A. L. Chistov, Polynomial-time factoring of polynomials and finding the compounds of a variety within the aubexponential time, *Zap. Nauchn. Sem. LOMI*, 1984, Volume 137, 124–188

А.Л.Чистов

АЛГОРИТМ ПОЛИНОМИАЛЬНОЙ СЛОЖНОСТИ ДЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНОВ И НАХОЖДЕНИЕ КОМПОНЕНТ МНОГООБРАЗИЯ В СУБЭКСПОНЕНЦИАЛЬНОЕ ВРЕМЯ

Введение

В работе предложен алгоритм полиномиальной сложности для разложения многочленов от многих переменных на неприводимые множители над полем конечнопорожденным над простым подполем. Другим новым результатом является алгоритм для разложения алгебраического многообразия на компоненты. В широком классе случаев полученная оценка сложности этого алгоритма неулучшаема.

В [4] описан алгоритм полиномиальной сложности для разложения многочленов от многих переменных над конечным полем (там же можно найти исторический обзор, см. также [8]). В настоящей работе построен алгоритм полиномиальной сложности для разложения многочленов от многих переменных над полями, конечнопорожденными над простыми подполями, см. основную теорему главы I (этот результат значительно расширяет результат [8]). Кроме того, в главе I предлагается ряд приложений основной теоремы главы I.

Пусть основное поле $F = H(T_1,\dots,T_\ell)[\eta]$, где либо $H=\mathbb{Q}$, либо $H=\mathbb{F}_q\langle x\rangle$, $q=\mathrm{char}(F)$, элементы $T_1,\dots,T_\ell$ алгебраически независимы над H; элемент η сепарабелен и алгебраичен над $H(T_1,\dots,T_\ell)$, обозначим через $\varphi = \sum_{0\le i\le \deg_Z(\varphi)} (\varphi_i^{(1)}/\varphi^{(2)}) Z^i \in H(T_1,\dots,T_\ell)[Z]$ его минимальный многочлен над $H(T_1,\dots,T_\ell)$ со старшим коэффициентом $lc_Z(\varphi)=1$, причем $\varphi_i^{(1)}, \varphi^{(2)} \in H[T_1,\dots,T_\ell]$ и $\deg(\varphi^{(2)})$ наименьшая возможная. Всякий элемент $f \in F[X_0,\dots,X_n]$ однозначно представляется в виде

$$f = \sum_{0\le i\le \deg_Z(\varphi);\, i_0,\dots,i_n} (a_{i,i_0,\dots,i_n}/b)\eta^i X_0^{i_0}\cdots X_n^{i_n}$$

где $a_{i,i_0,\dots,i_n}, b \in H[T_1,\dots,T_\ell]$ и $\deg(b)$ наименьшая возможная, многочлены $a_{i,i_0,\dots,i_n}$, b определены однозначно с

точностью до множителя из H^*. Положим $\deg_{T_j}(f) = \max_{i,i_0,\dots,i_n} \{\deg_{T_j}(a_{i,i_0,\dots,i_n}), \deg_{T_j}(b)\}$ Под длиной записи $l(h)$ в случае $h \in \mathbb{Q}$ будем понимать его битовую длину, а в случае $h \in \mathbb{F}_q$ $\varkappa$ - величину $\varkappa \log_2 q$. Через $l(f)$ обозначим максимум длин записей коэффициентов из H при мономах от $T_1, \dots, T_\ell$ в многочленах $a_{i,i_0,\dots i_n}, b$. В качестве размера $L_1(f)$ многочлена f в главе I будем рассматривать величину $(\max_{0\le i\le n} \deg_{X_i}(f)+1)^{n+\ell+1}(\max_{1\le j\le \ell} \deg_{T_j}(f)+1)^{\ell}(\deg_Z(\varphi)+1)l(f)$, аналогично

$$L_1(\varphi)=(\deg_Z(\varphi)+1)\left(\max_{1\le j\le \ell} \deg_{T_j}(\varphi)+1\right)^{\ell} l(\varphi).$$

На протяжении главы I предполагаем, что выполнены следующие оценки

$$\deg_{T_j}(\varphi)<r_1, \deg_Z(\varphi)<r_1, \deg_{X_i}(f)<r, \deg_{T_j}(f)<r_2, l(\varphi)\le M_1, l(f)\le M_2 \quad (I)$$

для всех i, j

ОСНОВНАЯ ТЕОРЕМА ГЛАВЫ I. Многочлен f можно разложить на неприводимые над F множители за полиномиальное от $L_1(f), L_1(\varphi), q$ время.

В § I главы I описано полиномиальное сведение для разложения многочлена над конечным расширением поля к разложению многочленов над подполем.

В § 2 завершается доказательство основной теоремы главы с помощью предложенной автором некоторой эффективной версии теоремы Гильберта о неприводимости (теорема I.2), а также сведéния разложения в $\mathbb{Z}[X_0,\dots,X_n]$ к разложению в кольцах $\mathbb{Z}[X]$ и в $\mathbb{F}_q[X_0,\dots,X_n]$ для подходящих простых q, и наконец, с использованием § I.

В § 3 описаны полиномиальные алгоритмы для абсолютного разложения многочленов, для построения примитивного элемента в конечном расширении полей, а также алгоритм для нахождения группы Галуа многочлена, работающий полиномиальное время от размера многочлена и порядка группы Галуа (см. также § I [9]).

Пусть даны многочлены $f_0,\dots,f_{k-1} \in F[X_0,\dots,X_n]$ (не ограничивая общности считаем, что $f_0,\dots,f_{k-1}$ линейно независимы). В действительности, в главе II предложен принадлежащий автору алгоритм, который разлагает произвольное проективное алгебраическое многообразие на неприводимые компоненты, поэтому можно считать,

что $f_0,\dots,f_{K-1}\in F[X_0,\dots,X_n]$ – однородные относительно $X_0,\dots,X_n$ многочлены (сведение общего случая к однородному см. в замечании 2 § 3). На протяжении главы II предполагаем, что выполнены следующие оценки

$$\deg_{T_1,\dots,T_\ell,Z}(\varphi)<d_1,\ \deg_{X_0,\dots,X_n}(f_i)<d,\ \deg_{T_1,\dots,T_\ell}(f_i)<d_2,$$
$$l(\varphi)\le M_1,\ l(f_i)\le M_2 \qquad (2)$$

для всех $0\le i\le K-1$.

В главе II под размером $L_2(f_i)$ будем понимать величину $\binom{d+n}{n} d_1 d_2^{\ell}\, l(f_i)$, аналогично $L_2(\varphi)=d_1^{\ell+1}\, l(\varphi)$.

Проективное многообразие $\{f_0=\dots=f_{K-1}=0\}\subset \mathbb{P}^n(\bar F)$ корней системы $f_0=\dots=f_{K-1}=0$ разложимо на компоненты $\{f_0=\dots=f_{K-1}=0\}=\bigcup_\alpha W_\alpha\subset \mathbb{P}^n(\bar F)$ [7], при этом компонента W_α определена и неприводима над максимальным чисто несепарабельным расширением $F^{q^{-\infty}}$ поля F [6]. Далее $W_\alpha=\bigcup_\beta W_{\alpha\beta}$, где (абсолютно неприводимые) компоненты $W_{\alpha\beta}$ определены и неприводимы над алгебраическим замыканием $\bar F$ поля F . Предлагаемый в настоящей работе алгоритм находит все компоненты W_α , а затем $W_{\alpha\beta}$ (фактически, W_α , $W_{\alpha\beta}$ определены над некоторыми конечными расширениями поля F , которые также строятся алгоритмом). Мы (а также алгоритм) будем представлять всякую компоненту W_α или $W_{\alpha\beta}$ следующими двумя способами: посредством ее общей точки [3], и с другой стороны, некоторой системой алгебраических уравнений, такой что многообразие ее корней совпадает с рассматриваемой компонентой, в подобных случаях будем говорить, что система задает многообразие.

Время работы построенного в главе II алгоритма полиномиально от размера $L_2=L_2(f_0)+\dots+L_2(f_{K-1})$ и от d^{n^2} в случае, когда основное поле $F=\mathbb{Q}$ или F – конечно (см. также §§ 5,6,7 [10]). В [4] описан принадлежащий Д.Ю.Григорьеву алгоритм, также находящий компоненты W_α , в оценку времени которого входит $d_2^{n^3}$ (см. также §§ 3,4 [9],[10]). Улучшение оценки до d^{n^2} потребовало разработки существенно новых конструкций. Фактически, оценка времени работы даже лучше. Например, когда основное поле $F=\mathbb{Q}$ или F – конечное поле, алгоритм находит компоненты W_α многообразия корней системы в полиномиальное от d^{nC} и от L_2 время, где $C=1+\max_\alpha \dim W_\alpha$. Отметим, что число компонент W_α не превосходит $(d-1)^n$ в силу теоремы

Безу ([7]), с другой стороны, число коэффициентов в многочленах в исходной системе оценивается сверху, в общем случае, как $\binom{d+n-1}{n} \leq d^n$. Таким образом, для маленьких C оценка времени работы полиномиальна от L и от ожидаемого размера выхода алгоритма. Кроме того, в верхнюю оценку размера представления компоненты также входит величина d^{nC} при $1 \leq C \leq n/2$.

Переходим теперь к точной формулировке основного результата главы II.

Пусть $W \subset \mathbb{P}^n(\bar{F})$ многообразие, $\operatorname{codim}_{\mathbb{P}^n}(W) = m$, определенное и неприводимое над некоторым полем F_1, являющимся конечным расширением поля F и F_2 – максимальное подполе поля F_1, являющееся сепарабельным расширением поля F. Пусть $t_1, \ldots, t_{n-m}$ – алгебраически независимы над F. Общая точка многообразия W может быть задана следующим изоморфизмом полей:

$$F_2(t_1,\ldots,t_{n-m})[\theta] \cong F_2\left(\frac{X_{j_1}}{X_{j_0}},\ldots,\frac{X_{j_{n-m}}}{X_{j_0}},\left(\frac{X_0}{X_{j_0}}\right)^{q^\nu},\ldots,\left(\frac{X_n}{X_{j_0}}\right)^{q^\nu}\right) \subset F_1(W) \qquad (*)$$

для некоторого q^ν и индекса $0 \leq j_0 \leq n$, где θ – алгебраический сепарабельный элемент над полем $F_2(t_1,\ldots,t_{n-m})$, и $\Phi(Z)$ его минимальный многочлен, $lc_Z(\Phi) = 1$; элементы X_j/X_{j_0} рассматриваются здесь как рациональные функции на многообразии W, причем W не содержится в гиперплоскости, определяемой уравнением $X_{j_0} = 0$; при изоморфизме $(*)$ $t_i \to X_{j_i}/X_{j_0}$, $1 \leq i \leq n-m$. Примем соглашение, что $\nu > 0$ при $q > 0$ и $q^\nu = 1$ в случае $\operatorname{char}(F) = 0$.

ОСНОВНАЯ ТЕОРЕМА ГЛАВЫ II. а) Предлагается алгоритм, который для каждой компоненты W_α определяет ее общую точку и строит некоторое семейство однородных многочленов $\Psi_1^{(\alpha)}, \ldots, \Psi_N^{(\alpha)} \in F[X_0,\ldots,X_n]$, таких, что множество корней системы $\Psi_1^{(\alpha)} = \ldots = \Psi_N^{(\alpha)} = 0$ совпадает с W_α. Обозначим $m = \operatorname{codim} W_\alpha$, $\theta_\alpha = \theta$, $\Phi_\alpha = \Phi$. Тогда $q^\nu \leq d^{2m}$, $\deg_Z(\Phi_\alpha) \leq \deg W_\alpha \leq (d-1)^m$; для всех i, j степени $\deg_{T_1,\ldots,T_\ell,t_1,\ldots,t_{n-m}}(\Phi_\alpha)$, $\deg_{T_1,\ldots,T_\ell,t_1,\ldots,t_{n-m}}\left((X_j/X_{j_0})^{q^\nu}\right)$ (последняя степень определяется согласно изоморфизму из $(*)$) оцениваются сверху некоторым полиномом от d^m, d_1, d_2 первой степени относительно d_2, далее размеры эле-

ментов $\Phi_\alpha, (X_j/X_{j_0})^{q^\nu}$ оцениваются сверху некоторым полиномом от M_1, $M_2, (d^m d_1 d_2)^{n-m+\ell+1}$. Число уравнений $N \leq m^2 d^{4m}$, степени $\deg_{X_0,\dots,X_n}(\Psi_s^{(\alpha)}) \leq d^{2m}$ и степени $\deg_{T_1,\dots,T_\ell}(\Psi_s^{(\alpha)})$ оцениваются сверху некоторым полиномом от d^m, d_1, d_2 первой степени относительно d_2, и всякое $\Psi_s^{(\alpha)}$ алгоритм представляет в виде $\Psi_s^{(\alpha)} = \overline{\Psi}_s^{(\alpha)}(Z_{s,0},\dots,Z_{s,n-m+2})$, где $Z_{s,j}$ суть некоторые линейные формы от $X_0,\dots,X_n$ с коэффициентами из поля H, размер всякого элемента $\overline{\Psi}_s^{(\alpha)} \in F[Z_{s,0},\dots,Z_{s,n-m+2}]$ не превосходит некоторого полинома от M_1, $M_2, (d^m d_1 d_2)^{n-m+\ell+1}$, размер формы $Z_{s,j}$ не превосходит некоторого полинома от $n, \log(d d_1 d_2 + 1)$ для всех s,j. Общее время работы алгоритма оценивается сверху некоторым полиномом от $M_1, M_2, (d^n d_1 d_2)^{c+\ell}, q$. Последняя величина, очевидно, не превосходит $O(L_2^{c+\ell+1}(q+1)) \leq O(L_2^{\log L_2}(q+1))$ при $n = O(d)$.

в) Можно построить алгоритм, который для каждой абсолютно неприводимой компоненты $W_{\alpha\beta}$ находит максимальное сепарабельное подполе $F_2 = F[\xi_\alpha]$ минимального поля определения F_1 (содержащего F) многообразия $W_{\alpha\beta}$. Алгоритм строит общую точку многообразия $W_{\alpha\beta}$ и некоторую определяющую многообразие $W_{\alpha\beta}$ систему уравнений с коэффициентами из поля F_2. Для параметров общей точки и системы уравнений выполнены те же оценки, что и в пункте а). Пусть $\varphi_{\alpha\beta} \in F[Z]$ минимальный многочлен для $\xi_{\alpha\beta}$ и $lc_Z(\varphi_{\alpha\beta}) = 1$, тогда $\deg_Z(\varphi_{\alpha\beta}) \leq \deg W_{\alpha\beta}$, степени $\deg_{T_1,\dots,T_\ell}(\varphi_{\alpha\beta})$ оцениваются сверху некоторым полиномом от d^m, d_1, d_2 первой степени относительно d_2, размеры полиномов $\varphi_{\alpha\beta}$ оцениваются сверху некоторым полиномом от $M_1, M_2, (d^m d_1 d_2)^{\ell+1}$. Оценка времени работы такая же, как в пункте а).

Отметим, что верхняя оценка размера выхода алгоритма из теоремы по порядку такая же, как и приведенная в теореме оценка времени работы, поэтому на дальнейшее улучшение времени работы можно надеяться лишь при другом, отличном от предложенного, представлении компонент многообразия. Автор позволяет себе высказать гипотезу о том, что возможно находить компоненты в полиномиальное от $d^{(c+\ell)n}(d_1 d_2)^{n+\ell}$ и от L_2 время, где $c' = \max_\alpha \min\{\dim W_\alpha + 1, \operatorname{codim} W_\alpha\}$.

В параграфе I главы II основная идея – шевеление многообра-

зия для приведения его в общее положение с последующим предельным переходом для нахождения компонент W_α исходного многообразия. Оценка времени работы алгоритма (см. теорему 2.1) близка к требуемой в основной теореме а).

Параграф 2 посвящен конструкции системы уравнений, задающей данную компоненту, представленную исходно своей общей точкой (см. теорему 2.2). Основываясь на теореме 2.2 (см. следствие из теоремы 2.2) мы получаем оценку времени работы для некоторым образом модифицированного алгоритма из § I, которая полиномиальна от $M_1, M_2, (d^m d_1 d_2)^{n+l}, q$.

Отметим, что время работы алгоритма при построении каждой из компонент W_α коразмерности m полиномиально от M_1, $M_2, (d^m d_1 d_2)^{n+l}, q$. Эта оценка лучше, чем в основной теореме, при малых m. Поэтому, если $c_1 = \max_\alpha \operatorname{codim} W_\alpha$ – коразмерность искомого многообразия, то через c_1 шагов работы в дереве компонент алгоритм уже фактически построит все компоненты W_α со временем работы полиномиальным от $M_1, M_2, (d^{c_1} d_1 d_2)^{n+l}$, q, но вообще говоря, придется строить все дерево компонент до конца. Если бы мы располагали достаточно быстрым алгоритмом вычисления коразмерности c_1, то тогда алгоритм строил бы компоненты W_α за только что указанное время.

В § 3 предлагается метод нахождения компонент W_α, который в отличие от алгоритмов из § I строит только некоторую часть дерева компонент. Этот метод приводит к требуемой в основной теореме а) оценке времени, см. теорему 2.3. Замечания в конце § 3 показывают, что основная теорема главы II позволяет отвечать на основные вопросы о системах алгебраических уравнений, например, о пустоте, размерности многообразия корней и т.п.

В § 4 излагается алгоритм, требуемый в пункте в) основной теоремы с той же оценкой времени работы, что и приведенная выше.

В процессе своей работы алгоритмы из основной теоремы расширяли поле H (см. выше) в случае, когда H конечно, и все общие точки и системы уравнений оказываются определенными над композитом основного поля F и некоторого конечного расширения поля H: В заключение § 4 мы показываем, как вернуться к представлению общих точек компонент W_α над исходным основным полем F (или, соответственно, над минимальными полями определения абсолютно неприводимых компонент $W_{\alpha\beta}$), и как построить систему уравнений над F (или, соответственно, над минимальными полями определения компонент $W_{\alpha\beta}$, задающую компоненту W_α (или, соответственно $W_{\alpha\beta}$); последнее построение в случае бесконечного F.

ГЛАВА I. РАЗЛОЖЕНИЕ МНОГОЧЛЕНОВ ОТ МНОГИХ ПЕРЕМЕННЫХ НА НЕПРИВОДИМЫЕ МНОЖИТЕЛИ В ПОЛИНОМИАЛЬНОЕ ВРЕМЯ

§ I. Разложение многочленов над конечными расширениями

Пусть $K = F[\theta] \supset F$ – конечное расширение полей и $0 \neq \psi \in F[Z]$ – минимальный многочлен для θ.

ПРЕДЛОЖЕНИЕ I.I. Допустим, что имеется полиномиальный алгоритм для разложения многочленов из $K[X]$. Тогда всякий многочлен $f \in F[X]$ можно разложить на неприводимые над F множители в полиномиальное время.

ДОКАЗАТЕЛЬСТВО. Можно считать, что старший коэффициент $lc(f) = 1$. Разложим $f = \prod_i f_i$ на неприводимые множители над K, где $lc(f_i) = 1$. Для всякого i вычислим норму ([I]) $g_i = N(f_i) = N_{K(X)/F(X)}(f_i) \in F[X]$ на основе леммы I.I (см. ниже) в полиномиальное время. Покажем, что $g_i = \tilde{g}_i^{\,\kappa_i} q^{d_i}$, где κ_i взаимно просто с q и $\tilde{g}_i \in F[X]$ неприводимо над F. Действительно, предположим противное, пусть $g_i = h_1^{d_1} \dots h_s^{d_s}$, где $h_i \in F[X]$ неприводимы над F и $s \geqslant 2$. Один из множителей h_j, скажем h_1, делится на f_i. Для некоторого вложения $\sigma : K \subset \overline{K}$ над F многочлен h_2 не взаимно прост с $\sigma(f_i)$ ([6]), следовательно, $\sigma(f_i) \mid h_2$, так как $\sigma(f_i) \in \sigma(K)[X]$ и неприводим над $\sigma(K)$. Поэтому $f_i \mid h_2$. Итак, h_1 и h_2 не взаимно просты, что доказывает равенство $g_i = \tilde{g}_i^{\,\kappa_i} q^{d_i}$.

Найдем сначала $\tilde{g}_i^{\,\kappa_i}$. С помощью алгоритма из условия предложения можно найти $h \in K[X]$, если h существует, такой что $g_i = h^q$. Затем следует проверить, верно ли, что $h \in F[X]$, и повторить эту процедуру. Далее, вычисляем наибольший общий делитель g многочленов $\tilde{g}_i^{\,\kappa_i}$ и $(\tilde{g}_i^{\,\kappa_i})'$, и находим $\tilde{g}_i = \tilde{g}_i^{\,\kappa_i}/g$. Окончательно $f = \prod_i \tilde{g}_i^{\,\beta_i}$ – разложение на неприводимые над F, и β_i находятся путем последовательного деления f на $\tilde{g}_i$, что завершает доказательство предложения.

Основным содержанием настоящего параграфа является доказательство обратного утверждения к предложению. Пусть теперь F – бесконечное поле. Далее будем предполагать, что

а) элементы F могут быть заданы эффективно;

в) имеется некоторый алгоритм для вычисления определителей с коэффициентами из F;

с) имеется некоторая процедура разложения многочленов от

одной переменной над F .

В дальнейшем ниже мы будем ссылаться на эти пункты а),в), с) без всякого специального напоминания (в §1).

Пусть h некоторая верхняя граница для времени работы алгоритмов из пунктов в), с). Рассмотрим примитивное алгебраическое сепарабельное расширение $K=F[\theta]$ и пусть $\varphi(\theta)=0$, $0\neq\varphi\in F[t]$ и φ неприводим над F . Через $L_1(\varphi)$ мы будем обозначать в дальнейшем размер многочлена φ (длина записи коэффициентов полинома φ определяется на основании пункта а)). Пусть $f\in K[X]$ и старший коэффициент f равен I. Мы рассматриваем элементы K как полиномы от θ степени меньше, чем $deg(\varphi)$. Используя такое представление элементов K , естественным образом можно определить длину $L_1(f)$.

ТЕОРЕМА I.I. Разложение на неприводимые многочлены f над полем K может быть осуществлено за время $P(h,L_1(\varphi),L_1(f))$ для некоторого полинома P .

Излагаемое ниже доказательство сходно по идее с доказательством из [22] , но непосредственно конструкция из [22] не может быть применена, т.к. там разложение над K сводится к разложению над F многочлена от двух переменных, в то время как наша редукция приводит к случаю многочленов от одной переменной.

ДОКАЗАТЕЛЬСТВО. Опишем прежде всего процедуру извлечения корня q-ой степени в K , если $q=char(F)>0$. Элементы $1,\theta^q,\theta^{2q},\ldots,\theta^{(deg\varphi-1)q}\in K$ линейно независимы над F , так как расширение $F[\theta^q]\subset F[\theta]$ чисто несепарабельно и $F\subset F[\theta]$ сепарабельно и, следовательно, $F[\theta^q]=F[\theta]$. Для любого $a\in K$ запишем a в виде $a=\sum_{0\leqslant i<deg(\varphi)} a_i\theta^{qi}$, где $a_i\in F$.
Тогда $a^{1/q}\in K$ эквивалентно тому, что $a_i^{1/q}\in F$ для любого i . Это можно легко проверить возведением в q-ю степень элементов общего вида из поля K . Для извлечения корня q-ой степени в F мы пользуемся с) для F .

Пусть $f=\sum c_j X^{jq^s}$ и S максимально возможное, если $q>0$, и $q^s=1$, если $char(F)=0$. Введем многочлен $g(Z)=\sum_j c_j Z^j$, тогда производная $g'\not\equiv 0$. Предположим, что у нас есть разложение $g=\prod_i g_i^{m_i}$ над K , где g_i - неприводимые попарно взаимно простые многочлены. Тогда $f=\prod_i f_i^{m_i}$, где $f_i(X)=g_i(X^{q^s})$. Фиксируем некоторый индекс i на некоторое время и положим $f_i(X)=\prod_{1\leqslant j\leqslant \varkappa} f_{ij}^{m_{ij}}(X)$ - разложение на неприводимые множители над K. Пусть $g_i(Z)=\prod_\alpha (Z-t_\alpha)^{e_\alpha}$

для $t_\alpha \in \bar{K}$. Тогда $f_i(X)=\prod_\alpha (X^{q^s}-t_\alpha)^{e_\alpha}=\prod_\alpha (X-t_\alpha^{1/q^s})^{e_\alpha q^s}$. Так как f_{ij} для различных j взаимно просты, мы получаем $f_{ij}^{m_{ij}}=\prod (X-t_\alpha^{1/q^s})^{e_\alpha q^s}$, где произведение берется над некоторым подмножеством α. Следовательно, $f_{ij}^{m_{ij}} = \sum_\beta d_{ij\beta} X^{\beta q^s}$, где $d_{ij\beta} \in K$. Отсюда вытекает, что $\varkappa = 1$, так как g_i неприводимы. Следовательно, $f = \prod_i f_{i1}^{m_i'}$ (где $m_i' = m_i m_{i1}$) - разложение f над K. Пусть $m_{i1} = q^{s_i} r_i$, где r_i взаимно просто с q. Многочлен $f_{i1}^{m_{i1}}(X) = f_i(X) = g_i(X^{q^s})$ имеет корни (в $\bar{K}$) кратностей, делящихся на m_{i1}. Так как g_i неприводим над K, то кратность любого его корня (в $\bar{K}$) есть некоторая степень q, следовательно, $r_i = 1$. Итак, чтобы найти f_{i1}, надо извлекать несколько раз, начиная с многочлена f_i, до тех пор пока это возможно, корень q-ой степени. Осуществляя это для всех i, мы получим разложение $f = \prod_i f_{i1}^{m_i'}$ над K (напомним, что мы предполагаем, что имеется разложение g).

Итак мы можем далее рассматривать только такие f, что производная $f' \not\equiv 0$. Если для наибольшего общего делителя выполнено $0 < \deg g.c.d.(f, f') < \deg f$, то мы получаем как и выше нетривиальный делитель $g = g.c.d.(f, f')$ (для вычисления g опирается на [II]) многочлена f и применяем далее описываемую процедуру к g и f/g по отдельности. В противном случае, многочлены f и f' взаимно просты и, следовательно, f сепарабельный. Поэтому мы будем предполагать ниже, что f сепарабельный.

Напомним теперь понятие нормы $N(g)$ многочлена $g \in K[X]$ из $K[X]$ в $F[X]$ (см. [1]). Именно, $N(g) = \prod_\sigma g^\sigma$, где σ пробегает все различные тождественные на F вложения поля K в некоторое фиксированное алгебраическое замыкание $\bar{K}$ поля K (тогда θ^σ пробегает по одному разу каждый все сопряженные к θ элементы из поля $\bar{K}$ и кроме того $K^\sigma = F[\theta^\sigma]$). Действие σ на g покоэффициентное и тождественное на X. Мы формулируем некоторые хорошо известные утверждения о норме в следующей лемме.

ЛЕММА I.I. *а)* Пусть $U_g : K(X) \to K(X)$ - линейный оператор умножения на g, где $K(X)$ рассматривается как векторное пространство над $F(X)$ размерности $\deg(\varphi)$. Тогда

$N(g)=\det(U_g)\in F(X)$; $\beta)$ $N(g)$ можно вычислить в полиномиальное от $L_1(g), L_1(\varphi)$ время.

Для доказательства части $\alpha)$ см., например, [I]. Часть $\beta)$ следует из $\alpha)$, поскольку определитель матрицы с коэффициентами из $F[X]$ может быть вычислен при помощи интерполяции аналогично [21], причем вычисление определителей над F основывается на пункте $\beta)$ из начала параграфа.

Пусть $f=\prod_i g_i(X)$ - разложение f на неприводимые множители над K, кроме того старшие коэффициенты всех g_i равны I. Для произвольного $y\in F$ рассмотрим многочлен $f(X+\theta y)$, и тогда $f(X+\theta y)=\prod_i g_i(X+\theta y)$ - его разложение на неприводимые множители над K. Очевидно $N(f(X+\theta y))=\prod_i N(g_i(X+\theta y))$. Обозначим $r=deg(\varphi)(deg(f))^2+1$, и пусть $y_1,\dots,y_r\in F$ - некоторые попарно различные элементы. Пусть $N(f(X+\theta y_m))=\prod_j h_{mj}$ - разложение на неприводимые множители над F $(1\le m\le r)$, и кроме того старшие коэффициенты всех h_{mj} равны I.

ЛЕММА I.2. Пусть для всех m, j $(1\le m\le r)$ утверждение $0<deg\, g.c.d.(h_{m,j}, f(X+\theta y_m))<deg\, f$ ложно, тогда f неприводим над K.

ДОКАЗАТЕЛЬСТВО. Для любых i, m выполняется соотношение $f(X+\theta y_m)\mid N(g_i(X+\theta y_m))$, так как иначе согласно условию, сформулированному в лемме, $\psi=g.c.d.(f(X+\theta y_m), N(g_i(X+\theta y_m)))=1$, но это невозможно, поскольку $g_i(X+\theta y_m)\mid\psi$.

Предположим, что g_{i_1}, g_{i_2} - два различных неприводимых множителя f. Тогда для каждого m существует такое вложение $\sigma=\sigma^{(m)}_{i_1 i_2}: K\subset\overline{K}$, тождественное на F, что $g.c.d.(g_{i_1}(X+\theta y_m), g_{i_2}^{\sigma}(X+\theta^{\sigma} y_m))\neq 1$. Действительно, если это не так, то любые два корня (в $\overline{K}$) многочленов $g_{i_1}(X+\theta y_m)$ и $g_{i_2}(X+\theta y_m)$ не сопряжены над F и, следовательно, $\mu=g.c.d.(N(g_{i_1}(X+\theta y_m)), N(g_{i_2}(X+\theta y_m)))=1$. Но это невозможно, так как $f(X+\theta y_m)\mid\mu$.

Для по крайней мере $(deg(f))^2+1$ попарно различных индексов $1\le m\le r$ соответствующие вложения $\sigma=\sigma^{(m)}_{i_1 i_2}$ совпадают (по принципу Дирихле). Не теряя общности, будем предполагать, что эти индексы есть $1\le m\le (deg\, f)^2+1$.

Рассмотрим следующий результант (относительно X): $R(Y) = Res_X(g_{i_1}(X+\theta Y),\ g_{i_2}^{\sigma}(X+\theta^{\sigma}Y)) \in \bar{K}[Y]$ (здесь Y - новая переменная). Так как $deg_Y R(Y) \leq (deg\, g_{i_1} + deg\, g_{i_2})^2 \leq (deg\, f)^2$, то $R(Y)$ имеет самое большее $(deg\, f)^2$ различных корней. Но с другой стороны, $R(y_m)=0$ для всех $1 \leq m \leq (deg\, f)^2 + 1$, следовательно, $R(Y) \equiv 0$ тождественно. Поэтому $g.c.d.(g_{i_1}(X+\theta Y),\ g_{i_2}^{\sigma}(X+\theta^{\sigma}Y)) \neq 1$, поскольку старшие коэффициенты (относительно X) многочленов g_{i_1}, g_{i_2} оба равны I. Мы покажем, что это возможно, только если $\theta^{\sigma} = \theta$ и, следовательно, $g_{i_2}^{\sigma} = g_{i_2}$, так как $g_{i_2} \in F[\theta][X]$. Это приводит к противоречию с сепарабельностью f , поскольку тогда $g.c.d.(g_{i_1}, g_{i_2}) \neq 1$.

Итак предположим, что для некоторого $h \in \bar{K}[X,Y]$, такого что $deg_{X,Y} h \geq 1$ (в $\bar{K}[X,Y]$) выполняются соотношения $h \mid g_{i_1}(X+\theta Y)$ и $h \mid g_{i_2}^{\sigma}(X+\theta^{\sigma}Y)$. Пусть $g_{i_1}(X) = \prod_{\alpha \in A}(X-a_\alpha)$, $g_{i_2}(X) = \prod_{\beta \in B}(X-b_\beta)$ для некоторых $a_\alpha, b_\beta \in \bar{K}$. Тогда $h = a^{(0)} \prod_{\bar{\alpha} \in \bar{A}}(X+\theta Y - a_{\bar{\alpha}}) = b^{(0)} \prod_{\bar{\beta} \in \bar{B}}(X+\theta^{\sigma}Y - b_{\bar{\beta}})$, где произведения берутся по некоторым подмножествам $\bar{A} \subset A$ и $\bar{B} \subset B$ и $a^{(0)}, b^{(0)} \in \bar{K}$. Принимая во внимание факториальность кольца $\bar{K}[X,Y]$ и то, что $deg_{X,Y} h \geq 1$, мы получаем, что $\theta = \theta^{\sigma}$. Это завершает доказательство леммы I.2.

Основываясь на лемме I.2, несложно дать полиномиальный алгоритм для разложения f на неприводимые. Именно, используя пункт c) из начала параграфа для поля F , найдем для каждого $1 \leq m \leq r$ разложение на неприводимые множители над F многочлена $N(f(X+\theta y_m)) = \prod_j h_{mj}$ (для вычисления нормы применяем часть β) леммы I.I) и вычислим для всех m, j (используя например, [II]) $u_{m,j}(X+\theta y_m) = g.c.d.(f(X+\theta y_m), h_{m,j})$.

Если $0 < deg(u_{m,j}) < deg\, f$ для некоторых m, j , то применяем описываемый алгоритм к многочленам $u_{m,j}$ и $f/u_{m,j}$ по отдельности (вместо f). В противном случае f неприводим.

Простой анализ времени работы предложенного алгоритма завершает доказательство теоремы I.I.

Отметим, что фактически мы доказали выполнение пунктов a),

в),с) (см.начало параграфа) для поля K .

Рассмотрим теперь случай примитивного алгебраического расширения (не обязательно сепарабельного) $K=F[\theta]\supset F$, причем как и выше $\varphi(\theta)=0$ и φ неприводим над F . В этом случае аналог теоремы I.I неверен (см. [I9] , [22]). Однако справедлива некоторая более слабая ее версия. Пусть $\varphi(t)=\varphi_1(t^{q^s})$, где $\varphi_1\in F[t]$ и s – наибольшее возможное. Тогда многочлен φ_1 сепарабелен и неприводим. Рассмотрим поле $K_1=F[\theta^{q^s}]$. Расширение $K_1\subset K$ чисто несепарабельно [6] , а расширение $F\subset K_1$ сепарабельно.

В дополнение к а), в), с) (см.начало параграфа) сделаем здесь предположение, что задан базис $\{\alpha_1,\dots,\alpha_\varkappa\}$ чисто несепарабельного расширения $F^q\subset F$ вместе с таблицей умножения (считаем здесь и ниже, что степень $[F:F^q]=q^{\deg_{F_q}F}<\infty$). Легко видеть [3] , что $\{\alpha_1,\dots,\alpha_\varkappa\}$ является также базисом расширения $K_1^q\subset K_1$. Тогда, во-первых, мы можем построить подполе $K_1^q[\theta^q]=K^q\subset K$ (в качестве его базиса над K_1^q можно взять, например, $1,\theta^q,\theta^{2q},\dots,\theta^{(q^s-1)q}$) и, во-вторых, мы можем построить базис $\{\beta_1,\dots,\beta_\varkappa\}$ поля K над K^q следующим образом. Семейство $\{\alpha_i\theta^j\}_{1\le i\le\varkappa,\,0\le j\le q^s-1}$ образует базис K над K_1^q , **следовательно, можно выбрать базис K над K^q из этого семейства, если только мы можем проверить линейную зависимость над K^q произвольного семейства элементов $e_1,\dots,e_m\in K$. Для проверки этого запишем соотношение линейной зависимости в виде** $\sum_{1\le j\le m}\Big(\sum_{0\le i\le q^s-1}Z_i\theta^{qi}\Big)e_j=0$, **где Z_i – неизвестные из поля K_1^q , и выясним имеет ли данная линейная система решение.**

В результате мы получаем возможность решать в поле K уравнения вида $X^q-\alpha=0$, где $\alpha\in K$ (если $\alpha\in K^q=K_1^q[\theta^q]$, то мы можем свести решение уравнения $X^q-\alpha=0$ к некоторому числу аналогичных уравнений в поле K_1).

Перейдем теперь к разложению над полем K многочлена f . Коэффициенты многочлена f^{q^s} принадлежат K_1 . Пусть $f^{q^s}=\prod_i g_i$ – разложение на неприводимые многочлены над K_1 (некоторые из g_i могут совпадать). Для всякого i вычислим $g.c.d(g_i,f)$, используя, например, субрезультантный алгоритм [II] (в дальнейшем, для вычисления $g.c.d$ мы будем всегда использовать субрезультантный алгоритм). Для вычисления определителей мы используем в). Если $0<\deg g.c.d.(g_i,f)<$

$deg\ f$ (обозначим $\overline{f} = g.c.d.(g_i, f)$) для некоторого i, то мы получаем нетривиальный делитель $\overline{f}$ многочлена f и продолжим применение описываемой процедуры к $\overline{f}$ вместо f и к частному $f/\overline{f}$ по отдельности.

Предположим теперь, что $f \mid g_i$ для всякого i. Отсюда следует, что f – степень неприводимого над K многочлена. Иначе, если $f = f_1^{m_1} \dots f_\omega^{m_\omega}$ – разложение на неприводимые над K, многочлены f_i попарно взаимно просты и $\omega > 1$, то $g_i \mid (f_1^{m_1})^{q^s}$ для некоторого i и, следовательно, $f \mid (f_1^{m_1})^{q^s}$, что приводит к противоречию и, следовательно, $\omega = 1$, т.е. $f = f_1^{m_1}$. Если все показатели, входящих в f степеней X делятся на q, то мы проверяем, можно ли извлечь корень q-ой степени из каждого коэффициента f на основании изложенного выше.

Если $f = \sum_j b_j X^{qj}$ и $b_j^{1/q} \in K$ для любого j, то $f = (\sum_j b_j^{1/q} X^j)^q$ и мы продолжаем применять описываемую процедуру к многочлену $\sum_j b_j^{1/q} X^j$ вместо f.

Предположим теперь, что $f = \sum_j c_j X^{jq^s}$ и, кроме того, не из всех c_j можно извлечь корень q-ой степени в K, и такое представление f невозможно для больших целых чисел $s \geqslant 0$. Из этих предположений следует, что из f не может быть извлечен корень q-ой степени и, следовательно, m_1 и q взаимно просты. Следовательно, $f_1 = \sum_j a_j X^{jq^s}$ для некоторых $a_j \in K$, так как корень q^s степени может быть извлечен из f_1 над $\overline{K}$ – алгебраическим замыканием поля K.

Рассмотрим многочлен $g(Z) = \sum_j c_j Z^j$ и $g_1(Z) = \sum_j a_j Z^j$, тогда $g = g_1^{m_1}$ и многочлен g_1 так же как f_1 неприводим над K. Согласно условию на s, производная $g' \neq 0$. Так как $g' = m_1 g_1^{m_1 - 1} g_1'$ и $g.c.d.(g, g') = g_1^{m_1 - 1}$, то можно легко найти g_1, и следовательно, f_1.

Итак, мы показали, что аналог теоремы I.I верен для примитивного алгебраического расширения $K = F[\delta] \supset F$ в общем случае, в предположении, что задан базис расширения $F^q \subset F$, причем время работы алгоритма полиномиально от h, $L_1(\varphi)$, $L_1(f)$ и кроме того от длины задания базиса расширения $F^q \subset F$.

В заключение параграфа отметим, что теорема I.I верна также и для многочленов f от многих переменных. Достаточно рассматривать f как многочлен от одной переменной и воспользоваться леммой Гаусса, но в оценку времени войдет еще d_1^n (см.введение).

§ 2. Разложение многочленов от многих переменных

Пусть $f \in F[X, u_1, \dots, u_n]$. Сделаем некоторые предварительные преобразования над f, так чтобы свести рассмотрение к случаю, когда многочлен $0 \neq f(X, 0, \dots, 0)$ сепарабелен и старший коэффициент $lc_X(f) = 1$. Запишем $f = \sum_{g \le i \le g} a_i X^i$, где $g = \deg_X(f) > 0, a_i \in F[u_1, \dots, u_n]$. Рассмотрим многочлен $g(X, u_1, \dots, u_n) = a_g^{g-1} f(X/a_g, u_1, \dots, u_n)$, тогда $lc_X(g) = 1$. Поэтому, в дальнейшем будем считать, не ограничивая общности, что $lc_X(f) = 1$.

Представим $f = f_1(X^{q^s}, u_1, \dots, u_n)$ для максимально возможного s (здесь предполагаем, что $q > 0$). Заменив f на f_1, будем считать, что $\partial f / \partial X \neq 0$. Вычислим в полиномиальное от $L_1(f), L_1(\varphi)$ время на основе [2I] дискриминант $D(u_1, \dots, u_n) = Res_X(f, \partial f / \partial X)$. Если $D = 0$, то $1 \neq HOD(f, \partial f / \partial X) \mid f$. Поэтому в дальнейшем можно считать, что $D \neq 0$. Найдем такие $\alpha_1, \dots, \alpha_n \in H$ (расширяя при необходимости поле H, если оно конечно), что $D(\alpha_1, \dots, \alpha_n) \neq 0$. Обозначим $f_2(X, u_1, \dots, u_n) = f(X, u_1 + \alpha_1, \dots, u_n + \alpha_n)$. Тогда многочлен $f_2(X, 0, \dots, 0)$ сепарабелен и $lc_X(f_2) = 1$.

В дальнейшем неоднократно используется следующее неравенство на параметры (степени и размер) делителей многочлена. Доказательство его опирается на теорему I.I и субрезультантный алгоритм ([II]).

ЛЕММА I.3. Пусть $f = gh$, многочлен f удовлетворяет оценкам (I) из введения, $g, h \in F[X_0, \dots, X_n]$ и $lc_{X_0}(f) = lc_{X_0}(g) = lc_{X_0}(h) = 1$. Тогда $\deg_{T_j}(g), \deg_{T_j}(h) \le \deg_{T_j}(f) P_1(r, r_1) \le r_2 P_1(r, r_1)$.

Здесь и ниже $P_1, P_2, \dots$ подходящие полиномы, далее, длины записи коэффициентов $l(g), l(h) \le (M_1 + M_2 + l r_2 + n) P_2(r, r_1)$.

Важным инструментом при разложении многочленов является лемма Гензеля (ср. [4], [5], [20]). Для нас будут существенны оценки на коэффициенты сомножителей.

ЛЕММА ГЕНЗЕЛЯ. Пусть многочлен $f \in F[X, u_1, \dots, u_n]$ удовлетворяет оценкам (I) из введения (с заменой $X_1, \dots, X_n$ на $X, u_1, \dots, u_n$); кроме того, $lc_X(f) = 1$ и многочлен $f_0 = f(X, 0, \dots, 0) \in F[X]$ сепарабелен. Предположим, что $f_0 = g_0 h_0$, где $g_0, h_0 \in F[X]$ и $lc(g_0) = lc(h_0) = 1$. Тогда для всякого мультииндекса $I = (i_1, \dots, i_n)$, где $i_j \ge 0$ и $i_1 + \dots + i_n \ge 1$ существуют и единственны многочлены $g_I, h_I \in F[X]$, такие что

$\deg g_I < \deg g_0$, $\deg h_I < \deg h_0$, и в кольце $F[[u_1,\dots,u_n]][X]$ многочленов над кольцом формально степенных рядов выполнено равенство $(g_0 + \sum_I g_I u^I)\cdot(h_0 + \sum_I h_I u^I) = f$, где $u^I = u_1^{i_1}\dots u_n^{i_n}$. При этом степени $g_I = \max_{j;J\le I}\{\deg_{T_j}(g_J), \deg_{T_j}(h_J)\}$ $\le \deg_{T_j}(f) P_3(\tau,\tau_1,(i_1+\dots+i_n)) \le \tau_2 P_3(\tau,\tau_1,(i_1+\dots+i_n))$, где $J=(j_1,\dots,j_n)\le I=(i_1,\dots,i_n)$ обозначает, что $j_1\le i_1,\dots,j_n\le i_n$. Длины записей коэффициентов $l(g_I)$, $l(h_I) \le (M_1+M_2+l\tau_2) P_5(\tau,\tau_1,(i_1+\dots+i_n))$.

Время построения g_I , h_I оценивается сверху как $P_6((M_1+M_2), (\tau\tau_1\tau_2 g_I)^l, (i_1+1)\cdots(i_n+1)) \le P_6((M_1+M_2),(\tau\tau_1\tau_2(i_1+\dots+i_n))^l,(i_1+1)\cdots(i_n+1))$.

ЗАМЕЧАНИЕ. Лемма Гензеля, а также лемма I.3 остаются справедливыми с теми же самыми оценками при рассмотрении разложения $f_0 = g_0^{(1)} g_0^{(2)} \cdots g_0^{(s)}$ (а также f) в произведение нескольких множителей.

Алгоритм разложения f опирается на приведенную ниже эффективную версию теоремы Гильберта о неприводимости (теорема I.2), которая является обобщением теоремы I.3 [4], полученной автором совместно с Д.Ю.Григорьевым. Доказательство теоремы I.2 здесь не приводится, поскольку оно представляет собой модификацию доказательства теоремы I.3 [4]. Для формулировки теоремы построим некоторое конечное расширение $F_1 = F[\theta]$ (считаем здесь, что поле F бесконечно). Обозначим $\beta = 1+2\tau n$, $\varrho = \deg_X(f) < \tau$.

(i) Пусть $\mathrm{char}(F) = 0$, $l = 0$ (см. введение). Выберем такое простое q_2 , что $q_2 > \varrho$, $q_2 > \tau_1$ и натуральное ε , что $q_1 = q_2^{\varepsilon} \ge \beta^n$. Положим $F_1 = F[\theta] = F[Z]/(Z^{q_1}-2)$, где $\theta^{q_1} = 2$. Отметим, что многочлен $Z^{q_1}-2$ неприводим над F , поскольку $\mathrm{HOД}([F:\mathbb{Q}],[\mathbb{Q}[Z]/(Z^{q_1}-2):\mathbb{Q}]) = 1$.

(ii) Пусть $l > 0$. Выберем простое $q_2 \ne q_1$ и $q_1 = q_2^{\varepsilon}$ как в (i). Положим $F_1 = F[\theta] = F[Z]/(Z^{q_1}-T_1)$, где $\theta^{q_1} = T_1$.

ТЕОРЕМА I.2. Пусть поле F бесконечно и многочлен $f \in F[X,u_1,\dots,u_n]$ неприводим над F , кроме того, $lc_X(f) = 1$ и $f(X,0,\dots,0)$ сепарабелен. Тогда многочлен $\overline{f}(X,u) = f(X,u,\theta^{\beta}u,\theta^{\beta^2}u,\dots,\theta^{\beta^{n-1}}u) \in F_1[X,u]$ неприводим над

$F_1 = F[\theta]$.

Перейдем теперь к изложению алгоритма для разложения многочлена $f \in F[X, U_1, \ldots, U_n]$. Напомним, что f удовлетворяет оценкам из введения. Опишем сначала сведение разложения f над F к разложению многочленов из $F[X]$ или $F_1[X, U]$ в полиномиальное время. Считаем, что алгоритм для разложения в $F_1[X, U]$ уже построен. Рассмотрим два случая A) $r \leq n$. Пусть $f_0(X) = f(X, 0, \ldots, 0) = \prod_{i \in J} \varphi_i$ - разложение f_0 над F и пусть $f(X, U_1, \ldots, U_n) = f_1 \ldots f_s$ - разложение $f(X, U_1, \ldots, U_n)$ над F, причем $lc_X(\varphi_i) = lc_X(f_j) = 1$ для всех i. Тогда для некоторого разбиения $J = J_1 \cup \ldots \cup J_s$ выполнено $f_j(X, 0, \ldots, 0) = \prod_{i \in J_j} \varphi_i$ для всех $1 \leq j \leq s$. Поэтому алгоритм в рассматриваемом случае находит разложение $f_0 = \prod_{i \in J} \varphi_i$ и затем перебирает все подмножества $\emptyset \neq J_1 \subsetneq J$. Обозначим $q_0 = \prod_{i \in J_1} \varphi_i$ и $h_0 = f_0 / q_0$. Применяем лемму Гензеля (см. выше) к разложению $f_0 = q_0 h_0$ вплоть до построения мономов $q_I U^I$, $h_I U^I$, у которых степень по переменной U_i не превосходит $deg_{U_i}(f)$, и кроме того, степени $deg_{T_j}(q_I), deg_{T_j}(h_I) \leq P_1(r, r_1, deg_{T_j}(f))$ (см. лемму I.3). Затем алгоритм проверяет, равно ли произведение двух получившихся многочленов $(\sum_I q_I U^I)(\sum_I h_I U^I)$ многочлену f. В результате, мы найдем нетривиальное разложение f над F, если f приводим, или установим его неприводимость.

Изложенная процедура сведения в силу леммы Гензеля и леммы I.3 требует времени не более $2^r P_6(M_1 + M_2, (r r_1 r_2 P_1(r r_1 r_2))^r, r^n)$, т.е. не более $P_7(L_1(f), L_1(\varphi))$, не считая времени разложения в $F[X]$.

B) $r > n$. Найдем разложение $\bar{f}(X, U) = f(X, U, \theta^\beta U, \theta^{\beta^2} U, \ldots, \theta^{\beta^{n-1}} U)$ над F_1 (см. теорему I.2). Пусть $\bar{f} = \prod_i \varphi_i$. Обозначим $\varphi_i = \varphi_{i,0} + \sum \varphi_{i,j} U^j$, где $\varphi_{i,j} \in F_1[X]$, $j \geqslant 0$; кроме того, $deg_X(\varphi_{ij})^j < deg_X(\varphi_{i0})$ при $j > 0$, так как $lc_X f = 1$ и можно потребовать, чтобы $lc_X(\varphi_i) = 1$ для всех i.

Можно показать, используя лемму Гензеля и конструкцию θ, что $\varphi_{i,0} \in F[X]$ для всех i.

По лемме Гензеля (см. замечание после леммы Гензеля), примененной к разложению $f_0 = \prod_i \varphi_{i,0}$, существуют $\Phi_i(X, U_1, \ldots, U_n) \in F[[U_1, \ldots, U_n]][X]$, такие что $\Phi_i(X, 0, \ldots, 0) = \varphi_{i,0}$

для всех i и $f = \prod \Phi_i$. Пусть $f = \prod \Psi_j$ – разложение f над Γ, т.е. $\Psi_j \in \Gamma[X, U_1, \ldots, U_n]$ и $lc_X(\Psi_j) = 1$ для всякого j. По теореме I.2, многочлен $\overline{\Psi}_j = \Psi_j(X, U, \theta^p U, \ldots, \theta^{p^{n-1}} U)$ неприводим над Γ_1. Поэтому для всякого j существует и единственен i, такой что $\overline{\Psi}_j = \varphi_i(X, U)$, в частности, $\Psi_j(X, 0, \ldots, 0) = \varphi_{i,0}$. Поэтому в силу леммы Гензеля имеем $\Psi_j = \Phi_i$, т.е. Φ_i – неприводимый над Γ многочлен.

Алгоритм при построении каждого Φ_i, применяя лемму Гензеля, кончает свою работу на построении мономов степеней не выше $\deg_{U_i}(f)$ по переменной U_i. Описание алгоритма сведения разложения f закончено. В силу оценок в лемме Гензеля и выбора θ время описанного сведения в случае B), не считая времени разложения в $\Gamma_1[X, U]$, не превосходит $(rn)^m P_8(M_1 + M_2, (r r_1 2rn r_2)^l, r^n) \le P_9(M_1 + M_2, r^{n+l}, (r_1 r_2)^l) \le P_{10}(L_1(f), L_1(\varphi))$.

Покажем теперь, как свести разложение многочлена $f \in \mathbb{Z}[X, U_1, \ldots, U_n]$ к разложению в $\mathbb{F}_p[X, U_1, \ldots, U_n]$ для подходящих простых p и разложению в $\mathbb{Z}[X]$. Полиномиальный алгоритм для разложения в $\mathbb{F}_p[X, U_1, \ldots, U_n]$ см. в главе I [4].

Обозначим $0 \neq D = Res_X(f_0, f_0') \in \mathbb{Z}$ и $N_3 = 2^{(M_1 + M_2 + lr_2)} P_5(r, r_1, rn)$, где оценка $l(q_I), l(h_I) \le (M_1 + M_2 + lr_2) P_5(r, r_1, rn)$ взята из леммы Гензеля. Выберем теперь перебором простые числа $p_1, \ldots, p_s$, такие что p_{i+1} – наименьшее простое число большее p_i и $p_{i+1} \nmid D$, кроме того, $p_1 \cdots p_{s-1} \le N_3 < p_1 \cdots p_s$.

Найдем затем следующие разложения на неприводимые множители: $f_0 = \prod_{i \in J} \varphi_i$, $lc_X(\varphi_i) = 1, \varphi_i \in \mathbb{Z}[X]$ на основании [20]; $f(\mathrm{mod}\, p_j) = \prod_{\kappa \in K_j} f_\kappa^{(j)}$, $lc_X(f_\kappa^{(j)}) = 1, f_\kappa^{(j)} \in \mathbb{F}_{p_j}[X, U_1, \ldots, U_n]$, $1 \le j \le s$ ([4]).

Построим, далее, минимальное относительно отношения включения непустое множество индексов $S \subset J$, такое что для всякого $1 \le j \le s$ существует подмножество $K_j' \subset K_j$, для которого $\prod_{i \in S} \varphi_i(\mathrm{mod}\, p_j) = \prod_{\kappa \in K_j'} f_\kappa^{(j)}(X, 0, \ldots, 0)$. Легко видеть, что такое множество S можно найти в полиномиальное время (надо начать построение S с любого одноэлементного множества $\{i_0\} \subset I$ и расширять далее его подходящим образом, пока не получится S).

ЛЕММА I.4. Пусть $g_0 = \prod_{i \in S} \varphi_i$, $h_0 = f_0 / g_0$ и $g = g_0 + \sum_I g_I U^I$, $h = h_0 + \sum_I h_I U^I$ получаются применением леммы Гензеля к h_0 и g_0. Тогда h, g

$\in \mathbb{Z}[X, U_1, \ldots, U_n]$, причем многочлен g неприводим.

ДОКАЗАТЕЛЬСТВО. Предположим, что g или h не является многочленом. Пусть $h_I = \sum_\alpha h_{\alpha I} X^\alpha$, $g_I = \sum_\alpha g_{\alpha I} X^\alpha$; $g_{\alpha I}, h_{\alpha I} \in \mathbb{Q}$; существуют индекс α и мультииндекс I, для которого выполнены неравенства $rn < |I| < 2rn$, такие что $h_{\alpha,I} \neq 0$ или $g_{\alpha,I} \neq 0$. Пусть, скажем, $g_{\alpha,I} \neq 0$. Тогда существует простое число p_i, $1 \leqslant i \leqslant S$, такое что p_i не делит числитель и знаменатель $g_{\alpha,I}$. Заметим, далее, что $g \pmod{p_i}, h \pmod{p_i}$ получаются применением леммы Гензеля к разложению $(g_0 \pmod{p_i})(h_0 \pmod{p_i}) = f_0 \pmod{p_i}$ В силу выбора множества S и единственности в лемме Гензеля мы получаем, что $g \pmod{p_i} = \prod_{k \in K_i} f_k^{(i)}, h \pmod{p_i} = \prod_{k \in K_i \setminus K_i'} f_k^{(i)}$. Поскольку $g_{\alpha I} \pmod{p_i} \neq 0$, то $\deg_{u_1,\ldots,u_n}(g \pmod{p_i}) \geqslant |I| > rn$. С другой стороны, $\deg_{u_1,\ldots,u_n}(g \pmod{p_i}) \leqslant \deg_{u_1,\ldots,u_n}(f \pmod{p_i}) \leqslant rn$ и мы получили противоречие. Многочлен g неприводим в силу минимальности S; наконец, $g, h \in \mathbb{Z}[X, u_1, \ldots, u_n]$ в силу леммы Гаусса, так как $lc_X(g) = lc_X(h) = 1$. Лемма доказана.

Теперь на основе леммы можно завершить описание алгоритма разложения многочленов над $F = \mathbb{Q}$: надо применить лемму Гензеля к разложению $f_0 = g_0 h_0$ и многочлену f вплоть до построения мономов степени, не большей r по каждой переменной, и, далее, применить описанное сведение разложения к многочлену h. Время работы описанного алгоритма полиномиально от $L_1(f)$.

Обратимся, наконец, к общему случаю. Предположим, что $r < n$. Тогда воспользуемся пунктом А) из сведения выше. Разложение многочленов из $F[X]$ можно проделать опираясь на теорему I.I §I, случай $F = H$ – конечное поле [4] и на только что рассмотренный случай $F = H = \mathbb{Q}$ в силу леммы Гаусса). Если же $r \geqslant n$, то применим пункт В) описанного выше сведения. Многочлен $\bar{f}(X, U) \in F_1[X, U]$ можно разложить с помощью следующей процедуры. Обозначим $F_3 = H(T_1, \ldots, T_l)[\theta]$ и применим к расширению полей $F_3 \subset F_3[\eta] = F_1$ теорему I.I; тем самым, сведем разложение $\bar{f}$ к разложению нескольких многочленов из $F_3[X, U]$. Допустим, что $l \geqslant 3$. Тогда, избавляясь от знаменателя и принимая во внимание, что $T_1 = \theta^{q_1}$ получим многочлены $\bar{q}^{(i)} \in H[\theta, T_2, \ldots, T_l, X, U] \subset H(\theta, X, U)[T_2, \ldots, T_l]$. Если $l \leqslant \max_{2 \leqslant j \leqslant l} \deg_{T_j}(\bar{q}^{(i)})$, то

используя снова пункт В), сведем разложение $\overline{g}^{(i)}$ к разложению некоторых многочленов $\overline{h}^{(i)} \in H(\theta, X, U)[\theta_1][T^{(2)}, T^{(3)}]$, где θ_1 алгебраичен и сепарабелен над полем $H(\theta, X, U)$. Если же $l > \max_{2 \le j \le l} \deg_{T_j}(\overline{g}^{(i)})$, то применяем для разложения $\overline{g}^{(i)}$ пункт А). Разложение многочленов $\overline{h}^{(i)}$ (а также многочлена $\overline{f}$ в случае $l \le 2$) проводится на основе теоремы I.I. Время работы описанного алгоритма полиномиально от $L_1(f), L_1(\varphi), q$.

§ 3. Абсолютное разложение многочленов, конструкция примитивного элемента и группы Галуа расширения полей

Рассмотрим многочлен $f \in F[X_0, \dots, X_n]$. Под абсолютным разложением многочлена f будем понимать разложение f над алгебраическим замыканием $\overline{F}$ поля F. Настоящий параграф посвящен, во-первых, сведению в полиномиальное время абсолютного разложения к разложению над F; далее, построению алгоритма для нахождения примитивного элемента конечного сепарабельного расширения поля F. Этот алгоритм сводится в полиномиальное от степени расширения время к разложению многочленов от одной переменной. Наконец, в заключение параграфа предлагается процедура для построения группы Галуа многочлена от одной переменной с коэффициентами из F, которая сводится в полиномиальное от порядка группы Галуа время также к разложению многочленов от одной переменной над F.

Мы можем предполагать без ограничения общности, что f неприводим над F, раскладывая многочлен f над F в общем случае согласно §§ I-2. Рассмотрим наибольшее целое β, такое что $f = \sum_{i_0, \dots, i_n} \alpha_{i_0, \dots, i_n} X_0^{i_0 q^\beta} \cdots X_n^{i_n q^\beta}$ (здесь мы предполагаем, что $q = char(F) > 0$) и положим $g = \sum_{i_0, \dots, i_n} \alpha_{i_0, \dots, i_n} X_0^{i_0} \cdots X_n^{i_n}$. Если $g = \prod_j g_j$ – абсолютное разложение сепарабельного и неприводимого над F многочлена g, то $f = \prod_j g_j(X_0^{q^\beta}, \dots, X_n^{q^\beta})$ и многочлен $g_j(X_0^{q^\beta}, \dots, X_n^{q^\beta})^{1/q^\beta}$ абсолютно неприводим для всякого j. Поэтому достаточно разложить абсолютно g. Пусть $0 \le \omega \le n$ – такой индекс, что $\partial g / \partial X_\omega \not\equiv 0$. Перенумеровав индексы, мы можем считать, что $\omega = 0$. Рассуждая как в § 2 (т.е. рассматривая многочлен $a_s^{s-1} g(X_0 / a_s, X_1, \dots, X_n)$, где $g = \sum_{0 \le i \le s} a_i X_0^i, a_i \in F[X_1, \dots, X_n]$, $a_s \not\equiv 0$), мы можем предполагать без ограничения общности, что старший коэффициент $lc_{X_0}(g) = 1$.

Принимая во внимание, что $g.c.d.(g,\partial g/\partial X_0)=1$, мы получаем, что $\mathcal{D}(X_1,\ldots,X_n)=Res_{X_0}(g_0,\partial g/\partial X_0)\neq 0$ (многочлен $\mathcal{D}$ можно вычислить в полиномиальное время при помощи [21]). Также как и в § 2 находим такие $\alpha_1,\ldots,\alpha_n\in F'$ (где $F'=F$ или F' некоторое конечное расширение F в случае, когда F - конечное поле), что $\mathcal{D}(\alpha_1,\ldots,\alpha_n)\neq 0$. Заменяя переменную X_i на $X_i+\alpha_i$ для всех $1\leqslant i\leqslant n$, мы получим, что многочлен от одной переменной $g(X_0,0,\ldots,0)$ сепарабелен. Поэтому, в дальнейшем, мы можем предполагать без ограничения общности, что f неприводим над F, многочлен $f(X_0,0,\ldots,0)$ сепарабелен и $lc_{X_0}(f)=1$.

Пусть теперь $f=\prod_{1\leqslant i\leqslant k} f_i$ - абсолютное разложение многочлена f и $lc_{X_0}(f_i)=1$ для любого $1\leqslant i\leqslant k$. Тогда все $f_i (1\leqslant i\leqslant k)$ попарно сопряжены. Обозначим через K_1 конечное расширение поля F, порожденное коэффициентами многочлена f_1. Мы утверждаем, что степень $[K_1:F]=k$. Действительно, рассмотрим все различные вложения $\sigma_1,\ldots,\sigma_s: K_1\hookrightarrow \overline{K}_1$, тождественные на F. Поскольку $f(X_0,0,\ldots,0)$ сепарабелен, его поле разложения K_2 (т.е. поле, порожденное всеми его корнями) сепарабельно над F. Лемма Гензеля (см., например, §2) влечет, что $K_1\subset K_2$, следовательно, K_1 также сепарабельно над F, следовательно, $[K_1:F]=s$ ([6]). Тогда $h=\prod_{1\leqslant i\leqslant s} f_1^{\sigma_i}\in F[X_0,\ldots,X_n]$ и поэтому $f\mid h$, поскольку f неприводим над F. Отсюда мы заключаем, что $s\geqslant k$. С другой стороны, если $s>k$, то для некоторой пары различных вложений (пусть это будут σ_1, σ_2) выполняется равенство $f_1^{\sigma_1}=f_1^{\sigma_2}$, т.е. $\sigma_1|_{K_1}=\sigma_2|_{K_1}$, что приводит к противоречию. Итак, $[K_1:F]=s=k$.

Предлагаемый ниже алгоритм строит поле K_1, и неприводимый над F многочлен $\varphi_1\in F[Z]$, такой что $K_1=F[Z]/(\varphi_1)$ (по только что доказанному $k=(deg\,\varphi_1)\,|\,g.c.d.\{deg_{X_i}(f)\}$). Помимо этого алгоритм строит абсолютно неприводимый многочлен $f_1\in K_1[X_0,\ldots,X_n]$, такой, что $f_1\mid f$ и $lc_{X_0}(f_1)=1$ ($lc_{X_0}(f)=1$, см. выше).

ЛЕММА I.5. Пусть $g\in F[X_0,\ldots,X_n]$ и многочлен g неприводим над F, многочлен от одной переменной $h(X_0)=g(X_0,0,\ldots,0)$ сепарабелен, $lc_{X_0}(g)=1$ и $h(X_0)$ имеет корень $c\in F$. Тогда g абсолютно неприводим.

ДОКАЗАТЕЛЬСТВО. Рассмотрим абсолютное разложение $g=\prod_i g_i$, причем $lc_{X_0}(g_i)=1$ для любого i. Тогда все g_i сопряжены над F. Поскольку $h(c)=0$, мы получаем, что $0=g_{i_0}(c,0,\ldots,0)$ для некоторого i_0, и, следовательно, $g_i(c,0,\ldots,0)=0$ для любого i в силу того, что $c\in F$.

Следовательно, $h=g_{i_0}(X_0,0,\dots,0)$ и $g=g_{i_0}$, поскольку h сепарабелен, что завершает доказательство леммы.

Основываясь на лемме I.5, несложно построить алгоритм для абсолютного разложения, который сводит его в полиномиальное время к разложению многочленов от многих переменных над F. Сначала разложим на множители $h(X_0)=f(X_0,0,\dots,0)=\prod_i h_i(X_0)$ над F. Рассмотрим сепарабельное расширение $F_1=F[\mu]=F[Z]/(h_1)\supset F$, где $h_1(\mu)=0$. Затем согласно основной теореме главы I ., мы раскладываем $f=\prod_j f_j$ над F_1, причем $lc_{X_0}(f_j)=1$ для любого j. Найдем такой единственный индекс j_0, что $f_{j_0}(\mu,0,\dots,0)=0$. Тогда f_{j_0} абсолютно неприводим по лемме I.5. Это завершает описание алгоритма для абсолютного разложения.

Теперь обратимся к построению примитивного элемента θ расширения $K=F(\alpha_1,\dots,\alpha_s)\supset F$, порожденного коэффициентами $\alpha_1,\dots,\alpha_s$ многочлена f_{j_0} (мы имеем $F(\alpha_1,\dots,\alpha_s)\subset K_2$). Более того, мы, в действительности, изложим обещанную в начале настоящего параграфа процедуру для построения примитивного элемента в конечном сепарабельном расширении полей. Пусть сначала поле F будет бесконечным. В этом случае мы последовательно найдем примитивные элементы $\theta_1=\alpha_1,\theta_2,\dots,\theta_s$ над полем F в башне полей $F\subset F(\theta_1)=F(\alpha_1)\subset F(\theta_2)=F(\alpha_1,\alpha_2)\subset\dots\subset F(\theta_s)=F(\alpha_1,\dots,\alpha_s)=K$. Если θ_i уже построен, то в качестве θ_{i+1} можно взять один из элементов вида $\theta_i+\gamma\alpha_{i+1}$ (см. [6]), где γ пробегает произвольные различные $[F(\theta_i,\alpha_{i+1}):F]$ элементов поля F. (является ли фиксированный элемент примитивным, несложно проверить, рассматривая его степени).

Пусть теперь поле F конечно. Требуется найти такой многочлен $\psi\in F[Z]$, что $K=F[Z]/(\psi)=F[\theta]$ и $\psi(\theta)=0$. Нам потребуется некоторая вспомогательная конструкция, которая, по-видимому, также интересна сама по себе. Итак, пусть $H_1\subset H_2$ - конечные поля характеристики q и $\delta_1,\dots,\delta_m$ - базис H_2 над H_1 (здесь и ниже мы предполагаем, что когда нам дан базис расширения полей, нам задана также и его таблица умножения). Заметим сначала, что если некоторое $\varkappa\mid m$, то поле H_3, такое, что $H_1\subset H_3\subset H_2$, $[H_3:H_1]=\varkappa$ и $[H_1:\mathbb{F}_q]=\varkappa_1$ совпадает с множеством $\{\beta\in H_2:\beta^{q^{\varkappa\varkappa_1}}=\beta\}$. Следовательно, можно построить базис H_3 над H_1 в полиномиальное от $m\varkappa_1\log q=\log|H_2|$ время.

Теперь мы покажем, как построить примитивный элемент ζ, такой что $H_2=H_1(\zeta)$. Разложим $m=\prod_i p_i^{e_i}$, где p_i - простые числа. Для каждого i построим подполе $H^{(i)}$, для которого вы-

полнено $H_1 \subset H^{(i)} \subset H_2$ и $[H^{(i)}:H_1]=p_i^{e_i}$, основываясь на упомянутом выше. Среди элементов базиса $H^{(i)}$ над H_1 существует по крайней мере один примитивный элемент расширения $H^{(i)} \supset H_1$ (обозначим его через $\zeta^{(i)}$), поскольку существует только одно максимальное собственное подполе поля $H^{(i)}$, содержащее H_1. Легко проверить, является ли выбранный среди элементов базиса элемент требуемым элементом, поскольку последнее эквивалентно неравенству $(\zeta^{(\bullet)})^{q^{\varkappa_1} p_i^{(e_i-1)}}$.

Следующая лемма имеет несколько более общую форму, чем нам потребуется для случая конечных полей, однако она интересна и сама по себе.

ЛЕММА I.6. Пусть $F \subset F_2 = F[\mu_2]$, $F \subset F_3 = F[\mu_3]$ – два расширения Галуа поля F, причем $F_2, F_3 \subset F_4$, где F_4 – некоторое поле, и пусть степени $[F_2:F]$ и $[F_3:F]$ взаимно просты. Тогда если $\mu_5 = \mu_2 + \mu_3$, то $F_5 = F[\mu_2, \mu_3]$ совпадает с $F[\mu_5]$.

ДОКАЗАТЕЛЬСТВО. Предположим, что подполе $F_6 = F[\mu_5] \subsetneqq F_5$. Рассмотрим группу Галуа $G = Gal(F_5/F_6)$. Пусть $1 \neq \sigma \in G$. Тогда $\sigma(\mu_5) = \mu_5$, следовательно, $\sigma(\mu_2) - \mu_2 = \mu_3 - \sigma(\mu_3) = c \in F_2 \cap F_3 = F$. Очевидно $c \neq 0$, так как $\sigma \neq 1$. Мы получаем, что

$$0 = Tr_{F_2/F}(\sigma(\mu_2) - \mu_2) = Tr_{F_2/F}(c) = c[F_2:F]$$

и

$$0 = Tr_{F_3/F}(\mu_3 - \sigma(\mu_3)) = Tr_{F_3/F}(c) = c[F_3:F]$$

Это приводит к противоречию, поскольку $[F_2:F]$ и $[F_3:F]$ взаимно просты, и завершает доказательство леммы.

Отметим, что в случае нулевой характеристики условие $F_2 \cap F_3 = F$ достаточно, а в случае ненулевой характеристики $q \neq 0$ достаточно, чтобы $F_2 \cap F_3 = F$ и, по крайней мере, одно из чисел $[F_2:F]$, $[F_3:F]$ не делилось на q.

Возвращаясь к построению примитивного элемента ζ поля H_2 над H_1, мы полагаем $\zeta = \sum_i \zeta^{(i)}$ согласно лемме I.7. Поскольку нам известен базис H_2 над H_1, то мы можем построить минимальный многочлен для ζ над H_1.

Для построения примитивного элемента $\theta \in K = F(\alpha_1, \ldots, \alpha_s)$ над F мы построим последовательно примитивные элементы $\theta_1 = \alpha_1, \theta_2, \ldots, \theta_s$ полей $F \subset F(\theta_1) = F(\alpha_1) \subset F(\theta_2) = F(\alpha_1, \alpha_2) \subset \ldots \subset F(\theta_s) = F(\alpha_1, \ldots, \alpha_s) = K$. Если θ_i уже построен для некоторого i, то среди элементов $\theta_i^u \alpha_{i+1}^v$ для $0 \leqslant u, v \leqslant [K:F]$ можно выбрать базис поля $F(\theta_i, \alpha_{i+1})$ над F и применить конструкцию, предложенную выше, полагая там $H_1 = F$, $H_2 = F(\theta_i, \alpha_{i+1})$.

10.1679

Это завершает описание алгоритма для построения примитивного элемента и, в частности, построение поля K, порожденного всеми коэффициентами некоторого абсолютно неприводимого делителя многочлена f.

В заключение настоящего параграфа мы изложим алгоритм для нахождения группы Галуа поля разложения заданного многочлена f от одной переменной X. В дальнейшем мы не будем его использовать, но мы включили его, поскольку он опирается на процедуру для построения примитивного элемента и, с другой стороны, построение группы Галуа является отдельной интересной проблемой. Излагаемый ниже алгоритм сводится в полиномиальное время от длины записи полинома f и порядка группы Галуа, которая строится, к разложению многочленов от одной переменной над основным полем.

Итак, пусть $0 \neq f \in F[X]$ - сепарабельный многочлен. Разложим его на неприводимые над F множители $f = \prod_j f_{0j}$. Положим $F_0 = F$, $\theta^{(0)} = 1$, $\varphi_0(X) = X - 1$. Если поле $F_i = F[X]/(\varphi_i) = F[\theta^{(i)}]$, а также $\varphi_i, \theta^{(i)}$ уже построены, то разложим $f = \prod_j f_{ij}$ над F_i (применяя § I). Если хотя бы один из множителей f_{ij} имеет степень больше, чем I (пусть - это будет f_{ij_0}), то мы полагаем $F_{i+1} = F_i[X]/(f_{ij_0})$ и, используя предложенную выше конструкцию, находим примитивный элемент $\theta^{(i+1)}$ и $\varphi_{i+1} \in F[X]$ такие, что $F_{i+1} = F[X]/(\varphi_{i+1}) = F[\theta^{(i+1)}]$, $\varphi_{i+1}(\theta^{(i+1)}) = 0$. В противном случае, если все множители f_{ij} линейные, то уже построенное поле $K = F_i = F[\theta] = F[X]/(\bar{\varphi})$ $(\theta = \theta^{(i)}, \bar{\varphi} = \varphi_i)$ является полем разложения многочлена f. Степень $[K : F]$ расширения Галуа равна порядку группы Галуа $G = Gal(K/F)$ многочлена f (т.е. группы Галуа поля разложения f).

Если некоторый автоморфизм $\sigma_i \in G$ отображает $\sigma(\theta) = \theta_i$, где θ_i - корень $\bar{\varphi}$, причем $\theta_i = \sum_j \beta_j^{(i)} \theta^j$, $\beta_j^{(i)} \in F$, то это определяет действие σ_i на всем поле $F[\theta]$, т.е. $\sigma_i(\theta_s) = \sum_j \beta_j^{(s)} (\sum_k \beta_k^{(i)} \theta^k)^j$ задает некоторую перестановку корней $\{\theta_j\}$.

Это завершает описание конструкции группы Галуа G, которая задается указанием всех ее элементов, представленных как перестановки на $[K : F] = |G|$ элементах.

Отметим, что то, что время работы алгоритма построения группы Галуа из настоящего параграфа (а также для разложения на множители из § I) ограничивается сверху полиномом от степени расширения полей, а не длиной задания поля в случае, если оно задано каким-либо другим способом, отличным от примитивного рас-

ширения, является по-видимому, существенным, так как иначе мы получили бы, например, полиномиальный алгоритм для распознания изоморфизма графов (см. [2]).

ГЛАВА II. РАЗЛОЖЕНИЕ МНОГООБРАЗИЙ НА НЕПРИВОДИМЫЕ КОМПОНЕНТЫ

§ 1. Построение общей точки компоненты за время полиномиальное от размера ее представления

Пусть дана система $f_0=\dots=f_{k-1}=0$ и однородные многочлены f_i удовлетворяют оценкам (2) из введения. Без ограничения общности будем считать в дальнейшем, что $\deg f_i = d$, $0\le i\le k-1$, заменяя при необходимости f_i на семейство $\{f_i x_j^{d-\deg f_i}\}_{0\le j\le n}$

Можно показать, что если линейные комбинации $\{h_i = \sum_{0\le j\le k-1} a_j^{(i)} f_j\}_{1\le i\le n+1}$, где коэффициенты $a_j^{(i)}\in \bar{F}$ взяты "в общем положении", то для любого $1\le m\le n+1$ всякая компонента коразмерности меньше m многообразия $\{h_1=\dots=h_m=0\}\subset \mathbb{P}^n(\bar{F})$ является также компонентой многообразия $\{f_0=\dots=f_{k-1}=0\}$. Поэтому достаточно для подходящих $\{h_i\}$ найти компоненты многообразий $\{h_1=\dots=h_m=0\}$ для всех m. Цель настоящего параграфа – описать рекурсивную конструкцию для нахождения общих точек (см. (*) из введения) компонент многообразий $\{h_1=\dots=h_m=0\}$ Кроме того, предложена простая процедура для построения системы уравнений, задающей компоненты, однако время ее работы не является полиномиальным от размера.

Будем считать, что многочлены $h_1,\dots,h_m$ уже построены, при этом $a_j^{(i)}$ принадлежат H (здесь и ниже считаем, что H содержит достаточно много элементов, при необходимости расширяя его, если H конечно, ср. § 4). Кроме того, построены общие точки и задающие системы уравнений для всех компонент многообра-

зия $\{h_1=\dots=h_m=0\}$. Именно, для всякой компоненты W_ν коразмерности s (очевидно, $s\le m$) заданы Φ_ν, $(X_j/X_{j_0})^{q^{\vartheta_j}}$ (см. (*) из введения) и однородные многочлены $\Psi_0^{(\nu)},\dots,\Psi_N^{(\nu)}\in\Gamma[X_0,\dots,X_n]$, такие что $W_\nu=\{\Psi_0^{(\nu)}=\dots=\Psi_N^{(\nu)}=0\}$. При этом выполнены следующие оценки: $q^{\vartheta_j}\le d^{2s}$, $\deg_{T_1,\dots,T_\ell,X_0,\dots,X_n}(\Psi_j^{(\nu)})\le (d+d_1+d_2)^{2s+1}$, $0\le j\le N\le(3(d+d_1+d_2)^{s+1}n+\ell)$, далее $\deg_Z(\Phi_\nu)\le d^s$, степени $\deg_{T_1,\dots,T_\ell,t_1,\dots,t_{n-s}}(\Phi_\nu)$, $\deg_{T_1,\dots,T_\ell,t_1,\dots,t_{n-s}}(X_j/X_{j_0})^{q^{\vartheta_j}}$ ограничены сверху некоторым полиномом от $d^s, d_1 d_2$. Длины записей коэффициентов из H могут быть оценены $l(h_j)$, $l(\Phi_\nu)$,

$$l((X_j/X_{j_0})^{q^{\vartheta_j}})\le(M_1+M_2+(\ell+n-s)d_2)P(d^m,d_1)$$

и $l(\Psi_j^{(\nu)})\le(M_1+M_2)P((d+d_1+d_2)^{s(n-s+\ell+1)}$ для подходящего полинома P.

Укажем сначала как построить h_{m+1}. Пусть $N_1=((\kappa-1)d^m+1)$ и элементы $\beta_1,\dots,\beta_{N_1}\in H$ попарно различны. Тогда в качестве h_{m+1} можно взять тот из многочленов семейства $\{\sum_{0\le i\le\kappa-1}\beta_j^i f_i\}_{1\le j\le N_1}$, который не обращается тождественно в нуль на максимальном числе компонент многообразия $\{h_1=\dots=h_m=0\}$, принимая во внимание, что число компонент многообразия $\{h_1=\dots=h_m=0\}$ не больше d^m по теореме Безу [7]. Пусть $\operatorname{codim} W_\nu=m$, обозначим $W=W_\nu\cap\{h_{m+1}=0\}$.

Для удобства изложения мы будем пользоваться языком дерева компонент [4], хотя, в действительности, его конструкция нам не понадобится. Дерево компонент определяется многочленами $h_1,\dots,h_{m+1}$; оно имеет корень, и уровнем вершины называется расстояние ее от корня. Каждой вершине ν уровня m соответствует некоторая компонента W_ν коразмерности m многообразия $\{h_1=\dots=h_m=0\}$. Сыновья ω вершины ν биективно соответствуют тем компонентам W_ω многообразия $W_\nu\cap\{h_{m+1}=0\}$, которые не содержатся собственно в компонентах многообразия $\{f_0=\dots=f_{\kappa-1}=0\}$. Листья дерева компонент разбиваются на два типа. Лист ν называется листом первого типа, если W_ν является компонентой многообразия $\{f_0=\dots=f_{\kappa-1}=0\}$, остальные листья называются листьями второго типа.

Перейдем к описанию конструкции общих точек компонент многообразия W .

Пусть Y трансцендентно над F . Введем следующую важную вспомогательную систему из $(m+1)$ однородного уравнения

$$h_1 - Y X_0^d = \ldots = h_{m+1} - Y X_m^d = 0 \qquad (3)$$

от $(n+1)$ переменной $X_0, \ldots, X_n$ над полем $K = F(Y)$ (напомним, что $d = deg(h_i)$ для всех i).

ЛЕММА 2.I Всякая компонента многообразия $U_K \subset \mathbb{P}^n(\bar{K})$, заданного системой (3), имеет размерность $n-m-1$

ДОКАЗАТЕЛЬСТВО. Обозначим $Y_1 = 1/Y$, тогда $K = F(Y_1)$ и система (3) эквивалентна системе $Y_1 h_1 - X_0^d = \ldots = Y_1 h_{m+1} - X_m^d = 0$, т.е. $U_K = \{Y_1 h_1 - X_0^d = \ldots = Y_1 h_{m+1} - X_m^d = 0\}$. Покажем, что система $Y_1 h_1 - X_0^d = \ldots = Y_1 h_{m+1} - X_m^d = X_{m+1} = \ldots = X_{n-1} = 0$ имеет конечное число корней в $\mathbb{P}^n(\bar{K})$. Отсюда будет следовать утверждение леммы по теореме о размерности пересечения ([7]). Конечность числа решений равносильна тому, что U - результант R последней системы (см. [I], [I8]) не равен нулю тождественно. С другой стороны $R(Y_1) \in F[Y_1][U_0, \ldots, U_n]$ и $R(0) \neq 0$, так как $R(0)$ является U -результантом системы $X_0^d = \ldots = X_m^d = X_{m+1} = \ldots = X_{n-1} = 0$, имеющей, очевидно, конечное число корней в $\mathbb{P}^n$, что завершает доказательство леммы.

Введем теперь многообразие $U_F \subset \mathbb{A}^{n+2}(\bar{F})$, заданное системой (3) рассматриваемой от переменных $X_0, \ldots, X_n, Y$ над полем F .

ЛЕММА 2. 2. Имеется биективное соответствие между компонентами, определенными над $K^{q^{-\infty}}$ многообразия U_K , и с другой стороны, теми компонентами, определенными над $F^{q^{-\infty}}$ многообразия U_F , которые не лежат ни в каком конечном объединении гиперплоскостей вида $\{Y = C\}$, где $C \in \bar{F}$. При этом размерность каждой из таких компонент равна $n-m+1$.

ДОКАЗАТЕЛЬСТВО. Обозначим через $\mathcal{J}_K$ (соответственно, через $\mathcal{J}_F$) идеал, порожденный полиномами $h_1 - Y X_0^d, \ldots, h_{m+1} - Y X_m^d$ в $K^{q^{-\infty}}$-алгебре $\Lambda_K = K^{q^{-\infty}}[X_0, \ldots, X_n]$ (соответственно, в $F^{q^{-\infty}}$-алгебре $F^{q^{-\infty}}[Y, X_0, \ldots, X_n]$). Компоненты многообразия U_K (соответственно, U_F) находятся в биективном соответствии с минимальными простыми идеалами факторкольца $\Lambda_K / \mathcal{J}_K$ (соответственно, $\Lambda_F / \mathcal{J}_F$), см., например, [3] , [7] .

Введем мультипликативно замкнутое подмножество $S=F[Y]\setminus\{0\} \subset \Lambda_F$. Тогда $\Lambda_K \supset S^{-1}\Lambda_F$ – чисто несепарабельное целое расширение колец, принимая во внимание, что $S^{-1}\Lambda_F \supset K[X_0,\dots,X_n]$. Поэтому имеется биективное соответствие, сохраняющее отношение включения (см. [3]), между простыми идеалами $\mathfrak{p}_K \subset \Lambda_K$, и с другой стороны, теми простыми идеалами $\mathfrak{p}_F \subset \Lambda_F$, для которых $\mathfrak{p}_F \cap S = \emptyset$ (отметим, что при этом соответствии $\mathfrak{p}_K \cap S^{-1}\Lambda_F = S^{-1}\mathfrak{p}_F$). Кроме того, всякому простому идеалу $\mathfrak{p}_F$ (здесь $\mathfrak{p}_F$ обозначает такой простой идеал, что $\mathfrak{p}_F \cap S = \emptyset$) соответствует неприводимое над F многообразие $V_{\mathfrak{p}_F} \subset \mathbb{A}^{n+2}(\bar{F})$, не лежащее ни в каком конечном объединении гиперплоскостей вида $\{Y=c\}$, где $c \in \bar{F}$ (и обратно). Обозначим через $V_{\mathfrak{p}_K} \subset \mathbb{P}^n(\bar{K})$ неприводимое над K подмногообразие, соответствующее $\mathfrak{p}_K$. Отныне $\mathfrak{p}_K \supset \mathfrak{J}_K$ будет обозначать некоторый простой идеал минимальный среди простых идеалов, содержащих $\mathfrak{J}_K$, иными словами, $\mathfrak{p}_K/\mathfrak{J}_K$ минимальный простой идеал в факторкольце $\Lambda_K/\mathfrak{J}_K$ (аналогичное верно и для соответствующего простого идеала $\mathfrak{p}_F \supset \mathfrak{J}_F$), следовательно, $V_{\mathfrak{p}_K}$ является компонентой многообразия U_K (аналогично, $V_{\mathfrak{p}_F}$ является компонентой многообразия U_F). Получаем цепочку равенств $\dim V_{\mathfrak{p}_F} = \deg tr_F(\Lambda_F/\mathfrak{p}_F) = \deg tr_F(S^{-1}\Lambda_F/S^{-1}\mathfrak{p}_F) = \deg tr_F(\Lambda_K/\mathfrak{p}_K) = \deg tr_K(\Lambda_K/\mathfrak{p}_K) + 1 = \dim V_{\mathfrak{p}_K} + 2 = n-m+1$ (последнее равенство вытекает из леммы 2.1). Лемма доказана.

Обозначим через $U'_F \subset U_F$ объединение тех компонент многообразия U_F, которые не лежат ни в каком конечном объединении гиперплоскостей вида $\{Y=c\}$. Многообразие $U'_F \cap \{Y=0\}$ является замкнутым конусом в $\mathbb{A}^{n+1}(\bar{F})$, ему однозначно соответствует замкнутое проективное многообразие $W' \subset \mathbb{P}^n(\bar{F})$, так что $con(W') = U'_F \cap \{Y=0\}$.

ЛЕММА 2.3. Для каждого сына w вершины v компонента W_w многообразия W является компонентой многообразия W'.

ДОКАЗАТЕЛЬСТВО. Очевидно, $\dim W_w = n-m-1$. Поэтому конус $con(W_w) \subset \mathbb{A}^{n+1}(\bar{F})$ и $\dim con(W_w) = n-m$. Кроме того, $con(W_w) \subset U_F \cap \{Y=0\}$. Пусть $V \subset U_F$ такая компонента многообразия U_F, что $con(W_w) \subset V$. Очевидно, $V \cap \{Y=0\} \subset con(\{h_1=\dots=h_{m+1}=0\})$, мы утверждаем, что $con(W_w)$ является компонентой многообразия $V \cap \{Y=0\}$. Действительно, если это не так, то $con(W_w) \subset V_1 \subset V \cap \{Y=0\}$ для некоторой компоненты V_1 многообразия $V \cap \{Y=0\}$, такой что $\dim V_1 \geq n-m+1$. Отсюда следует, что выполнено включение $V_1 \subset con(W_{v_1})$ для подходящего

листа v_1 первого типа уровня не большего m дерева компонент, что противоречит тому, что w является сыном вершины v (см.свойства дерева компонент выше).

Для завершения доказательства леммы осталось установить, что компонента V не лежит ни в каком конечном объединении гиперплоскостей вида $\{Y=c\}$. Предположим противное, тогда многообразие $V \cap \{Y=0\}$ является объединением нескольких абсолютно неприводимых компонент многообразия V. Вследствие этого, $con(W_w)$ также является объединением некоторых абсолютно неприводимых компонент многообразия V. С другой стороны, всякая абсолютно неприводимая компонента многообразия V имеет размерность не меньше $(n+2)-(m+1)$, учитывая, что V является компонентой многообразия, заданного системой (3). Следовательно, $\dim con(W_w) \geq n-m+1$. Полученное противоречие завершает доказательство леммы.

Очевидно $deg\, W' \leq deg\,(U_F' \cap \{Y=0\}) \leq deg\, U_F' \leq (d+1)^{m+1}$. Пусть $W'_{\rho_F} \subset W'$ - объединение тех компонент W'' многообразия W', что $con(W'')$- компонента многообразия $V_{\rho_F} \cap \{Y=0\}$ (см.доказательство леммы 2. 2), т.е. $con(W'_{\rho_F}) = V_{\rho_F} \cap \{Y=0\}$.

Обратимся теперь к вопросу о выборе базиса трансцендентности общего для всех компонент V_{ρ_K} и одновременно для всех компонент W'' многообразия W'.

Используя лемму 2.3 [4], алгоритм строит семейство $\mathfrak{M} = \mathfrak{M}_{n,n-m-1,2(d+1)^{m+1}}$, при этом $card\, \mathfrak{M} \leq (6(m+1)(d+1)^{m+1})^{n-m}$. Аналогично доказательству леммы 2.3[4] можно установить следующее.

ЛЕММА 2. 4. По крайней мере для одной $(n-m)$-ки $(Y_0,\dots, Y_{n-m-1}) \in \mathfrak{M}$ выполнены равенства $U_K \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$ и $W' \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$.

На самом деле, можно показать (но мы не будем этим пользоваться), что если $W' \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$, то $U_K \cap \{Y_0=\dots Y_{n-m-1}=0\}=\emptyset$. Таким образом, можно взять $\mathfrak{M} = \mathfrak{M}_{n,n-m-1,(d+1)^{m+1}}$.

Алгоритм перебирает все $(n-m)$-ки из $\mathfrak{M}$. Зафиксируем $(Y_0,\dots Y_{n-m-1}) \in \mathfrak{M}$. Сделаем замену переменных в системе (3), подставляя вместо X_i их выражения как линейных форм от Y_i для $0 \leq i \leq n$ (как раньше, мы дополняем $\{Y_i\}_{0\leq i\leq n-m-1}$ до базиса $\{Y_i\}_{0\leq i\leq n}$ пространства линейных форм). После этого алгоритм подставляет $t_i Y_0$ вместо Y_i для $1 \leq i \leq n-m-1$. Полученную систему однородных относительно переменных $Y_0, Y_{n-m},\dots, Y_n$ уравнений с коэф-

фициентами из поля $K'=K(t_1,\dots,t_{n-m-1})$ обозначим через (3'). Согласно лемме 2.2 из [4], равенство $U_K \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$ равносильно тому, что полученная система (3) имеет конечное число корней в $P^n(\bar{K})$, и для всякого ее корня $\Omega \in P^n(\bar{K})$ имеет место равенство $Y_0(\Omega)\neq 0$. Выполнимость последнего условия алгоритм проверяет на основе теоремы 2.3 [4] (если это условие не выполнено, то алгоритм переходит к рассмотрению другого набора из $\mathfrak{M}$). Поэтому можно предполагать в дальнейшем, не ограничивая общности, что $U_K \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$. Из следствия в §1 гл.2 [4] вытекает, что $Y_1/Y_0,\dots,Y_{n-m-1}/Y_0$ является общим базисом трансцендентности для всех компонент V_{p_K}.

В дальнейшем, при рассуждениях мы будем предполагать, что $W' \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$ (ср.лемму 2.4). Если это требование выполнено, алгоритм построит общие точки всех компонент W'' многообразия W'. Однако, даже если указанное требование не выполнено, алгоритм построит (если не остановится раньше) общие точки некоторых неприводимых многообразий коразмерности $m+1$, и в конце своей работы алгоритм проверит для каждого из этих многообразий, совпадает ли оно с W_w для некоторой вершины w уровня $(m+1)$. К сожалению, алгоритм не может априори проверить выполнимость требования $W' \cap \{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$ в рамках допустимого времени.

Опираясь на принятое только что предположение и на следствие из §1 гл.2 [4] можно вывести, что $Y_1/Y_0,\dots,Y_{n-m-1}/Y_0$ является общим базисом трансцендентности для всех компонент W'' многообразия W'.

Применим алгоритм из § 2 гл.2 [4] к системе (3'). На основании леммы 2.5 [4] алгоритм, тем самым, для каждой компоненты V_{p_K} строит ее общую точку, т.е. изоморфизм полей

$$K(Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^{\nu_{n-m}}},\dots,(Y_n/Y_0)^{q^{\nu_n}}) \simeq K'[\theta_p] \quad (4)$$

при этом $\Phi_{p_K}(Y,t_1,\dots,t_{n-m-1},\theta_{p_K})=0$ для подходящего неприводимого многочлена $\Phi_{p_K}\in F[Y,t_1,\dots,t_{n-m-1},Z]$ (последнее можно предполагать без ограничения общности, умножая, если это необходимо, многочлен Φ_{p_K} на некоторый элемент кольца $F[Y,t_1,\dots,t_{n-m-1}]$).

Наша ближайшая цель состоит в том, чтобы найти такой элемент $\zeta_{p_K}\in K'[\theta_{p_K}]$, что $K'[\theta_{p_K}]=K'[\zeta_{p_K}]$ и при этом $\zeta_{p_K}=\sum_{n-m\le i\le n}\gamma_i (Y_i/Y_0)^{q^{\nu}}$, где $d^{m+1}\max_{V_{p_K},\,n-m\le i\le n} q^{\nu_i}<q^{\nu}\le$

$q d^{m+1} \max_{\nu_i} \max_{\nu_{\rho_k}, n-m \le i \le n} q^{\nu_i}$, в действительности, зависят от компонент V_{ρ_k}, W'', но мы в дальнейшем не будем оговаривать это отдельно; наконец $\gamma_i \in H$. Помимо этого, мы требуем, чтобы для всякой неприводимой над F компоненты W'' многообразия W'_{ρ_F} имел место следующий изоморфизм полей

$$F(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0, (Y_{n-m}/Y_0)^{q^\nu}, \dots, (Y_n/Y_0)^{q^\nu}) \simeq F(t_1, \dots, t_{n-m-1})[\zeta_{W''}],$$

при котором $Y_i/Y_0 \longrightarrow t_i$, $1 \le i \le n-m-1$ (см. лемму 2. 4), здесь Y_i/Y_0 рассматриваются как рациональные функции на компоненте W'' и $\zeta_{W''} = \sum_{n-m \le i \le n} \gamma_i (Y_i/Y_0)^{q^\nu}$ при этом сепарабелен над $F' = F(t_1, \dots, t_{n-m-1})$.

Как в начале параграфа, построим семейство, состоящее из $N_1 = 2m((d+1)^{m+1} - 1) + 1$ векторов $(\gamma^{(1)}_{n-m}, \dots, \gamma^{(1)}_n), \dots, (\gamma^{(N_1)}_{n-m}, \dots, \gamma^{(N_1)}_n) \in H^{m+1}$ таких, что всякие $(m+1)$ из них линейно независимы. Для $1 \le j \le N_1$ обозначим $\zeta^{(j)} = \sum_{n-m \le i \le n} \gamma^{(j)}_i (Y_i/Y_0)^{q^\nu}$.

ЛЕММА 2. 5. По крайней мере для одного $1 \le j \le N_1$ элемент $\zeta^{(j)}$ удовлетворяет сформулированным требованиям.

ДОКАЗАТЕЛЬСТВО. Зафиксируем временно компоненту W'' (для компоненты V_{ρ_k} рассуждения проводятся аналогично). Зафиксируем кроме того некоторое вложение $\sigma \ne 1$ поля $F(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0, (Y_{n-m}/Y_0)^{q^{\nu_{n-m}}}, \dots, (Y_n/Y_0)^{q^{\nu_n}})$, рассматриваемого как подполе поля $\bar{F}(W'')$ в алгебраическое замыкание поля $F(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0)$, тождественное на последнем поле. Введем гиперплоскость $P^{(\sigma)}_{W''} \subset \overline{K(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0)}^{m+1}$, состоящую из векторов $(\gamma_{n-m}, \dots, \gamma_n)$, удовлетворяющих соотношению $\sum_{n-m \le i \le n} \gamma_i ((Y_i/Y_0)^{q^\nu} - \sigma(Y_i/Y_0)^{q^\nu}) = 0$ (в случае рассмотрения компоненты V_{ρ_k} соответствующую гиперплоскость обозначим через $P^{(\sigma_1)}_{V_{\rho_k}}$).

Допустим, что вектор $(\gamma_{n-m}, \dots, \gamma_n) \in \overline{F(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0)}^{m+1}$ не принадлежит ни одной из гиперплоскостей $P^{(\sigma)}_{W''}$, $P^{(\sigma_1)}_{V_{\rho_k}}$ для всех $\sigma \ne 1$, W'', а также всех $\sigma_1 \ne 1$. Установим, что при этом допущении, элемент $\zeta = \sum_{n-m \le i \le n} \gamma_i (Y_i/Y_0)^{q^\nu}$ удовлетворяет требованиям, сформулированным перед леммой. Действительно, для всякой W'' (аналогично для V_{ρ_k}) неравенство $\sigma(\zeta) \ne \zeta$ выполнено, когда $\sigma \ne 1$ (соответственно $\sigma_1(\zeta)$

$\neq \zeta$, когда $\sigma_1 \neq 1$), если Y_i/Y_0 рассматриваются как рациональные функции на W'' (соответственно на $V_{\mathfrak{p}_K}$). Отсюда следует, что ζ примитивный элемент [6], т.е. требования, сформулированные перед леммой, выполнены.

Количество введенных гиперплоскостей $P_{V_{\mathfrak{p}_K}}^{(\sigma_1)}$, $P_{W''}^{(\sigma)}$ не превосходит $(\deg V_{\mathfrak{p}_K}-1)+\sum_{W''}(\deg W''-1)\leqslant(\deg V_{\mathfrak{p}_K}-1)+(\deg V_{\mathfrak{p}_F}-1)$, так как число вложений σ (для данной компоненты W'') равно степени расширения $[F(Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^{\nu}},\dots,(Y_n/Y_0)^{q^{\nu}}):F(Y_1/Y_0,\dots,Y_{n-m-1}/Y_0)]\leqslant\deg W''$ согласно теореме 2.4 [4]. Подобная оценка имеет место и для количества вложений σ_1, соответствующих компоненте $V_{\mathfrak{p}_K}$.

Таким образом, среди N_1 рассматриваемых векторов найдется в силу принципа Дирихле по крайней мере один вектор $(\gamma_{n-m}^{(j)},\dots,\gamma_n^{(j)})\notin(\bigcup_{W''\sigma}P_{W''}^{(\sigma)})\cup(\bigcup_{\sigma_1}P_{V_{\mathfrak{p}_K}}^{(\sigma_1)})$. Тогда элемент $\zeta^{(j)}$ – требуемый по доказанному выше. Лемма доказана.

Зафиксируем на время идеал $\mathfrak{p}=\mathfrak{p}_K$ и элемент ζ, удовлетворяющий лемме 2.5. Рассмотрим неприводимый над F многочлен $\psi_{\mathfrak{p}}\in F[Y,t_1,\dots,t_{n-m-1},Z]$ такой, что $\psi_{\mathfrak{p}}(Y,t_1,\dots,t_{n-m-1},\zeta)=0$.

ЛЕММА 2.6. Пусть $\psi_{\mathfrak{p}}(0,t_1,\dots,t_{n-m-1},Z)=\lambda\prod\Phi_{W''}^{e_{W''}}(t_1,\dots,t_{n-m-1},Z)$ – разложение на неприводимые над F многочлены, здесь $\lambda\in(F')^*$. Тогда каждой компоненте W'' многообразия $W'_{\mathfrak{p}_F}$ соответствует подходящий множитель $\Phi_{W''}$, обратно при этом всякому множителю $\Phi_{W''}$ соответствуют некоторые компоненты (вообще говоря, не обязательно одна). Именно, для каждой W'' выполняется следующий изоморфизм полей

$$F(Y_1/Y_0,\dots,Y_{n-m-1}/Y_0,(Y_{n-m}/Y_0)^{q^{\nu_{n-m}}},\dots,(Y_n/Y_0)^{q^{\nu_n}})\simeq F'[\zeta_{W''}],$$

где Y_i/Y_0 понимаются как рациональные функции на W'' и $\Phi_{W''}(t_1,\dots,t_{n-m-1},\zeta_{W''})=0$, $Y_i/Y_0\longrightarrow t_i$, $1\leqslant i\leqslant n-m-1$.

ДОКАЗАТЕЛЬСТВО. Пусть $S_0,\dots,S_{K_1-1}\in F[Y,Y_0,\dots,Y_{n-m-1},Y'_{n-m},\dots,Y'_n]$ – однородные относительно переменных $Y_0,\dots,Y_{n-m-1},Y'_{n-m},\dots,Y'_n$ многочлены, порождающие простой идеал $\mathfrak{p}_F$, тогда $\mathfrak{p}_K=(S_0,\dots,S_{K_1-1})$. (в предположении, что

S_i рассматриваются как элементы из $K[Y_0,\dots,Y_{n-m-1},Y'_{n-m},\dots,Y'_n]$), здесь $Y'_{n-m}=\sum_{n-m\leqslant i\leqslant n}\gamma_i^{q^{\nu}}Y_i$ (очевидно, $\gamma_i^{q^{\nu}}\in H$) и остальные $Y'_{n-m+1},\dots,Y'_n$ дополняют $Y_0,\dots,Y_{n-m-1},Y'_{n-m}$ до базиса пространства линейных форм от $Y_0,\dots,Y_n$. Подставим

в полиномы $S_0,\dots,S_{k_1-1}$ вместо $Y_1,\dots,Y_{n-m-1}$ элементы $Y_0t_1,\dots,Y_0t_{n-m-1}$ соответственно. В качестве результата подстановки получаем следующую систему над полем

$$\bar S_0(Y_0,Y'_{n-m},\dots,Y'_n)=\dots=\bar S(Y_0,Y'_{n-m},\dots,Y'_n)=0, \qquad (5)$$

где $\bar S_i\in F[Y,t'_{n-m},\dots,t'_{n-m-1},Y_0,Y'_{n-m},\dots,Y'_n]$ для $0\leqslant i\leqslant k_1-1$. Подставляя нуль в полиномы $\bar S_0,\dots,\bar S_{k_1-1}$ вместо Y, мы приходим к следующей системе над полем F'

$$\tilde S_0(Y_0,Y'_{n-m},\dots,Y'_n)=\dots=\tilde S_{k_1-1}(Y_0,Y'_{n-m},\dots,Y'_n)=0. \qquad (6)$$

На основе конструкции из [I8] (см.также теорему 2.2 [4]) сопоставим системе (5) матрицу $\bar A$ над полем K' (пусть τ – число строк матрицы $\bar A$). Тогда матрица $\tilde A$, соответствующая системе (6), получается из $\bar A$ подстановкой нуля вместо Y. Применим [I8] к системам (5) и (6), принимая во внимание, что обе системы имеют конечное число решений в силу сделанного раньше предположения и леммы 2.4. В силу [I8] найдется такая неособая $\tau\times\tau$ подматрица $\tilde\Delta$ матрицы $\tilde A$, что $\det\tilde\Delta=\tilde R$ делит любой $\tau\times\tau$ минор матрицы $\tilde A$. Обозначим через $\bar\Delta$ подматрицу $\bar A$ размера $\tau\times\tau$, образованную столбцами с теми же номерами, что и $\tilde\Delta$. Можно доказать, что $0\neq\det\bar\Delta=\bar R$ также делит любой $\tau\times\tau$ минор матрицы $\bar A$.

Из леммы 2.5 [4] вытекает, что компоненты W'' многообразия W'_{ρ_R} находятся в биективном соответствии с классами сопряженных над F' корней системы (6). Лемма 2.5 влечет, что элемент $\zeta_{W''}=(Y'_{n-m}/Y_0)^{q^\nu}$ примитивен для компоненты W'', следовательно, применяя теорему 2.3 [4] и замечание непосредственно перед ней, заключаем, что $\tilde R^{q^\mu}(z^{1/q^\nu},-1,0,\dots,0)=\prod_{W''}(\tilde\Phi_{W''})^{\varepsilon_{W''}}$ (с точностью до множителя из $(F')^*$) для подходящих натуральных $\varepsilon_{W''}$ и многочленов $\Phi_{W''}\in F[t_1,\dots,t_{n-m-1},z]$ неприводимых над F (для различных W'' многочлены $\Phi_{W''}$ могут совпадать, см. уже упоминавшееся замечание из [4]) и таких, что $\tilde\Phi_{W''}(\zeta q^{\mu-\nu})=0$ (мы не предполагаем здесь старшие коэффициенты $lc_z(\tilde\Phi_{W''})$ равными единице). Итак, согласно замечанию, каждому классу сопряженных над F' корней системы (6) соответствует подходящий многочлен $\tilde\Phi_{W''}$ (через $\tilde\Phi_{W''}$ мы обозначаем многочлен, который соответствует компонен-

те w''); обратно, при этом асякому многочлену $\Phi_{w''}$ соответствуют некоторые компоненты, не обязательно одна.

Аналогично, с помощью леммы 2.5 [4], теоремы 2.3 [4] и замечания перед ней, можно вывести, что $\overline{R}^{q^{\mu}}(Z^{q^{\mu}},-1,0,\dots 0) = \overline{\Psi}^{\varepsilon}$ (с точностью до множителя из $F[Y,t_1,\dots,t_{n-m-1}] \setminus (Y)$, где (Y) обозначает главный идеал, порожденный Y) для подходящего неприводимого над F многочлена $\overline{\Psi} \in F[Y,t_1,\dots,t_{n-m-1},Z]$, при этом $\overline{\Psi}(\zeta q^{\mu-\nu}) = 0$ (снова, как и выше, мы не предполагаем, что $lc_Z(\overline{\Psi}) = 1$). Учитывая, что $\widetilde{R}$ получается из $\overline{R}$ подстановкой нуля вместо Y , мы приходим к выводу о том, что $\overline{\Psi}(0,t_1,\dots,t_{n-m-1},Z) = \prod_{w''}(\widetilde{\Phi}_{w''})^{\varepsilon_{w''}/\varepsilon}$ (с точностью до множителя из $(F')^*$), при этом $\varepsilon_{w''}/\varepsilon \in \mathbb{Z}$. Имеет место равенство

$$\Psi_p(Y,t_1,\dots,t_{n-m-1},Z) = \overline{\Psi}^{q^{-\mu+\nu}}(Y,t_1,\dots,t_{n-m-1},Z^{q^{\mu-\nu}})$$

(с точностью до множителя из F^*), так как оба полинома неприводимы. Следовательно, различные неприводимые множители многочлена $\Psi_p(0,t_1,\dots,t_{n-m-1},Z)$ соответствуют биективно неприводимым множителям многочлена $\overline{\Psi}(0,t_1,\dots,t_{n-m-1},Z)$. Это дает требуемое в формулировке леммы соответствие. Указанный в лемме изоморфизм полей следует из *леммы 2.5* [4] (отметим, что непосредственное применение *леммы 2.5* [4] к системе (6) дает изоморфизм полей, в котором стоит примитивный элемент $\zeta_{w''}^{q^{\alpha}}$ для некоторого $\alpha \geqslant 0$, следовательно, элемент $\zeta_{w''}$ также примитивен, принимая во внимание, что расширение $F' \subset F'[\zeta_{w''}]$ сепарабельно, (ср. § 3 главы I). Лемма доказана.

Изложим теперь алгоритм для определения того, удовлетворяет ли данный элемент $\zeta^{(j)} = \sum_{n-m<i<n} \gamma_i^{(j)}(Y_i/Y_0)^{q^j}$ условиям леммы 2. 5. Более того, этот алгоритм находит элемент, для которого выполнены требования, сформулированные перед леммой 2. 5, в множестве элементов, в котором такой элемент существует.

Не ограничивая общности, будем рассматривать множество элементов $\{\zeta^{(j)}\}_{1<j<N_1}$ и использовать обозначения, введенные перед леммой 2. 5. Для всякого фиксированного $\zeta^{(j)}$ выразим его в кольце $K'[\theta_p]$ и вычислим его минимальный многочлен $\Psi^{(j)} \in F'[Y,t_1,\dots,t_{n-m-1}][Z]$ неприводимый над F . Если $\deg_Z \Psi^{(j)} < \deg_Z \Phi_p$, то $\zeta^{(j)}$ не является примитивным в поле $K'[\theta_p]$. Будем предполагать, что $\deg_Z \Psi^{(j)} = \deg_Z \Phi_p$ для индексов j и j_0 , рассматриваемых ниже. Разложим $\Psi^{(j)}(0,t_1,\dots,t_{n-m-1},Z) = \lambda^{(j)} \prod_i (\Psi_i^{(j)})^{\varepsilon_{ij}}$ на неприводимые над F

множители, где $\lambda^{(i)} \in F[t_1,\dots,t_{n-m-1}]$ и $\deg_Z(\Psi_i^{(j)}) \geqslant 1$ для всех i.

ЛЕММА 2. 7. Пусть $\sum_i \varepsilon_{ij_0} = \min_j \{\sum_i \varepsilon_{ij}\}$ для некоторого j_0. Тогда $S^{(j_0)}$ удовлетворяет требованиям, сформулированным перед леммой 2. 5.

ДОКАЗАТЕЛЬСТВО. Пусть $S = S_p$ удовлетворяет лемме 2. 5 и $S \neq S^{(j_0)}$ (в противном случае все доказано). Сделаем линейную замену координат, при которой $Y_0 \to Y_0'$, $S \to (Y_1'/Y_0')^{q^\nu}$, $S^{(j_0)} \to (Y_2'/Y_0')^{q^\nu}$. Аналогично доказательству леммы 2. 6 введем системы, подобные системам (5), (6), соответственно. Так же как при доказательстве леммы 2. 6 установим, что

$$\overline{R}^{q^\mu}(Z^{1/q^\mu}, -U_0, -U_1, 0, \dots, 0) = (\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, U_0, U_1))^{\varepsilon},$$

$$\overline{R}^{q^\mu}(Z^{1/q^\mu} - 1, 0, \dots, 0) = (\Psi_p^{q^{\mu-\nu}}(Y, t_1, \dots, t_{n-m-1} Z^{q^\nu - \mu}))^{\varepsilon_p}$$

$$\overline{R}^{q^\mu}(Z^{1/q^\mu}, 0, -1, 0, \dots, 0) = ((\Psi^{(j_0)})^{q^{\mu-\nu}}(Y, t_1, \dots, t_{n-m-1} Z^{q^\nu - \mu}))^{\varepsilon_{j_0}}$$

(с точностью до множителей из $F[Y, t_1, \dots, t_{n-m-1}] \setminus (Y)$, причем многочлены $\Psi_p^{q^{\mu-\nu}}(Y, t_1, \dots, t_{n-m-1} Z^{q^\nu - \mu})$, $(\Psi^{(j_0)})^{q^{\mu-\nu}}(Y, t, \dots, t_{n-m-1}, Z^{q^\nu - \mu}) \in F[Y, t_1, \dots, t_{n-m-1}, Z]$ и $\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, U_0, U_1) \in F[Y, t_1, \dots, t_{n-m-1}, Z, U_0, U_1]$ неприводимы над F. Очевидно $\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, 1, 0) = (\Psi_p^{q^{\mu-\nu}}(Y, t_1, \dots, t_{n-m-1}, Z^{q^\nu - \mu}))^{\varepsilon_p/\varepsilon}$,

$\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, 0, 1) = ((\Psi^{(j_0)})^{q^{\mu-\nu}}(Y, t_1, \dots, t_{n-m-1}, Z^{q^\nu - \mu}))^{\varepsilon_{j_0}/\varepsilon}$ (с точностью до множителей из $F[Y, t_1, \dots, t_{n-m-1}]$), при этом $\varepsilon_p/\varepsilon$ и $\varepsilon_{j_0}/\varepsilon$ – натуральные числа. Покажем, что $\varepsilon_p/\varepsilon = \varepsilon_{j_0}/\varepsilon = 1$. Из [18] следует, что $\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, U_0, U_1) = \prod_\sigma (Z - U_0\sigma(S^{q^{\mu-\nu}}) - U_1\sigma((S^{(j_0)})^{q^{\mu-\nu}}))$ (с точностью до множителя из $(K')^*$, где σ пробегает все вложения поля $K'[S]$ в $\overline{K}'$ тождественные на поле K'. Все $\sigma(S^{q^{\mu-\nu}})$ попарно различны для разных σ, поэтому $\varepsilon_p/\varepsilon = 1$ так как многочлен $\Psi_1(Y, t_1, \dots, t_{n-m-1}, Z, 1, 0)$ не имеет кратных множителей. Так же проверяется, что $\varepsilon_{j_0}/\varepsilon = 1$.

Аналогично доказательству леммы 2. 6 разложим

$$\Psi_1(0, t_1, \dots, t_{n-m-1}, Z, U_0, U_1) = (\widetilde{R}^{q^\mu}(Z^{1/q^\mu}, -U_0, -U_1, 0, \dots, 0))^{1/\varepsilon} =$$

$$\prod_{w''} (\widetilde{\Phi}_{1,w''}(t_1, \dots, t_{n-m-1}, Z, U_0, U_1))^{\varepsilon_{w''}/\varepsilon} =$$

$$\prod_{W''}\prod_{\tau}\left(Z-U_0\tau\left(S_{W''}^{q^{\mu-\nu}}\right)-U_1\tau\left(\left(S^{(j_0)}\right)\left(S_{W''}\right)\right)^{q^{\mu-\nu}}\right)^{\varepsilon_{W''}/\varepsilon}$$

(с точностью до множителя из $(F')^*$), где τ при фиксированном W'' пробегает все вложения поля $F'[S_{W''}]$ в $\bar{F}'$, тождественные на F', при этом числа $\varepsilon_{W''}/\varepsilon \in Z$.

Выполнено равенство $\Phi_{1,W''}(t_1,\dots,t_{n-m+1},Z,1,0)=\prod_{\tau}\left(Z-\tau\left(S_{W''}^{q^{\mu-\nu}}\right)\right)=\Phi_{W''}^{q^{\mu-\nu}}\left(Z^{q^{\nu}-\mu}\right)$ (с точностью до множителя из $(F')^*$), причем $\Phi_{W''}^{q^{\mu-\nu}}$ – минимальный многочлен элемента $S_{W''}^{q^{\mu-\nu}}$ над полем F'. Следовательно, $\left(\Psi_p^{q^{\mu-\nu}}\right)\left(0,t_1,\dots,t_{n-m-1},Z^{q^{\nu}-\mu}\right)=\prod_{W''}\left(\Phi_{W''}^{q^{\mu-\nu}}\left(Z^{q^{\nu}-\mu}\right)\right)^{\varepsilon_{W''}/\varepsilon}$ (с точностью до множителя из $(F')^*$), поэтому для элемента $S=S_p$ сумма $\sum_i \varepsilon_{ij_p}=\sum_{W''}\varepsilon_{W''}/\varepsilon$. С другой стороны, для элемента $S^{(j_0)}$ $\left(\Psi^{(j_0)}\right)^{q^{\mu-\nu}}\left(0,t_1,\dots,t_{n-m-1},Z^{q^{\nu}-\mu}\right)=\prod_{W''}\left(\Phi_{1,W''}\left(t_1,\dots,t_{n-m-1},Z,0,1\right)\right)^{\varepsilon_{W''}/\varepsilon}$

Отсюда следует, что $\sum_i \varepsilon_{ij_0}\geqslant\sum_{W''}\varepsilon_{W''}/\varepsilon$. Кроме того, если $S^{(j_0)}$ не удовлетворяет требованиям, сформулированным перед леммой 2.5, то последнее неравенство является строгим, принимая во внимание, что по крайней мере один из многочленов $\tilde{\Phi}_{1,W''}(t_1,\dots,t_{n-m-1},Z,0,1)$ приводим в этом случае, так как равенство $\tau\left(S_{W''}^{(j_0)}\right)=\tau_2\left(S_{W''}^{(j_0)}\right)$ верно для некоторого W'' и вложений $\tau_1\neq\tau_2$, в противном случае $S_{W''}^{(j_0)}$ был бы примитивным в поле $F'[S_{W''}]$, что завершает доказательство леммы.

Опираясь на эту лемму, алгоритм без труда находит некоторый требуемый элемент $S=S_p$ (напомним, что мы проводим рассуждения в предположении $W'\cap\{Y_0=\dots=Y_{n-m-1}=0\}=\emptyset$, если это не так, то тем неменее алгоритм, возможно, находит некоторый элемент S).

Рассмотрим рациональную функцию $S_1=\sum_{n-m\leqslant j\leqslant n}\lambda_j\left(Y_j/Y_0\right)^{q^{\nu}}$ на V_{p_F}, где $\lambda_j\in F_u=F'(u)$, здесь u – вспомогательный трансцендентный элемент над полем K' (аналогично обозначим $K_u=K'(u)$). Через $(S_1)_{W''}$ обозначим ограничение этой рациональной функции на W''. Пусть $\Psi(Z)\in F[Y,t_1,\dots,t_{n-m-1},u][Z]$ минимальный многочлен для элемента $S_1\in K_u[S]$ над полем K_u. Зафиксируем на время компоненту W'', соответствующий ей многочлен $\tilde{\Phi}=\Phi_{W''}$ и его корень $\tilde{S}$, т.е. $\tilde{\Phi}(\tilde{S})=0$ (см. лемму 2.6).

ЛЕММА 2.8. Пусть $\Psi(0,t_1,\dots,t_{n-m-1},u,Z)=\lambda\prod_i\Psi_i^{e_i}$ –

разложение на неприводимые множители над полем $F_u[\zeta]$, где $\lambda \in F_u[\zeta]$ и $\psi_i \in F[t_1,\dots,t_{n-m-1},u,\zeta,Z]$, причем $deg_Z(\psi_i) \geq 1$. Предположим, что $\psi_i = \alpha Z - \beta$ – линейный относительно Z множитель, тогда ему соответствует некоторая компонента W_1'' многообразия $V_{p_F} \cap \{Y=0\}$ (напомним, что $con(W'_{p_F}) = V_{p_F} \cap \{Y=0\}$), для которой существует следующее вложение π полей, тождественное на F_u

$$\begin{array}{ccc} F_u[\zeta] & \supset & F_u[\beta/\alpha] \\ \uparrow \pi & \nearrow & \\ F_u[(\zeta_1)_{W_1''}] & \subset & F_u[\zeta_{W_1''}] \end{array}$$

при котором $\pi((\zeta_1)_{W_1''}) = \beta/\alpha$, и кроме того π является композицией указанных изоморфизма и вложения (компонента W_1'' не определена, вообще говоря, однозначно).

ДОКАЗАТЕЛЬСТВО. Аналогично доказательству леммы 2. 7, сделаем линейную замену координат $\{Y_i\}$ на $\{Y'_i\}$, при этом $Y_0 \to Y'_0, \zeta_1 \to (Y'_1/Y_0)^{q^\nu}$. Введем две системы уравнений сходные с системами (5) и (6), соответственно над полями K_u и F_u (в новых координатах). Как и при доказательстве леммы 2. 6 получаем, что $\overline{R}^{q^\mu}(Z^{1/q^\mu},-1,0,\dots,0) = ((\psi^{q^{\mu-\nu}})(Y,t_1,\dots,t_{n-m-1},u,Z^{q^{\nu-\mu}}))^{\varepsilon_1}$ (с точностью до множителя из $F[Y,t_1,\dots,t_{n-m-1},u] \setminus (Y)$). Отсюда следует, что $\overline{R}^{q^\mu}(Z^{1/q^\mu},-1,0,\dots,0) = \lambda \prod_i ((\psi_i^{q^{\mu-\nu}})(t_1,\dots,t_{n-m-1},u,Z^{q^{\nu-\mu}}))^{\varepsilon_i \varepsilon_1}$. Согласно [I8] всякий линейный множитель $\psi_i = (\alpha Z - \beta)|\overline{R}^{q^\mu}(Z^{1/q^\mu},-1,0,\dots,0)$ соответствует какому-то корню системы (6) (в новых координатах, см. выше), для которого $Y'_1/Y'_0 = \beta/\alpha \in F_u[\zeta]$. Из леммы 2.5 [4] вытекает, что каждому классу сопряженных над F_u корней системы (6) соответствует подходящая компонента многообразия $V_{p_F} \cap \{Y=0\}$. Таким образом, всякому линейному множителю $\psi_i = \alpha Z - \beta$ отвечает некоторая компонента W_1'', для которой существует вложение $\pi: F(u)^{q^{-\infty}}(W_1'') \hookrightarrow \overline{F}_u$, тождественное на $F_u \simeq F(u, Y_1/Y_0, \dots, Y_{n-m-1}/Y_0)$ такое, что $\pi((\zeta_1)W_1'') = \beta/\alpha$ в силу леммы 2.5 [4], что завершает доказательство леммы.

Алгоритм должен для каждой компоненты W'' многообразия W'_{p_F} построить изоморфизм полей из леммы 2. 6, другими словами, найти выражения для элементов $(Y_i/Y_0)^{q^{\nu_i}} \in F'[\zeta_{W''}]$. Это будет проделано индукцией по ϑ, где $1 \leq \vartheta = i - (n-m)+1 \leq m+1$. На первом шаге рассмотрим элемент $\zeta + u(Y_{n-m}/Y_0)^{q^\nu} \in K_u[\zeta]$ (напомним, что $\zeta = \zeta_p$), и алгоритм строит

его минимальный многочлен $\Phi_1(Z) \in F[Y, t_1, \ldots, t_{n-m-1}, u, Z]$ неприводимый над F. Далее алгоритм раскладывает многочлен $0 \neq \Phi_1(0, t_1, \ldots, t_{n-m-1}, u, Z) = \prod_i \psi_1^{(i)}$ на неприводимые множители над полем $F_u[\zeta_{w''}]$ для некоторой временно фиксированной компоненты w''.

Напомним, что $\widetilde{\Phi} = \Phi_{w''}$ и $\widetilde{\Phi}(\tilde{\zeta}) = 0$. Покажем теперь, что всякой компоненте w_1'', для которой существует вложение $F_u[Z]/(\Phi_{w_1''}) \hookrightarrow F_u[\tilde{\zeta}]$ тождественное на F_u, соответствует подходящий линейный множитель $\psi_1^{(i)}$ для некоторого i вида $\psi_1^{(i)} = Z - \zeta_{w_1''}(\tilde{\zeta}) - u(Y_{n-m}/Y_0)^{q^\nu}(\tilde{\zeta})$. Действительно, $\Phi_1(0, t_1, \ldots, t_{n-m-1}, u, \zeta_{w_1''} + u(Y_{n-m}/Y_0)^{q^\nu}) =$
$= \Phi_1(0, t_1, \ldots, t_{n-m-1}, u, \sum_{n-m \le i \le n} \gamma_i (Y_i/Y_0)^{q^\nu} + u(Y_{n-m}/Y_0)^{q^\nu}) = 0$ на w_1''. В силу упомянутого выше включения выполнено $\zeta_{w_1''} + u(Y_{n-m}/Y_0)^{q^\nu} \in F_u[\tilde{\zeta}]$ и мы получаем, что многочлен $\Phi_1(0, t_1, \ldots, t_{n-m-1}, u, Z)$ имеет однозначно определенный множитель $\psi_1^{(i)} = Z - \zeta_{w_1''}(\tilde{\zeta}) - u(Y_{n-m}/Y_0)^{q^\nu}(\tilde{\zeta})$, принимая во внимание, что рациональная функция $\zeta_{w_1''} + u(Y_{n-m}/Y_0)^{q^\nu} \in \overline{F(u)}(w_1'')$ однозначно выражается через элемент $\tilde{\zeta}$ (и тем самым, $\psi_1^{(i)}$ соответствует компоненте w_1''). Но алгоритм пока что не может выделить требуемый множитель $\psi_1^{(i)}$ среди всех множителей вида $\psi_1^{(i_1)} = Z - b_1 - u b_2$, где $b_1, b_2 \in F'[\tilde{\zeta}]$.

Согласно лемме 2. 8 имеют место равенства $\pi(\zeta_{w_2''} + u(Y_{n-m}/Y_0)^{q^\nu}) = \pi(\zeta_{w_2''}) + u\pi((Y_{n-m}/Y_0)^{q^\nu}) = b_1 + u b_2$ для некоторой компоненты w_2'' и подходящего вложения π: $F_u[\zeta_{w_2''} + u(Y_{n-m}/Y_0)^{q^\nu}] = F_u[\zeta_{w_2''}] \hookrightarrow F_u[\tilde{\zeta}]$. На первом шаге $s = 1$ алгоритм строит массив $\mathfrak{A}_\Phi^1 \subset F'[\tilde{\zeta}] \times F'[\tilde{\zeta}]$, состоящий из пар (b_1, b_2) для всех упомянутых выше линейных множителей $\psi_1^{(i_1)}$. После этого алгоритм находит такой $c_{n-m} \in H$, что выполняются следующие два условия. Во-первых, для всяких двух различных линейных множителей $\psi_1^{(i_1)} = Z - b_1^{(1)} - u b_2^{(1)}$ и $\psi_1^{(i_2)} = Z - b_1^{(2)} - u b_2^{(2)}$ имеет место неравенство $b_1^{(1)} + c_{n-m} b_2^{(1)} \neq b_1^{(2)} + c_{n-m} b_2^{(2)}$ и, во-вторых, элемент $\zeta + c_{n-m}(Y_{n-m}/Y_0)^{q^\nu}$ удовлетворяет требованиям, сформулированным перед леммой 2. 5. Для этого алгоритм выбирает $N_2 = 2((d+1)^{m+1} - 1) + 1$ элементов $c^{(1)}, \ldots, c^{(N_2)} \in H$, таких что $c^{(j)} \neq -(b_1^{(1)} - b_1^{(2)})/(b_2^{(1)} - b_2^{(2)})$ для всех $1 \le j \le N_2$ и всех пар линейных множителей $\psi_1^{(i_1)}, \psi_1^{(i_2)}$ для которых $b_2^{(1)} \neq b_2^{(2)}$. Рассуждая как при доказательстве леммы

2. 5, можно показать, что оба сформулированные условия выполнены, по крайней мере, для одного элемента $c_{n-m} = c^{(j)}$; алгоритм находит такой элемент $c^{(j)}$ на основе леммы 2. 7.

Допустим, что алгоритм осуществил уже $(s-1)$ шагов и построены элементы $c_{n-m}, \ldots, c_{n-m+s-2} \in H$. Помимо этого, алгоритм построил некоторый конечный массив $\mathfrak{A}_{\Phi}^{(s-1)} \subset \underbrace{F'[\zeta] \times \ldots \times F'[\zeta]}_{s}$ такой, что для каждой компоненты W_1'' , для которой существует вложение $\pi : F_u[Z]/(\Phi_{W_1''}) \hookrightarrow F_u[\zeta]$ (тождественное на F_u), вектор $(\pi(\zeta_{W_1''}), \pi((Y_{n-m}/Y_0)^{q^\nu}), \ldots, \pi((Y_{n-m+s-2}/Y_0)^{q^\nu})) \in \mathfrak{A}_{\Phi}^{(s-1)}$, и обратно, массив $\mathfrak{A}_{\Phi}^{(s-1)}$ исчерпывается векторами этого вида. При этом для всякой пары различных векторов $(a_0^{(1)}, a_{n-m}^{(1)}, \ldots, a_{n-m+s-2}^{(1)}), (a_0^{(2)}, a_{n-m}^{(2)}, \ldots, a_{n-m+s-2}^{(2)}) \in \mathfrak{A}_{\Phi}^{(s-1)}$ выполнено неравенство $a_0^{(1)} + \sum_{n-m \le j \le n-m+s-2} c_j a_j^{(1)} \neq a_0^{(2)} + \sum_{n-m \le j \le n-m+s-2} c_j a_j^{(2)}$ и кроме того, элемент $\zeta + \sum_{n-m \le j \le n-m+s-2} c_j (Y_j/Y_0)^{q^\nu}$ удовлетворяет требованиям, сформулированным перед леммой 2. 5 (ср. первый шаг алгоритма). Причем $card(\mathfrak{A}_{\Phi}^{(s-1)}) \le deg \Phi_{s-1} \le deg V_{p_F} \le (d+1)^{m+1}$, где Φ_{s-1} – минимальный многочлен элемента $\zeta + \sum_{n-m \le j \le n-m+s-2} c_j \cdot (Y_j/Y_0)^{q^\nu} + U(Y_{n-m+s-2}/Y_0)^{q^\nu}$ над полем K_u .

Для осуществления s-го шага алгоритм рассматривает элемент $\zeta_s = \zeta + \sum_{n-m \le j \le n-m+s-2} c_j (Y_j/Y_0)^{q^\nu} + U(Y_{n-m+s-2}/Y_0)^{q^\nu}$ и находит его минимальный над K_u многочлен $\Phi_s(Z) \in F[Y, t_1, \ldots, t_{n-m-1}, U, Z]$ неприводимый над F (ср. первый шаг). Затем алгоритм раскладывает многочлен $0 \neq \Phi_s(0, t_1, \ldots, t_{n-m-1}, U, Z) = \prod_i \psi_s^{(i)}$ на неприводимые множители над полем $F_u[\zeta]$. Подобно тому, как на первом шаге, всякой компоненте W_1'' , для которой существует вложение $\pi : F_u[Z]/(\Phi_{W_1''}) \hookrightarrow F_u[\zeta]$, соответствует подходящий линейный множитель $\psi_s^{(i)} = (Z - \pi(\zeta_{W_1''}) - \sum_{n-m \le j \le n-m+s-2} c_j \pi((Y_j/Y_0)^{q^\nu}) - U\pi((Y_{n-m+s-1}/Y_0)^{q^\nu}))$ для некоторого i . После этого алгоритм выбирает такое $c_{n-m+s-1} \in H$, что для каждой пары линейных множителей вида $\psi_s^{(i_1)} = Z - b_1^{(1)} - U b_2^{(1)}$ и $\psi_s^{(i_2)} = Z - b_1^{(2)} - U b_2^{(2)}$, где $b_1^{(1)}, b_2^{(1)}, b_1^{(2)}, b_2^{(2)} \in F'[\zeta]$ выполняются следующие два условия (ср. первый шаг). Во-первых, если $b_1^{(1)} + c_{n+m+s-1} b_2^{(1)} = b_1^{(2)} + c_{n+m+s-1} b_2^{(2)}$, то $b_1^{(1)} = b_1^{(2)}$, $b_2^{(1)} = b_2^{(2)}$. Во-вторых, элемент $\zeta + \sum_{n-m \le j \le n-m+s-1} c_j (Y_j/Y_0)^{q^\nu}$ удовлетворяет требованиям, сформулированным перед леммой 2. 5. Алгоритм выбирает $c_{n-m+s-1}$ так же как при осуществлении первого шага $(s=1)$.

Из леммы 2. 8 вытекает, что для всякого линейного множителя $\psi_s^{(i)} = Z - b_1 - ub_2$, для которого $b_1, b_2 \in F'[\xi]$, существует компонента W_1'' и вложение $\pi: F_u[Z]/(\Phi_{W_1''}) \hookrightarrow F_u[\xi]$ такие, что

$$\pi(\zeta_{W_1''} + \sum_{n-m \le j \le n-m+s-2} c_j (Y_j/Y_0)^{q^\nu}) = b_1, \quad \pi((Y_{n-m+s-1}/Y_0)^{q^\nu}) = b_2$$

в силу трансцендентности u, и учитывая, что равенство $F_u[Z]/(\Phi_{W_2''}) = F_u[(\zeta_2)_{W_2''}]$ имеет место для всех компонент W_2''. Индукционное предположение влечет, что вектор $(\pi(\zeta_{W_1''}), \pi((Y_{n-m}/Y_0)^{q^\nu}), \dots, \pi((Y_{n-m+s-2}/Y_0)^{q^\nu})) \in \mathfrak{A}_{\Phi}^{(s-1)}$.

Переходим к построению массива $\mathfrak{A}_{\Phi}^{(s)} \subset \underbrace{F'[\xi] \times \dots \times F'[\xi]}$

Для всякого линейного множителя вида $\psi_s^{(i)} = (Z - b_1 - u^{(s+1)} b_2)$ занесем в массив $\mathfrak{A}_{\Phi}^{(s)}$ вектор $(\pi(\zeta_{W_1''}), \pi((Y_{n-m}/Y_0)^{q^\nu}), \dots, \pi((Y_{n-m+s-2}/Y_0)^{q^\nu}), b_2)$, где $(\pi(\zeta_{W_1''}), \pi((Y_{n-m}/Y_0)^{q^\nu}), \dots, \pi((Y_{n-m+s-2}/Y_0)^{q^\nu}))$ – тот единственный (в силу индукционного предположения) вектор, для которого выполнено $\pi(\zeta_{W_1''}) + \sum_{n-m \le j \le n-m+s-2} c_j (Y_j/Y_0)^{q^\nu} = b_1$. Из свойств элемента $c_{n-m+s-1}$ следует, что для произвольной пары различных векторов выполнено неравенство $a_0^{(1)} + \sum_{n-m \le j \le n-m+s-1} c_j a_j^{(1)} \ne a_0^{(2)} + \sum_{n-m \le j \le n-m+s-1} c_j a_j^{(2)}$.

Выполняя таким образом $(m+1)$ шагов, алгоритм строит массив $\mathfrak{A}_{\Phi}^{(m+1)}$.

ЛЕММА 2. 9. Имеется биективное соответствие между теми векторами $(a_0, a_{n-m}, \dots, a_n) \in \mathfrak{A}_{\Phi}^{(m+1)}$, у которых $a_0 = \tilde{\xi}$ и, с другой стороны, теми компонентами W_1'' многообразия $V_{p_F} \cap \{Y = 0\}$, для которых многочлен $\Phi_{W_1''} = \tilde{\Phi}$; при этом $\pi(\zeta_{W_1''}) = \tilde{\zeta}$ и $\pi((Y_j/Y_0)^{q^\nu}(\zeta_{W_1''})) = a_j$ для всех $n - m \le j \le n$.

ДОКАЗАТЕЛЬСТВО. Заметим, что если $\pi(\zeta_{W_1''}) = \tilde{\zeta}$, то π является изоморфизмом и $\Phi_{W_1''} = \tilde{\Phi}$. Всякой компоненте W_1'', такой что $\Phi_{W_1''} = \tilde{\Phi}$, соответствует (согласно изложенной выше конструкции) единственный вектор $(\pi(\zeta_{W_1''}), \pi((Y_{n-m}/Y_0)^{q^\nu}(\zeta_{W_1''})), \dots, \pi((Y_n/Y_0)^{q^\nu}(\zeta_{W_1''}))) \in \mathfrak{A}_{\Phi}^{(m+1)}$; $\pi(\zeta_{W_1''}) = \tilde{\zeta}$, принимая во внимание, что π полностью определяется равенством $\pi(\zeta_{W_1''}) = \tilde{\zeta}$. Различным компонентам W_1'', W_2'' соответствуют при этом различные векторы, так как в противном случае получаем изоморфизм подколец $F[Y_1/Y_0, \dots, Y_{n-m-1}/Y_0, (Y_{n-m}/Y_0)^{q^\nu}, \dots, (Y_n/Y_0)^{q^\nu}]$ полей

рациональных функций компонент W_1'', W_2'' соответственно, при котором $Y_i/Y_0 \rightsquigarrow Y_i/Y_0$ для $1 \le i \le n-m-1$ и $(Y_i/Y_0)^{q^\nu} \rightsquigarrow (Y_i/Y_0)^{q^\nu}$ для $n-m \le i \le n$, здесь Y_i/Y_0 рассматриваются в левой части (соответственно, в правой) части отображения как рациональные функции на W_1'' (соответственно, на W_2''). Приходим к противоречию с тем, что $W_1'' \neq W_2''$, которое завершает доказательство леммы.

Алгоритм перебирает всевозможные многочлены $\tilde{\Phi} = \Phi_{W''}$ (см. лемму 2. 6) и опираясь на лемму 2. 9, строит общие точки тех компонент W_1'', для которых $\Phi_{W_1''} = \tilde{\Phi}$. Соответствующей компоненте по лемме 2. 9 вектор из массива $\mathfrak{N}_{\tilde{\Phi}}^{(m+1)}$ как раз и дает требуемую общую точку. Описанный выше алгоритм выполняем для всех простых идеалов вида $\mathfrak{p}_F$ (см. выше, например, доказательство леммы 2. 2), и тем самым, строим общие точки всех компонент W'' многообразия W'.

Вернемся теперь к вопросу о выборе $(Y_0, \dots, Y_{n-m-1}) \in \mathfrak{M}$. Если даже $W' \cap \{ Y_0 = \dots = Y_{n-m-1} = 0 \} \neq \emptyset$, то тем не менее, выходом алгоритма (в предположении, что алгоритм не остановится раньше) является некоторый массив $\mathfrak{N}_{\tilde{\Phi}}^{(m+1)}$. Всякий вектор $(\tilde{\zeta}, a_{n-m}, \dots, a_n) \in \mathfrak{N}_{\tilde{\Phi}}^{(m+1)}$ задает общую точку некоторого неприводимого $(n-m-1)$-мерного подмногообразия $\tilde{W} \subset \mathbb{P}^n(\bar{F})$, определяемого следующим образом. Вектор задает вложение $F^{q-\infty}(\tilde{W}) \supset F(Y_1/Y_0, \dots, Y_{n-m-1}/Y_0, (Y_{n-m}/Y_0)^{q^\nu}, \dots, (Y_n/Y_0)^{q^\nu}) \hookrightarrow F'[\tilde{\zeta}]$, при котором $\tilde{\pi}(Y_i/Y_0) = t_i$, $1 \le i \le n-m-1$ $\tilde{\pi}((Y_i/Y_0)^{q^\nu}) = a_i$, $n-m \le i \le n$. Если $\sum_{n-m \le i \le n} \gamma_i a_i \neq \tilde{\zeta}$ (напомним, что $\varphi = \sum_{n-m \le i \le n} \gamma_i (Y_i/Y_0)^{q^\nu}$), $W' \cap \{ Y_0 = \dots = Y_{n-m-1} = 0 \} \neq \emptyset$ и алгоритм прекращает рассматривать элемент $(Y_0, \dots, Y_{n-m-1}) \in \mathfrak{M}$. Если же $\sum_{n-m \le i \le n} \gamma_i (Y_i/Y_0)^{q^\nu} = \tilde{\zeta}$, то $\tilde{\pi}$ является изоморфизмом, который задает общую точку многообразия $\tilde{W}$. Затем алгоритм подставляет выражения $\tilde{\pi}((Y_{n-m}/Y_0)^{q^\nu}), \dots, \tilde{\pi}((Y_n/Y_0)^{q^\nu})$ в $h_1^{q^\nu}, \dots, h_{m+1}^{q^\nu}$ вместо $(Y_{n-m}/Y_0)^{q^\nu}, \dots, (Y_n/Y_0)^{q^\nu}$, соответственно, и $t_1, \dots, t_{n-m-1}$ вместо $Y_1/Y_0, \dots, Y_{n-m-1}/Y_0$ (см. выше описание дерева компонент). Если полученные элементы поля $F'[\tilde{\zeta}]$ равны нулю, то либо $\tilde{W} = W_w$ для подходящей вершины w дерева компонент уровня $(m+1)$, либо $\tilde{W} \subset W_{v_1}$ для некоторого листа v_1 первого типа уровня не большего m (см. начало параграфа). Семейство тех неприводимых многообразий $\tilde{W}$, для которых все полученные элементы равны нулю, обозначим через $\mathcal{J}$ (ниже считаем, что $\tilde{W}$ принадлежит $\mathcal{J}$).

Отметим, что до сих пор алгоритм не обращается к многочленам $\psi_j^{(v)}$ (см. начала параграфа). Далее, алгоритм подставляет выражения $\tilde{\pi}((Y_{n-m}/Y_0)^{q^v}),\ldots,\tilde{\pi}((Y_n/Y_0)^{q^v})$ в многочлены $\psi_0^{(v_1)},\ldots,\psi_{N_3}^{(v_1)}$ для временно фиксированного листа v_1 первого типа уровня не больше m. Если для всякого листа v_1 не все полученные элементы поля $F'[\zeta]$ равны нулю, то $\tilde{W}=W_w$ для подходящей вершины w уровня $(m+1)$ (ниже считаем, что $\tilde{W}=W_w$). Подставляя, наконец, выражения $\tilde{\pi}((Y_{n-m}/Y_0)^{q^v}),\ldots,\tilde{\pi}((Y_n/Y_0)^{q^v})$ в многочлены $\psi_0^{(v)},\ldots,\psi_N^{(v)}$ для вершины v уровня m, проверяем, не является ли вершина w сыном вершины v (последнее равносильно тому, что все полученные элементы поля $F'[\zeta]$ равны нулю).

Из леммы 2.3 вытекает, что среди многообразий $\tilde{W}$ содержатся многообразия W_w для всех вершин w уровня $(m+1)$. В результате, мы построили семейство, которое состоит из всех многообразий W_w для вершин w уровня $(m+1)$ (возможно, какие-то многообразия W_w входят в это семейство более, чем по одному разу). Для выделения различных среди построенных многообразий W_w, можно будет воспользоваться построенными ниже многочленами $\psi_j^{(w)}$.

Переходим теперь к построению многочленов $\psi_j^{(w)}$, $0\le j\le N_4\le(3(d+d_1+d_2)^{m+2})^{n+\ell}$. Зафиксируем компоненту $\tilde{W}=W_w$. Рассмотрим некоторое семейство многочленов $g_1,\ldots,g_3\in H[T_1,\ldots,T_\ell,T,X_0,\ldots,X_n]$ такое, что однородный идеал $g_1(T_1,\ldots,T_\ell,\eta,X_0,\ldots,X_n),\ldots,g_3(T_1,\ldots,T_\ell,\eta,X_0,\ldots,X_n))\subset F[X_0,\ldots,X_n]$ – простой и задает многообразие $\tilde{W}$. С другой стороны, $\tilde{W}$ является компонентой многообразия $\{h_1(T_1,\ldots,T_\ell,\eta,X_0,\ldots,X_n)=\ldots=h_{m+1}(T_1,\ldots,T_\ell,\eta,X_0,\ldots,X_n)=0\}$. Рассматривая многообразие $con(\tilde{W})\subset\mathbb{A}^{m+1}(\bar{F})$ можно получить, что многообразие $\{g_1(T_1,\ldots,T_\ell,T,X_0,\ldots,X_n)=\ldots=g_3(T_1,\ldots,T_\ell,T,X_0,\ldots,X_n)=\varphi(T_1,\ldots,T_\ell,T)=0\}\subset\mathbb{A}^{n+\ell+2}(\bar{H})$ является неприводимой над H компонентой многообразия $U=\{h_1(T_1,\ldots,T_\ell,T,X_0,\ldots,X_n)=\ldots=h_{m+1}(T_1,\ldots,T_\ell,T,X_0,\ldots,X_n)=\varphi(T_1,\ldots,T_\ell,T)=0\}\subset\mathbb{A}^{n+\ell+2}(\bar{H})$. Следовательно, $\deg U\le(d+d_1+d_2)^{m+1}d_1$.

Пусть $\psi_0^{(u)},\ldots,\psi_{N_3}^{(u)}\in H[T_1,\ldots,T_\ell,T,X_0,\ldots,X_n]$ – некоторый базис линейного пространства над H многочленов степени $\deg(\psi_i^{(u)})\le(d+d_1+d_2)^{m+1}d_1$, которые равны нулю на многообразии U, причем $\psi_i^{(u)}$ однороден относительно переменных $X_0,\ldots,X_n$. Нетрудно проверить, что выполнено равенство

$U = \{ \psi_0^{(u)} = \ldots = \psi_{N_3}^{(u)} = 0 \}$. Отсюда следует, что радикал $rad(\psi_0^{(u)}, \ldots, \psi_{N_3}^{(u)}) = rad(g_1, \ldots, g_3, \varphi) \subset H[T_1, \ldots, T_\ell, T, X_0, \ldots, X_n]$. Вследствие этого, $rad(\psi_0^{(u)}|_{T=\eta}, \ldots, \psi_{N_3}^{(u)}|_{T=\eta}) = rad(g_1, \ldots, g_3) \subset F[X_0, \ldots, X_n]$, поэтому $\tilde{W} = \{ \psi_0^{(u)}|_{T=\eta} = \ldots = \psi_{N_3}^{(u)}|_{T=\eta} = 0 \}$.

Таким образом, в качестве $\psi_0^{(w)}, \ldots, \psi_{N_4}^{(w)}$ алгоритм берет базис линейного пространства над H многочленов $g\varphi^\nu(T_1, \ldots, T_\ell, \eta, X_0, \ldots, X_n) \in F[X_0, \ldots, X_n]$ таких что g является многочленом также и от переменных $T_1, \ldots, T_\ell$ и η , кроме того $deg(g) \leq (d + d_1 + d_2)^{m+1} d_1$ (здесь под степенью $deg(g)$ мы имеем в виду степень относительно переменных $T_1, \ldots, T_\ell, X_0, \ldots, X_n$), и наконец, g равен нулю на $\tilde{W}$. Для построения многочленов $\psi_0^{(w)}, \ldots, \psi_{N_4}^{(w)}$ алгоритм решает линейную над H систему уравнений, неизвестными которой служат не более, чем $\left((d + d_1 + d_2)^{m+2} + n + \ell + 1\right) \leq \leq (3(d + d_1 + d_2)^{m+2})^{n+\ell+1}$ коэффициентов из H многочлена g . В этой системе количество уравнений оценивается сверху некоторым полиномом от

$$\left((d + d_1 + d_2)^{m+2} \max_{j, w''} \left\{ deg_{T_1, \ldots, T_\ell, t_1, \ldots, t_{n-m-1}} (X_j / X_{j_0})^{q^\nu}, \; deg_{T_1, \ldots, T_\ell, t_1, \ldots, t_{n-m-1}} (\Phi_{w''}) \right\}\right)^{n-m+\ell+1} .$$

Подставляя выражения для $(Y_j / Y_0)^{q^\nu}$ из построенных ранее общих точек компонент W_w в найденные только что системы уравнений, алгоритм выделяет среди компонент W_w попарно различные. Это завершает описание алгоритма построения дерева компонент, т.е. общих точек и задающих систем уравнений для многообразий W_w для всех вершин w уровня $(m+1)$.

Перейдем теперь к установлению требуемых оценок (см. начало настоящего параграфа). Оценки на степени элементов $(X_j / X_{j_0})^{q^\nu}$, Φ_w можно получить с помощью главы I и теоремы 2.3 [4], примененной к системе (3'). Обратимся к оценкам на длины записей коэффициентов из H . Напомним, что прежде всего алгоритм строит многочлены ψ_p , применяя §2 гл.2 [4] к системе (3'). Следовательно, $\ell(\psi_p) \leq (M_1 + M_2 + (n-m+\ell) \; d_2) \; P_1(d^m \, d_1)$ (здесь и ниже P_1, P_2, P_3, P_4 обозначают подходящие полиномы). Для делителей $\tilde{\Phi} = \Phi_{w''} \mid \psi_p(0, t_1, \ldots, t_{n-m-1}, Z)$ (см. лемму 2. 6) имеют место аналогичные оценки $\ell(\tilde{\Phi}) \leq (M_1 + M_2 + (n-m+\ell) \; d_2) P_2(d^m d_1)$ согласно главе I. После этого алгоритм строит выражения для $(Y_j / Y_0)^{q^\nu}$, для них (снова в силу главы I) выполнены

оценки $l((Y_j/Y_0)^{q^\nu}) \le (M_1+M_2+(n-m+l)\ d_2)P_3(d^m d_1)$. Используя процедуру, изложенную в конце [4], для перехода от координат $\{Y_i\}$ к $\{X_i\}$, алгоритм выражает общую точку и задающую систему уравнений через координаты $\{X_j\}$. Таким образом, аналогичная оценка верна также и для $l((X_j/X_{j_0})^{q^\nu})$. Кроме того $l(\psi_j^{(w)}) \le (M_1+M_2)P_4((d+d_1+d_2)^{m(n-m+l+1)})$, принимая во внимание, что $\psi_j^{(w)}$ получается из решения линейной системы над H, число уравнений которой не превосходит некоторого полинома от $(d+d_1+d_2)^{m(n-m+l+1)}$.

Оценим наконец, время работы алгоритма. Для построения многочленов ψ_p исходя из системы (3), достаточно полиномиального от $M_1, M_2, (d^m d_1 d_2)^{n-m+l+1}$ времени согласно теореме 2.3 [4]. Многочлены $\Phi = \Phi_{W''}$ алгоритм строит за время полиномиальное от $M_1, M_2, (d^m d_1 d_2)^{n-m+l+1}$ с помощью главы I (см.лемму 2.6). Время нахождения выражений $(Y_j/Y_0)^{q^\nu}$ (а, следовательно, также и $(X_j/X_{j_0})^{q^\mu}$, см. в конце [4] оценки на время работы процедуры для перехода от координат $\{Y_i\}$ к $\{X_i\}$, принимая во внимание, что здесь оценки на $deg(\chi)$ лучше, ср.оценки на $deg\,\psi_j^{(w)}$) можно оценить сверху некоторым полиномом от тех же величин в силу §2 гл.2 [4] и главы I (см.леммы 2.8., 2.9). Для построения многочленов $\psi_j^{(w)}$ алгоритм решает линейную систему за полиномиальное от $M_1, M_2, (d+d_1+d_2)^{m(n+l)}$ время. В оценку суммарного времени работы входит также время работы, необходимое для перебора $(n-m)$-ок из $\mathcal{M}$ (см.лемму 2.3 [4] и лемму 2.4) и перебора для нахождения $\gamma = \gamma_p$ (см.леммы 2.5, 2.7), но это не увеличивает установленной выше асимптотической оценки времени работы алгоритма.

Подытожим результаты настоящего параграфа в следующей теореме.

ТЕОРЕМА 2.1. Предлагается алгоритм, который для каждой компоненты W_ν (см. введение и начало параграфа) коразмерности m строит ее общую точку, причем $q^{\nu_j} \le d^{2m}$, $deg_Z(\Phi_\nu) \le d^m$, далее, степени $deg_{\tau_1,\dots,\tau_l,t_1,\dots,t_{n-m}}(\Phi_\nu)$, $deg_{\tau_1,\dots,\tau_l,t_1,\dots,t_{n-m}}(X_j/X_{j_0})^{q^{\nu_j}}$ не превосходят некоторого полинома от $d^m d_1 d_2$, кроме того

$$l(h_j),\ l(\Phi_\nu),\ l((X_j/X_{j_0})^{q^{\nu_j}}) \le M_1+M_2+(n-m+l)\ d_2)P(d^m d_1)$$

(здесь и ниже P обозначает некоторый подходящий полином). Помимо этого, алгоритм строит семейство многочленов $\psi_j^{(\nu)}$ $0 \le j \le N \le (3(d+d_1+d_2)^{m+1})^{n+l}$, такое что $W_\nu = \{\psi_0^{(\nu)} = \dots = \psi_N^{(\nu)} = 0\}$

при этом выполняются следующие неравенства $deg_{T_1,\dots,T_\ell X_0,\dots,X_n}(\psi_j^{(v)}) \le$ $\le (d+d_1+d_2)^{2m+1}$ $l(\psi_j^{(v)}) \le (M_1+M)\,P((d+d_1+d_2)^{m(n-m+l+1)})$.

Суммарное время работы алгоритма оценивается сверху некоторым полиномом от $M_1, M_2, (d+d_1+d_2)^{m(n-m+l+1)}, q$.

ЗАМЕЧАНИЕ. Отметим, что из приведенного описания алгоритма можно заключить, что если на предыдущем шаге работы в дереве компонент были построены многочлены $h_1,\dots,h_m$ и общие точки многообразий W_v для всех вершин v уровня m, причем на параметры элементов $\Phi_v, (X_j/X_{j_0})^{q^{v_j}}$ выполнены оценки, указанные в теореме 2.I, то на следующем шаге алгоритм строит, в действительности, общие точки некоторых неприводимых многообразий $\tilde{W}$ (из семейства $\mathcal{F}$, см.выше) коразмерности $(m+1)$, среди которых содержатся компоненты W_w для всех вершин w уровня $(m+1)$ (возможно, с повторениями). Только лишь для выделения из построенного семейства $\mathcal{F}$, во-первых, посторонних многообразий $\tilde{W}$, т.е. таких что $\tilde{W} \subset W_{v_1}$ для некоторого листа v_1 первого типа уровня не больше m в дереве компонент, используются многочлены $\psi_0^{(v_1)},\dots,\psi_{N_3}^{(v_1)}$ и, во-вторых, для выделения среди многообразий W_w из семейства $\mathcal{F}$ попарно различных используются многочлены $\psi_0^{(w)},\dots,\psi_{N_4}^{(w)}$, которые строятся на текущем шаге. Этим замечанием мы воспользуемся в §§ 2, 3.

В следующем параграфе будет предложен алгоритм, строящий за время, меньшее чем выше, систему уравнений, задающую W_v. К этому алгоритму мы применим только что сформулированное замечание, и таким образом получим алгоритм для построения общих точек и задающих систем уравнений многообразий W_v с лучшей оценкой на суммарное время работы.

§ 2. Улучшенная конструкция системы уравнений определяющих неприводимую компоненту

Мы используем обозначения из введения и § I.

Пусть проективное многообразие W является неприводимой над полем F компонентой многообразия $\{h_1=\dots=h_m=0\}$ (см. § I), $\operatorname{codim} W = m$ и пусть нам дана общая точка многообразия W, именно, задан изоморфизм полей

$$F(t_1,\dots,t_{n-m})[\theta] \xrightarrow{\sim} F(X_1/X_0,\dots,X_{n-m}/X_0,(X_{n-m+1}/X_0)^{q^{v}},\dots,(X_n/X_0)^{q^{v}}) \subset \bar{F}^{q^\infty}(W),$$

при котором $t_i \to X_i / X_0$, $1 \leqslant i \leqslant n-m$ (ср. введение); без ограничения общности мы предполагаем, что $W \not\subset \{X_0 = 0\}$. Предположим, что $\Phi(\theta) = 0$, многочлен $\Phi \in F(t_1, \dots, t_{n-m})[Z]$ неприводим над полем $F' = F(t_1, \dots, t_{n-m})$ и сепарабелен. Степень $deg_Z(\Phi) \leqslant deg\, W < d_3 \leqslant d^m$, кроме того $deg_{\tau_1, \dots, \tau_e, t_1, \dots, t_{n-m}}(\Phi)$, $deg_{\tau_1, \dots, \tau_e, t_1, \dots, t_{n-m}}(X_i / X_{j_0})^{q^\nu} < d_4$ и d_4 не превосходит полинома от d^m d_1 d_2 согласно теореме 2.I § I, далее $q^\nu \leqslant d_5 \leqslant d^m$ и, наконец, длины записей $l(\Phi), l((X_i / X_0)^{q^\nu}) \leqslant M_3$ и величина $M_3 \leqslant (M_1 + M_2 + (l + n - m)\ d_2)\ P_1(d^m d_1)$, где P_1 – некоторый полином, в силу теоремы 2.I. Можно показать, что многообразие W определено над полем $F^{q^{-\infty}}$.

Цель настоящего параграфа состоит в построении однородных многочленов $\Psi_1, \dots, \Psi_N \in F[X_0, \dots, X_n]$, таких что $W = \{\Psi_1 = \dots = \Psi_N = 0\}$, причем $N \leqslant m^2 d_3^3 d_5 \leqslant m^2 d^{4m}$. Оценки на степени многочленов и время работы алгоритма будут лучшими, чем в § I.

Прежде всего построим некоторый вспомогательный алгоритм для решения следующей задачи. Обозначим $(d_3 d_5)/q < q^\mu \leqslant d_3 d_5$, когда $q > 0$ и $q^\mu = 1$, как обычно, когда $char(F) = 0$. Мы хотим построить линейно независимое семейство линейных форм $U_0 = X_0, U_1, \dots, U_n$ от переменных $X_0, \dots, X_n$ с коэффициентами из H, удовлетворяющее следующим двум условиям:

а) рациональные функции $\chi_1 = U_1 / U_0, \dots, \chi_{n-m} = U_{n-m} / U_0$ образуют базис трансцендентности поля функций многообразия W;

в) проекция $\pi: \mathbb{P}^n(\bar{F}) \to \mathbb{P}^{n-m}(\bar{F})$, заданная формулой $\pi: (X_0 : \dots : X_n) \to (U_0 : \dots : U_{n-m})$ определена всюду на многообразии W (следовательно, $\pi(W) = \mathbb{P}^{n-m}$, см., например, гл.I [7]) и ограничение π на подмногообразие W является конечным морфизмом (см., например, [7]).

Для решения этой задачи индукцией по $0 \leqslant s \leqslant m$ алгоритм строит семейство линейно независимых форм $U_0^{(s)} = X_0, U_1^{(s)}, \dots, U_n^{(s)}$, удовлетворяющих условию $a^{(s)}$) аналогичному а) с заменой U_i на $U_i^{(s)}$ и χ_i на $\chi_i^{(s)} = U_i^{(s)} / U_0^{(s)}$. Кроме того, для этих форм выполнены следующие два условия ($в^{(s)}$) аналогично в)).

$в^{(s)}$) проекция $\pi_s : \mathbb{P}^n \to \mathbb{P}^{n-s}$, заданная формулой $\pi_s : (X_0 : \dots : X_n) \to (U_0^{(s)} : \dots : U_{n-s}^{(s)})$, определена всюду на W)следовательно, $\pi_s(W) \subset \mathbb{P}^{n-s}$ – замкнутое проективное подмногообразие, см. гл. I [7] и ограничение $\pi_s : W \to \pi_s(W)$ – конечный морфизм;

$с^{(s)}$) имеют место равенства $U_i^{(s)} = U_i^{(0)} + \sum_{0 \leqslant j \leqslant s-1} c_i^{(j)} U_{n-j}^{(0)}$

для подходящих $c_i^{(j)} \in H$, причем $\ell(c_i^{(j)}) \leqslant \log(d_3)$, кроме того $U_{n-m+i}^{(s)} = U_{n-m+i}^{(0)} = X_{n-m+i}$ для $1 \leqslant i \leqslant m$.

Когда $s = m$, положив $W_i = U_i^{(m)}$, мы получим, что для W_i выполнены условия а) и в).

В случае $s = 0$, пусть $U_i^{(0)} = X_i$ для $0 \leqslant i \leqslant n$.

Предположим теперь, что для некоторого $s < m$ требуемое семейство $U_0^{(s)}, \ldots, U_n^{(s)}$ уже построено. Тогда, решая линейную систему (ср. § 4 [4] и см. лемму 2.10 ниже) алгоритм находит неприводимый над F многочлен $0 \neq g = g_2^{q^\nu} \in F[Z_1, \ldots, Z_{n-m+1}]$, где $g_2 \in F^{q^\nu}[Z_1, \ldots, Z_{n-m+1}]$, такой что $g(Y_1^{(s)}, \ldots, Y_{n-m}^{(s)}, X_{n-s}/X_0) = 0$ на W, причем $\deg_{Z_1, \ldots, Z_{n-m-1}}(g) < d_3$. Обозначим через $\overline{g}$ форму старшей степени многочлена g. Алгоритм выбирает некоторые $c_1^{(s)}, \ldots, c_{n-m}^{(s)} \in H$, для которых значение $\overline{g}(-c_1^{(s)}, \ldots, -c_{n-m}^{(s)}, 1) \neq 0$.

Теперь положим $U_i^{(s+1)} = U_i^{(s)} + c_i^{(s)} X_{n-s}$ для $1 \leqslant i \leqslant n-m$. Следовательно, условие $c^{(s+1)}$ выполнено. Покажем, что $Y_1^{(s+1)}, \ldots, Y_{n-m}^{(s+1)}$ – базис трансцендентности для W (т.е. что выполнено $a^{(s+1)}$)). Действительно, $n-m = \deg tr_F\{Y_1^{(s)}, \ldots, Y_{n-m}^{(s)}, X_{n-s}/X_0\} = \deg tr_F\{Y_1^{(s+1)}, \ldots, Y_{n-m}^{(s+1)}, X_{n-s}/X_0\}$. Обозначим $g_1(Z_1, \ldots, Z_{n-m+1}) = g(Z_1 - c_1^{(s)} Z_{n-m+1}, \ldots, Z_{n-m} - c_{n-m}^{(s)} Z_{n-m+1}, Z_{n-m+1})$. Тогда g_1 неприводим над F, кроме того, $\deg_{Z_{n-m+1}}(g_1) = \deg(g) > 0$ и $g_1(Y_1^{(s+1)}, \ldots, Y_{n-m}^{(s+1)}, X_{n-m}/X_0) = 0$ на W. Следовательно, $\deg tr_F\{Y_1^{(s+1)}, \ldots, Y_{n-m}^{(s+1)}\} = n-m$, что доказывает $a^{(s+1)}$).

Рассмотрим точку $\Omega \in \mathbb{P}^{n-s}$ с координатами $(U_0^{(s+1)} : \ldots : U_{n-s}^{(s+1)}) = (0 : \ldots : 0 : 1)$. Обозначим $\tilde{g}_1(Z_0, \ldots, Z_{n-m+1}) = Z_0^{\deg(g_1)} g_1(Z_1/Z_0, \ldots, Z_{n-m+1}/Z_0)$ однородный многочлен. Тогда $\tilde{g}_1(X_0, U_1^{(s+1)}, \ldots, U_{n-m}^{(s+1)}, X_{n-s}) = 0$ на W по доказанному выше. С другой стороны $\tilde{g}_1(\Omega) = \overline{g}(-c_1^{(s)}, \ldots, -c_{n-m}^{(s)}, 1) \neq 0$, и поэтому $\Omega \notin \pi_s(W)$.

Рассмотрим проекцию $\pi' : \mathbb{P}^{n-s} \longrightarrow \mathbb{P}^{n-s-1}$, заданную формулой $\pi'(U_0^{(s+1)} : \ldots : U_{n-s}^{(s+1)}) \longrightarrow (U_0^{(s+1)} : \ldots : U_{n-s-1}^{(s+1)})$. Очевидно $\pi' \circ \pi_s = \pi_{s+1}$. Поскольку Ω является центром проекции π' и $\Omega \notin \pi_s(W)$, то $\pi' : \pi_s(W) \longrightarrow \pi_{s+1}(W)$ – конечный морфизм (см. [3], [7]). Отсюда следует, что $\pi_{s+1} : W \longrightarrow \pi_{s+1}(W)$ – также конечный морфизм в силу $в^{(s)}$), что завершает доказательство $в^{(s+1)}$), и, следовательно, а) и в).

Теперь обратимся непосредственно к построению многочленов Ψ_i. Согласно только что приведенной конструкции, расширение

колец $F[U_1/U_0,\dots,U_{n-m}/U_0]\subset F[U_1/U_0,\dots,U_n/U_0]$ является целым (см. [3], [7]). Как при выборе K_{m+1} в § I, алгоритм выбирает семейство m-ок линейных форм $\{(S^{(\alpha)}_{n-m+1},\dots,S^{(\alpha)}_n)\}_{0\le\alpha\le(m-1)d_3^2}$ от переменных $X_0,\dots,X_n$ с коэффициентами из H, такое что линейная над F оболочка $\mathcal{L}\{S^{(\alpha)}_{n-m+1},\dots,S^{(\alpha)}_n\}=\mathcal{L}\{X_{n-m+1},\dots,X_n\}$ для всякого α и, кроме того, любые m форм $S^{(\alpha_1)}_n,\dots,S^{(\alpha_m)}_n$ при $0\le\alpha_1<\dots<\alpha_m\le(m-1)d_3^2$ линейно независимы над F.

Введем переменную Y алгебраически независимую над $F[\chi_1,\dots,\chi_{n-m}]$. Для произвольного $n-m+1\le j\le n-1$ и $0\le\alpha\le(m-1)\,d_3^2$ рассмотрим линейные формы $S^{(\alpha)}_n+YS^{(\alpha)}_j$. Алгоритм находит, решая систему линейных уравнений над H (ср. § 4 [4] и см. лемму 2.IO ниже) и неприводимый над F многочлен $\Psi^{(\alpha)}_j=\Psi^{(\alpha)}_j(Y,Z_1,\dots,Z_{n-m},Z)$, такой что $\Psi^{(\alpha)}_j(Y,\chi_1,\dots,\chi_{n-m},S^{(\alpha)}_n/X_0+YS^{(\alpha)}_j/X_0)=0$ на многообразии W. Имеем $deg_{Z_1,\dots,Z_{n-m},Z}(\Psi^{(\alpha)}_j)\le q^{\nu}deg\,W$ и, следовательно, $deg_Y\Psi^{(\alpha)}_j\le q^{\nu}deg\,W$ ввиду того, что $\Psi^{(\alpha)}_j(Y,\chi_1,\dots,\chi_{n-m},Z)=\prod_{\sigma}(Z-\sigma(S^{(\alpha)}_n/X_0)-Y\sigma(S^{(\alpha)}_j/X_0))$, где σ пробегает все вложения поля $K(\chi_1,\dots,\chi_{n-m},S^{(\alpha)}_n/X_0+YS^{(\alpha)}_j/X_0)$ в его алгебраическое замыкание, тождественные на $K(\chi_1,\dots,\chi_{n-m})$. Пусть $\Psi^{(\alpha)}_j(Y,Z_1,\dots,Z_{n-m},Z^{(1)}+YZ^{(2)})=\sum_{0\le i\le deg_Y\Psi^{(\alpha)}_j}\Psi^{(\alpha)}_{ji}\,Y^i$ и при этом $\Psi^{(\alpha)}_{ji}\in F[Z_1,\dots,Z_{n-m},Z^{(1)},Z^{(2)}]$. Обозначим через $\tilde\Psi^{(\alpha)}_{ji}(X_0,Z_1,\dots,Z_{n-m}Z^{(1)},Z^{(2)})=X_0^{deg\,\Psi^{(\alpha)}_{ji}}\Psi^{(\alpha)}_{ji}(Z_1/X_0,\dots,Z_{n-m}/X_0,Z^{(1)}/X_0,Z^{(2)}/X_0)$ однородный многочлен. Наша цель – доказать, что многообразие $\tilde W=\{\Psi^{(\alpha)}_{ji}(X_0,U_1,\dots,U_{n-m},S^{(\alpha)}_n,S^{(\alpha)}_j)=0;\ 0\le\alpha\le(m-1)\,d_3^2,\ n-m+1\le j\le n-1,\ 0\le i\le deg_Y\Psi^{(\alpha)}_j\le d_3d_5\}\subset\mathbb{P}^n(\bar F)$ совпадает с W. Включение $W\subset\tilde W$ следует из определения общей точки.

Перейдем теперь к доказательству обратного включения. Пусть точка $\Omega\in\tilde W$. Покажем сначала, что существует такой индекс $0\le i_0\le n-m$, что $\Omega\in\{U_{i_0}\ne0\}\subset\mathbb{P}^n$. Предположим противное и для любого α и $n-m+1\le j<n$ рассмотрим многочлен $\bar\Psi^{(\alpha)}_j(Y_0,Y_1,Z_0,\dots,Z_{n-m},Z)=Y_0^{deg_{Y,Z}(\Psi^{(\alpha)}_j)}\cdot Z^{deg_{Z_1,\dots,Z_{n-m},Z}(\Psi^{(\alpha)}_j)}\cdot\Psi^{(\alpha)}_j(Y_1/Y_0,Z_1/Z_0,\dots,Z_{n-m}/Z_0,Z/Y_0Z_0)$. Тогда $\bar\Psi^{(\alpha)}_j(Y_0,Y_1,U_0,\dots,U_{n-m},Y_0S^{(\alpha)}_n+Y_1S^{(\alpha)}_j)=0$ на W и, кроме того $0\ne\ell c_Z(\bar\Psi^{(\alpha)}_j(Y_0;Y_1,Z_0,\dots,Z_{n-m},Z))\in F$ принимая во внимание, что расширение колец $F[Y,\chi_1,\dots,\chi_{n-m}]\subset F[Y,\chi_1,\dots,\chi_{n-m},S^{(\alpha)}_n/X_0,S^{(\alpha)}_j/X_0]$

является целым согласно пункту в) из начала настоящего параграфа и то, что $\Psi_j^{(\alpha)}$ неприводим над F. Кроме того, $\overline{\Psi}_j^{(\alpha)}(0,1,Z_0,\dots,Z_{n-m},Z)=\widetilde{\Psi}_{j,\deg_Y(\Psi_j^{(\alpha)})}^{(\alpha)}(Z_0,\dots,Z_{n-m},0,Z)$ и $\overline{\Psi}_j^{(\alpha)}(1,0,Z_0,\dots,Z_{n-m},Z)=\widetilde{\Psi}_{j0}^{(\alpha)}(Z_0,\dots,Z_{n-m},Z,0)$ (заметим, что $\widetilde{\Psi}_{j\deg_Y(\Psi_j^{(\alpha)})}^{(\alpha)}$ (соответственно $\Psi_{j0}^{(\alpha)}$) в действительности не зависит от предпоследнего (соответственно последнего) аргумента). Поэтому $0\neq lc_Z\widetilde{\Psi}_{j,\deg_Y(\Psi_j^{(\alpha)})}(Z_0,\dots,Z_{n-m},0,Z),\ lc_Z\widetilde{\Psi}_{j0}^{(\alpha)}(Z_0,\dots,Z_{n-m},Z,0)\in F$. Отсюда следует, что $\Omega\in\{S_j^{(\alpha)}=0\}$ и $\Omega\in\{S_n^{(\alpha)}=0\}$, что приводит к противоречию, так как $n-m+1\leq j<n$ – произвольный индекс. Таким образом, требуемый индекс $0\leq i_0\leq n-m$ существует.

Наша ближайшая цель – доказать, что для любого $0\leq\alpha\leq(m-1)d_3^2$ и $n-m+1\leq j\leq n$ существует такая точка $\Omega_{ij}^{(\alpha)}\in W$, что $(U_i/U_{i_0})(\Omega_{ij}^{(\alpha)})=(U_i/U_{i_0})(\Omega)$ для любого $0\leq i\leq n-m$, кроме того $(S_j^{(\alpha)}/U_{i_0})(\Omega_{ij}^{(\alpha)})=(S_j^{(\alpha)}/U_{i_0})(\Omega)$ и $(S_n^{(\alpha)}/U_i)(\Omega_{ij}^{(\alpha)})=(S_n^{(\alpha)}/U_{i_0})(\Omega)$. Рассмотрим линейную проекцию $\widetilde{\pi}:\mathbb{P}^n(\overline{K})\to\mathbb{P}^{n-m+1}(\overline{K})$, заданную формулой $\widetilde{\pi}(U_0:\dots:U_n)=(U_0:\dots:U_{n-m}:S_n^{(\alpha)}+YS_j^{(\alpha)})$. Введем многообразие $W(\overline{K})\subset\mathbb{P}^n(\overline{K})$, полученное из W с помощью расширения поля F до поля $\overline{K}$; другими словами, многообразие $W(\overline{K})$ может быть определено той же самой системой уравнений, что и W. Аналогично введем многообразие $\widetilde{W}(\overline{K})\subset\mathbb{P}^n(\overline{K})$. На многообразии $W(\overline{K})$ (и, следовательно, на его образе $\widetilde{\pi}(W(\overline{K}))$) выполняется соотношение $\overline{\Psi}_j^{(\alpha)}(1,Y,U_0/U_{i_0},\dots,U_{n-m}/U_{i_0},S_n^{(\alpha)}/U_{i_0}+YS_j^{(\alpha)}/U_{i_0})=0$. Это соотношение также выполнено на $\widetilde{\pi}(\widetilde{W}(\overline{K}))$ по определению многочленов $\Psi_{ji}^{(\alpha)}$. Образ $\widetilde{\pi}(W(\overline{K}))\subset\mathbb{P}^{n-m+1}(\overline{K})$ является замкнутой гиперповерхностью, поскольку $\widetilde{\pi}$ – конечный морфизм в силу пункта в), и многообразие $\widetilde{\pi}(W(\overline{K}))$ определено над полем $K^{q-\infty}$.

Поэтому $\widetilde{\pi}(W(\overline{K}))=\{\Psi_j^{(\alpha)}(1,Y,U_0,\dots,U_{n-m},S_n^{(\alpha)}+YS_j^{(\alpha)})=0\}$, поскольку $\Psi_j^{(\alpha)}$ неприводим над K. Отсюда следует, что существует точка $\Omega_{ij}^{(\alpha)}\in W(\overline{K})$, для которой $\widetilde{\pi}(\Omega_{ij}^{(\alpha)})=\widetilde{\pi}(\Omega)$. В действительности $\Omega_{ij}^{(\alpha)}\in W$, так как $(U_0/U_{i_0})(\Omega_{ij}^{(\alpha)}),\dots,(U_{n-m}/U_{i_0})(\Omega_{ij}^{(\alpha)})\in\overline{F}$ и, следовательно, $(U_i/U_{i_0})(\Omega_{ij}^{(\alpha)})\in\overline{F}$ для всех $n-m+1\leq i\leq n$ согласно в) и а). Таким образом, $(S_i^{(\alpha)}/U_{i_0})(\Omega_{ij}^{(\alpha)})\in\overline{F}$ при $n-m+1\leq i\leq n$, откуда следуют равенства

$(U_i/U_{i_0})(\Omega_{ij}^{(\alpha)}) = (U_i/U_{i_0})(\Omega)$ для $0 \leqslant i \leqslant n-m$
и $(S_i^{(\alpha)}/U_{i_0})(\Omega_{ij}^{(\alpha)}) = (S_i^{(\alpha)}/U_{i_0})(\Omega)$ для $i=j$ и $i=n$.

Покажем теперь, что существует такое $0 \leqslant \alpha \leqslant (m-1)\,d_3^2$, что для любой пары различных точек $\Xi_1, \Xi_2 \in \pi^{-1}(\pi(\Omega)) \cap W$ выполняется неравенство $(S_n^{(\alpha_0)}/U_{i_0})(\Xi_1) \neq (S_n^{(\alpha_0)}/U_{i_0})(\Xi_2)$. Предполагая противное и учитывая, что $\operatorname{card}(\pi^{-1}(\pi(\Omega)) \cap W \leqslant \deg W \leqslant d_3$, мы заключаем по принципу Дирихле, что для некоторой пары точек $\Xi_1, \Xi_2 \in \pi^{-1}(\pi(\Omega)) \cap W$ выполняются равенства $(S_n^{(\alpha_j)}/U_{i_0})(\Xi_1) = (S_n^{(\alpha_j)}/U_{i_0})(\Xi_2)$ для подходящих $0 \leqslant \alpha_1 < \alpha_2 < \ldots < \alpha_m < (m-1)\,d_3^2$, $1 \leqslant j \leqslant m$ и, поэтому $\Xi_1 = \Xi_2$, вследствие выбора $S_n^{(\alpha)}$, что приводит к противоречию.

По доказанному выше $(S_n^{(\alpha_0)}/U_{i_0})(\Omega) = (S_n^{(\alpha_0)}/U_{i_0})(\Omega_{ij}^{(\alpha_0)})$ для любого $n-m+1 \leqslant j \leqslant n$. Отсюда следует, что $\Omega_{ij_1}^{(\alpha_0)} = \Omega_{ij_2}^{(\alpha_0)} = \Omega_i \in W$ не зависит от j_1, j_2. Поэтому мы получаем из доказанного выше, что $(U_i/U_{i_0})(\Omega_i) = (U_i/U_{i_0})(\Omega)$ для всех $0 \leqslant i \leqslant n-m$ и $(S_j^{(\alpha_0)}/U_{i_0})(\Omega_i) = (S_j^{(\alpha_0)}/U_{i_0})(\Omega)$ для $n-m+1 \leqslant j \leqslant n$, т.е. $\Omega = \Omega_i \in W$, что завершает доказательство равенства $W = \widetilde{W}$.

Для оценок в дальнейшем нам потребуется следующая лемма.

ЛЕММА 2.10. Пусть $\overline{U}_0, \ldots, \overline{U}_s$ – линейные формы от переменных $X_0, \ldots, X_n$ с коэффициентами из $H[Y]$ степени относительно Y не выше 1. Предположим (без ограничения общности), что $\overline{U}_0$ не обращается тождественно в нуль на $W(\bar{K})$, и что рациональные функции $\overline{U}_1/\overline{U}_0, \ldots, \overline{U}_s/\overline{U}_0$ алгебраически зависимы на $W(\bar{K})$ над полем K. Тогда существует такой многочлен $g(Z_1, \ldots, Z_s) \in H[Y, T_1, \ldots, T_\ell, \eta, Z_1, \ldots, Z_s]$, что $g(U_1/U_0, \ldots, U_s/U_0) = 0$ на $W(\bar{K})$, кроме того $\deg_{Z_1,\ldots,Z_s}(g) \leqslant d_3 d_s$ и степень $\deg_{T_1,\ldots,T_\ell,Y}(g)$ не превосходит некоторого полинома от d^m, d_1, d_2 первой степени от d_2 и, наконец, $\ell(g) \leqslant (M_1 + M_2 + (\ell+n-m)\ d_2)P_2(d^m d_1)$ для подходящего полинома P_2.

Отметим, что лемма остается справедливой, когда $\overline{U}_0, \ldots, \overline{U}_s$ –линейные формы с коэффициентами из $F[Y]$ (вместо $H[Y]$) с несколько более громоздкими оценками.

ДОКАЗАТЕЛЬСТВО. Мы можем предположить, что $\overline{U}_{s_1}/\overline{U}_0, \ldots, \overline{U}_s/\overline{U}_0$ – максимальная алгебраически независимая система рациональных функций на $W(\bar{K})$ среди $\overline{U}_1/\overline{U}_0, \ldots, \overline{U}_s/\overline{U}_0$ и, кроме того, что $\overline{U}_0, \ldots, \overline{U}_s$ линейно независимы над K. Дополним формы

$\overline{u}_0, \ldots, \overline{u}_s$ формами $\overline{u}_{s+1}, \ldots, \overline{u}_n$ с коэффициентами из H до базиса пространства линейных форм, так что $\overline{u}_{s_1}/\overline{u}_0, \ldots, \overline{u}_{s_2}/\overline{u}_0$ (где $s_1 \leq s \leq s_2$ и $s_2 - s_1 = n-m-1$) – базис трансцендентности поля функций на многообразии $W(\overline{K})$ над $\overline{K}$. Обозначим $\widetilde{u}_0 = \overline{u}_0$, $\widetilde{u}_1 = \overline{u}_{s_1}, \ldots, \widetilde{u}_{n-m} = \overline{u}_{s_2}$, $\widetilde{u}_{n-m+1} = \overline{u}_1, \ldots, \widetilde{u}_{s_2} = \overline{u}_{s_1-1}, \widetilde{u}_{s_2+1} = \overline{u}_{s_2+1}, \ldots \widetilde{u}_n = \overline{u}_n$.

Рассмотрим следующую систему, состоящую из m однородных уравнений от $X_0, \ldots, X_n$ с коэффициентами из поля $K(Y_1)$ аналогичную системе (3) § I: $h_1 - Y_1 \widetilde{u}_{n-m+1}^d = \ldots = h_m - Y_1 \widetilde{u}_n^d = 0$, определяющую многообразие $V \subset \mathbb{P}^n(\overline{K(Y_1)})$ (при этом роль Y из § I играет Y_1 алгебраически независимый над K). Из леммы 2.I § I следует, что все неприводимые над $K(Y_1)$ компоненты V_i многообразия $V = \bigcup V_i$ имеют одну и ту же размерность $n-m$, и, кроме того, $V \cap \{\widetilde{u}_0 = \ldots = \widetilde{u}_{n-m} = 0\} = \phi$.

Пусть $t_1', \ldots, t_{n-m}'$ алгебраически независимы над $K(Y_1)$. Для любого многочлена $f \in \overline{K(Y_1)}[X_0, \ldots, X_n]$ обозначим $\widetilde{f}(\widetilde{u}_0, \ldots, \widetilde{u}_n) = f(X_0, \ldots, X_n)$. Рассмотрим теперь систему

$$\begin{aligned} &\widetilde{h}_1(\widetilde{u}_0, t_1'\widetilde{u}_0, \ldots, t_{n-m}'\widetilde{u}_0, \widetilde{u}_{n-m+1}, \ldots, \widetilde{u}_n) - Y_1 \widetilde{u}_{n-m+1}^d = 0 \\ &\widetilde{h}_m(\widetilde{u}_0, t_1'\widetilde{u}_0, \ldots, t_{n-m}'\widetilde{u}_0 u_{n-m+1}, \ldots, \widetilde{u}_n) - Y_1 \widetilde{u}_n^d = 0 \end{aligned} \qquad (7)$$

однородных относительно $\widetilde{u}_0, \widetilde{u}_{n-m+1}, \ldots, \widetilde{u}_n$ уравнений над полем $K_1 = K(Y_1, t_1', \ldots, t_{n-m}')$. В силу леммы 2.I из § I система (7) обладает конечным числом решений в $\mathbb{P}^m(\overline{K_1})$.

Аналогично доказательству леммы 2.6 § I, алгоритм применяет теорему 2.3 [4] к системе (7) и находит для каждого класса ее корней, сопряженных над полем K_1 некоторый неприводимый над F многочлен $\Phi(Y, Y_1, t_1', \ldots, t_{n-m}', Z) \in F[Y, Y_1, t_1', \ldots, t_{n-m}', Z]$. Классы сопряженных корней биективно соответствуют компонентам V_i многообразия V согласно лемме 2.5 [4]. Из леммы 2.3 § I следует, что многообразие $\operatorname{con} W(\overline{K}) \subset A^{n+1}(\overline{K})$ является компонентой многообразия $\widetilde{V}_0 \cap \{Y_1 = 0\}$ для подходящей (не обязательно единственной) компоненты $\widetilde{V}_0 \subset A^{n+2}(\overline{K})$ многообразия $\widetilde{V} = \{h_1 - Y_1 \widetilde{u}_{n-m+1}^d = \ldots = h_m - Y_1 \widetilde{u}_n^d = 0\}$ (напомним, что по лемме 2.2 § I существует биективное соответствие между компонентами V_i многообразия V и компонентами $\widetilde{V}_i$ многообразия $\widetilde{V}$, которые не содержатся в объединении конечного числа гиперплоскостей $\{Y_1 = c\}$.

Применяя [I8] к системе (7), мы получаем многочлен $R(\widetilde{u}_0, \widetilde{u}_{n-m+1}, \ldots, \widetilde{u}_n) \in F[t_1', \ldots, t_{n-m}', Y, Y_1, \widetilde{u}_0, \widetilde{u}_{n-m+1}, \ldots, \widetilde{u}_n]$

(без ограничения общности мы можем предполагать, что $Y_1 \nmid R$). Рассмотрим многочлен $\Psi(t'_1,\dots,t'_{n-m},Y,Y_1,Z)=R(Z,-1,0,\dots,0)$. Тогда однородный относительно $\tilde{u}_0,\tilde{u}_1,\dots,\tilde{u}_{n-m+1}$ многочлен $\Psi_1(Y_1,Y,\tilde{u}_0,\tilde{u}_1,\dots,\tilde{u}_{n-m+1})=\tilde{u}_0^{\deg_{t_1,\dots,t_{n-m},Z}(\Psi)}\psi(\tilde{u}_1/\tilde{u}_0,\dots,\tilde{u}_{n-m}/\tilde{u}_0,Y_2,Y,\tilde{u}_{n-m+1}/\tilde{u}_0)$ (мы будем предполагать, что этот многочлен не делится на Y_2 , деля его в противном случае на максимально возможную степень Y_2) обращается в нуль тождественно на многообразии $\bigcup_i \tilde{V}_i$, принимая во внимание, что Ψ_1 обращается в нуль в общей точке всякой компоненты V_i , которая может быть получена из решений системы (7), основываясь на лемме 2.5 [4]. Следовательно, ненулевой многочлен $g_1=\Psi_1(0,Y,\tilde{u}_0,\tilde{u}_1,\dots,\tilde{u}_{n-m+1})$ обращается в нуль тождественно на многообразии $\tilde{V}\cap\{Y_1=0\}\supset W$.

Покажем теперь, что неприводимый над F множитель $g\mid g_1$ такой, что $g(Y,\tilde{u}_0,\dots,\tilde{u}_{n-m+1})$ обращается в нуль тождественно на W удовлетворяет оценкам из формулировки леммы. (В действительности g зависит только от переменных $Y,\tilde{u}_0,\tilde{u}_1,\dots,\tilde{u}_{s-s_1+1},\tilde{u}_{n-m+1}$). Из [18] и теоремы 2.3 [4] следует, что $\deg_{\tilde{u}_0,\tilde{u}_1,\dots,\tilde{u}_{n-m+1}}(g)\leqslant d_3 d_5$. Кроме того $\deg_{T_1,\dots,T_\ell,Y}(g)$ может быть ограничена сверху (опять по теореме 2.3 [4]) некоторым полиномом от d^m, d_1, d_2 , поэтому полиномом от d^m, d_1, d_2 (причем d_2 входит в оба эти полинома в первой степени) могут быть также ограничены сверху степени $\deg_{T_1,\dots,T_\ell,Y}(g)$. Наконец, оценка на длину записи $l(g)$ также получается из теоремы 2.3[4] (ср. §1), что завершает доказательство леммы.

Обратимся теперь к оценке времени работы алгоритма. Для построения π алгоритм на каждом шагу находит многочлен g (который дает соотношение алгебраической зависимости между координатами).

Именно, алгоритм подставляет выражения для $(X_j/X_0)^{q^\nu}\in F(t_1,\dots,t_{n-m})[\theta]$ в многочлен g^{q^ν} , коэффициенты которого из H при мономах от $T_1,\dots,T_\ell,\eta,Z_1,\dots,Z_{n-m+1}$ рассматриваются как неизвестные системы линейных уравнений над H , получающейся приравниванием g^{q^ν} с подставленными выражениями к нулю. Затем алгоритм решает эту систему. Число переменных в системе меньше, чем $d_3^{n-m+2}(\deg_{T_1,\dots,T_\ell} g^{q^\nu})^\ell d_1$ (определения d_1, M_1 см. во введении). Число уравнений может быть ограничено сверху некоторым полиномом от $(\deg_{T_1,\dots,T_\ell}(g^{q^\nu})+d_3 d_4)^\ell$, $d_1(d_3 d_4)^{n-m+1}$. Длины записей коэффициентов из H системы не превосходят $(M_1+M_3+(\ell+n-m)\ d_4)P_3(d_1,d_3)$ для некоторого полинома

P_3 , принимая во внимание $c^{(s)}$) . Следовательно, алгоритм может решить систему за полиномиальное от $M_1, M_3, d_1, (\deg_{\tau_1,\dots,\tau_\ell} q^{q^\gamma})^{\gamma}, (d_3 d_4)^{n-m+\ell+1}$ время и, значит, в полиномиальное от $M_1, M_2, (d^m d_1 d_2)^{n-m+\ell+1}$ время в систему леммы 2.10. Поэтому проекция π , т.е. линейные формы $u_0, \dots, u_n$ могут быть найдены в полиномиальное от тех же самых величин время.

Построение многочленов $\tilde{\psi}_{ji}^{(\alpha)}$, задающих многообразие W , начинается с выбора семейства, состоящего из $((m-1)d_3^2 + 1)$ наборов линейных форм $(S_{n-m+1}^{(\alpha)}, \dots, S_n^{(\alpha)})$. После этого алгоритм находит многочлены $\psi_j^{(\alpha)}$. Из леммы 2.10 следует, что степени $\deg_{\tau_1,\dots,\tau_\ell, Y}(\psi_j^{(\alpha)})$ не больше некоторого полинома от d^m, d_1, d_2 первой степени от d_2 . Аналогично приведенным выше оценкам на время построения многочленов g (при построении π), мы можем ограничить время работы алгоритма при нахождении $\psi_j^{(\alpha)}$ подходящим полиномом от $M_1, M_3, (\deg_{\tau_1,\dots,\tau_\ell, Y} \psi_j^{(\alpha)})^{\ell+1}, (d_3 d_4)^{n-m+\ell+1}, d_1$. Наконец, алгоритм строит многочлены $\tilde{\psi}_{ji}^{(\alpha)}$ в полиномиальное от тех же самых величин время, т.е. в полиномиальное от $M_1, M_2 (d^m d_1 d_2)^{n-m+\ell+1}$ время.

Подытожим результаты настоящего параграфа в следующей теореме.

ТЕОРЕМА 2.2. Пусть компонента W многообразия $\{h_1 = \dots = h_m = 0\}$ удовлетворяет оценкам, сформулированным в начале настоящего параграфа. Предлагается алгоритм, который строит семейство многочленов $\overline{\psi}_1, \dots, \overline{\psi}_N \in F[Z_0, \dots, Z_{n-m+2}]$ и линейные формы $u_{ij} = \sum_{0 \le \beta \le n} c_{ij}^{(\beta)} X_\beta$ для $1 \le i \le N \le m^2 d_3^3 d_5 \le m^2 d^{4m}$, $0 \le j \le n-m+2$, $c_{ij}^{(\beta)} \in H$, длина записи $\ell(c_{ij}^{(\beta)}) \le m \log(m d_3 + 1) \le m \log(m d^m + 1)$, таких что $W = \{\psi_1 = \dots = \psi_N = 0\}$, где $\psi_i = \overline{\psi}_i(u_{i0}, \dots, u_{in-m+2})$. При этом $\deg_{Z_0,\dots,Z_{n-m+2}}(\overline{\psi}_i) \le d_3 d_5 \le d^{2m}$ и $\deg_{\tau_1,\dots,\tau_\ell}(\psi_i)$ не превосходит некоторого полинома от d^m, d_1, d_2 первой степени относительно d_2 . Длина записи $\ell(\overline{\psi}_i)$ коэффициентов из H многочлена $\overline{\psi}_i$ не превосходит $(M_1 + M_2 + (\ell + n - m)\ d_2) P_2(d^m, d_1)$. Наконец, время работы алгоритма при построении $\overline{\psi}_i$, u_{ij} ограничено некоторым многочленом от $(d^m d_1 d_2)^{n-m+\ell+1}$.

Используя эту теорему, можно модифицировать некоторым образом алгоритм из § I и улучшить там оценки на время работы. Именно, для построения многочленов $\psi_i^{(w)}$ в конце § I модифицированный алгоритм использует конструкцию из теоремы 2.2.

СЛЕДСТВИЕ. Можно модифицировать алгоритм из § I, так что новый алгоритм для всякой компоненты W_v коразмерности m строит ее общую точку с теми же самыми оценками на параметры, что и в теореме 2.I § I, причем степени $deg_{\tau_1,\dots,\tau_\ell,t_1,\dots,t_{n-m}}(\Phi_v)$, $deg_{\tau_1,\dots,\tau_\ell,t_1,\dots,t_{n-m}}(X_j/X_{j_0})^{q^{d_1}}$ оцениваются некоторым полиномом от d^m, d_1, d_2 первой степени относительно d_2 и, кроме того, семейство многочленов $\{\psi_i^{(v)}\}_{1\le i\le N\le m^2d^m}$, для которого выполняется равенство $W_v=\{\psi_1^{(v)}=\dots=\psi_N^{(v)}=0\}$, и всякий многочлен $\psi_i^{(v)}=\bar\psi_i^{(v)}(U_{j_0}^{(v)},\dots,U_{j_{n-m+\ell+2}}^{(v)})$ имеет такой же вид как в теореме 2.2 и с теми же самыми оценками на параметры как в теореме 2.2 (причем можно выразить $\psi_i^{(v)}$ явно через $X_0,\dots,X_n$ не изменяя оценку на время работы, но увеличив оценки на длину записи многочленов – см. замечание ниже). Наконец, модифицированный алгоритм работает в полиномиальное время от $M_1,M_2,(d^md_1d_2)^{n+\ell}$, q. Более того, время работы модифицированного алгоритма при построении W_v может быть ограничено многочленом от $M_1,M_2,(d^md_1d_2)^{n-m+\ell+1}$, q и от длины записи многочленов $\psi_i^{(v_1)}$ (в форме теоремы 2.2) для листьев первого типа уровня $s<m$ (см. начало § I), при условии, что у нас имеются многообразия W_{v_2} для всех вершин v_2 уровня $m-1$ и многочлены $\psi_i^{(v_1)}$ для всех листьев v_1 первого типа уровня меньше m. Из теоремы 2.2 следует, что длины записей многочленов $\psi_i^{(v_1)}$ не больше, чем $(M_1+M_2+(\ell+n-s)\ d_2)P_2(d^sd_1)$. Мы используем последние наблюдения в следующем параграфе.

ЗАМЕЧАНИЕ. Многочлены ψ_i в теореме 2.2 (соответственно $\psi_i^{(v)}$ в следствии) представлены не совсем явно. Именно, как композиция явно заданных многочленов и линейных форм. Несложно проверить, что длины записей многочленов в форме принятой в настоящей работе (см. введение) превосходят полученные границы, тем не менее, явное представление этих многочленов может быть получено в рамках указанных границ на время работы алгоритма. Было бы интересно построить семейство многочленов, определяющих заданную компоненту, длина записи которых меньше установленных оценок в теореме 2.2 на время работы.

§ 3. Улучшенный метод нахождения компонент многообразия

Снова мы используем обозначения из § I.

Цель настоящего параграфа состоит в описании некоторого алгоритма, который для всякой компоненты многообразия $\{f_0=\dots=f_{k-1}=0\}$ находит ее общую точку и задающую ее систему урав-

нений (ср. §§ I, 2). Однако, в отличие от §§ I, 2 предлагаемый алгоритм строит не все дерево компонент, и алгоритм имеет лучшие оценки на время работы, чем в § I, когда $\dim\{f_0=\ldots=f_{k-1}=0\}$ мала.

Сначала изложим вспомогательный алгоритм для нахождения общих точек всех неприводимых над F компонент старшей размерности многообразия $W=\{g_0=\ldots=g_{s-1}=0\}\subset\mathbb{P}^n(\bar{F})$, где $g_i\in F[X_0,\ldots,X_n]$ – однородные многочлены. Этот вспомогательный алгоритм будет строить также системы уравнений, задающие компоненты старшей размерности. Пусть $\deg g_i=d$. Алгоритм полагает последовательно $\bar{m}=-1,0,1,\ldots$. Зафиксируем $\bar{m}$. Основываясь на лемме 2.3 из [4], алгоритм выбирает семейство $\mathcal{M}=\mathcal{M}_{n,\bar{m},d^n}$, состоящее из $(\bar{m}+1)$-ок линейных форм от переменных $X_0,\ldots,X_n$ с коэффициентами из H, причем $\operatorname{card}(\mathcal{M})\le(3nd^n)^{(\bar{m}+1)}$, удовлетворяющее следующему свойству. Если $\dim W=\bar{m}$, то существует такой элемент $(Y_0,\ldots,Y_{\bar{m}})\in\mathcal{M}$, что $W\cap\{Y_0=\ldots=Y_{\bar{m}}=0\}\neq\emptyset$.

Предположим, что неравенство $\dim W\ge\bar{m}$ уже установлено. Тогда равенство $\dim W=\bar{m}$ эквивалентно тому, что для подходящего $(Y_0,\ldots,Y_{\bar{m}})\in\mathcal{M}$ выполняется $\dim(W\cap\{Y_1=\ldots=Y_{\bar{m}}=0\})=0$ и для всякой точки $\Omega\in W\cap\{Y_1=\ldots=Y_m=0\}$ справедливо $Y_0(\Omega)\neq 0$. Выполнение последнего условия алгоритм проверяет, используя следствие в § 2. Пусть $\dim W=\bar{m}$ и $W\cap\{Y_0=\ldots=Y_m=0\}=\emptyset$. Как и в §§ I, 2 дополним $Y_0,\ldots,Y_{\bar{m}}$ до базиса $Y_0,\ldots,Y_n$ пространства линейных форм, обозначим $\bar{g}_i(Y_0,\ldots,Y_n)=g_i(X_0,\ldots,X_n)$ и рассмотрим систему $g_i(Y_0,t_1Y_0,\ldots,t_{\bar{m}}Y_0,Y_{\bar{m}+1},\ldots,Y_n)=0,\ 0\le i\le s-1$ однородных уравнений от $Y_0,Y_{\bar{m}+1},\ldots,Y_n$ над полем $F'=F(t_1,\ldots,t_{\bar{m}})$, где $t_1,\ldots,t_{\bar{m}}$ трансцендентны над F. Эта система обладает конечным числом решений. . Применяя § 2 гл2 [4] к системе, алгоритм находит общие точки всех компонент старшей размерности $\bar{m}$, которые биективно соответствуют классам сопряженных над F корней системы согласно лемме 2.5 [4] и замечанию после нее.

Применим только что описанный вспомогательный алгоритм к многообразию $\{f_0=\ldots=f_{k-1}=0\}$, пусть его размерность равна $n-m$, и найдем общие точки всех его компонент старшей размерности $n-m$. После этого при помощи теоремы 2.2 алгоритм строит для каждой компоненты старшей размерности систему задающих ее уравнений. Далее, алгоритм возвращается назад от координат $\{Y_i\}$ к координатам $\{X_i\}$, используя лемму 2.I0 § 2 для получения оценок на степени.

12.1679

Наша ближайшая цель – построить такие линейные комбинации $h_i = \sum_{0 \le j \le K-1} \alpha_j^{(i)} f_j$, $1 \le i \le m$, что $\alpha_j^{(i)} \in H$ и всякая компонента многообразия $\{h_1 = \ldots = h_m = 0\}$ имеет размерность $n-m$ (многочлены $h_1, \ldots, h_m$ имеют смысл аналогичный многочленам h_i из §§ I,2).

Пусть $W = \{g_0 = \ldots = g_{s-1} = 0\} = \bigcup_i W_i$ – разложение W на неприводимые компоненты. Мы будем говорить, что g_j **существенен** в семействе $g_0, \ldots, g_{s-1}$ для компоненты W_i, если W_i является также компонентой многообразия $\{g_0 = \ldots = g_{j-1} = g_{j+1} = \ldots = g_{s-1} = 0\}$. Обозначим $\dim W = n-m$, $\deg(g_i) = d$.

ЛЕММА 2.II. Пусть g_0 существенен для компонент $W_1, \ldots, W_\alpha$ и g_1 существенен для компоненты $W_{\alpha+1}$ в семействе $g_0, \ldots, g_{s-1}$, причем $\dim W_i = n-m$, $1 \le i \le \alpha+1$, и многочлены $g_0, \ldots, g_{s-1}$ имеют одинаковую степень. Тогда по крайней мере для одного элемента β_j из произвольного множества попарно различных элементов $\beta_0, \ldots, \beta_\delta \in F$, где $\delta = d^{m-1}$ многочлен g_0 существенен в семействе $g_0, g_1 + \beta_j g_0, g_2, \ldots, g_{s-1}$ для каждой из компонент $W_1, \ldots, W_\alpha, W_{\alpha+1}$.

ДОКАЗАТЕЛЬСТВО. Предположим противное, тогда для любого $0 \le j \le \delta$ существует такая компонента $W_{i(j)}$, $1 \le i(j) \le \alpha+1$, что $W_{i(j)}$ содержит собственным образом некоторую компоненту $V_{\gamma(j)}$ многообразия $\{g_1 + \beta_j g_0 = g_2 = \ldots = g_{s-1} = 0\}$. Из условия леммы следует, что $\dim V_{\gamma(j)} = \dim W_{i(j)} = n-m+1$, и что $V_{\gamma(j)}$ является также компонентой многообразия $\{g_2 = \ldots = g_{s-1} = 0\}$. В силу принципа Дирихле существуют по крайней мере два индекса $0 \le j_1 < j_2 \le \delta$ такие, что $\gamma(j_1) = \gamma(j_2)$, и, следовательно, g_0 и g_1 обращаются одновременно в нуль тождественно на $V_{\gamma(j_1)}$, т.е. $W \supset V_{\gamma(j_1)} \supsetneq W_{i(j_1)}$. Это приводит к противоречию и завершает доказательство леммы.

Опишем теперь алгоритм, выясняющий, является ли многочлен несущественным в семействе $g_0, \ldots, g_{s-1}$ для компоненты W_i старшей размерности $n-m$ многообразия W (общие точки и системы определяющих уравнений для компонент старшей размерности могут быть найдены, используя вспомогательный алгоритм, изложенный в начале этого параграфа). Именно, алгоритм находит общие точки и определяющие системы уравнений для всех компонент V_{i_1} старшей размерности $n-m+1$ многообразия $\{g_0 = \ldots = g_{j-1} = g_{j+1} = \ldots = g_{s-1} = 0\}$ (если размерность этого многообразия равна $n-m+1$) и для каждого V_{i_1} алгоритм проверяет, выполняется ли включение $W_i \subset V_{i_1}$ с помощью подстановки общей точки. Многочлен g_j существенен в семействе $g_0, \ldots, g_{s-1}$ для ком-

поненты W_i в том и только в том случае, если не существует такой компоненты V_{i_1}, что $W_i \subset V_{i_1}$. В случае, когда $\dim\{g_0 = \ldots = g_{j-1} = g_{j+1} = \ldots = g_{s-1} = 0\} = n-m$, последнее условие, очевидно, выполняется.

Пусть $k > m$. Используя только что описанный алгоритм и лемму 2.II, алгоритм строит последовательность $\omega_1, \ldots, \omega_{k-1} \in H$ такую, что f_0 несущественен в семействе $f_0, f_1 + \omega_1 f_0, \ldots f_{k-1} + \omega_{k-1} t_0$ для всех компонент W_i размерности $n-m$ многообразия $\{f_0 = \ldots = f_{k-1} = 0\}$, при этом $0 \leq \omega_i < d^{m-1}$ и $\omega_i \in \mathbb{Z}$, когда $H = \mathbb{Q}$, или $card(H) > d^{m-1}$ в случае $q = char(H) > 0$. Алгоритм обязательно находит $\omega_1, \ldots, \omega_{k-1}$, учитывая, что для любой компоненты W_i существует такой индекс $0 \leq j \leq k-1$, что f_j несущественен в семействе $f_0, \ldots, f_{k-1}$ для W_i. Таким образом, $\dim\{f_1 + \omega_1 f_0 = \ldots = f_{k-1} + \omega_{k-1} f_0 = 0\} = n-m$ и, очевидно, всякая компонента W_i старшей размерности $n-m$ одновременно является компонентой многообразия $\{f_1 + \omega_1 f_0 = \ldots = f_{k-1} + \omega_{k-1} f_0 = 0\}$. Мы уменьшили число уравнений исходной системы на I. Продолжая таким же образом, алгоритм найдет требуемые многочлены $h_1, \ldots, h_m$. Несложно показать, что длина записи $l(x_j^{(\omega)})$ может быть ограничена сверху полиномом от k, $\log d$ (напомним, см. Введение, что $k \leq \binom{d+n}{n} < (d+1)^n$).

Отметим, что множество всех компонент W_v построенного многообразия $\{h_1 = \ldots = h_m = 0\}$ совпадает с множеством всех компонент уровня m в дереве компонент системы $f_0 = \ldots = f_{k-1} = 0$ при условии, что построенные $h_1, \ldots, h_m$ рассматриваются как многочлены с теми же самыми обозначениями из конструкции дерева компонент (см. § I). Мы применяем модифицированный алгоритм из следствия к теореме 2.2 § 2, начиная с компонент W_v и рассматривая их как компоненты, соответствующие построенным вершинам v уровня m дерева компонент. В результате, алгоритм строит все вершины дерева компонент уровня не меньше m и, следовательно, все компоненты многообразия $\{f_0 = \ldots = f_{k-1} = 0\}$.

Время работы вспомогательного алгоритма по вычислению $\dim\{f_0 = \ldots = f_{k-1} = 0\}$ и компонент старшей размерности, а также время работы алгоритма по построению $h_1, \ldots, h_m$ можно оценить с помощью теоремы 2.2 § 2. Оценка времени работы последнего этапа алгоритма может быть получена с помощью следствия к теореме 2.2 § 2.

Обозначим $\dim\{f_0 = \ldots = f_{k-1} = 0\} = c-1$; подытожим результаты настоящего параграфа в следующей теореме, завершающей доказательство пункта а) основной теоремы главы II (см. вве-

дение).

ТЕОРЕМА 2.3. Предлагается алгоритм, который в условиях теоремы 2.I для всякой компоненты W_v коразмерности m (очевидно $m \geqslant n-c+1$) строит ее общую точку в том же самом виде и с теми же самыми оценками на параметры, что и в теореме 2.I и, кроме того, систему уравнений, задающих W_v, в том же самом виде и с теми же самыми оценками на параметры, что и в теореме 2.2. Алгоритм работает в полиномиальное от $M_1, M_2, (d^n d_1 d_2)^{c+1}$ и q время.

ЗАМЕЧАНИЕ I. Алгоритмы из §§ I, 2 строят по ходу своей работы указанное в соответствующих теоремах семейство, состоящее из $n+1$ многочленов $h_1, \ldots, h_{n+1} \in F[X_0, \ldots, X_n]$, которые являются некоторыми линейными комбинациями $f_0, \ldots, f_{k-1}$ с коэффициентами из H и, таких что $\{f_0 = \ldots = f_{k-1} = 0\} = \{h_1 = \ldots = h_{n+1} = 0\}$.

ЗАМЕЧАНИЕ 2. Полученные результаты позволяют раскладывать квазипроективные многообразия на неприводимые компоненты с той же оценкой времени, что и в основной теореме. Именно, пусть $W = \{f_0 = \ldots = f_{k-1} = 0, g_0 \neq 0, \ldots, g_{s-1} \neq 0\}$, где $f_0, f_1, \ldots, f_{k-1}, g_0, \ldots, g_{s-1}$ – однородные многочлены. Сначала надо разложить многообразие $W' = \{f_0 = \ldots = f_{k-1} = 0\} = \bigcup W_i$ на неприводимые компоненты, затем, подставив общую точку, проверяем для каждого i, обращаются ли в нуль тождественно полиномы $g_0, \ldots, g_{s-1}$ на W_i. Если ни один из них не обращается в нуль тождественно на W_i, то неприводимое квазипроективное многообразие $W_i \cap \{g_0 \neq 0, \ldots, g_{s-1} \neq 0\} \neq \phi$ является компонентной многообразия W, и этими компонентами исчерпываются все компоненты многообразия W.

В частности, если нам дана система не обязательно однородных уравнений $\overline{f}_0 = \ldots = \overline{f}_{k-1} = 0$, где $\overline{f}_0, \ldots, \overline{f}_{k-1} \in F[X_1, \ldots, X_n]$, тогда стандартным образом (см. введение) ей соответствует система однородных уравнений $f_0 = \ldots = f_{k-1} = 0$, где $f_0, \ldots, f_{k-1} \in F[X_0, \ldots, X_n]$. Решение исходной системы эквивалентно нахождению компонент квазипроективного многообразия $\{f_0 = \ldots = f_{k-1} = 0, X_0 \neq 0\}$, т.е. выделению компонент проективного многообразия $\{f_0 = \ldots = f_{k-1} = 0\}$, которые не лежат на бесконечности.

ЗАМЕЧАНИЕ 3. Основная теорема дает также возможность выяснить, содержится ли одно из данных квазипроективных многообразий в другом.

§ 4. Разложение многообразия на абсолютно неприводимые компоненты и построение поля определения

Пусть нам дана общая точка неприводимого над F многообразия W (см. начало § 2) и семейство однородных многочленов $\psi_1, \dots, \psi_N \in F[X_0, \dots, X_n]$, таких что $W = \{\psi_1 = \dots = \psi_N = 0\}$ и пусть, кроме того, W является компонентой многообразия $\{h_1 = \dots = h_m = 0\}$ и выполняются те же самые оценки на параметры общей точки, что и в начале § 2, и те же самые оценки на параметры $\psi_1, \dots, \psi_N$, что и в теореме 2.2 § 2. Используя конструкцию из § 2, можно построить линейную проекцию $\pi : \mathbb{P}^n \to \mathbb{P}^{n-m}$, где $\pi(X_0 : \dots : X_n) = (U_0 : \dots : U_{n-m})$, которая определена всюду на W и, следовательно, $W \cap \{U_0 = \dots = U_{n-m} = 0\} = \phi$. Следовательно, делая линейную замену координат, основываясь на конструкции перехода от координат $\{Y_i\}$ к $\{X_i\}$ (см. §§ 2, 3) и изменяя обозначения координат, мы можем считать без ограничения общности, что $W \cap \{X_0 = \dots = X_{n-m} = 0\} = \phi$ (ср. §§ 1, 3).

В конце работы алгоритма мы можем опять, основываясь на все той же конструкции, вернуться к старым координатам.

Наша цель состоит в нахождении абсолютно неприводимых компонент W_i многообразия $W = \bigcup_i W_i$. Обозначим через $F^{(i)}$ минимальное поле определения компоненты W, содержащее F.

Различные компоненты W_i (а также поля $F^{(i)}$) попарно сопряжены относительно действия группы Галуа $Gal(\bar{F}/F)$. Поэтому достаточно построить поле $F^{(1)}$ и компоненту W_1.

Мы будем предполагать для удобства, что $\Phi(t_1, \dots, t_{n-m}, Z) \in F[t_1, \dots, t_{n-m}, Z]$, т.е. не обязательно выполнено $\ell_Z(\Phi) = 1$.

Разложим $\Phi(t_1, \dots, t_{n-m}, Z) = \varepsilon \prod_i \Phi_i$ на абсолютно неприводимые множители над $\bar{F}$, используя § 3 главы I. Мы будем предполагать, что Φ_1 попарно сопряжены над F, $\varepsilon \in F$ и что некоторый коэффициент каждого Φ_i равен 1 (при мономе от $t_1, \dots, t_{n-m}, Z$), последнее является условием нормировки. Обозначим через $F_s^{(i)}$ поле, порожденное над F коэффициентами многочлена Φ_i. Тогда $F \subset F_s^{(i)}$ – конечное сепарабельное расширение (см. § 3 главы I).

Применим теперь лемму 2.5 [4] к случаю $F_1 = F_s^{(1)}$. Из нее следует, что паре из пункта c) леммы, содержащей как первый член класс (он здесь единственный) сопряженных на полем

$F' = F(t_1,\dots,t_{n-m})$ корней системы

$0=\psi_1(X_0,t_1X_0,\dots,t_{n-m}X_0,X_{n-m+1},\dots,X_n)=\dots=\psi_N(X_0,t_1X_0,\dots,t_{n-m}X_0,X_{n-m+1},\dots,X_n)$

и как второй член – многочлен Φ_1, соответствует неприводимая над полем $F_s^{(1)}$ компонента W_1 многообразия W по пункту в) леммы. Проводя аналогичное рассуждение в случае $F_1=\overline{F}$, мы получаем, что W_1 – абсолютно неприводимая компонента многообразия W. Более того, W_1 определена над полем $(F_s^{(1)})^{q^{-\infty}}$. Наконец, общая точка многообразия W_1 согласно лемме 2.5[4] может быть задана следующим изоморфизмом полей: $\overline{F}(W_1)\supset F_s^{(1)}(X_1/X_0,\dots,X_{n-m}/X_0,(X_{n-m+1}/X_0)^{q^\nu},\dots,(X_n/X_0)^{q^\nu})\simeq F_s^{(1)}(t_1,\dots,t_{n-m})[\theta_{W_1}]\simeq F_s^{(1)}(t_1,\dots,t_{n-m})[Z]/(\Phi_1(Z))$, при котором $X_i/X_0\mapsto t_i$, $1\le i\le n-m$, кроме того, $\Phi_1(\theta_{W_1})=0$ и выражения для $(X_j/X_0)^{q^\nu}$ через θ_{W_1} для $n-m+1\le j\le n$ получены при помощи подстановки θ_{W_1} вместо θ_W в выражения для $(X_j/X_0)^{q^\nu}$ из общей точки из начала этого параграфа.

Покажем теперь, что $F_s^{(1)}$ – максимальное сепарабельное над F подполе поля $F^{(1)}$. Принимая во внимание, что W_1 определено над полем $F^{(1)}$, а коэффициенты линейных функций $L_1=X_1/X_0,\dots,L_{n-m}=X_{n-m}/X_0, L_{n-m+1}=\sum_{n-m+1\le i\le n}\gamma_i(X_i/X_0)$ (на аффинном многообразии $\{X_0\neq 0\}$) имеют коэффициенты из $H\subset F^{(1)}$, заключаем, что $\Phi_1(L_1,\dots,L_{n+m+1})=0$ на $W_1\cap\{X_0\neq 0\}\subset\mathbb{A}^{N'}(\overline{F^{(1)}})$ для подходящего Φ_1 неприводимого и единственного с точностью до константы. Отсюда следует, что $\Phi_1\in F^{(1)}[t_1,\dots,t_{n-m},Z]$, если один из коэффициентов многочлена Φ_1 равен 1, следовательно, $F_s^{(1)}\subset F^{(1)}$. С другой стороны, очевидно $F^{(1)}\subset(F_s^{(1)})^{q^{-\infty}}$, что доказывает требуемое утверждение.

Для построения системы уравнений, определяющих W_1, алгоритм применяет теорему 2.2 § 2 над полем $F^{(1)}$. При переходе от поля F к полю $F^{(1)}$ алгоритм должен представлять поле $F^{(1)}$ в виде $F^{(1)}=H(T_1,\dots,T_\ell)[\eta_1]$, где η_1 – сепарабельный алгебраический элемент над полем $H(T_1,\dots,T_\ell)$ и найти его минимальный многочлен φ_1 над этим полем. Основываясь на изложенном в § 3 главы I, можно выбрать η_1, так что $deg_{T,T_1,\dots,T_\ell}(\varphi_1)$ не превосходит некоторого полинома от d^m, d_1, d_2 первой степени относительно d_2 и длина записи $l(\varphi_1)$ не превосходит $(M_1+M_2+(n+\ell)\ d_2)P_3(d^m,d_1)$. Поэтому параметры общей точки компоненты W_1 ограничены сверху подходящим полиномом от $M_1+M_2, d^m, d_1, d_2, n+\ell$. Из теоремы 2.2 § 2 следует, что верхние границы на параметры определяющей системы урав-

нений будут полиномами от тех же самых величин. Общее время работы алгоритма будет не больше, чем некоторый полином от $M_1, M_2, (d^m d_1 d_2)^{n-m+\ell+1}$, q , если учесть, что абсолютное разложение из § 3 главы I требует полиномиального времени, а так же учитывая приведенную в теореме 2.2 § 2 верхнюю границу на время работы алгоритма по построению системы уравнений. Это завершает доказательство пункта в) основной теоремы из введения.

На протяжении работы алгоритма из пункта а) основной теоремы поле $H = H_0$ возможно неоднократно расширялось в случае, когда H – конечное поле. Обозначим через $H_1 \supset H_0$ получившееся в результате осуществления алгоритма конечное поле H . Наша цель вплоть до конца этого параграфа показать, что можно вернуться назад к начальному полю H_0 , построив при этом общие точки компонент многообразия. Если $\deg tr_{H_0} F > 0$, то алгоритм строит, кроме того, систему уравнений с коэффициентами из исходного поля F для неприводимых над F компонент или из поля $F_s^{(i)}$ для абсолютно неприводимых компонент (см. выше настоящий параграф), при этом $F_s^{(i)}$ определяется относительно исходного поля F . Все сказанное может быть осуществлено в пределах того же самого времени работы алгоритма с теми же самыми верхними границами на параметры общих точек и задающих систем уравнений как и в основной теореме.

Пусть W_i – некоторая построенная алгоритмом компонента многообразия $\{f_0 = \ldots = f_{k-1} = 0\}$. Алгоритмы, изложенные в §§ I, 3 находят ее общую точку. Обозначим через $W^{(i)}$ определенную и неприводимую над исходным полем $F^{q^{-\infty}}$ в случае а) или над полем $F^{(i)}$, где $F^{(i)}$ рассматривается относительно исходного поля F , в случае в) основной теоремы, компоненту многообразия $\{f_0 = \ldots = f_{k-1} = 0\}$ такую, что $W_i^{(i)} \supset W_i$. Напомним, что W_i определена либо над $F_1^{q^{-\infty}} = (H_1(T_1, \ldots, T_\ell)[\eta])^{q^{-\infty}}$ в случае а), либо над некоторым расширением поля $F^{(i)}$ в случае в) (см. основную теорему). Цель алгоритма – построить общую точку компоненты $W^{(i)}$.

Прежде всего алгоритм строит некоторую другую общую точку для W_i . Сохраним алгебраически независимые элементы $t_1, \ldots, t_{n-m}$. Для построения другого примитивного элемента ξ он использует процедуру (аналогично § I) для перехода от координат $\{Y_j\}$ к $\{X_j\}$ с той лишь разницей, что для примитивного элемента $\xi = \sum_{n-m+1 \le j \le n} \alpha_j^{q^\nu} (X_j / X_0)^{q^\nu}$ коэффициенты α_j выбираются из кольца многочленов $H_0[T_1, \ldots, T_\ell, t_1, \ldots, t_{n-m}]$,

при этом $\deg(a_j)$ меньше подходящего полинома от $m \log d$, если $l+n-m>0$. Кроме того, мы потребуем чтобы имел место изоморфизм $F(t_1,\dots,t_{n-m})[\mathcal{C}] = F'[\mathcal{C}] \cong F(X_1/X_0,\dots,X_{n-m}/X_0, (X_{n-m+1}/X_0)^{q^0},\dots,(X_n/X_0)^{q^0}) \subset F^{q^{-\infty}}(W^{(i)})$ в случае а) основной теоремы.

Чтобы найти элемент $\mathcal{C}$, удовлетворяющий сформулированным условиям, алгоритм просматривает набор $\mathcal{N}$ векторов коэффициентов $(a_{n-m+1},\dots,a_n)$, любые m из которых линейно независимы над H_0, при этом $card\,\mathcal{N} = (m-1)d^m+1$. Семейство $\mathcal{N}$ строится так, что степени $\deg(a_j)$ не превосходят некоторого полинома от $\log(d^m)$ (ср. §I, доказательство леммы 2.5). В дальнейшем, мы покажем, как проверить, удовлетворяет ли данный фиксированный элемент $\mathcal{C}$ всем требованиям. Если $l=n-m=0$, то $W^{(i)}$ – объединение конечного числа точек с координатами из конечного поля и в этом случае все тривиально.

Рассмотрим теперь два следующих случая (ср. основную теорему): а) W_i – неприводимая над $H_1(T_1,\dots,T_l)[\eta]$ компонента; в) W_i – абсолютно неприводимая компонента.

а) Обозначим $\Phi_i(Z) = \sum_j A_j Z^j \in H_1(T_1,\dots,T_l,\eta,t_1,\dots,t_{n-m})[Z]$ неприводимый над полем $F_1' = H_1(T_1,\dots,T_l,\eta,t_1,\dots,t_{n-m})$ многочлен для построенного представления общей точки компоненты W_i (см. введение), причем $\Phi_i(\mathcal{C}_{W_i}) = 0$, где $\mathcal{C}_{W_i} = \mathcal{C}_i \in F_1^{q^{-\infty}}(W_i)$, кроме того $lc_Z(\Phi_i) = 1$. Рассмотрим подполе $F_2' = F'(\{A_j\}) \subset F_1'$, порожденное коэффициентами многочлена Φ_i и конечное подполе $H_2 = H_1 \cap F_2'$. Алгоритм находит H_2 следующим образом, просматривая все промежуточные поля H_2' между H_0 и H_1. Представим $H_2' = H_0[\xi] \subset H_1$ и пусть $\varphi_2(\xi) = 0$; $\varphi_2 \in H_0[Z]$ – минимальный многочлен для ξ, $lc_Z(\varphi_2) = 1$.

Включение $H_2' \subset F_2'$ справедливо в том и только в том случае, если многочлен φ_2 раскладывается на линейные множители над полем F_2'. Очевидно H_2 – максимальное среди рассматриваемых полей H_2', для которых выполняется включение $H_2' \subset F_2'$. Из свойств композита полей (см., напр., [6]) следует, что F_2' является композитом F' и H_2, т.е. $F_2' = H_2(T_1,\dots,T_l,\eta,t_1,\dots,t_{n-m})$.

Рассмотрим произвольную систему однородных многочленов, такую что $W^{(i)} = \{g_0 = \dots = g_s = 0\}$. Как и в §I (см. систему (3')) заменим в этой системе X_j на $t_j X_0$ для $1 \le j < n-m$. Применим лемму 2.5 [4] к полученной системе, полагая сначала $F_1 = F$. Система имеет единственный класс сопряженных над F' корней. Предполагаемый выше изоморфизм $F(X_1/X_0,\dots, X_{n-m}/X_0, (X_{n-m+1}/X_0)^{q^0},\dots,(X_n/X_0)^{q^0}) \cong F[\mathcal{C}]$ доставляет корень этой

системы и показывает, что в качестве примитивного элемента можно взять $\xi_{W^{(i)}} = \xi$. Пусть $\Phi^{(i)}(Z) \in F'[Z]$ – минимальный многочлен для ξ над полем F' и $lc_Z(\Phi_i) = 1$. В кольце $F'[Z]$ выполнено соотношение $\Phi_i(t_1,\dots,t_{n-m},Z) \mid \Phi^{(i)}(t_1,\dots,t_{n-m},Z)$ в силу того, что $\Phi^{(i)}(X_1/X_0,\dots,X_{n-m}/X_0, \sum_{n-m+1\le j\le n} \alpha_j^{q^\nu}(X_j/X_0)^{q^\nu})$ тождественно равно нулю на компоненте $W^{(i)} \supset W_i$.

Следовательно, существует вложение полей $F'[\xi_{W^{(i)}}] \subset F'[\xi_{W_i}] = F'[Z]/(\Phi_i)$, при котором $\xi_{W^{(i)}} \mapsto \xi_{W_i}$. Принимая во внимание, что коэффициенты многочлена Φ_i принадлежат полю F_2', и с другой стороны $H_2 = H_1 \cap F_2'$, мы заключаем, что образ поля $F'[\xi_{W^{(i)}}]$ при этом вложении содержится (и даже совпадает, как это будет доказано ниже) в поле $F_2'[Z]/(\Phi_i(Z)) = F'[\xi_{W_i}] = H_2(T_1,\dots,T_\ell,\eta,t_1,\dots,t_{n-m})[\xi_{W_i}]$.

Вычислим $\Phi = \prod_{\sigma \in Gal(F_2'/F') \subset Gal(H_2/H_0)} \sigma(\Phi_i)$ – неприводимый над полем F' многочлен, равный произведению всех сопряженных к многочлену Φ_i над полем F'. Для этого алгоритм сначала может, например, вычислить группу Галуа $Gal(F_2'/F')$, используя § 3 главы I. Заметим, что $\Phi = \Phi^{(i)}$, поскольку оба эти многочлена неприводимы над F', делятся на Φ_i и $lc_Z(\Phi) = lc_Z(\Phi^{(i)}) = 1$.

Имеет место изоморфизм полей $F'[Z]/(\Phi) = F'[\xi_1] \xrightarrow{\tau} F_2'[Z]/(\Phi_i)$ (здесь $\Phi(\xi_1) = 0$) в силу того, что существует естественное вложение τ, и с другой стороны степени расширений $[F'[Z]/(\Phi) : F'] = deg_Z(\Phi) = deg_Z(\Phi_i)\, card\, Gal(F_2'/F') = [F_2'[Z]/(\Phi_i) : F']$ обоих полей равны. Отсюда следует, что многочлен φ_2 раскладывается над полем $F'[Z]/(\Phi)$ на линейные множители, так как φ_2 раскладывается на линейные множители над полем F_2'. Алгоритм находит разложение $\varphi_2 = \prod(Z - \xi_j)$, где $\xi_j \in F'[Z]/(\Phi)$.

Обратный изоморфизм к τ можно вычислить явно следующим образом. При обратном изоморфизме $\xi \xrightarrow{\tau^{-1}} \xi_j$ для некоторого j, такого что Φ_i обращается в нуль тождественно в поле $F'[\xi_1]$ при подстановке в него элементов ξ_j вместо ξ и ξ_1 вместо Z, соответственно. Отметим, что при изоморфизме $\tau \circ \rho$ элементы $(X_{i_1}/X_0)^{q^\nu} \in F^{q^{-\infty}}(W^{(i)})$, $n-m+1 \le i_1 \le n$ отображаются в элементы $(X_{i_1}/X_0)^{q^\nu}(\xi_{W_i})$ из построенной общей точки многообразия W_i, поскольку они отображаются в q^ν-ые степени некоторого решения системы

$g_0(X_0, t_1X_0 \ldots t_{n-m}X_0, X_{n-m+1}, \ldots, X_n) = \ldots = g_s(X_0, t_1X_0, \ldots, t_{n-m}X_0, X_{n-m+1}, \ldots, X_n) = 0$
все решений этой системы сопряжены над полем F', и примитивный элемент $\mathcal{E} = \sum_{n-m+1 \le i_q \le n} a_{i_q}^{q^q} (X_{i_q}/X_0)^{q^q}$ отображается в примитивный элемент $\mathcal{E}_{W_i} = \sum_{n-m+1 \le i_q \le n} a_{i_q}^{q^q} (X_{i_q}/X_0)^{q^q} (\mathcal{E}_{W_i})$. Таким образом, если для фиксированного (в начале описания алгоритма построения общей точки для $W^{(i)}$) элемента $\mathcal{E}$ элементы $(X_i/X_0)^{q^q} \in F_1[\mathcal{E}_{W_i}]$ принадлежат, в действительности, полю $F_2'[\mathcal{E}_{W_i}]$, то $\mathcal{E}$ удовлетворяет всем требованиям и изоморфизм τ^{-1} дает корень системы уравнений

$g_0(X_0, t_1X_0, \ldots, t_{n-m}X_0, X_{n-m+1}, \ldots, X_n) = \ldots = g_s(X_0, t_1X_0, \ldots, t_{n-m}X_0, X_{n-m+1}, \ldots, X_n) = 0$

в поле $F'[\mathcal{E}]$ и согласно лемме 2.5 [4] общую точку неприводимой над F компоненты $W^{(i)} \supset W_i$.

в) Пусть теперь W_i – абсолютно неприводимая компонента, и построено поле $F_3 = H_1(T_1, \ldots, T_\ell, \eta)[\eta_1']$, где η_1' – алгебраический сепарабельный над $H_1(T_1, \ldots, T_\ell, \eta)$ элемент, такой что W_i определено над полем $F_3^{q^{-\infty}}$. Алгоритм должен найти максимальное сепарабельное над F подполе F_1 минимального поля определения компоненты W_i. Тогда F_3 есть композит полей H_1 и F_1 в силу изложенного в начале параграфа. Следовательно, F_1 совпадает с множеством всех элементов поля F_3, которые инвариантны относительно некоторой степени образующей циклической группы $Gal(H_1/H_0)$, принимая во внимание, что $Gal(F_3/F_1) \subset Gal(H_1/H_0)$.

Алгоритм просматривает степени образующей и для каждой фиксированной степени вычисляет ее поле инвариантов $F_4 \subset F_3$. После этого он применяет пункт а), заменяя там F на F_4 и $H(T_1, \ldots, T_\ell, \eta)$ на F_3, соответственно. В результате будет получена общая точка некоторой неприводимой над F_4 компоненты $W^{(i)} \supset W_i$. Алгоритм выбирает минимальное поле среди рассматриваемых полей F_4, для которого выполняется равенство $W^{(i)} = W_i$ (последнее эквивалентно равенству $deg(\Phi) = deg(\Phi_i)$). Это поле и будет полем F_1.

Обратимся теперь к построению определяющей системы уравнений. Для этой цели мы используем только что построенную общую точку и алгоритм из теоремы 2.2 § 2, с той лишь разницей, что мы будем брать линейные формы $U_i^{(s)}$ с коэффициентами $C_i^{(s)}$ из кольца $H[T_1, \ldots, T_\ell]$.

Неисследованным остается вопрос, возможно ли в случае ко-

нечного поля $F=H$ построить определяющую систему уравнений с коэффициентами из H в пределах того же времени, что и в теореме 2.2.

Литература

1. Варден-ван-дер Б.Л. Современная алгебра. ч.I,2. - М.-Л., ОНТИ, I937.
2. Григорьев Д.Ю. Два сведения изоморфизма графов к задачам о полиномах. - Зап.научн.семинаров ЛОМИ АН СССР,I979, т.88, с.56-6I.
3. Зариский О., Самюэль П. Коммутативная алгебра. т.I,2. - М., ИЛ, I963.
4. Грйгорьев Д.Ю. Разложение многочленов над конечным полем и решение систем алгебраических уравнений. - Зап.научн. семинаров ЛОМИ АН, I984, т.I37, с.20-79.
5. Кнут Д. Искусство программирования для ЭВМ. т.2 - М., Мир, I977.
6. Ленг С. Алгебра. - М., Мир, I968.
7. Шафаревич И.Р. Основания алгебраической геометрии - М., Наука, I972.
8. Chistov A.L., Grigor'ev D.Yu. Polynomial-time factoring of the multivariable polynomials over a global field. - LOMI preprint E-5-82, Leningrad, 1982.
9. Chistov A.L., Grigor'ev D.Yu. Subexponential-time solving systems of algebraic equations. I. - LOMI preprint E-9-83, Leningrad, 1983.
10. Chistov A.L., Grigor'ev D.Yu. Subexponential-time solving systems of algebraic equations. II. - LOMI preprint E-10-83, Leningrad, 1983.
11. Collins G. Subresultants and reduced polynomial remainder sequences. - J.Assoc.Comput.Mach., 1967, vol.14, N1, p.128-142.
12. Grigor'ev D.Yu. Some new bounds on tensor rank. - LOMI preprint E-2-78, Leningrad, 1978.
13. Grigor'ev D.Yu. Multiplicative complexity of a bilinear form over a commutative ring. - Lect.Notes Comput. Sci., 1981, vol.118, p.281-286.
14. Heintz J. Definability and fast quantifier elimination in algebraically closed field. - Prepr.Univ.Frankfurt, West Germany, December, 1981.

15. K a l t o f e n E. A polynomial reduction from multivariate to bivariate integral polynomial factorization. - Proc. 14-th ACM Symp.Th.Comput., May, N.Y., 1982, p.261-266.
16. K a l t o f e n E. A polynomial-time reduction from bivariate to univariate integral polynomial factorization. - Proc.23-rd Ann.Symp.Found.Comp.Sci., October, N.Y., 1982.
17. L a z a r d D. Algebre linéaire sur $k[X_1,\dots,X_n]$ et élimination. - Bull.Soc.Math.France, 1977, vol.105, p.165-190.
18. L a z a r d D. Résolutions des systémes d'équations algébriques. - Theor.Comput.Sci., 1981, vol.15, p.77-110.
19. L a z a r d D. Commutative algebra and computer algebra. - Lect.Notes Comput.Sci., 1983, vol.144, p.40-48.
20. L e n s t r a A.K., L e n s t r a H.W., L o v a s z L. Factoring polynomials with rational coefficients. - Preprint. Math.Centrum Amsterdam IW 195/82, 1982.
21. M c C l e l l a n M.T. The exact solution of systems of linear equations with polynomial coefficients. - J.Assoc. Comput.Mach., 1973, vol.20, N 4, p.563-588.
22. S e i d e n b e r g A. Constructions in a polynomial ring over the ring of integers. - Amer.J.Math., 1978, vol. 100, N 4, p.685-704.

Chistov A.L. Polynomial-time factoring of polynomials and finding the compounds of a variety within the subexponential time.

Let $F = H(T_1,\dots,T_l)[\eta]$ where either $H = \mathbb{Q}$ or H is a finite field, $T_1,\dots,T_l$ be algebraically independent over H, a polynomial $\varphi \in H(T_1,\dots,T_l)[Z]$ be a minimal for η, denote $q = char(F)$. Let $L(f)$ be the size of $f \in F[X_0,\dots,X_n]$.

THEOREM 1. One can factor f over F within the polynomial in $L(f), L(\varphi), q$ time.

The theorem expands the result of [4] treating the case of a finite F.

Let homogeneous polynomials $f_0,\dots,f_K \in F[X_0,\dots,X_n]$ be given and $\deg_{X_0,\dots,X_n}(f_i) < d$, denote by L the size of the system $f_0 = \dots = f_K = 0$. The variety of common roots in $\mathbb{P}^n(\bar{F})$ of the latter system is decomposable on irreducible **compounds** W_α. **A compound** W_α **is represented further by its general point and by a system of equations whose variety of roots is** W_α. **The following theorem improves bounds from** [4].

THEOREM II. An algorithm is suggested finding all compounds W_α **within polynomial in** $(Ld^n)^{n+l}, q$ **time.**