МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

А. П. Пожидаев

Избранные разделы "ВЫСШЕЙ АЛГЕБРЫ"

Новосибирск, 2007

Данное пособие содержит запись некоторых разделов основного курса высшей алгебры, читавшегося автором в 2007 гг. на втором потоке первого курса механико-математического факультета Новосибирского государственного университета. Первые три параграфа излагают три теоремы Жордана, а оставшиеся четыре параграфа посвящены базисам Грёбнера и системам алгебраических уравнений.

ОГЛАВЛЕНИЕ

§ 1. Теорема Жордана о представлении пространства в виде прямой суммы инвариантных корневых подпространств 2
§ 2. Теорема Жордана — существование жордановой нормальной формы 5
§ 3. Теорема Жордана — единственность жордановой нормальной формы 7
§ 4. Эквивалентность систем алгебраических уравнений. Теорема Гильберта о базисе .. 10
§ 5. Идеал системы, аффинное алгебраическое многообразие, радикал идеала 11
§ 6. Базис Грёбнера идеала 13
§ 7. Системы алгебраических уравнений и базисы Грёбнера 15

1. Теорема Жордана о представлении пространства в виде прямой суммы инвариантных корневых подпространств.

В §1–3 будет доказана

Теорема (*Жордана*). *Пусть* $\varphi \in L(V,V)$, $\dim_F(V) = n$ *и* F *— алгебраически замкнутое поле. Тогда существует такой базис* $a_1, \ldots, a_n$ *пространства* V, *что* $[\varphi]_{a_1,\ldots,a_n} = J(\varphi)$, *где* $J(\varphi)$ *— матрица Жордана, которая определяется однозначно, с точностью до перестановки клеток.*

Эквивалентная формулировка в матричной форме:

Пусть $A \in M_n(F)$ *и* F *— алгебраически замкнутое поле. Тогда существует такая матрица Жордана* $J(A)$, *что* $A = T^{-1}J(A)T$, *где* T *— обратимая матрица. Матрица Жордана* $J(A)$ *определяется однозначно, с точностью до перестановки клеток.*

В этом параграфе мы сведем построение матрицы Жордана к φ-инвариантному подпространству U, где $\varphi_{|_U}$ нильпотентно. Пусть $\varphi \in L(V,V)$ и $\dim_F(V) = n$.

Для любого $\lambda \in Spec(\varphi)$ положим $V_\lambda := \{v \in V : \varphi(v) = \lambda v\}$ — множество собственных векторов, соответствующих $\lambda \in Spec(\varphi)$, и нулевой. Положим $V(\lambda) = \left\{v \in V : (\varphi - \lambda \cdot id)^k (v) = 0, \quad k \in \mathbb{N}\right\}$ — множество *корневых векторов*, соответствующих $\lambda \in Spec(\varphi)$. Элемент $v \in V$ называется корневым вектором высоты k, если $(\varphi - \lambda \cdot id)^k (v) = 0$ и $(\varphi - \lambda \cdot id)^{k-1} (v) \neq 0$.

Так как равенство $\varphi(v) = \lambda v$ эквивалентно $(\varphi - \lambda \cdot id)(v) = 0$, то $V_\lambda \subseteq V(\lambda)$ и собственные векторы являются корневыми векторами высоты 1.

Лемма 1. 1) V_λ, $V(\lambda)$ — *подпространства в* V;

2) $V(\lambda) = \{v \in V : (\varphi - \lambda id)^n (v) = 0\}$, *где* $n = \dim_F(V)$.

Доказательство. 1) $0 \in V_\lambda \subseteq V(\lambda)$, следовательно V_λ, $V(\lambda) \neq \varnothing$. Для любых $\alpha, \beta \in F$, $u, v \in V_\lambda$ имеем $\varphi(\alpha u + \beta v) = \alpha\varphi(u) + \beta\varphi(v) = \lambda(\alpha u + \beta v)$. Следовательно, $\alpha u + \beta v \in V_\lambda$ и V_λ — линейное подпространство.

Для любых $\alpha, \beta \in F$, $u, v \in V_\lambda$ существуют $k, m \in \mathbb{N}$ такие, что $(\varphi - \lambda \cdot id)^k (u) = (\varphi - \lambda \cdot id)^m (v) = 0$. Пусть $s = \max\{k, m\}$, тогда

$$(\varphi - \lambda \cdot id)^s (\alpha u + \beta v) = \alpha (\varphi - \lambda \cdot id)^s (u) + \beta (\varphi - \lambda \cdot id)^s (v) = 0.$$

Следовательно, $\alpha u + \beta v \in V(\lambda)$ и $V(\lambda)$ — подпространство.

2) Пусть $a_1, \ldots, a_m$ — некоторый базис $V(\lambda)$. Ясно, что $m \leq n = \dim_F(V)$. Тогда существуют k_i, $i = 1, \ldots, m$, такие, что $(\varphi - \lambda \cdot id)^{k_i}(a_i) = 0$. Пусть $k = \max\{k_1, \ldots, k_m\}$. Тогда для любых $\alpha_i \in F$, $i = 1, \ldots, m$,

$$(\varphi - \lambda \cdot id)^k \sum_{i=1}^{m} \alpha_i a_i = \sum_{i=1}^{m} \alpha_i (\varphi - \lambda \cdot id)^k a_i = 0$$

и $(\varphi - \lambda \cdot id)$ нильпотентно на $V(\lambda)$. Как мы уже знаем, индекс нильпотентности $(\varphi - \lambda \cdot id)$ на $V(\lambda)$ меньше либо равен m. Поэтому $(\varphi - \lambda \cdot id)^n = 0$ на $V(\lambda)$, и $V(\lambda) = \{v \in V : (\varphi - \lambda \cdot id)^n(v) = 0\}$. □

Пусть теперь F — алгебраически замкнутое поле, тогда $f_\varphi(x)$ раскладывается в $F[x]$ на линейные множители. Пусть

$$f_\varphi(x) = \prod_{i=1}^{p} (x - \lambda_i)^{n_i},$$

где $\lambda_i \neq \lambda_j$, при $i \neq j$, т. е. $Spec(\varphi) = \{\lambda_1, \ldots, \lambda_p\} \subseteq F$.

Теорема 1 (*Жордана о представлении пространства в виде прямой суммы инвариантных корневых подпространств*).

1) $V = V(\lambda_1) \oplus \ldots \oplus V(\lambda_p)$, где $V(\lambda_i)$ — φ-инвариантные подпространства;

2) $\dim_F V(\lambda_i) = n_i$ и $Spec\, \varphi|_{V(\lambda_i)} = \lambda_i$, т. е. λ_i — единственное собственное значение φ на $V(\lambda_i)$, $i = 1, \ldots, p$;

3) преобразование $(\varphi - \lambda_i \cdot id)$ нильпотентно на $V(\lambda_i)$ и невырождено на $V_i = V(\lambda_1) \oplus \ldots \oplus \widehat{V(\lambda_i)} \oplus \ldots \oplus V(\lambda_p)$, $i = 1, \ldots, p$.

Доказательство. Обозначим $f_i(x) = \prod\limits_{j \neq i} (x - \lambda_j)^{n_j}$, $i = 1, \ldots, p$, т. е.

$$f_i(x) = \frac{f_\varphi(x)}{(x - \lambda_i)^{n_i}} = (x - \lambda_1)^{n_1} \ldots \widehat{(x - \lambda_i)^{n_i}} \ldots (x - \lambda_p)^{n_p}.$$

Ясно, что Н.О.Д. $(f_1(x), \ldots, f_p(x)) = 1$. Следовательно, существуют

$$g_1(x), \ldots, g_p(x) \in F[x] \quad \text{такие, что} \quad \sum_{i=1}^{p} f_i(x) g_i(x) = 1. \quad (*)$$

Заметим, что для любого $\psi \in L(V, V)$ множество $\psi(V) = \{\psi(v) : v \in V\}$ является линейным пространством. Действительно, $0 = \psi(0) \in \psi(V)$ и для любых $\alpha, \beta \in F$, $\psi(u), \psi(v) \in \psi(V)$ имеем $\alpha\psi(u) + \beta\psi(v) = \psi(\alpha u + \beta v) \in \psi(V)$. Поэтому $W_i = f_i(\varphi) g_i(\varphi) V = \{f_i(\varphi) g_i(\varphi)(v) : v \in V\}$ — линейные подпространства в V при $i = 1, \ldots, p$. Заметим, что

$$\varphi(W_i) = \varphi f_i(\varphi) g_i(\varphi)(V) = f_i(\varphi) g_i(\varphi) \varphi(V) \subseteq f_i(\varphi) g_i(\varphi)(V) \subseteq W_i$$

для любого $i = 1, \ldots, p$. Поэтому W_i являются φ-инвариантными.

По теореме Гамильтона-Кэли имеем

$$(\varphi - \lambda_i \cdot id)^{n_i} W_i = (\varphi - \lambda_i \cdot id)^{n_i} f_i(\varphi) g_i(\varphi)(V) = f_\varphi(\varphi) g_i(\varphi)(V) = 0.$$

Поэтому $W_i \subseteq V(\lambda_i)$. Подставим $x = \varphi$ в $(*)$:

$$\sum_{i=1}^{p} f_i(\varphi) \cdot g_i(\varphi) = id.$$

Следовательно, $(\sum_{i=1}^{p} f_i(\varphi) \cdot g_i(\varphi))(V) = id(V) = V$, или

$$V = \sum_{i=1}^{p} f_i(\varphi) \cdot g_i(\varphi)(V) = \sum_{i=1}^{p} W_i.$$

Имеем $V = \sum\limits_{i=1}^{p} W_i \subseteq \sum\limits_{i=1}^{p} V(\lambda_i) \subseteq V$, поэтому $V = \sum\limits_{i=1}^{p} V(\lambda_i)$.

Пусть $v \in V(\lambda_i) \cap \left(\sum\limits_{j \neq i} V(\lambda_j) \right)$. Тогда $v = \sum\limits_{j \neq i} v_j$, где $v_j \in V(\lambda_j)$, $j \neq i$. По пункту 2 леммы 1 имеем $(\varphi - \lambda_i \cdot id)^n v = 0$. Более того, справедливы равенства

$$\prod_{j \neq i} (\varphi - \lambda_j \cdot id)^n (v) = \left(\prod_{j \neq i} (\varphi - \lambda_j \cdot id)^n \right) \left(\sum_{\ell \neq i} v_\ell \right) = \sum_{\ell \neq i} \left(\prod_{j \neq i} (\varphi - \lambda_j \cdot id)^n v_\ell \right) = 0.$$

Очевидно, что многочлены $a_i(x) = (x - \lambda_i)^n$ и $b_i(x) = \prod\limits_{j \neq i} (x - \lambda_j)^n$, $i = 1, \ldots, p$, взаимно просты. Следовательно, существуют такие $c_i(x)$, $d_i(x) \in F[x]$, что

$$c_i(x) \cdot a_i(x) + d_i(x) \cdot b_i(x) = 1,$$

$$c_i(\varphi) \cdot a_i(\varphi) + d_i(\varphi) \cdot b_i(\varphi) = id.$$

Поэтому

$$0 = c_i(\varphi) a_i(\varphi)(v) + d_i(\varphi) b_i(\varphi)(v) = v$$

и $V(\lambda_i) \cap \left(\sum\limits_{j \neq i} V(\lambda_j) \right) = 0$, $i = 1, \ldots, p$. Таким образом, $V = V(\lambda_1) \oplus \ldots \oplus V(\lambda_p)$.

Имеем, $V = W_1 + \ldots + W_p$, $W_i \subseteq V(\lambda_i)$, $i = 1, \ldots, p$. Следовательно, $V = W_1 \oplus \ldots \oplus W_p$, откуда $W_i = V(\lambda_i) = f_i(\varphi) g_i(\varphi) V$ и $V(\lambda_i)$ являются φ-инвариантными при $i = 1, \ldots, p$. Пункт 1) теоремы доказан.

Далее, $(\varphi - \lambda_i \cdot id)^{n_i} V(\lambda_i) = (\varphi - \lambda_i \cdot id)^{n_i} f_i(\varphi) g_i(\varphi) V = f_\varphi(\varphi) g_i(\varphi) V = 0$, и $(\varphi - \lambda_i \cdot id)$ нильпотентно на $V(\lambda_i)$, $i = 1, \ldots, p$. Поэтому минимальный многочлен φ на $V(\lambda_i)$ является делителем $(x - \lambda_i \cdot id)^{n_i}$, $i = 1, \ldots, p$. Следовательно, $Spec(\varphi_{|_{V(\lambda_i)}}) = \lambda_i$, $i = 1, \ldots, p$.

Выберем в каждом $V(\lambda_i)$ базис, тогда их объединение $a_1, \ldots, a_n$ — базис V. В этом базисе

$$[\varphi]_{a,\ldots,a_n} = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_p \end{pmatrix},$$

где $A_i \in M_{m_i}(F)$, $m_i = \dim_F V(\lambda_i)$. Из свойств характеристических многочленов следует, что $f_{A_i}(x) = (x - \lambda_i)^{m_i}$, $i = 1, \ldots, p$, и

$$f_\varphi(x) = f_{[\varphi]_{a_1,\ldots,a_n}}(x) = \prod_{i=1}^{p} f_{A_i}(x) = \prod_{i=1}^{p} (x - \lambda_i)^{m_i} = \prod_{i=1}^{p} (x - \lambda_i)^{n_i},$$

где $\lambda_i \neq \lambda_j$ при $i \neq j$. Так как $F[x]$ — факториальное кольцо, то $m_i = n_i$ при $i = 1, \ldots, p$. Следовательно, $\dim_F V(\lambda_i) = n_i$, $i = 1, \ldots, p$, и пункт 2) теоремы доказан.

Осталось доказать, что $(\varphi - \lambda_i \cdot id)$ — невырожденное преобразование на $V_i = V(\lambda_1) \oplus \ldots \oplus \widehat{V(\lambda_i)} \oplus \ldots \oplus V(\lambda_p)$, $i = 1, \ldots, p$. Преобразование $\varphi - \lambda_i \cdot id$ невырождено на $V_i \Leftrightarrow Ker(\varphi - \lambda_i \cdot id)_{|_{V_i}} = 0$. Пусть $v \in V_i$ и $(\varphi - \lambda_i \cdot id)v = 0$. Тогда $v \in V(\lambda_i)$, откуда $v \in V(\lambda_i) \cap V_i = 0$ и $v = 0$. □

2. Теорема Жордана — существование жордановой нормальной формы.

Доказательство теоремы мы начнем со случая нильпотентного преобразования. Пусть $\varphi \in L(V, V)$ и φ нильпотентно индекса m на V. Тогда $m \leq n = \dim_F(V)$.

Система линейно независимых векторов $a, \varphi(a), \ldots, \varphi^{k-1}(a)$, где $\varphi^k(a) = 0$, называется *цепочкой* длины k. Ясно, что $h(a) = k$. С другой стороны, для любого $a \in V$ такого, что $h(a) = k$, множество $a, \varphi(a), \ldots, \varphi^{k-1}(a)$ образует цепочку.

Базис пространства V, состоящий из цепочек $a_i, \varphi(a_i), \ldots, \varphi^{k_i-1}(a_i)$, где $i = 1, \ldots, p$, $k_1 + \ldots + k_p = n$, называется *базисом Жордана*. Ясно, что в этом базисе

$$[\varphi] = \begin{pmatrix} J_{k_1,0} & & 0 \\ & \ddots & \\ 0 & & J_{k_p,0} \end{pmatrix} \quad — \quad \text{матрица Жордана.}$$

Лемма 1. *Пусть $\varphi \in L(V, V)$ и φ нильпотентно индекса m на V. Тогда φ имеет базис Жордана.*

Доказательство. Индукция по m. При $m = 1$ имеем $\varphi = 0$. Тогда любой базис $a_1, \ldots, a_n$, $n = \dim_F(V)$, является объединением цепочек длины 1, т. е. образует базис Жордана. Предположим, что утверждение верно для $m-1$. Рассмотрим подпространство $\varphi(V) \subseteq V$. Ясно, что $\varphi(V)$ является φ-инвариантным и φ нильпотентно на $\varphi(V)$ индекса $m-1$. По предположению индукции $\varphi_{|_{\varphi(V)}}$ имеет базис Жордана. Так как для любого $x \in \varphi(V)$ существует $y \in V$ такой, что $x = \varphi(y)$, то можно записать этот базис в виде: $\varphi(a_i), \ldots, \varphi^{k_i}(a_i)$, $i = 1, \ldots, p$, $\sum\limits_{i=1}^{p} k_i = \dim_F \varphi(V)$. Докажем, что система $a_i, \varphi(a_i), \ldots, \varphi^{k_i}(a_i)$, $i = 1, \ldots, p$, состоит из линейно независимых векторов. Пусть

$$\sum_{i=1}^{p} \sum_{j=0}^{k_i} \alpha_{ij} \varphi^j(a_i) = 0, \quad \text{где} \quad \alpha_{ij} \in F.$$

Тогда

$$\varphi\left(\sum_{i=1}^{p} \sum_{j=0}^{k_i} \alpha_{ij} \varphi^j(a_i)\right) = \sum_{i=1}^{p} \sum_{j=0}^{k_i} \alpha_{ij} \varphi^{j+1}(a_i) = 0.$$

Поэтому $\alpha_{ij} = 0$, при $i = 1, \ldots, p$, $\quad j = 0, \ldots, k_i - 1$, так как $\{\varphi^j(a_i), i = 1, \ldots, p, j = 1, \ldots, k_i\}$ — базис $\varphi(V)$. Следовательно, $\sum\limits_{i=1}^{p} \alpha_{ik_i} \varphi^{k_i}(a_i) = 0$ и $\alpha_{ik_i} = 0$, $i = 1, \ldots, p$, по тем же причинам. Если $t = \sum\limits_{i=1}^{p} (k_i + 1) = n$, то построенные цепочки — базис Жордана. Если $t < n$, то дополним найденную систему векторами $b_1, \ldots, b_\ell$ до базиса пространства V.

Для любого $s = 1, \ldots, \ell$ имеем $\varphi(b_s) \in \varphi(V)$. Следовательно, мы можем однозначно разложить эти векторы по базису $\varphi(V)$:

$$\varphi(b_s) = \sum_{i=1}^{p} \sum_{j=1}^{k_i} \beta_{ij}^{(s)} \varphi^j(a_i),$$

где $\beta_{ij}^{(s)} \in F$, $\quad s = 1, \ldots, \ell$. С другой стороны, $\varphi(b_s) = \varphi(c_s)$, где

$$c_s = \sum_{i=1}^{p} \sum_{j=1}^{k_i} \beta_{ij}^{(s)} \varphi^{j-1}(a_i), \quad s = 1, \ldots, \ell.$$

Тогда $\varphi(b_s - c_s) = 0$, $s = 1, \ldots, \ell$, т. е. векторы $b_s - c_s$ образуют цепочки длины 1.

Докажем, что $\left\{\varphi^j(a_i),\ b_s - c_s : i = 1, \ldots, p,\ j = 0, \ldots, k_i,\ s = 1, \ldots, \ell\right\}$ — базис V. Пусть

$$\sum_{i=1}^{p} \sum_{j=0}^{k_i} \alpha_{ij} \varphi^j(a_i) + \sum_{s=1}^{\ell} \lambda_s (b_s - c_s) = 0,$$

где $\alpha_{ij},\ \lambda_s \in F$. Тогда

$$\sum_{i=1}^{p} \sum_{j=0}^{k_i} \alpha_{ij} \varphi^j(a_i) - \sum_{s=1}^{\ell} \lambda_s \left(\sum_{i=1}^{p} \sum_{j=1}^{k_i} \beta_{ij}^{(s)} \varphi^{j-1}(a_i)\right) + \sum_{s=1}^{\ell} \lambda_s b_s = 0.$$

Следовательно, $\lambda_1 = \ldots = \lambda_s = 0$ и $\alpha_{ij} = 0$, $i = 1, \ldots, p$, $j = 0, \ldots, k_i$. Так как построенный базис состоит из цепочек, то он является базисом Жордана. $\square$

Следствие. *Пусть $\varphi \in L(V,V)$ и $Spec\,\varphi = \{\lambda\}$. Тогда существует такой базис $a_1, \ldots, a_n$, что $[\varphi]_{a,\ldots,a_n} = J(\varphi)$ — матрица Жордана.*

Доказательство. Рассмотрим $\psi = (\varphi - \lambda \cdot id)$. По теореме Гамильтона-Кэли $\psi^n = (\varphi - \lambda \cdot id)^n = f_\varphi(\varphi) = 0$. Следовательно, ψ нильпотентно на V. Пусть $\{a_i, \psi(a_i), \ldots, \psi^{k_i-1}(a_i) : i = 1, \ldots, p\}$ — базис Жордана для ψ. Тогда в этом базисе имеем при $i = 1, \ldots, p,\ j = 0, \ldots, k_i - 1$:

$$\begin{cases} \psi\left(\psi^j(a_i)\right) = \psi^{j+1}(a_i), \\ \psi\left(\psi^{k_i-1}(a_i)\right) = 0, \end{cases} \quad \text{или} \quad \begin{cases} \varphi\left(\psi^j(a_i)\right) = \lambda\psi^j(a_i) + \psi^{j+1}(a_i), \\ \varphi\left(\psi^{k_i-1}(a_i)\right) = \lambda\psi^{k_i-1}(a_i), \end{cases}$$

и $[\varphi] = \begin{pmatrix} J_{k_1,\lambda} & & 0 \\ & \ddots & \\ 0 & & J_{k_p,\lambda} \end{pmatrix}$ — матрица Жордана. $\square$

Теорема 1 (*Жордана о существовании нормальной жордановой формы*). *Пусть $\varphi \in L(V,V)$, $\dim_F(V) = n$ и F — алгебраически замкнутое поле. Тогда существует такой базис $a_1, \ldots, a_n$ пространства V, что $[\varphi]_{a,\ldots,a_n} = J(\varphi)$ — матрица Жордана.*

Доказательство. Так как F — алгебраически замкнутое поле, то

$$f(x) = \prod_{i=1}^{p} (x - \lambda_i)^{n_i},\ \lambda_i \neq \lambda_j \text{ при } i \neq j.$$

В силу теоремы 1 §1, имеем $V = \bigoplus\limits_{i=1}^{p} V(\lambda_i)$, где $V(\lambda_i)$ является φ-инвариантным и $Spec\left(\varphi_{|_{V(\lambda_i)}}\right) = \{\lambda_i\}$, $i = 1, \ldots, p$. В силу следствия из леммы 1, в каждом $V(\lambda_i)$ можно найти базис Жордана для $\varphi_{|_{V(\lambda_i)}}$, $i = 1, \ldots, p$. Пусть $a_1, \ldots, a_n$ — объединение всех этих базисов. Тогда, как мы видели ранее, $[\varphi]_{a_1,\ldots,a_n} = J(\varphi)$ — матрица Жордана. $\square$

3. Теорема Жордана — единственность жордановой нормальной формы.

Пусть $\varphi \in L(V,V)$, $\dim_F(V) = n$ и F — алгебраически замкнутое поле. По теореме 1 §2, существует жорданов базис $a_1, \ldots, a_n$, в котором $[\varphi]_{a_1,\ldots,a_n} = J(\varphi)$ — матрица Жордана.

Обозначение. Обозначим через $N(m, \lambda)$ число жордановых клеток $J_{m,\lambda}$ порядка m, соответствующих $\lambda \in Spec(\varphi)$, в матрице $J(\varphi)$. Наша цель — доказать, что числа $N(m, \lambda)$ не зависят от выбора жорданова базиса.

Лемма 1. *Пусть* $b_1, \ldots, b_n$ *– некоторый базис* V *и* $[\varphi]_{b_1,\ldots,b_n} = A$. *Тогда* $r(A) = \dim(\varphi(V))$, *т. е.* $r(A)$ *не зависит от выбора базиса* $b_1, \ldots, b_n$.

Доказательство. Очевидно, что $\varphi(V) = L(\varphi(b_1), \ldots, \varphi(b_n))$. Таким образом, $\dim_F \varphi(V)$ есть максимальное число линейно независимых векторов среди $\varphi(b_1), \ldots, \varphi(b_n)$. Имеем $\varphi(b_i) = \sum_{j=1}^{n} \alpha_{ij} b_j$, $i = 1, \ldots, n$, где $A = (\alpha_{ij})$. Рассмотрим изоморфизм $[\ ]_{b_1,\ldots,b_n} : V \to F_n$, где если $x = \sum_{i=1}^{n} \alpha_i b_i$, то $[x]_{b_1,\ldots,b_n} = (\alpha_1, \ldots, \alpha_n)$. Тогда максимальное число линейно независимых векторов среди $\varphi(b_1), \ldots, \varphi(b_n)$ совпадает с максимальным числом линейно независимых векторов среди $[\varphi(b_1)]_{b_1,\ldots,b_n}, \ldots, [\varphi(b_n)]_{b_1,\ldots,b_n}$, т. е. совпадает с рангом по строкам A. □

Обозначим через $r_t = \dim_F (\varphi - \lambda \cdot id)^t V$, $t = 0, 1, \ldots$. В частности, $r_0 = \dim_F (\varphi - \lambda \cdot id)^0 V = \dim_F V = n$. По лемме 1, числа $r_t = \dim_F (\varphi - \lambda \cdot id)^t V = r\left[(\varphi - \lambda \cdot id)^t\right] = r([\varphi] - \lambda E)^t$ не зависят от выбора базиса пространства V.

Лемма 2. $N(m, \lambda) = r_{m-1} - 2r_m + r_{m+1}$ *при* $m \geq 1$.

Доказательство. Подсчитаем $\dim_F (\varphi - \lambda \cdot id)^t V$ при $t = 0, 1, 2, \ldots$. По теореме 1 §1, $V = V(\lambda) \oplus V'$, где $V' = \bigoplus_{\lambda' \neq \lambda} V(\lambda')$, $V(\lambda)$, $V(\lambda')$ — корневые подпространства, $\lambda, \lambda' \in Spec(\varphi)$. В силу следствия из леммы 1 §2, в $V(\lambda)$ можно выбрать жорданов базис $a_i, \psi(a_i), \ldots, \psi^{k_i - 1}(a_i)$, где $i = 1, \ldots, p$, $\psi = (\varphi - \lambda \cdot id)$. Каждому из этих наборов соответствует клетка жордана размерности k_i, $i = 1, \ldots, p$. Имеем

$$V(\lambda) = \bigoplus_{i=1}^{p} L\left(a_i, \psi(a_i), \ldots, \psi^{k_i - 1}(a_i)\right).$$

Очевидно, что для любого $1 \leq i \leq p$ пространство $L\left(a_i, \psi(a_i), \ldots, \psi^{k_i - 1}(a_i)\right)$ является ψ-инвариантным. Так как $V(\lambda)$ и V' инвариантны относительно ψ, то

$$r_m = \dim_F \psi^m(V) = \dim_F \psi^m(V(\lambda)) + \dim_F \psi^m\left(V'\right).$$

В силу теоремы 1 §1, преобразование ψ^m невырождено на V'. Следовательно, $\dim_F \psi^m(V') = \dim_F V'$. Далее,

$$\dim_F \psi^m(V(\lambda)) = \dim_F \psi^m\left(\bigoplus_{i=1}^{p} L\left(a_i, \psi(a_i), \ldots, \psi^{k_i - 1}(a_i)\right)\right) =$$

$$= \sum_{i=1}^{p} \dim_F L\left(\psi^m(a_i), \psi^{m+1}(a_i), \ldots, \psi^{m+k_i - 1}(a_i)\right).$$

Имеем

$$\dim_F L\left(\psi^m(a_i), \psi^{m+1}(a_i), \ldots, \psi^{m+k_i - 1}(a_i)\right) =$$

$$= \begin{cases} 0, & \text{при } \ m \geq k_i, \\ \dim_F L\left(\psi^m(a_i), \ldots, \psi^{k_i-1}(a_i)\right) = k_i - m, & \text{при } \ m < k_i, \end{cases}$$

так как $\psi^m(a_i), \ldots, \psi^{k_i-1}(a_i)$ линейно независимы.

Следовательно,

$$r_m = \sum_{k_i > m} (k_i - m) + \dim_F V'.$$

Тогда

$$r_m - r_{m+1} = \left(\sum_{k_i>m} (k_i - m) + \dim_F V'\right) - \left(\sum_{k_i>m+1} (k_i - m - 1) + \dim_F V'\right) =$$

$$= \sum_{k_i>m} (k_i - m) - \sum_{k_i>m+1} (k_i - m - 1) = \sum_{k_i>m} (k_i - m) - \sum_{k_i>m+1} (k_i - m) + \sum_{k_i>m+1} 1 =$$

$$= \sum_{k_i=m+1} (k_i - m) + \sum_{k_i>m+1} (k_i - m) - \sum_{k_i>m+1} (k_i - m) + \sum_{k_i>m+1} 1 =$$

$$= \sum_{k_i=m+1} (m + 1 - m) + \sum_{k_i>m+1} 1 = \sum_{k_i=m+1} 1 + \sum_{k_i>m+1} 1 = N(m+1, \lambda) + N(m+2, \lambda) + \ldots$$

Таким образом,

$$\begin{cases} r_m - r_{m+1} = N(m+1, \lambda) + N(m+2, \lambda) + \ldots, \\ r_{m+1} - r_{m+2} = N(m+2, \lambda) + N(m+3, \lambda) + \ldots. \end{cases}$$

Поэтому $N(m+1, \lambda) = r_m - 2r_{m+1} + r_{m+2}$. Окончательно имеем $N(m, \lambda) = r_{m-1} - 2r_m + r_{m+1}$, $m \geq 1$, где $r_m = r(\varphi - \lambda \cdot id)^m$, $r_0 = n$. □

Теорема 1 (*Жордана о единственности нормальной жордановой формы*). *Пусть* $\varphi \in L(V, V)$, $\dim_F V = n$ *и* F *— алгебраически замкнутое поле. Тогда жорданова форма* $J(\varphi)$ *единственна с точностью до перестановки клеток.*

Доказательство. По лемме 2, $N(m, \lambda)$ не зависят от жорданова базиса. □

4. Эквивалентность систем алгебраических уравнений. Теорема Гильберта о базисе.

Пусть F — поле, $f_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n], i \in \Omega$. *Системой алгебраических уравнений* (далее: системой) называется система вида $\{f_i(x_1, \ldots, x_n) = 0, i \in \Omega\}$. Если $|\Omega| < \infty$, то система называется *конечной*. Две системы называются *эквивалентными*, если множества их решений совпадают. Обозначение: $S_1 \sim S_2$.

Лемма 1. *Всякая конечная система над $\mathbb{R}$ эквивалентна системе из одного уравнения.*

Доказательство. Система $\{f_i(x_1, \ldots, x_n) = 0, i = 1, \ldots, m\}$ эквивалентна уравнению

$$f_1^2(x_1, \ldots, x_n) + \ldots + f_m^2(x_1, \ldots, x_n) = 0.$$

Упражнение. Доказать лемму 1 для произвольного алгебраически незамкнутого поля.

Лемма 2. *Над полем $\mathbb{C}$ система $\{x = 0, y = 0\}$ не эквивалентна никакому уравнению.*

Доказательство. Пусть уравнение $f(x, y) = 0$ имеет решение $x = 0, y = 0$. Пусть $f(x, y) = a_0(y) + a_1(y)x + \ldots + a_m(y)x^m$, где $a_m(y) \neq 0$. Тогда существует такое $y_0 \neq 0$, что $a_m(y_0) \neq 0$. Но тогда уравнение $a_0(y_0) + a_1(y_0)x + \ldots + a_m(y_0)x^m$ имеет корень x_0. Следовательно, (x_0, y_0) — решение уравнения $f(x, y) = 0$. □

Пусть A — ассоциативное коммутативное кольцо с 1. Говорят, что идеал $I \trianglelefteq A$ *порождается* элементами $a_i \in A, i \in \Omega$, если $I := (a_i, i \in \Omega) := \{a_{i_1}r_1 + \ldots + a_{i_n}r_n : r_i \in A\}$, т. е. I есть наименьший идеал в A, содержащий $a_i, i \in \Omega$. Говорят, что элементы $a_i, i \in \Omega$, составляют *базис идеала* I. Элементы $a_i, i \in \Omega$, называются *порождающими* (или *образующими* элементами идеала I. Говорят, что идеал $I \trianglelefteq A$ допускает *конечный базис*, если существуют $a_1, \ldots, a_n \in A$ такие, что $I = (a_1, \ldots, a_n)$.

Теорема 1 (*Гильберта о базисе*). *Пусть $I \trianglelefteq F[x_1, \ldots, x_n]$. Тогда I допускает конечный базис.*

Доказательство. Рассмотрим сначала случай, когда I порождается одночленами $m_1, m_2, \ldots$. Покажем, что в I можно выбрать базис $m_{i_1}, \ldots, m_{i_k}$. Индукция по n. При $n = 1$ утверждение очевидно. В случае n переменных подставим во все одночлены $x_n = 1$ и в полученной совокупности выберем базис $m'_1, \ldots, m'_s$. Пусть $m_i \in I$ соответствует m'_i и l есть наибольший показатель при x_n в одночленах $m_1, \ldots, m_s$. Рассмотрим все одночлены из I степени p относительно x_n, $p = 0, \ldots, l - 1$. Подставим в них $x_n = 1$ и в

полученном множестве вновь выберем базис $m_1^{(p)}, \ldots, m_{s_p}^{(p)}$. Легко видеть, что множество $\{m_1, \ldots, m_s, m_i^{(j)} x_n^j : j = 0, \ldots, l-1, i = 1, \ldots, s_j\}$ является базисом в I.

Далее, рассмотрим лексикографический порядок на множестве одночленов, т. е. $x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n}$, если либо $\alpha_1 > \beta_1$, либо $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k, \alpha_{k+1} > \beta_{k+1}$ для некоторого k. Пусть J — идеал, порожденный старшими членами f_C элементов f из I. Выберем конечный базис $m_1, \ldots, m_k$ в J. Пусть f_i — многочлены из I, старшие члены которых равны m_i. Покажем, что f_i образуют базис в I. Если $f \in I$, то $f_C = m_i r$ для некоторых i и одночлена r. Тогда $g = f - f_i r \in I$ и $g_C < f_C$. За конечное число шагов получим $f \in (f_1, \ldots, f_k)$. □

5. Идеал системы, аффинное алгебраическое многообразие, радикал идеала.

Для всякой системы $S = \{f_i(x_1, \ldots, x_n) = 0, i \in \Omega\}$ мы можем определить идеал $I(S) = (f_i, i \in \Omega)$.

Лемма 1. *Если $f \in I(S)$, то $f(x_1^0, \ldots, x_n^0) = 0$ для любого решения $(x_1^0, \ldots, x_n^0)$ системы S.*

Доказательство. $f \in I(S) \Leftrightarrow f = r_1 f_{i_1} + \ldots + r_m f_{i_m} \Rightarrow f(x_1^0, \ldots, x_n^0) = 0$. □

Предложение 1. *Пусть $\{f_1, \ldots, f_m\}$ и $\{g_1, \ldots, g_k\}$ — два базиса в I. Тогда системы $S_1 = \{f_1 = 0, \ldots, f_m = 0\}$ и $S_2 = \{g_1 = 0, \ldots, g_k = 0\}$ эквивалентны.*

Доказательство. Если $\bar{x} = (x_1^0, \ldots, x_n^0)$ — решение S_1, то $g_i(x_1^0, \ldots, x_n^0) = 0$ по лемме 1. Следовательно, $\bar{x}$ — решение системы S_2. Обратное аналогично. □

Таким образом, множество решений системы однозначно определяется идеалом системы, а различным базисам одного идеала отвечают эквивалентные системы.

Следствие 1. *Любая система эквивалентна конечной системе.*

Доказательство. Из теоремы 1 §4 следует, что во всяком идеале кольца $F[x_1, \ldots, x_n]$ можно выбрать конечный базис. □

Следствие 2. *Любая система от одного неизвестного эквивалентна системе из одного уравнения.*

Подмножество X в F_n называется *аффинным алгебраическим многообразием*, если существует система S такая, что $\bar{x} \in S \Leftrightarrow \bar{x} \in X(S)$, где $X(S)$ обозначает множество решений

системы S. Если $I \trianglelefteq F[x_1, \ldots, x_n]$, то через $X(I)$ обозначим подмножество в F_n, состоящее из элементов, на которых все многочлены из I равны 0. Ясно, что $S_1 \sim S_2 \Leftrightarrow X(S_1) = X(S_2)$, а также, что $X(S) = X(I(S))$.

Заметим, что системы могут быть эквивалентны, но их идеалы не совпадают.

*П*ример: $x = 0 \sim x^2 = 0$, но $(x^2) \neq (x)$.

Однако, для любого многообразия X существует наибольший идеал $J(X)$, задающий это многообразие:

$$J(X) = \{f \in F[x_1, \ldots, x_n] : f(x) = 0 \text{ для любого } x \in X\}.$$

Предложение 2. $S_1 \sim S_2 \Leftrightarrow J(X(S_1)) = J(X(S_2))$.

Доказательство. Покажем, что если $J(X(S_1)) = J(X(S_2))$, то $X(S_1) = X(S_2)$. Так как $S_i \subseteq I(S_i) \subseteq J(X(S_i))$, то для любого $f \in S_1$ имеем $f \in J(X(S_2))$, т. е. любое решение системы S_2 является решением системы S_1. Следовательно, $X(S_2) \subseteq X(S_1)$. Аналогично показывается обратное. Теперь очевидны эквивалентности: $S_1 \sim S_2 \Leftrightarrow X(S_1) = X(S_2) \Leftrightarrow J(X(S_1)) = J(X(S_2))$. □

Радикалом идеала I называется множество

$$r(I) = \{f \in F[x_1, \ldots, x_n] : f^s \in I \text{ для некоторого } s \in \mathbb{N}\}.$$

Предложение 3. 1) $I \subseteq r(I)$. 2) $r(I) \trianglelefteq F[x_1, \ldots, x_n]$. 3) $X(I) = X(r(I))$.

Доказательство. 1) Очевидно. 2) Пусть $f_1, f_2 \in r(I)$ и $f_1^{s_1} \in I, f_2^{s_2} \in I$. Тогда $(f_1 + f_2)^{s_1+s_2} = \sum \alpha_k f_1^k f_2^{s_1+s_2-k} \in I, \alpha_k \in F$. Если f_2 произвольный, то $(f_1 f_2)^{s_1} \in I \Rightarrow f_1 f_2 \in r(I)$. 3) Из $I \subseteq r(I)$ следует $X(r(I)) \subseteq X(I)$. Обратно, если $\bar{x} \in X(I)$ и $f(\bar{x}) \neq 0$ для некоторого $f \in r(I)$, то $f^s(\bar{x}) \neq 0$ для любого s, но существует s такое, что $f^s \in I$. □

Идеал I называется *радикальным*, если $I = r(I)$.

Упражнение. Показать, что $r(r(I)) = r(I)$.

Далее в этом параграфе считаем $F = \mathbb{C}$.

Предложение 4. [*см. Прасолов В.В.*, Многочлены, М.:МЦНМО, 2000.] *Если $f_1, \ldots, f_m$ без общих нулей, то существуют $g_1, \ldots, g_m$ такие, что $\sum_{i=1}^m f_i g_i = 1$.*

Теорема 1 (*Гильберта о нулях*). *Для любой системы S над $\mathbb{C}$ справедливо равенство*

$$J(X(S)) = r(I(S)).$$

Переформулировка: *Для системы* $\{f_i(x_1,\dots,x_n) = 0, i = 1,\dots,m\}$ *многочлен* $f(x_1,\dots,x_n)$ *обращается в нуль на всех решениях данной системы* $\Leftrightarrow$ *существуют* $r_1(x_1,\dots,x_n),\dots,r_m(x_1,\dots,x_n)$ *и* $s \in \mathbb{N}$ *такие, что* $f^s = \sum_{i=1}^m r_i f_i$.

Замечание: Над $\mathbb{R}$ теорема не верна.

Доказательство. Пусть $S = \{f_1 = 0,\dots,f_m = 0\}$ и $f(x_1^0,\dots,x_n^0) = 0$ для любого $(x_1^0,\dots,x_n^0) \in X(S)$. Покажем, что существует $s \in \mathbb{N}$ такое, что $f^s \in (f_1,\dots,f_m)$. При $f = 0$ утверждение очевидно. Добавим к переменным $x_1,\dots,x_n$ новую переменную $x_{n+1} = z$ и рассмотрим многочлены $f_1,\dots,f_m, 1 - zf$. Они не имеют общих нулей, поэтому

$$1 = \sum_{i=1}^m h_i f_i + h_{m+1}(1 - zf),$$

где $h_i \in F[x_1,\dots,x_n,z]$. Положим $z = 1/f$. После приведения к общему знаменателю получим $f^s = \sum_{i=1}^m r_i f_i$, где $r_i \in F[x_1,\dots,x_n]$. □

Следствие 3. $S_1 \sim S_2 \Leftrightarrow r(I(S_1)) = r(I(S_2))$.

Следствие 3 показывает, что существует биекция между аффинными алгебраическими многообразиями и радикальными идеалами кольца $\mathbb{C}[x_1,\dots,x_n]$.

Предложение 5. *Пусть* $f_1(x_1,\dots,x_n)$ *и* $f_2(x_1,\dots,x_n)$ *неприводимы. Тогда* $f_1 = 0 \sim f_2 = 0 \Leftrightarrow f_1 = \alpha f_2, \alpha \in \mathbb{C}$.

Доказательство. Из неприводимости f_i и факториальности кольца $\mathbb{C}[x_1,\dots,x_n]$ следует, что если некоторая степень f делится на f_i, то f делится на f_i. Следовательно, $r((f_i)) = (f_i)$. Таким образом, $f_1 = 0 \sim f_2 = 0 \Leftrightarrow (f_1) = (f_2) \Leftrightarrow f_1 = \alpha f_2$. □

Следствие 4. *Система* S *несовместна* $\Leftrightarrow 1 \in I(S)$.

Доказательство. $X(S) = \varnothing \Leftrightarrow S \sim 1 = 0 \Leftrightarrow r(I(S)) = r(\mathbb{C}[x_1,\dots,x_n]) \Leftrightarrow 1 \in r(I(S)) \Leftrightarrow 1 \in I(S)$. □

6. Базис Грёбнера идеала.

Задача вхождения: Пусть идеал $I \trianglelefteq F[x_1,\dots,x_n]$ задан базисом $I = (f_1,\dots,f_m)$. Требуется найти алгоритм, позволяющий за конечное число шагов выяснить, принадлежит ли данный многочлен $h = h(x_1,\dots,x_n)$ идеалу I.

Редукция: Предположим, что h_C делится на $(f_i)_C$, т. е. $h_C = (f_i)_C \cdot q$. Положим $h_1 = h - f_i \cdot q$. Тогда $(h_1)_C < h_C$ и $h \in I \Leftrightarrow h_1 \in I$. Таким образом, задачу вхождения теперь

можно решать для h_1. Если за конечное число редукций h сводится к нулю (редуцируется), то $h \in I$.

Базис $f_1, \ldots, f_m$ в I называется *базисом Грёбнера*, если любой $h \in I$ редуцируется к нулю при помощи $f_1, \ldots, f_m$.

Заметим, что $f_1, \ldots, f_m$ — базис Грёбнера в $I \Leftrightarrow I = (f_1, \ldots, f_m)$ и для любого $h \in I$ одночлен h_C делится на некоторый $(f_i)_C$.

Лемма 1. *Пусть $f_1, \ldots, f_m \in I$ такие, что для любого $h \in I$ одночлен h_C делится на $(f_i)_C$ для некоторого i. Тогда $f_1, \ldots, f_m$ — базис Грёбнера в I.*

Упражнение: н.о.д.$(f_C, g_C) = 1 \Rightarrow \{f, g\}$ — базис Грёбнера в $I = (f, g)$.

Таким образом, если нам известен базис Грёбнера идеала I и дан многочлен h, то, проводя всевозможные редукции с помощью элементов базиса, получаем, что $h \in I \Leftrightarrow h$ редуцируется к нулю.

Лемма 2. *Пусть $I \trianglelefteq F[x_1, \ldots, x_n]$. Тогда в I существует базис Грёбнера.*

Доказательство. Рассмотрим идеал, порожденный всеми элементами $f_C, f \in I$, и выберем в нем, по теореме Гильберта о базисе, конечный базис J. Тогда элементы исходного идеала, старшие члены которых образуют базис J, составляют конечный базис Грёбнера в I. □

Пусть $I = (f_1, \ldots, f_m)$. Говорят, что многочлены f_i и f_j допускают *композицию*, если $(f_i)_C$ и $(f_j)_C$ одновременно делятся на некоторый одночлен $g \notin F$.

Если $f_i, f_j \in I$ допускают композицию, т. е. $(f_i)_C = wq_1, (f_j)_C = wq_2$, то рассмотрим их композицию, т. е. многочлен $S(f_i, f_j) = f_i q_2 - f_j q_1 \in I$. Редуцируем $S(f_i, f_j)$ с помощью базиса к элементу $\bar{S}(f_i, f_j)$. Если $\bar{S}(f_i, f_j) = 0$, то говорим, что композиция тривиальна, иначе присоединяем $\bar{S}(f_i, f_j) := f_{m+1}$ к базису $f_1, \ldots, f_m$.

Упражнение: если н.о.д.$(f_C, g_C) = 1$, то $S(f, g) := f g_C - g f_C$ редуцируется к нулю при помощи f, g. В этом случае также говорим, что композиция f и g также тривиальна.

Лемма 3. *Пусть $f_i, i = 1, \ldots, s$, имеет старший член $a_i x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. Тогда если $f = \sum_{i=1}^{s} \lambda_i f_i$ и $f_C < x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, то $f = \sum_{i=1}^{s-1} \gamma_i S(f_i, f_{i+1}), \gamma_i \in F$.*

Доказательство. $S(f_i, f_{i+1}) = \frac{f_i}{a_i} - \frac{f_{i+1}}{a_{i+1}}$, $f = \sum_{i=1}^{s} \lambda_i f_i = \lambda_1 a_1 (\frac{f_1}{a_1} - \frac{f_2}{a_2}) + (\lambda_1 a_1 + \lambda_2 a_2)(\frac{f_2}{a_2} - \frac{f_3}{a_3}) + \ldots + (\lambda_1 a_1 + \ldots + \lambda_{s-1} a_{s-1})(\frac{f_{s-1}}{a_{s-1}} - \frac{f_s}{a_s}) + (\lambda_1 a_1 + \ldots + \lambda_s a_s)(\frac{f_s}{a_s})$. □

Теорема 1. *Для любого набора $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ после присоединения конечного числа нетривиальных композиций получим набор, в котором все композиции тривиальны.*

Доказательство от противного. Если при редуцировании получается бесконечное множество I нередуцируемых многочленов, то рассмотрим идеал J, порожденный их старшими членами. Выбираем в J конечное множество образующих $m_1, \ldots, m_k$. Пусть $f_i \in I$ такие, что $(f_i)_C = m_i, i = 1, \ldots, k$, и пусть $T = \{f_i, i = 1, \ldots, k\}$. Тогда для любого $f \in I \setminus T$ старший член f_C делится на $(f_i)_C$ для некоторого i, т. е. редуцируется. □

Теорема 2 (*Diamond Lemma*). *Базис $f_1, \ldots, f_m$ в I является базисом Грёбнера $\Leftrightarrow$ в базисе $f_1, \ldots, f_m$ все композиции тривиальны.*

Доказательство. В одну сторону утверждение очевидно. Докажем в обратную. Достаточно показать, что $f = \sum h_i f_i$ для любого $f \in I$, где старший член f_C совпадает с $(h_k f_k)_C$ для некоторого k. От противного. Предположим, что $f_C < (h_k f_k)_C$ для некоторого k и такое представление для f выбрано так, что $(h_k f_k)_C$ минимален. Пусть $h_i = (h_i)_C + (h_i)_M$ и $f = \sum_{i=1}^{t}((h_i)_C f_i + (h_i)_M f_i) + \sum_{i=t+1}^{m} h_i f_i$, где $(h_i f_i)_C = a_i x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, для $i = 1, \ldots, t, k < t, a_i \in F$. По лемме 3 имеем $\sum_{i=1}^{t}(h_i)_C f_i = \sum_{i=1}^{t-1} \gamma_i S((h_i)_C f_i, (h_{i+1})_C f_{i+1})$. Так как $(h_i)_C$ являются мономами, то $S((h_i)_C f_i, (h_{i+1})_C f_{i+1})$ делится на $S(f_i, f_{i+1})$. Так как $S(f_i, f_{i+1})$ редуцируется к нулю, то $S(f_i, f_{i+1}) = \sum g_l f_l$ и $S(f_i, f_{i+1})_C = g_k f_k$ для некоторого k. Следовательно, $f = \sum d_l f_l$, где $(d_i f_i)_C < (h_1 f_1)_C$ для любого i. Противоречие. □

7. Системы алгебраических уравнений и базисы Грёбнера.

В данном параграфе всюду $F = \mathbb{C}$.

Теорема 1. *Система S несовместна $\Leftrightarrow$ базис Грёбнера идеала $I(S)$ содержит ненулевую константу.*

Доказательство. Если $0 \neq \alpha \in I(S)$, то система несовместна. Если система несовместна, то, по следствию 4 §5, $1 \in I(S)$. Следовательно, $(f_i)_C$ делит 1 для некоторого f_i из базиса. □

Из следствия 3 §5 имеем

Теорема 2. $S_1 = \{f_i = 0, i = 1, \ldots, m\} \sim S_2 = \{g_i = 0, i = 1, \ldots, k\} \Leftrightarrow f_i \in r((g_1, \ldots, g_k)), g_j \in r((f_1, \ldots, f_m))$ *для любых* i, j.

Теорема 3. *Число решений системы S конечно $\Leftrightarrow$ базис Грёбнера идеала $I(S)$ содержит элементы $f_1, \ldots, f_n$ такие, что $(f_i)_C = x_i^{k_i}$.*

Доказательство. Пусть число решений системы конечно. Переменная x_1 может принимать на множестве решений лишь конечное число значений $\alpha_1, \ldots, \alpha_{n_1}$. Многочлен $f(x_1) = (x_1 - \alpha_1) \ldots (x_1 - \alpha_{n_1}) \equiv 0$ на множестве решений системы S. Следовательно, по теореме Гильберта о нулях существует $k_1 \in \mathbb{N}$ такое, что $f^{k_1} \in I(S)$. Далее, $(f^{k_1})_C = x_1^{n_1 k_1}$. По определению базиса Грёбнера существует f_1 в этом базисе такой, что $(f_1)_C$ делит $(f^{k_1})_C$, т. е. является степенью x_1. Аналогично и для остальных переменных.

Обратно, если $f_1, \ldots, f_n$ — такие элементы базиса Грёбнера, что $(f_i)_C = x_i^{n_i}$, то, в силу порядка, f_n зависит только от x_n, т. е. x_n может принимать лишь конечное число значений. Аналогично, f_{n-1} зависит только от x_n и x_{n-1} и его старший член не равен нулю при любых значениях x_n. Следовательно, x_{n-1} принимает конечное число значений, и т. д. $\square$