коэффициентов $\alpha_1, \ldots, \alpha_n$ в силу линейной независимости столбцов A и системы $(\gamma_1, \ldots, \gamma_r)$ имеем:

$$\sum_{i=1}^{r} \alpha_i A\gamma_i = A\left(\sum_{i=1}^{r} \alpha_i \gamma_i\right) \neq A0 = 0$$

Таким образом, система $(A\gamma_1, \ldots, A\gamma_r)$ линейно независима, откуда $\operatorname{rk} AB \geqslant \operatorname{rk} B$, тогда, по уже доказанному, $\operatorname{rk} AB = \operatorname{rk} B$. $\square$

Утверждение 6.17. *Пусть* V *— линейное пространство над полем* F, e *— базис в* V, $\overline{v_1}, \ldots, \overline{v_m} \in V$, *и* $(\overline{v_1}, \ldots, \overline{v_m}) = eA$, $A \in M_{n\times m}(F)$. *Тогда* $\operatorname{rk}(\overline{v_1}, \ldots, \overline{v_m}) = \operatorname{rk} A$.

Доказательство. Изоморфизм $\varphi : V \to F^n$, сопоставляющий векторам из V их координатные столбцы в базисе e, переводит линейно независимые системы в линейно независимые, поэтому $\operatorname{rk}(\overline{v_1}, \ldots, \overline{v_m}) \leqslant \operatorname{rk} A$. Аналогично, $\operatorname{rk}(\overline{v_1}, \ldots, \overline{v_m}) \geqslant \operatorname{rk} A$. $\square$

Теорема 6.8 (о базисном миноре)**.** *Пусть* $A \in M_{n\times k}(F)$, $\operatorname{rk} A = r$. *Тогда в* A *найдется подматрица размера* $r \times r$ *ранга* r. *Более того, если выбрать линейно независимую систему из* r *строк матрицы* A *и линейно независимую систему из* r *столбцов матрицы* A, *то искомая матрица будет расположена на их пересечении.*

Доказательство. Докажем сразу вторую часть утверждения. Без ограничения общности можно считать, что подматрица M на пересечении r линейно независимых строк и столбцов расположена в левом верхнем углу матрицы A. Пусть $R \in M_{r\times k}$ — подматрица из первых r строк A, $C \in M_{n\times r}$ — подматрица из первых r столбцов A.

Столбцы матрицы A выражаются через столбцы матрицы C, поэтому $A = CB$ для некоторой $B \in M_{r\times n}(F)$. Но тогда столбцы матрицы R выражаются через столбцы матрицы M с теми же коэффициентами, то есть $R = MB$. Кроме того, строки матрицы A выражаются через строки матрицы R, то есть $A = SR$ для некоторой $S \in M_{n\times r}(F)$. Таким образом, $A = SMB$, тогда $r = \operatorname{rk} A \leqslant \operatorname{rk} M \leqslant r$, откуда $\operatorname{rk} M = r$. $\square$

Утверждение 6.18. *Пусть* $A \in M_{n\times k}(F)$, *и* $D \in M_n(F)$ *— обратимая матрица. Тогда* $\operatorname{rk}(DA) = \operatorname{rk}(A)$.

Доказательство. Выполнены неравенства $rkA \geqslant \operatorname{rk}(DA) \geqslant \operatorname{rk}(D^{-1}DA) = \operatorname{rk} A$. $\square$

Утверждение 6.19. *Пусть* $A \in M_{n\times k}(F)$, *и* $D \in M_n(F)$ *— обратимая матрица. Тогда столбцы матрицы* A *с некоторыми номерами линейно зависимы* $\Leftrightarrow$ *столбцы матрицы* DA *с теми же номерами линейно зависимы.*

Доказательство. Пусть $\gamma \in F^k$, тогда:

$$A\gamma = 0 \Rightarrow DA\gamma = 0$$
$$DA\gamma = 0 \Rightarrow D^{-1}DA\gamma = 0 \Rightarrow A\gamma = 0$$

Значит, столбцы с одинаковыми номерами в A и DA образуют или не образуют линейно зависимую систему одновременно. $\square$

Следствие. При элементарных преобразованиях строк матрицы $A \in M_{n\times k}(F)$ не меняется ее ранг и линейная зависимость столбцов.

Утверждение 6.20. *Ранг ступенчатой матрицы $A \in M_{n\times k}(F)$ равен числу ступеней.*

Доказательство. Если в A всего r ступеней, то в ней всего r ненулевых строк, значит, $\operatorname{rk} A \leqslant r$. С другой стороны, эти строки образуют линейно независимую систему. Предположим, что это не так, тогда существует их нетривиальная линейная комбинация с коэффициентами $\alpha_1, \ldots, \alpha_r \in F$, равная нулю:

$$\sum_{i=1}^{r} \alpha_i a_{i*} = 0$$

Пусть j — наименьший индекс такой, что $\alpha_j \neq 0$, k — индекс главного элемента в строке a_{j*}, тогда на k-й позиции в данной линейной комбинации стоит элемент $\alpha_j a_{jk} \neq 0$. Получено противоречие. Значит, система из этих r строк линейно независима, и $\operatorname{rk} A = r$. □

Следствие. Для нахождения ранга матрицы $A \in M_{n\times k}(F)$ следует привести ее к ступенчатому виду, и число ступеней в полученной матрице будет равно искомому рангу.

Теорема 6.9. *Пусть $A \in M_{n\times k}(F)$, и U — пространство решений однородной системы $Ax = 0$. Тогда* $\dim U = n - \operatorname{rk} A$.

Доказательство. Приведем матрицу A к упрощенному виду A', тогда $\operatorname{rk} A' = \operatorname{rk} A = r$. В полученной матрице r ненулевых строк, поэтому в системе r главных переменных и $n - r$ свободных переменных. Тогда фундаментальная матрица Φ данной системы состоит из $n - r$ столбцов, откуда $\dim U = n - r = n - \operatorname{rk} A$. □

Теорема 6.10 (Кронекера-Капелли)**.** *Система $Ax = b$ совместна $\Leftrightarrow$ $\operatorname{rk} A = \operatorname{rk}(A|b)$.*

Доказательство. Приведем расширенную матрицу системы $(A|b)$ к упрощенному виду $(A'|b')$. Поскольку перестановки столбцов не происходит, то матрица A' — это упрощенный вид матрицы A. Тогда система совместна $\Leftrightarrow$ в $(A'|b')$ нет ступеньки, начинающейся в столбце b', $\Leftrightarrow$ у A' и $(A'|b')$ одно и то же число ступенек $\Leftrightarrow$ $\operatorname{rk} A = \operatorname{rk}(A|b)$. □

Определение 6.24. Матрица $A \in M_n(F)$ называется *невырожденной*, если $\operatorname{rk} A = n$.

Теорема 6.11. *Пусть $A \in M_n(F)$. Тогда следующие условия эквивалентны:*

1. *Матрица A невырожденна*
2. *Матрица A элементарными преобразованиями строк приводится к E*
3. *Матрица A является произведением элементарных матриц*
4. *Матрица A обратима*
5. *Матрица A обратима слева, то есть существует матрица $B \in M_n(F)$ такая, что $BA = E$, или справа*

Доказательство.

- ▷ $(1 \Rightarrow 2)$ Приведем A к упрощенному виду A'. Так как $\operatorname{rk} A' = \operatorname{rk} A = n$, то $A' = E$.

- $(2 \Rightarrow 3)$ Пусть последовательности преобразований, приводящих A к E, соответствует последовательность элементарных матриц $M_1, \ldots, M_k \in M_n(F)$, тогда:

$$M_k \ldots M_1 A = E \Rightarrow A = M_1^{-1} \ldots M_k^{-1}$$

- $(3 \Rightarrow 4)$ Если $A = M_1^{-1} \ldots M_k^{-1}$, то A обратима, причем $A^{-1} = M_k \ldots M_1$.

- $(4 \Rightarrow 5)$ Если A обратима, то, в частности, A обратима слева или справа.

- $(5 \Rightarrow 1)$ Пусть без ограничения общности A обратима слева, тогда существует матрица $B \in M_n(F)$ такая, что $BA = E$. Тогда $n = \operatorname{rk} E = \operatorname{rk} BA \leqslant \operatorname{rk} A$, откуда $\operatorname{rk} A = n$. □

Следствие. Пусть A — невырожденная матрица, и матрица $(A|E)$ приводится к упрощенному виду $(E|C)$. Тогда матрица C является обратной к A.

Доказательство. Пусть последовательности преобразований, приводящих $(A|E)$ к $(E|C)$, соответствует последовательность элементарных матриц $M_1, \ldots, M_k \in M_n(F)$, то есть $M_k \ldots M_1(A|E) = (E|C)$. Тогда:

$$M_k \ldots M_1(A|E) = (M_k \ldots M_1 A | M_k \ldots M_1 E) = (M_k \ldots M_1 A | M_k \ldots M_1)$$

Следовательно, $M_k \ldots M_1 = C$ и $CA = E$. □

Замечание. В общем случае, для матрицы $A \in M_{n \times k}(F)$ при $n \neq k$ не существует матрицы $B \in M_{k \times n}(F)$ такой, что $AB = BA = E$. Действительно, $\operatorname{rk} AB, \operatorname{rk} BA \leqslant \min\{n, k\}$, поэтому ни один из рангов не может равняться $\operatorname{rk} E_{\max\{n,k\}} = \max\{n, k\}$.

6.5 Сумма и пересечение подпространств

Утверждение 6.21. *Пусть V — линейное пространство, $U_1, U_2 \leqslant V$. Тогда $U_1 \cap U_2 \leqslant V$.*

Доказательство.

- $U_1 \cap U_2 \neq \varnothing$, поскольку $\overline{0} \in U_1 \cap U_2$
- Если $\overline{u}, \overline{v} \in U_1 \cap U_2$, то $\overline{u} \in U_1, U_2$ и $\overline{v} \in U_1, U_2$, откуда $\overline{u} + \overline{v} \in U_1, U_2$
- Если $\overline{u} \in U_1 \cap U_2$, то $\overline{u} \in U_1, U_2$, откуда $\forall \alpha \in F : \alpha\overline{u} \in U_1, U_2$ □

Определение 6.25. Пусть V — линейное пространство, $U_1, U_2 \leqslant V$. *Суммой* подпространств U_1, U_2 называется следующее множество:

$$U_1 + U_2 := \{\overline{u_1} + \overline{u_2} : \overline{u_1} \in U_1, \overline{u_2} \in U_2\}$$

Аналогично определяется сумма k подпространств $U_1, \ldots, U_k \leqslant V$.

Утверждение 6.22. *Пусть V — линейное пространство над полем F, $U_1, \ldots, U_k \leqslant V$. Тогда $U_1 + \cdots + U_k \leqslant V$.*

Доказательство. Сначала докажем справедливость утверждения для $U_1 + U_2$:

- $U_1 + U_2 \neq \varnothing$, поскольку $\overline{0} \in U_1 + U_2$

▷ Если $\overline{u_1}+\overline{u_2}, \overline{v_1}+\overline{v_2} \in U_1+U_2$, то $\overline{u_1}+\overline{u_2}+\overline{v_1}+\overline{v_2} = (\overline{u_1}+\overline{v_1})+(\overline{u_2}+\overline{v_2}) \in U_1+U_2$

▷ Если $\overline{u_1}+\overline{u_2} \in U_1+U_2$, то $\forall \alpha \in F : \alpha(\overline{u_1}+\overline{u_2}) = \alpha\overline{u_1}+\alpha\overline{u_2} \in U_1+U_2$

Чтобы обобщить утверждение на $U_1, \ldots, U_k \leqslant V$, заметим, что сложение подпространств ассоциативно в силу ассоциативности сложения в V. Тогда, по индукции, сумма любого числа подпространств образует подпространство в V. □

Замечание. Определить сумму $U_1+\cdots+U_k$ можно и другим эквивалентным способом:

$$U_1+\cdots+U_k = \langle U_1 \cup \cdots \cup U_k \rangle$$

Утверждение 6.23. *Пусть V — линейное пространство над полем F, $U_1, \ldots, U_k \leqslant V$, причем $U_1 = \langle A_1 \rangle, \ldots, U_k = \langle A_k \rangle$. Тогда:*

$$U_1+\ldots+U_k = \langle A_1 \cup \cdots \cup A_k \rangle$$

Доказательство.

$\subset$ Если $\overline{u_1}+\cdots+\overline{u_k} \in U_1+\ldots+U_k$, то для каждого $i \in \{1, \ldots, k\}$ вектор $\overline{u_i}$ выражается через A_i, тогда $\overline{u_1}+\cdots+\overline{u_k} \in \langle A_1 \cup \cdots \cup A_k \rangle$

$\supset$ Для каждого $i \in \{1, \ldots, k\}$ выполнено $A_i \subset U_i \subset U_1+\cdots+U_k$, поэтому имеет место включение $A_1 \cup \cdots \cup A_k \subset U_1+\cdots+U_k$, но сумма подпространств — это линейное пространство, тогда $\langle A_1 \cup \cdots \cup A_k \rangle \subset U_1+\cdots+U_k$ □

Следствие. Пусть V — линейное пространство над полем F, $U_1, \ldots, U_k \leqslant V$. Тогда:

$$\dim(U_1+\cdots+U_k) \leqslant \dim U_1+\cdots+\dim U_k$$

Доказательство. Возьмем в качестве $A_1, \ldots, A_k$ из утверждения выше базисы в соответствующих подпространствах. Тогда подпространство $U_1+\cdots+U_k$ порождено системой из не более, чем $\dim U_1+\cdots+\dim U_k$ векторов. □

Замечание. Если для подпространств $U_1, U_2, U_3 \leqslant V$ в пространстве V выполнено равенство $U_1+U_2 = U_1+U_3$, то необязательно $U_2 = U_3$. Например, любые два пересекающиеся прямые в плоскости V_2 в сумме дают всю плоскость V_2.

Определение 6.26. Пусть V — линейное пространство, $U_1, \ldots, U_k \leqslant V$. Сумма подпространств $U := U_1+\cdots+U_k$ называется *прямой*, если для любого вектора $\overline{u} \in U$ существует единственный набор векторов $\overline{u_1} \in U_1, \ldots, \overline{u_k} \in U_k$ такой, что $\overline{u} = \overline{u_1}+\cdots+\overline{u_k}$. Обозначение — $U = U_1 \oplus \cdots \oplus U_k$.

Утверждение 6.24. *Пусть V — линейное пространство, $U_1, \ldots, U_k \leqslant V$. Тогда сумма $U_1+\cdots+U_k$ — прямая $\Leftrightarrow$ существует единственный набор векторов $\overline{u_1} \in U_1, \ldots, \overline{u_k} \in U_k$ такой, что $\overline{u_1}+\cdots+\overline{u_k} = \overline{0}$.*

Доказательство.

$\Rightarrow$ По определению прямой суммы, вектор $\overline{0}$ имеет единственное представление в виде суммы векторов из $U_1, \ldots, U_k$, и оно имеет вид $\overline{0} = \overline{0}+\cdots+\overline{0}$.

- $\Leftarrow$ Пусть для вектора $\overline{u} \in U$ и наборов $\overline{u_1} \in U_1, \ldots, \overline{u_k} \in U_k$ и $\overline{w_1} \in U_1, \ldots, \overline{w_k} \in U_k$ выполнены следующие равенства:

$$\overline{u} = \overline{u_1} + \cdots + \overline{u_k} = \overline{w_1} + \cdots + \overline{w_k}$$

Вычитая третью часть равенства из выше из второй, получим:

$$\overline{0} = (\overline{u_1} - \overline{w_1}) + \cdots + (\overline{u_k} - \overline{w_k})$$

Но вектор $\overline{0}$ имеет единственное представление в виде суммы векторов из $U_1, \ldots, U_k$, поэтому $\overline{u_1} = \overline{w_1}, \ldots, \overline{u_k} = \overline{w_k}$. □

Теорема 6.12. *Пусть V — линейное пространство над F, $U_1, \ldots, U_k \leqslant V$. Тогда сумма $U_1 + \cdots + U_k$ — прямая $\Leftrightarrow$ для любого $i \in \{1, \ldots, k\}$ выполнено следующее равенство:*

$$U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k) = \{\overline{0}\}$$

Доказательство.

- $\Rightarrow$ Предположим, что существует $i \in \{1, \ldots, k\}$ и вектор $\overline{u_i} \in U_i$, $\overline{u_i} \neq \overline{0}$, такой, что $\overline{u_i} = \overline{u_1} + \cdots + \overline{u_{i-1}} + \overline{u_{i+1}} + \cdots + \overline{u_k} \in U_1 + \cdots + U_{i-1} + U_{i+1} + U_k$. Но тогда выполнено следующее:

$$\overline{0} = \overline{u_1} + \cdots + \overline{u_{i-1}} - \overline{u_i} + \overline{u_{i+1}} + \cdots + \overline{u_k}$$

Получено нетривиальное разложение нуля — противоречие.

- $\Leftarrow$ Предположим, что сумма не прямая, то есть существует нетривиальное разложение нуля $\overline{u_1} + \cdots + \overline{u_k} = \overline{0}$. Тогда существует $i \in \{1, \ldots, k\}$ такое, что $\overline{u_i} \neq 0$, причем выполнено следующее:

$$\overline{u_i} = -(\overline{u_1} + \cdots + \overline{u_{i-1}} + \overline{u_{i+1}} + \cdots + \overline{u_k}) \in U_i \cap (U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k)$$

Получено противоречие. □

Замечание. Можно по индукции показать, что вместо набора условий из теоремы выше достаточно проверять, что для любого $i \in \{1, \ldots, k-1\}$ выполнено следующее равенство:

$$U_{i+1} \cap (U_1 + \cdots + U_i) = \{\overline{0}\}$$

Замечание. Если для подпространств $U_1, U_2, U_3 \leqslant V$ в пространстве V выполнено равенство $U_1 \oplus U_2 = U_1 \oplus U_3$, то тоже необязательно $U_2 = U_3$. Контрпример аналогичен случаю обычной суммы.

Теорема 6.13. *Пусть V — линейное пространство, $U_1, \ldots, U_k \leqslant V$. Тогда следующие условия эквивалентны:*

1. *Сумма $U := U_1 + \ldots U_k$ — прямая*
2. $\dim (U_1 + \cdots + U_k) = \dim U_1 + \cdots + \dim U_k$
3. *Для любого набора базисов $e_1, \ldots, e_k$ в $U_1, \ldots, U_k$ система $(e_1, \ldots, e_k)$ образует базис в пространстве U*

4. *Существует такой набор базисов $e_1, \ldots, e_k$ в $U_1, \ldots, U_k$, что система $(e_1, \ldots, e_k)$ образует базис в пространстве U*

Доказательство. Пусть $e_1, \ldots, e_k$ — базисы в $U_1, \ldots, U_k$, тогда $U = \langle e_1, \ldots, e_k \rangle$. Докажем, что сумма прямая $\Leftrightarrow$ система $(e_1, \ldots, e_k)$ линейно независима, то есть образует базис в U.

$\Leftarrow$ Предположим, что сумма U не прямая, тогда существует нетривиальное разложение нуля $\overline{u_1} + \cdots + \overline{u_k} = \overline{0}$. Выразив каждый из векторов в соответствующем базисе, получим нетривиальную линейную комбинацию, равную нулю. Значит, система линейно зависима — противоречие.

$\Rightarrow$ Предположим, что система $(e_1, \ldots, e_k)$ линейно зависима. Сгруппируем нетривиальную линейную комбинацию, равную нулю, по базисам в подпространствах, и получим нетривиальное разложение нуля $\overline{u_1} + \cdots + \overline{u_k} = \overline{0}$. Значит, сумма не прямая — противоречие.

Теперь докажем, что $\dim(U_1 + \cdots + U_k) = \dim U_1 + \cdots + \dim U_k \Leftrightarrow$ система $(e_1, \ldots, e_k)$ линейно независима, то есть образует базис в U.

$\Leftarrow$ Если $(e_1, \ldots, e_k)$ — базис в U, то $\dim U = \dim U_1 + \cdots + \dim U_k$.

$\Rightarrow$ Предположим, что система $(\overline{e_1}, \ldots, \overline{e_k})$ линейно зависима, тогда, так как она выражает все пространство U, $\dim U < \dim U_1 + \cdots + \dim U_k$ — снова противоречие. $\square$

Определение 6.27. Пусть V — линейное пространство над полем F, $U \leqslant V$. Подпространство $W \leqslant V$ называется *прямым дополнением* подпространства U в пространстве V, если сумма $U + W$ — прямая и $U \oplus W = V$.

Замечание. По уже доказанному, $\dim U + \dim W = \dim V$.

Утверждение 6.25. *Пусть V — линейное пространство, $U \leqslant V$. Тогда существует прямое дополнение подпространства U в пространстве V.*

Доказательство. Выберем базис $(\overline{e_1}, \ldots, \overline{e_k})$ — базис в U. Линейно независимую систему e можно дополнить до базиса в V. Обозначим через $\overline{e_{k+1}}, \ldots, \overline{e_n} \in V$ векторы, дополняющие e до базиса, и рассмотрим $W := \langle \overline{e_{k+1}}, \ldots, \overline{e_n} \rangle$. Тогда $U + W = V$, и объединение базисов U и W является базисом в V, поэтому сумма $U \oplus W$ — прямая. $\square$

Теорема 6.14. *Пусть $U_1, U_2 \leqslant V$. Тогда выполнено следующее равенство:*

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

Доказательство. Пусть $U := U_1 \cap U_2 \leqslant U_1, U_2$. Выберем W_1, W_2 — прямые дополнения подпространства U в U_1, U_2 соответственно, тогда выполнены следующие равенства:

$$\dim U + \dim W_1 = \dim U_1$$
$$\dim U + \dim W_2 = \dim U_2$$

Докажем, что $U_1 + U_2 = U \oplus W_1 \oplus W_2$. Равенство $U_1 + U_2 = U + W_1 + W_2$ очевидно, поэтому достаточно проверить, что эта сумма — прямая. Пусть $\overline{0} = \overline{u} + \overline{w_1} + \overline{w_2}$ для некоторых $\overline{w_1} \in W_1, \overline{w_2} \in W_2, \overline{u} \in U$, тогда:

$$-\overline{w_1} = \overline{u} + \overline{w_2} \Rightarrow \overline{w_1} \in W_1 \cap U_2 = W_1 \cap U \Rightarrow \overline{w_1} = \overline{0}$$
$$-\overline{w_2} = \overline{u} + \overline{w_1} \Rightarrow \overline{w_2} \in W_2 \cap U_1 = W_2 \cap U \Rightarrow \overline{w_2} = \overline{0}$$

Значит, и $\overline{u} = \overline{0}$, поэтому сумма $U + W_1 + W_2$ — прямая. Тогда:

$$\dim(U_1 + U_2) = \dim U + \dim W_1 + \dim W_2 = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) \qquad \square$$

Замечание. В общем случае, по размерностям попарных пересечений подпространств $U_1, \ldots, U_k \leqslant V$ уже нельзя восстановить $\dim(U_1 + \cdots + U_k)$.

Определение 6.28. Пусть V — линейное пространство, $U, W \leqslant V$ и $V = U \oplus W$. Для любого вектора $\overline{v} \in V$ существует единственное разложение $\overline{v} = \overline{u} + \overline{w}$, $\overline{u} \in U, \overline{w} \in W$.

- Вектор $\overline{u}$ называется *проекцией* $\overline{v}$ *на* U *вдоль* W
- Вектор $\overline{w}$ называется *проекцией* $\overline{v}$ *на* W *вдоль* U

Замечание. Пусть V_1, V_2 — линейные пространства. Их *внешней прямой суммой* называется множество $V = V_1 \oplus V_2 := \{(\overline{v_1}, \overline{v_2 v_1} \in V_1, \overline{v_2} \in V_2)\}$. Если определить сложение и умножение на скаляр покоординатно, то V становится линейным пространством, причем выполнены следующие свойства:

- $U_1 := \{(\overline{v_1}, \overline{0}) : \overline{v_1} \in V_1\} \cong V_1$
- $U_2 := \{(\overline{0}, \overline{v_2}) : \overline{v_2} \in V_2\} \cong V_2$
- $V = U_1 \oplus U_2$

7 Линейные функционалы и отображения

7.1 Сопряженное пространство

Определение 7.1. Пусть V — линейное пространство над полем F. *Линейной функцией* на V, или *линейным функционалом* на V, называется отображение $f : V \to F$, обладающее свойством линейности:

- $\forall \overline{v_1}, \overline{v_2} \in V : f(\overline{v_1} + \overline{v_2}) = f(\overline{v_1}) + f(\overline{v_2})$
- $\forall \alpha \in F : \forall \overline{v} \in V : f(\alpha \overline{v}) = \alpha f(\overline{v})$

Определение 7.2. Пусть V — линейное пространство над полем F. Множество линейных функционалов на V называется *пространством, сопряженным к* V. Обозначение — V^*. На определены операции сложения и умножения на скаляр:

- $\forall \overline{f_1}, \overline{f_2} \in V^* : \forall \overline{v} \in V : (f_1 + f_2)(\overline{v}) := f_1(\overline{v}) + f_2(\overline{v})$
- $\forall \alpha \in F : \forall \overline{f} \in V^* : \forall \overline{v} \in V : (\alpha f)(\overline{v}) = \alpha f(\overline{v})$

Утверждение 7.1. *Пусть V — линейное пространство над полем F. Тогда сопряженное пространство V^* тоже является линейным пространством над F.*

Доказательство. Покажем сначала, что $(V^*, +)$ — абелева группа:

- Ассоциативность и коммутативность следуют из соответствующих свойств в $(F, +)$
- Нейтральный элемент — нулевой функционал 0 такой, что $\forall \overline{v} \in V : 0(\overline{v}) = \overline{0}$.

▷ Обратный к $f \in V^*$ элемент — это $(-1)f$.

Свойства линейного пространства проверяются непосредственно. □

Определение 7.3. Пусть V — линейное пространство, $e = (e_1, \dots, e_n)$ — базис в V. Тогда для каждого $i \in \{1, \dots, n\}$ определим $f_i \in V^*$ следующим образом: для любого $\overline{v} \in V$, $\overline{v} \leftrightarrow_e \alpha$, положим $f_i(\overline{v}) := \alpha_i$.

Утверждение 7.2. *Пусть V — линейное пространство, $e = (e_1, \dots, e_n)$ — базис в V. Тогда $(f_1, \dots, f_n)$ — базис в V^*.*

Доказательство. Сначала докажем, что система $(f_1, \dots, f_n)$ линейно независима. Действительно, если существует нетривиальная линейная комбинация $\lambda_1 f_1 + \dots + \lambda_n f_n$, равная нулю, то, в частности, она принимает нулевое значение на базисных векторах e. Но для любых $i, j \in \{1, \dots, n\}$ выполнено следующее:

$$f_i(\overline{e_j}) = \delta_{ij} = \begin{cases} 1, & \text{если } i = j \\ 0, & \text{если } i \neq j \end{cases}$$

Значит, $\lambda_1 = \dots = \lambda_n = 0$, поэтому система линейно независима. Теперь покажем, что $\langle f_1, \dots, f_n \rangle = V^*$. Выберем произвольный функционал $f \in V^*$ и вектор $\overline{v} \in V$, $\overline{v} \leftrightarrow_e \alpha$, тогда выполнены следующие равенства:

$$f(\overline{v}) = f\left(\sum_{i=1}^{n} \alpha_i \overline{e_i}\right) = \sum_{i=1}^{n} \alpha_i f(\overline{e_i}) = \sum_{i=1}^{n} f(\overline{e_i}) f_i(\overline{v}) = \left(\sum_{i=1}^{n} f(\overline{e_i}) f_i\right)(\overline{v})$$

Для каждого функционала f значения $f(\overline{e_i})$ фиксированы, поэтому каждый функционал f представим в виде линейной комбинации функционалов $f_1, \dots, f_n$. Таким образом, $(f_1, \dots, f_n)$ — базис в V^*. □

Замечание. Из доказательства выше, в частности, следует, что функционал $f \in V^*$ в базисе $(f_1, \dots, f_n)$ имеет координаты $(f(\overline{e_1}), \dots, f(\overline{e_n}))$.

Следствие. Если V — линейное пространство, то $\dim V^* = \dim V$.

Определение 7.4. Пусть V — линейное пространство, $e = (\overline{e_1}, \dots, \overline{e_n})$ — базис в V. Базис $\mathcal{F} = (f_1, \dots, f_n)^T$ в V^* называется *взаимным*, или (*сопряженным*, к базису e в V.

Замечание. Если в пространстве V базисные векторы записываются в строку, а координаты — в столбец, то в пространстве V^* удобнее делать это наоборот.

Утверждение 7.3. *Пусть V — линейное пространство над полем F, e, e' — базисы в V, $\mathcal{F}, \mathcal{F}'$ — взаимные к ним базисы в V^*, и $e' = eS$, $S \in M_n(F)$. Тогда $\mathcal{F} = S\mathcal{F}'$.*

Доказательство. Рассмотрим произвольный вектор $\overline{v} \in V$ с координатными столбцами α,α' в базисах e, e' соответственно, тогда $\overline{v} = e\alpha = e'\alpha'$, $\alpha = S\alpha'$. Тогда:

$$\mathcal{F}(\overline{v}) = (f_1(\overline{v}), \dots, f_n(\overline{v}))^T = (\alpha_1, \dots, \alpha_n)^T = \alpha$$
$$(S\mathcal{F}')(\overline{v}) = S(f_1'(\overline{v}), \dots, f_n'(\overline{v}))^T = S(\alpha_1', \dots, \alpha_n')^T = S\alpha' = \alpha$$

Значения функционалов из $\mathcal{F}$ и $S\mathcal{F}'$ на любом векторе совпадают, поэтому выполнено равенство $\mathcal{F} = S\mathcal{F}'$. □

Определение 7.5. Пусть V — линейное пространство над полем F. Пространством, *дважды сопряженным* к V, называется пространство $V^{**} := (V^*)^*$.

Определение 7.6. Пусть V — линейное пространство над полем F, $\overline{v} \in V$. Определим $v^{**} \in V^{**}$ следующим образом: для любого $f \in V^*$ положим $v^{**}(f) := f(\overline{v})$.

Замечание. Определение выше корректно, поскольку v^{**} действительно является линейным функционалом:

▷ $\forall f_1, f_2 \in V^* : v^{**}(f_1 + f_2) = (f_1 + f_2)(\overline{v}) = f_1(\overline{v}) + f_2(\overline{v}) = v^{**}(f_1) + v^{**}(f_2)$

▷ $\forall \alpha \in F : \forall f \in V^* : v^{**}(\alpha f) = (\alpha f)(\overline{v}) = \alpha f(\overline{v}) = \alpha v^{**}(f)$

Теорема 7.1. *Пусть V — линейное пространство над полем F. Тогда отображение $\varphi : V \to V^{**}$ такое, что $\varphi(\overline{v}) := v^{**}$ для любого $\overline{v} \in V$, является изоморфизмом линейных пространств V и V^{**}.*

Доказательство. Линейность отображения проверяется непосредственно. Докажем, что φ — биекция. Зафиксируем базис $e = (\overline{e_1}, \ldots, \overline{e_n})$ в V и проверим, что система $(e_1^{**}, \ldots, e_n^{**})$ линейно независима. Если ее линейная комбинация с коэффициентами $\alpha_1, \ldots, \alpha_n \in F$ равна нулю, то для любого $f \in V^*$ выполнены равенства:

$$0 = \left(\sum_{i=1}^{n} \alpha_i e_i^{**}\right)(f) = f\left(\sum_{i=1}^{n} \alpha_i \overline{e_i}\right) = \sum_{i=1}^{n} \alpha_i f(\overline{e_i})$$

Равенство должно выполняться, в частности, для функционалов из базиса $\mathcal{F}$, взаимного к e, поэтому $\alpha_1 = \cdots = \alpha_n = 0$, и система линейно независима. Но $\dim V = \dim V^* = \dim (V^*)^* = n$, поэтому $(e_1^{**}, \ldots, e_n^{**})$ — базис в V^{**}. Наконец, φ отображает вектор $\overline{v} \in V$, $\overline{v} \leftrightarrow_e \alpha$ в вектор $v^{**} \in V^{**}$, $v^{**} \leftrightarrow_{e^{**}} \alpha$, поэтому φ — биекция. □

Определение 7.7. Пусть V — линейное пространство. Изоморфизм V и V^{**} такой, что $\overline{v} \mapsto v^{**}$, называется *каноническим изоморфизмом* пространств V и V^{**}.

Замечание. Изоморфизм φ называется каноническим потому, что он построен инвариантно, то есть не опирается на выбор базиса. Благодаря каноническому изоморфизму, можно отождествить вектор $\overline{v} \in V$ с вектором $v^{**} \in V^{**}$, тогда для любого $f \in V^*$ выполнены следующие равенства:

$$f(\overline{v}) = v^{**}(f) = \overline{v}(f)$$

Утверждение 7.4. *Пусть V — линейное пространство. Тогда любой базис $\mathcal{F}$ в V^* взаимен некоторому базису e в V.*

Доказательство. Пусть $\mathcal{F} = (f_1, \ldots, f_n)$. У него есть взаимный базис $e^{**} = (e_1^{**}, \ldots, e_n^{**})$ в V^{**}, тогда базис $\mathcal{F}$ является взаимным к соответствующему базису $e = (\overline{e_1}, \ldots, \overline{e_n})$ в V, в который базис e^{**} переходит при каноническом изоморфизме. □

7.2 Аннуляторы

Определение 7.8. Пусть $f : A \to B$ — отображение, $A' \subset A$. *Образом* подмножества A' при отображении f называется $f(A') := \{f(a) : a \in A'\} \subset B$.

Определение 7.9. Пусть V — линейное пространство над полем F.

▷ *Аннулятором* подпространства $W \leqslant V$ называется следующее множество:

$$W^0 := \{f \in V^* : f(W) = \{0\}\}$$

▷ *Аннулятором* подпространства $U \leqslant V^*$ называется следующее множество:

$$U^0 := \{v^{**} \in V^{**} : v^{**}(U) = \{0\}\} = \{\overline{v} \in V : \forall f \in V^* : f(\overline{v}) = 0\}$$

Замечание. Аннуляторы $W^0 \leqslant V^*$ и $U^0 \leqslant V$ являются подпространствами в соответствующих пространствах как пространства решений однородных систем линейных уравнений. Однако их замкнутость относительно сложения и умножения на скаляры можно проверить и непосредственно.

Теорема 7.2. *Пусть V — линейное пространство, $\dim V = n$, $W \leqslant V$. Тогда выполнено следующее равенство:*

$$\dim W + \dim W^0 = n$$

Доказательство. Пусть $\dim W = k$, и $(\overline{e_1}, \ldots, \overline{e_k})$ — базис в W. Дополним его до базиса $e = (\overline{e_1}, \ldots, \overline{e_n})$ в V и выберем взаимный к нему базис $\mathcal{F} = (f_1, \ldots, f_n)$ в V^*. Пусть $f \in V^*$, $f \leftrightarrow_{\mathcal{F}} \alpha$. Тогда:

$$f \in W^0 \Leftrightarrow f(\overline{e_1}) = \cdots = f(\overline{e_k}) = 0 \Leftrightarrow \alpha_1 = \cdots = \alpha_k = 0 \Leftrightarrow f \in \langle f_{k+1}, \ldots, f_n \rangle$$

Таким образом, $W^0 = \langle f_{k+1}, \ldots, f_n \rangle$, причем система $(f_{k+1}, \ldots, f_n)$ образует базис в W^0, тогда $\dim W^0 = n - k$. □

Теорема 7.3. *Пусть V — линейное пространство, $W, W_1, W_2 \leqslant V$. Тогда выполнены следующие свойства:*

1. $(W^0)^0 = W$
2. $W_1 \leqslant W_2 \Leftrightarrow W_2^0 \leqslant W_1^0$
3. $(W_1 + W_2)^0 = W_1^0 \cap W_2^0$
4. $(W_1 \cap W_2)^0 = W_1^0 + W_2^0$

Доказательство.

1. С одной стороны, если $\overline{v} \in W$, то для любого $f \in W^0$ выполнено $f(\overline{v}) = 0 \Leftrightarrow \overline{v}(f) = 0$, поэтому $\overline{v} \in (W^0)^0$. Значит, $W \subset (W^0)^0$. С другой стороны, выполнено следующее:

$$\dim W + \dim W^0 = \dim V = \dim V^* = \dim W^0 + \dim (W^0)^0 \Rightarrow \dim W = \dim (W^0)^0$$

Значит, имеет место равенство $W = (W^0)^0$.

2. $\Rightarrow$ Пусть $W_1 \leqslant W_2$, тогда для любого $f \in W_2^0$ выполнено $f(W_1) \subset f(W_2) = \{0\}$, откуда $f \in W_1^0$, то есть $W_2^0 \leqslant W_1^0$

   $\Leftarrow$ Пусть $W_2^0 \leqslant W_1^0$, тогда $W_1 = (W_1^0)^0 \leqslant (W_2^0)^0 = W_2$.

3. $\leqslant$ Поскольку $W_1 \leqslant W_1 + W_2$, то, в силу пункта (2), выполнено $(W_1 + W_2)^0 \leqslant W_1^0$. Аналогично, $(W_1 + W_2)^0 \leqslant W_2^0$, поэтому $(W_1 + W_2)^0 \leqslant W_1^0 \cap W_2^0$

   $\geqslant$ Если $f \in W_1^0 \cap W_2^0$, то для любых $\overline{w_1} \in W_1$, $\overline{w_2} \in W_2$ выполнены равенства $f(\overline{w_1}) = f(\overline{w_2}) = \overline{0}$, откуда $f(\overline{w_1} + \overline{w_2}) = 0$, тогда $f \in (W_1 + W_2)^0$. Следовательно, $W_1^0 \cap W_2^0 \leqslant (W_1 + W_2)^0$.

4. Выполнены равенства $W_1^0 + W_2^0 = ((W_1^0 + W_2^0)^0)^0 = ((W_1^0)^0 \cap (W_2^0)^0)^0 = (W_1 \cap W_2)^0$. $\square$

Замечание. Из пункта (1) теоремы выше следует, что любое подпространство можно задать однородной системой линейных уравнений. Из пунктов (3) и (4) следует, что поиск суммы подпространств можно свети к поиску пересечения, и наоборот. Отметим также, что в случае пространств, не являющихся конечнопорожденными, не все утверждения данного раздела остаются справедливыми.

7.3 Линейные отображения

Определение 7.10. Пусть U, V — линейные пространства над полем F. *Линейным отображением*, или *линейным оператором*, называется отображение $\varphi : U \to V$, обладающее свойством линейности:

- $\forall \overline{u_1}, \overline{u_2} \in U : \varphi(\overline{u_1} + \overline{u_2}) = \varphi(\overline{u_1}) + \varphi(\overline{u_2})$
- $\forall \alpha \in F : \forall \overline{u} \in U : \varphi(\alpha\overline{u}) = \alpha\varphi(\overline{u})$

Линейное отображение $\varphi : V \to V$ называется *линейным преобразованием.*

Пример. Рассмотрим несколько примеров линейных отображений:

- Поворот вокруг точки, отражение относительно прямой, проекция на прямую в V_2
- Поворот вокруг прямой, отражение относительно плоскости, проекция на плоскость в V_3
- Линейные функционалы на произвольном линейном пространстве V
- Изоморфизм линейных пространств
- Отображение $\varphi : F^n \to F^k$, заданное на каждом $\alpha \in F^n$ как $\varphi(\alpha) := A\alpha$ для некоторой фиксированной матрицы $A \in M_{k\times n}(F)$

Замечание. Пусть $\varphi : U \to V$ — линейное отображение. Тогда:

- $\forall \alpha_1, \dots, \alpha_n \in F : \forall \overline{v_1}, \dots, \overline{v_n} \in V : \varphi(\alpha_1\overline{v_1} + \dots + \alpha_n\overline{v_n}) = \alpha_1\varphi(\overline{v_1}) + \dots + \alpha_n\varphi(\overline{v_n})$
- $\varphi(\overline{0}) = \overline{0}$
- Если система $(\overline{v_1}, \dots, \overline{v_n})$ векторов из U линейно зависима, то система $(\varphi(\overline{v_1}), \dots, \varphi(\overline{v_n}))$ тоже линейно зависима, причем с теми же коэффициентами

Утверждение 7.5. *Пусть U, V — линейные пространства над F, $(\overline{e_1}, \dots, \overline{e_k})$ — базис в U, $\overline{v_1}, \dots, \overline{v_n} \in V$. Тогда существует единственное линейное отображение $\varphi : U \to V$ такое, что для любого $i \in \{1, \dots, k\}$ выполнено $\varphi(\overline{e_i}) = \overline{v_i}$.*

Доказательство. С одной стороны, если некоторое отображение φ удовлетворяет условию, то вектор $\overline{u} \in U$ с координатами $\alpha \in F^n$ оно переводит в $(\overline{v_1}, \dots, \overline{v_k})\alpha$ в силу линейности. С другой стороны, заданное таким образом отображение линейно. $\square$

Определение 7.11. Пусть $\varphi : U \to V$ — линейное отображение.

- ▷ *Образом* отображения φ называется $\operatorname{Im}\varphi := \varphi(U)$.
- ▷ *Ядром* отображения φ называется $\operatorname{Ker}\varphi := \{\overline{u} \in U : \varphi(\overline{u}) = \overline{0}\}$

Утверждение 7.6. *Пусть $\varphi : U \to V$ — линейное отображение, $U' \leqslant U$, $V' \leqslant V$. Тогда:*

1. $\varphi(U') \leqslant V$
2. $\varphi^{-1}(V') = \{\overline{u} \in U : \varphi(\overline{u}) \in V'\} \leqslant U$

Доказательство.

1. Проверим свойства подпространства:
   - ▷ $\varphi(U') \neq \varnothing$, поскольку $\overline{0} \in \varphi(U')$
   - ▷ Если $\overline{v_1}, \overline{v_2} \in \varphi(U')$, то для некоторых $\overline{u_1}, \overline{u_2} \in U'$ выполнены равенства $\varphi(\overline{u_1}) = \overline{v_1}$, $\varphi(\overline{u_2}) = \overline{v_2}$, тогда $\overline{v_1} + \overline{v_2} = \varphi(\overline{u_1} + \overline{u_2}) \in \varphi(U')$
   - ▷ Аналогично предыдущему пункту, если $\overline{v} \in \varphi(U')$, то и для любого $\alpha \in F$ выполнено $\alpha\overline{v} \in \varphi(U')$
2. Проверим свойства подпространства:
   - ▷ $\varphi^{-1}(V') \neq \varnothing$, поскольку $\overline{0} \in \varphi^{-1}(V')$
   - ▷ Если $\overline{u_1}, \overline{u_2} \in \varphi^{-1}(V')$, то $\varphi(\overline{u_1}), \varphi(\overline{u_2}) \in V'$, тогда $\varphi(\overline{u_1} + \overline{u_2}) = \varphi(\overline{u_1}) + \varphi(\overline{u_2}) \in V'$
   - ▷ Аналогично предыдущему пункту, если $\overline{u} \in \varphi^{-1}(V')$, то и для любого $\alpha \in F$ выполнено $\alpha\overline{u} \in \varphi^{-1}(V')$ $\square$

Следствие. Пусть $\varphi : U \to V$ — линейное отображение, тогда $\operatorname{Im}\varphi \leqslant V$ и $\operatorname{Ker}\varphi \leqslant U$.

Утверждение 7.7. *Пусть $\varphi : U \to V$ — линейное отображение, $e = (\overline{e_1}, \dots, \overline{e_k})$ — базис в пространстве U. Тогда $\operatorname{Im}\varphi = \langle \varphi(\overline{e_1}), \dots, \varphi(\overline{e_k}) \rangle$.*

Доказательство.

- $\subset$ Любой вектор $\overline{u} \in U$ представляется в виде линейной комбинации базисных векторов, поэтому $\varphi(\overline{u}) \in \langle \varphi(\overline{e_1}), \dots, \varphi(\overline{e_k}) \rangle$
- $\supset$ Все векторы $\varphi(\overline{e_1}), \dots, \varphi(\overline{e_k})$ лежат в $\operatorname{Im}\varphi$, и $\operatorname{Im}\varphi$ — линейное пространство, поэтому $\langle \varphi(e) \rangle \subset \operatorname{Im}\varphi$ $\square$

Утверждение 7.8. *Пусть $\varphi : U \to V$ — линейное отображение. Тогда отображение φ инъективно* $\Leftrightarrow \operatorname{Ker}\varphi = \{\overline{0}\}$.

Доказательство.

- $\Rightarrow$ Если φ инъективно, то существует единственный вектор $\overline{0} \in U$, для которого $\varphi(\overline{u}) = \overline{0}$

$\Leftarrow$ Пусть для некоторых $\overline{u_1}, \overline{u_2} \in U$ выполнено $\varphi(\overline{u_1}) = \varphi(\overline{u_2})$, тогда $\varphi(\overline{u_1} - \overline{u_2}) = \overline{0}$, откуда $\overline{u_1} - \overline{u_2} = \overline{0} \Rightarrow \overline{u_1} = \overline{u_2}$ $\square$

Замечание. Можно также показать, что верен следующий критерий: линейное отображение $\varphi : U \to V$ инъективно $\Leftrightarrow$ φ переводит линейно независимые системы в линейно независимые.

Утверждение 7.9. *Пусть $\varphi : U \to V$ — линейное отображение, W — прямое дополнение подпространства $\operatorname{Ker}\varphi$ в U. Тогда сужение $\varphi|_W : W \to V$ осуществляет изоморфизм между W и $\operatorname{Im}\varphi$.*

Доказательство. Отображение $\varphi|_W$ линейно в силу линейности отображения φ, проверим его биективность. Оно инъективно, поскольку $\operatorname{Ker}\varphi|_W = \operatorname{Ker}\varphi \cap W = \{\overline{0}\}$. Докажем, что оно также сюръективно. Пусть $\overline{v} \in \operatorname{Im}\varphi$, тогда для некоторого $\overline{u} \in U$ выполнено равенство $\varphi(\overline{u}) = \overline{v}$, при этом вектор $\overline{u}$ можно представить в виде $\overline{u} = \overline{k} + \overline{w}$, где $\overline{k} \in \operatorname{Ker}\varphi$, $\overline{w} \in W$. Тогда $\varphi(\overline{u}) = \varphi(\overline{k}) + \varphi(\overline{w}) = \varphi(\overline{w})$, поэтому $\overline{v} = \varphi(\overline{w})$, что и требовалось. $\square$

Теорема 7.4. *Пусть $\varphi : U \to V$ — линейное отображение. Тогда выполнено следующее равенство:*

$$\dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = \dim U$$

Доказательство. Выберем $W \leqslant U$ такое, что $\operatorname{Ker}\varphi \oplus W = U$, тогда $W \cong \operatorname{Im}\varphi$. По свойству прямой суммы, $\dim U = \dim \operatorname{Ker}\varphi + \dim W = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi$. $\square$

Утверждение 7.10. *Пусть $\varphi : U \to V$ — линейное отображение, $\overline{u_0} \in U$, и $\overline{v_0} = \varphi(\overline{u_0})$. Тогда $\varphi^{-1}(\overline{v_0}) = \overline{u_0} + \operatorname{Ker}\varphi$.*

Доказательство. Если для некоторого вектора $\overline{u} \in U$ выполнено равенство $\varphi(\overline{u}) = \overline{v_0}$, то $\varphi(\overline{u}) = \varphi(\overline{u_0})$, откуда $\varphi(\overline{u} - \overline{u_0}) = \overline{0}$, то есть $(\overline{u} - \overline{u_0}) \in \operatorname{Ker}\varphi$, тогда $\overline{u} \in \overline{u_0} + \operatorname{Ker}\varphi$. $\square$

Замечание. Данное утверждение аналогично тому, что общее решение системы $Ax = b$ имеет вид $x_0 + \Phi\gamma$, $\gamma \in F^m$, где x_0 — частное решение системы, Φ — фундаментальная матрица однородной системы $Ax = 0$.

Определение 7.12. Пусть $\varphi : U \to V$ — линейное отображение, $e = (\overline{e_1}, \ldots, \overline{e_k})$ — базис в U, $\mathcal{F} = (\overline{f_1}, \ldots, \overline{f_n})$ — базис в V. *Матрицей отображения* φ в базисах e и $\mathcal{F}$ называется матрица $A \in M_{n\times k}(F)$ такая, что $(\varphi(\overline{e_1}), \ldots, \varphi(\overline{e_k})) = \mathcal{F}A$. Обозначение — $\varphi \leftrightarrow_{e,\mathcal{F}} A$.

Замечание. Матрица линейного преобразования определяется в одном базисе, а не в паре различных базисов в одном пространстве.

Замечание. Сопоставление линейным отображениям их матриц в фиксированной паре базисов взаимно однозначно: каждому отображению соответствует некоторая матрица, различным отображениям — различные матрицы, и, более того, каждой матрице соответствует некоторое отображение.

Определение 7.13. Множество линейных отображений из U в V обозначается через $\mathcal{L}(U, V)$. Множество линейных преобразований пространства V обозначается через $\mathcal{L}(V)$.

Утверждение 7.11. *Пусть U, V — линейные пространства над полем F. Тогда множество $\mathcal{L}(U, V)$ тоже является линейным пространством над F.*

Доказательство. Проверка свойств линейного пространства аналогична проверке для случая линейных функционалов. $\square$

Утверждение 7.12. *Пусть U, V — линейные пространства над полем F, e — базис в U, $\mathcal{F}$ — базис в V. Тогда сопоставление $\varphi \mapsto A$, $\varphi \leftrightarrow_{e,\mathcal{F}} A$, осуществляет изоморфизм между линейными пространствами $\mathcal{L}(U, V)$ и $M_{n\times k}(F)$.*

Доказательство. Уже доказано, что отображение $\psi : \mathcal{L}(U, V) \to M_{n\times k}(F)$ биективно. Его линейность следует из линейности сопоставления координат в линейном пространстве. $\square$

Утверждение 7.13. *Пусть $\varphi : U \to V$ — линейное отображение пространств над F, e — базис в U, $\mathcal{F}$ — базис в V, $\varphi \leftrightarrow_{e,\mathcal{F}} A$, и $\overline{u} \in U$, $\overline{u} \leftrightarrow_e \alpha$. Тогда $\varphi(\overline{u}) \leftrightarrow_{\mathcal{F}} A\alpha$.*

Доказательство. Выполнены равенства $\varphi(\overline{u}) = \varphi(e\alpha) = \varphi(e)\alpha = \mathcal{F}A\alpha$, поэтому справедливо соотношение $\varphi(\overline{u}) \leftrightarrow_{\mathcal{F}} A\alpha$. $\square$

Утверждение 7.14. *Пусть $\varphi : U \to V$ — линейное отображение, $e = (\overline{e_1}, \dots, \overline{e_k})$ — базис в U, $\mathcal{F} = (\overline{f_1}, \dots, \overline{f_n})$ — базис в V, $\varphi \leftrightarrow_{e,\mathcal{F}} A$. Тогда $\operatorname{rk} A = \dim \operatorname{Im} \varphi$.*

Доказательство. Пусть $\varphi(\overline{e_1}) \leftrightarrow_{\mathcal{F}} \alpha_1, \dots, \varphi(\overline{e_k}) \leftrightarrow_{\mathcal{F}} \alpha_k$. Тогда, поскольку пространства V и F^n изоморфны, то $\operatorname{rk} A = \dim \langle \alpha_1, \dots, \alpha_k \rangle = \dim \langle \varphi(\overline{e_1}), \dots, \varphi(\overline{e_k}) \rangle = \dim \operatorname{Im} \varphi$. $\square$

Определение 7.14. Пусть $\varphi : U \to V$ — линейное отображение. *Рангом отображения* φ называется величина $\operatorname{rk} \varphi := \dim \operatorname{Im} \varphi$

Утверждение 7.15. *Пусть U, V — линейные пространства над полем F, e, e' — два базиса в U, $e' = eS$, $S \in M_k(F)$, $\mathcal{F}, \mathcal{F}'$ — два базиса в V, $\mathcal{F}' = \mathcal{F}T$, $T \in M_n(F)$. Пусть также $\varphi : U \to V$ — линейное отображение, $\varphi \leftrightarrow_{e,\mathcal{F}} A$, $\varphi \leftrightarrow_{e',\mathcal{F}'} A'$. Тогда выполнено следующее равенство:*

$$A' = T^{-1}AS$$

Доказательство. Уже известно, что $\varphi(e) = \mathcal{F}A$, $\varphi(e') = \mathcal{F}'A'$. С другой стороны, в силу линейности выполнены равенства $\varphi(e') = \varphi(eS) = \varphi(e)S$, тогда $\varphi(e') = \mathcal{F}AS = \mathcal{F}'T^{-1}AS$, значит, $A' = T^{-1}AS$. $\square$

Следствие. Если V — линейное пространство над полем F, e, e' — два базиса в V, $e' = eS$, $S \in M_n(F)$. Пусть также $\varphi : V \to V$ — линейное преобразование пространства, $\varphi \leftrightarrow_e A$, $\varphi \leftrightarrow_{e'} A'$. Тогда выполнено следующее равенство:

$$A' = S^{-1}AS$$

Теорема 7.5. *Пусть $\varphi : U \to V$ — линейное отображение. Тогда существуют базисы e в U и $\mathcal{F}$ в V такие, что выполнено следующее:*

$$\varphi \leftrightarrow_{e,\mathcal{F}} \left(\begin{array}{c|c} E & 0 \\ \hline 0 & 0 \end{array}\right)$$

Доказательство. Рассмотрим $\operatorname{Ker} \varphi \leqslant U$ и выберем W — прямое дополнение подпространства $\operatorname{Ker} \varphi$ в U. Пусть $(\overline{e_1}, \dots, \overline{e_s})$ — базис в W, $(\overline{e_{s+1}}, \dots, \overline{e_k})$ — базис в $\operatorname{Ker} \varphi$, тогда $e = (\overline{e_1}, \dots, \overline{e_k})$ — базис в U. Уже было доказано, что $\varphi|_W$ — изоморфизм между W и $\operatorname{Im} \varphi$, тогда $(\varphi(\overline{e_1}), \dots \varphi(\overline{e_s})) = (\overline{f_1}, \dots, \overline{f_s})$ — базис в $\operatorname{Im} \varphi$. Дополним его до базиса $\mathcal{F} = (\overline{f_1}, \dots, \overline{f_n})$ в V. Тогда базисы e и $\mathcal{F}$ и являются искомыми. $\square$

Замечание. Если $\varphi \in \mathcal{L}(V)$, то базисы уже нельзя выбрать независимо друг от друга, поэтому аналогичная теорема неверна.

7.4 Алгебры

Определение 7.15. Пусть $f : A \to B$, $g : B \to C$ — отображения. *Композицией* отображений f, g называется отображение $g \circ f : A \to C$ такое, что для любого $a \in A$ выполнено $(g \circ f)(a) = g(f(a))$.

Утверждение 7.16. *Пусть U, V, W — линейные пространства над полем F с базисами $e, \mathcal{F}, \mathcal{G}$. $\varphi : U \to V$ и $\psi : V \to W$ — линейные отображения. Тогда $\psi \circ \varphi$ — тоже линейное отображение, причем если $\varphi \leftrightarrow_{e,\mathcal{F}} A$, $\psi \leftrightarrow_{\mathcal{F},\mathcal{G}} B$, то $\psi \circ \varphi \leftrightarrow_{e,\mathcal{G}} BA$.*

Доказательство. Линейность композиции очевидна. Поскольку $\varphi(e) = \mathcal{F}A$, $\psi(\mathcal{F}) = \mathcal{G}B$, выполнены следующие равенства:

$$(\psi \circ \varphi)(e) = \psi(\varphi(e)) = \psi(\mathcal{F}A) = \psi(\mathcal{F})A = \mathcal{G}BA \qquad \square$$

Следствие. Если $\varphi, \psi \in \mathcal{L}(V)$, e — базис V, $\varphi \leftrightarrow_e A$, $\psi \leftrightarrow_e B$, то $\psi \circ \varphi \leftrightarrow_e BA$.

Следствие. Пусть V — линейное пространство над полем F, $\dim V = n$. Тогда $(\mathcal{L}(V), +, \circ)$ является кольцом, изоморфным кольцу $(M_n(F), +, \cdot)$.

Доказательство. Зафиксируем базис e в V и рассмотрим отображение $\Theta : \mathcal{L}(V) \to M_n(F)$, сопоставляющее каждому отображению $\varphi \in \mathcal{L}(V)$ его матрицу в базисе e. Как уже было доказано, Θ — изоморфизм линейных пространств, значит, в частности, биекция. Кроме того, для любых операторов $\varphi, \psi \in \mathcal{L}(V)$ выполнено равенство $\Theta(\psi \circ \varphi) = \Theta(\psi)\Theta(\varphi)$. Следовательно, $\mathcal{L}(V)$ — кольцо, поскольку выполнение свойств кольца в нем равносильно выполнению этих свойств в $M_n(F)$. Например, для произвольных $\varphi_1, \varphi_2, \psi \in \mathcal{L}(V)$ выполнено следующее:

$$\begin{aligned}\Theta(\psi \circ (\varphi_1 + \varphi_2)) &= \Theta(\psi)\Theta(\varphi_1 + \varphi_2) = \Theta(\psi)(\Theta(\varphi_1) + \Theta(\varphi_2)) = \\ &= \Theta(\psi)\Theta(\varphi_1) + \Theta(\psi)\Theta(\varphi_2) = \Theta(\psi \circ \varphi_1) + \Theta(\psi \circ \varphi_2) = \Theta(\psi \circ \varphi_1 + \psi \circ \varphi_2)\end{aligned}$$

Тогда, поскольку Θ — биекция, имеем $\psi \circ (\varphi_1 + \varphi_2) = \psi \circ \varphi_1 + \psi \circ \varphi_2$, и получена дистрибутивность в $\mathcal{L}(V)$. Таким образом, $\mathcal{L}(V)$ — кольцо, а Θ — изоморфизм колец. $\square$

Определение 7.16. Кольцо $(R, +, \cdot)$ называется *алгеброй* над полем F, если на нем определено умножение на элементы поля F, удовлетворяющее следующим свойствам:

▷ $(R, +)$ — линейное пространство над F

▷ $\forall r_1, r_2 \in R : \forall \alpha \in F : \alpha(r_1 r_2) = (\alpha r_1) r_2 = r_1(\alpha r_2)$

Определение 7.17. *Изоморфизмом алгебр* называется такое отображение, которое одновременно является изоморфизмом колец и линейных пространств.

Замечание. Построенный ранее изоморфизм $\Theta : \mathcal{L}(V) \to M_n(F)$ является также изоморфизмом алгебр.

Пример. Рассмотрим несколько примеров алгебр

▷ Кольца $\mathcal{L}(V)$ и $M_n(F)$ являются алгербами над полем F

▷ Поле F является алгеброй над самим собой

▷ Кольцо $\mathbb{R}[x]$ является алгеброй над $\mathbb{R}$

8 Определитель

8.1 Перестановки

Определение 8.1. *Группой перестановок* S_n называется следующее множество:

$$S_n := \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} : \sigma \text{ — биекция}\}$$

Данное множество является группой с операцией композиции $\circ$. Элементы группы S_n называются *перестановками.*

Замечание. Перестановку $\sigma \in S_n$ можно записывать в следующем виде:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Определение 8.2. Пусть $a_1, \dots, a_k \in \{1, \dots, n\}$ — различные числа. *Циклом* $(a_1, \dots, a_k)$ называется такая перестановка $\sigma \in S_n$, что выполнены следующие условия:

- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\dots$, $\sigma(a_k) = a_1$
- $\sigma|_{\{1,\dots,n\}\setminus\{a_1,\dots,a_k\}} = \mathrm{id}$

Транспозицией называется цикл длины 2.

Определение 8.3. Циклы $(a_1, \dots, a_k), (b_1, \dots, b_l) \in S_n$ называются *независимыми*, если выполнено равенство $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \varnothing$.

Замечание. Композиция перестановок в группе S_n некоммутативна, однако независимые циклы коммутируют друг с другом.

Утверждение 8.1. *Любая перестановка $\sigma \in S_n$ может быть представлена в виде произведения попарно независимых циклов.*

Доказательство. Рассмотрим граф перестановки σ с множеством вершин $\{1, \dots, n\}$ и множеством ребер $\{(i, j) : \sigma(i) = j\}$. Исходящая и входящая степень каждой вершины в графе равна 1. Покажем, что тогда граф разбивается на циклы. Начнем обходить вершины в следующем порядке: $a_1 := 1$, $a_2 := \sigma(a_1)$, $a_3 := \sigma(a_2)$, и так далее. Процесс рано или поздно должен зациклиться. Пусть a_k — первая вершина такая, что $\sigma(a_k)$ уже попадала в обход. Тогда единственная вершина, которая может совпадать с $\sigma(a_k)$ — это a_1, потому что в остальные вершины уже входит некоторое ребро. Таким образом, получен независимый цикл $(a_1, \dots, a_k)$. Повторяя процедуру для оставшейся части графа перестановки, получим требуемое. $\square$

Утверждение 8.2. *Любая перестановка $\sigma \in S_n$ может быть представлена в виде произведения транспозиций, и даже в виде произведения транспозиций вида $(i, i+1)$.*

Доказательство. Докажем первую часть утверждения индукцией по n. База, $n = 1$, тривиальна, докажем переход. Зафиксируем перестановку $\sigma \in S_n$. Если $\sigma(n) = n$, то $\sigma|_{\{1,\dots,n-1\}}$ — перестановка $n-1$ элемента, и для нее утверждение верно по предположению индукции. Иначе — $\sigma(n) = i \in \{1, \dots, n-1\}$, тогда рассмотрим перестановку $\tau := (i, n)\sigma$. Поскольку $\tau(n) = n$, для τ утверждение верно, следовательно, и $\sigma = (i, n)^{-1}\tau = (i, n)\tau$.

Для доказательства второй части достаточно показать, что любая транспозиция представима в виде произведения транспозиций вида $(i, i+1)$. Это действительно так в силу следующего равенства для произвольных $i, k \in \{1, \dots, n\}$:

$$(i, k) = (i, i+1)(i+1, i+2)\dots(k-1, k)\dots(i+1, i+2)(i, i+1) \qquad \square$$

Замечание. Вторую часть утверждения можно также доказать, используя понятие сортировки пузырьком или независимых циклов.

Определение 8.4. *Беспорядком*, или *инверсией*, в перестановке $\sigma \in S_n$ называется пара индексов (i, j), $i, j \in \{1, \dots, n\}$ такая, что $i < j$, но $\sigma(i) > \sigma(j)$. Числа беспорядков в σ обозначается через $N(\sigma)$. *Знаком* перестановки $\sigma \in S_n$ называется величина $(-1)^{N(\sigma)}$. Обозначения — $\operatorname{sgn}\sigma$, $(-1)^{\sigma}$.

Определение 8.5. Перестановка $\sigma \in S_n$ называется:

- ▷ *Четной*, если $\operatorname{sgn}\sigma = 1$
- ▷ *Нечетной*, если $\operatorname{sgn}\sigma = -1$

Утверждение 8.3. *Пусть $\sigma \in S_n$. Тогда для любых $i, j \in \{1, \dots, n\}$ таких, что $i < j$, выполнено равенство* $\operatorname{sgn}\sigma = -\operatorname{sgn}(\sigma(i, j))$.

Доказательство. Рассмотрим сначала случай, когда $j = i + 1$. Положим $\tau := \sigma(i, i+1)$, тогда $\tau(i+1) = \sigma(i)$, $\tau(i) = \sigma(i+1)$ и для любого $k \in \{1, \dots, n\} \setminus \{i, i+1\}$ выполнено $\tau(k) = \sigma(k)$. Тогда:

- ▷ $(i, i+1)$ — беспорядок в $\sigma \Leftrightarrow (i, i+1)$ — не беспорядок в τ
- ▷ (i, k) при $k \notin \{i, i+1\}$ — беспорядок в $\sigma \Leftrightarrow (i+1, k)$ — беспорядок в τ
- ▷ $(i+1, k)$ при $k \notin \{i, i+1\}$ — беспорядок в $\sigma \Leftrightarrow (i, k)$ — беспорядок в τ
- ▷ (k, l) при $k, l \notin \{i, i+1\}$ — беспорядок в $\sigma \Leftrightarrow (k, l)$ — беспорядок в τ

Таким образом, $N(\tau) = N(\sigma) \pm 1$, и утверждение доказано. Если же $j \neq i+1$, то разложим (i, j) в произведение нечетного числа транспозиций вида $(k, k+1)$, тогда, применяя утверждение нечетное число раз, снова получим требуемое. $\square$

Следствие. Если перестановка $\sigma \in S_n$ представима в виде произведения k транспозиций, то $\operatorname{sgn}\sigma = (-1)^k$.

Следствие. При $n \geqslant 2$ число четных и нечетных перестановок в S_n одинаково.

Доказательство. Отображение $\sigma \mapsto (1, 2)\sigma$ биективно отображает четные перестановки в нечетные. $\square$

Утверждение 8.4. *Для любых $\sigma, \tau \in S_n$ выполнено следующее равенство:*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \operatorname{sgn}\tau$$

Доказательство. Разложим σ и τ в произведения k и l транспозиций соответственно. Тогда выполнены равенства $\operatorname{sgn}\sigma = (-1)^k$, $\operatorname{sgn}\tau = (-1)^l$ и $\operatorname{sgn}(\sigma\tau) = (-1)^{k+l}$. $\square$

Следствие. Множество A_n всех четных перестановок образует подгруппу в S_n.

Доказательство. Проверим свойства подгруппы для A_n:

- $A_n \neq \varnothing$, поскольку $\mathrm{id} \in A_n$
- Если $\sigma, \tau \in A_n$, то $\sigma\tau \in A_n$
- Если $\sigma \in A_n$, то $\sigma^{-1} \in A_n$, поскольку $\operatorname{sgn}\sigma \operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\mathrm{id} = 1$ □

8.2 Полилинейность и кососимметричность

Определение 8.6. Пусть V — линейное пространство над F. Отображение $g : V^n \to F$ называется *полилинейным*, если оно линейно по каждому из n аргументов.

Определение 8.7. Пусть V — линейное пространство над F. Отображение $g : V^n \to F$ называется *кососимметричным*, если для любых позиций аргументов $i, j \in \{1, \ldots, n\}$, $i < j$, выполнены следующие условия:

1. $\forall \overline{v_i}, \overline{v_j} \in V : g(\ldots, \underset{(i)}{\overline{v_i}}, \ldots, \underset{(j)}{\overline{v_j}}, \ldots) = -g(\ldots, \underset{(i)}{\overline{v_j}}, \ldots, \underset{(j)}{\overline{v_i}}, \ldots)$
2. $\forall \overline{v} \in V : g(\ldots, \underset{(i)}{\overline{v}}, \ldots, \underset{(j)}{\overline{v}}, \ldots) = 0$

Замечание. Если свойство (1) выполнено, то свойство (2) выполняется автоматически при $\operatorname{char} F \neq 2$. При этом свойство (1) следует из свойства (2), если отображение g полилинейно. Зафиксируем произвольные $\overline{v_i}, \overline{v_j} \in V$, тогда, опуская многоточия в записях вида $g(\ldots, \underset{(i)}{\overline{v_i}}, \ldots, \underset{(j)}{\overline{v_j}}, \ldots)$, имеем:

$$0 = g(\overline{v_i} + \overline{v_j}, \overline{v_i} + \overline{v_j}) = g(\overline{v_i}, \overline{v_i}) + g(\overline{v_i}, \overline{v_j}) + g(\overline{v_j}, \overline{v_i}) + g(\overline{v_j}, \overline{v_j}) = g(\overline{v_i}, \overline{v_j}) + g(\overline{v_j}, \overline{v_i})$$

Значит, $g(\overline{v_i}, \overline{v_j}) = -g(\overline{v_j}, \overline{v_i})$.

Утверждение 8.5. *Пусть отображение $g : V^n \to F$ кососимметрично. Тогда для любой перестановки $\sigma \in S_n$ и любых векторов $\overline{v_1}, \ldots, \overline{v_n} \in V$ выполнено следующее равенство:*

$$g(\overline{v_{\sigma(1)}}, \ldots, \overline{v_{\sigma(n)}}) = (-1)^\sigma g(\overline{v_1}, \ldots, \overline{v_n})$$

Доказательство. Разложим σ в произведение k транспозиций, тогда при применении транспозиций последовательно и значение функции, и перестановка будут каждый раз менять знак. □

Теорема 8.1. *Пусть V — линейное пространство над F, $e = (\overline{e_1}, \ldots, \overline{e_n})$ — базис в V, $C \in F$. Тогда существует единственное полилинейное кососимметричное отображение $g : V^n \to F$ такое, что $g(\overline{e_1}, \ldots, \overline{e_n}) = C$. Более того, если $(\overline{v_1}, \ldots, \overline{v_n}) = (\overline{e_1}, \ldots, \overline{e_n})A$ для некоторой матрицы $A = (a_{ij}) \in M_n(F)$, то выполнено следующее равенство:*

$$g(\overline{v_1}, \ldots, \overline{v_n}) = C \sum_{\sigma \in S_n} (-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$$

Доказательство. Покажем сначала, что отображение задается не более, чем однозначно. Действительно, если g удовлетворяет условиям теоремы, то для любого набора $(\overline{v_1}, \ldots, \overline{v_n})$

такого, что $(\overline{v_1},\ldots,\overline{v_n}) = (\overline{e_1},\ldots,\overline{e_n})A$, $A = (a_{ij}) \in M_n(F)$, выполнены следующие равенства:

$$g(\overline{v_1},\ldots,\overline{v_n}) = g\left(\sum_{i=1}^{n} a_{i1}\overline{e_i}, \sum_{i=1}^{n} a_{i2}\overline{e_i},\ldots,\sum_{i=1}^{n} a_{in}\overline{e_i}\right) =$$
$$= \sum_{i_1,\ldots,i_n\in\{1,\ldots,n\}} a_{i_1 1}a_{i_2 2}\ldots a_{i_n n} g(\overline{e_{i_1}},\overline{e_{i_2}},\ldots,\overline{e_{i_n}})$$

В силу кососимметричности, слагаемые, в которых у g совпадают хотя бы два аргумента, обращаются в 0, значит, остаются только слагаемые, где все $i_1,\ldots,i_n$ различны. Каждому такому набору индексов соответствует перестановка $\sigma \in S_n$ такая, что $\sigma(i_j) = j$ для всех $j \in \{1,\ldots,n\}$, и это соответствие биективно. Тогда:

$$g(\overline{v_1},\ldots,\overline{v_n}) = \sum_{\sigma\in S_n} a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)} g(\overline{e_{\sigma^{-1}(1)}},\overline{e_{\sigma^{-1}(2)}},\ldots,\overline{e_{\sigma^{-1}(1)}}) =$$
$$= \sum_{\sigma\in S_n} (-1)^{\sigma^{-1}} a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)} g(\overline{e_1},\ldots,\overline{e_n})$$

Итак, если искомое отображение g существует, то обязано следующий вид:

$$g(\overline{v_1},\ldots,\overline{v_n}) = C\sum_{\sigma\in S_n} (-1)^{\sigma} a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$$

Проверим, что полученное отображение удовлетворяет всем условиям:

▷ Проверим линейность g только по первому аргументу, поскольку линейность по остальным аргументам проверяется аналогично. Для этого заметим, что для любого набора $(\overline{v_1},\ldots,\overline{v_n})$ такого, что $(\overline{v_1},\ldots,\overline{v_n}) = (\overline{e_1},\ldots,\overline{e_n})A$, $A = (a_{ij}) \in M_n(F)$, выполнено следующее равенство:

$$g(\overline{v_1},\ldots,\overline{v_n}) = \sum_{i=1}^{n} a_{i1}U_i$$

Значения $U_1,\ldots,U_n$ не зависит от первого столбца матрицы A, тогда, в силу линейности сопоставления координат, отображение g линейно по первому столбцу A.

▷ Уже было доказано, что в случае, если g полилинейно, достаточно проверять свойство (2) из определения кососимметричности. Пусть в матрице A совпадают столбцы a_{*i} и a_{*j}, $i,j \in \{1,\ldots,n\}$, $i \neq j$. Разобьем все перестановки в S_n на пары $(\sigma,(i,j)\sigma)$ и заметим, что значения слагаемых, соответствующих таким перестановкам, равны по модулю и противоположны по знаку, поэтому их сумма равна нулю.

▷ Проверим, что $g(\overline{e_1},\ldots,\overline{e_n}) = C$. Поскольку $e = eE$, то, поэтому единственная перестановка, которой будет соответствовать ненулевое слагаемое в определении отображения g — это id, тогда:

$$g(\overline{e_1},\ldots,\overline{e_n}) = C\sum_{\sigma\in S_n} (-1)^{\sigma} a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)} = C(-1)^{id}a_{11}a_{22}\ldots a_{nn} = C$$

Получено требуемое. □

Определение 8.8. Пусть $A = (a_{ij}) \in M_n(F)$. *Определителем*, или *детерминантом*, матрицы A называется следующая величина:

$$\det A := \sum_{\sigma \in S_n} (-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

Замечание. Определитель полилинеен и кососимметричен как функция столбцов матрицы. Отметим также, что отображение g из теоремы выше можно переписать в виде $g(\overline{v_1}, \dots, \overline{v_n}) = C \det A$, где $(\overline{v_1}, \dots, \overline{v_n}) = (\overline{e_1}, \dots, \overline{e_n})A$, $A \in M_n(F)$, причем $C = g(E)$.

8.3 Свойства определителя

Теорема 8.2. *Для любой матрицы $A \in M_n(F)$ выполнено равенство $\det A^T = \det A$.*

Доказательство. Имеют место следующие равенства:

$$\det A = \sum_{\sigma \in S_n} (-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

$$\det A^T = \sum_{\sigma \in S_n} (-1)^\sigma a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n}$$

Заменим в выражении для $\det A^T$ переменную суммирования σ на $\tau := \sigma^{-1}$, тогда:

$$\det A^T = \sum_{\tau \in S_n} (-1)^{\tau^{-1}} a_{1\tau(1)} a_{2\tau(2)} \dots a_{n\tau(n)} = \sum_{\tau \in S_n} (-1)^{\tau} a_{1\tau(1)} a_{2\tau(2)} \dots a_{n\tau(n)} = \det A \qquad \square$$

Следствие. Определитель полилинеен и кососимметричен как функция строк матрицы.

Утверждение 8.6. *Пусть $A \in M_n(F)$ — верхнетреугольная матрица, имеющая следующий вид:*

$$A = \begin{pmatrix} a_{11} & \dots & * \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_{nn} \end{pmatrix}$$

Тогда $\det A = a_{11} a_{22} \dots a_{nn}$.

Доказательство. Если в перестановке $\sigma \in S_n$ существует такой индекс $i \in \{1, \dots, n\}$, что $\sigma(i) < i$, то соответствующее слагаемое в формуле определителя равно нулю, поскольку $a_{i\sigma(i)} = 0$. Единственная перестановка, в которой нет такого индекса, — это id, поэтому $\det A = a_{11} a_{22} \dots a_{nn}$. $\square$

Замечание. Поскольку определитель не меняется при транспонировании, для нижнетреугольных матриц верно аналогичное утверждение.

Утверждение 8.7. *Пусть $A \in M_n(F)$, $L \in M_n(F)$ — элементарная матрица. Тогда выполнено равенство* $\det AL = \det A \det L$.

Доказательство. Рассмотрим все три случая:

▷ Если $L = D_{ij}(\alpha) = E + \alpha E_{ji}$ — матрица прибавления к i-му столбцу j-го, умноженного на α, то $\det L = 1$, и, в силу полилинейности определителя:

$$\det AL = \det(a_{*1}, \dots, a_{*i} + \alpha a_{*j}, \dots, a_{*j}, \dots a_{*n}) =$$
$$= \det(a_{*1}, \dots, a_{*i}, \dots, a_{*j}, \dots a_{*n}) + \alpha \det(a_{*1}, \dots, a_{*j},, a_{*j}, \dots a_{*n}) = \det A \det L$$

▷ $L = T_i(\lambda) = E + (\lambda - 1)E_{ii}$ — матрица умножения i-го столбца на λ, тогда $\det L = \lambda$, и, в силу полилинейности определителя:

$$\det AL = \det(a_{*1}, \ldots, \lambda a_{*i}, \ldots a_{*n}) = \lambda \det(a_{*1}, \ldots, a_{*i}, \ldots a_{*n}) = \det A \det L$$

▷ $P_{ij} = E - (E_{ii} + E_{jj}) + (E_{ij} + E_{ji})$ — матрица перестановки i-го и j-го столбца местами, тогда $\det L = -1$, и, в силу кососимметричности определителя:

$$\det AL = -\det A = \det A \det L$$

Во всех трех случаях требуемое равенство выполнено. □

Замечание. Поскольку определитель не меняется при транспонировании, аналогичное утверждение справедливо для элементарных преобразований строк.

Следствие. Получен алгоритм вычисления определителя: следует привести матрицу к ступенчатому виду, то есть, в частности, верхнетреугольному виду, найти определитель полученной матрицы и матриц элементарных преобразований, тогда результатом будет произведение найденных определителей.

Теорема 8.3. *Пусть $A \in M_n(F)$. Тогда A невырожденна* $\Leftrightarrow \det A \neq 0$.

Доказательство. Приведем матрицу к ступенчатому виду A'. Поскольку определители элементарных матриц отличны от нуля, то $\det A \neq 0 \Leftrightarrow \det A' \neq 0$. Если A невырожденна, то в A' ровно n ступенек, и $\det A' \neq 0$. Если же A вырожденна, то в A' менее n ступенек, значит, в A' есть нулевой элемент на главной диагонали, и $\det A' = 0$. □

Теорема 8.4. *Для любых матриц $A, B \in M_n(F)$ выполнено следующее равенство:*

$$\det AB = \det A \det B$$

Первый способ доказательства. Если хотя бы одна из матриц A, B вырожденна, то ее определитель равен нулю, и, кроме того, $\operatorname{rk} AB < n$, тогда $\det AB = 0 = \det A \det B$. Если же A и B невырожденны, то они представимы в виде произведений элементарных матриц. Пусть $A = U_1 \ldots U_k$, $B = S_1 \ldots S_l$, тогда:

$$\det AB = \prod_{i=1}^{k} \det U_i \prod_{i=1}^{l} \det S_i = \det A \det B$$ □

Второй способ доказательства. Зафиксируем матрицу $A \in M_n(F)$ и рассмотрим функцию $f : M_n(F) \to F$ такую, что $f(X) := \det AX$ для любой матрицы $X \in M_n(F)$. Тогда f является полилинейной и кососимметричной функцией от столбцов матрицы X, и, по теореме о полилинейной и кососимметричной функции, $f(X) = f(E) \det X = \det A \det X$. □

Теорема 8.5 (об определителе с углом нулей)**.** *Пусть матрица $A \in M_n(F)$ имеет следующий вид:*

$$A = \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right), \; B \in M_k(F),\; D \in M_{n-k}(F)$$

Тогда $\det A = \det B \det D$.

Доказательство. Рассмотрим функцию $f : M_k(F) \to F$ такую, что для любой матрицы $X \in M_k(F)$ выполнено следующее равенство:

$$f(X) := \left|\begin{array}{c|c} X & C \\ \hline 0 & D \end{array}\right|$$

Заметим, что функция f является полилинейной и кососимметричной функцией от столбцов матрицы X, тогда:

$$f(X) = f(E)\det X = \left|\begin{array}{c|c} E & C \\ \hline 0 & D \end{array}\right| \det X$$

Аналогично, рассмотрим функцию $g : M_{n-k}(F) \to F$ такую, что для любой матрицы $Y \in M_{n-k}(F)$ выполнено следующее равенство:

$$g(Y) := \left|\begin{array}{c|c} E & C \\ \hline 0 & Y \end{array}\right|$$

Заметим, что функция g является полилинейной и кососимметричной функцией от строк матрицы Y, тогда:

$$g(X) = g(E)\det Y = \left|\begin{array}{c|c} E & C \\ \hline 0 & E \end{array}\right| \det Y = \det Y$$

Итак, $\det A = f(B) = \det B g(D) = \deg B \det D$. $\square$

Определение 8.9. Пусть $A \in M_n(F)$. *Минором* порядка k матрицы A называется определитель некоторой ее подматрицы размера $k \times k$.

Замечание. Теорему о базисном миноре можно переформулировать так: ранг матрицы $A \in M_{n\times k}(F)$ равен наибольшему из порядков его ненулевых миноров.

Определение 8.10. Пусть $A = (a_{ij}) \in M_n(F)$, $i, j \in \{1, \dots, n\}$.

- ▷ Минором, *дополнительным* к элементу a_{ij}, называется величина $M_{ij} := \det A'$, где матрица A' получена из A удалением i-й строки и j-го столбца
- ▷ *Алгебраическим дополнением* к элементу a_{ij} называется величина $A_{ij} := (-1)^{i+j} M_{ij}$

Утверждение 8.8. *Пусть матрица $A \in M_n(F)$ имеет следующий вид:*

$$A = \left(\begin{array}{c|c|c} * & * & * \\ \hline 0 & a_{ij} & 0 \\ \hline * & * & * \end{array}\right)$$

Тогда $\det A = a_{ij} A_{ij}$.

Доказательство. Последовательными перестановками строк и столбцов добьемся того, чтобы A приняла следующий вид:

$$A' = \left(\begin{array}{c|c} a_{ij} & 0 \\ \hline * & M'_{ij} \end{array}\right), \ M'_{ij} \text{ — подматрица, дополнительная к } a_{ij}$$

Такого результата можно добиться с помощью $i-1$ транспозиции строк и $j-1$ транспозиции столбцов. Значит, $\det A = (-1)^{i+j-2}\det A' = (-1)^{i+j}\det A'$. Тогда, по теореме об определителе с углом нулей, $\det A = (-1)^{i+j}a_{ij}M_{ij} = a_{ij}A_{ij}$. □

Теорема 8.6 (о разложении по строке или столбцу)**.** *Пусть $A = (a_{ij}) \in M_n(F)$. Тогда выполнены следующие равенства:*

$$\det A = \sum_{i=1}^{n} a_{ij}A_{ij} = \sum_{j=1}^{n} a_{ij}A_{ij}$$

Доказательство. Докажем без ограничения общности вторую формулу, поскольку первая может быть получена из второй транспонированием. Представим i-ю строку матрицы A в следующем виде:

$$a_{i*} = (a_{i1}, a_{i2}, \dots, a_{in}) = (a_{i1}, 0, \dots, 0) + (0, a_{i2}, \dots, 0) + \dots + (0, 0, \dots, a_{in})$$

Тогда, в силу линейности определителя как функции от строк A и предыдущего утверждения, получим:

$$detA = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}$$ □

Теорема 8.7 (правило Крамера)**.** *Пусть $A \in M_n(F)$, причем $\Delta := \det A \neq 0$, $b \in F^n$. Для каждого $i \in \{1, \dots, n\}$ положим $\Delta_i := \det(a_{*1}, \dots, a_{*i-1}, b, a_{*i+1}, \dots, a_{*n})$. Тогда система $Ax = b$ имеет единственное решение x, и это решение имеет следующий вид:*

$$x = \left(\frac{\Delta_1}{\Delta}, \dots, \frac{\Delta_n}{\Delta}\right)^T$$

Доказательство. Матрица A невырожденна и потому обратима, тогда $x := A^{-1}b$ — единственное решение системы. Заметим, что для этого решения и каждого $i \in \{1, \dots, n\}$ выполнены следующие равенства:

$$\Delta_i = \det\left(a_{*1}, \dots, a_{*i-1}, \sum_{j=1}^{n} x_j(a_{*j}), a_{*i+1}, \dots, a_{*n}\right) =$$
$$= \sum_{j=1}^{n} x_j \det\left(a_{*1}, \dots, a_{*i-1}, a_{*j}, a_{*i+1}, \dots, a_{*n}\right) =$$
$$= x_i \det\left(a_{*1}, \dots, a_{*i-1}, a_{*i}, a_{*i+1}, \dots, a_{*n}\right) = x_i\Delta$$

Таким образом, для любого $i \in \{1, \dots, n\}$ выполнено $x_i = \frac{\Delta_i}{\Delta}$. □

Утверждение 8.9. *Пусть $A \in M_n(F)$, $\Delta := \det A = 0$, но существует $i \in \{1, \dots, n\}$ такое, что $\Delta_i \neq 0$. Тогда система несовместна.*

Доказательство. Поскольку $\Delta = 0$, то A вырожденна, то есть $\operatorname{rk} A < n$. При этом существует $i \in \{1, \dots, n\}$ такой, что $\Delta_i \neq 0$, поэтому в $(A|b)$ существует система из n линейно независимых столбцов, тогда $\operatorname{rk}(A|b) > \operatorname{rk} A$. Значит, по теореме Кронекера-Капелли, система несовместна. □

Следствие (формула Крамера)**.** Пусть $A = (a_{ij}) \in M_n(F)$ — обратимая матрица, и пусть $B = (b_{ij}) \in M_n(F)$ — обратная к ней матрица. Тогда для любых $i, j \in \{1, \dots, n\}$ выполнено следующее равенство:

$$b_{ij} = \frac{A_{ji}}{\det A}$$

Доказательство. Каждый столбец b_{*j} матрицы B является единственным решением системы линейных уравнений $Ab_{*j} = e_{*j}$, где e_{*j} — j-й столбец единичной матрицы. Тогда:

$$b_{ij} = \frac{\det(a_{*1}, \ldots, a_{*i-1}, e_{*j}, a_{*i+1}, \ldots, a_{*n})}{\det A}$$

По уже доказанному утверждению, определитель в выражении выше равен A_{ji}. □

Теорема 8.8. *Пусть F — поле, причем для любого элемента $\alpha \in F$ выполнено $\alpha^2 \neq -1$. Рассмотрим следующее множество матриц:*

$$K := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(F) \right\}$$

Тогда K является полем, в которм существует $i \in K$ такое, что $i^2 = -1$. Кроме того, K содержит подполе, изоморфное F.

Доказательство.

1. Непосредственная проверка позволяет убедиться, что $(K, +)$ является подгруппой в $(M_2(F), +)$, причем K замкнуто относительно умножения и содержит нейтральный относительно умножения элемент — матрицу $E \in M_2(F)$. Значит, K является подкольцом в $M_2(F)$.

2. Покажем теперь, что K — поле. Для этого следует проверить, что $K^* = K \backslash \{0\}$. Действительно, если $a, b \in F$, и эти элементы не равны нулю одновременно, то без ограничения общности $b \neq 0$, тогда:

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 = b^2(1 + (ab^{-1})^2) \neq 0$$

Итак, согласно формуле Крамера, матрица выше обратима, причем выполнено следующее равенство:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in K$$

3. Поле K содержит подполе $F' := \{aE : a \in F\}$, изоморфное полю F. Легко проверить, что операции с его элементами этого подполя соответствуют операциям с элементами поля F.

4. В поле K есть элемент i следующего вида:

$$i := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in K$$

Тогда $i^2 = (-1)E$, и матрица $(-1)E$ соответствует числу -1 в подполе F'.

Получено требуемое. □

Следствие. Если $F = \mathbb{R}$, то полученное поле изоморфно $\mathbb{C}$, причем изоморфизм имеет следующий вид:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$$

Замечание. В теореме выше можно считать поле F подполем в K, тогда K — алгебра над F, причем $\dim K = 2$.

9 Основы теории групп

9.1 Изоморфизмы групп

Утверждение 9.1. *Невырожденные матрицы порядка n над полем F образуют группу по умножению.*

Доказательство. Проверим непосредственно свойства группы:

- ▷ Умножение матриц в $M_n(F)$ ассоциативно.
- ▷ Матрица $E_n \in M_n(F)$ — невырожденная, и она является нейтральным элементом по умножению.
- ▷ Если A, B — невырожденные матрицы порядка n, то AB — тоже, поскольку $\det AB = \det A \det B \neq 0$. Кроме того, матрицы A и B обратимы, и матрицы A^{-1}, B^{-1} — тоже невырожденные. □

Определение 9.1. Пусть F — поле, $n \in \mathbb{N}$.

- ▷ Группа невырожденных матриц порядка n над F обозначается через $\mathrm{GL}_n(F)$
- ▷ Группа невырожденных матриц порядка n над F с определителем, равным 1, обозначается через $\mathrm{SL}_n(F)$

Утверждение 9.2. $\mathrm{GL}_n(\mathbb{Z}) := \{A \in M_n(\mathbb{Z}) : \exists A^{-1} \in M_n(\mathbb{Z})\}$ *— это группа матриц из $M_n(\mathbb{Z})$ с определителем, равным ± 1.*

Доказательство.

- ▷ Если $A, A^{-1} \in \mathrm{GL}_n(\mathbb{Z})$, то $\det A \det A^{-1} = \det E = 1$, откуда $\det A = \det A^{-1} = \pm 1$
- ▷ Если $\det A = \pm 1$, то, по формуле Крамера, $A^{-1} \in M_n(\mathbb{Z})$, и, аналогично, $\det A^{-1} = \pm 1$, тогда $A^{-1} \in \mathrm{GL}_n(\mathbb{Z})$ □

Определение 9.2. *Порядком* группы G называется мощность множества G.

Определение 9.3. *Гомоморфизмом групп* G и H называется отображение $\varphi : G \to H$ такое, что для любых $a,b \in G$ выполнено равенство $\varphi(ab) = \varphi(a)\varphi(b)$. *Изоморфизмом групп* G и H называется биективный гомоморфизм $\varphi : G \to H$. Пространства G и H называются *изоморфными*, если между ними существует изоморфизм. Обозначение — $G \cong H$.

Замечание. Аналогичным образом можно определить изоморфизм и для других алгебраических структур, таких как кольцо или алгебра.

Утверждение 9.3. *Пусть $\varphi : G \to H$ — гомоморфизм групп, тогда:*

- $\varphi(e) = e$
- $\forall a \in G : \varphi(a^{-1}) = (\varphi(a))^{-1}$

Доказательство.

- $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e) \Rightarrow \varphi(e) = e$
- $\varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}\varphi(e) = (\varphi(a))^{-1}$ □

Пример. Гомоморфизмом групп $(\mathbb{Z}, +)$ и $(\mathbb{Z}_n, +)$ является отображение $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ такое, что для любого $a \in \mathbb{Z}$ выполнено $\varphi(a) := \overline{a}$.

Теорема 9.1 (Кэли)**.** *Пусть G — конечная группа, $|G| = n$. Тогда существует подгруппа $H \leqslant S_n$ такая, что $H \cong G$, то есть группа G вкладывается в группу S_n.*

Доказательство. Рассмотрим группу $S(G)$ перестановок множества G, тогда $S(G) \cong S_n$, поскольку имеет место биекция между G и $\{1, \ldots, n\}$. Найдем требуемую подгруппу в $S(G)$. Для каждого элемента $a \in G$ определим перестановку $\sigma_a \in S(G)$ такую, что для любого $b \in G$ выполнено $\sigma_a(b) := ab$. Положим $H := \{\sigma_a \in S(G) : a \in G\}$. Проверим, что $H \leqslant S(G)$:

- $H \neq \varnothing$, поскольку $\sigma_e = \mathrm{id} \in H$
- $\forall a, b \in G : \sigma_a \circ \sigma_b = \sigma_{ab} \in H$
- $\forall a \in G : (\sigma_a)^{-1} = \sigma_{a^{-1}} \in H$

Определим отображение $\varphi : G \to H$ для каждого $a \in G$ как $\varphi(a) := \sigma_a$. Очевидно, это гомоморфизм, причем сюръективный. Он также инъективен, поскольку для различных $a, b \in G$ выполнено $\sigma_a(e) \neq \sigma_b(e)$. Таким образом, $G \cong H \leqslant S(G) \cong S_n$. □

9.2 Циклические группы

Утверждение 9.4. *Пусть G — группа, $\{H_\alpha\}_{\alpha \in A}$ — произвольное семейство подгрупп в G. Тогда:*

$$\bigcap_{\alpha \in A} H_\alpha \leqslant G$$

Доказательство. Положим $K := \bigcap_\alpha H_\alpha$ и проверим свойства подгруппы:

- $K \neq \varnothing$, поскольку $e \in K$
- Если $a, b \in K$, то $a, b \in H_\alpha$ для любого $\alpha \in A$, тогда $ab \in H_\alpha$ для любого $\alpha \in A$, откуда $ab \in K$
- Аналогично предыдущему пункту, если $a \in K$, то $a^{-1} \in K$ □

Определение 9.4. Пусть G — группа, $X \subset G$. *Подгруппой, порожденной множеством* X, называется следующая подгруппа:

$$\langle X \rangle := \bigcap_{H \leqslant G, X \subset H} H$$

Замечание. $\langle X \rangle$ — наименьшая по включению подгруппа в G, содержащая множество X.

Пример. Рассмотрим несколько примеров порождающих множеств групп:

▷ $\mathbb{Z} = \langle 1 \rangle$

▷ $2\mathbb{Z} = \langle 2 \rangle$

▷ $\{e\} = \langle \varnothing \rangle$ для любой группы G с нейтральным элементом e

Утверждение 9.5. *Для любого $n \in \mathbb{N}$ выполнено равенство $S_n = \langle (1,2), (1,\ldots,n) \rangle$.*

Доказательство. Уже было доказано, что любую перестановку $\sigma \in S_n$ можно представить в виде произведения транспозиций вида $(i, i+1)$. В то же время, любую такую транспозицию можно представить в виде произведения двух перестановок из условия. Для этого сначала циклическими сдвигами следует поместить элементы $i, i+1$ на позиции $1, 2$, затем поменять их местами и циклическими сдвигами вернуть на свои позиции. □

Утверждение 9.6. *Пусть G — группа, $X \subset G$. Тогда выполнено следующее равенство:*

$$\langle X \rangle = \{x_1 \ldots x_n : x_i \in X \text{ или } x_i^{-1} \in X\}$$

Доказательство. Обозначим правую часть равенства через K.

$\supset$ Для любой подгруппы $H \leqslant G$, такой, что $X \subset H$, каждый из множителей x_i содержится в H, поэтому и $x_1 \ldots x_n \in H$. Значит, $K \subset \langle X \rangle$.

$\subset$ Множество K непусто потому, что пустым произведением считается элемент e, а свойства замкнутости множества K относительно умножения и взятия обратного элемента, очевидно, выполнены. Значит, $K \leqslant G$, причем $X \subset K$, поэтому $\langle X \rangle \subset K$. □

Замечание. В любой группе G можно определить степень $n \in \mathbb{Z}$ произвольного элемента $a \in G$, отличную от нулевой и первой:

▷ Если $n > 0$, то a^n — это произведение n элементов a

▷ Если $n < 0$, то a^n — это произведение $|n|$ элементов a^{-1}

Справедливо свойство, что для любых $k, n \in \mathbb{Z}$ выполнено $a^k a^n = a^{k+n}$. В этом можно убедиться непосредственной проверкой, перебрав все случаи знаков чисел k и n.

Определение 9.5. *Порядком* элемента a называется наименьшее $n \in \mathbb{N}$ такое, что $a^n = e$. Если такого n не существует, то порядок считается равным ∞. Обозначение — $\operatorname{ord} a$.

Утверждение 9.7. *Пусть G — группа, $a \in G$, $\operatorname{ord} a = n$. Тогда $a^k = e \Leftrightarrow n \mid k$.*

Доказательство. Разделим k на n с остатком, то есть представим его в виде $k = qn + r$, $q \in \mathbb{Z}$, $r \in \{0, \ldots, n-1\}$. Тогда $a^k = a^{qn+r} = (a^n)^q a^r = a^r$. Если $r \neq 0$, то $a^r \neq e$, иначе бы порядок a был меньше n, что противоречит условию. Значит, $a^k = e \Leftrightarrow r = 0 \Leftrightarrow n \mid k$. □

Утверждение 9.8. *Пусть G — группа, $a \in G$. Тогда $\operatorname{ord} a = |\langle a \rangle|$.*

Доказательство. Если $\operatorname{ord} a = n \in \mathbb{N}$, то $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{e, a, \ldots, a^{n-1}\}$, поэтому $|\langle a \rangle| \leqslant n$. Кроме того, все элементы различны $e, a, \ldots, a^{n-1}$. Действительно, если для некоторых $r, s \in \{1, \ldots, n-1\}$, $r < s$ выполнено $a^r = a^s$, то $a^{s-r} = e$, откуда $s - r = 0$ в силу минимальности порядка n. Значит, $|\langle a \rangle| = n$. Если же $\operatorname{ord} a = \infty$, то для любых $\forall r, s \in \mathbb{Z}$, $r < s$, выполнено $a^r \neq a^s$ из аналогичных соображений, тогда $|\langle a \rangle| = \infty$. $\square$

Определение 9.6. Группа G называется *циклической*, если существует элемент $\exists a \in G$ такой, что $\langle a \rangle = G$.

Пример. Рассмотрим несколько примеров циклических групп:

- ▷ $\mathbb{Z} = \langle 1 \rangle$
- ▷ $\mathbb{Z}_n = \langle \overline{1} \rangle$

Теорема 9.2. *Любые две циклических группы одного порядка изоморфны.*

Доказательство. Пусть G — циклическая группа, $a \in G$, $G = \langle a \rangle$.

- ▷ Пусть $|G| = \infty$. Докажем, что тогда $G \cong \mathbb{Z}$. Рассмотрим отображение $\varphi : \mathbb{Z} \to G$, для каждого $k \in \mathbb{Z}$ имеющее вид $\varphi(k) := a^k$. Очевидно, это гомоморфизм, причем сюръективный. Докажем его инъективность. Пусть для некоторых $k, l \in \mathbb{Z}$ выполнено равенство $a^k = a^l$, тогда $a^{k-l} = e$, что возможно только при $k = l$. Таким образом, получен изоморфизм между $\mathbb{Z}$ и G.
- ▷ Пусть $|G| = n \in \mathbb{N}$. Докажем, что тогда $G \cong \mathbb{Z}_n$. Рассмотрим отображение $\varphi : \mathbb{Z}_n \to G$, для каждого $\overline{k} \in \mathbb{Z}_n$ имеющее вид $\varphi(\overline{k}) := a^k$. Отображение φ определено корректно, поскольку если $a^k = a^l$ для некоторых $k, l \in \mathbb{Z}$, то $a^{k-l} = e$, откуда $n \mid (k - l)$ и $\overline{k} = \overline{l}$. Очевидно тогда, что это гомоморфизм, причем инъективный в силу уже доказанного и сюръективный. $\square$

Замечание. Циклическая группа не более, чем счетна. Более того, любая конечнопорожденная группа не более, чем счетна, поскольку $\mathbb{N}^k$ равномощно $\mathbb{N}$.

Теорема 9.3. *Подгруппа циклической группы тоже является циклической группой.*

Доказательство. Докажем более сильное утверждение и сразу опишем все возможные подгруппы циклической группы G.

- ▷ Пусть $|G| = \infty$, тогда можно считать, что $G = \mathbb{Z}$. Пусть $H \leqslant \mathbb{Z}$. Если $H = \{0\}$, то группа H — циклическая. Иначе — H содержит ненулевые и, в частности, положительные числа. Пусть n — наименьшее положительное число в H. Тогда, поскольку H — группа, $\langle n \rangle = n\mathbb{Z} \leqslant H$. Теперь рассмотрим $k \in H$. Разделим k на n с остатком, то есть представим его в виде $k = qn + r$, $q \in \mathbb{Z}$, $r \in \{0, \ldots, n-1\}$, тогда $r = k - qn \in H$, и, в силу минимальности числа n, $r = 0$, то есть $n \mid k$. Значит, $H = n\mathbb{Z}$.
- ▷ Пусть $|G| = n \in \mathbb{N}$, тогда можно считать, что $G = \mathbb{Z}_n$. Если $H = \{\overline{0}\}$, то группа H — циклическая. Иначе — H содержит ненулевые элементы. Пусть l — наименьшее положительное число такое, что $\overline{l} \in H$. Тогда поскольку H — группа, $\langle \overline{l} \rangle = l\mathbb{Z}_n \leqslant H$. Разделим n на l с остатком, то есть представим его в виде $n = ql + r$, где $q \in \mathbb{Z}$, $r \in \{0, \ldots, l-1\}$, тогда $r = n - ql \in H$, и, в силу минимальности числа l, $r = 0$, то есть $l \mid n$. Из аналогичных соображений деления с остатком получим, что $H = l\mathbb{Z}_n$. $\square$

Утверждение 9.9. *Пусть G — группа, $a \in G$, $\operatorname{ord} a = n$. Тогда для любого $k \in \mathbb{N}$ выполнено следующее равенство:*

$$\operatorname{ord} a^k = \frac{n}{(n,k)}$$

Доказательство. Пусть для некоторого $l \in \mathbb{N}$ выполнено $(a^k)^l = a^{kl} = e$. Разделим kl с остатком на n, то есть представим его в виде $kl = qn + r$, $q \in \mathbb{Z}$, $r \in \{0, \ldots, n-1\}$, тогда $a^{kl} = (a^n)^q a^r = a^r$, поэтому если $r \neq 0$, то порядок $\operatorname{ord} a < n$, что неверно. Значит, $r = 0$ и $n \mid kl$. Наименьшее число, одновременно кратное числам n и k — это $[n,k]$, тогда $l = \frac{[n,k]}{k} = \frac{n}{(n,k)}$. □

Замечание. Одна и та же группа может быть порождена множествами различной мощности. Например, $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle = \langle 6, 10, 15 \rangle$.

9.3 Смежные классы

Определение 9.7. Пусть G — группа, $A, B \subset G$. Определим следующие операции с множествами:

- ▷ $AB := \{ab :\in A, b \in B\}$
- ▷ $A^{-1} := \{a^{-1} : a \in A\}$

Замечание.

- ▷ Умножение множеств ассоциативно в силу ассоциативности умножения в G.
- ▷ В общем случае неверно, что множество A^{-1} — обратное к A, поскольку не всегда $AA^{-1} = \{e\}$.

Определение 9.8. Пусть G — группа, $H \leqslant G$, $a \in G$.

- ▷ *Левым смежным классом* элемента a по подгруппе H называется множество aH
- ▷ *Правым смежным классом* элемента a по подгруппе H называется множество Ha

Множество левых смежных классов по подгруппе H в группе G обозначается через G/H, множество правых смежных классов — через $H \backslash G$.

Замечание. Если $a \in H$, то $aH = H$, поскольку H — группа.

Утверждение 9.10. *Пусть G — группа, $H \leqslant G$, $a, b \in G$. Тогда следующие утверждения эквивалентны:*

1. $aH \cap bH \neq \varnothing$
2. $b^{-1}a \in H$
3. $aH = bH$
4. $a \in bH$

Доказательство.

- ▷ $(1 \Rightarrow 2)$ По условию, $\exists h_1, h_2 \in H : ah_1 = bh_2$, откуда $b^{-1}a = h_2 h_1^{-1} \in H$

▷ $(2 \Rightarrow 3)$ Поскольку H — группа и $b^{-1}a \in H$, то $(b^{-1}a)H = H$, откуда $aH = bH$

▷ $(3 \Rightarrow 4)$ Заметим, что $a = ae$, поэтому $a \in aH = bH$

▷ $(4 \Rightarrow 1)$ Поскольку $a = ae$ и $a \in bH$, то $a \in aH \cap bH$, следовательно, $aH \cap bH \neq \varnothing$ □

Замечание. Аналогичное утверждение для правых смежных классов будет верно, если заменить в формулировке второго пункта $b^{-1}a \in H$ на $ab^{-1} \in H$.

Теорема 9.4 (Лагранжа)**.** *Пусть G — конечная группа, $H \leqslant G$. Тогда выполнены следующие равенства:*

$$|G| = |H||G/H| = |H||H\backslash G|$$

Доказательство. Если смежные классы в G пересекаются хотя бы по одному элементу, то они совпадают. Тогда, поскольку для любого $a \in G$ выполнено $a \in aH$, вся группа G разбивается на непересекающиеся смежные классы порядка $|H|$, откуда и следует требуемое равенство. □

Замечание. Из аналогичных соображений можно показать, что $|G| = |H| \cdot |H\backslash G|$, тогда в случае, когда G — конечная группа, верно, что $|G/H| = |H\backslash G|$.

Следствие. Пусть G — конечная группа, $a \in G$. Тогда:

1. $\operatorname{ord} a \mid |G|$
2. $a^{|G|} = e$

Доказательство.

1. По теореме Лагранжа, $\operatorname{ord} a = |\langle a \rangle| \mid |G|$
2. Пусть $\operatorname{ord} a = k$, тогда $k \mid |G|$ в силу пункта (1), откуда $a^{|G|} = e$ □

Следствие (малая теорема Ферма)**.** Пусть p — простое число, $a \in \mathbb{Z}$, $p \nmid a$. Тогда $a^{p-1} \equiv_p 1$.

Доказательство. Рассмотрим группу $(\mathbb{Z}_p \backslash \{\overline{0}\}, \cdot)$, $|\mathbb{Z}_p \backslash \{\overline{0}\}| = p - 1$, и применим пункт (2) следствия выше. Получим, что $\overline{a}^{p-1} = \overline{1}$. □

Определение 9.9. *Функцией Эйлера* следующая функция $\varphi : \mathbb{N} \to \mathbb{N}$, для любого $n \in \mathbb{N}$ определенная следующим образом как $\varphi(n) := |\{a \in \mathbb{N} : a \leqslant n, (a, n) = 1\}|$

Замечание. Если $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение числа $n \in \mathbb{N}$, $n \geqslant 2$, на простые множители, то выполнено равенство $\varphi(n) = n\big(1 - \frac{1}{p_1}\big) \dots \big(1 - \frac{1}{p_k}\big)$.

Теорема 9.5 (Эйлера)**.** *Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, n) = 1$. Тогда $a^{\varphi(n)} \equiv_n 1$.*

Доказательство. Рассмотрим группу $(\mathbb{Z}_n^*, \cdot)$, тогда $\mathbb{Z}_n^* = \{\overline{b} \in \mathbb{Z}_n : b \in \mathbb{Z}, (b, n) = 1\}$ и $|\mathbb{Z}_n^*| = \varphi(n)$. Применим пункт (2) следствия выше и получим, что $\overline{a}^{|\mathbb{Z}_n^*|} = \overline{a}^{\varphi(n)} = \overline{1}$. □

Утверждение 9.11. *Пусть G — группа. Тогда $\forall H \leqslant G : |G/H| = |H\backslash G|$.*

Доказательство. Сопоставление $aH \mapsto (aH)^{-1} = Ha^{-1}$ является биекцией, поскольку оно обратимо, из чего следует и сюръективность, и инъективность. □

Определение 9.10. Пусть G — группа, $H \leqslant G$. *Индексом* подгруппы H в G называется величина $|G : H| := |G/H| = |H\backslash G|$.