Геометрия, 1 курс

Городенский

3 сентября 2020 г. — 11 октября 2020 г.

Формула оценки: $\min\left(\frac{S+C+E+L+K}{40}, 10\right)$*, где* S, C, E, L, K *— оценки за семинары, коллоквиум, экзамен, листки и контрольные; каждая из этих оценок от 0 до 100.*

Векторные и аффинные пространства

Определение 1. Векторное пространство — множество V (элементы которого называются «векторами») с операциями $+ : V \times V \to V$ и $\cdot : \mathbb{F} \times V \to V$, обладающими следующими свойствами:

- V — абелева группа по сложению.
- $\forall \lambda, \mu \in \mathbb{F}, \overline{v} \in V : \lambda(\mu\overline{v}) = (\lambda\mu)\overline{v}$;
- $\forall \lambda, \mu \in \mathbb{F}, \overline{v} \in V : (\lambda + \mu)\overline{v} = \lambda\overline{v} + \mu\overline{v}$;
- $\forall \lambda \in \mathbb{F}, \overline{v}, \overline{w} \in V : \lambda(\overline{v} + \overline{w}) = \lambda\overline{v} + \lambda\overline{w}$;
- $\forall \overline{v} \in V : 1 \cdot \overline{v} = \overline{v}$.

Определение 2. Линейное отображение — функция $f : U \to W$ (между векторными пространствами), такая, что $f(\lambda\overline{u} + \mu\overline{v}) = \lambda f(\overline{u}) + \mu f(\overline{v})$ для всех $\overline{u}, \overline{v} \in U$.

Определение 3. Изоморфизм пространств — биективное линейное отображение.

Определение 4. Одномерное пространство — пространство V, такое, что в нём есть $\overline{v} \neq \overline{0}$ и $\forall \overline{u} \in V \exists \lambda : \lambda\overline{v} = \overline{u}$.

Определение 5. Двумерное пространство — пространство V, такое, что в нём есть непропорциональные $\overline{v}$ и $\overline{w}$, и $\forall \overline{u} \in V \exists \lambda, \mu \in \mathbb{F} : \overline{u} = \lambda\overline{v} + \mu\overline{w}$.

Определение 6. Определитель двумерной матрицы — выражение

$$\det\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = \det\left(\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}\right) = a_1b_2 - a_2b_1.$$

Лемма 1. Определитель билинеен и кососимметричен (т.е. $\det(\overline{v_1}, \overline{v_2}) = -\det(\overline{v_2}, \overline{v_1})$).

Теорема 2 (Крамер). Векторы $\overline{v_1}, \overline{v_2}$ образуют в $\mathbb{F}^2$ базис тогда и только тогда, когда $\det(\overline{v_1}, \overline{v_2}) \neq 0$. В этом случае для любого вектора $\overline{u} \in \mathbb{F}^2$ выполняется

$$\overline{u} = \frac{\det(\overline{u}, \overline{v_2})}{\det(\overline{v_1}, \overline{v_2})}\overline{v_1} + \frac{\det(\overline{v_1}, \overline{u})}{\det(\overline{v_1}, \overline{v_2})}\overline{v_2}.$$

Определение 7. Площадь ориентированного параллелограмма — функция $S : V \times V \to \mathbb{F}$, обладающая следующими свойствами:

- $S(\overline{a}, \overline{b}) = S(\overline{a}, \overline{b} + \lambda\overline{a}) = S(\overline{a} + \mu\overline{b}, \overline{b})$;
- $S(\lambda\overline{a}, \overline{b}) = \lambda S(\overline{a}, \overline{b}) = S(\overline{a}, \lambda\overline{b})$.

Теорема 3. На любом двумерном V существует ровно одна функция S с точностью до пропорциональности.

Доказательство. С одной стороны, $f(\overline{a}, \overline{b}) = \det\left(\overline{a}, \overline{b}\right)$ подходит. Пусть $\overline{u}, \overline{v}$ — базис на V и $c = S(\overline{u}, \overline{v})$. Рассмотрим $S(\overline{a}, \overline{b})$:

$$S(\overline{a}, \overline{b}) = S(x_1\overline{u} + y_1\overline{v}, x_2\overline{u} + y_2\overline{v}) = S(\overline{u}, \overline{v}) \cdot (x_1y_2 - x_2y_1) = c \cdot \det\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}. \blacksquare$$

Определение 8. Аффинное пространство — множество $\mathbb{A}$ (элементы которого называются «точками») такое, что $\forall a, b \in \mathbb{A} \exists \overline{ab} \in V$ со следующими свойствами:

- $\forall p \in \mathbb{A}$ верно, что $f : \mathbb{A} \to V, q \mapsto \overline{pq}$ биективно;
- $\forall a, b, c \in \mathbb{A} : \overline{ab} + \overline{bc} = \overline{ac}$.

Определение 9. Центр тяжести набора точек — точка c, такая, что $\sum_i \mu_i \overline{cp_i} = 0$, где p_i — точки набора, а $\mu_i \in \mathbb{F}$ — веса этих точек.

Теорема 4. Если $\sum \mu_i \neq 0$, то центр тяжести существует и единственен.

Лемма 5. Пусть есть системы точек (p_i, λ_i) и (q_i, μ_i), при этом $\sum \lambda_i \neq 0, \sum \mu_i \neq 0$. Пусть P, Q — центры тяжести этих систем. Тогда центр тяжести объединения этих систем совпадает с центром тяжести системы $\{(P, \sum \lambda_i), (Q, \sum \mu_i)\}$.

Определение 10. Коллинеарные точки — три элемента $a, b, p \in \mathbb{A}$ такие, что $\overline{pa} \sim \overline{pb}$.

Определение 11. Аффинная прямая — множество таких p, что a, b, p коллинеарны для фиксированных a, b.

Определение 12. Координатный репер — тройка $(O \in \mathbb{A}, \overline{v}, \overline{w})$ такая, что $\overline{v} \not\sim \overline{w}$. Если $Y = O + \lambda \overline{v} + \mu \overline{w}$, то пара (λ, μ) называется координатами Y в этом репере.

Определение 13. Треугольник — тройка неколлинеарных точек из $\mathbb{A}^2$.

Определение 14. Площадь треугольника — функция $S(a,b,c) = \frac{1}{2} S(\overline{ab}, \overline{ac})$, где $S(\overline{u}, \overline{v})$ — площадь параллелограмма.

Лемма 6. Для любых точек $p, a, b, c \in \mathbb{A}^2$ таких, что a, b, c неколлинеарны, выполняется $S(abc) = S(pab) + S(pbc) + S(pca)$.

Определение 15. Барицентрические координаты — набор весов α, β, γ такой, что $\alpha + \beta + \gamma = 1$ и $p = a\alpha + b\beta + c\gamma$ (где p — точка, координаты которой мы ищем).

Лемма 7. Координаты точки p равны $\alpha = \frac{S(pbc)}{S(abc)}, \beta = \frac{S(pca)}{S(abc)}, \gamma = \frac{S(pab)}{S(abc)}$.

Аффинные преобразования

Определение 16. Полуаффинное преобразование — биекция $f : \mathbb{A}^2 \to \mathbb{A}^2$, переводящая прямые в прямые.

Определение 17. Дифференциал полуаффинного преобразования — функция $D_f : V \to V, \overline{ab} \mapsto \overline{f(a)f(b)}$.

Свойства

- f сохраняет параллельность и переводит параллелограммы в параллелограммы.
- Дифференциал определён корректно, кроме того, $D_f(\overline{v}) + D_f(\overline{w}) = D_f(\overline{v} + \overline{w})$.
- $D_f(\lambda \overline{v})$ пропорционален $D_F(\overline{v})$.

Обозначим за $\psi_v(\lambda)$ такую функцию $\mathbb{F} \to \mathbb{F}$, что $D_f(\lambda \overline{v}) = \psi_v(\lambda) D_f(\overline{v})$.

Лемма 8. ψ_v не зависит от v (дальше мы будем обозначать эту функцию ψ).

Лемма 9. ψ является автоморфизмом $\mathbb{F}$.

Лемма 10. Полуаффинное преобразование однозначно задаётся $f(o)$ и $D_f(\overline{v})$, а дифференциал полулинеен, т.е. $\exists \psi : \mathbb{F} \to \mathbb{F}; D_f(\lambda \overline{u} + \mu \overline{v}) = \psi(\lambda) f(\overline{u}) + \psi(\mu) f(\overline{v})$.

Рассмотрим в $\mathbb{F}$ простое подполе (множество элементов вида $\frac{1 \pm 1 \pm \ldots \pm 1}{1 \pm 1 \pm \ldots \pm 1}$). Очевидно, что на нём автоморфизм — это тождественное преобразование. Тогда если $\mathbb{F}$ само простое (т.е. $\mathbb{Q}$ или $\mathbb{Z}/\mathbb{Z}p$), то $\psi(x) = x$. Кроме того, из непрерывности $\mathbb{R}$ получается то же самое для $\mathbb{R}$. Почему это так: $x \in \mathbb{R} > 0 \iff \exists y : x = y^2$, поэтому ψ будет монотонной, а ещё $\psi(t) = t \forall t \ \in \mathbb{Q}$.

Теорема 11 (по анализу). $\psi(x) : \mathbb{R} \to \mathbb{R}$ возрастает, и $\psi(x) = x \forall x \in \mathbb{Q}$. Тогда $\psi(x) = x \forall x$.

Определение 18. Аффинное преобразование — функция $f : \mathbb{A}(U) \to \mathbb{A}(W)$ (между аффинными пространствами над векторными пространствами U, W), такая, что существует линейное отображение $D_f : U \to V$ такое, что $\forall p \in \mathbb{A}(U) : f(p) = f(o) + D_f(\overline{op})$ для некоторой фиксированной точки $o \in \mathbb{A}(U)$.

Лемма 12. В качестве o можно выбрать любую точку в $\mathbb{A}(U)$, и D_f не зависит от выбора.

Лемма 13. Отображение $f : \mathbb{A}(U) \to \mathbb{A}(V)$ аффинно тогда и только тогда, когда

$$\forall p_1, \ldots, p_n \in \mathbb{A}(U), \mu_1, \ldots, \mu_n \in \mathbb{F} : f(\mu_1 p_1 + \ldots + \mu_n p_n) = \mu_1 f(p_1) + \ldots + \mu_n f(p_n).$$

Лемма 14. Аффинное преобразование $f : \mathbb{A}(U) \to \mathbb{A}(V)$ однозначно задаётся значениями $f(o)$ и $D_f(e_i)$, где $o \in \mathbb{A}(U)$ и $\{e_i\}$ — базис в $\mathbb{U}$.

Лемма 15. Для любого $\triangle abc \in \mathbb{A}(U)$ и любых точек $x, y, z \in \mathbb{A}(V)$ существует единственное аффинное преобразование, переводящее a, b, c в x, y, z соответственно.

Определение 19. Произведение матриц — такая матрица $C = A \times B$, что $c_{i,j} = \sum_k a_{i,k} b_{k,j}$. В частности, произведение строки $(a_1, \ldots, a_n)$ на столбец $(b_1, \ldots, b_n)$ равно $\sum_i a_i b_i$.

Пусть V, W двумерные, $f : V \to W$ линейно, $f\binom{1}{0} = f\binom{a_{11}}{a_{21}}$ и $f\binom{0}{1} = f\binom{a_{12}}{a_{22}}$. Тогда

$$f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{22} \\ a_{21} & a_{22} \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Значит, все линейные отображения имеют вид $\overline{x} \mapsto A\overline{x}$, где столбцы A — это координаты $f(e_k)$ (по крайней мере для двумерных пространств, но для n-мерных это тоже верно).

Лемма 16. Любые 3 различные конкурентные прямые в $\mathbb{A}(U)$ можно перевести в любые 3 различные конкурентные прямые в $\mathbb{A}(V)$ ровно одним аффинным преобразованием с точностью до гомотетии в точке пересечения прямых.

Пусть у нас 4 конкурентные прямые, пересекающиеся в точке O, и с направляющими векторами $e_1, e_2, e_1 + e_2, e_2 + te_1$ (с концами в точках P_1, P_2, P_3, P_4), где $t \in \mathbb{F} \cup \infty$ (при значениях $\infty, 0, 1$ получаются соответственно первая, вторая и третья прямые). Тогда если преобразование из прошлой задачи перевело первые 3 прямые в m_1, m_2, m_3, то 4-ю прямую оно переведёт в m_4 с таким же значением t.

Лемма 17. В предыдущем рассуждении выполняется

$$t = \frac{S(\overline{OP_1}, \overline{OP_3}) S(\overline{OP_2}, \overline{OP_4})}{S(\overline{OP_1}, \overline{OP_4}) S(\overline{OP_2}, \overline{OP_3})}.$$

Определение 20. Двойное отношение четвёрки прямых — t из леммы. Обозначение: $(l_1 : l_2 : l_3 : l_4)$.

Как меняется площадь при аффинном преобразовании. Можно считать, что f линейно, т.к. аффинное преобразование — композиция линейного и сдвига. Пусть $S(\overline{u}, \overline{v})$ — ненулевая функция площади. Тогда $S_f(\overline{u}, \overline{v}) := S(f(\overline{u}), f(\overline{v}))$ — тоже функция площади (т.к. $S_f(\lambda\overline{u}, \overline{v}) = \lambda S_f(\overline{u}, \overline{v})$ и $S_f(\overline{u} + \lambda\overline{v}, \overline{v}) = S_f(\overline{u}, \overline{v})$). Значит, площадь при аффинном преобразовании умножается на какую-то константу.

Определение 21. Определитель линейного преобразования — такое число $\det(f)$, что $S(f(\overline{u}), f(\overline{v})) = \det(f) S(\overline{u}, \overline{v})$ (это число равно определителю матрицы отображения f).

Заметим, что композиция двух линейных отображений (в одном и том же векторном пространстве) линейна, и биективные линейные отображения обратимы. Значит, биективные линейные отображения образуют группу. Эту группу будем обозначать $GL(V)$. Кроме того, то же верно и для аффинных отображений, эту группу будем обозначать $Aff(V)$.

Обозначим $\tau_{\overline{v}}$ — параллельный перенос на вектор $\overline{v}$. Пусть F аффинно. Тогда

$$F \circ \tau_{\overline{v}}(p) = F(p + \overline{v}) = F(p) + D_F(\overline{v}) \implies F \circ \tau_{\overline{v}} \circ F^{-1} = \tau_{D_F(\overline{v})}.$$

Лемма 18. Подгруппа $Aff(V)$ из преобразований с фиксированной неподвижной точкой изоморфна $GL(V)$.

Лемма 19. $Aff(V)$ изоморфна $GL(V) \times V$, и композиция двух преобразований из $Aff(V)$ вычисляется следующим способом (это полупрямое произведение):

$$(v, F) \circ (w, G) = (v + F(w), F \circ G).$$

Длины

В этом разделе мы предполагаем, что $\mathbb{F} = \mathbb{R}$.

Определение 22. Скалярное произведение — функция $V \times V \to \mathbb{R}$, обладающая следующими свойствами:

- Билинейность: $(ax + by, cz + dt) = ac(x, z) + ad(y, t) + bc(y, z) + bd(y, t)$ (здесь x, y, z, t — вектора, а $a, b, c, d \in \mathbb{R}$);
- Симметричность: $(v, w) = (w, v)$;
- Положительность: $(v, v) > 0$ при $v \neq 0$.

Определение 23. Евклидова структура — векторное пространство со скалярным произведением.

Определение 24. Длина вектора — число $|v| = \sqrt{(v, v)}$.

Определение 25. Перпендикулярные вектора — два вектора v, w такие, что $(v, w) = 0$.

Примеры таких структур

- Стандартная евклидова структура: $V = \mathbb{R}^n$ и $\overline{x} \cdot \overline{y} = \sum x_i y_i$.
- Непрерывные функции $[0, 1] \to \mathbb{R}$, и скалярное произведение равно $f \cdot g = \int_0^1 f(x)g(x)dx$.

Теорема 20 (Пифагор). $a \perp b$ тогда и только тогда, когда $|a + b|^2 = |a|^2 + |b|^2$.

Лемма 21. $\forall \overline{a} \neq 0, \overline{b}\ \exists! b_a, b_{a\perp}$ со следующими свойствами:

- $b = b_a + b_{a\perp}$;
- $b_a = \lambda a$;
- $b_{a\perp} \perp a$.

Теорема 22 (Неравенство Коши-Буняковского-Шварца). $\forall a, b : (a, b)^2 \leqslant (a, a)(b, b)$, и равенство тогда и только тогда, когда $\lambda a + \mu b = 0$.

Доказательство. Если $a = 0$, то утверждение тривиально. Пусть $a \neq 0$. Тогда $(b_{a\perp}, b_{a\perp}) \geqslant 0$ и равенство тогда и только тогда, когда a и b пропорциональны. Тогда

$$0 \leqslant (b_{a\perp}, b_{a\perp}) = \left(b - a\frac{(a, b)}{(a, a)}, b - a\frac{(a, b)}{(a, a)}\right) = (b, b) - (b, a)\frac{(a, b)}{(a, a)} = \frac{(a, a)(b, b) - (a, b)^2}{(a, a)},$$

откуда и следует утверждение. ■

Лемма 23 (Неравенство треугольника). $|a + b| \leqslant |a| + |b|$ и равенство, только если $\lambda a + \mu b = 0$, где $\lambda\mu \leqslant 0$.

Доказательство. Возведём в квадрат: $(a+b, a+b) \overset{?}{\leqslant} (a, a)+(b, b)+2|a||b|$. Это равносильно тому, что $(a, b) \leqslant |a||b|$, что верно при $(a, b) < 0$ и равносильно **Т. 22** в противном случае. ■

Определение 26. Ортонормальный базис — базис (e_1, e_2) т.ч. $(e_1, e_2) = 0$ и $|e_1| = |e_2| = 1$.

Лемма 24. Ортонормальный базис всегда существует.

Доказательство. Пусть (a, b) — базис. Рассмотрим $e_1 = \frac{a}{|a|}$ и $e_2 = \frac{b_{a\perp}}{|b_{a\perp}|}$. Они подходят. ■

Определение 27. Матрица Грама — матрица $G_u = \binom{u_1}{u_2}(u_1, u_2) = \begin{pmatrix} (u_1,u_1) & (u_1,u_2) \\ (u_2,u_1) & (u_2,u_2) \end{pmatrix}$.

Лемма 25. Пусть $\overline{x} = (x_1, x_2)\binom{u_1}{u_2}, \overline{y} = (u_1, u_2)\binom{y_1}{y_2}$. Тогда $(\overline{x}, \overline{y}) = (x_1, x_2)G_u\binom{y_1}{y_2}$.

Рассмотрим аффинное пространство $\mathbb{A}$, ассоциированное с V.

Определение 28. Отрезок — множество таких $x \in \mathbb{A}$, что $|x - a| + |b - x| = |b - a|$.

Лемма 26. Пусть $(u_1, u_2) = (e_1, e_2)G_u$. Тогда $s^2(u_1, u_2) = s^2(e_1, e_2) \det G_u$.

Лемма 27. Если (e_1, e_2) и (e_1', e_2') — два ортонормальных базиса, то $s(e_1, e_2) = \pm s(e_1', e_2')$.

Из **Т. 27** следует, что есть два типа ортонормальных базисов: «положительно ориентированные» и «отрицательно ориентированные».

Пусть (e_1, e_2) положительно ориентированный и $u = x_1e_1 + x_2e_2$. Тогда $|u| = 1 \iff x_1^2 + y_1^2 = 1$. Значит, $\exists! t \in [0, 2\pi k) : u = \cos t \cdot e_1 + \sin t \cdot e_2$. Это t называется *углом между* e_1 *и* u.

Лемма 28. Если $|u| = 1$, то $(e_1, u) = \cos\angle(e_1, u)$ и $s(e_1, u) = \sin\angle(e_1, u)$.

Лемма 29. Для любых a, b выполняется $\cos\angle(a, b) = \frac{(a,b)}{|a||b|}$ и $\sin\angle(a, b) = \frac{s(a,b)}{|a||b|}$.

Тригонометрия. Пусть $(e, e^\perp)$ — ортонормальный базис, $|f| = |g| = 1$. Заметим, что если $f = xe + ye^\perp$, то $f^\perp = xe^\perp - ye$. Тогда

$$(e, e^\perp)\begin{pmatrix}\cos\angle(e, g)\\ \sin\angle(e, g)\end{pmatrix} = g = (f, f^\perp)\begin{pmatrix}\cos\angle(f, g)\\ \sin\angle(f, g)\end{pmatrix} = (e, e^\perp)\begin{pmatrix}\cos\angle(e, f), -\sin\angle(e, f)\\ \sin\angle(e, f), \cos\angle(e, f)\end{pmatrix}\begin{pmatrix}\cos\angle(f, g)\\ \sin\angle(f, g)\end{pmatrix}.$$

Отсюда можно вывести формулы для $\sin(a + b)$ и $\cos(a + b)$.

Движения

Определение 29. Движение — отображение $f : \mathbb{A}(V) \to \mathbb{A}(V)$ евклидовой плоскости такое, что $|f(a), f(b)| = |a, b|$.

Свойства

- Любое движение переводит прямые в прямые.
- Любое движение биективно, а значит, аффинно.
- Движения сохраняют скалярное произведение.

Как мы знаем, любое движение — композиция движения с неподвижной точкой O и параллельного переноса (см. **Т. 19**). Попытаемся понять, как устроены линейные движения (они образуют группу, которая обозначается $O(V)$). При движении ортонормальный базис (e_1, e_2) переходит в ортонормальный базис $(f(e_1), f(e_2))$. Будем считать, что $s(e_1, e_2) = 1$, тогда $s(f(e_1), f(e_2)) = \pm 1$. Если $s(f(e_1), f(e_2)) = 1$, то движение называется собственным (они образуют группу, которая обозначается $SO(V)$), иначе несобственным.

Лемма 30. Любое собственное движение, сохраняющее точку O, является поворотом вокруг O, а несобственное — отражением относительно прямой, проходящей через O.

Будем обозначать τ_v — сдвиг на вектор v, $\rho_{O,\varphi}$ — поворот вокруг O на угол φ, σ_ℓ — симметрия относительно прямой ℓ.

Лемма 31. Композиция $\tau_v \circ \rho_{O,\varphi}$ — собственное движение.

Доказательство. Если $\varphi = 0$, то это очевидно. Пусть $\varphi \neq 0$. Построим p, q так, что $\overline{pq} = v$ виден из O под углом φ. Тогда эта композиция будет поворотом $\rho_{p,\varphi}$. ■

Определение 30. Скользящая симметрия — композиция $\tau_v \circ \sigma_\ell$ такая, что $\ell \perp v$ (преобразование однозначно определяет ℓ, т.к. это ГИТ $\frac{1}{2}(x + f(x))$).

Лемма 32. Любое несобственное движение является скользящей симметрией. Иными словами, даже если v, ℓ не перпендикулярны, $\tau_v \circ \sigma_\ell$ — скользящая симметрия.

Доказательство. Докажем, что $\tau_v \circ \sigma_\ell = \tau_w \circ \sigma_{\tau_{v/2}(\ell)})$, где w — ортогональная проекция v на ℓ. Это так, потому что можно взять репер (O, e_1, e_2) для $O \in \ell$ и $e_1 \parallel \ell$ и на нём эти два преобразования одинаковы. ■

Теорема 33 (Шаль). Любое собственное движение евклидовой плоскости является сдвигом или поворотом, а любое несобственное — скользящей симметрией.

Определение 31. Преобразование подобия — отображение $f : \mathbb{A}(V) \to \mathbb{A}(V)$ евклидовой плоскости, если $\exists\gamma\forall a, b : |f(a), f(b)| = \gamma|a, b|$. γ называется коэффициентом подобия.

Пусть V — векторное пространство над $\mathbb{F}$.

Определение 32. Порождающий набор векторов — такой набор векторов $w_1, \ldots, w_n \in V$, что для любого $v \in V$ выполняется $v = \sum w_i \lambda_i$ для какого-то набора $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$.

Определение 33. Линейно независимый набор векторов — такой набор векторов $w_1, \ldots, w_n$, что из равенства $\sum_i w_i \lambda_i = 0$ следует, что $\lambda_i = 0\ \forall i$.

Определение 34. Базис — порождающий линейно независимый набор векторов.

Лемма 34 (о замене). Пусть $w_1, \ldots, w_n$ порождающий, а $u_1, \ldots, u_k$ линейно независимы. Тогда $m \geqslant k$; векторы w_i можно перенумеровать так, что $u_1, \ldots, u_k, w_{k+1}, \ldots, w_m$ порождают V.

Доказательство. Мы знаем, что $u_1 = \sum \lambda_k w_k \neq 0$ и есть $\lambda_i \neq 0$. Тогда можно перенумеровать w_i так, чтобы $\lambda_1 \neq 0$, и заменить w_1 на $\lambda_1^{-1}(u_1 - \lambda_2 v_2 - \ldots - \lambda_m w_m)$, тогда набор $u_1, w_2, \ldots, w_m$ тоже будет порождающим.

Теперь пусть $u_1, \ldots, u_i, w_{i+1}, \ldots, w_m$ порождающий и $i < k$. Тогда $u_{i+1} = \sum u_k \mu_k + \sum w_k \lambda_k$. У нас существует $\lambda_i \neq 0$, т.к. u_i линейно независимы. Индукция по i. ■

Лемма 35 (о базисе). Если существует какой-то конечный порождающий набор, то в любом порождающем наборе есть базис, любой линейно независимый набор можно дополнить до базиса, и в каждом базисе одинаковое количество векторов.

Доказательство. Первое утверждение очевидно: если порождающий набор линейно зависим, то один из его векторов можно убрать и получить меньший порождающий набор. Через конечное количество шагов получим базис.

Последнее утверждение следует из **Т. 34**: возьмём в качестве u_i один базис, а в качестве w_i другой базис, тогда в первом из них элементов не меньше, чем во втором.

Второе утверждение тоже следует из **Т. 34** очевидным образом. ■

Определение 35. Размерность пространства — количество векторов в его базисе.

Теорема 36. В конечном поле $\mathbb{F}$ всегда p^n элементов, где p — простое.

Доказательство. Рассмотрим $\mathbb{A} \subset \mathbb{F}$ — простое подполе. Оно изоморфно $\mathbb{Z}/\mathbb{Z}p$ для какого-то p. Заметим, что $\mathbb{F}$ — векторное пространство из $\mathbb{A}$. Тогда по **Т. 35** получится, что в этом поле p^n элементов, где $n = \dim \mathbb{F}$. ■

Определение 36. Векторное подпространство — такое подмножество $U \subset V$, что $\forall u, v \in U : u + v \in U$ и $\forall u \in U, \lambda \in \mathbb{F} : u\lambda \in U$.

Лемма 37. Если $\dim V < \infty$ и U — подпространство, то $\dim U \leqslant \dim V$.

Лемма 38. Если $U, W, U \cup W$ — подпространства, то $U \subset W$ или $W \subset U$.

Определение 37. Сумма подпространств — множество $U + W = \{u + w \mid u \in U, w \in W\}$.

Теорема 39. Пусть $U, W \subset V$ — конечномерные подпространства. Тогда

$$\dim(U + V) = \dim U + \dim V - \dim U \cap W.$$

Доказательство. Пусть $e_1, \ldots, e_k$ — базис в $U \cap W$. Рассмотрим базисы $e_1, \ldots, e_k, u_1, \ldots, u_n$ в U и $e_1, \ldots, e_k, w_1, \ldots, w_m$ в W. Докажем, что $e_1, \ldots, e_K, u_1, \ldots, u_n, w_1, \ldots, w_m$ — базис в $U + W$. Очевидно, что это порождающий набор. Пусть какая-то линейная комбинация равна 0, т.е.

$$\lambda_1 e_1 + \ldots + \lambda_k e_k + \nu_1 u_1 + \ldots + \nu_n u_n = \mu_1 w_1 + \ldots + \mu_m w_m.$$

Заметим, что левая часть этой суммы лежит в U, а правая в W. Значит, каждая из этих частей лежит в $U \cap W$. Тогда левая часть выражается единственным образом и в $U \cap W$, и в U, т.е. $\nu_i = 0$. Аналогично $\mu_i = 0$. Тогда $\sum \lambda_i e_i = 0$, т.е. $\lambda_i = 0$. ■

Определение 38. Трансверсальные подпространства — подпространства U, W такие, что $U \cap W = \{0\}$.

Лемма 40. Пусть $K = U_1 + \ldots + U_k$, причем для любого $k \in K$ представление $k = \sum u_i$ единственно. Это выполняется тогда и только тогда, когда $\forall i : U_i$ трансверсально $\sum_{j \neq i} U_j$.

Теорема 41 (Полиномиальная интерполяция с кратными узлами). Пусть заданы числа $\alpha_1, \dots \alpha_n \in \mathbb{F}$ и для каждого i заданы $m_i + 1$ значений: $\beta_{i,0}, \dots, \beta_{i,m_i} \in \mathbb{F}$. Пусть $N = \sum_i (m_i + 1)$. Тогда существует единственный многочлен $P \in \mathbb{F}[x]$ степени меньше N такой, что $f^{(k)}(\alpha_i) = \beta_{i,k}$ для всех i, k.

Доказательство. Обозначим $S = \mathbb{F}[x]_{\deg P < N}$ и рассмотрим это как векторное пространство над $\mathbb{F}$. Заметим, что $\dim S = N$, и кроме того, отображение

$$H : S \to \mathbb{F}^n, f \mapsto (f(\alpha_1), f'(\alpha_1), \dots, f^{(m_1)}(\alpha_1), \dots, f^{(m_n)}(\alpha_n))$$

линейно. Рассмотрим $\ker H$. Если $H(f) = 0$, то f делится на $g = (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_n)^{m_n}$, но степени многочленов в S меньше степени g, т.е. $f = 0$. Кроме того, размерности S и $\mathbb{F}^N$ совпадают. Значит, H — изоморфизм. Тогда для любого набора α_i и $\beta_{i,j}$ существует единственный f такой, что $H(f) = (\beta_{1,0}, \dots, \beta_{n,m_n})$. ■

Теорема 42. Пусть $f : V \to W$ линейно и $\dim V < \infty$. Тогда $\dim V = \dim \operatorname{Im} f + \dim \ker f$.

Доказательство. Пусть $e_1, \dots, e_k$ — базис в $\ker f$. Дополним его до базиса в V, т.е. $e_1, \dots, e_k, u_1, \dots, u$ — базис в V. Докажем, что $f(u_1), \dots, f(u_m)$ — базис в $\operatorname{Im} f$. Действительно, для любого $v \in V$ существует единственное представление $v = \sum \lambda_i e_i + \sum \mu_i u_i$, тогда $f(v) = f(\sum \lambda_i e_i) + \sum \mu_i f(u_i)$, причём левое слагаемое равно 0 (т.к. $\sum \lambda_i e_i \in \ker f$), значит, набор μ_i тоже единственный. ■

Лемма 43. Для линейного оператора $f : V \to V$ следующие условия равносильны:

- f инъекция (т.е. $\ker f = \{0\}$);
- f сюръекция (т.е. $\operatorname{Im} f = V$);
- f биекция.

Определение 39. Аффинное подпространство — множество $p + U = \{p + u \mid u \in U\}$, где U — векторное подпространство. По определению, $\dim(p + U) = \dim U$.

Лемма 44. $(p + U) \cap (q + W) \neq \emptyset \iff \overline{pq} \in U + W$. В этом случае $(p + U) \cap (q + W)$ — аффинное подпространство с направляющим векторным пространством $U \cap W$.