ВЕСТНИК НОВОСИБИРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Серия «Математика, механика, информатика»
Том VI, 2006 г. Выпуск 3. С. 25–48

УДК 512.54+517.27

Разделенные разности в теории дифференциально-разностных уравнений и в теории групп

А. А. Коробов

В § 1 доказан аннонсированный в [1] результат. Оказалось, что описанные в статье [2] непредставимые над полем характеристики 0 группы автоморфизмов относительно свободных групп не являются линейными. В § 2 описан и проиллюстрирован метод разложения целочисленного многочлена на простые в $\mathbb{Q}[x]$ множители, опирающийся на свойства разделенных разностей, который позволил сделать заключение о нелинейности некоторых минимальных неособых подгрупп указанных групп. В § 3 доказан результат, аннонсированный в [3]. При естественных (в теории управляемости) ограничениях на $n \times n$-матрицу A с вещественным спектром ее матричная экспонента не лежит в линейной оболочке матриц $A^0, A^1, \ldots, A^{n-2}$. Последнее свойство важно для получения простых критериев точечной вырожденности автономного дифференциально-разностного уравнения с одним постоянным запаздыванием [4–6].

§ 1. О некоторых группах автоморфизмов относительно свободных групп

Будем говорить, что группа G действует на группе M, если существует гомоморфизм θ группы G в группу $\mathrm{Aut}\,(M)$ всех автоморфизмов группы M, а подгруппу $\mathrm{Ker}\,\theta$ группы G назовем стабилизатором этого действия и обозначим ее через $C_G(M)$. Будем говорить, что группа G действует на группе M как конечная группа, если группа G^θ конечна. Следующее утверждение является простым следствием определений.

Лемма 1.1. *Подгруппа группы G, действующей на группе M как конечная группа, сама действует на M как конечная группа.*

Пусть K, L — нормальные подгруппы в G и $L \leq K$. Если g^θ — это автоморфизм сек-

ции K/L, индуцированный сопряжением группы K элементом $g \in G$, то будем говорить, что группа G действует сопряжением на секции K/L.

Лемма 1.2. *Пусть K, L — нормальные подгруппы в группе G и $L \leq K$. Если группа G/L действует сопряжением на секции K/L как конечная группа, то и группа G действует на секции K/L как конечная группа.*

Утверждение леммы 1.2 следует из совпадения образов в группе $\mathrm{Aut}\,(K/L)$ групп G/L и G при соответствующих гомоморфизмах.

Рассмотрим теперь другой важный пример действия. Пусть K, L — автоморфно допустимые подгруппы в G, $\Phi \leq \mathrm{Aut}\,(G)$. Будем говорить, что группа Φ действует автоморфизмами на секции K/L, если φ^θ — это автоморфизм секции K/L, индуцированный автоморфизмом $\varphi \in \Phi$.

Напомним, что голоморфом $\mathrm{Hol}\,G$ называется множество пар φg, $\varphi \in \Phi = \mathrm{Aut}\,(G)$, $g \in G$, умножаемых по правилу $\varphi g \cdot \varphi' g' = \varphi\varphi' g^{\varphi} g'$ (мы пишем пары без скобок и запятых). Непосредственно проверяется, что отображения $\Phi \to \mathrm{Hol}\,(G)$, $G \to \mathrm{Hol}\,(G)$, задаваемые правилами $\varphi \rightarrowtail \varphi 1$, $g \rightarrowtail 1g$, являются изоморфными вложениями. Важнейшее свойство голоморфа состоит в следующем: каждый автоморфизм образа группы G является сопряжением образом подходящего автоморфизма группы G.

Лемма 1.3. *Пусть G — группа, факторизацию по ее центру Z обозначим волной. Пусть K, L такие две автоморфно допустимые подгруппы в G, что $Z \leq L \leq K$; $\Phi \leq \mathrm{Aut}\,(G)$. Тогда стабилизатор действия группы Φ автоморфизмами на секции K/L совпадает со стабилизатором действия группы Φ сопряжением на секции $\tilde{K}/\tilde{L}$.*

ДОКАЗАТЕЛЬСТВО. Неограничивая общности, можно считать, что группы G и Φ — подгруппы голоморфа $\mathrm{Hol}\,(G)$. Тогда, как легко следует из правила умножения, важнейшее свойство голоморфа $\mathrm{Hol}\,(G)$ можно сформулировать более точно: $\varphi^{-1} g \varphi = g^{\varphi}$ для $\varphi \in \Phi$, $g \in G$. Пусть гомоморфизм $\theta_1\colon \Phi \to \mathrm{Aut}\,(K/L)$ индуцирован автоморфизмами, а гомоморфизм $\theta_2\colon \Phi \to \mathrm{Aut}\,(\tilde{K}/\tilde{L})$ индуцирован сопряжением. Необходимо доказать, что $\mathrm{Ker}\,\theta_1 = \mathrm{Ker}\,\theta_2$.

Пусть сначала $\varphi \in \mathrm{Ker}\,\theta_1$. Тогда для любого $k \in K$ найдется такой $l \in L$, что $k^{\varphi} = kl$. Пусть $k' \in K/Z$ выбран произвольно. Тогда существует $k \in K$: $\tilde{k} = k'$. Теперь доказательство включения $\mathrm{Ker}\,\theta_1 \leq \mathrm{Ker}\,\theta_2$ заканчивает следующая цепочка равенств, полученная с учетом основного свойства голоморфа и отмеченного свойства группы K^{φ}:

$$(k'\tilde{L})^{\varphi^{\theta_2}} = \widetilde{\varphi^{-1} k \varphi}\tilde{L} = \widetilde{k^{\varphi}}\tilde{L} = \tilde{k}\tilde{l}\tilde{L} = k'\tilde{L}\,.$$

Докажем теперь включение в другую сторону. Пусть $\varphi \in \ker\,\theta_2$, и элемент $k' \in K/L$ выбран произвольно, скажем $k' = kL$, $k \in K$. Так как $(\tilde{k}\tilde{L})^{\varphi^{\theta_2}} = \tilde{k}\tilde{L}$, то найдется такой $l \in L$, что $\widetilde{\varphi^{-1} k \varphi} = \tilde{k}\tilde{l}$. Тогда, учитывая основное свойство голоморфа, найдется такой $z \in Z$, что $k^{\varphi} = klz$. Поэтому $(k')^{\varphi^{\theta_1}} = k^{\varphi} L = kL = k'$. Лемма полностью доказана.

Следующая лемма выясняет соотношения между стабилизаторами действий сопряжениями фиксированной группы на двух различных группах.

Лемма 1.4.

а) Пусть $A \leq B \leq G$; A, H — нормальные подгруппы в группе G. Тогда стабилизатор действия группы G сопряжением на секции BH/AH совпадает со стабилизатором действия группы G сопряжением на секции $B/A(B \cap H)$.

б) Пусть G действует сопряжением на группах M/M_1 и M/M_2. Если $M_1 \leq M_2$, то стабилизатор действия группы G сопряжением на M/M_1 содержится в стабилизаторе действия группы G сопряжением на M/M_2.

в) Пусть G — действует сопряжением на M и M_0 — подгруппа в M, инвариантная относительно указанного действия группы G. Тогда стабилизатор действия группы G сопряжением на секции M/U содержится в стабилизаторе действия группы G сопряжением на секции $M_0/M_0 \cap U$.

ДОКАЗАТЕЛЬСТВО. Докажем сначала первое утверждение леммы. Пусть $g \in C_G(BH/AH)$. Тогда для любого $b \in B$ найдутся такие $a \in A$, $h \in H$, что $b^g = bah$. Тогда $h = a^{-1}b^{-1}b^g \in B \cap H$. Значит, $g \in C_G(B/A(B \cap H))$. Докажем теперь включение в другую сторону. Пусть $g \in C_G(B/A(B \cap H))$. Тогда для любого $b \in B$ найдутся такие $a \in A$, $b_1 \in B \cap H$, что $b^g = bab_1$. Тогда для любого $h \in H$ имеем $(bh)^g = bhr$, где $r = a(h^{-1})^a b_1 h^g \in AH$.

Докажем теперь второе утверждение. Пусть $g \in C_G(M/M_1)$. Тогда для любого $m \in M$ имеем $m^{-1}m^g \in M_1 \subseteq M_2$. Значит, $g \in C_g(M/M_2)$.

Приступая к доказательству последнего утверждения леммы, предположим, что $g \in C_G(M/U)$. Тогда для любого $m \in M$ имеем $m^{-1}m^g \in U$. Значит, для любого $m_0 \in M_0$ справедливо: $m_0^{-1}m_0^g \in M_0 \cap U$. Лемма полностью доказана.

Для линейной группы G будем через $\bar{G}$ обозначать ее замыкание в полиномиальной топологии, $\bar{G}_0$ — связную компоненту единицы группы $\bar{G}$, $\mathrm{u}(\bar{G}_0)$ — наибольшую унипонтентную подгруппу группы $\bar{G}_0$.

Лемма 1.5. *Пусть Ω — универсальная область, $H \leq Gl_n(\Omega)$, $G \lhd H$ и группа G без свободных неабелевых подгрупп. Тогда H действует сопряжением на секции $G_0/(G_0 \cap \mathrm{u}(\bar{G}_0))$ как конечная группа.*

ДОКАЗАТЕЛЬСТВО. Пусть сначала G, H — алгебраические группы. По альтернативе Титса любая конечно порожденная подгруппа в G почти разрешима [7, теорема 55.2.1]. Тогда G_0 (связная компонента единицы группы G) разрешима. Покажем, что $|H : C_H(G_0/\mathrm{u}(G_0))| < \infty$.

По лемме 1.2 $|H/\mathrm{u}(G_0) : C_{H/\mathrm{u}(G_0)}(G_0/\mathrm{u}(G_0))| = |H : C_H(G_0/\mathrm{u}(G_0))|$. Поэтому достаточно доказать конечность указанного индекса в случае, когда $\mathrm{u}(G_0) = e$. Тогда G_0 — связная диагонализируемая подгруппа в H. Можно считать, что G_0 состоит из диаго-

нальных матриц. Достаточно показать, что автоморфизм φ группы G_0, индуцированный сопряжением любым элементом из H, совпадает с автоморфизмом, индуцированным сопряжением некоторой мономиальной матрицей из нулей и единиц. Оба автоморфизма являются рациональными отображениями группы G_0. Поэтому их равенство достаточно установить на некоторой общей точке g группы G_0. Образ g^{φ} имеет те же характеристические числа, что и матрица g и является диагональной матрицей. Поэтому нетрудно указать такую мономиальную матрицу t, что $g^{\varphi} = g^t$. Итак, конечность указанного индекса установлена.

Пусть теперь группы G и H, удовлетворяющие условиям леммы, произвольны. Тогда группы $\bar{H}$, $\bar{G}$ — замыкание групп H, G, соответственно, — являются алгебраическими группами, и поэтому группа $\bar{H}$ действует сопряжением на секции $\bar{G}/\mathrm{u}\,(\bar{G}_0)$ как конечная группа. По лемме 1.1 индекс $|H : C_H(\bar{G}_0/\mathrm{u}\,(\bar{G}_0))|$ тоже конечен. Тогда группа H действует сопряжением на группе $\bar{G}_0$ и ее подгруппа $G_0 = G \cap \bar{G}_0$ инвариантна относительно указанного действия. Поэтому по лемме 1.4 H действует на секции $G_0/G_0 \cap \mathrm{u}\,(\bar{G}_0)$ как конечная группа. Лемма доказана.

Пусть $\mathfrak{M}$ — некоторое многообразие групп. Обозначим через $F_n(\mathfrak{M})$ — свободную группу ранга n многообразия $\mathfrak{M}$ (относительно свободную группу). Пусть $\mathfrak{N}_c$ — многообразие всех нильпотентных групп класса $c\,(c \geq 1)$, $\mathfrak{A}$ — многообразие всех абелевых групп, $\mathfrak{A}_k$ — многообразие всех абелевых групп экспоненты k, $\mathfrak{B}_m$ — многообразие всех локально конечных групп экспоненты m. Обозначим через $\mathfrak{A}_k\mathfrak{A}$, $\mathfrak{N}_c\mathfrak{A}\mathfrak{B}_m$ — произведение этих многообразий.

Пусть G — группа. Обозначим через $\mathrm{Aut}\,G$ группу всех автоморфизмов группы G, $\mathrm{Inn}\,G$ группу всех внутренних автоморфизмов группы G. Прежде чем, сформулировать основной результат, дадим следующее определение.

Пусть G — группа. Группа A, удовлетворяющая условию $\mathrm{Inn}\,G \leq A \leq \mathrm{Aut}\,G$, называется неособой, если группа $\tilde{A}$ автоморфизмов $\mathbb{Z}$-модуля G/G', индуцированная группой A, удовлетворяет следующему условию: сужение группы $\tilde{A}$ на любой $\tilde{A}$-инвариантный подмодуль модуля G/G' бесконечно.

Основной результат этого параграфа следующий:

Теорема 1.1. *Пусть n — натуральное число, $\mathfrak{M}$ — собственное подмногообразие в многообразии всех групп.*

1) Если для любых натуральных чисел m и c справедливо условие $\mathfrak{M} \not\subseteq \mathfrak{N}_c\mathfrak{A}\mathfrak{B}_m$, то любая неособая подгруппа в $\mathrm{Aut}\,F_n(\mathfrak{M})$ нелинейна.

2) Если натуральные числа m, k, c такие, что $\mathfrak{M} \subseteq \mathfrak{N}_c\mathfrak{A}\mathfrak{B}_m$ и $\mathfrak{A}_k\mathfrak{A} \subseteq \mathfrak{M}$, то любая неособая подгруппа в группе $\mathrm{Aut}\,F_n(\mathfrak{M})$ нелинейна.

3) Если найдутся натуральные числа m и c такие, что $\mathfrak{M} \subseteq \mathfrak{N}_c\mathfrak{A}\mathfrak{B}_m$, но для любого натурального числа k справедливо условие $\mathfrak{A}_k\mathfrak{A} \not\subseteq \mathfrak{M}$, то голоморф группы $F_n(\mathfrak{M})$ линеен.

ДОКАЗАТЕЛЬСТВО. Сначала докажем первое утверждение. Пусть, напротив, нашлась неособая линейная подгруппа A в $\operatorname{Aut} F_n(\mathfrak{M})$. Тогда линейна группа $G = F_n(\mathfrak{M})/Z \cong \operatorname{Inn} F_n(\mathfrak{M})$, где Z — центр группы $F_n(\mathfrak{M})$. Пусть $\bar{G}$ — замыкание группы G в полиномиальной топологии; $\bar{G}_0$ — ее связная компонента единицы. Так как $\bar{G}_0$ — связная группа с нетривиальным тождеством, то $\bar{G}_0$ триангулируема, а, значит, группа $G_0 = G \cap \bar{G}_0$ имеет нильпотентный коммутант. Пусть c — ступень нильпотентности группы G_0', m — период группы G/G_0. Тогда матрешка $1 \leq G_0' \leq G_0 \leq G$ показывает, что $G \in \mathfrak{N}_c\mathfrak{A}\mathfrak{B}_m$, а полные прообразы членов этой матрешки в $F_n(\mathfrak{M})$ дают матрешку, из которой следует, что $F_n(\mathfrak{M}) \in \mathfrak{N}_{c+1}\mathfrak{A}\mathfrak{B}_m$. Полученное противоречие заканчивает доказательство первого утверждения теоремы.

Теперь докажем второе утверждение теоремы. Пусть, напротив, нашлась неособая линейная подгруппа A в $\operatorname{Aut} F_n(\mathfrak{M})$. Тогда фактор-группа группы $F_n(\mathfrak{M})$ по ее центру изоморфна группе $G = \operatorname{Inn}(F_n(\mathfrak{M}))$, которая поэтому не содержит свободных подгрупп. Очевидно, что группа G нормальна в A, и поэтому по лемме 1.5 группа A действует сопряжением на секции $G_0/(G_0 \cap \mathrm{u}(\bar{G}_0))$ как конечная группа.

Пусть N — произведение всех нормальных нильпотентных подгрупп группы G. Очевидно, что N — автоморфно допустимая подгруппа в G, а, следовательно, нормальна в A. Поскольку $\mathrm{u}(\bar{G}_0) \cap G_0 \leq G_0 \cap N$, то по лемме 1.4 и на секции $G_0/G_0 \cap N$ группа A действует как конечная группа. Тогда по лемме 1.4 группа A действует сопряжением на секции G_0N/N как конечная группа.

Пусть M_1 и N_1 — полные прообразы групп G_0N и N в группе $F_n(\mathfrak{M})$. Поскольку центр группы является ее автоморфно допустимой подгруппой, то M_1 является автоморфно допустимой подгруппой конечного индекса в $F_n(\mathfrak{M})$. А поскольку нильпотентность сохраняется при центральном расширении, то N_1 — произведение всех нильпотентных подгрупп группы $F_n(\mathfrak{M})$. Более того, N_1 нильпотентна, так как N нильпотентна. По лемме 1.3 группа A действует автоморфизмами на секции M_1/N_1 как конечная группа.

Так как N_1 — эндоморфно допустимая подгруппа относительно свободной группы $F_n(\mathfrak{M})$, то N_1 — вербальная подгруппа в $F_n(\mathfrak{M})$ [8, теорема 13.31]. Поэтому либо фактор-группа $F_n(\mathfrak{M})/N$ имеет ограниченный период, либо $N_1 \leq F_n(\mathfrak{M})'$. Поскольку группа $F_n(\mathfrak{M})$ принадлежит классу почти разрешимых групп, в котором любая периодическая группа является локально конечной, то в первом случае группа $F_n(\mathfrak{M})$ оказалась бы почти нильпотентной, что не совместимо с существованием (по условию) гомоморфизма группы $F_n(\mathfrak{M})$ на группу $F_n(\mathfrak{A}_k\mathfrak{A})$.

Итак, $N_1 \leq F_n(\mathfrak{M})'$, и поэтому по лемме 1.4 (утверждение б)) группа A действует на секции $M_1/F_n(\mathfrak{M})' \cap M_1$ как конечная группа. Тогда ввиду утверждения а) леммы 1.4 группа A и на секции $M_1F_n(\mathfrak{M})'/F_n(\mathfrak{M})'$ действует как конечная группа. Кроме того, существование гомоморфизма группы $F_n(\mathfrak{M})$ на группу $F_n(\mathfrak{A}_k\mathfrak{A})$ гарантирует существование гомоморфизма группы $F_n(\mathfrak{M})$ на группу $F_n(\mathfrak{A})$, откуда следует, что абелизация

$F_n(\mathfrak{M})/F_n(\mathfrak{M})'$ является свободной абелевой группой, в частности, — бесконечной. Если бы теперь секция $M_1F_n(\mathfrak{M})'/F_n(\mathfrak{M})'$ была бы тривиальной, то конечность индекса M_1 в $F_n(\mathfrak{M})$ означала бы конечность абелизации $F_n(\mathfrak{M})/F_n(\mathfrak{M})'$, что противоречит доказанному.

Итак, $M_1F_n(\mathfrak{M})'/F_n(\mathfrak{M})'$ — нетривиальный подмодуль свободного $\mathbb{Z}$-модуля $F_n(\mathfrak{M})/F_n(\mathfrak{M})'$, инвариантный относительно группы автоморфизмов $\tilde{A}$ модуля $F_n(\mathfrak{M})/F_n(\mathfrak{M})'$, индуцированной действием группы A автоморфизмами на секции $F_n(\mathfrak{M})/F_n(\mathfrak{M})'$. По условию группа $\tilde{A}$ бесконечна. Поэтому группа A действует на секции $M_1F_n(\mathfrak{M})'/F_n(\mathfrak{M})'$ как бесконечная группа. Полученное противоречие с установленным выше заканчивает доказательство второго утверждения теоремы.

Докажем теперь последнее утверждение. Из [18] следует, что группа $F_n(\mathfrak{M})$ при данных условиях является почти нильпотентной. Хорошо известно, что в конечно порожденной группе всякая подгруппа конечного индекса содержит вербальную подгруппу конечного индекса [9, упражнение 15.2.3]. Пусть V — нильпотентная вербальная подгруппа в $F_n(\mathfrak{M})$ конечного индекса. Будучи подгруппой конечно порожденной группы, группа V сама является конечно порожденной и, следовательно, полициклической. Хорошо известно, что линейность голоморфа произвольной группы равносильна линейности ее некоторой автоморфно допустимой подгруппы конечного индекса [7, упражнение 59.3.2]. Поскольку по теореме Ю.И. Мерзлякова голоморф группы V линеен, то тем самым доказана линейность голоморфа группы $F_n(\mathfrak{M})$. Теорема полностью доказана.

Приведем несколько примеров неособых групп. Напомним, что автоморфизм группы G называется ручным, если он индуцирован некоторым автоморфизмом соответствующей накрывающей свободной группы. Как следует из основного результата этого параграфа, самый интересный случай следующий: группа G является конечно порожденной, относительно свободной почти разрешимой, но не является почти нильпотентной. Класс всех таких групп обозначим через $\mathcal{P}$. В этом случае группа всех ручных автоморфизмов группы G является конечно порожденной [10] и неособой, поскольку абелизация G/G' является свободным конечномерным $\mathbb{Z}$-молулем и не существует в нем собственного нетривиального подмодуля, инвариантного относительно полной группы автоморфизмов $\mathbb{Z}$-модуля G/G'.

Основной результат статьи [2] состоит в том, что группа всех автоморфизмов рассматриваемой группы G не представима матрицами над полем характеристики 0. В этом параграфе будет доказано, что уже группа $\mathrm{Raut}(G)$ всех ручных автоморфизмов такой группы G нелинейна. Более того, причиной нелинейности группы $\mathrm{Raut}(G)$ являются ее конечно порожденные почти разрешимые подгруппы. Это будет следовать из другого примера неособых групп автоморфизмов группы G, к которому мы теперь приступаем.

Лемма 1.6. *Пусть $G = гр(x_1, \ldots, x_n)$ — не почти нильпотентная относительно свободная группа, являющаяся почти разрешимой; $f = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ —*

не имеющий на единичной окружности корней целочисленный многочлен, $a_n \in \{-1, 1\}$; $a = (a_1, \dots, a_n)$. *Тогда если к* $\operatorname{Inn} G$ *добавить внешний ручной автоморфизм* φ_a ($\varphi_a(x_i) = x_{i+1}$, $i < n$, $\varphi_a(x_n) = x_1^{-a_n} x_2^{-a_{n-1}} \dots x_n^{-a_1}$), *то получится неособая группа автоморфизмов.*

ДОКАЗАТЕЛЬСТВО. Пусть сначала G — свободная группа. Очевидно φ_a продолжается до гомоморфизма группы G на себя. Из линейности (или финитной аппроксимируемости) группы G следует ее хопфовость [7, следствие 51.2.2]. Другими словами, отображение φ_a задает автоморфизм группы G. Значит, найдутся такие слова $w_i(x_1, \dots, x_n)$ от $x_1, \dots, x_n$ ($i = 1, \dots, n$), что $\varphi_a^{-1}(x_i) = w_i(x_1, \dots, x_n)$, $i = 1, \dots, n$.

Пусть теперь G — произвольная относительно свободная группа. Тогда отображение ψ_a ($\psi_a(x_i) = w_i(x_1, \dots, x_n)$, $i = 1, \dots, n$) продолжается до эндоморфизма группы G, и отображение $\varphi_a\psi_a$ действует на порождающих тождественно. Следовательно, φ_a — ручной автоморфизм группы G.

Далее, можно утверждать, что абелизация G/G' является нециклическим свободным $\mathbb{Z}$-модулем. В частности, φ_a — внешний автоморфизм группы G. Рассмотрим собственный нетривиальный подмодуль U_0, который инвариантен относительно индуцированного автоморфизма $\bar{\varphi}_a$. Пусть V — $\mathbb{Q}$-оболочка $\mathbb{Z}$-модуля G/G', U — $\mathbb{Q}$-оболочка подмодуля U_0. Дополним базис подпространства U до базиса всего векторного пространства V. Пусть M — матрица линейного преобразования φ_a в указанном базисе. Тогда $f(\lambda) = \chi_M(\lambda)$ делится на характеристический многочлен линейного преобразования $\bar{\varphi}_a|_U$ пространства U. Значит, последний многочлен не имеет корней на единичной окружности. Теперь, если бы автоморфизм $\bar{\varphi}_a|_U$ модуля U_0 имел бы конечный порядок, то линейное преобразование $\varphi_a|_U$ имело бы конечный порядок и все его характеристические числа лежали бы на единичной окружности, что невозможно. Лемма доказана.

Замечание. Доказательство леммы полностью проходит, если заменить слова «f не имеет корней на единичной окружности» на слова «корни f не являются корнями из единицы». Однако, в следующем параграфе будет показано, что это формальное усиление формулировки леммы не приводит к увеличению числа примеров неособых групп.

Следствие 1.1. *Пусть* $\varepsilon \in \{-1, 1\}$, $f = x^n + ax^m + \varepsilon$ *— целочисленный многочлен,* $d = (n, m)$, *многочлен* g *определяется равенством* $g(x^d) = f(x)$. *Пусть* $G = \text{гр}\,(x_1, \dots, x_n) \in \mathcal{P}$, φ *— автоморфизм группы* G, *задаваемый на свободных образующих следующим образом:* $\varphi(x_i) = x_{i+1}$, $i < n$; $\varphi(x_n) = x_1^{-\varepsilon} x_{m+1}^{-a}$. *Тогда* $\text{гр}\,(\varphi, \operatorname{Inn} G)$ *— конечно порожденная почти разрешимая нелинейная группа, если выполнено одно из следующих условий: а)* $|a| > 2$; *б)* $|a| = 2$ *и* $g(-1)g(1) \neq 0$; *в)* $|a| = 1$ *и* $n + m$ *не делится на 3; г)* $|a| = 1$ *и* $(g, (x^2 - x + 1)(x^2 + x + 1)) = 1$.

Следствие 1.2. *Пусть* $\varepsilon \in \{-1, 1\}$, $n \geq 4$, $G = \text{гр}\,(x_1, \dots, x_n) \in \mathcal{P}$, φ *— автоморфизм,*

задаваемый на свободных образующих следующим образом: $\varphi(x_i) = x_{i+1}$, $i < n$; $\varphi(x_n) = x_1 x_2^{\varepsilon} x_{n-1}^{-\varepsilon} x_n^{4\varepsilon}$. *Тогда группа* $\mathrm{гр}\,(\varphi, \operatorname{Inn} G)$ *нелинейна.*

Следствие 1.3. *Пусть* n, m, p *убывающая последовательность натуральных чисел, целочисленный многочлен* f *имеет вид:* $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, $|\varepsilon_1| = |\varepsilon_2| = |\varepsilon_3| = 1$. *Пусть* $G = \mathrm{гр}\,(x_1, \ldots, x_n) \in \mathcal{P}$, φ *— автоморфизм группы* G, *задаваемый на свободных образующих следующим образом:* $\varphi(x_i) = x_{i+1}$, $i < n$; $\varphi(x_n) = x_1^{-\varepsilon_3} x_{p+1}^{-\varepsilon_2} x_{m+1}^{-\varepsilon_1}$. *Если многочлен* f *неприводим над* $\mathbb{Q}$, *то* $\mathrm{гр}\,(\varphi, \operatorname{Inn} G)$ *нелинейна.*

ДОКАЗАТЕЛЬСТВО следствий. Пусть $f_1 = x^n + a_1 x^m + \varepsilon_1$, $f_2 = x^n + 4\varepsilon_2 x^{n-1} + 2x^{n-2} - \varepsilon_2 x - 1$, $f_3 = x^n + \tau_1 x^m + \tau_2 x^p + \tau_3$, где встретившиеся параметры удовлетворяют условиям следствий 1, 2, 3 соответственно. В § 2 будет показано, что многочлен f_2 имеет хотя бы один корень в области $|z| < 1$ и неприводим над $\mathbb{Q}$ (см. лемму 2.5). Покажем, что многочлен f_3 имеет корень в области $|z| \neq 1$. В противном случае, можно считать, что $(n, m, p) = 1$, f_3 — возвратный многочлен четной степени. Значит, $m = n - p$, $\tau_1 = \tau_2$. Тогда оба числа m и p нечетны и $f_3(-\tau_1) = 0$. Полученное противоречие, с учетом леммы 2.3 и леммы 2.7, показывает, что многочлены f_1, f_2, f_3 не имеют корней на единичной окружности.

Тогда $\mathrm{гр}\,(\varphi, \operatorname{Inn} G)$ — неособая группа автоморфизмов (см. лемму 1.6) и, согласно теореме этого параграфа, не является линейной. Поскольку $\operatorname{Inn} G$ — гомоморфный образ почти разрешимой группы, то $\operatorname{Inn} G$ — почти разрешимая группа. Пусть H — разрешимая автоморфно допустимая подгруппа в $\operatorname{Inn} G$ конечного индекса [9, упражнение 15.2.3]. Тогда $H \lhd \operatorname{Aut} G$ [9, упражнение 5.2.3], и соответствующий гомоморфизм обозначим чертой. Тогда группа $G_1 = \overline{\mathrm{гр}\,(\varphi, \operatorname{Inn} G)}$ — содержит конечную нормальную подгруппу G_2 и соответствующая фактор-группа G_1/G_2 бесконечная циклическая. По теореме Ф. Холла стабилизатор матрешки $G_1 \geq G_2 \geq G_3 = 1$ нильпотентен [9, теорема 16.3.2]. Пусть T_i — стабилизатор действия группы G_1 сопряжением на секции G_i/G_{i+1}, $i = 1, 2$. Так как полные группы автоморфизмов указанных секций конечны, то группа $T = T_1 \cap T_2$ имеет в G_1 конечный индекс. С другой стороны, T — подгруппа стабилизатора указанной матрешки, и поэтому нильпотентна. Взяв в $\mathrm{гр}\,(\varphi, \operatorname{Inn} G)$ полный прообраз этой группы, получим искомую разрешимую подгруппу конечного индекса в ней. Доказательство следствий закончено.

§ 2. Разделенные разности в элементарной теории чисел

Результаты предыдущего параграфа свели задачу нахождения минимальных неособых групп автоморфизмов к задаче разложения унитарного целочисленного многочлена, модуль значения которого в нуле равен 1, на неприводимые множители над $\mathbb{Q}$. В этом параграфе мы покажем, что каждый невозвратный такой многочлен, неприводимый над

простым конечным полем, определяет неособую группу автоморфизмов. Примеры таких многочленов ограниченной степени могут выбраны из существующих таблиц [11, 19]. В обзоре [20] анализируется метод Цассенхауза разложения целочисленного многочлена на неприводимые множители над $\mathbb{Q}$, и показано, что для определения делителей многочленов

$$u = x^8 + 8x^7 + 21x^6 + 21x^5 + 42x^4 + 13x^3 + 12x^2 - 14x - 12,$$
$$v = x^{15} + 30x^{14} + 5x^{13} + 2x^{12} + 5x + 2$$

по методу Цассенхауза требуется слишком большой перебор. С другой стороны, классический метод Кронекера, решающий эту же задачу, даже после того, как его усовершенствовали Рунге [21] и Мандль [22], продолжает оставаться «очень громоздким и практически неприменимым» [12, с. 272]. Наконец, метод Яковкина [13, глава 3], особенно эффективный для гурвицевых многочленов, оказывается практически неприменимым уже для многочлена u.

В этом параграфе будет изложен метод для разложения унитарного целочисленного многочлена на неприводимые множители в поле рациональных чисел, который дает ответ для многочленов u и v, указанных выше. Этот метод основан на сочетании свойства разделенной разности в целых узлах и идеи О. Перрона [23]. В основании метода лежит следующее наблюдение.

Лемма 2.1. *Значение разделенной разности целочисленного многочлена в различных целых узлах интерполяции является целым числом.*

Доказательство этой леммы будет дано в следующем параграфе. Применение этого наблюдения мы проиллюстрируем на примере, упомянутом в обзоре [20].

Лемма 2.2. *Многочлен* $g = x^8 + 8x^7 + 21x^6 + 21x^5 + 42x^4 + 16x^3 + 12x^2 - 14x - 12$ *неприводим над* $\mathbb{Q}$.

ДОКАЗАТЕЛЬСТВО. Сначала проверим, что многочлен g не имеет рациональных корней. Согласно известному признаку [14, задача 690], вещественные корни многочлена g не превосходят $\rho + \sqrt[7]{\max\{14, \frac{12}{\rho}\}}$, где ρ — любое положительное число. В частности, при $\rho = \frac{6}{7}$ получаем, что нет корней многочлена g в интервале $[3, +\infty)$. С другой стороны, разделив многочлен $g(-x)$ на $x - 3$, получим, что $g(-x) = 2460 + 3056(x-3) + 1596(x-3)^2 + F(x)(x-3)^3$, где $F(x)$ — многочлен с положительными коэффициентами. Отсюда заключаем, что все производные многочлена $h(x) = g(-x)$ в точке $x = 3$ неотрицательны. Поэтому все отрицательные корни многочлена g лежат в интервале $(-3, 0)$. Поскольку старший коэффициент многочлена g равен 1, то рациональные корни многочлена g принадлежат множеству $\{-2, -1, 0, 1, 2\}$. Поскольку в указанном множестве нет корней многочлена g, то многочлен g не имеет рациональных корней.

Пусть $f(x) = -g^*(-x)$, где $g^*(x) = x^8 g\left(\frac{1}{x}\right)$ — двойственный многочлен к многочлену g. В силу принципа двойственности в теории приводимости многочленов [13, теоре-

ма 2], достаточно доказать неприводимость многочлена f над $\mathbb{Q}$. Очевидно, что выше приведенные рассуждения показывают отсутствие рациональных корней у многочлена f.

Теперь покажем, что вещественные корни многочлена f лежат в интервале (-2,2). Действительно, имеем $f(x) = (x-2)F(x) + 355$, где $F(x)$ — многочлен с положительными коэффициентами. Поэтому все производные многочлена f в точке $x = 2$ неотрицательны. С другой стороны, $f(-x) = (x-2)Q(x) + 2739$, где $Q(x)$ — многочлен с положительными коэффициентами. Поэтому все производные многочлена $h(x) = f(-x)$ в точке $x = 2$ неотрицательны. Это и означает, что корни многочлена f лежат в интервале $(-2, 2)$.

Предположим, что многочлен f приводим над $\mathbb{Q}$. Тогда по известной лемме Гаусса [15, гл. 8, § 1, теорема 4] найдутся такие целочисленные многочлены φ и ψ, что $f = \varphi\psi$. Пусть сначала степень многочлена φ четна. Тогда можно считать, что $\varphi(-2) > 0$, $\varphi(2) > 0$. Имеем $f(2) = 5 \cdot 71$.

Предположим, что $\varphi(2) = 5$. Покажем, что $\varphi(0) = -1$. В самом деле, в противном случае, из определения разделенной разности $\varphi(2; 0; -2)$ следовало бы, что $\varphi(-2)$ — положительное число вида $8k - 3$, которое делит $f(-2) = 3 \cdot 11 \cdot 83$. Поскольку число $f(-2)$ не имеет натуральных делителей вида $8k - 3$, то это невозможно. Полученное противоречие показывает, что $\varphi(0) = -1$.

Тогда из определения разделенной разности $\varphi(2; 0; -2)$ следует, что $\varphi(-2)$ — положительное число вида $8k + 1$, которое делит $f(-2)$. Поэтому $\varphi(-2) \in \{1, 33, 249, 913\}$. Предположим, что $\varphi(-2) \in \{33, 913\}$. Тогда из определения разделенной разности $\varphi(2; 0; -2; 3)$ следует, что $\varphi(3)$ — положительное число вида $15k - 7$, которое делит $f(3) = 4 \cdot 41 \cdot 241$. Полученное противоречие показывает, что $\varphi(-2) \in \{1, 249\}$.

Тогда из определения разделенной разности $\varphi(2; 0; -2; 3; 4)$ следует, что $\varphi(4)$ — положительное число вида $48k + 19$ или $48k - 21$, которое делит $f(4) = 3 \cdot 53 \cdot 3217$. Поскольку число $53 \cdot 3217$ не имеет натуральных делителей вида $48k + 19$, $16k - 7$, то случай $\varphi(-2) \in \{1, 249\}$ невозможен.

Итак, можно считать, что $\varphi(2) = 1$. Покажем, что $\varphi(0) = 1$. В самом деле, в противном случае, из определения разделенной разности $\varphi(2; 0; -2)$ следовало бы, что $\varphi(-2)$ — положительное число вида $8k - 3$, которое делит $f(-2)$. Поскольку число $f(-2)$ не имеет натурального делителя вида $8k - 3$, то $\varphi(0) = 1$.

Теперь из определения разделенной разности $\varphi(2; 0; -2)$ следует, что $\varphi(-2)$ — положительное число вида $8k + 1$, которое делит $f(-2)$. Поэтому $\varphi(-2) \in \{1, 33, 249, 913\}$. Предположим, что $\varphi(-2) \in \{33, 913\}$. Тогда из определения разделенной разности $\varphi(2; 0; -2; 3)$ следует, что $\varphi(3)$ — положительное число вида $15k - 2$, которое делит $f(3)$. Поскольку число $f(3)$ не имеет натуральных делителей вида $15k - 2$, то $\varphi(-2) \in \{1, 249\}$.

Тогда из определения разделенной разности $\psi(2; 0; -2; 3)$ следует, что 3 делит чис-

ло $\psi(3)$. Полученное противоречие с условием $f(3) = \varphi(3)\psi(3)$ завершает рассмотрение случая, когда $\deg\varphi$ — четное число.

Итак, можно считать, что степень многочлена φ нечетна, $\varphi(-2) < 0,\ \ \varphi(2) > 0$. Предположим, что $\varphi(2) = 5$. Покажем, что $\varphi(0) = 1$. В самом деле, в противном случае, из определения разделенной разности $\varphi(2;0;-2)$ следовало бы, что $-\varphi(-2)$ — положительное число вида $8k-1$, которое делит $f(-2)$. Поскольку число $f(-2)$ не имеет натуральных делителей вида $8k-1$, то $\varphi(0) = 1$.

Тогда из определения разделенной разности $\varphi(2;0;-2)$ следует, что $-\varphi(-2)$ — положительное число вида $8k+3$, которое делит $f(-2)$. Поэтому $-\varphi(-2) \in \{3, 11, 83, 3{\cdot}11{\cdot}83\}$. Тогда из определения разделенной разности $\varphi(2;0;-2;3;4)$ следует, что $\varphi(4)$ — положительный делитель числа $f(4)$ одного из видов: $48k+1,\ \ 48k+9,\ \ 48k-23$. Так как число $53 \cdot 3217$ не имеет натуральных делителей вида $16k+3$ и $48k-23$, то $\varphi(-2) = -11$, $\varphi(4) = 3217$.

Предположим, что $\varphi(3) = 4$. Так как многочлен f не имеет рациональных корней, то либо степень многочлена φ равна 3, либо степень многочлена ψ равна 3. Оба случая невозможны, поскольку ни $\varphi(2;0;-2;4)$, ни $\psi(2;0;-2;3)$ не являются делителями старшего коэффициента многочлена f. Итак, $\varphi(3) \neq 4$.

Теперь из определения разделенной разности $\varphi(2;0;-2;3)$ следует, что $\varphi(3)$ — положительное число вида $15k+4$, которое делит $f(3)$. Поэтому $\varphi(3) \in \{4, 4 \cdot 241\}$. Значит, $\varphi(3) = 4 \cdot 241$. Тогда $\psi(3) = 41$, а из определения разделенной разности $\psi(2;0;-2;3)$ следует, что $\psi(3)$ — положительное число вида $15k+1$. Полученное противоречие завершает рассмотрение случая $\varphi(2) = 5$.

Можно считать, что $\varphi(2) = 355$. Покажем, что $\varphi(0) = 1$. В самом деле, в противном случае, из определения разделенной разности $\varphi(2;0;-2)$ следовало бы, что $-\varphi(-2)$ — положительное число вида $8k-3$, которое делит $f(-2)$. Поскольку число $f(-2)$ не имеет натуральных делителей вида $8k-3$, то случай $\varphi(0) = -1$ невозможен.

Теперь из определения разделенной разности $\varphi(2;0;-2)$ следует, что $-\varphi(-2)$ — положительное число вида $8k+1$, которое делит $f(-2)$. Поэтому $-\varphi(-2) \in \{1, 33, 249, 913\}$. Тогда из определения разделенной разности $\varphi(2;0;-2;3;4)$ следует, что $\varphi(4)$ — положительное число, делящее $f(4)$, одного из видов: $48k-3,\ \ 48k+5,\ \ 48k+21$. Так как число $53 \cdot 3217$ не имеет натуральных делителей вида $16k-1,\ \ 16k+7$, то $-\varphi(-2) \in \{1, 913\}$. Тогда из определения разделенной разности $\psi(2;0;-2;3;4)$ следует, что $\psi(4)$ — положительное число вида $48k+3$, которое делит $f(4)$. Поэтому $\psi(4) = 3$. Снова либо φ — кубический многочлен, либо ψ — кубический многочлен. Оба случая невозможны, поскольку ни $\psi(2;0;-2;4)$, ни $\varphi(2;0;-2;4)$ не являются делителями старшего коэффициента многочлена f. Полученное противоречие завершает доказательство леммы.

Лемма 2.3. *Пусть целочисленный многочлен f обладает следующим свойством: найдется комплексное число симметричное относительно единичной к корню многочлена*

f, не являющееся его корнем. Если по крайней мере один корень многочлена f лежит на единичной окружности, то многочлен f приводим над $\mathbb{Q}$.

ДОКАЗАТЕЛЬСТВО. Пусть $f = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$, $f^* = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 = a_n(x - x_1^*)\ldots(x - x_n^*)$, где корни многочлена f^* связаны с корнями x_i многочлена f соотношениями $x_i^* = \frac{1}{\overline{x_i}}$. Если x_0 — такой корень многочлена f, что $|x_0| = 1$, то $x_0^* = x_0$. Значит, x_0 — корень многочлена $h = (f, f^*) \in \mathbb{Q}[x]$ и $1 \leq \deg h < n$. Так как многочлен h делит f, то многочлен f приводим над $\mathbb{Q}$. Лемма доказана.

Замечание. Известно несколько семейств унитарных многочленов, для которых верно и обращение этой леммы. Наиболее простое из них следующее: $x^n + ax \pm 1$, $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Полностью описаны корни из 1, которые являются причиной приводимости над $\mathbb{Q}$ многочленов из этого семейства [24, теоремы 1, 2], и показано, что других причин нет, то есть частное многочлена из указанного семейства от деления на множитель, состоящий из всех корней, лежащих на единичной окружности, является неприводимым над $\mathbb{Q}$ многочленом. Это обстоятельство дает один путь к построению семейства неприводимых многочленов сколь угодно большой степени. С другой стороны, определенные способы варьирования коэффициентов многочлена, основанные на теореме Руше, не изменяют указанный множитель. Иногда единственной причиной приводимости проварьированного многочлена остаются все те же корни из 1. Это дает другой путь к построению семейства неприводимых многочленов сколь угодно большой степени. Реализацию этого второго пути мы проиллюстрируем в доказательстве следующего утверждения.

Лемма 2.4. *Пусть $n \geq 3$. Тогда многочлен $x^n + 9x^{n-1} + \ldots + 9x^2 + 5x + 3$ неприводим над $\mathbb{Q}$.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим многочлен $f = x^{n+1} - 2x^n + 1 = (x - 1)g$. Известно, что многочлен g неприводим над $\mathbb{Q}$ [24, теорема 2]. В частности, $x_0 = 1$ — простой корень многочлена f. Тогда по правилу Декарта многочлен f имеет другой положительный корень. Последнее обстоятельство позволяет нам сделать два важных наблюдения. Во-первых, по лемме 2.3 многочлен g не имеет корней на единичной окружности. Во-вторых, по крайней мере n корней многочлена f лежат в области $|z| \leq 1$ [25, теорема 9.8]. Поскольку не все корни многочлена f лежат на единичной окружности, то многочлен f имеет ровно n корней в области $|z| \leq 1$ [14, задача 867].

Итак, многочлен g имеет ровно $n - 1$ корней в области $|z| < 1$. Пусть $h = (x + 2)f$. Применяя второе правило Кона к многочлену h [25, гл. 11, § 5], получим, что многочлен $q = -2h + h^* = x^{n+1} + 8x^n - 4x^2 - 2x - 3$ имеет ровно $n - 1$ корней в области $|z| < 1$. Значит, многочлен $\frac{q}{x-1}$ имеет ровно $n - 1$ корней в области $|z| < 1$. По правилу Декарта многочлен q имеет единственный положительный корень, который, поэтому, совпадает с единицей. Поскольку $q(-1) \neq 0$, то исследуемый многочлен имеет единственный корень в области $|z| > 1$. Теперь из унитарности исследуемого многочле-

на, как заметил Перрон [23], следует его неприводимость над $\mathbb{Q}$. В самом деле, если бы он был приводим, то по лемме Гаусса нашелся бы целочисленный унитарный его делитель, имеющий все корни в области $|z| < 1$. Согласно теореме Виета таких делителей не существует. Лемма доказана.

Замечание. Сравним какая из двух задач разложения на неприводимые множители сложнее: для многочлена из этой леммы или для многочлена v, указанного в начале параграфа. По теореме Пеле существует единственный корень x_0 многочлена v, лежащий в области $|z| \geq 1$. Так как $v(\pm 1) \neq 0$, то $|x_0| > 1$. Теперь продемонстрированный в доказательстве последней леммы аргумент О. Перрона показывает неприводимость многочлена v над $\mathbb{Q}$. В то же время, применение теоремы Пеле к любому многочлену из леммы 2.4 ничего не дает.

Лемма 2.5. *Пусть $n \geq 4$, $\varepsilon \in \{-1, 1\}$. Тогда многочлены $x^n + 4\varepsilon x^{n-1} + 2x^{n-2} - \varepsilon x - 1$, $x^n - 4\varepsilon x^{n-1} - 2x^{n-2} + \varepsilon x + 3$ неприводимы над $\mathbb{Q}$.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим многочлен $f(x) = x^n + ax^{n-1} + 1$. Известно, что при целом значении параметра a многочлен f имеет ровно $n - 1$ корней в области $|z| < 1$ для любого a такого, что $|a| \geq 3$ [25, теорема 9.8]. Тогда многочлен $h_\varepsilon = (2x + \varepsilon)f$ имеет n корней в области $|z| < 1$. По первому правилу Кона [25, гл. 11, § 5] многочлен $2h_\varepsilon - h_\varepsilon^*$ имеем ровно n корней в области $|z| < 1$. Полагая $a = \pm 3$, получим унитарные многочлены $f_\varepsilon = x^n + 4\varepsilon x^{n-1} + 2x^{n-2} - \varepsilon x - 1$, $g_\varepsilon = x^n - 4\varepsilon x^{n-1} - 2x^{n-2} + \varepsilon x + 3$. По правилу Декарта многочлен f_ε имеет по крайней мере один положительный корень и $f_\varepsilon(1) \neq 0$. Поэтому не все корни многочлена f_ε лежат на единичной окружности, и это же заключение справедливо относительно многочлена g_ε, так как $g_\varepsilon(0) = 3$. Если бы все корни многочлена f_ε (g_ε) лежали в области $|z| \leq 1$, они были бы корнями из 1 [14, задача 867]. Полученное противоречие с установленными выше свойствами корней многочлена f_ε (g_ε) показывает, что ровно один корень многочлена f_ε (g_ε) лежит в области $|z| > 1$. Продемонстрированный выше аргумент Перрона завершает доказательство леммы.

Лемма 2.6. *Пусть $\varepsilon \in \{-1, 1\}$, $p > 2$, $n > 2$. Тогда ровно $n - 2$ корней многочлена $x^n + px^{n-2} + \varepsilon$ лежат в области $|z| < 1$ и вне ее нет вещественных корней этого многочлена. В частности, указанный многочлен неприводим над $\mathbb{Q}$.*

ДОКАЗАТЕЛЬСТВО. Сначала покажем, что все вещественные корни многочлена $f = x^n + px^{n-2} + \varepsilon$ лежат в интервале $(-1, 1)$. Пусть $f(x_0) = 0$, $x_0 \in \mathbb{R}$. Заменяя $f(x)$ на $(-1)^n f(-x)$, можно считать, что $x_0 > 0$. Поскольку функция $f(x)$ возрастает при положительных значениях аргумента, то $f(x) \geq f(1) > 0$ при любом $x \geq 1$. Поэтому $x_0 < 1$.

Теперь по правилу Декарта многочлен $g = x^n - px^{n-2} + 1$ имеет либо два положительных корня, либо не имеет ни одного положительного корня. Последняя ситуация

невозможна, поскольку $g(1) = 2 - p < 0$. Тогда по теореме Пеле [25, теорема 9.8] ровно $n - 2$ корней многочлена f лежат в области $|z| < 1$.

Наконец, из унитарности исследуемого многочлена, как заметил Перрон [23], следует его неприводимость над $\mathbb{Q}$. В самом деле, если бы он был приводим, то по лемме Гаусса многочлен f можно было бы представить в виде произведения двух унитарных целочисленных многочленов, один из которых содержал бы ту единственную пару комплексно сопряженных корней с наибольшим модулем. Тогда все корни другого многочлена лежали бы в области $|z| < 1$. Согласно теореме Виета такого унитарного целочисленного многочлена не существует. Лемма доказана.

Унитарный делитель целочисленного унитарного многочлена f, который образуют все корни, лежашие на единичной окружности обозначим через f_0. В случае, когда многочлен f не имеет корней на единичной окружности, полагаем $f_0 = 1$.

Лемма 2.7. *Пусть* $\varepsilon \in \{-1, 1\}$, $f = x^n + ax^{n-r} + \varepsilon \in \mathbb{Z}[x]$, $d = (n, r)$, *многочлен* g *определяется равенством* $g(x^d) = f(x)$. *Тогда и только тогда* $f_0 \neq 1$, *когда либо* $a = 0$; *либо* $|a| = 1$, 3 *делит* $n + r$ *и* $g_0 = x^2 \pm x + 1$; *либо* $|a| = 2$, $g_0 = x \pm 1$ *или* $g = (x \pm 1)^2$.

ДОКАЗАТЕЛЬСТВО. Пусть $f(\alpha) = 0$, $|\alpha| = 1$. Можно считать, что $a \neq 0$. Тогда $\alpha^{n-r}(\alpha^r + a) + \varepsilon = 0$ и $|\alpha^r + a| = 0$. Поскольку точка α^r лежит на пересечении окружности радиуса 1 с центром в целой точке и единичной окружности, то $|a| \leq 2$. Пусть $|a| = 2$. Тогда $\alpha^r = \varepsilon_0 \in \{-1, 1\}$, $\alpha^n = \frac{-\varepsilon_0 \varepsilon}{a + \varepsilon_0}$. Так как $|\alpha| = 1$, то $|a + \varepsilon_0| = 1$ и $\alpha^{2n} = 1$. Поскольку $(2n, 2r) = 2d$, то $(\alpha^d)^2 - 1 = 0$ и один из двучленов $(x \pm 1)$ делит $g = x^{n_1} + ax^{n_1 - r_1} + \varepsilon$.

Покажем, что двучлен $x^2 - 1$ не делит g_0. В самом деле, в противном случае нашлись бы корни α, β многочлена f, лежащие на единичной окружности, такие, что $\alpha^d = 1$, $\beta^d = -1$. Из соотношения $\alpha^r = 1$ следует $\alpha^n = \frac{-\varepsilon}{a+1}$. Значит, $a = -2$, $\varepsilon = -1$. Из соотношения $\beta^d = -1$ следует альтернатива: $\beta^r = -1$ или $\beta^n = -1$. Если $\beta^n = -1$, то $\beta^r = 1$ и $\beta^n = -\frac{\varepsilon}{a+1} = 1$, что невозможно. Если $\beta^r = -1$, то $\beta^n = \frac{+\varepsilon}{a-1} = \frac{1}{3}$, что также невозможно. Полученное противоречие, с учетом произвольного выбора корня многочлена f, показывает, что g_0 — некоторая степень одного из двучленов $(x \pm 1)$.

Пусть теперь многочлен g_0 без кратных корней, тогда он имеет единственный корень и поэтому $g_0 = x \pm 1$.

Пусть, наконец, x_0 — кратный корень многочлена g_0. Приравнивая к нулю значение производной g' в точке x_0, получаем $n_1 = 2(n_1 - r_1)$. Из соотношения $g(x_0) = 0$ следует, что $\varepsilon = 1$ и $g = (x \pm 1)^2$.

Наконец, пусть $|a| = 1$. Если $f_0 = f$, то ввиду соотношений $f(-1) \neq 0 \neq f(1)$ имеем f — возвратный многочлен четной степени. Значит, $g_0 = x^2 - x + 1$ или $g_0 = x^2 + x + 1$.

Пусть $f_0 \neq f$. Тогда трехчлен f приводим над $\mathbb{Q}$ по лемме 2.3. По критерию неприводимости [26, теорема 3], тогда $n + r \equiv 0 \pmod 3$, $x^2 + \tau x - 1$ делит g_0 при некотором $\tau \in \{-1, 1\}$ и многочлен $q = \frac{g}{x^2 + \tau x + 1}$ неприводим. Если бы $g_0 \neq x^2 + \tau x + 1$, то много-

член q имел бы по крайней мере один корень на единичной окружности, а из условия $g_0 \neq g$ и леммы 2.3 следовала бы приводимость q. Полученное противоречие завершает доказательство леммы.

Пусть $\mathcal{K}_n$ — множество таких целочисленных многочленов f с ненулевым свободным членом, что f — сумма n одночленов, абсолютные значения коэффициентов которых равны 1.

Предложение 2.1 [26, лемма 1]. *Пусть $f \in \mathcal{K}_4$. Если четырехчлен f приводим над $\mathbb{Q}$, то f имеет такой целочисленный множитель φ, что $(\varphi^*)^2 = \varphi^2$.*

Нам понадобится также следующая альтернатива [26, лемма 2], которую мы переформулируем в симметричном виде.

Предложение 2.2. *Пусть заданы три различных натуральных числа n, m, p; ε_n, ε_m, $\varepsilon_p \in \{-1, 1\}$. Если оба числа λ и λ^{-1} являются корнями уравнения $\varepsilon_n x^n + \varepsilon_m x^m + \varepsilon_p x^p + 1 = 0$, то либо $\lambda^n = -\varepsilon_n$ и $\lambda^{m-p} = -\varepsilon_n\varepsilon_p$, либо $\lambda^m = -\varepsilon_m$ и $\lambda^{n-p} = -\varepsilon_n\varepsilon_p$, либо $\lambda^p = -\varepsilon_p$ и $\lambda^{n-m} = -\varepsilon_n\varepsilon_m$.*

Замечание. Если сумма коэффициентов многочлена f из предложения 2.1 не равна нулю, то можно дополнительно утверждать возвратность указанного множителя φ. В самом деле, из предложения 2 следует, что все корни многочлена φ лежат на единичной окружности. Поскольку $f(1) \neq 0$, то φ — произведение многочлена четной степени на степень возвратного многочлена $x + 1$, и поэтому φ — возвратный многочлен.

Теорема 2.1. *Пусть n, m, p — различные натуральные числа, $d = (n, m, p)$. Пусть целочисленный четырехчлен f имеет вид: $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, $|\varepsilon_1| = |\varepsilon_2| = |\varepsilon_3| = 1$. Пусть многочлен g, определяемый равенством $g(x^d) = f(x)$, удовлетворяет условию: $g(-1) \neq 0 \neq g(1)$. Многочлен f является приводимым над $\mathbb{Q}$ тогда и только тогда, когда выполнены следующие условия: а) ненулевая четная степень переменной x в g единственна; б) $g(c) = 0$, где c — корень из -1 степени, равной наибольшему общему делителю четной степени в g и разности нечетных степеней многочлена g.*

Прежде чем дать доказательство этой теоремы, докажем одну теоретико-групповую лемму. Напомним, что в произвольной группе инволюцией называется неединичный элемент второго порядка.

Лемма 2.8. *Пусть n — нечетное число. Тогда в группе $\mathbb{C}_n$ всех корней из 1 степени n нет инволюций.*

ДОКАЗАТЕЛЬСТВО. В противном случае, в группе $\mathbb{C}_n$ нечетного порядка нащлась бы подгруппа порядка 2, порожденная этой инволюцией, что противоречит теореме Лагранжа [9, теорема 2.4.5].

ДОКАЗАТЕЛЬСТВО (Теоремы 2.1). Пусть $f = x^{n_1} + \varepsilon_1 x^{m_1} + \varepsilon_2 x^{p_1} + \varepsilon_3$, $n_1 = n_2 d$, $m_1 = m_2 d$, $p_1 = p_2 d$. Через n обозначим один нечетный элемент множества $\{n_2, m_2, p_2\}$;

если существует другой нечетный элемент этого множества, то мы его обозначим через p, а оставшийся элемент через m. Если же другого нечетного элемента не нащлось, то через m и p обозначим четные элементы множества $\{n_2, m_2, p_2\}$. Предположим, что многочлен f приводим. Поскольку $f(1) \neq 0$, то по предложению 1, с учетом сделанного замечания, многочлен f имеет возвратный целочисленный множитель. Пусть λ — корень этого множителя. Тогда оба числа λ^d и λ^{-d} являются корнями уравнения: $\varepsilon'_n x^n + \varepsilon'_m x^m + \varepsilon'_p x^p + 1 = 0$; $\varepsilon'_n, \varepsilon'_m, \varepsilon'_p \in \{-1, 1\}$. Поэтому оба числа $\mu = \varepsilon'_n \lambda^d$ и μ^{-1} являются корнями уравнения $x^n + \varepsilon_m x^m + \varepsilon_p x^p + 1 = 0$; $\varepsilon_m, \varepsilon_p \in \{-1, 1\}$. Ввиду указанной альтернативы выполнено одно из следующих условий: а) $\mu^n = -1$ и $\mu^{m-p} = -\varepsilon_p \varepsilon_m$; б) $\mu^m = -\varepsilon_m$ и $\mu^{n-p} = -\varepsilon_p$; в) $\mu^p = -\varepsilon_p$ и $\mu^{n-m} = -\varepsilon_m$.

Пусть сначала $\varepsilon_m = \varepsilon_p = 1$. Ввиду условий $g(-1) \neq 0 \neq g(1)$ можно считать, что количество нечетных степеней в многочлене g нечетно. Тогда по альтернативе найдется такой элемент $\nu \in \mathbb{C}_{\overline{n}}$, $\overline{n} \in \{|n - m + p|, |m - n + p|\}$, что $\nu^s = -1$ для некоторого $s \in \mathbb{N}$. Получили противоречие с предыдущей леммой.

Итак, можно, учитывая условия $g(-1) \neq 0 \neq g(1)$, считать, что $\varepsilon_m \varepsilon_p = -1$. Теперь из этих же условий следует, что выполнено условие а) теоремы. Тогда по определению p нечетно.

1. Пусть $\varepsilon_p = -1$. Тогда реализация альтернативных пунктов а) и в) приводит к существованию инволюции в группе $\mathbb{C}_n$ и $\mathbb{C}_p$, соответственно, что противоречит предыдущей лемме. Поэтому $\mu^m = -1$, $\mu^{n-p} = 1$. Обозначим $d_0 = (m, n - p)$, $\nu = \mu^{d_0}$. Тогда $\nu^{\frac{m}{d_0}} = -1$, $\nu^{\frac{n-p}{d_0}} = 1$ и порядок элемента ν делит $\left(2\frac{m}{d_0}, \frac{n-p}{d_0}\right) = 2$. Значит, $\nu^2 = 1$, $\nu = -1$. Получили, что выполнено условие б) теоремы.

Итак, можно считать, что $\varepsilon_p = 1$, $\varepsilon_m = -1$. Теперь реализация пунктов а) и в) альтернативы приводит к существованию инволюции в группе $\mathbb{C}_n$ и $\mathbb{C}_{n-m}$, соответственно, что опять невозможно. Далее, аналогично тому, как был разобран случай 1, показывается выполнение условия б) теоремы.

Докажем теперь импликацию в противоположную сторону. Пусть у многочлена g ненулевая нечетная степень единственна и корнем многочлена g является некоторый корень из -1. Предположим, что многочлен f неприводим. Значит, многочлен g неприводим тоже. Тогда неприводимость многочлена g и наличие у него корня на единичной окружности позволяет на основании леммы 2.3 сделать вывод, что все корни многочлена g лежат на единичной окружности, откуда, с учетом условий $g(-1) \neq 0 \neq g(1)$, выводим, что g — возвратный многочлен четной степени, удовлетворяющий условию а) теоремы. Поскольку возвратного четырехчлена, удовлетворяющего условию а), не существует, то теорема полностью доказана.

Замечание. При $n < 6$ множество многочленов $\mathcal{K}_n$ обладает определенной замкнутостью. Более точно, приводимость элемента $f \in \mathcal{K}_n$ влечет двойное разложение многочлена ff^*, причем оба сомножителя второго разложения опять принадлежат множеству

$\mathcal{K}_n$ и имеют степень, равную $\deg f$. Отсюда при $n = 4$ в [26] выведен факт, который мы назвали предложением 1. Отсюда, по-видимому, можно вывести аналогичный результат при $n = 5$, что сделает несложной задачу полного описания неприводимых над $\mathbb{Q}$ многочленов из $\mathcal{K}_5$.

При $n = 6$ отмеченной замкнутости уже нет. Мешают примеры (хотя и очень редкие) такого сорта: $f = x^7 + x^6 - x^3 + x^2 + x - 1$, $g = x^7 - 2x^5 - 1$, $ff^* = gg^*$. Поэтому для достижения желаемой замкнутости $\mathcal{K}_n$ при $n \geq 6$ потребуется наложить, по крайней мере, такое дополнительное ограничение: приводимый многочлен f не должен иметь целых корней.

§ 3. Старший коэффициент матричной экспоненты

Пусть $x_1, \ldots, x_n$ различные точки из $\mathbb{R}$, $f : \mathbb{R} \to \mathbb{R}$ — бесконечно дифференцируемая функция. Обобщением понятия производной является понятие разделенной разности. Разделенные разности нулевого порядка $f(x_i)$ совпадают со значениями функций $f(x_i)$; разделенные разности первого порядка определяются равенством $f(x_i; x_j) = \dfrac{f(x_j) - f(x_i)}{x_j - x_i}$; разности k-го порядка $f(x_1; \ldots; x_{k+1})$ определяются через разности $(k-1)$-го порядка по формуле

$$f(x_1; \ldots; x_{k+1}) = \frac{f(x_2; \ldots; x_{k+1}) - f(x_1; \ldots; x_k)}{x_{k+1} - x_k}\,.$$

Лемма 3.1 [16, глава 2, § 3]. *Справедливо равенство*

$$f(x_1; \ldots; x_k) = \sum_{j=1}^{k} \frac{f(x_j)}{\prod\limits_{i \neq j} (x_j - x_i)}\,.$$

Лемма 3.2. *Пусть $L_n(x)$ — интерполяционный многочлен Лагранжа, приближающий функцию $f(x)$, с узлами интерполяции $x_1, \ldots, x_n$. Тогда*
$f(x) - L_n(x) = f(x; x_1; \ldots; x_n)(x - x_1)\ldots(x - x_n)$. *Кроме того,*
$L_n(x) = f(x_1) + f(x_1; x_2)(x - x_1) + \ldots + f(x_1; \ldots; x_n)(x - x_1)\ldots(x - x_{n-1})$.

ДОКАЗАТЕЛЬСТВО. Имеем

$$f(x) - L_n(x) = f(x) - \sum_{i=1}^{n} f(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} =$$

$$= \prod_{i=1}^{n} (x - x_i) \left(\frac{f(x)}{\prod\limits_{i=1}^{n} (x - x_i)} + \sum_{i=1}^{n} \frac{f(x_i)}{(x_i - x) \prod\limits_{j \neq i} (x_i - x_j)} \right)\,.$$

Сравнение с формулой из леммы 3.1 завершает доказательство первого утверждения леммы.

Пусть $L_m(x)$ — интерполяционный многочлен Лагранжа с узлами интерполяции $x_1, \ldots, x_m$. Многочлен $L_n(x)$ можно представить в виде

$$L_n(x) = L_1(x) + (L_2(x) - L_1(x)) + \ldots + (L_n(x) - L_{n-1}(x)).$$

Разность $L_m(x) - L_{m-1}(x)$ есть многочлен степени $m-1$, обращающийся в нуль в точках $x_1, \ldots, x_{m-1}$, поскольку $L_{m-1}(x_j) = L_m(x_j)$ при $1 \le j \le m-1$. Следовательно, $L_m(x) - L_{m-1}(x) = A_{m-1}\omega_{m-1}(x)$, $\omega_{m-1}(x) = (x - x_1)\ldots(x - x_{m-1})$, $A_{m-1} = const$. Полагая $x = x_m$, получим $f(x_m) - L_{m-1}(x_m) = A_{m-1}\omega_{m-1}(x_m)$. Согласно доказанному первому утверждению $A_{m-1} = f(x_i; \ldots; x_m)$. Подстановка последнего выражения для коэффициентов A_{m-1} в указанную выше формулу для многочлена $L_n(x)$ завершает доказательство леммы 3.2.

Интерполяционный многочлен, записанный в форме, полученной в лемме 3.2, называют интерполяционным многочленом Ньютона с разделенными разностями. Непосредственным следствием леммы 3.2 и хорошо известного факта (см. предложение 3.1) является следующее утверждение.

Лемма 3.3. *Пусть f — бесконечно дифференцируемая функция. Тогда* $f(x; x_1; \ldots; x_n) = \dfrac{f^{(n)}(\xi)}{n!}$, *где* $\min\{x, x_1, \ldots, x_n\} \le \xi \le \max\{x, x_1, \ldots, x_n\}$.

Теперь уместно отметить следующее свойство разделенных разностей.

Лемма 3.4. *Значение разделенной разности целочисленного многочлена f в различных целых узлах интерполяции является целым числом.*

ДОКАЗАТЕЛЬСТВО. Утверждение леммы будем доказывать индукцией по степени n многочлена f. Основание индукции при $n = 0$, очевидно, выполняется. Предположим, что для всех многочленов, степень которых меньше n, утверждение леммы справедливо.

Пусть $x_1, \ldots, x_{n+1}$ — различные целые точки $f = a_0x^n + \ldots + a_n$. Очевидно, что интерполяционный многочлен Лагранжа $L_{n+1}(x)$, приближающий функцию $f(x)$, с узлами интерполяции $x_1, \ldots, x_{n+1}$ совпадает с многочленом $f(x)$. Тогда из леммы 3.2 следует, что $f(x_1; \ldots; x_{n+1})$ — старший коэффициент многочлена f. По условию это число целое. Значит, $g = f - f(x_1; \ldots; x_{n+1})(x - x_1)\ldots(x - x_n)$ — это целочисленный многочлен, степень которого меньше n. По предположению индукции $g(x_1; \ldots; x_i)$, $i = 1, \ldots, n$, — целые числа. Кроме того, $g(x_i) = f(x_i)$, $i = 1, \ldots, n$. Поэтому искомые разделенные разности, порядки которых меньше n, являются целыми числами. Разделенные разности порядков больших n равны 0 по лемме 3.3. Лемма доказана.

Разделенные разности позволяют взглянуть с иной стороны и на многочлен Лагранжа-Сильвестера. Пусть требуется построить многочлен $g_s(x)$ степени $s-1$, удовлетворяющий условиям: $g_s(x_1) = f(x_1), \ldots, g_s^{(m_1-1)}(x_1) = f^{(m_1-1)}(x_1); \ldots;$ $g_s(x_n) = f(x_n), \ldots,$ $g_s^{(m_n-1)}(x_n) = f^{(m_n-1)}(x_n)$; здесь все x_i различные, $s = m_1 + \ldots + m_n$. Хорошо извест-

но, что указанная задача имеет единственное решение — соответствующий многочлен Лагранжа-Сильвестера. Кроме того, справедливо следующее утверждение.

Предложение 3.1 [16, глава 2, § 7, задача 2]. *Справедливо равенство*

$$f(x) - g_s(x) = \frac{f^{(s)}(\xi)}{s!}\prod_{i=1}^{n}(x - x_i)^{m_i}, y_1 \le \xi \le y_2, \text{где}$$

$$y_1 = \min\{x, x_1, \ldots, x_n\}, y_2 = \max\{x, x_1, \ldots, x_n\}.$$

Пусть $\varepsilon > 0$, $g_s^\varepsilon(x)$ — интерполяционный многочлен степени $s-1$, совпадающий с $f(x)$ в точках $x_{ij}^\varepsilon = x_i + (j-1)\varepsilon$, $i = 1, \ldots, n$, $j = 1, \ldots, m_i$.

Лемма 3.5. *Многочлены $g_s(x)$ и $\lim\limits_{\varepsilon\to 0} g_s^\varepsilon(x)$ совпадают.*

ДОКАЗАТЕЛЬСТВО. Пусть $A_0^\varepsilon = f(x_{11}^\varepsilon)$, $A_1^\varepsilon = f(x_{11}^\varepsilon; x_{12}^\varepsilon), \ldots$, $A_{s-1}^\varepsilon = f(x_{11}^\varepsilon; x_{12}^\varepsilon; \ldots$ $\ldots; x_{nm_n}^\varepsilon)$. Тогда интерполяционная формула с разделенными разностями для многочлена $g_s^\varepsilon(x)$ примет вид:

$$g_s^\varepsilon(x) = A_0^\varepsilon + A_1^\varepsilon(x - x_{11}^\varepsilon) + A_2^\varepsilon(x - x_{11}^\varepsilon)(x - x_{12}^\varepsilon) + \ldots$$
$$\ldots + A_{s-1}^\varepsilon(x - x_{11}^\varepsilon)\ldots(x - x_{n,m_n-1}^\varepsilon)\,.$$

Пусть $A_i = \lim\limits_{\varepsilon\to 0} A_i^\varepsilon$, $p_s(x) = \lim\limits_{\varepsilon\to 0} g_s^\varepsilon(x)$. Тогда

$$p_s(x) = A_0 + A_1(x - x_1) + A_2(x - x_1)^2 + \ldots$$

$$\ldots + A_{s-1}(x - x_1)^{m_1}\ldots(x - x_{n-1})^{m_{n-1}}(x - x_n)^{m_n - 1}\,.$$

Далее из леммы 3.3 следует, что $\lim\limits_{\varepsilon\to 0} f(x_{11}^\varepsilon; x_{12}^\varepsilon; \ldots; x_{1k}^\varepsilon) = \dfrac{f^{k-1}(x_1)}{(k-1)!}$, $k = 1, \ldots, m_1$. Поэтому многочлен $p_s(x)$ записывается в виде:

$$p_s(x) = \sum_{i=1}^{m_1}\frac{f^{(i-1)}(x_1)}{(i-1)!}(x - x_1)^{i-1} + O((x - x_1)^{m_1})\,.$$

Отсюда вытекает, что он удовлетворяет условиям:

$$p_s(x_1) = f(x_1), \ldots, p_s^{(m_1-1)}(x_1) = f^{(m_1-1)}(x_1)\,.$$

Выберем произвольное число k из $\{2, \ldots, n\}$. Обозначим через τ транспозицию $(1, k)$. Пусть $y_i = x_{i\tau}$, $y_{ij}^\varepsilon = x_{i\tau,j}^\varepsilon$, $q_s^\varepsilon(x)$ — интерполяционный многочлен степени $s-1$, совпадающий с $f(x)$ в точках y_{ij}^ε. Вследствие единственности интерполяционного многочлена имеем $g_s^\varepsilon(x) \equiv q_s^\varepsilon(x)$. Поэтому, рассуждая аналогично предыдущему, заключаем, что $p_s(y_1) = f(y_1), \ldots, p_s^{(m_{1\tau}-1)}(y_1) = f^{(m_{1\tau}-1)}(y_1)$. Поскольку $y_1 = x_k$, $m_{1\tau} = m_k$ и номер k был выбран произвольно, то лемма 3.5 полностью доказана.

Обобщением леммы 3.3 на случай кратных узлов является следующее утверждение.

Лемма 3.6. *Пусть $g_{s+1}(x)$ — интерполяционный многочлен Лагранжа-Сильвестра, приближающий функцию $f(x)$ в узлах интерполяции $x_1, \ldots, x_n$:*

$$g_{s+1}(x_1) = f(x_1), \ldots, g_{s+1}^{(m_1)}(x_1) = f^{(m_1)}(x_1);$$
$$g_{s+1}(x_2) = f(x_2), \ldots, g_{s+1}^{(m_2-1)}(x_2) = f^{(m_2-1)}(x_2); \ldots; g_{s+1}(x_n) =$$
$$= f(x_n), \ldots, g_{s+1}^{(m_n-1)}(x_n) = f^{(m_n-1)}(x_n).$$

Тогда старший коэффициент многочлена $g_{s+1}(x)$ равен $\dfrac{f^{(s)}(\xi)}{s!}$, где $y_1 \le \xi \le y_2$, $y_1 = \min\{x_1, \ldots, x_n\}$, $y_2 = \max\{x_1, \ldots, x_n\}$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varepsilon > 0$. Рассмотрим узлы интерполяции $x_{12}^{\varepsilon}, \ldots, x_{1,m_1+1}^{\varepsilon}$, $x_{21}^{\varepsilon}, \ldots, x_{nm_n}^{\varepsilon}$. Применим к этому набору узлов лемму 3.2: $f(x) - L_n^{\varepsilon}(x) = B_x^{\varepsilon}(x - x_{12}^{\varepsilon}) \ldots$ $\ldots (x - x_{nm_n}^{\varepsilon})$. Обозначим $B_x = \lim\limits_{\varepsilon \to 0} B_x^{\varepsilon}$. Переходя к пределу при $\varepsilon \to 0$, получим: $f(x) - g_s(x) = B_x \prod\limits_{i=1}^{n} (x - x_i)^{m_i}$. Поэтому из предложения следует, что $B_x = \dfrac{f^{(s)}(\xi_x)}{s!}$, где $\min\{x, y_1\} \le \xi_x \le \max\{x, y_2\}$. Кроме того, согласно лемме 3.5, $A_s = \lim\limits_{\varepsilon \to 0} f(x_{11}^{\varepsilon}; \ldots$ $\ldots; x_{1,m_1+1}^{\varepsilon}; \ldots; x_{n,m_n}^{\varepsilon}) = B_{x_1}$. Итак, можно взять $\xi = \xi_{x_1}$. Лемма 3.6 доказана.

Пусть $\psi(\lambda) = (\lambda - \lambda_1)^{r_1}(\lambda - \lambda_2)^{r_2} \ldots (\lambda - \lambda_s)^{r_s}$ — минимальный многочлен матрицы A степени $r = r_1 + r_2 + \ldots + r_s$. Здесь r_k — кратность корня λ_k как корня минимального многочлена $\psi(\lambda)$. Если для функции $f(\lambda)$ существуют числа $f(\lambda_k)$, $f'(\lambda_k)$, $f''(\lambda_k), \ldots, f^{(r_k-1)}(\lambda_k)$ $(k = 1, 2, \ldots, s)$, то говорят, что функция $f(\lambda)$ определена на спектре матрицы A и эту систему чисел называют системой значений функции $f(\lambda)$ на спектре матрицы A. Хорошо известно следующее утверждение.

Предложение 3.2 [17, задача 1147]. *Значения многочленов $g(\lambda)$ и $h(\lambda)$ от матрицы A совпадают тогда и только тогда, когда совпадают значения этих многочленов на спектре матрицы A.*

В общем случае, когда $g : \mathbb{C} \to \mathbb{C}$ — произвольная аналитическая функция, совпадение значений функции $g(\lambda)$ и многочлена $h(\lambda)$ на спектре матрицы A означает, что $h(\lambda)$ — интерполяционный многочлен, приближающий функцию $g(\lambda)$ в узлах интерполяции $\lambda_1, \ldots, \lambda_s$. Таким образом, указанное предложение дает в некоторых важных случаях еще один способ для нахождения старшего коэффициента интерполяционного многочлена Лагранжа-Сильвестера.

Пусть $q \in \mathbb{C}_n$, $A \in M_n(\mathbb{C})$, $0 \ne h \in \mathbb{R}$. Будем говорить, что пара (q^*, A) полностью наблюдаема, если строки $q^*, q^*A, \ldots, q^*A^{n-1}$ линейно независимы. Хорошо известно, что $\exp(-hA) = a_0A^{n-1} + a_1A^{n-2} + , \ldots + a_{n-1}E$. Число a_0 назовем старшим коэффициентом экспоненты $\exp(-hA)$.

Сравним старшие коэффициенты экспонент $\exp(A)$ и $\exp(A - \lambda E)$, где λ — произвольное число из $\mathbb{C}$. Имеем $\exp(A - \lambda E) = e^{-\lambda}\exp(A) = e^{-\lambda}(a_0A^{n-1} + \ldots + a_{n-1}) =$

$= e^{-\lambda}a_0B^{n-1} + b_1B^{n-2} + \ldots + b_{n-1} = h(B)$, где $B = A - \lambda E$. Старший же коэффициент экспоненты $\exp(B)$ — это старший коэффициент некоторого многочлена $g(x)$, причем $\deg g < n$.

Согласно предложению из соотношения $g(B) = h(B)$ выводим, что многочлены g и h совпадают на спектре матрицы B. Поскольку $\deg(g - h) < n$, то это означает, что $g \equiv h$. Итак, старший коэффициент экспоненты $\exp(A - \lambda E)$ получается из старшего коэффициента экспоненты $\exp(A)$ умножением на число $e^{-\lambda}$.

Теорема 3.1. *Пусть h — ненулевое вещественное число, A — комплексная матрица и найдется строка, образующая с матрицей A полностью наблюдаемую пару. Если спектр матрицы A лежит на параллельной вещественной оси прямой в комплексной плоскости, то старший коэффициент экспоненты $\exp(-hA)$ отличен от нуля.*

ДОКАЗАТЕЛЬСТВО. Пусть нашлась такая строка $q^*, q \in \mathbb{C}^n$, что строки $q^*, q^*A, \ldots$ $\ldots, q^*A^{n-1}$ образуют базис векторного пространства $(\mathbb{C}^n)^*$. Пусть λ — собственное значение матрицы A и $B = A - \lambda E$. Очевидно, что строки $q^*, q^*B, \ldots, q^*B^{n-1}$ снова будут образовывать базис пространства $(\mathbb{C}^n)^*$. Поэтому, в виду установленной связи между старшим коэффициентом экспоненты $\exp(A)$ и старшим коэффициентом экспоненты $\exp(B)$, можно считать, что прямая, на которой лежит спектр матрицы A, проходит через центр комплексной плоскости.

Сделаем теперь следующее общее замечание, которым не раз будем пользоваться: каждому собственному значению матрицы A в ее жордановой форме соответствует единственная жорданова клетка и размер этой единственной клетки равен кратности этого собственного значения. В самом деле, прямой подсчет матрицы оператора, соответствующего матрице A^*, в базисе $q, A^*q, \ldots, (A^*)^{n-1}q$ (с использованием теоремы Гамильтона-Кэли для A^*) показывает, что ранг матрицы $A - \lambda E$ не меньше $n - 1$ для любого вещественного числа λ. Поэтому для любого собственного значения матрицы A существует единственный (с точностью до пропорциональности) собственный вектор ему отвечающий. Итак, жорданова форма матрицы A имеет указанный вид.

В частности, минимальный многочлен матрицы A совпадает с ее характеристическим многочленом. Поэтому, ввиду сделанного выше замечания, теорема будет доказана, если мы покажем, что для любой матрицы A, образующей с q полностью наблюдаемую пару, с вещественным спектром выполнено следующее: старший коэффициент многочлена степени $< n$, совпадающего с функцией $f(x) = \exp(x)$ на спектре матрицы A, отличен от нуля.

Приведем матрицу A к жордановой форме J: $J = T^{-1}AT$ для некоторой матрицы T из $GL_n(\mathbb{C})$. Поскольку сопряжение матрицей T является автоморфизмом кольца $M_n(\mathbb{C})$, то можно считать, что матрица A совпадает со своей жордановой формой. В частности, $A \in M_n(\mathbb{R})$. Поскольку $(n-1)$-ая производная функции $f(x)$ отлична от нуля , то при-

менение последней леммы к интерполяционному многочлену Лагранжа-Сильвестера, совпадающего с системой значений функции $f(x)$ на спектре матрицы A, завершает доказательство теоремы.

Следующий пример показывает, что условие вещественности собственных значений матрицы A в теореме существенно.

Пример 1. Пусть $h = 1$, $a = -\frac{4}{3\pi}\frac{4e^2 - 3\pi}{9\pi^2 + 16}$, $b = \frac{2}{3\pi}\frac{9\pi^2 e^2 + 24\pi - 16e^2}{9\pi^2 + 16}$, μ — ненулевой корень уравнения $e^{-\mu} = a\mu^2 + b\mu + 1$. Рассмотрим

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & \mu(4 + \frac{9\pi^2}{4}) & 4\mu - 4 - \frac{9\pi^2}{4} & \mu - 4 \end{pmatrix}.$$

Тогда число $-2 + \frac{3}{2}\pi i$ — характеристическое число матрицы A, пара $((1,0,0,0), A)$ полностью наблюдаема и старший коэффициент матрицы e^{-A} равен нулю.

Поскольку прямой способ для нахождения характеристических чисел матрицы A является достаточно громоздким, то для обоснования примера мы пойдем другим путем. Мы убедимся, что $0, \mu, -2 \pm \frac{3}{2}\pi i$ — все характеристические числа матрицы A, воспользовавшись теоремой Виета для корней уравнения четвертой степени со старшим коэффициентом 1. Для вычисления характеристического многочлена матрицы A мы воспользуемся свойством полной наблюдаемости пары $((1,0,0,0), A)$, которое проверяется непосредственно. Пусть $p(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ — характеристический многочлен матрицы A. По теореме Гамильтона-Кэли имеем $A^4 = -a_1A^3 - a_2A^2 - a_3A - a_4E$. Вычисляя теперь строку $(1,0,0,0)A^4$ двумя способами (по определению и через выражение A^4) и пользуясь полной наблюдаемостью указанной пары, заключаем, что $a_1 = -\mu + 4$, $a_2 = 4 + \frac{9\pi^2}{4} - 4\mu$, $a_3 = -\mu(4 + \frac{9\pi^2}{4})$, $a_4 = 0$. Теперь по теореме Виета проверяем непосредственно, что многочлен $x(x - \mu)(x^2 + 4x + 4 + \frac{9\pi^2}{4})$ совпадает с $p(x)$.

Итак, все характеристические числа матрицы A различны. Поэтому для проверки равенства $e^{-A} = aA^2 + bA + E$ достаточно проверить равенство $e^{-\lambda} = a\lambda^2 + b\lambda + 1$ для любого характеристического числа λ матрицы A. Очевидно, что последнее равенство справедливо для $\lambda = 0$. Обоснуем теперь существование такого ненулевого числа μ, что $e^{-\mu} = a\mu^2 + b\mu + 1$. Поскольку $b > 0$, то парабола $y = ax^2 + bx + 1$ не может касаться графика функции $y = e^{-x}$. Поскольку $a < 0$, то ветви параболы $y = ax^2 + bx + 1$ направлены вниз и, поэтому, кроме точки $x = 0$ существует еще одна точка пересечения графиков $y = e^{-x}$ и $y = ax^2 + bx + 1$.

Для завершение обоснования примера, осталось рассмотреть указанное равенство при $\lambda = -2 \pm i\beta$, где $\beta = \frac{3}{2}\pi$. Сначала проверяем, что $(4-\beta^2)a - 2b = -1$, $-4a + b = \frac{e^2}{\beta}$. Пользуясь этими соотношениями, получаем, что $a\lambda^2 + b\lambda + 1 = \pm ie^2(-\sin\beta) = e^{-\lambda}$. Обоснование примера закончено.

Пример 2. Пусть A — нильпотентная матрица, удовлетворяющая условию теоремы. Тогда $a_0 = \frac{(-h)^{n-1}}{(n-1)!}$ отличен от нуля.

Пример 3. Пусть $h = 2\pi$, $n = 3$

$$A = \begin{pmatrix} 1 & 2 & 2 \\ -1 & -2 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

Тогда $a_0 = 0$. В самом деле, легко проверить, что матрица A имеет следующие характеристические числа 0, i, $-i$. Очевидно они должны быть корнями квазиполинома $e^{-hx} - a_0x^2 - a_1x - a_2$. Поэтому $a_0 = 1 - \cos h = 0$.

Литература

[1] *А. А. Коробов*, О нелинейных подгруппах групп автоморфизмов относительно свободных групп, 2-ой Сиб. конгресс по прикл. и индустр. мат., Новосибирск, 1996, 191.

[2] *О. М. Матейко, О. И. Тавгень*, Линейность групп автоморфизмов относительно свободных групп, Мат. заметки, **58**, 3 (1995), 465–467.

[3] *А. А. Коробов*, О старшем коэффициенте матричной экспоненты, в сб. «Современные методы теории функций и смежные проблемы. Материалы конференции», Воронеж, ВГУ, 2005, 125.

[4] *А. А. Коробов*, Алгебраический метод для решения одной задачи оптимального управления, 5-ая Межд. конф. «Алгебра и теория чисел», Тула, ТГПУ, 2003, 139–140.

[5] *А. А. Коробов*, Об алгебраическом методе для решения новой задачи оптимального управления, Вычисл. технологии, **8**, № 4 (2003), 283–289.

[6] *А. А. Коробов*, Некоторые условия точечной вырожденности для линейных систем с запаздыванием, в сб. «Труды Всерос. научн. шк. «Компьютерная логика, алгебра и интеллектуальное управление», Иркутск, Ир. ВЦ, 1995, 230 – 244.

[7] *Ю. И. Мерзляков*, Рациональные группы, М., Наука, 1987.

[8] *Х. Нейман*, Многообразия групп, М., Мир, 1969.

[9] *М. И. Каргаполов, Ю. И. Мерзляков*, Основы теории групп, М., Наука, 1982.

[10] *Г. С. М. Коксетер, У. О. Дж. Мозер*, Порождающие элементы и определяющие соотношения дискретных групп, М., Наука, 1980.

[11] *Р. Лидл, Г. Нидеррайтер*, Конечные поля, М., Мир, 1988.

[12] *А. Г. Курош*, Курс высшей алгебры, М., Гостехиздат, 1946.

[13] *М. В. Яковкин*, Численная теория приводимости многочленов, М., АН СССР, 1959.

[14] *Д. К. Фаддеев, И. С. Соминский*, Сборник задач по высшей алгебре, М., Наука, 1968.

[15] *Д. К. Фадеев*, Лекции по алгебре, Санкт-Петербург, Лань, 2002.

[16] *Н. С. Бахвалов, Н. П. Жидков, Г. М. Кобельков*, Численные методы, М., БИНОМ, 2004.

[17] *И. В. Проскуряков*, Сборник задач по линейной алгебре, М., Наука, 1974.

[18] *J. R. J. Groves*, Varieties of soluble groups and a dichotomy of P. Hall, Bull. Austral. Math. Soc., **5**, № 3 (1971), 391–410.

[19] *J. A. Chang, H. J. Godwin*, A table of irreducible polynomials and theis exponents, Proc. Cambridge Philos. Soc., **65** (1969), 513–522.

[20] *H. G. Zimmer*, Computational Problems, Methods and Results in Algebraic Number Theory, Berlin – Heidelberg – New York, Springer-Verlag, 1972.

[21] *Runge*, Über die Zerlegung ganzzahliger Functionen in Irreductibile Factoren, J. reine angew. Math., **99** (1885), 89–97.

[22] *M. Mandl*, Über die Zerlegung ganzer, ganzzahliger Functionen in Irreductibile Factoren, J. reine angew. Math., **113** (1894), 252–261.

[23] *O. Perron*, Neue Kriterien für die Irreduzibilität algebraischer Gleichungen, J. reine angew. Math., **132** (1907), 288–307.

[24] *E. S. Selmer*, On the irreducibility of certain trinomials, Math. Scand., **4** (1956), 287–302.

[25] *N. Obrechkoff*, Zeros of polynomials, Sofia, Marin Drinov Academic Publishing House, 2003.

[26] *W. Ljunggren*, On the irreducibility of certain trinamials and quadrinomials, Math. Scand., **8** (1960), 81–96.

Поступило 28 сентября 2005 г.

Адрес автора:
КОРОБОВ Алексей Александрович,
РОССИЯ, 630090, г. Новосибирск,
просп. Академика Коптюга, 4
Институт математики СО РАН,
Отдел теоретической кибернетики
e-mail: alexegor@math.nsc.ru