СОДЕРЖАНИЕ

Глава 6

Многочлены

6.1 Кольцо многочленов

Пусть k — некоторое фиксированное поле.

Определение 6.1.1. Многочленом от неизвестного x над кольцом k называется формальное выражение вида

$$\sum_{i=0}^{\infty} \alpha_i x^i,$$

где x — символ неизвестного, α_i — элементы поля k, почти все равные 0, то есть $(\exists\ n \in \mathbb{N})\ (\forall\ i > n) \quad \alpha_i = 0$.

В дальнейшем многочлены будем обозначать $f(x)$, $g(x)$, $h(x)$, $f_1(x)$, $f_2(x)$,... или короче f, g, h, f_1, f_2,...

$$f(x) = \sum_{i=0}^{\infty} \alpha_i x^i. \tag{6.1}$$

Если в многочлене (6.1) $\forall\ 0 \leqslant i < \infty \quad \alpha_i = 0$, то многочлен будем называть нулевым и обозначать 0.

Определение 6.1.2. Слагаемые $\alpha_i x^i$ будем называть членами многочлена (6.1), а элементы α_i будем называть коэффициентами многочлена (6.1).

Если в многочлене (6.1) $\forall\ i > n \quad \alpha_i = 0$, то будем писать:

$$f(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{или} \quad f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n. \tag{6.2}$$

Здесь при переходе от записи (6.1) к записи (6.2) мы пишем α_0 вместо $\alpha_0 x^0$. При этом α_0 называется свободным членом многочлена $f(x)$.

Определение 6.1.3. Степенью ненулевого многочлена $f(x)$ называется наибольший номер отличного от нуля коэффициента этого многочлена.

Обозначим через $\deg f(x)$ степень многочлена $f(x)$.

Если в записи (6.2) $\alpha_n \neq 0$, то степень многочлена $f(x)$ равна n, то есть $\deg f(x) = n$. В этом случае, $\alpha_n x^n$ называется старшим членом многочлена, α_n называется старшим коэффициентом многочлена.

Множество всех многочленов от неизвестного x над полем k обозначается $k[x]$ и называется кольцом многочленов над полем k.

Пусть

$$f(x) = \sum_{i=0}^{\infty} \alpha_i x^i,\ g(x) = \sum_{i=0}^{\infty} \beta_i x^i, \quad f, g \in k[x].$$

Определение 6.1.4. Два многочлена $f(x), g(x) \in k[x]$ называются равными, если равны все их коэффициенты при одинаковых степенях x, то есть $(\forall\ 0 \leqslant i < \infty) \quad \alpha_i = \beta_i$.

В множестве $k[x]$ введем две операции: сложения и умножения многочленов.

Определение 6.1.5. Суммой двух многочленов f и g называется многочлен

$$f + g = \sum_{i=0}^{\infty} (\alpha_i + \beta_i) x^i.$$

Произведением двух многочленов f и g называется многочлен

$$f \cdot g = \sum_{i=0}^{\infty} \gamma_i x^i, \quad \text{где} \quad \gamma_i = \sum_{\substack{\nu+\mu=i \\ \nu,\mu \geqslant 0}} \alpha_\nu \beta_\mu.$$

Замечание 6.1.1. Формула для умножения означает, что для того, чтобы перемножить два многочлена, достаточно каждый член первого многочлена умножить на каждый член второго многочлена и привести подобные члены.

Определение 6.1.5 корректно в том смысле, что $f+g$ и $f\cdot g$ действительно будут многочленами. Так как f и g — многочлены, то $(\exists\ n\in \in \mathbb{N})\ (\forall\ i>n)\quad \alpha_i=0,\ \beta_i=0$. Тогда $(\forall\ i>n)\quad \alpha_i+\beta_i=0\Rightarrow f+g$ является многочленом.

Для $f\cdot g$ подсчитаем $\gamma_i, \forall\ i>2n$. Так как $i=\nu+\mu$, то из условия $i>2n\Rightarrow \nu>n$ или $\mu>n\Rightarrow \alpha_\nu=0$ или $\beta_\mu=0\Rightarrow \gamma_i=\sum \alpha_\nu\beta_\mu=0$ для $i>2n$. А это означает, что $f\cdot g$ является многочленом.

Рассмотрим вопрос о степени суммы и произведения двух многочленов.

Пусть $f\neq 0$ и $g\neq 0$ — многочлены из $k[x]$,

$$f(x)=\sum_{i=0}^{\infty}\alpha_i x^i,\quad g(x)=\sum_{i=0}^{\infty}\beta_i x^i.$$

Пусть $\deg f=n$, то есть $\alpha_n\neq 0,\ \deg g=m$, то есть $\beta_m\neq 0$. Обозначим через $N=\max(n,m)$.

Рассмотрим

$$f+g=\sum_{i=0}^{\infty}(\alpha_i+\beta_i)x^i.$$

Ясно, что $(\forall\ i>N)\quad \alpha_i=0$ и $\beta_i=0\Rightarrow \gamma_i=\alpha_i+\beta_i=0$. Следовательно, $\deg(f+g)\leqslant N$. Значит, $\underline{\deg(f+g)\leqslant \max(\deg f,\deg g)}$. Знак равенства достигается, например, при $n\neq m$.

Рассмотрим

$$f\cdot g=\sum_{i=0}^{\infty}\gamma_i x^i\quad \text{где}\quad \gamma_i=\sum_{\substack{\nu+\mu=i\\ \nu,\mu\geqslant 0}}\alpha_\nu\beta_\mu.$$

Если $i>n+m$, то $\nu>n$ или $\mu>m\Rightarrow \alpha_\nu=0$ или $\beta_\mu=0\Rightarrow \gamma_i=0$. Получаем $\deg f\cdot g\leqslant n+m$. Значит, $\deg f\cdot g\leqslant \deg f+\deg g$.

Сосчитаем

$$\gamma_{n+m} = \sum_{\nu+\mu=n+m} \alpha_\nu \beta_\mu = \alpha_n \beta_m.$$

Так как $\alpha_n \neq 0$ и $\beta_m \neq 0$, то $\alpha_n \beta_m \neq 0$. В этом случае $\gamma_{n+m} \neq 0$ и $\deg f \cdot g = \deg f + \deg g$.

6.2 Теорема о делении с остатком. Теорема Безу. Схема Горнера

ТЕОРЕМА 6.2.1 (о делении с остатком). *Пусть k — поле, f и $g \in k[x]$, причем $g \neq 0$. Тогда существует единственная пара многочленов $q, r \in k[x]$ такая, что*

1) $f = gq + r$;

2) $r = 0$ (или $r \neq 0, \deg r < \deg g$).

Доказательство. I) Существование многочленов q и r.
а) Пусть $f = 0$ (или $f \neq 0, \deg f < \deg g$). В этом случае можно записать $f = 0 \cdot g + f, (q = 0,\ r = f)$. Условия 1) и 2) выполнены.
б) $f \neq 0$ и $\deg f \geqslant \deg g$. Пусть

$$f = \alpha_n x^n + \ldots + \alpha_0, \quad \alpha_n \neq 0,$$

$$g = \beta_m x^m + \ldots + \beta_0, \quad \beta_m \neq 0.$$

$\deg f = n,\ \deg g = m,\ n \geqslant m$. Построим многочлен

$$f_1 = f - \alpha_n \beta_m^{-1} x^{n-m} g. \tag{1}$$

Многочлен f_1 построен так, чтобы уничтожить старший член многочлена f. Имеем $f_1 = 0$ или $f_1 \neq 0$ и $\deg f_1 = n_1 < n$.

Если $n_1 < m$, то процесс построения многочленов заканчиваем. Если $n_1 \geqslant m$, то, обозначая через $\alpha_{n_1}^{(1)}$ старший коэффициент f_1, строим многочлен

$$f_2 = f_1 - \alpha_{n_1}^{(1)} \beta_m^{-1} x^{n_1-m} g. \tag{2}$$

Опять многочлен f_2 строится таким образом, чтобы уничтожить старший член многочлена f_1. Имеем $f_2 = 0$ или $f_2 \neq 0$ и $\deg f_2 = n_2 < n_1$.

Если $n_2 < m$, то процесс построения многочленов заканчиваем. Если $n_2 \geqslant m$, то продолжаем и т. д.

Заметим, что степени многочленов f, f_1, f_2, f_3,... образуют строго убывающую последовательность натуральных чисел, тогда в конце концов получим $n > n_1 > n_2 > \ldots > n_s$, где $n_s < m$.

$$f_s = f_{s-1} - \alpha_{n_{s-1}}^{(s-1)} \beta_m^{-1} x^{n_{s-1}-m} g, \qquad (s)$$

где $f_s = 0$ или $f_s \neq 0$ и $\deg f_s = n_s < m$.

Сложим почленно все равенства $(1), (2), \ldots, (s)$, получим

$$f_s = f - \left(\alpha_n \beta_m^{-1} x^{n-m} + \alpha_{n_1}^{(1)} \beta_m^{-1} x^{n_1-m} + \ldots + \alpha_{n_{s-1}}^{(s-1)} \beta_m^{-1} x^{n_{s-1}-m} \right) g.$$

Обозначим f_s через r,а содержимое скобки через q. Получим $r = f_s - qg \Rightarrow f = qg + r$, то есть получили равенство 1), где $\overline{r} = 0 \vee (\overline{r} \neq 0 \wedge \deg \overline{r} < \deg g)$ — условие 2).

II) Единственность q и r.

Допустим, что наряду с парой многочленов q и r, установленных в части I), существует другая пара многочленов $\overline{q}$ и $\overline{r}$, удовлетворяющая условиям 1) и 2), то есть $f = \overline{q}g + \overline{r}$ и $\overline{r} = 0 \vee (\overline{r} \neq 0 \wedge \deg \overline{r} < \deg g)$. Имеем

$$qg + r = \overline{q}g + \overline{r} \Rightarrow (q - \overline{q})g = \overline{r} - r. \qquad (*)$$

Покажем, что $q - \overline{q} = 0$. Допустим противное, то есть $q - \overline{q} \neq 0$. Пусть $\alpha \neq 0$ — старший коэффициент этого многочлена, тогда старший коэффициент многочлена $(q - \overline{q})g$ будет $\alpha\beta_m \neq 0$. Если бы $\alpha\beta_m = 0$, то $\alpha = 0$. Значит $\deg(q - \overline{q})g = \deg(q - \overline{q}) + \deg g \geqslant \deg g$.

С другой стороны $\overline{r} - r = 0$ или $\overline{r} - r \neq 0, \deg(\overline{r} - r) < \deg g$. Мы получили, что в равенстве $(*)$ слева стоит многочлен, степень которого не меньше $\deg g$, а справа стоит нулевой многочлен или многочлен, степень которого меньше $\deg g$. Это и есть противоречие. $\square$

Определение 6.2.1. В обозначениях теоремы 6.2.1 многочлены q и r называются соответственно неполным частным и остатком от деления многочлена f на многочлен g.

ТЕОРЕМА 6.2.2 (Безу). *Остаток от деления многочлена $f(x)$ на $x-\gamma$ равен значению многочлена $f(x)$ при $x=\gamma$, то есть $f(\gamma)$.*

Доказательство. Пусть $f(x)=q(x)(x-\gamma)+r(x), \quad r(x)=0 \vee (r(x)\neq \neq 0 \wedge \deg r(x)<1)$. Получаем $r(x)=0 \vee \deg r(x)=0$, в любом случае $r(x)=r\in k$.

Пусть $q(x)=\beta_0+\beta_1 x+\ldots+\beta_s x^s$, тогда $f(x)=q(x)\cdot x-q(x)\gamma+r= = \beta_0 x+\beta_1 x^2+\ldots+\beta_s x^{s+1}-\beta_0\gamma-\beta_1 x\gamma-\ldots-\beta_s x^s\gamma+r$.

Сосчитаем $f(\gamma)=\beta_0\gamma+\beta_1\gamma^2+\ldots+\beta_s\gamma^{s+1}-\beta_0\gamma-\beta_1\gamma^2-\ldots+\beta_s\gamma^{s+1}+r= = r$. Таким образом, $r=f(\gamma)$. □

Представляет интерес деление многочлена $f(x)$ на $(x-\gamma)$ по так называемой схеме Горнера.

Пусть $f(x)=\alpha_0 x^n+\alpha_1 x^{n-1}+\ldots+\alpha_n, \alpha_0\neq 0$. Разделим $f(x)$ на $(x-\gamma)$ с остатком, получим $f(x)=q(x)(x-\gamma)+r$. Многочлен $q(x)$ будем искать в виде $q(x)=\beta_0 x^{n-1}+\beta_1 x^{n-2}+\ldots+\beta_{n-1}$. Наша задача найти коэффициенты $\beta_0,\beta_1,\ldots,\beta_{n-1}$ и остаток r.

Подставим в это соотношение вместо $q(x)$ и $f(x)$ их значения. Имеем, $\alpha_0 x^n+\alpha_1 x^{n-1}+\ldots+\alpha_n=\left(\beta_0 x^{n-1}+\beta_1 x^{n-2}+\ldots+\beta_{n-1}\right)(x-\gamma)+r$. Два многочлена равны тогда и только тогда, когда равны их коэффициенты при соответствующих степенях. Сравним коэффициенты.

$$
\begin{array}{lll}
x^n: & \alpha_0=\beta_0 & \Rightarrow \ \beta_0=\alpha_0;\\
x^{n-1}: & \alpha_1=\beta_1-\beta_0\gamma & \Rightarrow \ \beta_1=\beta_0\gamma+\alpha_1;\\
x^{n-2}: & \alpha_2=\beta_2-\beta_1\gamma & \Rightarrow \ \beta_2=\beta_1\gamma+\alpha_2;\\
\ldots & & \\
x^1: & \alpha_{n-1}=\beta_{n-1}-\beta_{n-2}\gamma & \Rightarrow \ \beta_{n-1}=\beta_{n-2}\gamma+\alpha_{n-1};\\
x^0: & \alpha_n=r-\beta_{n-1}\gamma & \Rightarrow \ r=\beta_{n-1}\gamma+\alpha_n.
\end{array}
$$

Таким образом видно, что коэффициенты неполного частного и остаток находятся с помощью однотипных вычислений, а именно, чтобы найти $\beta_k = \beta_{k-1}\gamma + \alpha_k$. Эти вычисления удобно записывать в виде следующей схемы Горнера.

	α_0	α_1	α_2	$\dots$	α_{n-1}	α_n
γ	α_0	$\beta_0\gamma + \alpha_1$	$\beta_1\gamma + \alpha_2$	$\dots$	$\beta_{n-2}\gamma + \alpha_{n-1}$	$\beta_{n-1}\gamma + \alpha_n$
	$\|\|$	$\|\|$	$\|\|$		$\|\|$	$\|\|$
	β_0	β_1	β_2	$\dots$	β_{n-1}	$r = f(\gamma)$

Пример: $f(x) = x^5 - 2x^4 + 3x^3 - 4x^2 + x - 1$. Найдем $f(4)$.

	1	-2	3	-4	1	-1
4	1	2	11	40	161	643

$f(4) = 643, \quad f(x) = (x^4 + 2x^3 + 11x^2 + 40x + 161)(x - 4) + 643.$

6.3 Делимость многочленов. Наибольший общий делитель и наименьшее общее кратное

Определение 6.3.1. Говорят, что многочлен $f(x)$ делится на многочлен $g(x) \neq 0$ или, что многочлен $g(x)$ делит многочлен $f(x)$ или, что многочлен $g(x)$ является делителем многочлена $f(x)$ или, что многочлен $f(x)$ кратен многочлену $g(x)$, если существует такой многочлен $q(x)$, что $f(x) = q(x) \cdot g(x)$.

Определение 6.3.2. Говорят, что многочлен $f(x)$ делится на многочлен $g(x) \neq 0$, если остаток от деления $f(x)$ на $g(x)$ равен нулю.

То, что многочлен $g(x)$ делит $f(x)$ обозначается как $g|f$.

Определение 6.3.3. Два ненулевых многочлена $f(x)$ и $g(x)$ называются ассоциированными $f \sim g$, если они отличаются друг от друга множителем равным ненулевой константе, то есть $f = \alpha g$, $\alpha \in k^* = k\backslash\{0\}$.

Свойства делимости

1. $(\forall\ f \neq 0) \quad f|f$.

2. $(\forall\ g \neq 0) \quad g|0$.

3. Два ненулевых многочлена ассоциированы тогда и только тогда, когда они делят друг друга, то есть $f \sim g \Leftrightarrow f|g$ и $g|f$.

4. Если $h|g$, $g|f$, то $h|f$ (транзитивность).

5. Если $h|g$, $h|f$, то $(\forall\ u, v \in k[x]) \quad h|(ug + vf)$.

6. Делителями ненулевых констант могут быть только ненулевые константы, то есть если $g|f$ и $\deg f = 0$, то $\deg g = 0$.

7. Ненулевая константа делит ненулевой многочлен, то есть если $\deg g = 0$, то $(\forall\ f) \quad g|f$.

8. Если $g|f$ и $f \neq 0$, то $\deg g \leqslant \deg f$, причем знак равенства достигается тогда и только тогда, когда $g \sim f$.

9. Отношение делимости, есть отношение между классами ассоциированных многочленов, то есть если $g|f$, $g_1 \sim g$, $f_1 \sim f$, то $g_1|f_1$.

Доказательство. 1) $f(x) = 1 \cdot f(x)$, то есть $f|f$ и $q(x) = 1$.

2) $0 = 0 \cdot g(x)$, то есть $g|0$ и $q(x) = 0$.

3) a) Необходимость.

Пусть $f \sim g$, тогда $f = \alpha g$, где $\alpha \in k^*$, то есть $g|f$ и $q = \alpha$. Так как $\alpha \neq 0$, то $g = \alpha^{-1} f$, то есть $f|g$ и $q = \alpha^{-1}$.

b) Достаточность.

Пусть $g|f$ и $f|g$. Имеем, $f = qg$, $g = q_1 f$, следовательно $f = q(q_1 f)$, то есть $(1 - qq_1)f = 0$. Так как $f \neq 0$, то $1 - qq_1 = 0$, то есть $qq_1 = 1$. Значит $\deg qq_1 = 0 \Rightarrow \deg q + \deg q_1 = 0 \Rightarrow \deg q = \deg q_1 = 0$, следовательно q и q_1 — константы. Имеем $f = qg$, где $q \in k^* \Rightarrow f \sim g$.

4) Имеем $g = qh,\ f = q_1 g$. Тогда $f = q_1(qh) = (q_1 q)h \Rightarrow h|f$.

5) Имеем $g = qh$, $f = q_1 h$. Тогда $ug = uqh$, $vf = vq_1 h$. Рассмотрим $ug + vf = (uq + vq_1)h \Rightarrow h|(ug + vf)$.

6) Имеем $\deg f = 0$ и $f = qg \Rightarrow \deg f = \deg q + \deg g = 0 \Rightarrow \deg q = = \deg g = 0$, то есть q и g — константы.

7) Так как $\deg g = 0$, то $g \in k^*$, поэтому существует $g^{-1} \in k^*$. Тогда $f = (fg^{-1})g \Rightarrow g|f$.

8) Имеем $f = qg \Rightarrow \deg f = \deg g + \deg q \Rightarrow \deg f \geqslant \deg g$. Видно, что знак равенства будет выполняться тогда и только тогда, когда $\deg q = = 0 \Rightarrow q \in k^* \Leftrightarrow f \sim g$.

9) Имеем $f = qg$, $g = \alpha q_1$, $f = \beta f_1$, где $\alpha, \beta \in k^*$. Тогда $\beta f_1 = q\alpha g_1 \Rightarrow \Rightarrow f_1 = (\beta^{-1} q\alpha) g_1 \Rightarrow g_1 | f_1$. □

В дальнейшем будем рассматривать конечную систему многочленов $\{f_1, f_2, \ldots, f_s\}$, среди которых по крайней мере один многочлен отличен от нуля.

Определение 6.3.4. Многочлен d называется общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$, если он делит все многочлены данной системы, то есть $(\forall\ 1 \leqslant i \leqslant s) \quad d|f_i$.

ТЕОРЕМА 6.3.1 (о равносильных условиях, определяющих НОД). *Пусть $\{f_1, f_2, \ldots, f_s\}$ — система многочленов, среди которых по крайней мере один многочлен отличен от нуля, и d — некоторый ненулевой многочлен $(d \neq 0)$. Равносильны следующие два утверждения:*

1) *совокупность делителей многочлена d совпадает с совокупностью общих делителей системы многочленов $\{f_1, f_2, \ldots, f_s\}$;*

2) *многочлен d является общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$, который делится на любой другой общий делитель этой системы.*

Доказательство. 1) $\Rightarrow$ 2)

Так как среди делителей многочлена d находится сам многочлен d, то по условию 1), d является общим делителем $\{f_1, f_2, \ldots, f_s\}$.

Пусть теперь d' — любой общий делитель $\{f_1, f_2, \ldots, f_s\}$, тогда по условию 1) d' совпадает с одним из делителей многочлена d, то есть d делится на d'.

2) $\Rightarrow$ 1)

Выполнение условия 1) установим в два шага.

а) Пусть d' — любой делитель многочлена d. Имеем $d'|d$, а по условию 2) $(\forall\ 1 \leqslant i \leqslant s) \quad d|f_i \Rightarrow (\forall\ 1 \leqslant i \leqslant s) \quad d'|f_i$, то есть d' является общим делителем системы многочленов $\{f_1, f_2, \ldots, f_s\}$.

б) Обратно. Пусть d' — любой общий делитель системы многочленов $\{f_1, f_2, \ldots, f_s\}$. Тогда по условию 2) многочлен d делится на d', то есть d' является делителем многочлена d. □

Определение 6.3.5. Наибольшим общим делителем (НОД) системы многочленов $\{f_1, f_2, \ldots, f_s\}$, называется любой ненулевой многочлен d, удовлетворяющий любому из равносильных условий теоремы 6.3.1.

Определение 6.3.6. НОД системы многочленов называется такой общий делитель этой системы, который делится на любой другой общий делитель этой системы многочленов.

Следствие 6.3.1.1. Если НОД системы многочленов существует, то он определен однозначно с точностью до ассоциированности.

Доказательство. Пусть d_1, d_2 — два НОД системы многочленов $f_1, f_2, \ldots, f_s$, будем рассматривать d_1 как НОД системы, а d_2 как ОД системы $f_1, f_2, \ldots, f_s$. Тогда по определению 6.3.6 $d_2|d_1$. Поменяем ролями d_1 и d_2, то есть d_1 будем рассматривать как ОД, а d_2 — как НОД системы $f_1, f_2, \ldots, f_s$. По определению 6.3.6 $d_1|d_2$, тогда по 3 свойству делимости $d_1 \sim d_2$. □

Возникает естественный вопрос: существует ли НОД системы многочленов $\{f_1, f_2, \ldots, f_s\}$? Ответ на этот вопрос положительный. Убедимся в этом сначала для системы из 2-х многочленов. Мы докажем существование НОД 2-х многочленов и укажем алгоритм его нахождения. Этот алгоритм называется алгоритмом Евклида и он основан на методе последовательного деления. Пусть f и g — два ненулевых многочлена, $\deg f \geqslant \deg g$. Разделим f на g с остатком, получим

$$f = q_1 g + r_1, \quad \text{где} \quad r_1 = 0 \quad \text{или} \quad (r_1 \neq 0 \text{ и } \deg r_1 < \deg g)\,.$$

Если $r_1 = 0$, то процесс деления заканчивается. Если $r_1 \neq 0$, то делим g на r_1 с остатком, получим

$$g = q_2 r_1 + r_2, \quad \text{где} \quad r_2 = 0 \quad \text{или} \quad (r_2 \neq 0 \text{ и } \deg r_2 < \deg r_1)\,.$$

Если $r_2 = 0$, то процесс деления заканчивается. Если $r_2 \neq 0$, то делим r_1 на r_2 с остатком, получим

$$r_1 = q_3 r_2 + r_3, \quad \text{где} \quad r_3 = 0 \quad \text{или} \quad (r_3 \neq 0 \text{ и } \deg r_3 < \deg r_2)\,.$$

И так далее. Возникает вопрос: наш процесс конечен или бесконечен? Заметим, что степени остатков образуют строго убывающую последовательность натуральных чисел, а именно $\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \ldots$, которая не может быть бесконечной. В конце концов получим равенства

$$r_{k-2} = q_k r_{k-1} + r_k;$$

$$r_{k-1} = q_{k+1} r_k,$$

где r_k — последний не равный нулю остаток в алгоритме Евклида.

ТЕОРЕМА 6.3.2. *Наибольший общий делитель 2-х ненулевых многочленов f и g существует и равен последнему не равному нулю остатку в алгоритме Евклида, примененному к многочленам f и g.*

Доказательство. Запишем равенства, определяющие алгоритм Евклида к многочленам f и g

$$f = q_1 g + r_1 \Rightarrow r_1 = f - q_1 g; \tag{1}$$

$$g = q_2 r_1 + r_2 \Rightarrow r_2 = g - q_2 r_1; \tag{2}$$

$$r_1 = q_3 r_2 + r_3 \Rightarrow r_3 = r_1 - q_3 r_2; \tag{3}$$

$$\dots$$

$$r_{k-2} = q_k r_{k-1} + r_k \Rightarrow r_k = r_{k-2} - q_k r_{k-1}; \tag{k}$$

$$r_{k-1} = q_{k+1} r_k. \tag{$k+1$}$$

Из последнего равенства видно, что $r_k | r_{k-1}$.

Из равенства (k) видно, что $r_k | r_{k-2}$.

Из равенства $(k-1)$ видно, что $r_k | r_{k-3}$.

$\dots$

$r_k | r_2,\ r_k | r_1$

Из равенства (2) видно, что $r_k | g$.

Из равенства (1) видно, что $r_k | f$.

Следовательно r_k является общим делителем системы многочленов $\{f, g\}$. Пусть d — любой общий делитель $\{f, g\}$, тогда
из равенства (1) видно, что $d | r_1$,
из равенства (2) видно, что $d | r_2$,
$\dots$
из равенства (k) видно, что $d | r_k$,
то есть r_k — общий делитель $\{f, g\}$, который делится на любой другой общий делитель $\{f, g\}$. Тогда по определению 6.3.6 r_k — НОД $\{f, g\}$. $\square$

Существование НОД любой конечной системы многочленов устанавливается следующей теоремой, которая так же дает метод его нахождения.

ТЕОРЕМА 6.3.3 (рекуррентная формула). *НОД конечной системы многочленов существует и при этом справедливо соотношение*

$$\mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}, f_s\} = \mathcal{HOD}\{\mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}\}, f_s\}.$$

Доказательство. Применим метод математической индукции по s. Если $s = 2$, то утверждение теоремы очевидно. Предположим, что теорема верна для $(s-1)$ многочленов, тем самым предполагается, что существует наибольший общий делитель d системы многочленов $\{f_1, f_2, \ldots, f_{s-1}\}$. Обозначим через $\bar{d} = \mathcal{HOD}\{d, f_s\}$. Имеем, $\bar{d}|d$, $\bar{d}|f_s$, кроме того $(\forall\ 1 \leqslant i \leqslant s-1)\quad d|f_i$, тогда по транзитивности делимости $(\forall\ 1 \leqslant i \leqslant s-1)\quad \bar{d}|f_i$, $\bar{d}|f_s$, следовательно $\bar{d}$ является общим делителем $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. Пусть d' — любой общий делитель $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$, тогда $(\forall\ 1 \leqslant i \leqslant s-1)\quad d'|f_i$ и $d'|f_s$ следовательно d' является общим делителем $\{f_1, f_2, \ldots, f_{s-1}\}$. Тогда по определению 6.3.6 $d'|d$. Таким образом $d'|d$, $d'|f_s$ следовательно d' является общим делителем $\{d, f_s\}$. Тогда из определения 6.3.6 следует $d'|\bar{d}$. Итак $\bar{d}$ является общим делителем $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$ и $\bar{d}$ делится на любой общий делитель $\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. Тогда по определению 6.3.6 $\bar{d} = \mathcal{HOD}\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. □

ТЕОРЕМА 6.3.4 (критерий НОД системы многочленов). *Для того чтобы многочлен d являлся НОД системы многочленов $\{f_1, f_2, \ldots, f_s\}$ необходимо и достаточно, чтобы этот многочлен d был ОД этой системы и чтобы он линейно выражался через эти многочлены, то есть* $(\exists\ u_1, u_2, \ldots, u_s, \in k[x])\quad d = u_1f_1 + u_2f_2 + \ldots + u_sf_s$.

Доказательство. 1) Достаточность.

Пусть d является ОД $\{f_1, f_2, \ldots, f_s\}$ и $\exists\ u_1, u_2, \ldots, u_s \in k[x]\quad d = u_1f_1+u_2f_2+\ldots+u_sf_s$. Пусть d' — любой общий делитель $\{f_1, f_2, \ldots, f_s\}$. Это означает, что $(\forall\ 1 \leqslant i \leqslant s)\quad d'|f_i$. Тогда по 5 свойству делимости $d'|(u_1f_1 + u_2f_2 + \ldots + u_sf_s)$, то есть $d'|d$. По определению 6.3.6

$d = \mathcal{НОД}\{f_1, f_2, \ldots, f_s\}$.

2)Необходимость.

Пусть d является НОД $\{f_1, f_2, \ldots, f_s\}$. Тогда d является ОД $\{f_1, f_2, \ldots, f_s\}$. Остается показать, что d линейно выражается через $f_1, f_2, \ldots, f_s$. Установим этот факт методом математической индукции. Пусть $s = 2$. Обозначим $f_1 = f, f_2 = g$. Запишем равенство, определяющее алгоритм Евклида.

$$f = q_1 g + r_1; \tag{1}$$

$$g = q_2 r_1 + r_2; \tag{2}$$

$$\ldots$$

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}; \tag{$k-1$}$$

$$r_{k-2} = q_k r_{k-1} + r_k; \tag{k}$$

$$r_{k-1} = q_{k+1} r_k. \tag{$k+1$}$$

Известно, что НОД d многочленов $\{f, g\}$ равен r_k. Из равенства (k) видно, что

$$d = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) =$$

$$= (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3} = \ldots = ug + vf.$$

Предположим, что утверждение теоремы справедливо для системы, состоящей из $(s-1)$ многочленов. Докажем ее справедливость для систем, состоящих из s многочленов. По теореме 6.3.3 наибольший общий делитель d системы многочленов $\{f_1, f_2, \ldots, f_s\}$ совпадает с НОД 2-х многочленов $\{d_1, f_s\}$, где d_1 — НОД $\{f_1, \ldots f_{s-1}\}$. По предположению индукции существуют многочлены $v_1, \ldots, v_{s-1} \in k[x]$ такие, что $d_1 = v_1 f_1 + v_2 f_2 + \ldots + v_{s-1} f_{s-1}$. Так как d является НОД $\{d_1, f_s\}$, то существуют многочлены $w_1, w_2 \in k[x]$ такие, что $d = w_1 d_1 + w_2 f_s$. Имеем $d = w_1 v_1 f_1 + \cdots + w_1 v_{s-1} f_{s-1} + w_2 f_s = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s$. $\square$

Определение 6.3.7. Многочлен называется нормированным, если его старший коэффициент равен 1.

Ясно, что в каждом классе ассоциированных многочленов существует нормированный многочлен. В частности среди НОД системы многочленов, которые определяются с точностью до ассоциированности, существует единственный нормированный НОД. Этот нормированный НОД будем обозначать $(f_1, f_2, \ldots, f_s)$.

Определение 6.3.8. Система многочленов $\{f_1, f_2, \ldots, f_s\}$ называется взаимнопростой в совокупности, если нормированный НОД $(f_1, f_2, \ldots, f_s) = 1$. В случае двух многочленов говорят, что они взаимнопростые.

ТЕОРЕМА 6.3.5 (свойства взаимнопростых многочленов). *Справедливы следующие утверждения.*

1. *Система многочленов $\{f_1, f_2, \ldots, f_s\}$ взаимнопроста в совокупности тогда и только тогда, когда некоторая их линейная комбинация равна единице, то есть* $(\exists\, u_1, \ldots, u_s \in k[x])\ u_1 f_1 + \ldots + u_s f_s = 1$;
2. *Если* $\mathcal{HOD}\{f_1, \ldots f_s\} = d$, *то* $\left(\frac{f_1}{d}, \frac{f_2}{d}, \ldots, \frac{f_s}{d}\right) = 1$;
3. *Если* $(f, h) = 1$ *и* $(g, h) = 1$, *то* $(fg, h) = 1$;
4. *Если* $h | fg$ *и* $(h, g) = 1$,*то* $h | f$;
5. *Если* $h | f$ *и* $g | f$ *и* $(h, g) = 1$, *то* $hg | f$.

Доказательство. 1) Положим в теореме 6.3.4 $d = 1$. Ясно, что d является ОД системы $\{f_1, f_2 \ldots, f_s\}$, тогда по теореме 6.3.4 $d = 1$ будет НОД $\{f_1, f_2 \ldots, f_s\}$ тогда и только тогда, когда существуют многочлены $u_1, u_2, \ldots, u_s \in k[x]$ такие, что $u_1 f_1 + \ldots + u_s f_s = 1$.

2) Так как $\mathcal{HOD}\{f_1, f_2 \ldots, f_s\} = d$, то по теореме 6.3.4 существуют многочлены $u_1, u_2, \ldots, u_s \in k[x]$ такие, что $d = u_1 f_1 + \ldots + u_s f_s$. Разделим

обе части равенства на d. $1 = u_1\frac{f_1}{d} + \ldots + u_s\frac{f_s}{d}$, из свойства 1 следует, что $(\frac{f_1}{d}, \frac{f_2}{d}, \ldots, \frac{f_s}{d}) = 1$.

3) Так как $(f, g) = 1$, то по теореме 6.3.4 $\exists\ u, v \in k[x] \quad 1 = uf + vh$. Так как $(g, h) = 1$, то $(\exists\ u_1, v_1 \in k[x]) \quad 1 = u_1 g + v_1 h$. Почленно перемножим эти соотношения. $1 = (uu_1)fg + (vu_1 g + uv_1 f + vv_1 h)h$. По свойству 1 видно что линейная комбинация многочленов fg и h равна единице, следовательно $(fg, h) = 1$.

4) Так как $(h, g) = 1$, то $\exists\ u, v \in k[x] \quad uh + vg = 1$. Умножим обе части этого равенства на f, получим $uhf + vgf = f$. Так как $h|fg$, то $fg = qh$, тогда $uhf + vqh = f \Rightarrow (uf + vq)h = f \Rightarrow h|f$.

5) Так как $h|f$, то $f = qh$. Имеем $g|qh$ и $(g, h) = 1$, по свойству 4 получаем, что $g|q$, следовательно $q = q_1 g$. Таким образом $f = q_1 gh \Rightarrow$ $\Rightarrow gh|f$. □

Будем теперь рассматривать систему многочленов $\{f_1, f_2, \ldots, f_s\}$, каждый из которых не равен нулю. Для таких систем многочленов изложим теорию наименьшего общего кратного (НОК) по схеме, аналогичной изучению НОД.

Определение 6.3.9. Многочлен m называется общим кратным системы многочленов $\{f_1, f_2, \ldots, f_s\}$, каждый из которых отличен от нуля, если он делится на все многочлены этой системы, то есть $(\forall\ 1 \leqslant i \leqslant s) \quad f_i|m$.

ТЕОРЕМА 6.3.6. *Пусть $\{f_1, f_2, \ldots, f_s\}$ — система ненулевых многочленов и $m \neq 0$ (некоторый ненулевой многочлен). Равносильны следующие утверждения:*

1) *совокупность кратных многочлена m совпадает с совокупностью ОК системы многочленов $\{f_1, f_2, \ldots, f_s\}$;*

2) *многочлен m является ОК $\{f_1, f_2, \ldots, f_s\}$, которое делит любое другое ОК этой системы.*

Определение 6.3.10. Наименьшим общим кратным (НОК) системы многочленов $\{f_1, f_2, \ldots, f_s\}$ называется любой ненулевой многочлен m, удовлетворяющий любому из равносильных условий теоремы 6.3.6.

Определение 6.3.11. НОК системы многочленов называется такое общее кратное этой системы, которое делит любое другое общее кратное этой системы многочленов.

Следствие 6.3.6.1. Если НОК системы многочленов существует, то оно определено с точностью до ассоциированности.

ТЕОРЕМА 6.3.7. *Если существует НОК 2-х любых ненулевых многочленов, то существует НОК и любой конечной системы многочленов, при этом имеет место следующая индукционная формула:*

$$\mathcal{НОК}\{f_1, f_2, \ldots, f_{s-1}, f_s\} = \mathcal{НОК}\{\mathcal{НОК}\{f_1, f_2, \ldots, f_{s-1}\}, f_s\}.$$

Теорема 6.3.7 сводит нахождение НОК системы многочленов к нахождению НОК 2-х многочленов.

ТЕОРЕМА 6.3.8. *Если f и g — два ненулевых многочлена, то их НОК существует и равно $\frac{fg}{(f,g)}$.*

Доказательство. Обозначим многочлен $\frac{fg}{(f,g)} = m$. Видно, что

$$m = \frac{g}{(f,g)}f \Rightarrow f|m$$

и

$$m = \frac{f}{(f,g)}g \Rightarrow g|m,$$

то есть m является ОК многочленов $\{f, g\}$. Пусть M — любое ОК $\{f, g\}$. Это означает, что $M = uf,\ M = vg \Rightarrow uf = vg$. Разделим обе части этого равенства на (f, g). Получим

$$u\frac{f}{(f,g)} = v\frac{g}{(f,g)} \Rightarrow \frac{g}{(f,g)}\Big| u\frac{f}{(f,g)}.$$

По свойству 2 теоремы 6.3.5 имеем $\left(\frac{f}{(f,g)}, \frac{g}{(f,g)}\right) = 1$. По 4 свойству теоремы 6.3.5 имеем $\frac{g}{(f,g)} \Big| u$. Тогда $u = \frac{g}{(f,g)}q$. $M = uf = \frac{fg}{(f,g)}q = mq$. Видно, что $m|M$. По определению 6.3.11 m является НОК $\{f, g\}$. □

6.4 Неприводимость. Каноническое разложение. Кратность

Пусть f — многочлен положительной степени, $\alpha \in k^* = k\backslash\{0\}$. Известно, что $\alpha|f$ и $\alpha f|f$.

Определение 6.4.1. Тривиальными делителями многочлена f положительной степени называются ненулевые константы и многочлены, ассоциированные с многочленом f.

Следствие. Делитель d многочлена f является нетривиальным тогда и только тогда, когда $0 < \deg d < \deg f$.

Следствие. Многочлен f положительной степени имеет нетривиальные делители тогда и только тогда, когда его можно представить в виде произведения 2-х многочленов, степени которых меньше степени многочлена f, то есть $(\exists\ u, v \in k[x]) \quad f = uv$, где $\deg u, \deg v < \deg f$.

Определение 6.4.2. Многочлен P положительной степени называется неприводимым над полем k, если он имеет над этим полем только тривиальные делители. В противном случае, многочлен P называется приводимым.

Определение 6.4.3. Многочлен P положительной степени называется неприводимым над полем k, если его нельзя представить над этим полем в виде произведения 2-х многочленов, степени которых меньше степени многочлена P.

Замечание 6.4.1. Понятие неприводимости существенно зависит от основного поля k. Так, например, многочлен $f = x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ неприводим над полем $\mathbb{Q}$. Но он приводим над полем $\mathbb{R}$.

Замечание 6.4.2. Многочлены 1-й степени являются неприводимыми над любым полем.

Это следует из того, что многочлены 1-й степени имеют только тривиальные делители.

ТЕОРЕМА 6.4.1 (свойства неприводимых многочленов). *Справедливы следующие утверждения:*

1. *Если многочлен P является неприводимым, то и любой ассоциированный с ним многочлен также является неприводимым.*

2. *Если P — неприводимый многочлен, f — любой многочлен, то либо $(P, f) = 1$, либо $P|f$.*

3. *Если P — неприводимый многочлен и $P|fg$, то $P|f$ или $P|g$.*

4. *Если P и Q — два неприводимых многочлена, то либо $(P, Q) = 1$, либо P и Q ассоциированы.*

Доказательство. 1) Пусть P — неприводимый многочлен. Рассмотрим αP, где $\alpha \in k^*$. Надо доказать, что αP является неприводимым. Допустим противное, то есть у αP есть нетривиальный делитель, то есть $(\exists\ d \in k[x])\quad d|\alpha P$, где $0 < \deg d < \deg \alpha P = \deg P$. Имеем, $d|\alpha P$ и $\alpha P|P \Rightarrow d|P$ и $0 < \deg d < \deg P$. Это противоречит неприводимости многочлена P.

2) Обозначим $(P, f) = d$. Имеем $d|P$. Так как P — неприводим, то d должен быть тривиальным делителем, то есть либо $d = \alpha \in k^*$, либо $d \sim P$. В первом случае имеем $(P, f) = 1$. Во втором случае, имеем $P|d$ и $d|f \Rightarrow P|f$.

3) Пусть $P|fg$. Если $P|f$, то все доказано. Если $P \nmid f$, то по свойству 2 $(P, f) = 1$. Итак, $P|fg$ и $(P, f) = 1$, тогда по свойству 4 теоремы 6.3.5 $P|g$.

4) Пусть P и Q — два неприводимых многочлена. Если $(P, Q) = 1$, то все доказано. Пусть $(P, Q) \neq 1$, тогда по свойству 2 $P|Q$. Меняя ролями P и Q, получаем $Q|P \Rightarrow P \sim Q$. □

ТЕОРЕМА 6.4.2 (о разложении на неприводимые множители). *Любой многочлен f положительной степени над полем k может быть представлен в виде $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$, где $\alpha \in k^*$, P_i — нормированные неприводимые над k многочлены. Это представление единственно с точностью до порядка следования сомножителей и при этом необходимо, чтобы α являлась старшим коэффициентом многочлена f.*

Доказательство. 1) Существование.

Рассмотрим множество M всех нормированных делителей положительной степени многочлена f. В этом множестве M выберем многочлен P_1 наименьшей степени. Покажем, что многочлен P_1 является неприводимым. Допустим противное, то есть многочлен P_1 является приводимым. Следовательно $P_1 = du$, где $0 < \deg d < \deg P_1$, а это противоречит выбору многочлена P_1. Имеем

$$f = P_1 f_1, \quad \text{где} \quad 0 \leqslant \deg f_1 < \deg f. \tag{1}$$

Если $\deg f_1 = 0$, то процесс выделения неприводимых множителей заканчивается. Если $\deg f_1 > 0$, то с многочленом f_1 проводим те же рассуждения, что и с многочленом f. Получим, что у многочлена f_1 есть нормированный неприводимый множитель P_2. Будем иметь

$$f_1 = P_2 f_2, \quad \text{где} \quad 0 \leqslant \deg f_2 < \deg f_1. \tag{2}$$

Если $\deg f_2 = 0$, то процесс выделения неприводимых множителей заканчиваем. Если $\deg f_2 > 0$, то процесс продолжаем. И так далее. Возникает вопрос: наш процесс конечен или бесконечен? Заметим, что степени

многочленов $f_1, f_2, \ldots$ образуют строго убывающую последовательность натуральных чисел $\deg f > \deg f_1 > \deg f_2 > \ldots$, которая не может быть бесконечной. В конце концов получим

$$f_{s-1} = P_s f_s, \quad \text{где} \quad \deg f_s = 0. \tag{s}$$

Это означает, что $f_s = \alpha \in k^*$. Перемножим почленно все равенства $(1), (2), \ldots, (s)$, получим $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$. Так как$P_i$ является нормированными многочленами, то сравнивая в этом равенстве коэффициенты при старшей степени x, получим, что α является старшим коэффициентом многочлена f.

2) Единственность.

Пусть наряду с представлением $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$ имеет место другое представление $f = \beta Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t$, где $\beta \in k^*$, Q_j — нормированные неприводимые над k многочлены. Тогда, по доказанному выше, β является старшим коэффициентом многочлена f, то есть $\beta = \alpha$.

$$f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s = \beta Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t. \tag{$*$}$$

Равенство $(*)$ указывает на то, что $P_1 | (Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t)$. По свойству 3 теоремы 6.4.1 $(\exists\ 1 \leqslant j \leqslant t) \quad P_1 | Q_j$. Будем считать, что $P_1 | Q_1$. Тогда по свойству 4 теоремы 6.4.1 $P_1 \sim Q_1$. Так как оба многочлена нормированы, то $P_1 = Q_1$. Тогда равенство $(*)$ сокращаем на P_1. Получим

$$P_2 \cdot \ldots \cdot P_s = Q_2 \cdot \ldots \cdot Q_t. \tag{$**$}$$

С многочленом P_2 рассуждаем также, как с многочленом P_1. Равенство $(**)$ указывает на то, что $P_2 | (Q_2 \cdot \ldots \cdot Q_t) \Rightarrow (\exists\ 2 \leqslant j \leqslant t) \quad P_2 | Q_j$. Будем считать, что $P_2 | Q_2$. Тогда $P_2 \sim Q_2 \Rightarrow P_2 = Q_2$. И так далее. Если $s = t$, то в конце концов получим $P_s = Q_s$.

Может ли $s \neq t$? Предположим, что $s < t$, тогда сокращая равенство $(*)$ на $P_1 \cdot P_2 \cdot \ldots \cdot P_s$ получим, что $1 = Q_{s+1} \cdot \ldots \cdot Q_t$ — этого быть не

может так как слева стоит многочлен нулевой степени, а справа многочлен положительной степени. Аналогично не может быть и $s > t$ таким образом Q_j — те же самые P_i, только написанные возможно в другом порядке. □

ТЕОРЕМА 6.4.3 (о каноническом представлении). *Любой многочлен f положительной степени над полем k может быть представлен в виде $f = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}$, где $\alpha \in k^*$, P_i — различные нормированные, неприводимые над k многочлены, $k_i \in \mathbb{N}$. Это представление единственно с точностью до порядка следования сомножителей и при этом α необходимо являться старшим коэффициентом многочлена f.*

Доказательство. По теореме 6.4.2 имеем $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$. Объединяя в этом представлении произведение одинаковых множителей в степени, получим

$$f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}, \qquad (t \leqslant s).$$

□

Определение 6.4.4. Представление многочлена f в виде $f = \alpha P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}$ называется каноническим представлением многочлена f. Многочлены $P_1^{k_1}, P_2^{k_2}, \ldots, P_t^{k_t}$ называются элементарными делителями многочлена f. Натуральные числа $k_1, k_2, \ldots, k_t$ называются кратностями неприводимых многочленов $P_1, P_2, \ldots, P_t$ в многочлене f.

Пусть $\gamma \in k$. Мы уже заметили, что многочлены 1-й степени неприводимы над любым полем k. В частности $x - \gamma$ является нормированным неприводимым над k многочленом, поэтому можно говорить о кратности многочлена $x - \gamma$ в многочлене f.

Определение 6.4.5. Кратностью элемента $\gamma \in k$ в многочлене f называется кратность неприводимого многочлена $x - \gamma$ в многочлене f.

Определение 6.4.6. Элемент $\gamma \in k$ называется корнем многочлена $f(x)$, если $f(\gamma) = 0$.

Предложение 6.4.1. *Для того, чтобы элемент $\gamma \in k$ был корнем многочлена $f(x)$ необходимо и достаточно, чтобы многочлен f делился на $x - \gamma$, то есть, чтобы элемент γ имел положительную кратность в многочлене f.*

Доказательство. В самом деле, по теореме Безу $f(x) = Q(x)(x - \gamma) + + f(\gamma)$, тогда $(x - \gamma)|f(x) \Leftrightarrow f(\gamma) = 0$, то есть по определению 6.4.6 γ является корнем $f(x)$. □

Следствие. Элемент $\gamma \in k$ не является корнем многочлена $f(x)$ тогда и только тогда, когда элемент γ имеет нулевую кратность в многочлене $f(x)$.

Определение 6.4.7. Корень γ в многочлене $f(x)$ называется простым, если он имеет первую кратность.

Пусть каноническое представление многочлена f имеет вид

$$f = \alpha(x - \gamma_1)^{k_1} \dots (x - \gamma_s)^{k_s} P_1^{l_1} \dots P_t^{l_t}, \quad \text{где} \quad \deg P_i \geqslant 2.$$

Видно, что

$$\deg \left[(x - \gamma_1)^{k_1} \dots (x - \gamma_s)^{k_s}\right] \leqslant \deg f,$$

то есть

$$k_1 + k_2 + \dots + k_s \leqslant \deg f.$$

Ясно, что $(\forall\ 1 \leqslant i \leqslant s) \quad f(\gamma_i) = 0$, то есть $\gamma_1, \gamma_2, \dots, \gamma_s$ являются корнями многочлена f. Если каждый корень γ_i считать k_i раз, то число $k_1 + k_2 + \dots + k_s$ — число корней многочлена f с учетом их кратностей.

Предложение 6.4.2. *Число корней многочлена $f(x)$ с учетом их кратностей не превосходит степень многочлена f.*

6.5 Производная и кратность

Пусть k — некоторое фиксированное числовое поле.

Определение 6.5.1. Производной многочлена $f = \sum\limits_{i=0}^{\infty} \alpha_i x^i$ называется многочлен вида

$$f' = \sum_{i=0}^{\infty} i\alpha_i x^{i-1}.$$

ТЕОРЕМА 6.5.1 (основные правила дифференцирования). *Имеют места следующие свойства:*

1. $\alpha' = 0$, *где* $\alpha \in k$;
2. $(\alpha f)' = \alpha f'$, *где* $\alpha \in k$;
3. $(f \pm g)' = f' \pm g'$;
4. $(fg)' = f'g + fg'$;
5. $(f^n)' = nf^{n-1}f',\ n \in \mathbb{N}$.

Определение 6.5.2. Полагают $f^{(0)} = f,\ f^{(l+1)} = (f^{(l)})'$, где $l \geqslant 0,\ l \in \mathbb{Z}$.

Ясно, что если $\deg f = n$, то $(\forall\ l > n) \quad f^{(l)} = 0$.

Лемма 6.5.1. Если f — многочлен положительной степени n, то $f' \neq 0$ и $\deg f' = n - 1$.

Доказательство. Имеем $f = \alpha_n x^n + \ldots + \alpha_1 x + \alpha_0$, где $\alpha_n \neq 0,\ n \geqslant 1$. По определению 6.5.1 $f' = n\alpha_n x^{n-1} + \ldots + \alpha_1$. Старший коэффициент у многочлена f' равен $n\alpha_n$, где $n \in \mathbb{N},\ \alpha_n \neq 0$. Тогда $n\alpha_n \neq 0$, следовательно $f' \neq 0$ и $\deg f' = n - 1$. □

ТЕОРЕМА 6.5.2. *Пусть f — многочлен положительной степени и неприводимый множитель P имеет положительную кратность k в многочлене f. Тогда этот неприводимый множитель P имеет кратность $k - 1$ в производной f'.*

Доказательство. Имеем $f = P^l g$, где $P \nmid g$. Составим $f' = lP^{l-1}P'g + + P^l g' = P^{l-1}(lP'g + Pg')$. Видно, что $P^{l-1}|f'$, то есть кратность P в f' не меньше, чем $l-1$. Покажем, что $P^l \nmid f'$. Допустим противное, то есть $P^l|f'$. Тогда $P|(lP'g + Pg')$. Видно, что $P|Pg'$, следовательно $P|(lP'g)$. Ясно, что $(P, l) = 1$. По лемме $P' \neq 0$ и $\deg P' < \deg P \Rightarrow (P, P') = 1$. По свойству 3 теоремы 6.4.1 имеем, что $P|g$, а это противоречит тому, что дано. Следовательно $P^l \nmid f'$ и кратность P в составе f' точно $l-1$. □

Следствие 6.5.2.1. Элемент γ имеет кратность k в многочлене f тогда и только тогда, когда $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$.

Доказательство. 1) Необходимость.

Пусть γ имеет кратность k в многочлене f. По определению это означает, что $(x-\gamma)$ имеет кратность k в многочлене f. По теореме 6.5.2 $x-\gamma$ имеет кратность $k-1$ в f', $x-\gamma$ имеет кратность $k-2$ в f'', $\ldots$, $x-\gamma$ имеет кратность 1 в $f^{(k-1)}$, $x-\gamma$ имеет кратность 0 в $f^{(k)}$. Применяя предложение 6.4.1 $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$.
2) Достаточность.

Пусть $f(\gamma) = f'(\gamma) = \ldots = f^{(k-1)}(\gamma) = 0$, но $f^{(k)}(\gamma) \neq 0$. Пусть кратность γ в многочлене f равна l .Надо доказать, что $l = k$. Допустим противное. Пусть, например, $l < k$. Тогда по первой части доказательства будем иметь $f(\gamma) = f'(\gamma) = \ldots = f^{(l-1)}(\gamma) = 0$, но $f^{(l)}(\gamma) \neq 0$. Этого быть не может, потому что по условию $f^{(l)}(\gamma) = 0$ так как $l \leqslant k-1$. Аналогично приводит к противоречию и предположение, что $l > k$. □

Следствие 6.5.2.2. Кратность элемента γ в многочлене f равна наименьшему порядку производной многочлена f, не имеющего γ своим корнем.

ТЕОРЕМА 6.5.3 (об отделении кратных множителей). *Пусть f — многочлен положительной степени над полем k. Тогда многочлен $F = \dfrac{f}{(f, f')}$ имеет те же самые неприводимые множители, что и многочлен f, но только первой кратности.*

Доказательство. Пусть $f = \alpha P_1^{k_1} P_2^{k_2} \dots P_t^{k_t}$ — каноническое разложение многочлена f. Тогда по теореме 6.5.2

$$f' = P_1^{k_1-1} P_2^{k_2-1} \dots P_t^{k_t-1} g, \quad \text{где} \quad (\forall\ 1 \leqslant i \leqslant t) \quad P_i \nmid g.$$

Составим $(f, f') = P_1^{k_1-1} P_2^{k_2-1} \dots P_t^{k_t-1}$.

$$F = \frac{f}{(f, f')} = \alpha P_1 P_2 \dots P_t.$$

□

6.6 Алгебраически замкнутые поля

Пусть k — основное поле.

ТЕОРЕМА 6.6.1 (о равносильных условиях, определяющих алгебраически замкнутое поле). *Относительно фиксированного основного поля k справедливы следующие равносильные утверждения.*

1) *любой многочлен f положительной степени с коэффициентами из поля k, имеет в поле k, по крайней мере, один корень;*

2) *неприводимыми над полем k являются многочлены только первой степени;*

3) *многочлен поля k распадается над полем k на линейные множители;*

4) *любой многочлен f положительной степени с коэффициентами из поля k имеет в поле k столько корней с учетом их кратностей, какова степень многочлена f.*

Доказательство. 1) $\Rightarrow$ 2)

Пусть f — любой многочлен, $\deg f \geqslant 2$. Тогда по условию 1) этот многочлен имеет в поле k по крайне мере один корень γ. Тогда по предложению 6.4.1 $f = (x - \gamma)g$. Следовательно f является приводимым над k.

2) $\Rightarrow$ 3)

Пусть f многочлен положительной степени. Тогда по теореме 6.4.2 его можно представить в виде $f = \alpha P_1 \cdot P_2 \cdot \ldots \cdot P_s$, где $\alpha \in k^*$, P_i — нормированные неприводимые над k многочлены. Из условия 2) следует, что $P_i = x - \gamma_i \Rightarrow f = \alpha(x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_n)$. Таким образом многочлен распадается на линейные множители.

3) $\Rightarrow$ 4)

Имеем $f = \alpha(x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_s)$. Объединим произведение одинаковых множителей в степени.

$$f = (x-\gamma_1)^{k_1}(x-\gamma_2)^{k_2}\ldots(x-\gamma_t)^{k_t}, \quad k_i \in \mathbb{N}.$$

Видно, что $\gamma_1, \ldots, \gamma_t$ — корни многочлена f с кратностями $k_1, \ldots, k_t$ и $\deg f = k_1 + \ldots + k_t$. Таким образом число корней многочлена f с учетом их кратностей равно степени многочлена f.

4) $\Rightarrow$ 1)

Пусть многочлен f имеет $\deg > 0$. Тогда по условию 4) $k_1 + k_2 + \ldots + k_t = \deg f \geqslant 1 \Rightarrow (\exists\ 1 \leqslant i \leqslant t) \quad k_i \geqslant 1$. Значит, многочлен f имеет по крайней мере корень γ_i. □

Определение 6.6.1. Поле k называется алгебраически замкнутым, если оно удовлетворяет любому из равносильных условий теоремы 6.6.1.

Замечание 6.6.1. Поля $\mathbb{Q}$ и $\mathbb{R}$ не являются алгебраически замкнутыми, так как не выполняется 1) условие теоремы 6.6.1. Примером может служить многочлен $f = x^2 + 1$. Он не имеет ни одного корня ни в поле $\mathbb{Q}$, ни в поле $\mathbb{R}$.

Определение 6.6.2. Алгебраическим замыканием поля k называется наименьшее алгебраически замкнутое расширение поля k.

Определение 6.6.3. Поле $\overline{k}$ называется алгебраическим замыканием поля k, если выполнены следующие 3 условия:

1. $k \subset \overline{k}$;

2. $\overline{k}$ является алгебраически замкнутым полем;

3. если $k \subset k' \subset \overline{k}$ и k' — алгебраически замкнутое поле, то $k' = \overline{k}$.

ТЕОРЕМА 6.6.2 (основная теорема алгебры). *Поле комплексных чисел $\mathbb{C}$ является алгебраически замкнутым полем.*

Следствие 6.6.2.1. Алгебраическим замыканием поля действительных чисел $\mathbb{R}$ является поле комплексных чисел, то есть $\overline{\mathbb{R}} = \mathbb{C}$.

Доказательство. Действительно, пусть $\overline{\mathbb{R}}$ — алгебраическое замыкание поля $\mathbb{R}$. Тогда $\mathbb{R} \subset \overline{\mathbb{R}}$. Далее, многочлен $x^2 + 1$ имеет корень в $\overline{\mathbb{R}}$, то есть $i \in \overline{\mathbb{R}}$. Это выполняется тогда и только тогда, когда $(\forall\ x, y \in \mathbb{R})\quad x + yi \in \overline{\mathbb{R}}$, то есть $\mathbb{C} \subset \overline{\mathbb{R}}$. Имеем $\mathbb{R} \subset \mathbb{C} \subset \overline{\mathbb{R}}$. По теореме 6.6.2 $\mathbb{C}$ является алгебраически замкнутым, тогда по определению 6.6.3 имеем $\mathbb{C} = \overline{\mathbb{R}}$. $\square$

Пусть $\gamma_1, \gamma_2, \ldots, \gamma_n$ — элементы поля k.

Определение 6.6.4. Элементарными симметрическими многочленами от элементов $\gamma_1, \ldots, \gamma_n$ называются суммы вида:

$$\sigma_1 = \gamma_1 + \gamma_2 + \ldots + \gamma_n;$$

$$\sigma_2 = \gamma_1\gamma_2 + \gamma_1\gamma_3 + \ldots + \gamma_1\gamma_n + \gamma_2\gamma_3 + \ldots + \gamma_2\gamma_n + \ldots + \gamma_{n-1}\gamma_n;$$

$$\ldots$$

$$\sigma_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \gamma_{i_1} \ldots \gamma_{i_k};$$

$$\ldots$$

$$\sigma_n = \gamma_1 \ldots \gamma_n.$$

Предложение 6.6.1. *Если $\gamma_1, \gamma_2, \ldots, \gamma_n \in k$, то*

$$f(x) = (x+\gamma_1)(x+\gamma_2)\ldots(x+\gamma_n) = x^n + \sigma_1 x^{n-1} + \ldots + \sigma_k x^{n-k} + \ldots + \sigma_n,$$

где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — элементарные симметрические многочлены от $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Доказательство. Чтобы установить этот факт, достаточно перемножить скобки стоящие слева и привести подобные слагаемые. □

Следствие. Если $\gamma_1, \gamma_2, \ldots, \gamma_n \in k$, то $f(x) = (x - \gamma_1)(x - \gamma_2)\ldots(x - - \gamma_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^k \sigma_k x^{n-k} + \ldots + (-1)^n \sigma_n$, где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — элементарные симметрические многочлены от $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Доказательство. В самом деле, достаточно в предложении 6.6.1 вместо γ_i подставить $-\gamma_i$. Тогда σ_k заменится на $(-1)^k \sigma_k$ и тем самым следствие будет установлено. □

ТЕОРЕМА 6.6.3 (теорема Виета). *Пусть* $f(x) = x^n + \alpha_1 x^{n-1} + + \alpha_2 x^{n-2} + \ldots + \alpha_n$ *и этот многочлен имеет в алгебраическом замыкании* $\overline{k}$ *корни* $\gamma_1, \gamma_2, \ldots, \gamma_n$. *Тогда* $\sigma_k = (-1)^k \alpha_k$, *где* $\sigma_1, \sigma_2, \ldots, \sigma_n$ — *элементарные симметрические многочлены от корней* $\gamma_1, \gamma_1, \ldots, \gamma_n$.

Доказательство. Над полем $\overline{k}$ многочлен

$$f(x) = (x - \gamma_1)(x - \gamma_2)\ldots(x - \gamma_n),$$

где $\gamma_1, \gamma_2, \ldots, \gamma_n$ — корни $f(x)$ в $\overline{k}$. По следствию из предложения 6.6.1 имеем:

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^k \sigma_k x^{n-k} + \ldots + (-1)^n \sigma_n.$$

С другой стороны, по условию $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$. Таким образом имеем два выражения одного и того же многочлена по убывающим степеням x. Тогда, коэффициенты при одинаковых степенях x должны совпадать. Имеем $-\sigma_1 = \alpha_1,\ \sigma_2 = \alpha_2, \ldots, (-1)^k \sigma_k = \alpha_k, \ldots, (-1)^n \sigma_n = = \alpha_n$. Имеем $(\forall\ 1 \leqslant k \leqslant n) \quad (-1)^k \sigma_k = \alpha_k$. Умножим на $(-1)^k$, получим $\sigma_k = (-1)^k \alpha_k$. □

Частный случай теоремы 6.6.3:

n=2, $f(x) = x^2 + px + q$. Пусть $x_1,\ x_2$ — корни $f(x)$, тогда

$$\begin{cases} \sigma_1 = x_1 + x_2 = -p; \\ \sigma_2 = x_1 \cdot x_2 = q. \end{cases}$$

n=3, $f(x) = x^3 + px^2 + qx + r$. Пусть $x_1,\ x_2\ x_3$ — корни $f(x)$, тогда

$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 = -p; \\ \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = q; \ . \\ \sigma_3 = x_1x_2x_3 = -r \end{cases}$$

6.7 Многочлены над числовыми полями

Рассмотрим случай, когда $k = \mathbb{C}$. По основной теореме алгебры, поле $\mathbb{C}$ является алгебраически замкнутым, поэтому многочлены над полем $\mathbb{C}$ обладают любым из равносильных условий теоремы 6.6.1. В частности, неприводимыми над полем $\mathbb{C}$ являются многочлены только первой степени. Далее, любой многочлен положительной степени над полем $\mathbb{C}$ имеет, по крайне мере, один корень. Наконец, каноническое разложение любого многочлена f положительной степени над полем $\mathbb{C}$ имеет вид:

$$f(x) = \alpha(x - \gamma_1)^{k_1}(x - \gamma_2)^{k_2} \dots (x - \gamma_t)^{k_t},$$

где $\gamma_1, \gamma_2, \dots, \gamma_t \in \mathbb{C}$.

Рассмотрим случай, когда $k = \mathbb{R}$. Пусть $\gamma = \alpha + \beta_i$, где $\alpha, \beta \in \mathbb{R},\ \beta \neq \neq 0$. В этом случае говорят, что γ — существенно комплексное число.

Предложение 6.7.1. *Если γ — существенно комплексное число, то многочлен $(x-\gamma)(x-\overline{\gamma})$ является квадратным трехчленом с действительными коэффициентами и отрицательным дискриминантом.*

Доказательство. Действительно, $(x - \gamma)(x - \bar{\gamma}) = x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} = = x^2 - 2\alpha x + \alpha^2 + \beta^2 \in \mathbb{R}[x]$, тогда $D = (-2\alpha)^2 - 4(\alpha^2 + \beta^2) = -4\beta^2 < 0$, так как γ — существенно комплексное число. □

ТЕОРЕМА 6.7.1. *Если существенно комплексное число γ является корнем многочлена f с действительными коэффициентами, то комплексно сопряженное число $\bar{\gamma}$ также является корнем этого многочлена и при том той же кратности, что и корень γ.*

Доказательство. Пусть $f(x) = \alpha_n x^n + \ldots + \alpha_1 x + \alpha_0$, где $\alpha_i \in \mathbb{R}$ и γ — существенно комплексный корень $f(x)$, то есть $f(\gamma) = 0$.

$$\alpha_n \gamma^n + \ldots + \alpha_1 \gamma + \alpha_0 = 0.$$

Перейдем к комплексно сопряженным числам, получим

$$\overline{\alpha_n \gamma^n + \ldots + \alpha_1 \gamma + \alpha_0} = \bar{0}.$$

Воспользуемся свойствами комплексно сопряженных чисел, а именно

$$\bar{\alpha}_n \cdot \bar{\gamma}^n + \ldots + \bar{\alpha_1} \cdot \bar{\gamma} + \bar{\alpha_0} = \bar{0}.$$

Так как α_i и $0 \in \mathbb{R}$, то $\bar{\alpha}_i = \alpha_i,\ \bar{0} = 0$. Получаем

$$\alpha_n (\bar{\gamma})^n + \ldots + \alpha_1 \bar{\gamma} + \alpha_0 = 0.$$

Это равенство указывает на то, что $f(\bar{\gamma}) = 0$ то есть $\bar{\gamma}$ является корнем многочлена $f(x)$. Покажем, что кратность корня $\bar{\gamma}$ совпадает с кратностью корня γ. Пусть кратность γ равна k, а кратность $\bar{\gamma}$ равна l. Необходимо доказать, что $k = l$. Допустим противное, то есть $k \neq l$. Пусть, например, $k > l$, тогда $f = (x-\gamma)^k (x-\bar{\gamma})^l g(x)$, где $g(\gamma) \neq 0, g(\bar{\gamma}) \neq 0$. Тогда $f(x) = [(x-\gamma)(x-\bar{\gamma})]^l (x-\gamma)^{k-l} g(x) = [(x-\gamma)(x-\bar{\gamma})]^l g_1(x)$, то есть $g_1 = \frac{f(x)}{[(x-\gamma)(x-\bar{\gamma})]^l}$. По предложению $(x-\gamma)(x-\bar{\gamma}) \in \mathbb{R}[x]$, поэтому

$$g_1 = \frac{f(x)}{[(x-\gamma)(x-\bar{\gamma})]^l} \in R[x].$$

Видно, что $g_1(x) = (x-\gamma)^{k-l} g(x)$ имеет γ своим корнем положительной кратности, $k - l > 0$, но не имеет своим корнем $\bar{\gamma}$. Это противоречит первому утверждению доказываемой теоремой. Аналогично приводит к противоречию предположение, что $l > k$. $\square$

Следствие 6.7.1.1. Существенно комплексные корни многочлена с действительными коэффициентами попарно комплексно сопряжены.

ТЕОРЕМА 6.7.2 (о неприводимых многочленах над $\mathbb{R}$). *Над полем действительных чисел $\mathbb{R}$ неприводимыми являются многочлены первой степени и те и только те квадратные трехчлены, дискриминант которых отрицательный.*

Доказательство. Пусть $f(x) \in \mathbb{R}[x]$ и $\deg f(x) \geqslant 3$. Этот многочлен имеет в алгебраическом замыкании $\overline{\mathbb{R}} = \mathbb{C}$ имеет по крайне мере один корень α. Если $\alpha \in \mathbb{R}$, то $f(x) = (x-\alpha)g(x)$, где $g(x) \in \mathbb{R}[x]$ то есть многочлен f приводим над $\mathbb{R}$. Если α — существенно комплексное число, то $\bar{\alpha}$ также будет корнем многочлена f. Получим

$$f(x) = (x-\alpha)(x-\bar{\alpha})g(x) = (x^2 - 2Re\alpha \cdot x + |\alpha|^2)g(x).$$

В этом случае

$$g(x) = \frac{f(x)}{(x-\alpha)(x-\bar{\alpha})} \in \mathbb{R}[x].$$

Видно, что $f(x)$ снова приводим над $\mathbb{R}$. Таким образом, любой многочлен f, степень которого $\deg f \geqslant 3$, является приводимым над $\mathbb{R}$.

Пусть $f = ax^2+bx+c, a \neq 0$. Известно, что этот квадратный трехчлен распадается на линейные множители $f = a(x-x_1)(x-x_2)$ над $\mathbb{R}$ тогда и только тогда, когда его дискриминант $D \geqslant 0$. В этом случае, многочлен f приводим над $\mathbb{R}$. Следовательно, он будет неприводим над $\mathbb{R}$ тогда и только тогда, когда $D = b^2 - 4ac < 0$. А многочлены первой степени являются неприводимыми над любым полем. □

Следствие 6.7.2.1. Любой многочлен положительной степени над полем действительных чисел имеет каноническое представление вида:

$$f = \alpha(x-\gamma_1)^{k_1} \dots (x-\gamma_t)^{k_t}(x^2+\beta_1 x+\delta_1)^{l_1} \dots (x^2+\beta_r x+\delta_r)^{l_r},$$

где $\alpha, \beta_i, \delta_i, \gamma_j \in \mathbb{R},\ \beta_i^2 - 4\delta_i < 0,\ k_j, l_i \in \mathbb{N}$ при $i = \overline{1,r},\ j = \overline{1,t}$.

Следствие 6.7.2.2. Любой многочлен с действительными коэффициентами нечетной степени имеет, по крайне мере, один действительный корень.

Доказательство. В самом деле, по следствию 6.7.2.1 $\deg f = k_1 + \ldots + k_t + 2l_1 + \ldots + 2l_r$. По условию степень f — число нечетное, следовательно $k_1 + \ldots + k_t$ — нечетное число, значит $(\exists\ 1 \leqslant i \leqslant t) \quad k_i \geqslant 1$, то есть γ_i является действительным корнем многочлена f. $\square$

Глава 7

Основные алгебраические структуры

Глава 8

Линейные пространства

8.1 Понятие линейного пространства

Определение 8.1.1. Пусть k и V — два произвольных множества. Говорят, что на множестве V определена внешняя алгебраическая операция со множеством мультипликаторов k, если задано отображение декартового произведения $k \times V \to V$. При этом отображении, образ упорядоченный пары (α, a), где $\alpha \in k,\ a \in V$ называется произведением α на a и обозначается αa.

Замечание 8.1.1. Алгебраические операции, изучаемые ранее на множестве V, называются внутренними алгебраическими операциями. В качестве множества k чаще всего будет выступать поле, которое будем называть основным. Элементы поля k будем обозначать $\alpha, \beta, \gamma, \alpha_1, \alpha_2, \ldots$

Определение 8.1.2. Линейным (векторным) пространством над полем k называется множество V, рассмотренное вместе с определенной на нем внутренней алгебраической операцией сложения и внешней алгебраической операцией умножения на скаляры поля k, удовлетворяемыми следующим семи аксиомам.

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

3. $(\forall\ a, b \in V)\ \ (\exists\ x \in V) \quad b + x = a$;

4. $\alpha(a + b) = \alpha a + \alpha b$;

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

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

7. $1 \cdot a = a$,

где $a, b, c, x \in V$; $\alpha, \beta, 1 \in k$.

Замечание 8.1.2. Множество V часто называют базисным множеством линейного пространства. Его элементы будем обозначать $a, b, c, a_1, a_2, \ldots$ и называть векторами.

Свойства линейных пространств

1. $(\forall\ a \in V)\ \ (\exists\ 0 \in V) \quad a + 0 = a$;

2. $(\forall\ a \in V)\ \ (\exists\ (-a) \in V) \quad a + (-a) = 0$;

3. $(\forall\ a, b \in V)\ \ (\exists\ (a - b) \in V) \quad a - b = a + (-b)$;

4. $\alpha a = 0 \Leftrightarrow \alpha = 0$ или $a = 0$;

5. $\alpha(-a) = (-\alpha)a = -\alpha a$;

6. $\alpha(a - b) = \alpha a - \alpha b$;

7. $(\alpha - \beta)a = \alpha a - \beta a$.

Доказательство. Аксиомы 1–3 линейного пространства указывают на то, что $(V, +)$ образует аддитивную группу, поэтому справедливы свойства 1)–3).

4) *Необходимость.*

Имеем $\alpha a = (\alpha + 0)a = \alpha a + 0a \Rightarrow 0a = \alpha a - \alpha a = 0$. Получаем, что $0a = 0$.

Имеем $\alpha a = \alpha(a+0) = \alpha a + \alpha 0 \Rightarrow \alpha 0 = \alpha a - \alpha a = 0$. Получаем, что $\alpha 0 = 0$.

Достаточность.

Пусть $\alpha a = 0$. Если $\alpha = 0$, то все доказано. Если $\alpha \neq 0$ то будет существовать $\alpha^{-1} \in k$. Тогда $a = 1 \cdot a = (\alpha^{-1}\alpha)a = \alpha^{-1}(\alpha a) = \alpha^{-1} \cdot 0 = 0$.

5) Расмотрим $\alpha a + \alpha(-a) = \alpha(a + (-a)) = \alpha \cdot 0 = 0 \Rightarrow \alpha(-a) = -\alpha a$. Далее, $\alpha a + (-\alpha)a = (\alpha + (-\alpha))a = 0 \cdot a = 0 \Rightarrow (-\alpha)a = -\alpha a$.

6) Имеем, $\alpha(a-b) = \alpha(a + (-b)) = \alpha a + \alpha(-b) = \alpha a - \alpha b$.

7) Подсчитаем $(\alpha - \beta)a = (\alpha + (-\beta))a = \alpha a + (-\beta)a = \alpha a - \beta a$. $\square$

Примеры линейных пространств:

1. $V = \{0\}$ — нулевое линейное пространство (тривиальное).
2. $V = k^n = \{(\alpha_1, \ldots, \alpha_n) | \alpha_i \in k\}$ — координатное линейное пространство над полем k.
3. $V = M(m \times n, k)$ — матрицы размерности $m \times n$ с элементами из k.
4. $V = L$ — множество решений однородной системы линейных уравнений.
5. $V = k[x]$ — множество многочленов от одного неизвестного с коэффициентами из k.
6. $V = \{f(x) \in k[x] \,| deg\ f \leqslant n\}$.

8.2 Конечномерные и бесконечномерные линейные пространства. Базис линейного пространства

Легко заметить, что основные понятия и факты, определенные в координатном линейном пространстве переносятся на абстрактные линейные пространства. Связано это с тем, что эти понятия и факты использовали

только свойства операций над векторами, но не использовали природу самих векторов. А как видно из определения 8.1.2, операции в абстрактном линейном пространстве обладают теми же самыми свойствами, что и операции в координатном линейном пространстве. Поэтому, в абстрактных линейных пространствах можно говорить о линейной комбинации векторов, о линейно зависимых и линейно не зависимых системах векторов, о критерии и свойствах линейной зависимости, об основной теореме о линейной зависимости, о линейном выражении одной системы векторов через другую, об эквивалентных системах векторов, о базисе и ранге системы векторов. Но есть и отличия.

Пример: $V = k[x]$. Рассмотрим следующую систему векторов: $1, x, x^2, \ldots, x^n \in V$. Эта система векторов является линейно не зависимой. Действительно,

$$\alpha_0 \cdot 1 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n = 0 \Leftrightarrow \alpha_0 = \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0,$$

а это и означает, что $1, x, x^2, \ldots, x^n$ является линейно не зависимой системой векторов. Совершенно ясно, что n можно брать любым и как угодно большим. Поэтому в пространстве V существуют линейно не зависимые системы векторов с каким угодно большим числом этих векторов.

Определение 8.2.1. Линейное пространство V называется конечномерным, если существует натуральное число N такое, что число линейно не зависимых векторов в любой системе пространства V не превосходит N. В противном случае, линейное пространство V называется бесконечномерным.

Пример:

1. $V = k^n$ — конечномерное линейное пространство.

2. $V = k[x]$ — бесконечномерное линейное пространство.

В конечномерных линейных пространствах можно говорить о базисе как конечной, так и бесконечной системы векторов. В частности, можно говорить о базисе всего конечномерного линейного пространства V.

Определение 8.2.2. Базисом ненулевого конечномерного пространства V называется упорядоченная линейно не зависимая подсистема векторов $B = \{e_1, e_2, \ldots, e_n\}$, удовлетворяя любому из следующих равносильных условий:

1. любой вектор $a \in V$ линейно выражается через подсистему B;
2. $\forall\ a \in V$ подсистема (B, a) является линейно зависимой;
3. в пространстве V не существует линейно не зависимых подсистем с числом векторов большим, чем в B.

Определение 8.2.3. Размерностью нулевого линейного пространства считается число 0. Размерностью ненулевого конечномерного линейного пространства V называется число векторов в любом базисе этого пространства или максимальное число линейно не зависимых векторов этого пространства V.

Размерность конечномерного линейного пространства V будем обозначать $dim\ V$ или $rang\ V$.

Пример:

1. $dim\ \{0\} = 0$;
2. $dim\ k^n = n$;
3. $dim\ M(m \times n, k) = mn$;
4. $dim\ L = n - r$;
5. $dim\,\{f(x) \in k[x] | deg\ f(x) \leqslant n\} = n + 1$.

Пусть V — конечномерное линейное пространства и $e_1, e_2, \ldots, e_n$ — его базис. Тогда любой вектор $a \in V$ можно выразить чрез этот базис

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n. \tag{8.1}$$

Так как базис является линейно не зависимой системой векторов, то это выражение (8.1) для вектора a единственно. Таким образом, каждому вектору $a \in V$ ставится в соответствие упорядоченная система $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ относительно базиса $e_1, e_2, \ldots, e_n$.

Определение 8.2.4. Координатами (компонентами) вектора $a \in V$ относительно заданного базиса $e_1, e_2, \ldots, e_n$ линейного пространства V называется упорядоченная совокупность коэффициентов линейного выражения вектора a через этот базис.

Пишут, вектор $a = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Определение 8.2.5. Координатным столбцом вектора a относительно заданного базиса $e_1, e_2, \ldots, e_n$ называется столбец, составленный из координат вектора a относительно этого базиса.

Обозначим $\check{a} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \ldots \\ \alpha_n \end{pmatrix}$.

Определение 8.2.6. Сопоставление вектору $a \in V$ его координатного столбца относительно заданного базиса пространства V называется стандартным отображением линейного пространства V размерности n в координатное линейное пространство k^n.

Ясно, что каждый базис $e_1, e_2, \ldots, e_n$ определяет свое стандартное отображение $V \to k^n$.

Предложение 8.2.1. *Координатный столбец суммы двух векторов равен сумме координатных столбцов слагаемых векторов. Координатный столбец произведения вектора на скаляр, равен координатному столбцу этого вектора, умноженному на этот скаляр.*

Это предложение 8.2.1 означает, что $a \check{+} b = \check{a} + \check{b}$ и $\check{\alpha a} = \alpha \check{a}$.

Дадим другую форму записи (8.1). Ясно, что $\check{a}^\top = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ — матрица размерности $1 \times n$. Рассмотрим базисный столбец пространства V $\tilde{e} = \begin{pmatrix} e_1 \\ e_2 \\ \ldots \\ e_n \end{pmatrix}$ — матрица размерности $n \times 1$. Тогда $\check{a}^\top \tilde{e} = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n = a$. Таким образом, $a = \check{a}^\top \tilde{e}$ — матричная запись равенства (8.1).

8.3 Изоморфизм линейных пространств

Пусть V и V' — два линейных пространства над одним и тем же основным полем k.

Определение 8.3.1. Изоморфизмом линейного пространства V на линейное пространство V' над одним и тем же основным полем k называется всякая биекция $f : V \to V'$, удовлетворяющая условиям линейности:

1. $(\forall\ a, b \in V) \quad f(a + b) = f(a) + f(b)$;
2. $(\forall\ \alpha \in k,\ a \in V) \quad f(\alpha a) = \alpha f(a)$.

Условие 1 означает, что отображение f является изоморфизмом аддитивной группы $(V, +)$ в аддитивную группу $(V', +)$.

Определение 8.3.2. Линейное пространство V называется изоморфным линейному пространству V' ($V \cong V'$), если существует хотя бы один изоморфизм $f : V \to V'$.

Предложение 8.3.1. *Отношение изоморфизма является отношением эквивалентности на классе линейных пространств над одним и тем же основным полем k.*

Это предложение 8.3.1 означает, что для отношения изоморфности справедливы следующие утверждения

1. $V \cong V$, то есть выполняется свойство рефлексивности;
2. если $V \cong V'$, то $V' \cong V$ (симметричность);
3. если $V'' \cong V'$ и $V' \cong V$, то $V'' \cong V$ (транзитивность).

ТЕОРЕМА 8.3.1 (о свойствах изоморфных линейных пространств). *Справедливы следующие утверждения:*

1. *при изоморфизме линейно зависимой системы векторов переходят в линейно зависимые, а линейно не зависимые системы векторов переходят в линейно не зависимые;*
2. *изоморфные линейные пространства одновременно либо конечномерные, либо бесконечномерные;*
3. *при изоморфизме базис системы векторов переходит в базис, ранг системы векторов при изоморфизме не изменяется.*

Доказательство. 1) Пусть $f : V \to V'$ является изоморфизмом. Возьмем линейно зависимую систему векторов $a_1, a_2, \ldots, a_s$ из V. Это означает, что существуют скаляры $\alpha_1, \alpha_2, \ldots, \alpha_s$ не все равные нулю такие, что $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$. Перейдем к образам этих векторов $f(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s) = f(0)$. Так как f — изоморфизм, то $\alpha_1 f(a_1) + \alpha_2 f(a_2) + \ldots + \alpha_s f(a_s) = 0$, здесь не все $\alpha_i = 0$. Последнее соотношение указывает на то, что векторы $f(a_1), f(a_2), \ldots, f(a_s)$ являются линейно зависимыми в V'.

Пусть $a_1, a_2, \ldots, a_s$ линейно не зависимая система векторов из V. Надо доказать, что $f(a_1), f(a_2), \ldots, f(a_s)$ также является линейно не зависимой. Допустим противное, то есть система $f(a_1), f(a_2), \ldots, f(a_s)$ является линейно зависимой. Тогда рассмотрим отображение $f^{-1} : V' \to V$, которое также является изоморфизмом. При этом отображении линейно зависимые векторы $f(a_1), f(a_2), \ldots, f(a_s)$ перейдут в линейно зависимые векторы $a_1, a_2, \ldots, a_s$, а это противоречит линейной независимости $a_1, a_2, \ldots, a_s$.

2) Пусть $f : V \to V'$ и V является конечномерным линейным пространством. Это означает, что существует натуральное число N такое, что число векторов в любой линейно не зависимой системы из пространства V не превосходит этого числа N. Так как при изоморфизме только линейно не зависимая система векторов переходит в линейно не зависимую, то в пространстве V' число векторов в любой линейно не зависимой системе также будет ограничено этим числом N, следовательно пространство V' будет конечномерным.

Пусть V является бесконечномерным линейным пространством. Надо доказать, что и V' в этом случае также будет бесконечномерным. Допустим противное, то есть V' является конечномерным линейным пространством. Тогда рассмотрим изоморфизм $f^{-1} : V' \to V$. При этом изоморфизме из конечномерности V' будет следовать конечномерность V, а это противоречит условию.

3) Пусть A — система векторов из V, B — базис системы векторов A и $f : V \to V'$ —изоморфизм. Тогда, так как $B \subset A$, то $f(B) \subset f(A)$. Далее, A линейно выражается через B, тогда $f(A)$ будет линейно выражаться через $f(B)$. Наконец, так как B — линейно независимая система векторов, $f(B)$ также является линейно независимой. Таким образом, $f(B)$ является базисом $f(A)$, то есть базис B системы векторов A переходит в базис $f(B)$ системы векторов $f(A)$. Так как f является биекцией, то чис-

ло векторов в B равно числу векторов $f(B)$, то есть $r(A) = r(f(A))$. $\square$

Следствие 8.3.1.1. Изоморфные конечномерные линейные пространства имеют одинаковую размерность.

Доказательство. Действительно, $f : V \to V'$ — изоморфизм и V и V' являются конечномерными линейными пространствами. Тогда базис $e_1, e_2, \ldots, e_n$ пространства V переходит в базис $f(e_1), f(e_2), \ldots, f(e_n)$ пространства V', то есть $dim\ V = n = dim\ V'$. $\square$

ТЕОРЕМА 8.3.2. *Любое конечномерное линейное пространство V размерности n изоморфно координатному линейному пространству k^n и при этом изоморфизм достигается с помощью стандартного отображения $f : V \to k^n$ относительно любого базиса пространства V.*

Доказательство. Пусть $dim\ V = n$ и $\tilde{e} = \begin{pmatrix} e_1 \\ e_2 \\ \ldots \\ e_n \end{pmatrix}$ — базис V. Рассмотрим стандартное отображение $f : V \to k^n$. Известно, что если $a = \check{a}^\top \tilde{e}$, то $f(a) = \check{a}$. Покажем, что это отображение f является изоморфизмом.

Во-первых, f является инъекцией. Действительно, если $f(a) = f(b)$, то $\check{a} = \check{b} \Rightarrow a = b$.

Во-вторых, f является сюръекцией. В самом деле, возьмем любой столбец $\check{a} \in k^n$ и построим вектор $a = \check{a}^\top \tilde{e}$. Тогда $f(a) = \check{a}$.

Остается показать, что отображение f сохраняет операции. Рассмотрим $f(a + b) = a \check{+} b = \check{a} + \check{b} = f(a) + f(b)$. $f(\alpha a) = \alpha \check{a} = \alpha \check{a} = \alpha f(a)$. Таким образом $f : V \to k^n$ является изоморфизмом, следовательно $V \cong k^n$. $\square$

Следствие 8.3.2.1. Конечномерные линейные пространства одинаковой размерности изоморфны.

Доказательство. Действительно, пусть размерность $dim\ V = n$ и $dim\ V' = n$. Тогда по теореме 8.3.2 $V \cong k^n$ и $V' \cong k^n$, следовательно $V \cong V'$. □

Следствие 8.3.2.2. Ранг системы векторов конечномерного линейного пространства V равен рангу системы координатных столбцов векторов этой системы относительно любого базиса пространства V.

Доказательство. Пусть $a_1, a_2, \ldots, a_s$ — система векторов из V. Рассмотрим $f : V \to k^n$ — стандартный изоморфизм, тогда система векторов $a_1, a_2, \ldots, a_s$ переходит в $\check{a}_1, \check{a}_2, \ldots, \check{a}_s$. Но по утверждению 3 теоремы 8.3.1 $r(a_1, a_2, \ldots, a_s) = r(\check{a}_1, \check{a}_2, \ldots, \check{a}_s)$. □

8.4 Переход от одного базиса к другому. Матрица перехода

Пусть V — конечномерное линейное пространство над k, $dim\ V = n$ и пусть

$$\widetilde{e} = \begin{pmatrix} e_1 \\ e_2 \\ \ldots \\ e_n \end{pmatrix} \qquad \text{и} \qquad \widetilde{u} = \begin{pmatrix} u_1 \\ u_2 \\ \ldots \\ u_n \end{pmatrix}$$

— два базиса пространства V. Выразим векторы базиса $\widetilde{u}$ через векторы базиса $\widetilde{e}$:

$$\begin{gathered} u_1 = \alpha_{11}e_1 + \alpha_{21}e_2 + \ldots + \alpha_{n1}e_n; \\ u_2 = \alpha_{12}e_1 + \alpha_{22}e_2 + \ldots + \alpha_{n2}e_n; \\ \ldots \\ u_n = \alpha_{1n}e_1 + \alpha_{2n}e_2 + \ldots + \alpha_{nn}e_n. \end{gathered} \tag{8.2}$$

Определение 8.4.1. Матрицей перехода от базиса $\widetilde{e}$ к базису $\widetilde{u}$ называется матрица, транспонированная к матрице, составленной из коэффи-

циентов линейного выражения векторов базиса $\widetilde{u}$ через векторы базиса $\widetilde{e}$.

Определение 8.4.1 означает, что матрица перехода

$$Q = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \dots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \dots & \alpha_{n2} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn} \end{pmatrix}^{\top} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}.$$

Первым столбцом матрицы является координатный столбец вектора u_1. Вторым — координатный столбец вектора u_2, и т.д.

Определение 8.4.2. Матрицей перехода от базиса $\widetilde{e}$ к базису $\widetilde{u}$ называется матрица Q, столбцами которой являются координатные столбцы векторов базиса $\widetilde{u}$ относительно базиса $\widetilde{e}$, то есть

$$Q = (\widetilde{u}_1|_{\widetilde{e}}, \widetilde{u}_2|_{\widetilde{e}}, \dots, \widetilde{u}_n|_{\widetilde{e}}) .$$

Определение 8.4.3. Матрицей перехода от базиса $\widetilde{e}$ к базису $\widetilde{u}$ называется матрица Q, определяемая равенством $\widetilde{u} = Q^{\top}\widetilde{e}$ — матричная запись системы (8.2).

ТЕОРЕМА 8.4.1 (о матрице перехода). *Справедливы следующие утверждения*

1. *Матрица перехода от одного базиса к другому является не особенной. Обратно, любую не особенную матрицу можно рассматривать как матрицу перехода от заданного базиса к некоторому другому базису.*

2. *Матрицы перехода от базиса $\widetilde{e}$ к базису $\widetilde{u}$ и от базиса $\widetilde{u}$ к базису $\widetilde{e}$ являются взаимно обратными.*

Доказательство. 1) Пусть Q — любая не особенная матрица и $\widetilde{e}$ — заданный базис пространства V. Построим векторы $u_1, u_2, \dots, u_n$ таким

образом, чтобы их координатные столбцы относительно базиса $\widetilde{e}$ совпадали со столбцами матрицы Q.

Так как $|Q| \neq 0$, то столбцы матрицы Q являются линейно независимыми, поэтому и векторы $u_1, u_2, \ldots, u_n$ будут линейно независимыми. В силу этого, векторы $u_1, u_2, \ldots, u_n$ можно взять в качестве базиса $\widetilde{u}$ пространства V.

По построению будем иметь $\widetilde{u} = Q^\top \widetilde{e}$, то есть матрица Q является матрицей перехода от заданного базиса $\widetilde{e}$ к вновь построенному базису $\widetilde{u}$.

2) Пусть $\widetilde{e}$ и $\widetilde{u}$ — два базиса пространства V. Пусть Q — матрица перехода от $\widetilde{e}$ к $\widetilde{u}$, R — матрица перехода от $\widetilde{u}$ к $\widetilde{e}$. Тогда по определению 8.4.3 будем иметь $\widetilde{u} = Q^\top \widetilde{e}$, $\widetilde{e} = R^\top \widetilde{u}$. Отсюда, $\widetilde{e} = R^\top (Q^\top \widetilde{e}) = (R^\top Q^\top)\widetilde{e} = (QR)^\top \widetilde{e}$.

Это равенство указывает на то, что матрица QR является матрицей перехода от $\widetilde{e}$ к $\widetilde{e}$. Но этой матрицей является матрица E, следовательно $QR = E$. Это соотношение указывает на то, что Q и R — не особенные взаимно обратные матрицы, то есть $Q = R^{-1}$. □

ТЕОРЕМА 8.4.2. *Координатный столбец вектора относительно нового базиса равен координатному столбцу этого вектора относительно старого базиса, умноженному слева на матрицу перехода от нового базиса к старому, то есть*

$$\check{a}|_{\widetilde{u}} = R \cdot \check{a}|_{\widetilde{e}},$$

где R — матрица перехода от базиса $\widetilde{u}$ к базису $\widetilde{e}$.

Доказательство. Пусть $\widetilde{e}$ — старый базис, $\widetilde{u}$ — новый базис, R — матрица перехода от $\widetilde{u}$ к $\widetilde{e}$, то есть $\widetilde{e} = R^\top \widetilde{u}$. С одной стороны, вектор $a = \check{a}^\top|_{\widetilde{u}} \cdot \widetilde{u}$. С другой стороны, вектор $a = \check{a}^\top|_{\widetilde{e}} \cdot \widetilde{e} = \check{a}^\top|_{\widetilde{e}} \cdot (R^\top \widetilde{u}) = (\check{a}^\top|_{\widetilde{e}} \cdot R^\top)\widetilde{u} = (R \cdot \check{a}|_{\widetilde{e}})^\top \widetilde{u}$.

Так как выражение вектора a через базис $\widetilde{u}$ является единственным, то $\check{a}^\top|\widetilde{u} = (R \cdot \check{a}|_{\widetilde{e}})^\top$. Транспонируя эти матрицы, получим $\check{a}|_{\widetilde{u}} = R \cdot \check{a}|_{\widetilde{e}}$. □

8.5 Линейные подпространства

Пусть V — линейное пространство над полем k.

Определение 8.5.1. Подмножество L базисного множества V называется устойчивым подмножеством, если оно устойчиво относительно внутреннего сложения и внешнего умножения, то есть

1. $(\forall\ a, b \in L) \quad a + b \in L$;

2. $(\forall\ \alpha \in k,\ a \in L) \quad \alpha a \in L$.

Следствие. Устойчивое подмножество L, рассмотренное вместе с индуцированными на нем операциями, образует линейное пространство.

Доказательство. $L \subset V$ и L — устойчивое подмножество, тогда на L можно рассмотреть индуцированные операции внутреннего сложения и внешнего умножения. Покажем, что $(\forall\ a, b \in L) \quad a - b \in L$. Действительно, $-b = -(1 \cdot b) = (-1)b \in L$, тогда $a - b = a + (-b) \in L$. Таким образом, $(L, +)$ образует аддитивную подгруппу группы $(V, +)$. Поэтому первые три аксиомы линейного пространства выполняются в L, остальные четыре аксиомы, относящиеся к внешнему умножению, выполняясь в пространстве V, будут выполняться и на устойчивом подмножестве L. Этим установлено, что L является линейным пространством. □

Определение 8.5.2. Линейным подпространством пространства V называется всякое его устойчивое подмножество L, рассмотренное вместе с индуцированными на нем операциями.

Предложение 8.5.1. *Пересечение семейства линейных подпространств линейного пространства V снова является подпространством пространства V.*

Доказательство. В самом деле, пусть $\{L_i\}$ — семейство линейных подпространств пространства V. Рассмотрим множество

$$L = \bigcap_{(i)} L_i.$$

Надо показать, что L — устойчивое подмножество в пространстве V.

Пусть $a, b \in L \Rightarrow (\forall\ i) \quad a, b \in L_i$. Так как L_i — линейное подпространство, то $(\forall\ i) \quad a + b \in L_i \Rightarrow a + b \in \bigcap\limits_{(i)} L_i = L$. Следовательно, L устойчиво относительно внутреннего сложения.

Аналогично показывается, что $(\forall\ \alpha \in k, a \in L) \quad \alpha a \in L$.

Следовательно, L — подпространство пространства V. □

Пусть теперь A — подмножество линейного пространства V. Рассмотрим все линейные подпространства L пространства V, содержащие множество A. Такие подпространства существуют, например, все множество V. Устроим пересечение всех этих подпространств L, то есть

$$\bigcap_{L \supset A} L = L(A).$$

Предложение 8.5.2. *Множество $L(A)$ — наименьшее линейное подпространство пространства V, содержащее множество A.*

Доказательство. Действительно, тот факт, что $L(A)$ является подпространством пространства V следует из предложения 8.5.1. Далее, множество A содержится во всех L которые мы пересекаем, следовательно $A \subset L(A)$.

Наконец, возьмем любое линейное подпространство L', такое, что $A \subset L'$. Тогда оно находится среди пересекаемых подпространств L, следовательно $L(A) \subset L'$. □

Определение 8.5.3. Линейной оболочкой множества A пространства V называется наименьшее линейное подпространство $L(A)$ пространства V, содержащее множество A.

Часто говорят, что подпространство $L(A)$ порождено множеством A или натянуто на множество A.

Предложение 8.5.3 (строение $L(A)$). *Линейная оболочка $L(A)$ состоит из множества линейных комбинаций конечных подмножеств множества A с коэффициентами из основного поля k, то есть*

$$L(A) = \left\{ \sum_{a \in A} \alpha_a a \,\middle|\, \alpha_a \in k \text{ и почти все } \alpha_a = 0 \right\}.$$

Доказательство. В самом деле, введем обозначение: $L' = \left\{ \sum\limits_{a \in A} \alpha_a a \right\}$. Необходимо показать, что $L(A) = L'$.

С одной стороны, так как $A \subset L(A)$, то $L(A)$ содержит любую линейную комбинацию конечного подмножества множества векторов A, то есть $L' \subset L(A)$.

С другой стороны, ясно, что L' — устойчивое подмножество пространства V, следовательно, L' — линейное подпространство пространства V. Кроме того, множество $A \subset L'$ (так как $a = 1 \cdot a + 0 \cdot a_1 + 0 \cdot a_2 + \ldots$). Тогда по предложению 8.5.2 $L(A) \subset L'$.

В итоге получаем, что $L(A) = L'$. □

Следствие 8.5.0.1. Если $A = \{a_1, a_2, \ldots, a_s\}$, где векторы $a_1, a_2, \ldots, a_s$ являются линейно независимыми, то $L(A)$ — конечномерно, $dim\ L(A) = s$ и

$$L(A) = \left\{ \sum_{i=1}^{s} \alpha_i a_i \,\middle|\, \alpha_i \in k \right\}.$$

Доказательство. Действительно, тот факт, что $L(A)$ имеет указанный вид следует из предложения 8.5.3. Тогда векторы $a_1, a_2, \ldots, a_s$ можно взять в качестве базиса $L(A)$, следовательно, $dim\ L(A) = s$. □

Следствие 8.5.0.2. Если линейное пространство V конечномерное, то любое его линейное подпространство L также является конечномерным и $dim\ L \leqslant dim\ V$. Если $dim\ L = dim\ V$, то $L = V$.

Доказательство. В самом деле, пусть $dim\ V = n$ и $e_1, e_2, \ldots, e_n$ — базис V. Так как L — подпространство линейного пространства V, то оно должно быть конечномерным. В противном случае, из бесконечномерности пространства L вытекало бы бесконечномерность пространства V.

Пусть $a_1, a_2, \ldots, a_s$ — базис L, то есть $dim\ L = s$. Так как $a_1, a_2, \ldots, a_s$ линейно выражаются через базис $e_1, e_2, \ldots, e_n$ пространства V, то по основной теореме о линейной зависимости $s \leqslant n$, то есть $dim\ L \leqslant dim\ V$.

Если $dim\ L = dim\ V$, то есть $s = n$, то векторы $a_1, a_2, \ldots, a_n$ можно взять в качестве базиса пространства V. В силу предложения 8.5.3 будем иметь

$$L = \left\{ \sum_{i=1}^{n} \alpha_i a_i \right\} = V.$$

□

Определение 8.5.4. Суммой семейства линейных подпространств $\{L_i\}$ пространства V называется линейная оболочка множества, равная теоретико-множественному объединению базисных множеств этих линейных подпространств, то есть

$$\sum_{(i)} L_i = L\left(\bigcup_{(i)} L_i \right).$$

Определение 8.5.5. Суммой семейства линейных подпространств $\{L_i\}$ пространства V называется наименьшее линейное подпространство пространства V, содержащее все подпространства данного семейства.

Предложение 8.5.4 (строение суммы). *Сумма $L_1 + L_2$ двух линейных подпространств совпадает со множеством векторов вида* $\{a_1 + a_2 |\ a_1 \in L_1, a_2 \in L_2\}$.

Доказательство. Действительно, по определению 8.5.4 имеем $L_1 + L_2 = = L(L_1 \cup L_2)$. Введем обозначение $L' = \{a_1 + a_2 |\ a_i \in L_i,\ i = 1, 2\}$. Надо показать, что $L_1 + L_2 = L'$.

С одной стороны, ясно, что L' — устойчивое подмножество пространства V, поэтому L' — линейное подпространство пространства V.

Далее, $L_1 \subset L'$. Действительно, $(\forall\ a_1 \in L_1) \quad a_1 = a_1 + 0$, где $0 \in L_2$. Аналогично, $L_2 \subset L'$, имеем $(\forall\ a_2 \in L_2) \quad a_2 = 0 + a_2$, где $0 \in L_1$. Отсюда, $L_1 \cup L_2 \subset L'$, следовательно $L(L_1 \cup L_2) \subset L'$, то есть $L_1 + L_2 \subset L'$.

С другой стороны, возьмем произвольный вектор $a \in L'$. Его можно представить в виде $a = a_1 + a_2$, где $a_1 \in L_1,\ a_2 \in L_2$. Векторы $a_1, a_2 \in$ $\in L_1 \cup L_2$, следовательно $a = a_1 + a_2 \in L(L_1 \cup L_2) = L_1 + L_2$, то есть $a \in L_1 + L_2$. Имеем $L' \subset L_1 + L_2$.

Таким образом, из двух включений получаем, что $L_1 + L_2 = L'$. $\square$

Замечание 8.5.1. Можно показать, что в общем случае

$$\sum_{(i)} L_i = \left\{ \sum_{(i)} a_i \Big| \ \ a_i \in L_i \text{ и почти все } a_i = 0 \right\}.$$

Определение 8.5.6. Сумма линейных подпространств $L_1 + L_2$ называется прямой, если $L_1 \cap L_2 = \{0\}$.

Прямая сумма обозначается $L_1 \oplus L_2$.

Лемма 8.5.1. Любую линейно независимую систему векторов конечномерного линейного пространства V можно дополнить до базиса пространства V.

Доказательство. Пусть $a_1, a_2, \ldots, a_s$ — линейно независимая система векторов из V и $e_1, e_2, \ldots, e_n$ — базис пространства V, $dim\ V = n$. Рассмотрим следующую систему векторов

$$a_1, a_2, \ldots, a_s, e_1, e_2, \ldots, e_n. \tag{8.3}$$

Из этой системы векторов (8.3) начнем удалять векторы, которые линейно выражаются через предыдущие. Первые s векторов остаются на месте, так как они линейно независимые. Получим

$$a_1, a_2, \ldots, a_s, e_{i_1}, e_{i_2}, \ldots, e_{i_k}. \tag{8.4}$$

Система векторов (8.4) будет линейно независимой, так как ни один вектор не выражается через остальные векторы.

Далее, любой вектор $a \in V$, линейно выражаясь через систему (8.3), будет линейно выражаться и через систему (8.4), так как удаленные векторы из системы (8.3), линейно выражаются через систему (8.4). Таким образом, система векторов (8.4) будет составлять базис пространства V. Этот базис получен из системы $a_1, a_2, \ldots, a_s$ добавлением некоторых векторов. $k = n - s$. □

ТЕОРЕМА 8.5.1 (о размерности суммы двух линейных подпространств). *Размерность суммы двух линейных подпространств конечномерного линейного пространства V равна сумме размерностей этих линейных подпространств без размерности их пересечения, то есть*

$$dim\ (L_1 + L_2) = dim\ L_1 + dim\ L_2 - dim\ (L_1 \cap L_2).$$

Доказательство. Пусть L_1 и L_2 — два линейных подпространства пространства V. Обозначение через $L = L_1 \cap L_2$. Пусть система векторов

$$e_1, e_2, \ldots, e_r \tag{8.5}$$

— базис L. Если $L = \{0\}$, то $r = 0$ и базисом будет пустое множество. По лемме базис L можно дополнить до базиса L_1

$$e_1, e_2, \ldots, e_r, u_{r+1}, \ldots, u_s, \tag{8.6}$$

где (8.6) — базис L_1, $dim\ L_1 = s$. Аналогично, по лемме базис L можно дополнить до базиса L_2

$$e_1, e_2, \ldots, e_r, v_{r+1}, \ldots, v_t, \tag{8.7}$$

где (8.7) — базис L_2, $dim\ L_2 = t$.

Рассмотрим следующую систему векторов

$$e_1, e_2, \ldots, e_r, u_{r+1}, \ldots, u_s, v_{r+1}, \ldots, v_t. \tag{8.8}$$

Покажем что система (8.8) является базисом $L_1 + L_2$. Действительно, возьмем произвольный вектор $x \in L_1 + L_2$. Тогда $x = a + b$, где $a \in L_1,\ b \in L_2$. Разлагая вектор a по базису (8.6), вектор b по базису (8.7) и складывая полученные выражения, мы получим, что вектор x линейно выражается через систему (8.8).

Остается показать, что система векторов (8.8) является линейно независимой. Рассмотрим линейную комбинацию

$$\alpha_1 e_1 + \ldots + \alpha_r e_r + \beta_{r+1} u_{r+1} + \ldots + \beta_s u_s + \gamma_{r+1} v_{r+1} + \ldots + \gamma_t v_t = 0. \quad (8.9)$$

Нужно показать, что все скаляры $\alpha_i, \beta_i, \gamma_i = 0$. Рассмотрим вектор

$$x = \alpha_1 e_1 + \ldots + \alpha_r e_r + \beta_{r+1} u_{r+1} + \ldots + \beta_s u_s. \quad (8.10)$$

Из равенства (8.9) видно, что вектор

$$x = -\gamma_{r+1} v_{r+1} - \ldots - \gamma_t v_t. \quad (8.11)$$

Равенство (8.10) указывает на то, что вектор $x \in L_1$, а равенство (8.11) указывает на то, что вектор $x \in L_2$, следовательно $x \in L_1 \cap L_2 = L$. Следовательно, вектор x можно выразить через базис L.

$$x = \alpha'_1 e_1 + \ldots + \alpha'_r e_r. \quad (8.12)$$

Сравним (8.10) и (8.12). Выражение вектора x через базис (8.6) должно быть единственным, тогда

$$\alpha_1 = \alpha'_1, \ldots, \alpha_r = \alpha'_r, \beta_{r+1} = 0, \ldots, \beta_s = 0.$$

Тогда равенство (8.9) принимает вид

$$\alpha_1 e_1 + \ldots + \alpha_r e_r + \gamma_{r+1} v_{r+1} + \ldots + \gamma_t v_t = 0. \quad (8.13)$$

Так как базис (8.7) является линейно независимой системой векторов, то из равенства (8.13) следует, что все скаляры $\alpha_1 = \ldots = \alpha_r = \gamma_{r+1} = = \ldots = \gamma_t = 0$.

Видно, что система векторов (8.8) является линейно независимой, следовательно, система векторов (8.8) является базисом $L_1 + L_2$. Тогда $dim\ (L_1 + L_2) =$ числу векторов в базисе (8.8) $= r + (s - r) + (t - r) = s + t - r = dim\ L_1 + dim\ L_2 - dim\ L = dim\ L_1 + + dim\ L_2 - dim\ (L_1 \cap L_2)$. $\square$

Следствие 8.5.1.1. Размерность прямой суммы равна сумме размерностей слагаемых.

Доказательство. Действительно, если $L_1 + L_2$ — прямая сумма, то по определению $L_1 \cap L_2 = \{0\}$, $dim\ \{0\} = 0$. Получаем, что $dim\ (L_1 \oplus L_2) = dim\ L_1 + dim\ L_2$. $\square$

Глава 9

Линейные операторы в линейном пространстве

9.1 Пространство и алгебра линейных операторов

Пусть V и V' — два линейных пространства над одним и тем же основным полем k.

Определение 9.1.1. Линейным оператором из пространства V в пространство V' над одним и тем же полем k называется всякое отображение $f : V \to V'$, удовлетворяющее двум условиям:

1. $(\forall\ a, b \in V) \quad f(a+b) = f(a) + f(b)$;
2. $(\forall\ \alpha \in k, a \in V) \quad f(\alpha a) = \alpha f(a)$.

Видно, что понятие «линейный оператор» является обобщением понятия «изоморфизм». В случае изоморфизма, требовалось чтобы f было биекцией. Условие 1) означает, что f является гомоморфизмом $(V, +)$ на $(V', +)$. Условие 1) называется условием аддитивности, а условие 2) называется условием однородности.

Определение 9.1.2. Линейным оператором из пространства V в пространство V' над одним и тем же основным полем k называется всякое

отображение $f : V \to V'$, удовлетворяющее условию линейности:

$$(\forall\ \alpha, \beta \in k,\ a, b \in V) \quad f(\alpha a + \beta b) = \alpha f(a) + \beta f(b).$$

Обозначим через $L(V, V')$ множество всех линейных операторов из пространства V в пространство V'. На этом множестве рассмотрим две алгебраические операции: внутреннее сложение и внешнее умножение.

Определение 9.1.3. Пусть $f, g \in L(V, V')$ и $\alpha \in k$. Полагают, что $(f + g)(a) = f(a) + g(a)$ и $(\alpha f)(a) = \alpha f(a)$.

Определение 9.1.3 корректно в том смысле, что $f + g$ и αf являются линейными операторами.

Действительно, $(\forall\ \alpha, \beta \in k,\ a, b \in V) \quad (f+g)(\alpha a+\beta b) = f(\alpha a+\beta b)+ + g(\alpha a + \beta b) = \alpha f(a) + \beta f(b) + \alpha g(a) + \beta g(b) = \alpha(f(a) + g(a)) + \beta(f(b) + + g(b)) = \alpha(f + g)(a) + \beta(f + g)(b)$. Следовательно $f + g \in L(V, V')$.

Еще проще доказывается, что $\alpha f \in L(V, V')$.

ТЕОРЕМА 9.1.1. *Множество $L(V, V')$, рассмотренное вместе с определенными на нем внутренней алгебраической операцией сложения и внешней алгебраической операцией умножения, образует линейное пространство над полем k.*

Доказательство. Пусть $f, g, h \in L(V, V'), \alpha, \beta, 1 \in k$. Для доказательства теоремы достаточно показать, что выполняются 7 аксиом линейного пространства, а именно

1. $f + g = g + f$;
2. $f + (g + h) = (f + g) + h$;
3. $(\forall\ f, g)\,(\exists\ h) \quad g + h = f$;
4. $\alpha(f + g) = \alpha f + \alpha g$;
5. $(\alpha + \beta)f = \alpha f + \beta f$;

6. $(\alpha\beta)f = \alpha(\beta f) = \beta(\alpha f)$;

7. $1 \cdot f = f$.

Проверим некоторые из них.

1) Имеем $(\forall\ a \in V) \quad (f+g)(a) = f(a)+g(a) = g(a)+f(a) = (g+f)(a)$. Следовательно, $f + g = g + f$.

3) Имеем $f, g \in L(V, V')$. Рассмотрим отображение $h : V \to V'$, определенное следующим образом $(\forall\ a \in V) \quad h(a) = f(a) - g(a)$. Легко показать, что это отображение удовлетворяет условию линейности, следовательно, $h \in L(V, V')$. Подсчитаем $(\forall\ a \in V) \quad (g+h)(a) = g(a)+h(a) =$ $= g(a) + (f(a) - g(a)) = f(a)$. Следовательно, $g + h = f$. □

Пусть V, V', V'' — три линейных пространства над полем k, пусть $f \in L(V, V')$, $\varphi \in L(V', V'')$. Тогда можем рассматривать композицию линейных операторов $\varphi \circ f : V \to V''$, которая определяется следующим образом $(\varphi \circ f)(a) = \varphi(f(a))$. Эту композицию $\varphi \circ f$ будем обозначать φf.

Покажем, что φf есть линейный оператор из пространства V в V''.

Действительно, $\varphi f(\alpha a + \beta b) = \varphi(f(\alpha a + \beta b)) = \varphi(\alpha f(a) + \beta f(b)) =$ $= \alpha\varphi(f(a)) + \beta\varphi(f(b)) = \alpha(\varphi f)(a) + \beta(\varphi f)(b)$. Следовательно, $\varphi f \in$ $\in L(V, V'')$.

ТЕОРЕМА 9.1.2. *Пусть $f, g \in L(V, V')$, $\varphi, \psi \in L(V', V'')$, $h \in L(V'', V''')$, $\alpha \in k$. Тогда справедливы следующие соотношения:*

1. $\varphi(f + g) = \varphi f + \varphi g$;

2. $(\varphi + \psi)f = \varphi f + \psi f$;

3. $h(\varphi f) = (h\varphi)f$;

4. $\alpha(\varphi f) = (\alpha\varphi)f = \varphi(\alpha f)$.

Пусть $f, g, \varphi, \psi, h \in L(V, V)$, то есть это линейные операторы из линейного пространства V в себя.

Определение 9.1.4. Линейный оператор из V в V называется эндоморфизмом.

На множестве $L(V, V)$ можно рассматривать третью алгебраическую операцию — внутреннее умножение. Если $f, \varphi \in L(V, V)$, то полагают $\varphi f = \varphi \circ f : V \to V$, $\varphi f \in L(V, V)$. Для этой операции умножения операторов справедливы соотношения 1)– 4) теоремы 9.1.2.

ТЕОРЕМА 9.1.3. *Множество $L(V, V)$, рассмотренное вместе с определенными на нем тремя алгебраическими операциями: внутренними сложением и умножением и внешним умножением, образует алгебру над полем k.*

Теорема 9.1.3 означает, что операции в множестве $L(V, V)$ удовлетворяют следующим 10 аксиомам:

1)–7) — аксиомы линейного пространства;

8) $f(g + h) = fg + fh$, $(f + g)h = fh + gh$;

9) $f(gh) = (fg)h$;

10) $\alpha(fg) = (\alpha f)g = f(\alpha g)$.

Как и всякая алгебра, алгебра линейных операторов есть соединение двух алгебраических структур: структуры линейного пространства (аксиомы 1)–7)) и структуры кольца (аксиомы 1)–3) и 8)–9)). Эти структуры связаны между собой свойством 10).

В дальшейшем, множество $L(V, V)$ будем обозначать $L(V)$.

Примеры:

1) Нулевой линейный оператор из $L(V)$. Он обозначается 0_V. Определяется таким образом $(\forall\, a \in V) \quad 0_V(a) = 0$. Ясно, что $(\forall\, f \in L(V)) \quad f + 0_V = f$.

2) Тождественный линейный оператор из $L(V)$. Обозначается 1_V. Определяется таким образом $(\forall\, a \in V) \quad 1_V(a) = a$. Ясно, что $(\forall\, f \in L(V)) \quad 1_V \cdot f = f \cdot 1_V = f$. Это означает, что в алгебре $L(V)$ есть единица.

9.2 Матрица линейного оператора в конечномерном линейном пространстве

Здесь мы получим обозрение всех линейных операторов алгебры $L(V)$, где $dim\ V = n$.

ТЕОРЕМА 9.2.1. *Пусть $e_1, e_2, \ldots, e_n$ — базис линейного пространства V. Пусть V' — другое линейное пространство над полем k и $a'_1, a'_2, \ldots, a'_n$ — произвольная система векторов из V'. Тогда существует единственный линейный оператор $f \in L(V, V')$, переводящий базис пространства V в заданную систему векторов пространства V', то есть*

$$(\forall\ 1 \leqslant i \leqslant n) \quad f(e_i) = a'_i.$$

Доказательство. 1) Единственность.

Пусть существует линейный оператор $f \in L(V, V')$ такой, что $(\forall\ 1 \leqslant \leqslant i \leqslant n) \quad f(e_i) = a'_i$. Любой вектор $a \in V$ можно представить в виде $a = \sum\limits_{i=1}^{n} \alpha_i e_i$. Тогда

$$f(a) = f\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \alpha_i f(e_i) = \sum_{i=1}^{n} \alpha_i a'_i.$$

Допустим, что существует другой линейный оператор $f_1 \in L(V, V')$, удовлетворяющий условию $(\forall\ 1 \leqslant i \leqslant n) \quad f_1(e_i) = a'_i$. Тогда

$$f_1(a) = f_1\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \alpha_i f_1(e_i) = \sum_{i=1}^{n} \alpha_i a'_i = f(a).$$

Следовательно $f_1 = f$.

2) Существование.

Пусть $a \in V$. Тогда $a = \sum\limits_{i=1}^{n} \alpha_i e_i$. Определим отображение $f : V \to V'$ следующим образом

$$f(a) = \sum_{i=1}^{n} \alpha_i a'_i.$$

Покажем, что это отображение удовлетворяет условиям линейности. Действительно, пусть $b \in V$, $b = \sum\limits_{i=1}^{n} \beta_i e_i$. Тогда

$$f(b) = \sum_{i=1}^{n} \beta_i a'_i.$$

$$f(a+b) = f\left(\sum_{i=1}^{n} (\alpha_i + \beta_i) e_i\right) = \sum_{i=1}^{n} (\alpha_i + \beta_i) a'_i =$$

$$= \sum_{i=1}^{n} \alpha_i a'_i + \sum_{i=1}^{n} \beta_i a'_i = f(a) + f(b).$$

Еще проще доказывается, что $f(\alpha a) = \alpha f(a)$, где $\alpha \in k$. Таким образом, отображение $f \in L(V, V')$. Наконец, $(\forall\ 1 \leqslant i \leqslant 1) \quad f(e_i) = f(0 \cdot e_1 + \ldots + 1 \cdot e_i + \ldots + 0 \cdot e_n) = 0 \cdot a'_i + \ldots + 1 \cdot a'_i + \ldots + 0 \cdot a'_n = a'_i$. □

Следствие 9.2.1.1. Линейный оператор из V в V' однозначно определяется образами базисных векторов пространства V.

Это вытекает из доказательства первой части теоремы 9.2.1.

Следствие 9.2.1.2. Множество линейных операторов из V в V' находится во взаимно однозначном соответствии с множеством упорядоченных систем из n-векторов пространства V.

Пусть V — линейное пространство над полем k, $dim\ V = n$, $e_1, e_2, \ldots, e_n$ — базис пространства V. Пусть, далее, $f \in L(V)$, по следствию из теоремы 9.2.1, этот оператор единственным образом определяется образами базисных векторов $f(e_1), f(e_2), \ldots, f(e_n) \in V$. Разложим

эти образы по базису пространства V, получим

$$\begin{gathered} f(e_1) = \alpha_{11}e_1 + \alpha_{12}e_2 + \ldots + \alpha_{1n}e_n; \\ f(e_2) = \alpha_{21}e_1 + \alpha_{22}e_2 + \ldots + \alpha_{2n}e_n; \\ \ldots \\ f(e_n) = \alpha_{n1}e_1 + \alpha_{n2}e_2 + \ldots + \alpha_{nn}e_n. \end{gathered} \tag{9.1}$$

Определение 9.2.1. Матрицей линейного оператора $f \in L(V)$ относительно базиса $e_1, e_2, \ldots, e_n$ называется матрица, транспонированная к матрице, составленной из коэффициентов линейного выражения образов базисных векторов через этот базис.

$$A_{f|_{\widetilde{e}}} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix}^{\top} = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \ldots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \ldots & \alpha_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{1n} & \alpha_{2n} & \ldots & \alpha_{nn} \end{pmatrix}.$$

Определение 9.2.2. Матрицей линейного оператора $f \in L(V)$ относительно базиса $e_1, e_2, \ldots, e_n$ называется матрица, столбцами которой являются координатные столбцы векторов $f(e_1), f(e_2), \ldots, f(e_n)$ относительно базиса $\widetilde{e}$, то есть

$$A_{f|_{\widetilde{e}}} = (\check{f}(e_1)|_{\widetilde{e}}, \check{f}(e_2)|_{\widetilde{e}}, \ldots, \check{f}(e_n)|_{\widetilde{e}}).$$

Определение 9.2.3. Если обозначить

$$\widetilde{e} = \begin{pmatrix} e_1 \\ e_2 \\ \ldots \\ e_n \end{pmatrix} \quad \text{и} \quad f(\widetilde{e}) = \begin{pmatrix} f(e_1) \\ f(e_2) \\ \ldots \\ f(e_n) \end{pmatrix},$$

то матрицей линейного оператора f относительно базиса $\widetilde{e}$ называется матрица A_f, определяемая из равенства

$$f(\widetilde{e}) = A_f^{\top}\widetilde{e}.$$

ТЕОРЕМА 9.2.2. *При фиксированном базисе $\widetilde{e}$ линейного пространства V, $\dim V = n$, отображение $\sigma : L(V) \to M(n,k)$, сопоставляющее линейному оператору f его матрицу относительно базиса $\widetilde{e}$ ($f \to A_{f|_{\widetilde{e}}}$), является изоморфизмом алгебры линейных операторов $L(V)$ на алгебру квадратных матриц n-го порядка $M(n,k)$.*

Доказательство. Путь $\widetilde{e}$ некоторый базис пространства V. Рассмотрим отображение $\sigma : L(V) \to M(n,k)$, $\sigma(f) = A_f$, где A_f — матрица линейного оператора f относительно базиса $\widetilde{e}$. Покажем, что это отображение является изоморфизмом.

1) *Инъективность σ.*

Пусть $\sigma(f) = \sigma(g)$, где $f, g \in L(V)$. Это означает, что $A_f = A_g \Rightarrow$ $\Rightarrow A_f^\top = A_g^\top \Rightarrow A_f^\top \widetilde{e} = A_g^\top \widetilde{e} \Rightarrow f(\widetilde{e}) = g(\widetilde{e})$. Мы получили, что образы базисных элементов пространства V совпадают. Тогда по следствию из теоремы 9.2.1 следует, что $f = g$.

2) *Сюръективность σ.*

Пусть $A \in M(n,k)$. Построим n векторов пространства V так, чтобы координатные столбцы этих векторов относительно базиса $\widetilde{e}$ совпадали со столбцами матрицы A. Тогда по теореме 9.2.1 существует линейный оператор $f \in L(V)$, переводящий базис $\widetilde{e}$ в построенные нами векторы. По построению будем иметь $f(\widetilde{e}) = A^\top \widetilde{e}$. Отсюда видно, если сравнивать с определением 9.2.3, что $A^\top = A_f^\top$. Таким образом, $\sigma(f) = A_f = A$.

3) *Сохранение операций.*

Пусть $f, g \in L(V)$ и A_f, A_g — матрицы этих линейных операторов относительно базиса $\widetilde{e}$. Тогда $f(\widetilde{e}) = A_f^\top \widetilde{e},\ g(\widetilde{e}) = A_g^\top \widetilde{e}$.

Рассмотрим действие суммы линейных операторов $f + g$ на базисные векторы. С одной стороны, $(f+g)(\widetilde{e}) = A_{f+g}^\top \widetilde{e}$.

С другой стороны, $(f+g)(\widetilde{e}) = f(\widetilde{e}) + g(\widetilde{e}) = A_f^\top \widetilde{e} + A_g^\top \widetilde{e} = (A_f^\top + A_g^\top)\widetilde{e} =$ $= (A_f + A_g)^\top \widetilde{e}$.

Отсюда, $A_{f+g}^\top = (A_f + A_g)^\top \Rightarrow A_{f+g} = A_f + A_g$. Таким образом, мат-

рица суммы линейных операторов равна сумме матриц этих операторов. Следовательно

$$\sigma(f+g) = A_{f+g} = A_f + A_g = \sigma(f) + \sigma(g),$$

то есть отображение σ сохраняет внутреннее сложение.

Рассмотрим действие произведения линейных операторов fg на базисные векторы. С одной стороны, $(fg)(\widetilde{e}) = A_{fg}^{\top}\widetilde{e}$.

С другой стороны, $(fg)(\widetilde{e}) = f(g(\widetilde{e})) = f(A_g^{\top}\widetilde{e}) = A_g^{\top}f(\widetilde{e}) = = A_g^{\top}(A_f^{\top}\widetilde{e}) = (A_g^{\top}A_f^{\top})\widetilde{e} = (A_fA_g)^{\top}\widetilde{e}$.

Отсюда, $A_{fg}^{\top} = (A_fA_g)^{\top} \Rightarrow A_{fg} = A_fA_g$, то есть матрица произведения линейных операторов равна произведению матриц этих операторов. Следовательно

$$\sigma(fg) = A_{fg} = A_fA_g = \sigma(f)\sigma(g),$$

то есть отображение σ сохраняет внутреннее умножение.

Наконец, совсем просто доказывается, что $A_{\alpha f} = \alpha A_f \Rightarrow \sigma(\alpha f) = = \alpha\sigma(f)$, где $\alpha \in k$. □

Предложение 9.2.1. *Координатный столбец образа вектора при действии линейным оператором равен координатному столбцу этого вектора, умноженному слева на матрицу этого линейного оператора, то есть*

$$f(\check{a}) = A_f\check{a}.$$

Доказательство. Действительно, вектор $a = \check{a}^{\top}\widetilde{e}$. С одной стороны, $f(a) = f(\check{a})^{\top}\widetilde{e}$. С другой стороны, $f(a) = f(\check{a}^{\top}\widetilde{e}) = \check{a}^{\top}f(\widetilde{e}) = \check{a}^{\top}(A_f^{\top}\widetilde{e}) = = (\check{a}^{\top}A_f^{\top})\widetilde{e} = (A_f\check{a})^{\top}\widetilde{e}$. Имеем, $f(\check{a})^{\top} = (A_f\check{a})^{\top} \Rightarrow f(\check{a}) = A_f\check{a}$. □

Определение 9.2.4. Матрица B называется подобной матрице A ($B \sim A$) над полем k, если существует не особенная матрица Q с элементами из поля k такая, что

$$B = Q^{-1}AQ.$$

Иногда говорят, что матрица B получена трансформированием матрицы A с помощью матрицы Q, или матрица B преобразована из матрицы A с помощью матрицы Q.

Замечание 9.2.1. Если матрицы B и A подобны, то они должны быть квадратными одинаковой размерности.

Предложение 9.2.2. *Отношение подобия является отношением эквивалентности на множестве* $M(n,k)$.

Доказательство. 1) *Рефлексивность.*

Имеем $A = E^{-1}AE$, тогда $A \sim A$, роль матрицы Q играет единичная матрица.

2) *Симметричность.*

Пусть $B \sim A$. Это означает, что $(\exists\ Q, |Q| \neq 0)\quad B = Q^{-1}AQ \Rightarrow$ $\Rightarrow QBQ^{-1} = Q(Q^{-1}AQ)Q^{-1} \Rightarrow QBQ^{-1} = A \Rightarrow A = (Q^{-1})^{-1}BQ^{-1} \Rightarrow$ $\Rightarrow A \sim B$, роль матрицы Q играет Q^{-1}.

3) *Транзитивность.*

Пусть $C \sim B$, $B \sim A$, тогда $(\exists\ R, |R| \neq 0)\quad C = R^{-1}BR$, и $(\exists\ Q, |Q| \neq 0)\quad B = Q^{-1}AQ$. Следовательно $C = R^{-1}(Q^{-1}AQ)R =$ $= (QR)^{-1}A(QR) \Rightarrow C \sim A$, роль матрицы Q играет QR. □

ТЕОРЕМА 9.2.3. *Матрицы одного и того же линейного оператора* f *в различных базисах подобны. При этом матрица* $A_{f|_{\widetilde{u}}}$ *получается из матрицы* $A_{f|_{\widetilde{e}}}$ *трансформированием при помощи матрицы перехода от базиса* $\widetilde{e}$ *к базису* $\widetilde{u}$*, то есть*

$$A_{f|_{\widetilde{u}}} = Q^{-1}A_{f|_{\widetilde{e}}}Q,$$

где Q *— матрица перехода от* $\widetilde{e}$ *к* $\widetilde{u}$.

Доказательство. Пусть $dim\ V = n$, $\widetilde{e}$ и $\widetilde{u}$ — два базиса пространства V, $f \in L(V)$, $A_{f|_{\widetilde{e}}}$ и $A_{f|_{\widetilde{u}}}$ — матрицы оператора f относительно $\widetilde{e}$ и $\widetilde{u}$

соответственно. Тогда

$$f(\widetilde{e}) = A^{\top}_{f|_{\widetilde{e}}}\widetilde{e}, \quad f(\widetilde{u}) = A^{\top}_{f|_{\widetilde{u}}}\widetilde{u}.$$

Пусть, наконец, Q — матрица перехода от $\widetilde{e}$ к $\widetilde{u}$, то есть $\widetilde{u} = Q^{\top}\widetilde{e}$. С одной стороны, $f(\widetilde{u}) = f(Q^{\top}\widetilde{e}) = Q^{\top}f(\widetilde{e}) = Q^{\top}(A^{\top}_{f|_{\widetilde{e}}}\widetilde{e}) = (Q^{\top}A^{\top}_{f|_{\widetilde{e}}})\widetilde{e} = (A_{f|_{\widetilde{e}}}Q)^{\top}\widetilde{e}$. С другой стороны, $f(\widetilde{u}) = A^{\top}_{f|_{\widetilde{u}}}\widetilde{u} = A^{\top}_{f|_{\widetilde{u}}}(Q^{\top}\widetilde{e}) = (A^{\top}_{f|_{\widetilde{u}}}Q^{\top})\widetilde{e} = (QA_{f|_{\widetilde{u}}})^{\top}\widetilde{e}$. Таким образом, $(A_{f|_{\widetilde{e}}}Q)^{\top} = (QA_{f|_{\widetilde{u}}})^{\top} \Rightarrow QA_{f|_{\widetilde{u}}} = A_{f|_{\widetilde{e}}}Q \Rightarrow A_{f|_{\widetilde{u}}} = Q^{-1}A_{f|_{\widetilde{e}}}Q$. □

Следствие 9.2.3.1. Если A_f — матрица линейного оператора f относительно базиса $\widetilde{e}$ и $B \sim A_f$, то матрицу B можно рассматривать как матрицу линейного оператора f относительно некоторого другого базиса.

Доказательство. Действительно, так как $B \sim A_f$, то $(\exists\ Q, |Q| \neq \neq 0) \quad B = Q^{-1}A_fQ$. Рассмотрим новый базис $\widetilde{u} = Q^{\top}\widetilde{e}$. Так как Q — не особенная матрица, то $\widetilde{u}$ будет новым базисом. По теореме 9.2.3 имеем $A_{f|_{\widetilde{u}}} = Q^{-1}A_fQ = B$. □

9.3 Ранг и дефект линейного оператора

Пусть V и V' — два линейных пространства над полем k, пусть $f \in \in L(V, V')$.

Определение 9.3.1. Образом линейного оператора f ($Im\ f$) называется множество образов всех элементов пространства V. Ядром линейного оператора f ($Ker\ f$) называется множество тех векторов пространства V, которые при отображении f переводятся в ноль пространства V'.

Из этого определения видно, что

$$Im\ f = \{f(a)|\ a \in V\}, \qquad Ker\ f = \{a \in V|\ f(a) = 0\}.$$

Предложение 9.3.1. *Ядро и образ линейного оператора $f \in L(V, V')$ являются линейными подпространствами пространств V и V' соответственно.*

Доказательство. Действительно, $(\forall\ \alpha, \beta \in k, a, b \in Ker\ f)$ имеем

$$f(\alpha a + \beta b) = \alpha f(a) + \beta f(b) = \alpha \cdot 0 + \beta \cdot 0 = 0 \Rightarrow \alpha a + \beta b \in Ker\ f.$$

Это означает, что $Ker\ f$ является устойчивым подмножеством пространства V, следовательно, является его линейным подпространством.

Пусть $a', b' \in Im f$. Это означает, что $(\exists\, a, b \in V) \quad f(a) = a', f(b) = b'$. Тогда $(\forall\ \alpha, \beta \in k, a', b' \in Im\ f)$ имеем

$$\alpha a' + \beta b' = \alpha f(a) + \beta f(b) = f(\alpha a + \beta b) \in Im\ f.$$

Отсюда $Im\ f$ является устойчивым подмножеством пространства V', следовательно, является его линейным подпространством. □

Предложение 9.3.2. *Если V — конечномерное линейное пространство и $f \in L(V, V')$, то ядро и образ линейного оператора f являются конечномерными линейными пространствами.*

Доказательство. В самом деле, так как V конечномерное линейное пространство, то и любое его подпространство, в частности $Ker\ f$, так же является конечномерным.

Перейдем к образу $Im\ f$. Пусть $e_1, e_2, \ldots, e_n$ — базис пространства V. Тогда $V = \left\{ \sum\limits_{i=1}^{n} \alpha_i e_i \,\middle|\, \alpha_i \in k \right\}$. Тогда

$$Im\ f = f(V) = \left\{ \sum_{i=1}^{n} \alpha_i f(e_i) \right\} = L(\{f(e_1), \ldots, f(e_n)\}).$$

Но линейная оболочка, порожденная конечным числом векторов, является конечномерной и при этом

$$dim\ L(\{f(e_1), \ldots, f(e_n)\}) = rang\,\{f(e_1), \ldots, f(e_n)\}\,.$$

Следовательно, $Im\ f$ является конечномерным линейным пространством. □

Определение 9.3.2. Если V — конечномерное линейное пространство и $f \in L(V, V')$, то рангом линейного оператора f $r(f)$ называется размерность его образа, а дефектом линейного оператора f $d(f)$ называется размерность его ядра.

Из этого определения видно, что $r(f) = dim\ Im\ f$, а $d(f) = dim\ Ker\ f$.

Следствие. $r(f) = r\{f(e_1), \ldots, f(e_n)\}$.

Следствие. Если $f \in L(V)$, то ранг линейного оператора f равен рангу матрицы этого линейного оператора относительно любого базиса, то есть $r(f) = r(A_f)$.

Доказательство. Действительно, по предыдущему следствию имеем $r(f) = r\{f(e_1), \ldots, f(e_n)\}$. Рассмотрим стандартный изоморфизм $\sigma : V \to k^n$ относительно базиса $\widetilde{e}$. Тогда $(\forall\ a \in V)\quad \sigma(a) = \check{a}|_{\widetilde{e}}$. При изоморфизме ранг системы векторов не изменяется, поэтому

$$r\{f(e_1), \ldots, f(e_n)\} = r\left\{\check{f}(e_1)|_{\widetilde{e}}, \ldots, \check{f}(e_n)|_{\widetilde{e}}\right\} = r\left\{A_{f|_{\widetilde{e}}}\right\}.$$

□

ТЕОРЕМА 9.3.1 (о ранге и дефекте линейного оператора). *Если V — конечномерное линейное пространство, $dim\ V = n$, $f \in L(V, V')$, то сумма ранга и дефекта линейного оператора f равна размерности пространства V, то есть $r(f) + d(f) = n$.*

Доказательство. Введем обозначение $d = d(f) = dim\ Ker\ f$. Пусть $e_1, e_2, \ldots, e_d$ — базис $Ker\ f$. Дополним этот базис до базиса пространства V, получим $e_1, e_2, \ldots, e_d, e_{d+1}, \ldots, e_n$ — базис V. По следствию к предложению 9.3.2 имеем

$$r(f) = r\{f(e_1), f(e_2), \ldots, f(e_d), f(e_{d+1}), \ldots, f(e_n)\} = r\{f(e_{d+1}), \ldots, f(e_n)\}.$$

Покажем, что векторы $f(e_{d+1}), \ldots, f(e_n)$ являются линейно независимыми. Пусть

$$\alpha_{d+1} f(e_{d+1}) + \ldots + \alpha_n f(e_n) = 0;$$

$$f(\alpha_{d+1} e_{d+1} + \ldots + \alpha_n e_n) = 0 \Rightarrow \alpha_{d+1} e_{d+1} + \ldots + \alpha_n e_n \in Ker\ f.$$

Разложим этот элемент по базису $Ker\ f$. Имеем

$$\alpha_{d+1} e_{d+1} + \ldots + \alpha_n e_n = \beta_1 e_1 + \ldots + \beta_d e_d;$$

$$-\beta_1 e_1 - \ldots - \beta_d e_d + \alpha_{d+1} e_{d+1} + \ldots + \alpha_n e_n = 0.$$

Так как $e_1, e_2, \ldots, e_n$ — базис пространства V, то $\beta_1 = \ldots = \beta_d = \alpha_{d+1} = \ldots = \alpha_n = 0$. Таким образом, векторы $f(e_{d+1}), \ldots, f(e_n)$ являются линейно независимыми. Тогда $r(f) = r\{f(e_{d+1}), \ldots, f(e_n)\} = n - d \Rightarrow$ $\Rightarrow r(f) + d(f) = n - d + d = n$. □

9.4 Обратимость линейного оператора

Пусть V — линейное пространство над полем k. Рассмотрим алгебру $L(V)$. В этой алгебре есть единица, роль единицы выполняет тождественный оператор 1_V. Напомним, что $(\forall\ a \in V) \quad 1_V(a) = a$.

Определение 9.4.1. Линейный оператор $f \in L(V)$ называется обратимым, если он обратим как элемент мультипликативной полугруппы кольца $L(V)$, то есть $(\exists\ f^{-1} \in L(V)) \quad ff^{-1} = f^{-1}f = 1_V$.

ТЕОРЕМА 9.4.1 (критерий обратимости линейного оператора). *Для того, чтобы линейный оператор $f \in L(V)$ был обратимым необходимо и достаточно, чтобы он как отображение был биективным. Другими словами, f — обратим тогда и только тогда, когда f — изоморфизм из V в V.*

Доказательство. 1) *Необходимость.*

Пусть $f \in L(V)$ является обратимым. По определению 9.4.1 $(\exists\ f^{-1} \in L(V)) \quad ff^{-1} = f^{-1}f = 1_V$. Надо показать, что f является биекцией. Пусть $f(a) = f(b)$. Применим к этому равенству отображение f^{-1}, получим $f^{-1}(f(a)) = f^{-1}(f(b)) \Rightarrow (f^{-1}f)(a) = (f^{-1}f)(b) \Rightarrow 1_V(a) = 1_V(b) \Rightarrow$ $\Rightarrow a = b$. Пусть $b \in V$. Надо показать, что $(\exists\ a \in V) \quad f(a) = b$. Построим по данному вектору b вектор $a = f^{-1}(b)$. Тогда $f(a) = f(f^{-1}(b)) =$ $= (ff^{-1})(b) = 1_V(b) = b$, то есть f является биекцией.

2) *Достаточность.*

Пусть $\in L(V)$ и f является биекцией. Тогда $(\exists\ f^{-1} : V \to V) \quad ff^{-1} =$ $= ff^{-1} = 1_V$. Это отображение f^{-1} также является биекцией. Надо показать, что $f^{-1} \in L(V)$, то есть f^{-1} удовлетворяет условиям линейности. Пусть $a, b \in V$, тогда $(\exists\ a', b' \in V) \quad f(a') = a, f(b') = b$. Отсюда $f^{-1}(a) = a',\ f^{-1}(b) = b'$. Возьмем произвольные $\alpha, \beta \in k$, сосчитаем

$$f(\alpha a' + \beta b') = \alpha f(a') + \beta f(b') = \alpha a + \beta b \Rightarrow$$

$$\Rightarrow f^{-1}(\alpha a + \beta b) = \alpha a' + \beta b' = \alpha f^{-1}(a) + \beta f^{-1}(b).$$

Отображение f^{-1} удовлетворяет условиям линейности, следовательно $f^{-1} \in L(V)$. □

9.5 Характеристический многочлен матрицы и линейного оператора

Пусть k —основное поле и $k[\lambda]$ — кольцо многочленов от неизвестного λ.

Определение 9.5.1. λ-матрицей (многочленной матрицей) над полем k называется матрица, элементами которой являются элементы кольца $k[\lambda]$, то есть многочлены от λ с коэффициентами из поля k.

λ-матрицы можно складывать, умножать, умножать на скаляры по тем же правилам, что и скалярные матрицы. Пусть теперь $A =$ $= (\alpha_{ij}),\ \alpha_{ij} \in k,\ i, j = \overline{1, n}$. Такие матрицы будем называть скалярными.

Определение 9.5.2. Характеристической матрицей для квадратной скалярной матрицы A называется λ-матрица вида $\lambda E - A$, то есть

$$\lambda E - A = \begin{pmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \dots & -\alpha_{1n} \\ \alpha_{21} & \lambda - \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ -\alpha_{n1} & -\alpha_{n2} & \dots & \lambda - \alpha_{nn} \end{pmatrix}.$$

Определение 9.5.3. Характеристическим многочленом для скалярной матрицы A называется определитель, порожденный характеристической матрицей для матрицы A.

Характеристический многочлен матрицы A обозначается через $\chi_A(\lambda) = |\lambda E - A|$.

Определение 9.5.4. Следом квадратной скалярной матрицы A ($Tr(A)$) называется сумма элементов ее главной диагонали. Нормой матрицы A ($N(A)$) называется ее определитель.

Это определение означает, что

$$Tr(A) = \alpha_{11} + \alpha_{22} + \ldots + \alpha_{nn}, \qquad N(A) = |A|.$$

Ясно, что $Tr(\alpha A + \beta B) = \alpha Tr(A) + \beta Tr(B)$; $N(AB) = N(A) \cdot N(B)$.

ТЕОРЕМА 9.5.1 (о строении характеристического многочлена). *Характеристический многочлен для скалярной матрицы A является нормированным многочленом от λ степени n, имеющим следующий вид:* $\chi_A(\lambda) = \lambda^n - Tr(A)\lambda^{n-1} + \ldots + (-1)^n N(A)$.

Доказательство. Имеем,

$$\chi_A(\lambda) = \begin{vmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \dots & -\alpha_{1n} \\ \alpha_{21} & \lambda - \alpha_{22} & \dots & \alpha_{2n} \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots \\ -\alpha_{n1} & -\alpha_{n2} & \dots & \lambda - \alpha_{nn} \end{vmatrix} =$$

$$\underbrace{(\lambda-\alpha_{11})(\lambda-\alpha_{22})\dots(\lambda-\alpha_{nn})}_{(*)}+\text{ еще }(n!-1)\text{ слагаемых.}$$

В оставшихся $(n!-1)$ слагаемых отсутствует по крайней мере два элемента главной диагонали. Поэтому оставшиеся слагаемые могут дать степень у λ не выше, чем $n-2$. Слагаемые с λ^n и с λ^{n-1} получаются за счет произведения $(*)$. В произведение $(*)$ λ^n входит с коэффициентом 1. Коэффициент при λ^{n-1} равен $-\alpha_{11}-\alpha_{22}-\ldots-\alpha_{nn}=-Tr(A)$. Получаем $\chi_A(\lambda)=\lambda^n-Tr(A)\lambda^{n-1}+\alpha_{n-2}\lambda^{n-2}+\ldots+\alpha_1\lambda+\alpha_0$, где $\alpha_0=\chi_A(0)=$ $=|0\cdot E-A|=|-A|=(-1)^n|A|=(-1)^nN(A)$. □

Определение 9.5.5. Характеристическими корнями (числами) матрицы A называются все n корней ее характеристического многочлена, лежащие, вообще говоря, в алгебраическом замыкании основного поля k.

Замечание 9.5.1. В самом основном поле k может вообще не быть характеристических корней, или их может быть меньше, чем n.

Пример: $k=\mathbb{R}$,

$$A=\begin{pmatrix}1 & -2\\ 1 & -1\end{pmatrix};$$

$$\chi_A(\lambda)=\begin{vmatrix}\lambda-1 & 2\\ -1 & \lambda+1\end{vmatrix}=\lambda^2-1+2=\lambda^2+1.$$

$\chi_A(\lambda)=0\Rightarrow\lambda^2+1=0\Rightarrow\lambda_1=i,\ \lambda_2=-i$. Видно, что $\lambda_1,\lambda_2\notin$ $\notin\mathbb{R},\ \lambda_1,\lambda_2\in\overline{\mathbb{R}}=\mathbb{C}$. В дальнейшем характеристические корни матрицы A будем обозначать $\lambda_1,\lambda_2,\dots,\lambda_n$.

Следствие 9.5.1.1. Сумма характеристических корней матрицы A равно ее следу, а произведение характеристических корней равно ее норме.

Доказательство. Это вытекает из теоремы 9.5.1 и теоремы Виета. Действительно,

$$\lambda_1+\lambda_2+\ldots+\lambda_+n=-(-Tr(A))=Tr(A),$$

$$\lambda_1, \lambda_2, \ldots, \lambda_n = (-1)^n \cdot (-1)^n \cdot N(A) = N(A).$$

□

Следствие 9.5.1.2. Квадратная матрица A не особенная тогда и только тогда, когда все ее характеристические числа отличны от нуля.

Доказательство. В самом деле, $|A| \neq 0 \Leftrightarrow N(A) \neq 0 \Leftrightarrow \lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_n \neq 0 \Leftrightarrow (\forall\ 1 \leqslant i \leqslant n) \quad \lambda_i \neq 0.$ □

Пусть V — конечномерное линейное пространство над k и $f \in L(V)$. Пусть $\tilde{e}$ — базис V и $A_{f|_{\tilde{e}}}$ — матрица f относительно базиса $\tilde{e}$. Так как эта матрица зависит от базиса, то понятие характеристической матрицы для линейного оператора не вводится.

Предложение 9.5.1. *Характеристические многочлены подобных матриц равны.*

Доказательство. Пусть $B \sim A$, то есть $(\exists\ Q, |Q| \neq 0) \quad B = Q^{-1}AQ$. Рассмотрим характеристический многочлен матрицы B. $\chi_B(\lambda) = |\lambda E - B| = |\lambda E - Q^{-1}AQ| = |Q^{-1}(\lambda E)Q - Q^{-1}AQ| = |Q^{-1}(\lambda E - A)Q| = |Q^{-1}||\lambda E - A||Q| = |\lambda E - A| = \chi_A(\lambda).$ □

Следствие. Следы и нормы подобных матриц равны.

Следствие. Характеристический многочлен матрицы линейного оператора не зависит от выбора базиса, относительно которого строилась матрица оператора, а зависит только от самого линейного оператора.

Определение 9.5.6. Характеристическим многочленом линейного оператора называется характеристический многочлен матрицы этого линейного оператора относительно любого базиса.

Обозначим характеристический многочлен линейного оператора f через $\chi_f(\lambda)$. Тогда $\chi_f(\lambda) = \chi_{A_f}(\lambda)$.

Определение 9.5.7. Следом $Tr(f)$ и нормой $N(f)$ линейного оператора f называется след и норма матрицы этого линейного оператора относительно любого базиса.

Определение 9.5.8. Характеристическимим корнями линейного оператора называются все корни характеристического многочлена этого линейного оператора, лежащие, в общем случае, в алгебраическом замыкании основного поля.

9.6 Собственные векторы и собственные значения линейного оператора и матрицы

Пусть V — линейное пространство над полем k, $f \in L(V)$. Пусть V' — линейное подпространство пространства V. В общем случае $f(V') \subset V$, но может быть так, что $f(V') \subset V'$.

Определение 9.6.1. Подпространство V' линейного пространства V называется инвариантным относительно линейного оператора $f \in L(V)$, если $f(V') \subset V'$, то есть любой вектор из подпространства V' переходит в вектор того же подпространства.

Займемся изучением одномерных инвариантных подпространств. Пусть V' — одномерное инвариантное подпространство. Возьмем любой вектор $a \in V', a \neq 0$. Так как $dim\ V' = 1$, то вектор a можно взять в качестве базиса V' и тогда $V' = \{\alpha a | \alpha \in k\}$. $f(a)$ будет принадлежать V', так как V' инвариантно. Тогда $f(a) = \alpha a,\ a \neq 0, \alpha \in k$.

Обратно, пусть V' — одномерное подпространство и $a \neq 0,\ a \in V',\ f(a) = \alpha a$, где $\alpha \in k$. Так как V' — одномерное подпространство, то a можно взять в качестве базиса V'. Поэтому $V' = \{\beta a | \beta \in k\}$. Сосчитаем $f(\beta a) = \beta f(a) = \beta(\alpha a) = (\beta\alpha)a \in V'$. Таким образом $f(V') \subset V'$, то есть V' — инвариантное подпространство. Таким образом изучение одномер-

ных инвариантных подпространств приводит нас к изучению ненулевых векторов $a \in V'$, для которых $f(a) = \alpha a$, где $\alpha \in k$.

Определение 9.6.2. Скаляр α называется собственным значением линейного оператора $f \in L(V)$, если существует ненулевой вектор $a \in V$ такой, что $f(a) = \alpha a$. В этом случае вектор a называется собственным вектором линейного оператора f, принадлежащим скаляру α.

В этом случае говорят, что α и a есть принадлежащие друг другу собственное значение и собственный вектор линейного оператора f.

Определение 9.6.3. Говорят, что скаляр α и ненулевой столбец $X \neq 0$ из k^n есть принадлежащие друг другу собственное значение и собственный вектор матрицы $A \in M(n, k)$, если $AX = \alpha X$.

Предложение 9.6.1. *Для того, чтобы скаляр α и вектор $a \in V$ были принадлежащими друг другу собственным значением и собственным вектором линейного оператора f конечномерного линейного пространства V необходимо и достаточно, чтобы α и координатный столбец $\check{a}$ относительно некоторого базиса были принадлежащими друг другу собственным значением и собственным вектором матрицы A_f этого линейного оператора относительно того же базиса.*

Доказательство. Действительно, пусть $f(a) = \alpha a$, где $a \neq 0$ и $\alpha \in k$, тогда $f(a) = \alpha a \Leftrightarrow f\check{(a)} = \alpha\check{a} \Leftrightarrow A_f\check{a} = \alpha\check{a}$. Причем $\check{a} \neq 0 \Leftrightarrow a \neq 0$. $\square$

ТЕОРЕМА 9.6.1 (критерий собственного значения). *Для того, чтобы скаляр α был собственным значением матрицы A (линейного оператора конечномерного пространства) необходимо и достаточно, чтобы α был характеристическим корнем матрицы A (линейного оператора), лежащим в основном поле.*

Доказательство. 1) *Необходимость.*

Пусть α является собственным значением матрицы A, это означает, что

$$AX = \alpha X, \tag{9.2}$$

где $X \neq 0$ и $X \in k^n$. Перепишем равенство (9.2):

$$\alpha EX - AX = 0,$$

$$(\alpha E - A)X = 0. \tag{9.3}$$

На равенство (9.3) можно смотреть как на однородную систему n-линейных уравнений с n неизвестными. Эта система записана в матричном виде. Видно, что ненулевым решением этой системы является столбец $X \in k^n,\ X \neq 0$. Тогда по следствию из критерия наличия ненулевого решения ОСЛУ следует, что определитель системы (9.3) должен быть равен нулю, то есть $|\alpha E - A| = 0$. Таким образом $\chi_A(\alpha) = 0$, следовательно α является характеристическим корнем матрицы A и $\alpha \in k$.
2) *Достаточность.*

Пусть $\alpha \in k$ и α является характеристическим корнем матрицы A. Тогда $\chi_A(\alpha) = 0$, это означает, что $|\alpha E - A| = 0$. Рассмотрим однородную систему n-линейных уравнений с n неизвестными (9.3)

$$(\alpha E - \alpha)X = 0,$$

где X — столбец неизвестных. По следствию из критерия наличия ненулевого решения ОСЛУ следует, что эта система (9.3) имеет ненулевое решение $X \neq 0$. Это ненулевое решение $X \in k^n$, так как элементы матрицы $(\alpha E - A)$ принадлежат полю k. Подставив это ненулевое решение в систему (9.3) получим тождество. Будем иметь $\alpha EX - AX = 0$, то есть $AX = \alpha X$, где $X \neq 0$ и $X \in k^n$. По определению 9.6.2 видно, что α является собственным значением матрицы A. □

Следствие 9.6.1.1. Если основное поле k алгебраически замкнуто, то все собственные значения матрицы A совпадают с ее характеристическими корнями.