IDENTITIES IN ALGEBRA

L. N. SHEVRIN

The object of this article is to give an overview of the concept of algebraic identity. The presentation is based on the consideraion of a number of fundamental identities which appear in school mathematics. Some definitions and facts are also given to disclose the problems of contemporary investigations concerning identities of algebraic systems.

Цель статьи – бросить общий взгляд на понятие алгебраического тождества. Изложение базируется на рассмотрении ряда основных тождеств из школьного курса математики. Приведены также некоторые определения и факты, приоткрывающие проблематику современных исследований, относящихся к тождествам алгебраических систем.

ТОЖДЕСТВА В АЛГЕБРЕ

Л. Н. ШЕВРИН

Уральский государственный университет, Екатеринбург

1. ВВЕДЕНИЕ

Понятие тождества можно считать уникальным по “дистанции”, охватываемой им в математике – от самых начальных фактов, с которыми знакомятся младшеклассники, до крупных научных достижений последнего времени и открытых проблем, над решением которых бьются специалисты. Цель настоящей статьи – бросить общий взгляд на это понятие, обсудить несколько важных примеров и рассмотреть некоторые связанные с ним понятия, служащие отправным пунктом многочисленных исследований в современной алгебре.

Простейший пример тождества доставляет то свойство сложения (и, аналогично, умножения) натуральных чисел, которое в школе принято называть переместительным законом и которое гласит, что *от перемены мест слагаемых* (*множителей*) *сумма* (соответственно *произведение*) *не меняется*. Символически:

$$a + b = b + a, \qquad ab = ba. \tag{1}$$

В школьном курсе к переместительному закону вскоре добавляется сочетательный, выражаемый соответственно формулами

$$(a + b) + c = a + (b + c), \qquad (ab)\,c = a\,(bc). \tag{2}$$

Позднее констатируется так называемый распределительный закон, в котором участвуют оба упомянутых действия над числами:

$$a\,(b + c) = ab + ac. \tag{3}$$

В ходе дальнейшего изучения указанные законы распространяются на все более широкие числовые области: на целые числа, рациональные, действительные. Попутно отмечаются и некоторые другие свойства такого же типа. Вот несколько примеров:

$$a\,(b - c) = ab - ac, \tag{4}$$

$$(a + b)^2 = a^2 + 2ab + b^2, \quad a^2 - b^2 = (a + b)(a - b). \tag{5}$$

Что объединяет такие свойства действий? Во-первых, каждое из них выражается р а в е н с т в о м, обе части которого – буквенные выражения. Во-вторых, соответствующие равенства верны при л ю б ы х значениях входящих в них букв. Эти два атрибута и характеризуют общее понятие тождества как *равенства с переменными, верного при любых значениях входящих в него переменных*. Приведенная формулировка дает “свернутое” определение тождества, нуждающееся, вообще говоря, в уточнении. Например, естественно оттенить, что переменные пробегают значения из некоторого (заранее объявленного) множества. Кроме того, говоря о тех или иных тождествах, всегда подразумевают определенный тип выражений, составляющих левую и правую части тождества. В общем виде можно сказать, что в тождестве $f = g$ выражения f и g суть записи функций от нескольких переменных. При желании явно обозначить последние мы можем записать тождество, например, в виде

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n). \qquad (6)$$

Выбор символов для переменных в нашей власти; это могут быть и разные буквы, как в тождествах (1) – (5), и одна буква с разными индексами. В конкретных тождествах левая и правая части не обязательно содержат одни и те же переменные; но, допуская, что в общей записи рассматриваемых функций некоторые переменные могут участвовать "фиктивно" (то есть на самом деле функция от них не зависит), мы, как обычно говорят математики, без ограничения общности можем считать, что формула (6) представляет нам общий вид тождества. Не исключен, разумеется, случай, когда $n = 1$; типичные примеры – тождества

$$-(-x) = x, \quad (-x)^2 = x^2, \quad \sin 2x = 2\sin x\cos x.$$

Не исключен и случай, когда в одной из функций f, g тождества (6) все переменные фиктивны, то есть соответствующая функция есть константа. Типичный пример – знаменитое тригонометрическое тождество

$$\sin^2 x + \cos^2 x = 1.$$

Предметом рассмотрения в статье будут тождества, в которых функции, фигурирующие в левой и правой части, получаются из алгебраических операций (в результате последовательного применения одной или нескольких операций в указанном порядке). В следующем пункте мы напомним необходимые определения.

2. ОБ АЛГЕБРАИЧЕСКИХ ОПЕРАЦИЯХ

Бинарной операцией на множестве A называется всякое отображение множества всех упорядоченных пар элементов из A в множество A, то есть правило, по которому любой такой паре (x, y) ставится в соответствие некоторый элемент $a(x, y)$ из A. В школе изучается целый ряд бинарных операций, преимущественно на числовых множествах. Главные из них – сложение и умножение, и в этих случаях вместо $a(x, y)$ пишут $x + y$ и $x \cdot y$ соответственно, очень часто опуская точку в качестве знака умножения. Мы будем пользоваться стандартными обозначениями **N, Z, Q** и **R** для "главных" числовых множеств: всех натуральных, всех целых, всех рациональных и всех действительных чисел. Еще одна важная бинарная операция – вычитание на множестве **Z** (или **Q**, или **R**).

Стоит отметить следующие две известные бинарные операции на множестве **N**: взятие наибольшего общего делителя и наименьшего общего кратного. Стандартные обозначения для них – $НОД(x, y)$ и $НОК(x, y)$. А вот еще две естественные бинарные операции на любом подмножестве множества **R**: взятие минимума и максимума. Стандартные обозначения для них: $\min\{x, y\}$, $\max\{x, y\}$. При изучении бинарных операций удобно обозначать их символами, записываемыми между переменными, наподобие плюса, точки и минуса. Договоримся обозначать ниже операции *НОД*, *НОК*, min, max символами Δ, ∇, $\wedge$ и $\vee$ соответственно. Так что $x\Delta y = НОД(x, y)$ и т.д. Имеем, например, $4\Delta 6 = 2$, $4\nabla 6 = 12$, $4\wedge 6 = 4$, $4\vee 6 = 6$.

Можно дать общее определение n-арной алгебраической операции для любого натурального n. Такая операция на множестве A – это отображение множества всех упорядоченных n-ок элементов из A в множество A. Кроме случая $n = 2$, наиболее часто в самых разных ситуациях встречается случай $n = 1$. В этом случае операция называется *унарной*; тем самым, унарная операция на множестве A – это фактически то же, что и преобразование множества A, то есть отображение A в себя. Важные с алгебраической точки зрения примеры унарных операций: взятие противоположного элемента $-a$ для элемента a из **R** (в частности, из **Q** или **Z**) и взятие обратного элемента a^{-1} для элемента a из $\mathbf{R}\backslash\{0\}$ (в частности, из $\mathbf{Q}\backslash\{0\}$); с общей точки зрения мы посмотрим на эти операции ниже, в п. 5.2. Здесь, кстати, уместно обратить внимание читателя на несколько смыслов, в которых используется знак "минус": например, в выражении типа $-a$ он обозначает унарную операцию взятия противоположного элемента, в выражении типа $a - b$ он обозначает бинарную операцию вычитания. Связь между обоими отмеченными смыслами дается равенством

$$a - b = a + (-b), \qquad (7)$$

на которое можно смотреть и как на тождество, где участвуют две бинарные операции и одна унарная, и как на определение операции вычитания в терминах операций сложения и взятия противоположного элемента. В ряде случаев оказывается целесообразным рассматривать n-арные операции и при $n = 0$, так называемые *нуль-арные* операции. Формально соответствующее понятие как будто бы не охватывается приведенным выше определением n-арной операции, но естественно считать, что нуль-арная операция на множестве A – это фиксирование какого-то элемента из A.

Среди наиболее важных тождеств, которые выделяются при изучении алгебраических операций, уже упоминавшиеся во введении тождества, называемые в школьной математике переместительным, сочетательным и распределительным законами. Рассмотрим их несколько подробнее. В первых двух из них фигурирует одна бинарная операция (в стандартной школьной ситуации – сложение или умножение), в третьем – две бинарные операции. При обсуждении общей ситуации, чтобы не связывать себя привычным подтекстом, желательны символы для рассматриваемых операций, отличающиеся от знаков сложения и умножения. Будем произвольную рассматриваемую бинарную операцию обозначать символом $\circ$, а если мы имеем дело с двумя бинарными операциями, то обозначим их символами $\circ$ и $*$. Желая проверить или проинтерпретировать те или иные положения в какой-то конкретной ситуации, вместо указанных символов нужно подставлять символы соответствующих операций. Если рассматриваемая операция обозначена знаком $+$ (знаком $\cdot$ или отсутствием знака), то, как обычно, ее называют *сложением* (соответственно *умножением*) и говорят об *аддитивной* (соответственно *мультипликативной*) записи и терминологии. Подчеркнем, что речь при этом идет вовсе не обязательно об операциях над числами! Складывать и/или перемножать приходится векторы, матрицы, преобразования, функции и т.д.

Операция $\circ$ (на некотором множестве) называется *коммутативной* (*ассоциативной*), если выполняется тождество $x \circ y = y \circ x$ (соответственно $(x \circ y) \circ z = x \circ (y \circ z)$). Хрестоматийные примеры операций, одновременно коммутативных и ассоциативных, доставляют сложение и умножение чисел; мы начали с этих примеров изложение в п.1, напомнив общеизвестные формулы (1), (2). Введенные выше операции Δ, ∇, $\wedge$ и $\vee$ также коммутативны и ассоциативны; их коммутативность очевидна, ассоциативность $\wedge$ и $\vee$ проверяется очень легкими рассуждениями, доказательство же ассоциативности Δ и ∇ потребует несколько более кропотливых выкладок. Еще два важных примера операций, одновременно коммутативных и ассоциативных, – пересечение $\cap$ и объединение $\cup$ на множестве $P(M)$ всех подмножеств множества M; коммутативность здесь опять-таки очевидна, ассоциативность доказывается очень легко. Вычитание на множестве $\mathbf{Z}$ служит примером операции, не коммутативной и не ассоциативной; первое очевидно, второе устанавливается без труда. А вот еще операция $\circ$, которая и не коммутативна, и не ассоциативна: на множестве $\mathbf{N}$ положим $a \circ b = a^b$.

В примерах, упомянутых в предыдущем абзаце, операции были либо одновременно коммутативны и ассоциативны, либо одновременно не коммутативны и не ассоциативны. Наблюдение такого типа, как обычно, вызывает вопрос, не связаны ли обсуждаемые два свойства зависимостью одного от другого. Примеры ассоциативных и некоммутативных операций легко обнаружить среди важных в математике операций. Одна из таковых – умножение квадратных матриц. Напомним соответствующее определение для случая матриц 2-го порядка (с элементами, например, из $\mathbf{R}$). Полагают

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}.$$

Прямой подсчет убеждает в ассоциативности этого умножения. Вместе с тем, оно некоммутативно, так как существуют неперестановочные матрицы. Например,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};$$

первое произведение равно

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

второе произведение равно

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Можно указать и совсем простой пример ассоциативной и некоммутативной операции; такова, например, операция $\circ$ на произвольном неодноэлементном множестве, заданная правилом $a \circ b = a$. Примером операции, которая коммутативна, но не ассоциативна, служит операция $\circ$ на $\mathbf{R}$, заданная правилом $a \circ b = |a - b|$.

Если на множестве A заданы две бинарные операции $\circ$ и $*$, то тождества

$$\begin{aligned} x \circ (y * z) &= (x \circ y) * (x \circ z), \\ (y * z) \circ x &= (y \circ x) * (z \circ x) \end{aligned} \qquad (8)$$

называют соответственно *левым* и *правым дистрибутивными законами* операции $\circ$ относительно операции $*$. Операция $\circ$ может не быть коммутативной, поэтому оба варианта дистрибутивности заслуживают выделения и выполнение одного из тождеств (8) вовсе не обязательно влечет за собой выполнение другого. Так, если на множестве $\mathbf{N}$ символ $\circ$ обозначает возведение в степень, а $*$ – умножение, то из тождеств (8) выполняется только второе. Если же операция $\circ$ коммутативна, то, разумеется, каждое из тождеств (8) влечет другое и в этом случае говорят просто о дистрибутивном законе (опуская прилагательные "левый" и "правый"). Один из важнейших примеров такой ситуации дают числовые множества, рассматриваемые относительно операций сложения и умножения, где сложение играет роль операции $*$, а умножение – роль операции $\circ$; мы уже записывали соответствующее тождество, см. формулу (3). Если поменять здесь роли, то тождества (8) выполняться не будут, в чем легко убедиться. А вот в следующих примерах дистрибутивный закон оказывается верным при любом "назначении на роли" операций $\circ$ и $*$. Рассмотрим множество $\mathbf{N}$ относительно операций Δ и ∇. Не очень трудно убедиться, что здесь имеет место и дистрибутивность Δ относительно ∇, и дистрибутивность ∇ относительно Δ. На любом подмножестве множества $\mathbf{R}$ для операций $\wedge$ и $\vee$ тоже имеет место дистрибутивность каждой из них относительно другой.

Если на каком-то множестве заданы бинарная операция $\circ$ и унарная операция $'$, то они могут быть связаны теми или иными тождествами. Типичный пример – тождество $(x \circ y)' = x' \circ y'$. Оно, например, выполняется на множестве **R**, если $\circ$ интерпретируется как сложение, а штрих – как взятие противоположного элемента.

Дальнейший разговор о тождествах требует рассмотрения вопроса о следовании одних тождеств из других. Мы коснемся его в п. 4, но прежде сделаем отступление.

3. НЕСКОЛЬКО ЗАМЕЧАНИЙ ДИДАКТИЧЕСКОГО ХАРАКТЕРА

В этом пункте мне хочется обратить внимание читателя-педагога на некоторые моменты при изложении в школьном курсе математики определений и свойств, относящихся к тождествам.

3.1. Пусть операция $\circ$ ассоциативна (например, под $\circ$ можно понимать сложение или умножение чисел). Согласно определению, это означает, что результат ее применения к любым трем элементам a, b, c из рассматриваемого множества, взятым в определенном порядке (скажем, именно так: a, b, c), не зависит от того, как расставлены скобки: $(a \circ b) \circ c$ или $a \circ (b \circ c)$. Это позволяет договориться вообще в соответствующем выражении, не опасаясь недоразумений, не ставить скобки, то есть писать $a \circ b \circ c$. Объяснение как обоснованности наличия подобных соглашений, так и их роли является одним из многочисленных компонентов воспитания математической культуры учащихся.[1] Между тем, в данном конкретном случае учащиеся привыкли видеть записи без скобок вида $a + b + c$ (и аналогичные записи произведений, причем и с более чем тремя слагаемыми или множителями) задолго до знакомства с сочетательным законом. Налицо – если иметь в виду не формальное заучивание материала учеником (что, к сожалению, нередко приходится обнаруживать), а вдумчивое овладение им – определенная коллизия. Впрочем, можно сказать, что она ликвидируется тем, что в записи типа $a + b + c$ подразумевается выполнение действий по порядку слева направо, то есть, по определению, $a + b + c = (a + b) + c$. Но тогда формулу сочетательного закона надо бы записывать в виде $a + b + c = a + (b + c)$. (Так, кстати, и поступают, ничтоже сумняшеся, авторы некоторых учебников.) Однако последнюю запись в качестве записи закона нельзя считать удовлетворительной с психологической точки зрения: в ней пропадает естественная в данной ситуации симметричность в облике левой и правой частей тождества, а отсутствие в левой части явного распределения скобок "затемняет" суть соответствующего тождества; внушать же учащимся, что в записи $a + b + c$ предписан определенный порядок действий значило бы как раз мешать воспитанию обсуждаемой установки при восприятии такой записи, а именно – установки, что порядок действий здесь может быть любой!

Так или иначе, перед учителем в этой и других подобных ситуациях стоит определенная дидактическая задача, и требуется проявить мастерство, чтобы в нужные моменты дать необходимые пояснения и комментарии, сделать должные акценты, сформулировать возникающие договоренности.

3.2. Для ассоциативной операции $\circ$ привычны записи типа $a_1 \circ a_2 \circ \ldots \circ a_n$ и при $n > 3$; в частности, складывая и перемножая числа, мы пишем $a_1 + a_2 + \ldots + a_n$ и $a_1a_2 \ldots a_n$. Корректность таких записей обусловлена тем, что результат последовательного применения рассматриваемой операции не зависит от расстановки скобок. Но надо ясно понимать, что указанная независимость есть вовсе не само собой разумеющийся факт, а теорема, которая доказывается методом математической индукции. Доказательство сравнительно короткое, но из-за недостатка места мы не будем приводить его; заинтересованный читатель может найти его в некоторых книгах, например, в [2, с. 136]; [3, с. 56]. В условиях школьного преподавания в большинстве случаев вряд ли удастся сообщить учащимся доказательство упомянутой теоремы, но, как бы ни поступил учитель в этой и других сходных ситуациях, он должен ясно сознавать, какова допускаемая им "мера умолчания". В том частном случае, когда в произведении все множители равны, мы приходим к понятию степени и к стандартным записям типа a^n. И здесь, разумеется, надо ясно понимать, что корректность подобных записей обеспечивается ассоциативностью умножения.

---

[1] Чтобы оттенить роль тождества ассоциативности, пишущий эти строки в своем общении со студентами-первокурсниками или школьниками старших классов иногда предлагает такой вопрос: чему равна дробь 2/3/5? Вызывающий оживление, он обычно не находит сразу должного ответа. Раздаются реплики: "две пятнадцатых", "десять третьих" что позволяет уверенно утверждать, что хотя бы один из предложенных ответов неверен), "а какая черта длиннее?" (что намного лучше, ибо демонстрирует обоснованный дискомфорт, вызванный заданным вопросом, и попытку избавиться от него), "надо поставить скобки" (что просто хорошо, ибо приближает нас к сути дела). После этого, что особенно связно получается, если прозвучит реплика подобие последней, я намечаю возможный адекватный отклик в виде следующего диалога между профессором и студентом:

– Чему равна дробь 2/3/5/?

– Ваш вопрос некорректен.

– Почему же?

– Потому что в предложенной записи не указан порядок выполнения действий, например, при помощи скобок.

– А зачем это делать? Ведь, скажем, в аналогичной записи $2 \cdot 3 \cdot 5$ (где вместо черты как знака деления фигурирует точка как знак умножения) нет скобок!

– Дело в том, что умножение ассоциативно, поэтому результат не зависит от расстановки скобок, а деление (в множестве ненулевых чисел) – операция неассоциативная, так что для корректности записи нужно расставить скобки.

В заключение я обращаю внимание удовлетворенных слушателей на существование аналогичной проблемы однозначности "декодирования" не только в математике: классический пример – фраза "казнить нельзя помиловать".

3.3. Коснемся еще вопроса о словесных формулировках некоторых основных тождеств, употребляемых в школьной практике. Прежде всего важно подчеркивать учащимся, что в соответствующих фактах фигурируют *любые* числа. Этот акцент без труда реализуется в “академических” формулировках типа “для любых чисел a и b верно равенство $a+b=b+a$”. Но имеются варианты формулировок, где буквы, обозначающие числа, не используются. Классический пример – упомянутая в начале статьи формулировка переместительного закона. Она отличается афористичностью и прочно сохраняется в памяти даже тех, кто “навсегда” расстается с математикой после окончания школы. В этом отношении сочетательному и распределительному законам повезло меньше. Обсудим, например, следующую расхожую формулировку сочетательного закона (для случая сложения): “Чтобы к сумме двух чисел прибавить третье число, можно к первому числу прибавить сумму второго и третьего чисел”. (Иногда здесь вместо слова “можно” употребляют “достаточно”.) Почему приведенную формулировку следует, на мой взгляд, считать неудачной? Во-первых, она не обладает желательной краткостью. Во-вторых, она, так сказать, несимметрична, то есть неоправданно ориентирует восприятие только на переход от левой части тождества к правой. В-третьих, и это особенно существенно, она не констатирует некое равенство, некую инвариантность (что должно быть присуще “закону”, представляющему собой тождество), а носит характер рецепта, что, к тому же, нарушает желательную однотипность формулировок переместительного и сочетательного законов. Когда автор совместно с сотрудниками работал над школьным учебником [1], возникло желание придумать для сочетательного закона – в дополнение к академической формулировке с явной записью тождества ассоциативности – словесную формулировку, родственную упомянутой афористичной формулировке переместительного закона. В результате родилась такая формулировка: *от изменения расстановки скобок сумма* (*произведение*) *не меняется*.

4. СЛЕДОВАНИЕ ОДНИХ ТОЖДЕСТВ ИЗ ДРУГИХ

Наличие одного или нескольких тождеств, выполняющихся для данной совокупности операций (в частности, для одной операции) на фиксированном множестве, позволяет выводить новые тождества для рассматриваемых операций. Например, если операция $\circ$ коммутативна и ассоциативна, то среди прочих выполняется тождество $(x \circ (y \circ x)) \circ x = ((x \circ x) \circ x) \circ y$. Оно получается следующей цепочкой равенств, в каждом из которых используется тождество коммутативности или тождество ассоциативности:

$$(x \circ (y \circ x)) \circ x = (x \circ (x \circ y)) \circ x = ((x \circ x) \circ y) \circ x =$$
$$= (x \circ x) \circ (y \circ x) = (x \circ x) \circ (x \circ y) = ((x \circ x) \circ x) \circ y.$$

Можно дать общее определение того, что данное тождество $f=g$ есть следствие данной совокупности тождеств Σ. Мы не будем останавливаться на строгих формулировках, приводящих к этому определению. Смысл же его состоит в том, что в таком тождестве $f=g$ выражение g получается из выражения f цепочкой равенств, в каждом из которых (аналогично разобранному только что примеру) применяется одно из тождеств системы Σ. Разумеется, проходя по такой цепочке в обратном направлении, мы получим из выражения g выражение f. Система Σ может, в частности, состоять из одного тождества.

При рассмотрении одной бинарной операции чаще всего договариваются называть эту операцию умножением (и преимущественно не пишут точку как знак умножения). В свете такой договоренности упомянутая в п. 3.2. теорема означает, другими словами, что из тождества $(xy)z = x(yz)$ следуют всевозможные тождества вида $u(x_1, ..., x_n) = \upsilon(x_1, ..., x_n)$, $n \geq 3$, где каждое из выражений u, υ представляет собой произведение переменных $x_1, ..., x_n$, записанных именно в таком порядке, с произвольной расстановкой скобок. (Например, при $n = 4$ имеется всего пять произведений указанного типа: $((x_1x_2)x_3)x_4$, $(x_1(x_2x_3))x_4$, $x_1((x_2x_3)x_4)$, $x_1(x_2(x_3x_4))$, $(x_1x_2)(x_3x_4)$.) Из тождеств ассоциативности и коммутативности умножения следует, как нетрудно убедиться, привычное глазу изучавшего школьную математику тождество

$$(xy)^n = x^n y^n \tag{9}$$

при любом n. Конечно, при $n=1$ (9) выполняется и без каких бы то ни было ограничений на умножение, но уже при $n=2$ тождество (9) может не выполняться; действительно, $(xy)^2 = xyxy$ и поставить рядом оба множителя x, вообще говоря, не удастся.

В заключение этого пункта еще упомянем привычные в школьной математике тождества (4), (5). Читателю предлагается проследить, что первое из тождеств (5) есть следствие ассоциативности сложения, коммутативности умножения и дистрибутивности умножения относительно сложения с учетом договоренности заменять сумму $ab+ab$ записью $2ab$ (которая, заметим, в общем случае вовсе не обязана означать произведение 2 и ab, такое произведение может попросту не иметь смысла). Следствием каких тождеств являются два других упомянутых тождества, мы отметим в следующем пункте.

5. АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ И ИХ ТОЖДЕСТВА

Алгебраической системой называется множество с заданными на нем алгебраическими операциями. Ясно, что рассмотрение алгебраических тождеств происходит всегда в рамках тех или иных алгебраических систем. Осознание этого обстоятельства приводит к очень многим постановкам задач и даже направлениям исследований. Так, при изучении тождеств, выполняющихся в алгебраических системах, естественно возникают вопросы о таких совокупностях тождеств Σ данной алгебраической системы A, что любое тождество, выполняющееся в A, является следствием из Σ. Всякую совокупность Σ с указанным свойством принято называть *базисом тождеств* алгебраической системы A. Отметим, что множество всех тождеств, выполняющихся в любой алгебраической системе, бесконечно, поэтому особый интерес вызывают ситуации, когда рассматриваемые системы имеют конечный базис тождеств. Это приводит к проблемам выяснения, существуют или отсутствуют такие базисы.

В алгебре выделен целый ряд основных типов алгебраических систем. Ниже для трех из них (полугрупп, групп и колец) мы очень кратко рассмотрим некоторые первоначальные свойства, связанные с тождествами, и, кроме того, сформулируем несколько существенных результатов о конечных базисах тождеств, а также одну открытую проблему.

5.1. *Полугруппой* называется множество с заданной на нем бинарной ассоциативной операцией. Если эта операция коммутативна, то полугруппа называется *коммутативной*. Принципиальным фактом о тождествах, выполняющихся в любой полугруппе, является теорема, упомянутая в п. 3.2. Школьная математика фактически имеет дело с многими полугруппами, начиная с аддитивной и мультипликативной полугрупп натуральных чисел. Небезынтересно разобраться в базисах тождеств таких полугрупп. Рассмотрим для примера три мультипликативные полугруппы: $S_1 = \mathbf{N}$, $S_2 = \{0, 1\}$, $S_3 = \{-1, 1\}$. Можно показать, что S_1 имеет базис тождеств, состоящий из двух "основополагающих" тождеств $(xy)z = x(yz)$, $xy = yx$, S_2 (соответственно S_3) имеет базис из трех тождеств, состоящий из только что указанных тождеств плюс тождество $x^2 = x$ (соответственно тождество $x^2y = y$). Высказанные утверждения (достаточно банальные для специалистов) могут быть предложены в качестве интересных и нетривиальных задач для студентов или продвинутых школьников на факультативных занятиях.

5.2. *Группой* называется множество (скажем, G) с заданной на нем бинарной операцией (скажем, $\circ$), удовлетворяющей следующим условиям: а) операция $\circ$ ассоциативна, б) в G существует нейтральный элемент e, определяемый равенствами

$$e \circ x = x \circ e = x \qquad (10)$$

при любых x из G, в) для любого x из G существует симметричный к нему элемент x', определяемый равенствами

$$x \circ x' = x' \circ x = e. \qquad (11)$$

Азбучны и вполне тривиальны факты, что нейтральный элемент единствен и каждый элемент группы обладает единственным симметричным к нему элементом; тем самым фиксирование e можно рассматривать как нуль-арную операцию, а отображение $x \longmapsto x'$ есть унарная операция. Таким образом, группу можно рассматривать и как алгебраическую систему с одной бинарной операцией, то есть как специальный тип полугруппы, и как алгебраическую систему с тремя операциями — бинарной, унарной (взятие симметрического элемента) и нуль-арной (фиксирование нейтрального элемента). В мультипликативной терминологии нейтральный элемент, как известно, называют *единицей*, а симметричный элемент к данному — *обратным элементом*; в аддитивной терминологии используются соответственно термины *нуль* и *противоположный элемент*.

Понятие группы принадлежит к числу наиболее важных понятий алгебры. В школьной математике главные представители групп — аддитивные группы $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, а также мультипликативные группы $\mathbf{Q}\backslash\{0\}$, $\mathbf{R}\backslash\{0\}$. Все они коммутативны. Заметим, что коммутативную группу принято называть *абелевой*.

Вернемся к определению группы. Мы видим, что в нем условие а) представляет собой выполнимость тождества, а условия б) и в) не имеют характера тождеств для операции $\circ$. Возникает вопрос: можно ли задать класс групп какой-либо совокупностью тождеств для бинарной операции? Ответ отрицателен и довольно легко может быть обоснован доказательством от противного. Однако, если посмотреть на группу как на алгебраическую систему с тремя указанными выше операциями — бинарной, унарной и нуль-арной, — то класс всех групп может быть задан тождествами. А именно, тогда не только условие а), но также условия б) и в) из определения группы оказываются тождествами; явный вид последних дают формулы (10) и (11). Если u и υ — выражения с переменными, связанными групповыми операциями, то легко понять, что тождество $u = \upsilon$ выполняется в данной группе тогда и только тогда, когда в ней выполняется тождество $u \circ \upsilon' = e$. Следовательно, при изучении групповых тождеств можно без ограничения общности иметь дело только с тождествами вида $w = e$. Так почти всегда и поступают в теории групп.

В качестве следствий из тождеств, определяющих группу, могут быть выведены многие полезные тождества. Одно из важнейших следствий — тождество $(x \circ y)' = y' \circ x'$. Среди других полезных следствий отметим тождество $(x')' = x$. В мультипликативной (аддитивной) записи оно имеет вид $(x^{-1})^{-1} = x$ (соответственно $-(-x) = x$). Читателю предлагается вывести указанные тождества.

Любопытно, что множества всех тождеств аддитивных групп $\mathbf{Z}$, $\mathbf{Q}$ и $\mathbf{R}$ совпадают; в качестве базиса их тождеств можно взять тождества, определяющие группу, плюс тождество коммутативности групповой операции.

5.3. *Кольцом* называется множество с заданными на нем двумя бинарными операциями, называемыми сложением и умножением и удовлетворяющими следующим условиям: а) для сложения выполняются аксиомы абелевой группы, б) выполняются левый и правый дистрибутивные законы умножения относительно сложения. Для уменьшения числа скобок в записи выражений в кольцах пользуются стандартным соглашением, что умножение "связывает теснее", нежели сложение, так что упомянутые дистрибутивные законы (ср. их записи в общем виде (8)) записываются привычным для глаза образом: $x(y + z) = xy + xz$, $(y + z)x = yx + zx$. Кольцо, в котором умножение коммутативно (ассоциативно), принято называть *коммутативным* (соответственно *ассоциативным*). Наиболее важные примеры колец, встречающиеся в школьной математике, – кольца **Z**, **Q** и **R** относительно обычных операций сложения и умножения. Все они коммутативны и ассоциативны; **Q** и **R** являются даже полями, но на понятии поля мы здесь не будем останавливаться.

С учетом сказанного в п. 5.2, ясно, что класс всех колец задается тождествами для бинарных операций сложения и умножения, унарной операции взятия противоположного элемента и нуль-арной операции фиксирования нуля 0. Подчеркнем, что 0 по определению есть нейтральный элемент аддитивной группы кольца, то есть элемент, участвующий в тождестве $x + 0 = x$. Для числового же нуля очень привычно его "пожирающее" мультипликативное свойство

$$x0 = 0x = 0, \tag{12}$$

которое хорошо запоминают дети еще в начальной школе. Свойство (12) объясняется в школе каким-либо "содержательным" способом. Но весьма примечательно то, что это свойство, представляющее собой совокупность двух тождеств, не есть прерогатива числа нуль, а выполняется для нуля произвольного кольца, то есть следует из тождеств, участвующих в определении кольца. Вот цепочка равенств, доказывающая тождество $x0 = 0$ (для тождества $0x = 0$ такая цепочка совершенно аналогична): $x0 = x0 + 0 = x0 + (x0 + (-x0)) = (x0 + x0) + (-x0) = x(0 + 0) + (-x0) = x0 + (-x0) = 0$. Читателю предлагается проследить, какие именно условия из определения кольца применялись в каждом равенстве этой цепочки.

Привычное глазу тождество (7), выражающее левую дистрибутивность умножения относительно вычитания, также есть следствие кольцевых аксиом. Читателю предлагается найти соответствующий вывод, а также доказать, что второе из тождеств (5) выполняется в данном кольце тогда и только тогда, когда это кольцо коммутативно.

5.4. Как уже отмечалось, множество всех тождеств, выполняющихся в любой алгебраической системе, бесконечно. Но при этом во многих важных случаях рассматриваемые системы имеют конечный базис тождеств; несколько примеров таких полугрупп и групп мы приводили выше. Уместен вопрос: существуют ли полугруппы и группы, не имеющие конечного базиса тождеств? Такие группы удалось найти в конце 60-х годов; этим была решена проблема, стоявшая открытой более 30 лет. Примеры полугрупп с тем же свойством были указаны ранее, в начале 60-х годов. Аналогичные же примеры ассоциативных колец до сих пор не найдены. Другими словами, не известно, каждое ли ассоциативное кольцо имеет конечный базис тождеств. Эта проблема (один из вариантов так называемой проблемы Шпехта) принадлежит к числу наиболее интригующих открытых проблем в современной алгебре.

А что можно сказать о базисах тождеств конечных алгебр? В 60-х годах было установлено, что любая конечная группа имеет конечный базис тождеств. Десять лет спустя аналогичный факт был получен для конечных ассоциативных колец. Для полугрупп же ситуация иная: существует шестиэлементная полугруппа, не имеющая конечного базиса тождеств. Это мультипликативная полугруппа, состоящая из матриц

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Указанный удивительный факт был установлен в конце 60-х годов. Сразу же возник вопрос: а как обстоит дело с полугруппами, содержащими менее шести элементов? В конце концов, к середине 80-х годов было доказано, что любая такая полугруппа имеет конечный базис тождеств.

5.5. В заключение отметим, что в огромном числе работ, относящихся к самым разным областям современной алгебры, так или иначе приходится иметь дело с тождествами алгебраических систем. Собственно исследованиям, связанным с тождествами, посвящено в общей сложности уже, пожалуй, несколько тысяч работ. Сформировалось широкое направление исследований, называемое *теорией многообразий* (*многообразием* в данном контексте принято называть всякий класс алгебраических систем, который может быть задан некоторой совокупностью тождеств). Имеется немало обобщающих трудов (книг, обзорных статей), полностью или частично относящихся к проблематике теории многообразий. Мы ограничимся здесь упоминанием для заинтересованного читателя лишь книг [4 – 8] и обзорных статей [9, 10]. Из научно-популярных трудов упомянем книгу [11], в которой простым и доходчивым языком освещаются многие основные понятия современной алгебры; естественно, в книге в соответствующих местах появляются и тождества.

ЛИТЕРАТУРА

1. *Шеврин Л.Н.*, *Гейн А.Г.*, *Коряков И.О.*, *Волков М.В.* а) Математика 5 – 6. Учебник-собеседник. М.: Просвещение, 1989; б) Математика 5. Учебник-собеседник. М.: Просвещение, 1992, 1994; в) Математика 6. Учебник-собеседник. М.: Просвещение, 1992, 1995.

2. *Кострикин А.И.* Введение в алгебру. М.: Наука, 1977.
3. *Скорняков Л.А.* Элементы алгебры М.: Наука, 1986.
4. *Нейман Х.* Многообразия групп. М.: Мир, 1970.
5. *Адян С.И.* Проблема Бернсайда и тождества в группах. М.: Наука, 1975.
6. *Бахтурин Ю.А.* Тождества в алгебрах Ли. М.: Наука, 1985.
7. *Кострикин А.И.* Вокруг Бернсайда. М.: Наука, 1986.
8. *Смирнов Д.М.* Многообразия алгебр. Новосибирск: Наука, 1992.
9. *Шеврин Л.Н.*, *Волков М.В.* Тождества полугрупп // Изв. вузов. Математика. 1985. № 11. С. 3 – 47.
10. *Бахтурин Ю.А.*, *Ольшанский А.Ю.* Тождества. Итоги науки и техн. Современные проблемы математики. Фундаментальные направления. Т. 18. М.: ВИНИТИ АН СССР, 1987. С. 117 – 240.
11. *Фрид Э.* Элементарное введение в абстрактную алгебру. М.: Мир, 1979.

* * *

Лев Наумович Шеврин, доктор физико-математических наук, профессор, зав. кафедрой алгебры и дискретной математики Уральского государственного университета, заслуженный деятель науки Российской Федерации, академик Академии гуманитарных наук. Лауреат Международной премии по образованию им. Хосе Васконселоса Всемирного Совета по Культуре. Автор более 160 работ, в том числе двух монографий, двух школьных учебников, трех научно-художественных книг по математике для маленьких детей.