Math-Net.Ru

All Russian mathematical portal

R. M. Korotkova, O. V. Kudinov, A. S. Morozov, On mutual definability of operations on fields, *Sibirsk. Mat. Zh.*, 2019, Volume 60, Number 6, 1324–1334

DOI: <https://doi.org/10.33048/smzh.2019.60.611>

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 107.22.136.117

April 26, 2023, 13:37:58

О ВЗАИМНОЙ ОПРЕДЕЛИМОСТИ ОПЕРАЦИЙ НАД ПОЛЯМИ

Р. М. Короткова,
О. В. Кудинов, А. С. Морозов

Аннотация. Изучается возможность определения одних операций на полях через другие. В частности, доказывается, что операция умножения на произвольном поле может быть определена через операцию сложения тогда и только тогда, когда это поле является конечным расширением своего простого подполя. Приведено достаточное условие для неопределимости сложения через умножение. В частности, доказано, что операции умножения и сложения на вещественных и комплексных числах не могут быть определены одна через другую посредством отношений с параметрами, устойчивых относительно автоморфизмов. Также изучена взаимная определимость операций сложения, умножения и экспоненцирования в полях вещественных и комплексных чисел через две остальные операции.

DOI 10.33048/smzh.2019.60.611

Ключевые слова: поле, определимость, экспонента.

Изучение определимости одних математических объектов через другие играет заметную роль в математике. Разнообразные классы используемых при этом определений могут давать определенную информацию об определяемых ими математических объектах. Некоторые определения позволяют лучше понять структуру классов объектов и самих объектов, другие — конструировать эти объекты вплоть до реализации некоторых из них на компьютере или в рамках некоторой (порой достаточно абстрактной) обобщенной концепции вычислимости; некоторые определения пригодны для распознавания объектов из определяемого класса. Например, компьютерную программу для вычисления функции можно рассматривать как определение для этой функции. Наоборот, некоторые определения, видимо, можно рассматривать как вычислительные программы в рамках той или иной концепции обобщенной вычислимости; при этом классическая вычислимость занимает один из «нижних этажей» среди всего многообразия возможных вычислимостей. Результаты о невозможности определения объекта с помощью определений из того или иного класса иногда рассматриваются как отрицательные и даже как ненужные. Однако в некотором смысле такие результаты тоже полезны. Дело в том, что в итоге они позволяют построить сложностную классификацию объектов в соответствии с классами возможных определений для них. Кроме того, в некоторых случаях

Работа О. В. Кудинова поддержана программой фундаментальных научных исследований СО РАН № I.1.1 (проект № 0314–2019–0001), работа А. С. Морозова — программой фундаментальных научных исследований СО РАН № I.1.1 (проект № 0314–2019–0003), О. В. Кудинов и А. С. Морозов также частично поддержаны грантом РФФИ № 17–01–00247.

они могут показать несостоятельность попыток поиска тех или иных способов задания объектов или найти методологически корректные пути решения практических задач. Например, хорошо известные сегодня результаты об алгоритмической неразрешимости некоторых элементарных теорий (т. е. фактически о невозможности их задания с помощью определений из некоторого класса) показывают бессмысленность попыток построения «глобального математического компьютера», «универсального математика», который бы всегда давал правильные ответы на вопросы об истинности математических утверждений. Более простыми примерами являются хорошо известные результаты о неразрешимости задачи о трисекции угла с помощью циркуля и линейки, а также о неразрешимости произвольных алгебраических уравнений в радикалах; эти результаты также можно рассматривать в рамках нашего видения ситуации как результаты об отсутствии определений из некоторого класса. С этой же точки зрения можно рассматривать и проблемы алгоритмических сводимостей (см. [1]) и их обобщений — интерпретациях определимости одних алгебраических структур в других. Одним из наиболее интересных и развитых направлений исследований здесь является изучение определимости алгебраических структур в допустимых множествах посредством Σ -формул (Σ -определимости). С основными понятиями и идеями этого подхода можно ознакомиться по [2, 3]. Работа [4] содержит довольно полный обзор результатов на момент ее публикации. Перечислим лишь некоторые результаты. М. В. Коровина [5] доказала, что операция $\sin(x)$ и некоторые другие операции не могут быть определены Σ -формулами в наследственно списочной надстройке над упорядоченным полем вещественных чисел $\mathbb{R}$. Этот результат легко переизлагается для наследственно конечной надстройки над $\mathbb{R}$. М. В. Коровина и А. С. Морозов [6] получили ряд результатов об определимости счетных структур в наследственно конечных надстройках над $\mathbb{R}$ и $\mathbb{C}$. А. С. Морозов получил серию результатов об отсутствии простых Σ -определений для широкого класса структур над $\mathbb{R}$ и взаимоотношениях их различных представлений [7–13].

Весьма интересным в рамках данной проблематики оказывается также вопрос о представимости одних широко используемых в математике операций через другие. Так, например, операция сложения на натуральных числах может быть определена через операцию следования посредством обычной схемы примитивной рекурсии, а операция умножения, в свою очередь, через операцию сложения. Можно также легко выписать разумные определения для операции умножения на рациональных числах через операцию сложения. Более интересными и нетривиальными оказываются вопросы об определимости операций на вещественных числах, в частности, о взаимной определимости операций сложения и умножения. В свое время такой вопрос об определимости с помощью Σ -формул для упорядоченного поля вещественных чисел был задан третьему автору Джулией Найт. В данной работе содержится ответ на этот вопрос.

Перейдем к изложению результатов. Поле рациональных чисел будем обозначать, как обычно, через $\mathbb{Q}$. Наследственно конечную надстройку над произвольной структурой M будем обозначать через $\mathbb{HF}(M)$. Чтобы подчеркнуть, что мы рассматриваем сигнатурное ограничение структуры и будем отдельно указывать операции этого ограничения. Например, если F — поле, то $\langle F; + \rangle$ — его аддитивная группа.

Все результаты о неопределимости получены с помощью построения специфических автоморфизмов сигнатурных обиднений полей. Ввиду этого отдельно

формулируем утверждения о существовании таких автоморфизмов.

1. Умножение через сложение

Изучим возможности определения операции умножения через сложение.

Предложение 1. Пусть F — произвольное поле. Тогда следующие условия эквивалентны:

- (1) для любого конечного подмножества $A \subseteq F$ существует автоморфизм структуры $\langle F; + \rangle$, оставляющий на месте все элементы из A и не сохраняющий операции умножения на F ;
- (2) для любого конечного подмножества $A \subseteq F$ существует нетривиальный автоморфизм структуры $\langle F; + \rangle$, оставляющий на месте все элементы из A ;
- (3) поле F является бесконечным расширением своего простого подполя.

ДОКАЗАТЕЛЬСТВО. (1) $\Rightarrow$ (2) Тривиально.

(2) $\Rightarrow$ (3) Пусть для поля F выполнено условие (2). Предположим для получения противоречия, что F — конечное расширение своего простого подполя P . Возьмем в качестве A базис $\{b_0, \dots, b_{k-1}\}$ векторного пространства F над P . Возьмем произвольные $x \in F$ и автоморфизм φ структуры $\langle F; + \rangle$, оставляющий на месте все элементы из A . По x однозначно определяется кортеж $\beta_0, \dots, \beta_{k-1} \in P$ такой, что $x = \sum_{i=0}^{k-1} \beta_i b_i$. Поскольку каждый элемент β_i простого подполя с точностью до знака есть частное двух конечных сумм единиц, каждый элемент $\beta_i b_i$ — единственное решение подходящего уравнения вида $\underbrace{x + \dots + x}_m = \underbrace{b_i + \dots + b_i}_n$ либо $\underbrace{x + \dots + x}_m + \underbrace{b_i + \dots + b_i}_n = 0$. Отсюда следует, что все элементы $\beta_i b_i$ неподвижны относительно φ . Следовательно, и $\varphi(x) = x$, т. е. φ тривиален. Значит, F не имеет нетривиальных автоморфизмов, оставляющих на месте все элементы из A ; противоречие.

(3) $\Rightarrow$ (1) Пусть F — бесконечное расширение своего простого подполя P , т. е. $\langle F; + \rangle$ является бесконечномерным векторным пространством над P . Зафиксируем в нем некоторый базис B . Пусть A — произвольное конечное подмножество F . Выберем в множестве $B \setminus P$ произвольные попарно различные элементы a, b, c , не участвующие в разложении ни одного элемента из A . Определим обратимое линейное преобразование (трансвекцию) L этого линейного пространства заданием его значений на элементах базиса B следующим образом:

$$L(x) = \begin{cases} b + c, & \text{если } x = a, \\ x & \text{в остальных случаях.} \end{cases}$$

Очевидно, что для любого $x \in F$ найдется $\beta \in P$ со свойством $L(x) = x + \beta c$. Отображение L является автоморфизмом структуры $\langle F; + \rangle$, оставляющим на месте все элементы из A . Предположим, что L сохраняет операцию умножения. Тогда для подходящего $\beta \in P$ справедливо

$$ab + bc = a(b + c) = L(a)L(b) = L(ab) = ab + \beta c.$$

Из этого равенства с учетом $c \neq 0$ получаем $a = \beta \in P$; противоречие.

Предложение доказано.

Следствие 1. Пусть F — произвольное поле. Тогда следующие условия эквивалентны:

(1) операция умножения на F определима Σ -формулой с параметрами над структурой $\mathbb{HF}(\langle F; + \rangle)$;

(2) F является конечным расширением своего простого подполя.

ДОКАЗАТЕЛЬСТВО. (1) $\Rightarrow$ (2) Предположим, что операция умножения определима над структурой $\mathbb{HF}(\langle F, + \rangle)$ некоторой Σ -формулой с параметрами $\bar{p}$, но тем не менее F — бесконечное расширение своего простого подполя. В силу предложения 1 найдется автоморфизм структуры $\langle F, + \rangle$, оставляющий на месте все элементы из носителя множества параметров и не сохраняющий операции умножения. Этот автоморфизм естественным образом продолжается до автоморфизма всей структуры $\mathbb{HF}(\langle F, + \rangle)$, в которой он оставляет все параметры $\bar{p}$ на месте но не сохраняет графика операции умножения. Значит, наша формула с параметрами не может определять операцию умножения; противоречие.

(2) $\Rightarrow$ (1) Пусть F — конечное расширение своего простого подполя P и $\{e_i \mid i < k\}$ — базис векторного пространства F над P . Зафиксируем элементы $\gamma_{ij}^{(s)} \in P$, $i, j, s < k$, так, чтобы для всех $i, j < k$ выполнялись равенства $e_i e_j = \sum_{s < k} \gamma_{ij}^{(s)} e_s$. Тогда $xy = z$ эквивалентно следующему условию:

$$\exists \alpha_0 \dots \alpha_{k-1} \beta_0 \dots \beta_{k-1} \in P \left[x = \sum_{i < k} \alpha_i e_i \wedge y = \sum_{i < k} \beta_i e_i \wedge z = \sum_{s < k} \left(\sum_{i, j < k} \alpha_i \beta_j \gamma_{ij}^{(s)} \right) e_s \right]. \quad (1)$$

Все элементы поля P являются частными от сумм конечного числа единиц и противоположных к ним элементов. Заметим, что умножение на каждое конкретное частное от таких сумм единиц можно записать в виде $\exists$ -формулы. Ввиду этого в случае конечного поля P условие (1) можно записать в виде конечной $\exists$ -формулы с параметрами $e_i, \gamma_{ij}^{(s)}, i, j, s < k$, сигнатуры $\langle + \rangle$. В случае бесконечного P (т. е. $P = \mathbb{Q}$) это условие записывается в виде бесконечной вычислимой дизъюнкции $\exists$ -формул сигнатуры $\langle + \rangle$ с тем же набором параметров. Такие формулы, как известно, эквивалентны Σ -формулам (см. [4]). Следствие доказано.

Следствие 2. В любом бесконечном расширении простого подполя операцию умножения невозможно определить через операцию сложения не только в языке первого порядка, но также и в любом языке, формулы которого выделяют подмножества, устойчивые относительно автоморфизмов.

Следствие 3. Пусть F — одно из полей $\mathbb{C}, \mathbb{R}$. Тогда операцию умножения на F невозможно определить с параметрами в структуре $\langle F; + \rangle$ ни в каком языке, формулы которого выделяют множества, устойчивые относительно автоморфизмов. В частности, это верно для языка первого порядка и языка Σ -формул для $\mathbb{HF}(\langle F; + \rangle)$.

Следствие 4. В языке первого порядка операцию умножения можно определить (с параметрами) через операцию сложения только в конечных полях.

ДОКАЗАТЕЛЬСТВО. Из доказанного следует, что нетривиален лишь случай, когда поле F является конечным расширением поля рациональных чисел $\mathbb{Q}$. Хорошо известно, что элементарная теория группы $\langle F, + \rangle$ в этом случае разрешима (см. обзор по теориям абелевых групп в [14]), причем допускает элиминацию кванторов, обеспечивающую разрешимость теории и при конечном константном обогащении языка. Если бы операция умножения в поле F

оказалась определимой, то и элементарная теория самого поля F стала бы также разрешимой, однако неразрешимость таких теорий доказана в [15, 16].

2. Сложение через умножение

Изучим возможности определения сложения через умножение. Укажем общее достаточное условие, выполненное для ряда хорошо известных полей и гарантирующее непредставимость его операции сложения через операцию умножения.

Пусть G — произвольная абелева группа. Поскольку будем иметь дело с мультипликативной группой поля, здесь будем использовать мультипликативную нотацию. Следующее определение достаточно стандартно. Будем говорить, что подмножество $B \subseteq G$ *независимо*, если для любых $m_1, \dots, m_k \in \mathbb{Z}$ и любых попарно различных $b_1, \dots, b_k \in B$ из равенства $b_1^{m_1} \dots b_k^{m_k} = 1$ следует $m_1 = \dots = m_k = 0$. В противном случае будем называть это множество *зависимым*. Любое максимальное линейно независимое подмножество в группе G будем называть ее *базисом*. Очевидно, что любое независимое подмножество расширяется до базиса и что любая абелева группа обладает базисом. Заметим, что базис может быть пустым. Более того, можно заметить, что группа обладает пустым базисом тогда и только тогда, когда она периодическая, что также эквивалентно тому, что все ее базисы пусты. Будем говорить, что абелева группа G *богата автоморфизмами*, если в ней существует такой базис B , что для любого конечного $H \subseteq B$ найдутся $a, b \in B \setminus H$ и автоморфизм φ группы G , который неподвижен на всех элементах из множества $B \setminus \{a\}$, и $\varphi(a) = ab$. В следующем предложении, говоря о прямом произведении $G_0 \times G_1$ групп G_0 и G_1 , отождествляем элементы этих групп с их образами относительно канонических вложений: так $g \in G_0$ отождествляется с $\langle g, 1 \rangle$ и $g \in G_1$ — с $\langle 1, g \rangle$.

Предложение 2. Пусть G_0 и G_1 — абелевы группы и G_0 богата автоморфизмами. Тогда и их прямое произведение $G_0 \times G_1$ тоже богато автоморфизмами.

Доказательство. Пусть $B_0 \subseteq G_0$ — базис для G_0 , как в определении, и $B_1 \subseteq G_1$ — произвольный базис для G_1 . Докажем, что $B = B_0 \cup B_1$ — базис для $G_0 \times G_1$. Независимость множества B очевидна. Докажем его максимальность. Возьмем произвольный элемент $g = g_0 g_1$, где $g_i \in G_i$, $i = 0, 1$. Поскольку B_i — базис в G_i , $i = 0, 1$, найдутся $s_0, s_1 \in \mathbb{Z} \setminus \{0\}$ и произведения элементов соответствующих базисов $\beta_i \in G_i$ такие, что $g_i^{s_i} \beta_i = 1$, $i = 0, 1$. Имеем

$$g^{s_0 s_1} (\beta_0)^{s_1} (\beta_1)^{s_0} = (g_0 g_1)^{s_0 s_1} (\beta_0)^{s_1} (\beta_1)^{s_0} = (g_0^{s_0} \beta_0)^{s_1} (g_1^{s_1} \beta_1)^{s_0} = 1.$$

Поскольку $s_0 s_1 \neq 0$ и $(\beta_0)^{s_1} (\beta_1)^{s_0}$ — произведение элементов из B , получаем, что произвольно выбранный элемент $g \in G_0 \times G_1$ не может принадлежать никакому собственному независимому расширению, т. е. B — базис для $G_0 \times G_1$. Пусть H — произвольное конечное подмножество в B . Поскольку G_0 богата автоморфизмами, найдутся автоморфизм φ группы G_0 и $a, b \in B_0$ такие, что φ тождествен на $H \cap B_0$ и $\varphi(a) = ab$. Нетрудно проверить, что отображение $\varphi^* : G_0 \times G_1 \rightarrow G_0 \times G_1$, определенное как $\varphi^*(x_0 x_1) = \varphi(x_0) x_1$, для любых $x_0 \in G_0$, $x_1 \in G_1$ является автоморфизмом группы $G_0 \times G_1$ со свойством $\varphi^*(a) = ab$, тождественным на $B \setminus \{a\}$. Предложение доказано.

Предложение 3. Мультипликативные группы полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, а также поле рациональных дробей $F(t)$ над произвольными полями F богаты автоморфизмами.

ДОКАЗАТЕЛЬСТВО. Заметим, что подгруппа $(\mathbb{Q}^*)^+$ в $\mathbb{Q}^*$, образованная всеми положительными рациональными числами, богата автоморфизмами. В качестве базиса B можно рассмотреть множество всех простых натуральных чисел. Остается заметить, что $\mathbb{Q}^* \cong \mathbb{Z}_2 \times (\mathbb{Q}^*)^+$, и применить предложение 2.

Для поля $\mathbb{R}$ доказательство проводится аналогично. Сначала заметим, что подгруппа $(\mathbb{R}^*)^+$ в $\mathbb{R}^*$, образованная положительными элементами, богата автоморфизмами; в качестве базиса B можно взять базис векторного пространства над $\mathbb{Q}$, в котором сложение имеет вид $x \oplus y = xy$, а умножение x на скаляр $r \in \mathbb{Q}$ — вид $r \odot x = x^r$. Утверждение следует из того, что $\mathbb{R}^* \cong \mathbb{Z}_2 \times (\mathbb{R}^*)^+$.

Чтобы доказать утверждение для $\mathbb{C}$, достаточно заметить, что $\mathbb{C}^* \cong (\mathbb{R}^*)^+ \times U$, где $U = \{x \in \mathbb{C} \mid |x| = 1\}$ (поскольку $x = |x|(x|x|^{-1})$).

Для доказательства утверждения для полей вида $F(t)$ сначала рассмотрим подгруппу G в $(F(t))^*$, порожденную унитарными неприводимыми многочленами над F . Эта группа богата автоморфизмами. Доказательство аналогично доказательству для $\mathbb{Q}$. Поскольку любой элемент из $(F(t))^*$ единственным образом представим в виде $\alpha p/q$, где $\alpha \in F$, а p и q — взаимно простые произведения унитарных многочленов над F , G выделяется прямым слагаемым в $(F(t))^*$, и утверждение следует из предложения 2.

Предложение доказано.

Теорема 1. Пусть F — произвольное поле, мультипликативная группа которого богата автоморфизмами. Тогда для любого конечного подмножества $A \subseteq F$ существует автоморфизм структуры $\langle F; \cdot \rangle$, тождественный на элементах из A и не сохраняющий операции сложения.

ДОКАЗАТЕЛЬСТВО. Пусть множество $A = \{\bar{p}\} \subseteq F$ конечно. Зафиксируем в F^* некоторый базис B , как в определении группы, богатой автоморфизмами. Существует конечное множество $B_0 \subseteq B$ такое, что любой элемент из A вместе с B_0 образует линейно зависимое множество. Выберем $a, b \in B \setminus B_0$ и соответствующий им автоморфизм φ_0 из определения группы, богатой автоморфизмами, такой, что $\varphi_0(a) = ab$, тождественный на B_0 .

Покажем, что для некоторого натурального $n > 0$ автоморфизм φ_0^n действует тождественно на A . Действительно, рассмотрим произвольный элемент q из кортежа $\bar{p}$, образующего множество A . Для него найдутся $b_1, \dots, b_k \in B_0$ и $s, s_1, \dots, s_k \in \mathbb{Z}$ такие, что $s \neq 0$ и $q^s b_1^{s_1} \dots b_k^{s_k} = 1$. Учитывая, что все b_j , $j = 1, \dots, k$, неподвижны относительно φ_0 , получим, что для любого натурального m справедливо $(\varphi_0^m(q))^s b_1^{s_1} \dots b_k^{s_k} = 1$. Это означает, что все элементы $\varphi_0^m(q)$, $m < \omega$, являются корнями одного и того же многочлена ненулевой степени s . Стало быть, множество всех таких элементов конечно. Отсюда следует, что конечно и множество всех кортежей вида $\varphi_0^m(\bar{p})$. Значит, существует натуральное число $n > 0$ со свойством $\varphi_0^n(\bar{p}) = \bar{p}$. Зафиксируем такое n и положим $\varphi = \varphi_0^n$. Заметим, что $\varphi(a) = ab^n$.

Покажем, что автоморфизм φ не может сохранять операции сложения. Предположим противное. Тогда φ — автоморфизм всего поля и $K = \{x \mid \varphi(x) = x\}$ — подполе в F со свойством $B \setminus \{a\} \subseteq K$. Покажем, что элемент a алгебраичен над K . Действительно, поскольку B — базис, найдутся $\ell, s, s_1, \dots, s_k \in \mathbb{Z}$ и $b_1, \dots, b_k \in B \setminus \{a\}$ такие, что $\ell \neq 0$ и $(a+1)^\ell a^s c = 1$, где $c = b_1^{s_1} \dots b_k^{s_k} \in K$. Последнее ввиду $\ell \neq 0$ дает нам нетривиальный полином, корнем которого является a .

Пусть f — произвольный нетривиальный многочлен над K такой, что

$f(a) = 0$. Тогда для любого $k < \omega$ будет выполнено равенство

$$0 = \varphi^k(f(a)) = f(\varphi^k(a)) = f(ab^{nk}).$$

Поскольку a и b принадлежат базису B и $n > 0$, получаем, что элементы ab^{nk} , $k < \omega$, будут образовывать бесконечное множество корней многочлена f ; противоречие.

Теорема доказана.

Следствие 5. Пусть F — произвольное поле, мультипликативная группа которого богата автоморфизмами, $P(x, y, z, \bar{t})$ — произвольное отношение на F , устойчивое относительно автоморфизмов структуры $\langle F; \cdot \rangle$, и пусть $\bar{p}$ — произвольный набор параметров из F . Тогда множество $\{\langle x, y, z \rangle \mid P(x, y, z, \bar{p})\}$ не совпадает с графиком операции сложения на F .

Аналогично предыдущему получаем

Следствие 6. Пусть F — произвольное поле, мультипликативная группа которого богата автоморфизмами (в том числе F может быть любым из полей $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$). Тогда операция сложения на F не определима ни в каком языке, формулы которого выделяют подмножества, устойчивые относительно автоморфизмов структуры $\langle F; \cdot \rangle$. В частности, эта операция не определима никакой Σ -формулой с параметрами в $\text{HF}(\langle F; \cdot \rangle)$.

3. Добавим экспоненту

Ограничим наше рассмотрение только полями вещественных и комплексных чисел в сигнатуре $\langle +, \cdot, \text{exp} \rangle$, где exp — операция экспоненцирования $\text{exp}(x) = e^x$, и выясним, какие из операций этой сигнатуры Σ -определимы через другие.

Теорема 2. (1) Операция exp не Σ -определима ни с какими параметрами ни над $\text{HF}(\langle \mathbb{R}; +, \cdot \rangle)$ ни над $\text{HF}(\langle \mathbb{C}; +, \cdot \rangle)$.

(2) Операция $+$ Σ -определима без параметров над $\text{HF}(\langle \mathbb{R}; \cdot, \text{exp} \rangle)$ и над $\text{HF}(\langle \mathbb{C}; \cdot, \text{exp} \rangle)$.

(3) Операция $\cdot$ Σ -определима без параметров над $\text{HF}(\langle \mathbb{R}; +, \text{exp} \rangle)$ и над $\text{HF}(\langle \mathbb{C}; +, \text{exp} \rangle)$.

ДОКАЗАТЕЛЬСТВО. Докажем (1). Для $\mathbb{R}$ это доказано в [12, теорема 6.1].

Лемма 1. Не существует подмножества $E \subseteq \mathbb{C}$, имеющего в $\mathbb{C}$ предельную точку, формулы первого порядка $\varphi(x, y, \bar{t})$ и параметров $\bar{p} \in \mathbb{C}$ таких, что для любых $x \in E$ и $y \in \mathbb{C}$ справедлива эквивалентность $\varphi(x, y, \bar{p}) \leftrightarrow y = e^x$.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ. Пусть формула $\varphi(x, y, \bar{p})$ вместе с множеством E образуют контрпример к данному утверждению. Ввиду элиминации кванторов для $\mathbb{C}$ можно считать формулу φ дизъюнктивной нормальной формой от утверждений вида $f(x, y, \bar{p}) = 0$, где f — полином. Очевидно, что некоторый ее дизъюнкт

$$\psi(x, y, \bar{p}) = \bigwedge_{j < k} f_j(x, y, \bar{p}) = 0 \wedge \bigwedge_{j < \ell} g_j(x, y, \bar{p}) \neq 0$$

вместе с множеством E также образует контрпример. Покажем, что все полиномы f_j тождественно равны нулю. Действительно, для всех $x \in E$ значение аналитической функции $f_j(x, e^x, \bar{p})$ равно нулю, откуда по одному из основных

свойств аналитических функций получим, что и сама эта функция тождественно равна нулю. Представим ее в виде

$$f_j(x, e^x, \bar{p}) = \sum_{1 \leq k \leq n} e^{kx} h_k(x) + h(x),$$

где $n \geq 0$, а h, h_k ($1 \leq k \leq n$) — полиномы над $\mathbb{C}$, при этом $h_n \neq 0$ в случае $n \geq 1$. Предположим, что $n \geq 1$. Тогда имеет место равенство $f_j(x, e^x, \bar{p}) = e^{nx}(h_n(x) + F)$, где F — сумма слагаемых вида cx^q/e^{rx} , $c \in \mathbb{C}$, $q, r < \omega$, $r > 0$. Учитывая, что значение $\lim_{|x| \rightarrow \infty} |h_n(x)|$ ограничено снизу строго положительным числом и что при $r > 0$ выполняется $\lim_{|x| \rightarrow \infty} |cx^q/e^{rx}| = 0$, получаем, что $\lim_{|x| \rightarrow \infty} |f_j(x, e^x, \bar{p})| = \infty$, т. е. $f_j(x, e^x, \bar{p})$ не может быть тождественно равным нулю; противоречие. Значит, $n = 0$. Тогда полином $f_j = h$ тождественно равен нулю. Поскольку все f_j нулевые, формула $\psi(x, y, \bar{p})$ не может определять никакой функции на E : при некоторых x существует бесконечно много y со свойством $\psi(x, y, \bar{p})$; противоречие.

Лемма доказана.

Пусть некоторая Σ -формула с параметрами $\bar{p}$ определяет в структуре $\mathbb{HF}(\langle \mathbb{C}; +, \cdot \rangle)$ график функции $\exp$. Возьмем ее эквивалентное представление в виде бесконечной дизъюнкции $\bigvee_{j < \omega} \varphi_j(x, y, \bar{p})$ (о существовании такого представления см. [4]). По теореме Бэра найдутся $j < \omega$ и его подмножество E , обладающее предельной точкой в $\mathbb{C}$, такое, что формула $\varphi_j(x, y, \bar{p})$ определяет на E ограничение функции $\exp$. Это противоречит лемме 1. Тем самым доказали (1).

Докажем (2). Определимость сложения над $\mathbb{R}$ следует из эквивалентности

$$x + y = z \Leftrightarrow e^x \cdot e^y = e^z.$$

Для $\mathbb{C}$ эта эквивалентность не выполнена, так как в этой ситуации число z со свойством $e^z = a$ определено с точностью до слагаемого вида $2k\pi i$, $k \in \mathbb{Z}$. Поэтому доказательство будет немного сложнее. В структуре $\langle \mathbb{C}; \cdot, \exp \rangle$ число 0 можно выделить, например, Σ -условием $\exists y \neq x(y \cdot x = x \wedge x^2 = x)$. Число 1 можно выделить Σ -условием $x^2 = x \wedge x \neq 0$, число -1 — Σ -условием $x^2 = 1 \wedge x \neq 1$. Заметим, что если $t^2 = -1$, то

$$\{z \mid e^z = e^x \cdot e^y\} = \{x + y + 2k\pi t \mid k \in \mathbb{Z}\}, \quad \{z \mid e^{tz} = e^{tx} \cdot e^{ty}\} = \{x + y + 2k\pi \mid k \in \mathbb{Z}\}.$$

Пересечение этих двух множеств состоит из единственного элемента $x + y$. Отсюда следует, что

$$x + y = z \Leftrightarrow \exists t(t^2 = -1 \wedge e^z = e^x \cdot e^y \wedge e^{tz} = e^{tx} \cdot e^{ty}),$$

т. е. сложение можно определить Σ -формулой без параметров.

Докажем (3). Сначала докажем утверждение для $\mathbb{R}$. Заметим, что число 0 определимо формулой $x + x = x$, функция $-x$ определима формулой $x + y = 0$, множество строго положительных чисел определимо Σ -условием $\exists y(x = e^y)$, а множество строго отрицательных чисел — Σ -условием $\exists y(-x = e^y)$. Для строго положительных чисел умножение определяется Σ -условием

$$\exists x_0 \exists y_0 (x = e^{x_0} \wedge y = e^{y_0} \wedge z = e^{x_0 + y_0}), \quad (2)$$

для строго отрицательных — соответственно Σ -условием

$$\exists x_0 \exists y_0 (-x = e^{x_0} \wedge -y = e^{y_0} \wedge z = e^{x_0 + y_0}).$$

Для случаев, когда одно из чисел x, y строго положительное, а другое — строго отрицательное, Σ -условия выписываются аналогично. Наконец, для случая, когда одно из чисел x, y равно нулю, соответствующая формула выписывается очевидным образом. Собирая все случаи, получим Σ -определение для умножения через операции $\cdot$ и exp .

Для $\mathbb{C}$ доказательство проще: нужно заметить, что 0 определяется той же самой формулой, а для ненулевых x и y умножение определяется условием (2), и снова собрать все частные случаи в одно Σ -определение для умножения.

Теорема доказана.

Нами фактически доказано более сильное утверждение: в пп. (2) и (3) теоремы получена определимость с помощью $\exists$ -формул.

Заметим, что результат М. В. Коровиной из [5] показывает специфичность ситуации для поля вещественных чисел: с одной стороны, операция exp над ним не имеет Σ -определения, в то время как утверждение о невозможности определения этой операции с помощью отношений, устойчивых относительно автоморфизмов, ложное, поскольку $\mathbb{R}$ не имеет нетривиальных автоморфизмов.

Теорема 3. Пусть F — одно из полей $\mathbb{C}, \mathbb{R}$. Пусть также $P(x, y, z, \bar{t})$ — произвольное отношение на F , устойчивое относительно автоморфизмов структуры $\langle F; \text{exp} \rangle$, и $\bar{p}$ — набор параметров из F . Тогда множество $\{\langle x, y, z \rangle \mid P(x, y, z, \bar{p})\}$ не совпадает ни с графиком операции сложения, ни с графиком операции умножения на F . Таким образом, операции $+$ и $\cdot$ не могут быть определены над $\langle F; \text{exp} \rangle$ ни в каком языке, формулы которого выделяют множества, устойчивые относительно автоморфизмов этой структуры.

ДОКАЗАТЕЛЬСТВО. Докажем утверждение для случая $F = \mathbb{C}$. Для этого, как и ранее, достаточно доказать, что для любого конечного $A \subseteq \mathbb{C}$ существует автоморфизм структуры $\langle \mathbb{C}; \text{exp} \rangle$, сохраняющий все элементы из A , но не сохраняющий графика операции сложения. Рассмотрим ориентированный граф, образуемый на $\mathbb{C}$ отображением exp . Автоморфизмы данного графа и автоморфизмы структуры $\langle \mathbb{C}; \text{exp} \rangle$ — это одни и те же отображения. Заметим, что уравнение $\text{exp}(x) = a$ имеет счетное число решений над $\mathbb{C}$ при $a \neq 0$ и не имеет решений при $a = 0$. Таким образом, в каждую вершину $a \neq 0$ из $\mathbb{C}$ этого графа приходит счетное число ребер, элемент 0 единственный, в который не приходит ни одного ребра. Кроме того, из каждого элемента этого графа выходит ровно одно ребро. Отсюда следует, что каждая компонента связности этого графа может содержать не более одного конечного цикла. Нетрудно убедиться, что любые две компоненты с конечными циклами одной и той же ненулевой длины изоморфны. В графе имеется ровно одна компонента, содержащая 0 . Остальные компоненты, не имеющие циклов, изоморфны между собой. Таким образом, в рассматриваемом графе имеется лишь счетное число типов изоморфизма компонент связности, каждая из которых счетна. Следовательно, существует тип изоморфизма, реализуемый бесконечным числом компонент. Зафиксируем в этом типе две различные компоненты связности X и Y , не содержащие элементов из A и содержащие элементы $x \in X$ и $y \in Y$ такие, что ни одно из чисел x, y, xy не равно нулю.

Рассмотрим два случая.

СЛУЧАЙ 1. $xy \notin X$. В этом случае автоморфизм, оставляющий на месте все элементы из компонент связности, содержащих хотя бы один элемент из A , элемент xy , а также все элементы из Y , и отправляющий компоненту X в отличную от нее компоненту, не будет сохранять операции умножения.

СЛУЧАЙ 2. $xy \notin Y$. Этот случай рассматривается аналогично.

Таким образом, утверждение для случая $F = \mathbb{C}$ доказано.

Случай $F = \mathbb{R}$ рассматривается аналогичным образом.

Теорема доказана.

Можно суммировать полученные результаты для полей $\mathbb{C}$ и $\mathbb{R}$ в виде диаграммы, изображенной на рис. 1, в которой наличие стрелки из области A в область B означает Σ -определимость набора операций, указанных в области A над операциями, указанными в B . Кроме того, если в диаграмме присутствует стрелка из области A в область B , но обратная стрелка отсутствует, то невозможна и Σ -определимость набора операций, указанных в области B над операциями, указанными в A . При этом данная диаграмма описывает ситуацию как для $\mathbb{R}$, так и для $\mathbb{C}$.

Рис. 1. Соотношения Σ -определимости между группами операций для $\mathbb{C}$ и $\mathbb{R}$

Авторы благодарят анонимного рецензента за устранение неточностей и замечания по улучшению изложения.

ЛИТЕРАТУРА

1. Soare R. I. Recursively enumerable sets and degrees. A study of computable functions and computably generated sets. Berlin: Springer-Verl., 1987.
2. Barwise J. Admissible sets and structures. Berlin; Göttingen; Heidelberg: Springer-Verl., 1975.
3. Ershov Yu. L. Definability and computability. New York: Plenum Publ. Co., 1996.
4. Ershov Yu. L., Puzarenko V. G., Stukachev A. I. HF-Computability // Computability in context. Computation and logic in the real world. London: Imperial College Press, 2011. P. 169–242.
5. Коровина М. В. Обобщенная вычислимость функций на вещественных числах // Вычисл. системы. 1990. № 133. С. 38–68.
6. Морозов А. С., Коровина М. В. О Σ -определимости счетных структур над вещественными, комплексными числами и кватернионами // Алгебра и логика. 2008. Т. 47, № 3. С. 335–363.
7. Морозов А. С. Непредставимость некоторых структур анализа в наследственно конечных надстройках // Алгебра и логика. 2017. Т. 56, № 6. С. 691–711.
8. Морозов А. С. Об отношении Σ -сводимости между допустимыми множествами // Сиб. мат. журн. 2004. Т. 45, № 3. С. 634–652.

9. Морозов А. С. Непредставимость полугруппы ω^ω над $\mathbf{HF}(\mathbb{R})$ // Сиб. мат. журн. 2014. Т. 55, № 1. С. 156–164.
10. Морозов А. С. Σ -жесткие представления вещественного порядка // Сиб. мат. журн. 2014. Т. 55, № 3. С. 562–572.
11. Морозов А. С. О Σ -представлениях вещественного порядка // Алгебра и логика. 2014. Т. 55, № 3. С. 340–371.
12. Морозов А. С. О некоторых представлениях поля вещественных чисел // Алгебра и логика. 2012. Т. 51, № 1. С. 96–128.
13. Морозов А. С. Об одном достаточном условии непредставимости структур в наследственно-конечных надстройках // Алгебра и логика. 2016. Т. 55, № 3. С. 366–379.
14. Ершов Ю. Л. Проблемы разрешимости и конструктивные модели. М.: Наука, 1980.
15. Robinson J. Definability and decision problems in arithmetic // J. Symb. Logic. 1949. V. 14, N 2. P. 98–114.
16. Robinson J. The undecidability of algebraic rings and fields // Proc. Amer. Math. Soc. 1959. N 10. P. 950–957.

Поступила в редакцию 13 июля 2018 г.

После доработки 8 июля 2019 г.

Принята к публикации 24 июля 2019 г.

Короткова Роза Михайловна
Новосибирский государственный университет,
механико-математический факультет,
ул. Пирогова, 1, Новосибирск 630090
rozulka93@mail.ru

Кудинов Олег Викторович, Морозов Андрей Сергеевич
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090;
Новосибирский государственный университет,
механико-математический факультет,
ул. Пирогова, 1, Новосибирск 630090
kud@math.nsc.ru, morozov@math.nsc.ru