А.М. Водолазов, О.А. Королева, В.В. Кривобок

А Л Г Е Б Р А.

ЧАСТЬ II

Саратовский государственный университет им. Н.Г. Чернышевского

А.М. Водолазов, О.А. Королева, В.В. Кривобок

А Л Г Е Б Р А.

ЧАСТЬ II

Учебное пособие по курсу «Алгебра» для студентов механико-математического факультета и факультета компьютерных наук и информационных технологий

ИЗДАТЕЛЬСТВО «АМИРИТ»

2017

УДК 512.5

Водолазов А.М., Королева О.А., Кривобок В.В.

Алгебра. Часть II: Учеб. пособие для студ.мех.-мат.фак.

и фак. КНиИТ — Саратов: Изд-во «Амирит»,2017.— 64 с.: ил.

ISBN

В учебном пособии отражены основные темы второго семестра курса «Алгебра»: многочлены, квадратичные формы.

Для студентов младших курсов механико-математического факультета и факультета компьютерных наук и информационных технологий, изучающих курс «Алгебра».

Рекомендуют к печати:

Кафедра компьютерной алгебры и теории чисел

механико-математического факультета

Саратовского государственного университета

Доктор физико-математических наук *Ю.А. Блинков*

Доктор физико-математических наук *Д.А. Бредихин*

УДК 512.5

Работа издана в авторской редакции

ISBN

СОДЕРЖАНИЕ

Введение

Учебное пособие соответствует материалу, изучаемому студентами в курсе «Алгебра» механико-математического факультета и факультета компьютерных наук и информационных технологий. В нем отражены темы, рассматриваемые в этом курсе: многочлены и квадратичные формы.

Учебное пособие содержит курс лекций по предлагаемым разделам и может быть использовано при подготовке к экзамену по предмету «Алгебра» во втором семестре, а так же при самостоятельной работе студентов, обучающихся по заочной форме обучения.

Для более подробного изучения теоретического материала может быть рекомендована следующая литература:

1. *Воеводин В.В.* Линейная алгебра. М., 1974.
2. *Курош А.Г.* Курс высшей алгебры. М., 1975.
3. *Ильин В.А., Позняк Э.Г.* Линейная алгебра. М., 1978.
4. *Проскуряков И.В.* Сборник задач по линейной алгебре. М., 1970.
5. *Фадеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. М., 1968.

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

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

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 $\underline{\deg f \cdot g = \deg f + \deg g}$.

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 $\beta f_1 = q\alpha g_1 \Rightarrow f_1 = (\beta^{-1} q\alpha) g_1 \Rightarrow g_1 | f_1$. □

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*

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

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 $\bar{d} = \mathcal{НОД}\{d, f_s\}$. 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 $\bar{d} = \mathcal{НОД}\{f_1, f_2, \ldots, f_{s-1}, f_s\}$. □

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 $f = \alpha P_1^{k_1} \cdot \cdot P_2^{k_2} \cdot \ldots \cdot P_t^{k_t}$ 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'', ..., $x-\gamma$ 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. $\square$

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

Квадратичные формы

7.1 Многочлены от n неизвестных

Пусть k — основное поле, $x_1, x_2, \ldots, x_n$ — символы неизвестных.

Определение 7.1.1. Одночленом он неизвестных $x_1, x_2, \ldots, x_n$ называется выражение вида $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, где $i_1, i_2, \ldots, i_n$ — целые неотрицательные числа.

В дальнейшем, ради краткости, обозначим набор $(i_1, i_2, \ldots, i_n) = i$, а $x^i = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$.

Определение 7.1.2. Произведение одночленов x^i и x^j назовем одночлен x^{i+j}.

Определение 7.1.3. Многочленом от неизвестных над полем k называется всякая конечная линейная комбинация одночленов с коэффициентами из поля k.

Определение 7.1.3 означает, что

$$F(x_1, x_2, \ldots, x_n) = \sum_{i \in \mathbb{Z}_+^n} \alpha_i x^i,$$

где $\alpha_i \in k$, и почти все α_i равны нулю. $\alpha_i x^i$ — члены многочлена F. Если все α_i равны нулю, то F называется нулевым, $F = 0$.

Множество всех многочленов от неизвестных $x_1, x_2, \ldots, x_n$ над полем k обозначается $k[x_1, x_2, \ldots, x_n]$. Это множество становится кольцом, и даже областью целостности, если в нем ввести операции сложения и умножения многочленов. При сложении многочленов, складываются коэффициенты при одинаковых степенях x^i, умножение определяется по дистрибутивности, с помощью определения 7.1.2 умножения одночленов и последующего приведения подобных членов. Это означает, что

$$\sum_{(i)} \alpha_i x^i + \sum_{(i)} \beta_i x^i = \sum_{(i)} (\alpha_i + \beta_i) x^i,$$

$$\sum_{(i)} \alpha_i x^i \cdot \sum_{(j)} \beta_j x^j = \sum_{(i)} \sum_{(j)} \alpha_i \beta_j x^{i+j}.$$

Определение 7.1.4. Степенью одночлена $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ называется сумма $i_1 + i_2 + \ldots + i_n$. Степенью ненулевого многочлена F называется максимум из степеней его членов.

Само поле k является подкольцом кольца $k[x_1, x_2, \ldots, x_n]$. 0_k поля k рассматривается как нулевой многочлен, а любой элемент $a \in k^*$ рассматривается как многочлен нулевой степени, а именно $a = a x_1^0 x_2^0 \ldots x_n^0$.

Определение 7.1.5. Однородным многочленом (или формой) степени α от неизвестных $x_1, x_2, \ldots, x_n$ называется ненулевой многочлен $F(x_1, x_2, \ldots, x_n)$, все члены которого имеют степень α, то есть

$$F(x_1, x_2, \ldots, x_n) = \sum_{i_1 + i_2 + \ldots + i_n = \alpha} \alpha_i x^i.$$

В частности, линейная форма, или форма первой степени, имеет вид $F = \alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n$, где $\alpha_i \in k$.

7.2 Линейные преобразования неизвестных

Пусть k — основное поле, $k[x_1, x_2, \ldots, x_n]$ — кольцо многочленов и $F(x_1, x_2, \ldots, x_n)$ — многочлен из $k[x_1, x_2, \ldots, x_n]$. Рассмотрим n линей-

ных форм от новых неизвестных $y_1, y_2, \ldots, y_n$

$$\begin{aligned} x_1 &= \alpha_{11}y_1 + \alpha_{12}y_2 + \ldots + \alpha_{1n}y_n; \\ x_2 &= \alpha_{21}y_1 + \alpha_{22}y_2 + \ldots + \alpha_{2n}y_n; \\ &\ldots \\ x_n &= \alpha_{n1}y_1 + \alpha_{n2}y_2 + \ldots + \alpha_{nn}y_n. \end{aligned} \tag{7.1}$$

Если в многочлене F вместо $x_1, x_2, \ldots, x_n$ подставить их выражения по формулам (7.1) и произвести указанные действия, то мы получим новый многочлен $G(y_1, y_2, \ldots, y_n)$.

Определение 7.2.1. Линейным преобразованием L неизвестных $x_1, x_2, \ldots, x_n$ в неизвестные $y_1, y_2, \ldots, y_n$ по формулам (7.1) называется сопоставление каждому многочлену $F(x_1, x_2, \ldots, x_n)$ многочлена $FL(y_1, y_2, \ldots, y_n)$, получающегося из многочлена F заменой $x_1, x_2, \ldots, x_n$ их значениями по формулам (7.1) и выполнением соответствующих действий.

Линейные преобразования будем обозначать L, L_1, L', M и будем писать $L : x \to y$. Через FL будем обозначать многочлен, получающийся из многочлена F с помощью преобразования L.

Определение 7.2.2. Матрицей линейного преобразования $L : x \to y$ выполненного по формулам (7.1), называется матрица, составленная из коэффициентов линейного выражения старых неизвестных $x_1, x_2, \ldots, x_n$ через новые неизвестные $y_1, y_2, \ldots, y_n$.

Матрицу линейного преобразования L будем обозначать через

$$A_L = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix}, \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix}.$$

Определение 7.2.3. Линейное преобразование L неизвестных x_i в неизвестные y_i с матрицей A называется преобразование вида $X = AY$.

Определение 7.2.4. Произведением линейного преобразования $L : x \to y$ на линейное преобразование $M : y \to z$, называется последовательное выполнение сначала преобразования L, а затем преобразования M.

Это определение означает, что $(F)LM = (FL)M$.

Предложение 7.2.1. *Произведение линейных преобразование неизвестных является линейным преобразованием, матрица которого равна произведению матриц данных преобразований.*

Доказательство. Пусть $L : x \to y$ по формуле $X = A_L Y$, а $M : y \to z$ по формуле $Y = A_M Z$. Рассмотрим многочлен $F(X)$ и подействуем на него преобразованием LM, получим

$$(F(X))LM = (F(X)L)M = (F(A_L Y))M = F(A_L(A_M Z)) = F((A_L A_M)Z).$$

Мы видим, что $LM : x \to z$ по формуле $X = A_L A_M Z$, тогда по определению 7.2.3 LM является линейным преобразованием неизвестных $x \to z$ с матрицей $A_{LM} = A_L A_M$. □

Определение 7.2.5. Тождественным линейным преобразованием неизвестных называется линейное преобразование, матрица которой равна единичной матрице.

Тождественное преобразование будем обозначать через 1_L. Из определения $A_{1_L} = E$, то есть $1_L : \ x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$.

Определение 7.2.6. Линейное преобразование неизвестных L называется невырожденным (неособенным) если его матрица A_L является неособенной, то есть $|A_L| \neq 0$.

С точностью до обозначения неизвестных, между множеством линейных преобразований $\{L\}$, рассмотренного вместе с операцией умножения, и множеством $(M(n,k), \cdot)$ можно установить изоморфизм $f : L \to$

A_L. Поэтому каждому понятию или свойству, относящемуся к матрицам, соответствует такое же понятие или свойство линейных преобразований. Ввиду этого, можно высказать ряд утверждений.

Утверждение 7.2.1. *Умножение линейных преобразований ассоциативно.*

Утверждение 7.2.2. *Произведение нескольких линейных преобразований невырожденно тогда и только тогда, когда каждое из перемножаемых линейных преобразований является невырожденным.*

Утверждение 7.2.3. *Линейное преобразование L невырожденно тогда и только тогда, когда оно допускает обратное линейное преобразование L^{-1} такое, что $LL^{-1} = L^{-1}L = 1_L$.*

Утверждение 7.2.4. *Матрица обратного линейного преобразования равна обратной матрице для первоначального преобразования, то есть $A_{L^{-1}} = A_L^{-1}$.*

Утверждение 7.2.5. *Невырожденные линейные преобразования образуют группу по умножению, изоморфную группе неособенных квадратных матриц.*

7.3 Квадратичная форма, ее матрица и ранг

Пусть k — основное поле. Характеристика $k \neq 2$, $k[x_1, x_2, \ldots, x_n]$ — кольцо многочленов от n неизвестных над полем k.

Определение 7.3.1. Квадратичной формой от n неизвестных $x_1, x_2, \ldots, x_n$ над полем k называется форма второй степени над полем k, то есть однородный многочлен второй степени от неизвестных $x_1, x_2, \ldots, x_n$ над полем k.

Определение 7.3.2. Квадратичной формой от неизвестных $x_1, x_2, \ldots, x_n$ над полем k называется многочлен от неизвестных $x_1, x_2, \ldots, x_n$ с коэффициентами из поля k следующего вида

$$F(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \beta_i x_i^2 + \sum_{1 \leqslant i < j \leqslant n} \beta_{ij} x_i x_j. \tag{7.2}$$

Придадим записи (7.2) так называемый стандартный вид, для этого обозначим

$$\alpha_{ii} = \beta_i, \quad \alpha_{ij} = \frac{1}{2}\beta_{ij}, \quad \text{а вторую половину} \quad \frac{1}{2}\beta_{ij} = \alpha_{ji}. \tag{7.3}$$

Формулы (7.3) показывают, что члены многочлена (7.2) примут вид:

$$\beta_i x_i^2 = \alpha_{ii} x_i x_i, \quad \beta_{ij} x_i x_j = \frac{1}{2}\beta_{ij} x_i x_j + \frac{1}{2}\beta_{ij} x_i x_j = \alpha_{ij} x_i x_j + \alpha_{ji} x_j x_i,$$

$$F(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \alpha_{ii} x_i x_i + \sum_{1 \leqslant i < j \leqslant n} \alpha_{ij} x_i x_j + \sum_{1 \leqslant i < j \leqslant n} \alpha_{ji} x_j x_i =$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j \tag{7.4}$$

Предложение 7.3.1. *Всякую квадратичную форму вида (7.2) можно привести к виду (7.4) с помощью формул (7.3).*

Определение 7.3.3. Запись квадратичной формы $F(x_1, x_2, \ldots, x_n)$ в виде (7.4) с условием, что $\alpha_{ij} = \alpha_{ji}$, $\forall i, j = \overline{1, n}$ называется стандартной формой записи.

Определение 7.3.4. Матрицей квадратичной формы $F(x_1, x_2, \ldots, x_n)$ называется матрица, составленная из коэффициентов при произведениях неизвестных в ее стандартной форме записи.

Обозначим

$$A_F = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix},$$

Пример.

$$F(x_1, x_2) = 2x_1^2 + 4x_1x_2 + 5x_2^2 = 2x_1x_1 + 2x_1x_2 + 2x_2x_1 + 5x_2x_2,$$

$$A_F = \begin{pmatrix} 2 & 2 \\ 2 & 5 \end{pmatrix}.$$

Ясно, что матрица A_F квадратичной формы является симметрической. Каждой квадратичной форме соответствует симметрическая матрица A_F. Каждой симметрической матрице A_F соответствует квадратичная форма F, поэтому между множеством квадратичных форм от n неизвестных и множеством симметрических матриц n-порядка существует взаимнооднозначное соответствие (биекция).

Определение 7.3.5. Рангом квадратичной формы $F(x_1, x_2, \ldots, x_n)$ называется ранг матрицы этой квадратичной формы $r(F)$, то есть $r(F) = r(A_F)$.

Определение 7.3.6. Дискриминантом квадратичной формы $F(x_1, x_2, \ldots, x_n)$ называется определитель матрицы этой квадратичной формы $D(F)$, то есть $D(F) = |A_F|$.

Определение 7.3.7. Квадратичная форма $F(x_1, x_2, \ldots, x_n)$ называется невырожденной, если матрица этой квадратичной формы неособенна.

Следствие. Квадратичная форма $F(x_1, x_2, \ldots, x_n)$ является неособенной, тогда и только тогда, когда ее дискриминант не равен 0 или, тогда и только тогда, когда ее ранг равен числу неизвестных.

7.4 Влияние линейного преобразования на квадратичную форму

Пусть F — квадратичная форма с матрицей A, то есть

$$F = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j,$$

как всегда через $X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$, будем обозначать столбец неизвестных, тогда $X^T = (x_1, x_2, \dots, x_n)$.

Предложение 7.4.1. *Квадратичную форму F с матрицей A можно записать в виде $F = X^T AX$.*

Доказательство. AX является столбцом размерности $n \times 1$. В i-строке этого столбца

$$(AX)_i = \sum_{j=1}^{n} \alpha_{ij} x_j,$$

тогда

$$X^T(AX) = \sum_{i=1}^{n} x_i \left(\sum_{j=1}^{n} \alpha_{ij} x_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j.$$

□

ТЕОРЕМА 7.4.1 (о влиянии линейного преобразования)**.** *Пусть F — квадратичная форма с матрицей A и L — линейное преобразование неизвестных $L : x \to y$ с матрицей Q, тогда*

1. *FL является квадратичной формой с матрицей $Q^T AQ$, то есть $A_{FL} = A_L^T A_F A_L$;*
2. *$D(FL) = D(F)|Q|^2$;*
3. *если L — невырожденное линейное преобразование, то $r(FL) = r(F)$, то есть формы FL и F одновременно вырождены или не вырождены.*

Доказательство. 1. По предположению $F = X^T AX$. Далее линейное преобразование $L : x \to y$ происходит по формуле $X = QY$, тогда

$$FL = (QY)^T AQY = (Y^T Q^T) A (QY) = Y^T (Q^T AQ) Y,$$

то есть $FL = Y^T BY$, где $B = Q^T AQ$. Покажем, что матрица B является симметрической

$$B^T = (Q^T AQ)^T = Q^T A^T (Q^T)^T = Q^T AQ = B.$$

Видно, что FL является квадратичной формой от неизвестных $y_1, y_2, \ldots, y_n$ с матрицей $A_{FL} = Q^T AQ$.

2. Подсчитаем $D(FL)$.

$$D(FL) = |A_{FL}| = |Q^T AQ| = |Q^T| \cdot |A| \cdot |Q| = D(F)|Q|^2.$$

3. Видно, что матрица $A_{FL} = Q^T AQ$ получается из матрицы A умножением слева и справа на не особенные матрицы. $|Q| \neq 0$ так как L — невырожденное преобразование. По теореме о ранге произведений матриц $r(A_{FL}) = r(A)$, то есть $r(FL) = r(F)$. □

7.5 Приведение квадратичной формы к каноническому виду

Определение 7.5.1. Квадратичная форма F имеет канонический вид, если матрица A_F этой формы является диагональной, то есть

$$A_L = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}.$$

Это означает, что

$$F = \sum_{i=1}^{n} \alpha_i x_i^2.$$

Причем среди чисел $\alpha_1, \alpha_2, \ldots, \alpha_n$ могут быть и нули.

Следствие. Ранг канонической квадратичной формы равен числу отличных от нуля коэффициентов при квадратах неизвестных.

Доказательство. $r(F) = r(A_F) =$ количеству неравных нулю элементов α_i. □

Определение 7.5.2. Квадратичная форма F имеет нормальный вид, если матрица этой формы является единичной, то есть $A_F = E$, то есть $F = x_1^2 + x_2^2 + \ldots + x_n^2$.

Определение 7.5.3. Линейное преобразование $L : x \to y$ приводит квадратичную форму F к каноническому виду, если квадратичная форма FL имеет канонический вид. В этом случае, если L является невырожденным линейным преобразованием, то FL называют каноническим видом формы F.

Замечание 7.5.1. Канонический вид квадратичной формы F определяется неоднозначно. Этот вид существенно зависит от применяемого невырожденного преобразования неизвестных.

ТЕОРЕМА 7.5.1 (Лагранжа)**.** *Любую квадратичную форму с помощью невырожденного линейного преобразования неизвестных можно привести к каноническому виду.*

Доказательство. Доказательство проводим методом математической индукции по n.

1) Пусть $n = 1$, тогда $F = \alpha_{11}x_1^2$ — она уже имеет канонический вид $1_L : x = y$.

2) Предположим, что теорема верна для квадратичных форм, зависящих от $n-1$ неизвестных. Докажем ее справедливость для квадратичных форм, зависящих от n неизвестных.

Пусть $F = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} \alpha_{ij}x_ix_j$. Рассмотрим 2 случая.

а) Не все коэффициенты при квадратах неизвестных равны нулю. Пусть для определенности $\alpha_{nn} \neq 0$. Запишем выражение для формы

F, выделив в ней члены, содержащие x_n, получим

$$F = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1}\alpha_{ij}x_ix_j + 2\sum_{i=1}^{n-1}\alpha_{in}x_ix_n + \alpha_{nn}x_n^2 = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1}\alpha_{ij}x_ix_j +$$

$$+\alpha_{nn}\left(x_n^2 + 2\sum_{i=1}^{n-1}(\alpha_{in}/\alpha_{nn})x_ix_n + \left(\sum_{i=1}^{n-1}(\alpha_{in}/\alpha_{nn})x_i\right)^2\right) -$$

$$-\alpha_{nn}\left(\sum_{i=1}^{n-1}(\alpha_{in}/\alpha_{nn})x_i\right)^2 = F_1(x_1, x_2, \ldots, x_{n-1}) +$$

$$+\alpha_{nn}\left(x_n + \sum_{i=1}^{n-1}(\alpha_{in}/\alpha_{nn})x_i\right)^2 =$$

$$= F_1(x_1, x_2, \ldots, x_{n-1}) + \alpha_{nn}^{-1}\left(\alpha_{nn}x_n + \sum_{i=1}^{n-1}\alpha_{in}x_i\right)^2.$$

Здесь $F_1(x_1, x_2, \ldots, x_{n-1})$ является квадратичной формой, зависящей от $n-1$ неизвестных. Рассмотрим линейное преобразование $L_1 : y \to x$, осуществляемое по формулам $y_i = x_i, \forall i = \overline{1, n-1}, y_n = \alpha_{1n}x_1 + \ldots + \alpha_{nn}x_n$. Это преобразование является невырожденным, так как $|A_{L_1}| = \alpha_{nn} \neq 0$, тогда существует обратное линейное преобразование $L_1^{-1} : x \to y$ так же являющееся невырожденным. Это преобразование L_1^{-1} переведет форму F к виду $FL_1^{-1} = F_1(y_1, y_2, \ldots, y_{n-1}) + \alpha_{nn}^{-1}y_n^2$, так как форма F_1 зависит от $n-1$ неизвестных, то к ней можно применить предположение индукции, а именно, существует M — невырожденное линейное преобразование $M : y \to z$, которое переводит форму F_1 в канонический вид $F_1M = \beta_1z_1^2 + \ldots + \beta_{n-1}z_{n-1}^2$. Тогда рассмотрим линейное преобразование $L_2 : y \to z$ по формулам для $n-1$ переменной $L_2 = M$, при $y_n = z_n$. Это преобразование L_2 является невырожденным, так как $|A_{L_2}| = \begin{vmatrix} A_M & 0 \\ 0 & 1 \end{vmatrix} = |A_M| \neq 0$. Это преобразование L_2 переводит форму FL_1^{-1} к виду $(FL_1^{-1})L_2 = \beta_1z_1^2 + \ldots + \beta_{n-1}z_{n-1}^2 + \alpha_{nn}^{-1}z_n^2$. Видно, что квадратичная форма F с помощью линейного преобразования $L = L_1^{-1}L_2$

приводится к каноническому виду, при этом преобразование L является невырожденным, как произведение двух невырожденных линейных преобразований.

b) Все коэффициенты при квадратах неизвестных в форме F равны нулю. В этом случае не все коэффициенты при произведениях $x_i x_j$ равны нулю, в противном случае $F = 0$, а это не есть квадратичная форма. Пусть $\alpha_{12} \neq 0$, значит форма имеет вид $F = 2\alpha_{12}x_1x_2 +$ слагаемые, каждый член которых содержит, по крайней мере, одно из неизвестных $x_3, x_4, \ldots, x_n$. Рассмотрим линейное преобразование неизвестных $L_1 : x \to z$ по формулам $x_1 = z_1 - z_2,\ x_2 = z_1 + z_2,\ x_i = z_i,\ \forall\, i = \overline{3,n}$. Это линейное преобразование невырожденное $|A_{L_1}| = 2 \neq 0$, $FL_1 = 2\alpha_{12}z_1^2 - 2\alpha_{12}z_2^2 +$ слагаемые, каждый член которых содержит, по крайней мере одну из неизвестных $z_3, z_4, \ldots, z_n$. Видно, что форма FL_1, содержит отличные от нуля коэффициенты при двух переменных, и эти два первые члена не могут уничтожаться с последующими слагаемыми. Тогда мы находимся в условиях первого рассмотренного случая. Следовательно, существует невырожденное линейное преобразование $L_2 : z \to y$, которое форму FL_1 переводит в канонический вид $(FL_1)L_2 = \alpha_1 y_1^2 + \alpha_2 y_2^2 + \ldots + \alpha_n y_n^2$. Форма F с помощью линейного преобразования $L = L_1L_2$ переводится в канонический вид. □

Следствие 7.5.1.1. Ранг квадратичной формы F равен количеству не равных нулю коэффициентов при квадратах неизвестных в любом ее каноническом виде.

Доказательство. Пусть $r(F) = r$. Переведем форму F с помощью невырожденного линейного преобразования L в канонический вид, получим $FL = \beta_1 y_1^2 + \ldots + \beta_n y_n^2$. По теореме 7.4.1 $r(FL) = r(F)$, поэтому $r(F) = r(A_{FL}) = r$. Последнее равенство равносильно тому, что среди элементов $\beta_1, \beta_2, \ldots, \beta_n$ ровно r штук отличных от нуля. □

Следствие 7.5.1.2. Любую квадратичную форму F ранга r над полем комплексных чисел C с помощью невырожденных линейных преобразований можно привести к сумме r квадратов.

Доказательство. Квадратичную форму F ранга r по следствию 7.5.1.1 с помощью невырожденного линейного преобразования можно привести к виду $FL_1 = \beta_1 y_1^2 + \ldots + \beta_r y_r^2$, где все $\beta_i \neq 0$. Так как в поле комплексных чисел $\mathbb{C}$ можно извлечь корень из любого числа, то рассмотрим преобразование

$$L_2 : y_1 = \frac{1}{\sqrt{\beta}_1} z_1, \ldots, y_r = \frac{1}{\sqrt{\beta}_r} z_r,\ y_i = z_i,\ \forall\ i = \overline{r+1, n}.$$

Это преобразование является невырожденным, потому что

$$|A_{L_2}| = \frac{1}{\sqrt{\beta_1 \beta_2 \ldots \beta_r}}.$$

Это преобразование L_2 приведет форму FL_1 к виду

$$(FL_1)L_2 = z_1^2 + z_2^2 + \ldots + z_r^2.$$

Форма F с помощью линейного преобразования $L = L_1 L_2$ переводится к сумме r квадратов. □

7.6 Действительные квадратичные формы

Основное поле k в этом параграфе — это поле действительных чисел $\mathbb{R}$. Рассмотрим квадратичные формы

$$F = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j$$

с коэффициентами $\alpha_{ij} \in \mathbb{R}$. Линейное преобразование неизвестных также будем рассматривать с действительными коэффициентами.

Квадратичная форма F ранга r с помощью невырожденного линейного преобразования приводится к каноническому виду

$$FL = \alpha_1 y_1^2 + \alpha_2 y_2^2 + \ldots + \alpha_r y_r^2,$$

где $\alpha_i \neq 0$. Пусть p — число положительных коэффициентов, а q — число отрицательных коэффициентов. Ясно, что $p + q = r$. Квадратичная форма F различными линейными невырожденными действительными преобразованиями приводится к различным каноническим видам. Возникает вопрос «Что общего у этих канонических видов?».

ТЕОРЕМА 7.6.1 (Закон инерции действительных квадратичных форм)**.** *Число положительных и число отрицательных коэффициентов при квадратах неизвестных в каноническом виде, к которому приводится действительная квадратичная форма F с помощью невырожденного действительного преобразования неизвестных, не зависит от выбора линейного преобразования.*

Доказательство. Допустим противное, то есть квадратичная форма F с помощью двух линейных действительных преобразований L и M приводится к каноническим видам с различным числом положительных коэффициентов. Допустим, что квадратичная форма F ранга r с помощью преобразования $L : x \to y$ и с помощью $M : x \to z$ приводится к виду

$$FL = \alpha_1 y_1^2 + \alpha_2 y_2^2 + \ldots + \alpha_p y_p^2 - \alpha_{p+1} y_{p+1}^2 - \ldots - \alpha_r y_r^2, \tag{7.5}$$

$$FM = \beta_1 z_1^2 + \beta_2 z_2^2 + \ldots + \beta_{p'} z_{p'}^2 - \beta_{p'+1} z_{p'+1}^2 - \ldots - \beta_r z_r^2, \tag{7.6}$$

где $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r > 0$.

Предположим для определенности, что $p < p'$. Так как преобразование $L : x \to y$ является невырожденным, то невырожденным будет и преобразование $L^{-1} : y \to x$. Заметим, что

$$L^{-1} : \begin{array}{l} y_1 = \alpha_{11} x_1 + \ldots + \alpha_{1n} x_n \\ \ldots \\ y_n = \alpha_{n1} x_1 + \ldots + \alpha_{nn} x_n \end{array} .$$

Точно так же и M. Так как $M : x \to z$ является невырожденным преоб-

разованием, то M^{-1} является невырожденным.

$$M^{-1}: \begin{array}{l} z_1 = \beta_{11}x_1 + \ldots + \beta_{1n}x_n \\ \ldots \\ z_n = \beta_{n1}x_1 + \ldots + \beta_{nn}x_n \end{array}.$$

Теперь рассмотрим однородную систему линейных уравнений с n-неизвестными $x_1, \ldots, x_n$ следующего вида:

$$\begin{cases} \alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0 \\ \ldots \\ \alpha_{p1}x_1 + \ldots + \alpha_{pn}x_n = 0 \\ \beta_{p'+1,1}x_1 + \ldots + \beta_{p'+1,n}x_n = 0 \\ \ldots \\ \beta_{n1}x_1 + \ldots + \beta_{nn}x_n = 0 \end{cases}. \tag{7.7}$$

Число уравнений в системе (7.7) равно $p+(n-p') = n-(p'-p) < n$. Так как в однородной системе (7.7) число уравнений меньше числа неизвестных, то она имеет ненулевое действительное решение $x_1^{(0)}, \ldots, x_n^{(0)}$. Подставим в формулы (7.5), (7.6) вместо y и z их выражения через $x_1, \ldots, x_n$ и затем, полагая $x_1 = x_1^{(0)}, \ldots, x_n = x_n^{(0)}$, обозначим

$$y_i^{(0)} = \sum_{j=1}^{n} \alpha_{ij}x_j^{(0)}, \quad z_i^{(0)} = \sum_{j=1}^{n} \beta_{ij}x_j^{(0)}.$$

Заметим что в силу системы (7.7)

$$y_1^{(0)} = \ldots = y_p^{(0)} = 0 \quad \text{и} \quad z_{p'+1}^{(0)} = \ldots = z_n^{(0)} = 0.$$

В результате равенства (7.5) и (7.6) примут вид:

$$F(x_1^{(0)}, \ldots, x_n^{(0)}) = -\alpha_{p+1}{y_{p+1}^{(0)}}^2 - \ldots - \alpha_r{y_r^{(0)}}^2, \tag{7.8}$$

$$F(x_1^{(0)}, \ldots, x_n^{(0)}) = \beta_1{z_1^{(0)}}^2 + \ldots + \beta_{p'}{z_{p'}^{(0)}}^2. \tag{7.9}$$

Так как все коэффициенты системы (7.7) действительны, то квадраты чисел, входящих в (7.8) и (7.9) — неотрицательны. Из (7.8) видно, что

$F(x_1^{(0)}, \ldots, x_n^{(0)}) \leqslant 0$, а из (7.9), что $F(x_1^{(0)}, \ldots, x_n^{(0)}) \geqslant 0$. Это означает, что $F(x_1^{(0)}, \ldots, x_n^{(0)}) = 0$. Подставим полученный результат в равенство (7.9), получаем, что $z_1^{(0)} = \ldots = z_p^{(0)} = 0$.

Объединяя последние равенства получим $z_1^{(0)} = \ldots = z_n^{(0)} = 0$. Эти равенства указывают на то, что система линейных уравнений

$$\begin{cases} \beta_{11}x_1 + \ldots + \beta_{1n}x_n = 0 \\ \ldots \\ \beta_{n1}x_1 + \ldots + \beta_{nn}x_n = 0 \end{cases}$$

имеет не нулевое решение $x_1 = x_1^{(0)}, \ldots, x_n = x_n^{(0)}$. Но эта система содержит n линейных уравнений с n неизвестными. Тогда из критерия наличия не нулевого решения однородно системы линейных уравнений определитель этой системы должен быть равен нулю, то есть определитель этой системы $|A_{M^{-1}}| = 0$. А это протеворечит тому, что M является невырожденным линейным преоброзованием.

Аналогично, если предположить, что $p > p'$ мы получаем противоречие с невырожденным преобразованием L^{-1}. □

Определение 7.6.1. Положительным (отрицательным) индексом инерции действительной квадратичной формы называется число положительных (отрицательным) коэффициентов при квадратах неизвестных в любом каноническом виде этой квадратичной формы.

Мы уже отмечали, что $p + q = r$, где p — положительный индекс, q — отрицательный индекс. Обозначим $S = p - q$. Ясно, что при заданном ранге r, задание одного из чисел p, q или S вполне определяет два других числа.

Определение 7.6.2. Линейное преобразование неизвестных L называется ортогональным, если его матрица ортогональна, то есть

$$A_L{}^{-1} = A_L{}^T.$$

Предложение 7.6.1. *Линейное преобразование неизвестных L ортогонально тогда и только тогда, когда оно нормальную квадратичную форму переводит в нормальную квадратичную форму.*

Доказательство. 1) Пусть форма F имеет нормальный вид и L — ортогональное линейное преобразование $A_F = E$. Рассмотрим FL. Имеем, что матрица этой формы $A_{FL} = A_L^T A_F A_L = {A_L}^{-1} E A_L = {A_L}^{-1} A_L = E$, следовательно форма FL имеет нормальный вид.

2) Пусть F и FL имеют нормальный вид. Это означает что $A_F = A_{FL} = E$. С другой стороны $A_{FL} = A_L^T A_F A_L \Rightarrow A_L^T E A_L = E \Rightarrow$ $\Rightarrow A_L^T A_L = E \Rightarrow {A_L}^{-1} = A_L^T$, то есть L является ортогональным преобразованием. □

ТЕОРЕМА 7.6.2 (о приведении к главным осям)**.** *Любую действительную квадратичную форму с помощью ортогонального преобразования неизвестных можно привести к каноническому виду, при этом коэффициентами при квадратах неизвестных необходимо будут являться характеристические корни матрицы этой квадратичной формы.*

Доказательство. Пусть F — квадратичная форма от $x_1, \ldots, x_n$ с матрицей A. Известно, что матрица A является симметрической. По теореме **??** существует ортогональная матрица Q такая, что

$$Q^{-1} A Q = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix},$$

где $\alpha_1, \ldots, \alpha_n$ — характеристические корни матрицы A.

Пользуясь этим фактом, к форме F применим преобразование $L : x \to y$ с матрицей Q, то есть $X = QY$. Тогда матрица формы примет вид

$$A_{FL} = Q^T A Q = Q^{-1} A Q = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}.$$

Таким образом форма FL примет вид $FL = \alpha_1 y_1^2 + \ldots + \alpha_n y_n^2$. Видно, что форма F с помощью ортогонального преобразования L приведена к каноническому виду, где коэффициенты при квадратах неизвестных являются характеристическими корнями матрицы A. □

Определение 7.6.3. Приведение действительной квадратичной формы к каноническому виду с помощью ортогонального преобразования неизвестных называется приведение этой формы к главным осям.

Следствие 7.6.2.1. Положительный (отрицательный) индекс инерции действительной квадратичной формы равен числу положительных (отрицательных) характеристических корней матрицы этой формы. Ранг равен сумме положительных и отрицательных характеристических корней матрицы.

Доказательство. По теореме 7.6.1 число положительных и отрицательных коэффициентов не зависит от выбора невырожденного линейного преобразования неизвестных. С другой стороны по теореме 7.6.2 число положительных и отрицательных коэффициентов совпадают с числом положительных и отрицательных характеристических корней матрицы этой формы. □

Предложение 7.6.2. *Любую действительную квадратичную форму F ранга r с положительным индексом p, можно с помощью невырожденного линейного преобразования привести к виду*

$$FL = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2.$$

Доказательство. Применим к форме F ортогональное линейное преобразование $L_1 : x \to z$. Получим

$$FL_1 = \alpha_1 z_1^2 + \ldots + \alpha_p z_p^2 - \alpha_{p+1} z_{p+1}^2 - \ldots - \alpha_r z_r^2.$$

Применим теперь преобразование $L_2 : z \to y$:

$$\begin{aligned} z_1 &= \tfrac{1}{\sqrt{\alpha_1}} y_1 \\ &\dots \\ z_r &= \tfrac{1}{\sqrt{\alpha_r}} y_r \\ z_i &= y_i \quad \forall i = \overline{r+1, n}. \end{aligned}$$

Преобразование L_2 является невырожденным. После этого преобразования форма FL примет вид: $(FL_1)L_2 = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2$. Преобразование $L = L_1 L_2$ является невырожденным. □

Определение 7.6.4. Две квадратичные формы от n неизвестных называются эквивалентными над полем k, если они переходят друг в друга с помощью невырожденного линейного преобразования с коэффициентами из поля k.

Предложение 7.6.3. *Две действительные квадратичные формы от n неизвестных являются эквивалентными над полем $\mathbb{R}$ тогда и только тогда, когда они имеют одинаковые индексы инерции (ранги и сигнатуры).*

Доказательство. 1) Пусть квадратичные формы F и G эквивалентны над полем $\mathbb{R}$, тогда $F = GL$, где L —невырожденное линейное преобразование с коэффициентами из $\mathbb{R}$. Приведем эти формы к каноническому виду FL_1 и GL_2. Эти канонические виды должны совпадать. Допустим противное, то есть FL_1 и GL_2 имеют различный канонический вид, тогда форма G будет иметь два канонических вида: с одной стороны GL_2, а с другой $(GL)L_1$, которые различны. А это противоречит теореме 7.6.1, следовательно FL_1 и GL_2 имеют одинаковый канонический вид и индексы инерции форм F и G совпадают.

2) Пусть F и G имеют одинаковые индексы инерции. Это означает, что по предложению 7.6.2 существуют такие линейные преобразования

L_1 и L_2, что формы принимают вид:

$$FL_1 = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2 = GL_2.$$

Таким образом, из того, что $FL_1 = GL_2$ следует, что $(FL_1){L_2}^{-1} = F(L_1L_2^{-1}) = G$, то есть $FL = G$, где $L = L_1{L_2}^{-1}$ — невырожденное линейное преобразование. Следовательно формы F и G эквивалентны. □

7.7 Классификация типов квадратичных форм

Пусть

$$F = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}x_ix_j$$

— действительная квадратичная форма с матрицей A. В этом пункте будем рассматривать форму F как действительную функцию от n действительных переменных. Как известно форма

$$F = X^TAX = X^TA^TX = (AX)^T\overline{X} = \langle AX, X\rangle .$$

Заметим, что $\langle AX, X\rangle$ всегда является действительным числом, даже если A_F — эрмитова матрица и $x \in \mathbb{C}^n$. Квадратичную форму F можно рассматривать, как функцию от X, которая принимает вид:

$$F(X) = \langle AX, X\rangle .$$

Определение 7.7.1 (классификация типов)**.** Действительная квадратичная форма F называется:

1. положительно определенной, если: $\forall\ X \neq 0, \quad F(X) > 0$;
2. отрицательно определенной, если: $\forall\ X \neq 0, \quad F(X) < 0$;
3. положительно полуопределенной, если:

$$\forall\ X, \quad F(X) \geqslant 0, \quad \text{и} \quad \exists\ X \neq 0, \quad F(X) = 0;$$

4. отрицательно полуопределенной, если:

$$\forall\, X, \quad F(X) \leqslant 0, \quad \text{и} \quad \exists\, X \neq 0, \quad F(X) = 0;$$

5. неопределенной, если: $\exists\, X \neq 0,\ Y \neq 0, \quad F(X) > 0,\ F(Y) < 0.$

Предложение 7.7.1. *Невырожденное линейное преобразование неизвестных не меняют классификационного типа квадратичной формы.*

Доказательство. Пусть $L : x \to y$ невырожденное линейное преобразование с матрицей Q, то есть $X = QY$. Тогда $FL(Y) = F(QY)$, видно, что функции F и FL имеют одно и тоже множество значений, причем одновременно столбцы Y и $X = QY$ либо нулевые, либо ненулевые. □

Следствие. Действительные квадратичные формы можно классифицировать по их каноническому виду.

ТЕОРЕМА 7.7.1 (о характеристиках классификационных типов)**.** *Следующие группы утверждений равносильны:*

1. (a) *Квадратичная форма F является положительно определенной;*
   (b) *Квадратичная форма F является невырожденной и $q = 0$;*
   (c) $p = n$;
   (d) *Все характеристические корни матрицы A_F являются положительными.*
2. (a) *Квадратичная форма F является отрицательно определенной;*
   (b) *Квадратичная форма F является невырожденной и $p = 0$;*
   (c) $q = n$;
   (d) *Все характеристические корни матрицы A_F являются отрицательными.*

3. (a) *Квадратичная форма F является положительно полуопределенной;*

   (b) *Квадратичная форма F является вырожденной и $q = 0$;*

   (c) $p < n$, $q = 0$;

   (d) *Характеристические корни матрицы $A_F \geqslant 0$ и есть характеристические корни равные нулю.*

4. (a) *Квадратичная форма F является отрицательно полуопределенной;*

   (b) *Квадратичная форма F является вырожденной и $p = 0$;*

   (c) $q < n$, $p = 0$;

   (d) *Характеристические корни матрицы $A_F \leqslant 0$ и есть характеристические корни равные нулю.*

5. (a) *Квадратичная форма F является неопределенной;*

   (b) $p \neq 0$, $q \neq 0$;

   (c) *Существуют как положительные так и отрицательные характеристические корни матрицы A_F.*

Доказательство. Как показывает следствие, достаточно рассматривать квадратичную форму в каноническом виде. Любую действительную квадратичную форму F ранга r с положительным индексом инерции p можно привести к виду $F = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2$. Будем доказывать равносильность утверждений первой группы.

1. Пусть F — положительно определенная квадратичная форма. Покажем что ранг $r = n$. Допустим противное, то есть $r < n$, тогда

рассмотрим столбец

$$Y = \begin{pmatrix} y_1 \\ \dots \\ y_r \\ y_{r+1} \\ y_n \end{pmatrix},$$

где $y_1 = 0, \dots, y_r = 0,\ y_{r+1} \neq 0, \dots, y_n \neq 0$. Ясно, что $Y \neq 0$, но при этом $F(Y) = 0$, а это противоречит положительной определенности, то есть $r = n$, следовательно F невырожденная квадратичная форма. Покажем что $q = 0$. Допустим противное, $q \neq 0$. Наша форма имеет вид: $F = y_1^2 + \dots + y_p^2 - y_{p+1}^2 - \dots - y_r^2$. Рассмотрим столбец

$$Y = \begin{pmatrix} y_1 \\ \dots \\ y_p \\ y_{p+1} \\ y_n \end{pmatrix},$$

где $y_1 = 0, \dots, y_p = 0,\ y_{p+1} \neq 0, \dots, y_n \neq 0$. Ясно, что $Y \neq 0$, но при этом $F(Y) < 0$. Это противоречит тому, что F положительно определенная, то есть $q = 0$.

2. Дано $r = n,\ q = 0$. Известно, что $p + q = r$, следовательно $p = n$.

3. Пусть $p = n$, значит количество положительных характеристических корней матрицы A_F равно n, а всего характеристических корней у матрицы A_F тоже n. Следовательно все характеристические корни матрицы A_F положительны.

4. Пусть все характеристические корни матриц A_F положительны. Следовательно $p = n$, тогда квадратичная форма F имеет вид:

$$F = y_1^2 + \dots + y_n^2,$$

то есть $\forall\, Y \neq 0, \quad F(Y) > 0$, что по определению 7.7.1 означает, что квадратичная форма F является положительно определенной.

Равносильность утверждений первой группы доказана. Аналогично доказываются равносильность утверждений других групп. □

Теорема 7.7.1 не позволяет выяснить тип квадратичной формы по ее коэффициентам. Для этого служит следующая теорема.

Определение 7.7.2. Угловыми минорами матрицы A называются миноры матрицы A, составленные из элементов α_{ij}, расположенных в ее левом верхнем углу, то есть

$$\Delta_1 = \alpha_{11},\ \Delta_2 = \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix}, \ldots,\ \Delta_n = \begin{vmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{vmatrix}.$$

ТЕОРЕМА 7.7.2 (критерий Сильвестра)**.** *Квадратичная форма F является положительно определенной тогда и только тогда, когда все угловые миноры матрицы этой формы A_F положительны.*

Доказательство. Доказательство проводим методом математической индукции по n.

Пусть $n = 1$, тогда форма $F(x_1) = \alpha_{11}x_1^2$. Ясно, что

$$\forall\ x_1 \neq 0,\ F(x_1) > 0 \Leftrightarrow \alpha_{11} > 0.$$

Считаем что теорема справедлива для $(n-1)$-мерной квадратичной формы. Докажем ее справедливость для n-мерной формы.

Пусть

$$F = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_{ij}x_ix_j.$$

Представим эту форму в виде:

$$F = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} \alpha_{ij}x_ix_j + \sum_{i=1}^{n-1} 2\alpha_{in}x_ix_n + \alpha_{nn}x_n^2. \tag{7.10}$$

Обозначим

$$G = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \alpha_{ij} x_i x_j,$$

получим

$$F = G + \sum_{i=1}^{n-1} 2\alpha_{in} x_i x_n + \alpha_{nn} x_n^2.$$

В этой формуле G — квадратичная форма зависящая от $x_1, \ldots, x_{n-1}$ неизвестных, она получается из тех членов формы F, в которые не входят x_n. Ясно, что все угловые миноры матрицы A_G этой формы совпадают с $n-1$ угловыми минорами матрицы A_F.

Необходимость. Пусть F является положительно определенной квадратичной формой. Покажем, что тогда и форма G должна быть положительно определенной. Допустим противное, то есть существуют $(x_1^{(0)}, \ldots, x_{n-1}^{(0)})$ такие, что $G(x_1^{(0)}, \ldots, x_{n-1}^{(0)}) \leqslant 0$, тогда из равенства (7.10) следует, что

$$F(x_1^{(0)}, \ldots, x_{n-1}^{(0)}, 0) = G(x_1^{(0)}, \ldots, x_{n-1}^{(0)}) \leqslant 0.$$

А это противоречит тому, что форма F является положительно определенной. Следовательно G — положительно определена. Применим к ней предположение индукции. Все ее угловые миноры будут положительны, поэтому первые $n-1$ угловых миноров матрицы A_F будут положительны. Остается доказать, что последний угловой минор матрицы A_F, $\Delta_n = |A_F| > 0$, то есть $D(F) > 0$. Так как форма F — положительно определена, то $\exists\ L : x \to y$ — невырожденное линейное преобразование с матрицей Q такое, что $FL = y_1^2 + \ldots + y_n^2$, $D(FL) = |A_{FL}| = 1$. Из ранее доказанного $D(FL) = D(F)|Q|^2$. Заметим, что $|Q| \neq 0$, так как L — невырожденное, следовательно $D(F) = \frac{1}{|Q|^2} > 0$.

Достаточность. Пусть все угловые миноры матрицы A_F положительны. Тогда, в частности, положительными будут первые $n-1$ угловых миноров, то есть положительными являются все угловые миноры матрицы

A_G и $D(F) = |A_F| > 0$. Используя предположение индукции получим, что форма G является положительно определенной. Это означает, что $\exists\ L_1 : x \to y$ — невырожденное преобразование переводящее форму G к виду $GL_1 = y_1^2 + \ldots + y_{n-1}^2$,

$$L_1 : \begin{pmatrix} x_1 \\ \ldots \\ x_{n-1} \end{pmatrix} \to \begin{pmatrix} y_1 \\ \ldots \\ y_{n-1} \end{pmatrix}.$$

Рассмотрим преобразование $L : x \to y$, которое на первых $n-1$ переменных совпадает с L_1, а $x_n = y_n$. Это преобразование невырожденное, так как $|A_L| = |A_{L_1}| \neq 0$. Таким образом, преобразование L приведет форму F к виду:

$$FL = y_1^2 + \ldots + y_{n-1}^2 + \sum_{i=1}^{n-1} 2\beta_{in} y_i y_n + \alpha_{nn} y_n^2.$$

Выделим полные квадраты:

$$FL = \sum_{i=1}^{n-1} (y_i^2 + 2\beta_{in} y_i y_n + \beta_{in}^2 y_n^2) - \sum_{i=1}^{n-1} \beta_{in}^2 y_n^2 + \alpha_{nn} y_n^2 =$$
$$= \sum_{i=1}^{n-1} (y_i + \beta_{in} y_n)^2 + y_n^2 \left(\alpha_{nn} - \sum_{i=1}^{n-1} \beta_{in}^2 \right) = \sum_{i=1}^{n-1} (y_i + \beta_{in} y_n)^2 + b y_n^2. \tag{7.11}$$

Рассмотрим линейное преобразование неизвестных $M : z \to y$:

$$\begin{aligned} z_1 &= y_1 + \beta_{1n} y_n \\ &\ldots \\ z_{n-1} &= y_{n-1} + \beta_{n-1,n} y_n \\ z_n &= y_n. \end{aligned}$$

M — невырожденное, так как $|A_M| = 1 \neq 0$, тогда у него существует невырожденное преобразование $M^{-1} : y \to z$. Согласно формуле (7.11), это преобразование приводит форму FL к виду

$$(FL)M^{-1} = z_1^2 + \ldots + z_{n-1}^2 + b z_n^2.$$

Для доказательства положительной определенности формы F используем линейное преобразование $L_2 = LM$, где $|A_{L_2}| \neq 0$, так как L_2 — невырожденное преобразование. Тогда $b = D(FL_2) = D(F)|A_{L_2}|^2 > 0$. Получаем, что $p = n$, тогда из теоремы 7.7.1 следует, что форма F — положительно определена. □

Следствие 7.7.2.1. Для того, чтобы действительная квадратичная форма F была отрицательно определенной необходимо и достаточно, чтобы знаки угловых миноров матрицы этой формы A_F чередовались, начиная со знака минус.

Доказательство. Прежде всего заметим, что если матрица A_F имеет угловые миноры $\Delta_1, \ldots, \Delta_n$, то матрица A_{-F} формы $-F$ будет иметь своими угловыми минорами $\Delta'_k = (-1)^k \Delta_k$. Тогда справедлива следующая цепочка равносильных условий:
квадратичная форма F является отрицательно определенной $\Leftrightarrow$
квадратичная форма $-F$ является положительно определенной $\Leftrightarrow$
$\Delta'_k = (-1)^k \Delta_k > 0 \Leftrightarrow$
$\Delta_1 < 0,\ \Delta_2 > 0,\ \Delta_3 < 0,\ \Delta_4 > 0, \ldots$. □

Учебное пособие

ВОДОЛАЗОВ Александр Михайлович
КОРОЛЕВА Ольга Артуровна
КРИВОБОК Валерий Викторович

АЛГЕБРА. ЧАСТЬ II

Учебное пособие для студентов
механико-математического факультета
и факультета компьютерных наук и информационных технологий

Подписано в печать . .2017. Формат 60×84 1/16. Бумага офсетная.
Гарнитура Times. Печать офсетная.
Усл.печ.л. ( ) Уч.-изд.л. Тираж экз. Заказ

Издательство «Амирит»
410000, Саратов, Чернышевского, 88.
Типография «Амирит»
410000, Саратов, Чернышевского, 88.