Десять доказательств основной теоремы алгебры

В. М. Тихомиров В. В. Успенский

1. Введение

Всякий многочлен степени $\geqslant 1$ с комплексными коэффициентами имеет комплексный корень. Эту теорему часто называют *основной теоремой алгебры*. Это один из самых фундаментальных результатов во всей математике. Существуют разные точки зрения по вопросу о том, кто первым доказал эту теорему (и что вообще это означает: «доказать теорему»). Ее называют и «теоремой Даламбера» [16], и «теоремой Эйлера–Лагранжа» [3], однако чаще всего связывают с именем Гаусса (считается, что Гаусс дал четыре доказательства основной теоремы).

Дадим слово Феликсу Клейну [4, с. 69]:

> «Основная теорема алгебры сформулирована и в известной мере доказана Даламбером в его „Recherches sur le calcul intégral“ („Исследования по интегральному исчислению“, 1746 г.). $< \cdots >$ Французы поэтому и сейчас называют эту теорему „теоремой Даламбера“, а Гаусс назвал свою диссертацию „demonstratio nova“ („новое доказательство“), чем, следовательно, подчеркнул, что он никоим образом не претендует на достижение, которое так часто ему приписывается, — создание „первого строгого доказательства“ этой теоремы. Разумеется, его сочинение начинается подробной критикой всех предшествующих доказательств».

А вот что пишет по этому поводу Н. Бурбаки [2, с. 161–162] (цитируем с некоторыми сокращениями):

> «В течение XVII и XVIII вв. математики постепенно приходят к убеждению, что мнимые числа, дающие возможность решать уравнения второй степени, позволяют также решать алгебраические уравнения любой степени. В XVIII в. были опубликованы многочисленные попытки доказательства этой теоремы; среди них не было ни одной, которая бы не вызывала серьезных возражений. В результате внимательного изучения всех попыток доказательств и детальной критики их пробелов Гаусс поставил целью своей диссертации (написанной в 1797 г., изданной в 1799 г.) дать, наконец, строгое доказательство. Взяв за основу идею, высказанную мимоходом Даламбером, он замечает, что точки (a, b) плоскости,

> для которых $a + bi$ являются корнями многочлена $P(x + yi) = X(x, y) + +iY(x, y)$, представляют собой точки пересечения кривых $X = 0$ и $Y = 0$. Путем качественного изучения этих кривых он показывает, что кривые пересекаются. Это доказательство по своей ясности и оригинальности представляет замечательный прогресс по сравнению со всеми предшествующими и является примером чисто топологического рассуждения, примененного к алгебраической проблеме.»

Гаусс, критикуя рассуждение Даламбера, добавляет, что «истинный стержень доказательства не затрагивается всеми этими возражениями». Действительно, с современной точки зрения пробелы в доказательстве Даламбера легко устранить. Суть этого доказательства такова. Пусть $p(z)$ — многочлен с комплексными коэффициентами. Рассмотрим точку a, в которой функция $|p(z)|$ достигает минимума. Тогда $p(a) = 0$, так как иначе можно было бы найти направление, при движении вдоль которого из точки a модуль функции $p(z)$ уменьшался бы. Здесь все правильно, но почему $|p(z)|$ достигает минимума? Современный ответ краток: по соображениям компактности. Однако в 1746 г., когда появилось доказательство Даламбера, до теоремы Больцано–Вейерштрасса: всякая ограниченная последовательность имеет предельную точку — оставалось еще около века. Привычное же определение компактности: всякое открытое покрытие содержит конечное подпокрытие — появилось уже в нашем веке, когда П. С. Александров и П. С. Урысон приняли за определение свойство отрезка, установленное Борелем и Лебегом.

Доказательства Эйлера и Лагранжа также содержали «истинные стержни», но имели и серьезные упущения с точки зрения современных понятий о строгости. Вообще говоря, то же можно сказать и о гауссовских доказательствах: использованные в них «очевидные» топологические факты нуждаются в обосновании. Впрочем, во втором доказательстве Гаусса все сводилось к минимуму: к тому, что вещественный полином нечетной степени имеет вещественный корень.

Сейчас известно много различных доказательств основной теоремы алгебры; ниже мы приводим десять из них. Разумеется, чтобы убедиться в истинности какого-либо утверждения, в математике достаточно одного доказательства (это отличие математики от исторической науки сыграло важную роль при выборе великим математиком А. Н. Колмогоровым своей профессии — см. [17, с. 4]). Но наша цель состоит как раз в том, чтобы показать разнообразие методов, которые можно применить для доказательства основной теоремы алгебры, и тем самым установить связи этой теоремы с топологией, комплексным анализом и другими областями математики. Рассматриваемая нами теорема как никакая другая подходит для подобных целей.

Наши доказательства сильно варьируются по уровню того, что предполагается известным, и потому не все они одинаково хорошо подходят для первоначального знакомства с теоремой. Доказательства 1 и 7 опираются на минимум предварительных сведений, а в других доказательствах мы ссылаемся на теорию Галуа или на теорему Лефшеца о неподвижной точке, не смущаясь тем, что соответствующие понятия не входят в обязательную университетскую программу. Заинтересованный читатель сумеет найти необходимые сведения в цитируемой литературе. Во многих доказательствах мы пользуемся понятием голоморфной функции и римановой поверхности; эти понятия восходят к Коши, Риману и Герману Вейлю.

В основе большинства доказательств основной теоремы алгебры лежит идея геометрического изображения комплексных чисел: множество комплексных чисел отождествляется с плоскостью. Эта идея принадлежит Гауссу и развивает великую мысль Декарта о единстве алгебры и геометрии: каждой точке плоскости или пространства можно поставить в соответствие числа — ее координаты, после чего язык алгебры и язык геометрии становятся взаимозаменяемыми. Сейчас это кажется настолько привычным, что трудно представить, насколько революционными были эти идеи в свое время.

2. Эквивалентные формулировки

Понятие комплексного числа мы считаем известным (см. [7, 5]). Напомним лишь, что всякое комплексное число однозначно записывается в виде $a + bi$, где a и b — действительные числа, а i — мнимая единица, удовлетворяющая равенству $i^2 = -1$. Комплексные числа можно складывать и умножать по обычным правилам, при этом каждое ненулевое комплексное число z имеет обратное z^{-1}. Таким образом, комплексные числа образуют *поле*. Это поле обозначается через $\mathbb{C}$.

Для произвольного поля K через $K[X]$ обозначается *кольцо многочленов над* K (или *с коэффициентами в* K). Многочлен с коэффициентами в K — это формальное выражение вида

$$p(X) = a_nX^n + \cdots + a_1X + a_0, \text{ где } a_0, \ldots, a_n \in K.$$

Такой многочлен можно рассматривать как функцию из K в K, которая каждому $x \in K$ ставит в соответствие элемент $p(x) = a_nx^n + \cdots + a_1x + a_0 \in K$. *Корень* многочлена $p(X)$ — это такое $x \in K$, для которого $p(x) = 0$.

Степень ненулевого многочлена $p(X)$ — это такое целое число n, для которого $p(X) = a_n X^n + \dots + a_0$ и $a_n \neq 0$.

Лемма 1. *Число различных корней ненулевого многочлена не превосходит его степени.*

Докажем лемму индукцией по степени n многочлена. Предположим, что многочлен $p(X) = a_n X^n + \dots + a_0$ степени n имеет по меньшей мере $n+1$ различных корней $a_1, \dots, a_{n+1}$. Рассмотрим многочлен $q(X) = a_n(X - a_1)\dots(X - a_n)$. Тогда $p \neq q$, так как $p(a_{n+1}) = 0 \neq q(a_{n+1})$. Разность $r = p - q$ является ненулевым многочленом степени $< n$, имеющим по меньшей мере n корней $a_1, \dots, a_n$. Это противоречит предположению индукции.

Если поле K бесконечно (о строении конечных полей см. [5, 9]), то всякий ненулевой многочлен $p(X)$ представляет ненулевую функцию (поскольку число корней многочлена $p(X)$ конечно) и, следовательно, различные многочлены представляют различные функции.

Многочлены нулевой степени отождествляются с ненулевыми элементами поля K и корней не имеют. Всякий многочлен первой степени имеет ровно один корень. Всякий ли многочлен степени $\geqslant 2$ имеет хотя бы один корень? Ответ зависит от поля K. Пусть $\mathbb{R}$ — поле действительных (или вещественных) чисел. Многочлен $X^2 + 1$, рассматриваемый как элемент кольца $\mathbb{R}[X]$, не имеет корней в $\mathbb{R}$, и именно это обстоятельство мотивирует расширение поля $\mathbb{R}$ до поля комплексных чисел $\mathbb{C}$, в котором многочлен $X^2 + 1$ имеет корни i и $-i$. Из каждого комплексного числа можно извлечь квадратный корень, поэтому известная формула для решения квадратного уравнения показывает, что всякий многочлен из $\mathbb{C}[X]$ второй степени имеет корень в $\mathbb{C}$. Если бы существовал многочлен p из $\mathbb{C}[X]$ степени > 2, не имеющий корней в $\mathbb{C}$, то можно было построить конечное расширение поля $\mathbb{C}$, в котором p имеет корень (по аналогии с тем, как само поле $\mathbb{C}$ получается присоединением к $\mathbb{R}$ корней многочлена $X^2 + 1$). *Конечное расширение* поля K — это поле L, содержащее K в качестве подполя и такое, что L является конечномерным векторным пространством над K. Размерность векторного пространства L над K называется *степенью* расширения L и обозначается через $[L : K]$. Одна из эквивалентных формулировок основной теоремы алгебры заключается в том, что у поля $\mathbb{C}$ нет собственных (т. е. отличных от самого поля $\mathbb{C}$) конечных расширений.

Теперь дадим общее определение: поле K называется *алгебраически замкнутым*, если всякий многочлен степени > 0 с коэффициентами в K

имеет корень в K. Эквивалентно, поле K алгебраически замкнуто, если у него нет собственных конечных расширений. Нам будет удобно использовать еще две характеризации алгебраически замкнутых полей. Многочлен над K называется *неприводимым*, если он имеет степень > 0 и не представи́м в виде произведения двух многочленов из $K[X]$ степени > 0. Неприводимые многочлены в кольце $K[X]$ аналогичны простым числам в кольце $\mathbb{Z}$ целых чисел: всякий многочлен из $K[X]$ раскладывается в произведение неприводимых, причем разложение однозначно с точностью до порядка сомножителей и их умножения на элементы из K. Это свойство кольца $K[X]$ вытекает из того, что $K[X]$ является *кольцом главных идеалов*: каждый идеал порождается одним элементом. Все многочлены степени 1 неприводимы, а обратное верно тогда и только тогда, когда поле K алгебраически замкнуто.

Пусть E — векторное пространство над полем K и $A : E \to E$ — линейный оператор. Вектор $v \in E$ называется *собственным вектором* оператора A, если $v \neq 0$ и $Av = \lambda v$ для некоторого $\lambda \in K$.

Теорема 1. *Для всякого поля K следующие условия равносильны:*

1) *всякий многочлен из $K[X]$ степени > 0 имеет корень в K (иными словами, поле K алгебраически замкнуто);*

2) *если E — конечномерное векторное пространство над K, не сводящееся к нулю, то всякий линейный оператор $A : E \to E$ имеет собственный вектор;*

3) *поле K не имеет конечных расширений, отличных от K;*

4) *всякий неприводимый многочлен над K имеет степень 1.*

1) $\Longrightarrow$ 2). Пусть $A : E \to E$ — линейный оператор и $p(X) = \det(X \cdot 1_E - A)$ — характеристический многочлен оператора A. Здесь 1_E — тождественный оператор в E. Если K алгебраически замкнуто, то многочлен p имеет корень. Следовательно, при некотором $\lambda \in K$ оператор $\lambda \cdot 1_E - A$ имеет нулевой определитель и потому $(\lambda \cdot 1_E - A)v = 0$ для некоторого ненулевого вектора $v \in E$. Тогда $Av = \lambda v$, так что v — собственный вектор оператора A.

2) $\Longrightarrow$ 3). Пусть L — конечное расширение поля K. Зафиксируем $x \in L$, и пусть $A : L \to L$ — линейный оператор умножения на x, определенный формулой $A(y) = xy$. Согласно 2), у оператора A есть собственный вектор над K. Таким образом, $xv = Av = \lambda v$ при некоторых $\lambda, v \in K$, $v \neq 0$. Следовательно, $x = \lambda \in K$ и $L = K$.

3) $\Longrightarrow$ 4). Если $p \in K[X]$ — неприводимый многочлен степени $n > 1$, то факторкольцо кольца $K[X]$ по идеалу, порожденному многочленом p, является собственным расширением поля K (степени n).

4) $\Longrightarrow$ 1). Это очевидно, поскольку всякий многочлен разлагается в произведение неприводимых.

Мы видим, что основную теорему алгебры можно сформулировать так: поле комплексных чисел удовлетворяет эквивалентным условиям теоремы 1. Можно дать еще одну по существу эквивалентную формулировку, относящуюся уже к полю $\mathbb{R}$ действительных чисел: *всякий неприводимый многочлен над* $\mathbb{R}$ *имеет степень* $\leqslant 2$. Покажем, что это утверждение равносильно алгебраической замкнутости поля $\mathbb{C}$. Для каждого $a \in \mathbb{C}$ пусть $p_a \in \mathbb{R}[X]$ — *минимальный многочлен* числа a, т. е. многочлен минимальной возможной степени, имеющий a своим корнем. Главный идеал $\{p \in \mathbb{R}[X] : p(a) = 0\}$ кольца $\mathbb{R}[X]$ порождается многочленом p_a. Иными словами, всякий многочлен из $\mathbb{R}[X]$, имеющий a своим корнем, делится на p_a. Если $a \in \mathbb{R}$, то $p_a = X - a$, если же $a \in \mathbb{C}\backslash\mathbb{R}$, то $p_a = (X-a)(X-\bar{a})$, где $\bar{a}$ означает число, комплексно сопряженное к a (если $a = x + yi$, $x, y \in \mathbb{R}$, то $\bar{a} = x - yi$). Предположим теперь известным, что поле $\mathbb{C}$ алгебраически замкнуто. Пусть $q \in \mathbb{R}[X]$ — произвольный многочлен степени > 2. Тогда q имеет корень $a \in \mathbb{C}$. Следовательно, q делится в $\mathbb{R}[X]$ на многочлен p_a степени $\leqslant 2$ и потому не является неприводимым. Обратно, пусть известно, что все неприводимые многочлены в $\mathbb{R}[X]$ имеют степень $\leqslant 2$. Тогда всякий отличный от константы многочлен из $\mathbb{R}[X]$ разлагается в произведение многочленов степени $\leqslant 2$ и потому имеет корень в $\mathbb{C}$. Пусть теперь p — отличный от константы многочлен над $\mathbb{C}$, а $\bar{p}$ — многочлен, полученный из p заменой всех коэффициентов на комплексно-сопряженные. Многочлен $p\bar{p}$ имеет вещественные коэффициенты и, следовательно, имеет корень $a \in \mathbb{C}$. Число a является корнем либо многочлена p, либо многочлена $\bar{p}$. В последнем случае $\bar{a}$ является корнем для p. Таким образом, p имеет корень.

3. Доказательства

Первое доказательство. ◀ Пусть $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ — многочлен степени $n \geqslant 1$ с комплексными коэффициентами (старший коэффициент мы считаем равным единице, это не ограничивает общности). Предположим, что p не имеет корней, и придем к противоречию.

Пусть z равномерно движется по окружности радиуса R с центром в нуле в положительном направлении (т. е. против часовой стрелки). Точка z^n будет при этом двигаться по окружности радиуса R^n с угловой скоростью, в n раз превосходящей угловую скорость точки z. Это следует из представления z в «тригонометрической форме»: если $z = R(\cos\varphi + \sin\varphi)$, то $z^n = R^n(\cos n\varphi + \sin n\varphi)$. Когда z совершает один полный оборот, точка z^n совершает n оборотов вокруг нуля. Положим $b(z) = a_{n-1}z^{n-1} + \dots + a_0$. При больших R число $b(z)$ пренебрежимо мало по сравнению с z^n, поэтому движение точки $p(z) = z^n + b(z)$, если наблюдать его издалека, будет практически неотличимо от движения точки z^n. Следовательно, точка $p(z)$ совершает столько же оборотов вокруг нуля, сколько и z^n, т. е. n оборотов. Существенно здесь то, что отрезок, соединяющий $p(z)$ с z^n, не проходит через 0 (при $|b(z)| < |z^n|$), поэтому движение точек $p(z)$ и z^n можно продеформировать одно в другое, не проходя при этом через 0 и тем самым не меняя числа оборотов.

С другой стороны, если R близко к нулю, то $p(z)$ близко к a_0. Когда z совершает полный оборот по окружности малого радиуса, $p(z)$ описывает замкнутую кривую вблизи a_0. Поскольку $a_0 \neq 0$ (иначе p имел бы корень 0), такая кривая не охватывает нуля, так что при малых R точка $p(z)$ совершает 0 оборотов вокруг нуля.

Будем теперь менять R и следить за тем, какое число $n(R)$ оборотов совершает точка $p(z)$ вокруг нуля, когда z делает один полный оборот по окружности радиуса R. «Число оборотов» точки $p(z)$ вокруг нуля было бы не определено, если бы эта точка при своем движении проходила через нуль. Так как мы предполагаем, что $p(z) \neq 0$ при всех z, то $n(R)$ определено при всех R. Ясно, что $n(R)$ непрерывно зависит от R. Поскольку функция $n(R)$ принимает только целые значения, она должна быть постоянна. Однако мы видели, что $n(R) = n$ при больших R и $n(R) = 0$ при малых R — противоречие. ▶

Комментарий. Это доказательство приводится в [6]. Неясно, кто придумал его первым; Колмогоров излагал его в своих лекциях в 30-е годы. Вот как пишут об этом В. Г. Болтянский и И. М. Яглом [8, с.11]: «В 1937 году в своей лекции „Основная теорема алгебры“ академик А. Н. Колмогоров изложил по существу полное доказательство теоремы о существовании комплексного корня у всякого алгебраического уравнения. Это доказательство, получившее в школьном кружке наименование „Дама с собачкой“ (если дама гуляет вокруг дома с собачкой на поводке, то собачка будет вынуждена сделать столько же оборотов вокруг дома, сколько и сама дама) впоследствии точно в такой же форме было опубликовано в [6].»

Ценители математической строгости могут остаться неудовлетворенными таким рассуждением: ведь мы не определили, что такое «число оборотов», и не доказали, что оно остается постоянным при непрерывных деформациях. Укажем, как устранить эти недостатки.

Пусть f — непрерывная комплексная функция, определенная на отрезке $[0,1]$ и принимающая равные значения на концах отрезка. Предположим, что $f(t) \neq 0$ при всех t. Тогда *число оборотов* вокруг нуля, совершаемых точкой $f(t)$ при движении t от 0 к 1 (это число мы будем обозначать через $W(f)$), определяется следующим образом. Пусть $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ — единичная окружность, и $e : \mathbb{R} \to \mathbb{U}$ — функция, определенная формулой $e(t) = \cos 2\pi t + i \sin 2\pi t$ (эта функция «наматывает» прямую на окружность). Предположим сперва, что f принимает значения в $\mathbb{U}$, то есть что $|f(t)| = 1$ при всех t. Существует непрерывная функция $h : [0,1] \to \mathbb{R}$, такая, что $f(t) = e(h(t))$ для всех $t \in [0,1]$. Если h' — другая функция с таким же свойством, то $h' = h + c$ для некоторой константы c (являющейся целым числом), поэтому целое число $W(f) = h(1) - h(0)$ определено однозначно. Это целое число и называется числом оборотов. В общем случае, когда значения функции f необязательно лежат в $\mathbb{U}$, полагаем $W(f) = W(g)$, где $g : [0,1] \to \mathbb{U}$ — функция, определенная формулой $g(t) = f(t)/|f(t)|$.

Пусть теперь для каждого $s \in [0,1]$ задана функция $f_s : [0,1] \to \mathbb{C}\setminus\{0\}$, такая, что $f_s(0) = f_s(1)$. Предположим, что семейство $\{f_s\}$ непрерывно зависит от параметра s в том смысле, что функция $F(s,t) = f_s(t)$ непрерывна на квадрате $[0,1]^2$. Тогда $W(f_s)$ не зависит от s (это и означает, что число оборотов не меняется при непрерывных деформациях). Для доказательства предположим, что значения функции F лежат в $\mathbb{U}$ (общий случай сводится к этому заменой функции F на $F/|F|$). Существует такая непрерывная функция $H : [0,1]^2 \to \mathbb{R}$, для которой $F = e \circ H$. Целое число $W(f_s) = H(s,1) - H(s,0)$ непрерывно зависит от s и потому постоянно.

При определении числа $W(f)$ и при доказательстве его инвариантности при деформациях мы пользовались следующим свойством функции $e : \mathbb{R} \to \mathbb{U}$: если X — отрезок или квадрат и $F : X \to \mathbb{U}$ — непрерывная функция, то существует непрерывная функция $H : X \to \mathbb{R}$ такая, что $F = e \circ H$. Такая функция H называется *поднятием* функции F относительно e. Существование поднятий в нашем случае нетрудно доказать непосредственно: например, если X — квадрат, то можно разбить X на маленькие квадратики, образ каждого из которых при F является собственным подмножеством окружности $\mathbb{U}$, и строить поднятие H последовательно на этих квадратиках, проходя их ряд за рядом. На самом деле отображение e является примером *накрытия*, и можно сослаться на общую теорему: отображение односвязного пространства всегда может быть поднято в накрытие [15, 13].

Мы определили отображение e через синус и косинус. При последовательном построении основ анализа более естественно поступить наоборот: сперва ввести отображение e, а затем через него определить синус и косинус [12]. Именно, $e(t) = e^{2\pi it}$, где $e^z = \sum_{n=0}^{\infty} z^n/n!$ для любого комплексного z. Отметим, что накрытие $e : \mathbb{R} \to \mathbb{U}$ является гомоморфизмом топологических групп.

Второе доказательство [10]. ◀ Многочлен $p \in \mathbb{C}[X]$ степени n задает отображение степени n комплексной проективной прямой в себя. Следовательно, это отображение сюръективно при $n > 0$. В частности, уравнение $p(z) = 0$ имеет решение. ▶

Комментарий. Поясним понятия, которые использованы в этом доказательстве. Для наших целей комплексную проективную прямую $\mathbb{C}P^1$ можно определить просто как одноточечную компактификацию пространства $\mathbb{C}$. Иными словами, $\mathbb{C}P^1 = \mathbb{C} \cup \{\infty\}$, причем окрестностями бесконечно удаленной точки служат дополнения до замкнутых ограниченных подмножеств в $\mathbb{C}$. Пространство $\mathbb{C}P^1$ имеет естественную структуру ориентированного гладкого многообразия, при этом $\mathbb{C}P^1$ диффеоморфно двумерной сфере. Отображение $p : \mathbb{C} \to \mathbb{C}$ продолжается до гладкого отображения $\hat{p} : \mathbb{C}P^1 \to \mathbb{C}P^1$ такого, что $\hat{p}(\infty) = \infty$.

Каждому непрерывному отображению между ориентированными компактными связными топологическими многообразиями одной размерности сопоставляется целое число, называемое *степенью* отображения. В первом доказательстве мы фактически ввели (под названием «число оборотов») понятие степени отображения окружности в себя. Для гладких отображений гладких многообразий степень можно определить следующим образом. Пусть $f : M \to N$ — гладкое отображение между k-мерными ориентированными компактными связными многообразиями. Точка $x \in M$ называется *критической*, если дифференциал df_x, являющийся линейным отображением касательного пространства T_xM в касательное пространство $T_{f(x)}N$, вырожден. Точка $y \in N$ называется *регулярным значением*, если она не является образом никакой критической точки $x \in M$. Из теоремы Сарда вытекает [10], что регулярные значения существуют. Пусть $y \in N$ регулярно. Тогда число точек $x \in X$, таких, что $f(x) = y$, конечно. Пусть $x_1, \ldots, x_p, x_{p+1}, \ldots, x_{p+q}$ — все такие точки, причем дифференциал отображения f сохраняет ориентацию в точках $x_1, \ldots, x_p$ и обращает ориентацию в точках $x_{p+1}, \ldots, x_{p+q}$. *Степенью* отображения f называется число $p - q$. Доказывается, что это число не зависит от выбора регулярного $y \in N$. Если $f(M)$ отлично от N, то степень равна нулю, так как любое $y \in N \setminus f(M)$ регулярно, а для такого y мы имеем $p = q = 0$. Таким образом, если степень отображения $f : M \to N$ отлична от нуля, то $f(M) = N$.

Для отображения $\hat{p} : \mathbb{C}P^1 \to \mathbb{C}P^1$ критическими точками служат нули производной p' и (при $n > 1$) точка ∞. Таких точек конечное число. Во всякой некритической точке z дифференциал является умножением на ненулевое комплексное число $p'(z)$ и потому сохраняет ориентацию. Отсюда вытекает, что степень отображения $\hat{p}$ положительна и, следовательно, $\hat{p}$ сюръективно. На самом деле степень отображения $\hat{p}$ равна n. Это следует из того, что для каждого регулярного y уравнение $p(z) = y$ имеет n различных решений.

Отображение $\hat{p} : \mathbb{C}P^1 \to \mathbb{C}P^1$ является *n-листным разветвленным накрытием* [14]. Для таких отображений корректность определения степени (т. е. независимость от выбора регулярного значения y) очевидна. Поэтому проведенное доказательство имеет вариант, не зависящий от общего определения степени.

Третье доказательство. Рассуждение, намеченное в предыдущем абзаце, можно обобщить.

◀ Непостоянное голоморфное отображение между компактными связными римановыми поверхностями является n-листным разветвленным накрытием при некотором $n > 0$ и потому сюръективно [14]. Применим эту теорему к отображению $\hat{p} : \mathbb{C}P^1 \to \mathbb{C}P^1$, определенному многочленом p степени $n > 0$. Комплексная проективная прямая $\mathbb{C}P^1$ имеет естественную структуру компактной связной римановой поверхности, а отображение $\hat{p}$ голоморфно. Следовательно, $\hat{p}$ сюръективно. В частности, p имеет корень. ▶

Комментарий. *Риманова поверхность* — это голоморфное многообразие комплексной размерности 1. Такое многообразие может быть покрыто открытыми множествами, каждое из которых биголоморфно эквивалентно (т. е. изоморфно как риманова поверхность) открытому единичному кругу U в $\mathbb{C}$. Всякое голоморфное отображение $f : X \to Y$ одной римановой поверхности в другую локально устроено так же, как отображение $z \mapsto z^k$ из U в себя при некотором $k > 0$ [14, предложение 2.1]. Точнее, пусть $x \in X$ и $y = f(x)$. Если f непостоянно на компоненте поверхности X, содержащей точку x, то существуют окрестности Ox и Oy точек x и y на X и Y, соответственно, изоморфизмы римановых поверхностей $\varphi : U \to Ox$ и $\psi : Oy \to U$ и целое число $k > 0$, такие, что $\varphi(0) = x$,

$\psi(y) = 0$, $f(Ox) = Oy$ и $\psi f \varphi(z) = z^k$ для всех $z \in U$. Каждая точка в $Oy \setminus \{y\}$ имеет ровно k прообразов в Ox. Число k называется *индексом ветвления* отображения f в точке x. Обозначим этот индекс через $e_f(x)$. Если $e_f(x) > 0$, то говорят, что f *разветвлено* в x. Предположим, что X и Y компактны и связны. Пусть $y \in Y$, $f^{-1}(y) = \{x_1, \ldots, x_p\}$, $k_i = e_f(x_i)$, $i = 1, \ldots, p$. У точки y есть такая окрестность Oy, что $f^{-1}(Oy) = Ox_1 \cup \cdots \cup Ox_p$, причем окрестности $Ox_1, \ldots, Ox_p$ попарно не пересекаются и отображение $f|Ox_i : Ox_i \to Oy$ изоморфно отображению $z \mapsto z^{k_i}$ круга U в себя, $i = 1, \ldots, p$. Положим $n = n(y) = k_1 + \cdots + k_p$. Для любого $y' \in Oy \setminus \{y\}$ прообраз $f^{-1}(y')$ состоит ровно из n точек, в каждой из которых отображение f не разветвлено, поэтому $n(y') = n$. Таким образом, функция $n(y)$ локально постоянна на Y. Ввиду связности Y она постоянна и всюду принимает значение n. В частности, $n(y) > 0$ для любого $y \in Y$, так что f сюръективно. Утверждение, что f является n-листным разветвленным накрытием, означает, что f устроено так, как описано выше.

Четвертое доказательство [14, 16]. ◀ Многочлен p степени n задает мероморфную функцию на $\mathbb{C}P^1$ с полюсом порядка n в точке ∞. Мероморфная функция на компактной римановой поверхности имеет одинаковое число нулей и полюсов, если каждый нуль и полюс считать столько раз, какова его кратность. Следовательно, многочлен p имеет, с учетом кратностей, ровно n нулей. ▶

Комментарий. *Мероморфная функция* на римановой поверхности X — это такая голоморфная функция $f : X \setminus D$, что D замкнуто и дискретно в X, а f имеет полюс в каждой точке $a \in D$, т. е. $\lim_{x\to a} |f(x)| = \infty$. Такую функцию можно отождествить с голоморфной функцией из X в $\mathbb{C}P^1$, которую мы обозначим снова через f. Определим *порядок* $\operatorname{ord}_x f$ функции f в точке $x \in X$. Предположим для простоты, что $X = U$ и $x = 0$. Существует и единственно такое целое k, что $f(z) = z^k g(z)$ при всех $z \in U \setminus \{0\}$, где g — голоморфная функция в U, такая, что $g(0) \neq$ $\neq 0$. Полагаем $\operatorname{ord}_x f = k$. Это определение переносится на произвольные римановы поверхности. Если $k = \operatorname{ord}_x f > 0$, то f имеет нуль порядка k (или кратности k) в точке x, если $\operatorname{ord}_x f = -k < 0$, то f имеет полюс порядка k.

Утверждение, что *мероморфная функция f на компактной римановой поверхности X имеет одинаковое число нулей и полюсов*, означает, что *сумма $\sum_{x\in X} \operatorname{ord}_x f$, в которой только конечное число членов отлично от нуля, равна нулю.* Будем рассматривать f как голоморфное отображение из X в $\mathbb{C}P^1$. Если x — нуль функции f, то индекс ветвления $e_f(x)$ равен порядку $\operatorname{ord}_x(f)$, если x — полюс, то $e_f(x) = -\operatorname{ord}_x(f)$. Таким образом, равенство $\sum_{x\in X} \operatorname{ord}_x f = 0$ вытекает из установленного в предыдущем доказательстве постоянства функции $y \mapsto n(y) = \sum_{f(x)=y} e(x)$, которая каждому $y \in \mathbb{C}P^1$ сопоставляет сумму индексов ветвления по всем точкам $x \in f^{-1}(y)$.

Дадим другое доказательство этого факта, основанное на понятии вычета дифференциальной формы и на теореме Стокса.

◀ Мероморфная дифференциальная форма ω в открытом множестве $X \subset \mathbb{C}$ записывается в виде $\omega = f\,dz$, где f — мероморфная функция в X. *Вычет* $\operatorname{res}_x \omega$ формы ω в точке $x \in X$ — это деленный на $2\pi i$ интеграл формы ω по краю маленькой окрестности точки x. Если f имеет полюс в точке x и $f(z) = \sum_{n=k}^{\infty} a_n(z-x)^n$, где $k = \operatorname{ord}_x f < 0$, то $\operatorname{res}_x f\,dz = a_{-1}$. Если f голоморфна в x, то $\operatorname{res}_x f\,dz = 0$. Понятие мероморфной формы и ее вычета в точке переносится на произвольные римановы поверхности.

Докажем, что *сумма вычетов мероморфной дифференциальной формы на компактной римановой поверхности равна нулю.* Пусть ω — мероморфная дифференциальная форма на компактной римановой поверхности X, и $x_1, \ldots, x_n \in X$ — все полюса формы ω. Окружим каждый полюс x_j маленькой открытой окрестностью V_j с гладкой границей и положим $V = V_1 \cup \cdots \cup V_n$. Тогда

$$\sum_{x\in X} \operatorname{res}_x \omega = \sum_{j=1}^{n} \operatorname{res}_{x_j} \omega = \sum_{j=1}^{n} \int_{\partial V_j} \omega/2\pi i = \int_{\partial V} \omega/2\pi i.$$

При этом считается, что V имеет естественную ориентацию римановой поверхности, а ∂V имеет ориентацию края. Рассмотрим ориентированное компактное многообразие с краем $Y = X \setminus V$. Его краем является ориентированное многообразие $\partial Y = -\partial V$, где знак минус указывает на изменение ориентации. Применим теорему Стокса к многообразию Y и дифференциальной форме ω. Согласно этой теореме, $\int_{\partial Y} \omega = \int_Y d\omega$. Форма ω голоморфна в окрестности $X \setminus \{x_1, \ldots, x_n\}$ многообразия Y и потому замкнута: $d\omega = 0$. Таким образом,

$$\sum_{x\in X} \operatorname{res}_x \omega = \int_{\partial V} \omega/2\pi i = -\int_{\partial Y} \omega/2\pi i = 0,$$

что и требовалось.

Пусть теперь f — мероморфная функция на компактной римановой поверхности X. Докажем, что f имеет одинаковое число нулей и полюсов (с учетом кратностей), т. е. что $\sum_{x\in X} \operatorname{ord}_x f = 0$. Рассмотрим мероморфную дифференциальную форму $\omega = df/f$. Эта форма имеет полюса в нулях и полюсах функции f, причем $\operatorname{res}_x \omega = \operatorname{ord}_x f$ для каждого $x \in X$. Для доказательства этого равенства можно ограничиться случаем, когда $x = 0$ и $f(z) = z^k g(z)$, где $g(z)$ голоморфна в окрестности нуля и $g(0) \neq 0$. Тогда $\omega = df/f = kdz/z + dg/g$. Форма dg/g голоморфна в нуле, поэтому $\operatorname{res}_0 \omega = \operatorname{res}_0 kdz/z = k = \operatorname{ord}_0 f$. Таким образом,

$$\sum_{x\in X} \operatorname{ord}_x f = \sum_{x\in X} \operatorname{res}_x \omega = 0. \qquad \blacktriangleright$$

Пятое доказательство [14]. Мы видели, что основная теорема алгебры вытекает из следующего факта: *всякое непостоянное голоморфное отображение $f : M \to N$ между компактными связными римановыми поверхностями сюръективно.* Выведем этот факт из теоремы об открытом отображении: *f переводит открытые множества в открытые.*

$\blacktriangleleft$ Из теоремы об открытом отображении следует, что $f(M)$ открыто в N. С другой стороны, так как M компактно, то и $f(M)$ компактно и, следовательно, замкнуто в N. Так как N связно, т. е. не содержит собственных непустых открыто-замкнутых множеств, то $f(M) = N$.$\blacktriangleright$

Комментарий. По сути дела, это и есть «истинный стержень» доказательства Даламбера. Для Даламбера был, вероятно, очевиден тот факт, что $f(\mathbb{C})$ замкнуто, и тогда (в предположении отсутствия корня) можно найти точку этого множества, ближайшую к нулю. А далее Даламбер утверждал, что это ведет к противоречию, по сути дела, доказывая открытость f. Для этого он разлагал обратную к f функцию в ряд по дробным степеням. Конечно, не зная того, чему сейчас учат у нас на первом курсе, Даламбер не мог доказать свой результат так, чтобы получить хорошую оценку у придирчивого современного преподавателя, но суть дела он понимал прекрасно!

Шестое доказательство. Предыдущее доказательство имеет вариант, в котором ссылка на теорему об открытом отображении заменяется ссылкой на теорему об обратной функции.

$\blacktriangleleft$ Пусть p — многочлен степени > 0, $f = \hat{p} : \mathbb{C}P^1 \to \mathbb{C}P^1$ — отображение, определенное этим многочленом. Пусть $X \subset \mathbb{C}P^1$ — конечное множество, состоящее из всех нулей производной p' многочлена p и из бесконечно удаленной точки. В каждой точке $x \in \mathbb{C}P^1 \setminus X$ дифференциал отображения f невырожден, и из теоремы об обратной функции следует, что f является локальным диффеоморфизмом в точке x. В частности, f

открыто в x, т. е. образ любой окрестности точки x является окрестностью точки $f(x)$. Следовательно, множество $V = f(\mathbb{C}P^1 \setminus X)$ открыто в $\mathbb{C}P^1$. С другой стороны, множество $F = f(\mathbb{C}P^1)$ компактно и потому замкнуто. Так как $F = V \cup f(X)$, разность $F \setminus V$ содержится в $f(X)$ и потому конечна. Поскольку $\mathbb{C}P^1$ гомеоморфно двумерной сфере, достаточно установить следующую лемму:

Лемма. *Пусть V и F — такие подмножества двумерной сферы $\mathbb{S}^2$, что V открыто и непусто, F замкнуто, $V \subset F$ и $F \setminus V$ конечно. Тогда $F = \mathbb{S}^2$.*

◀ Предположим противное: найдется точка $a \in \mathbb{S}^2 \setminus F$. Возьмем произвольную точку $b \in V$. Точки a и b можно соединить на сфере бесконечным множеством путей, попарно не имеющих общих точек, кроме a и b. Каждый из этих путей должен пересекаться с границей ∂V множества V. Таким образом мы получаем бесконечное множество точек в ∂V. Это противоречит тому, что ∂V содержится в конечном множестве $F \setminus V$. ▶

Седьмое доказательство. По-видимому, самое простое доказательство, которое чаще других встречается в учебниках, таково [7, 12].

◀ Пусть, как и раньше, $p(z)$ — многочлен степени $n > 0$. Тогда существует точка $a \in \mathbb{C}$, в которой функция $|p(z)|$ достигает минимума. Действительно, так как $|p(z)|$ стремится к бесконечности при z, стремящемся к бесконечности, то $\inf_{z\in\mathbb{C}} |p(z)| = \inf_{z\in B} |p(z)|$, где B — достаточно большой замкнутый круг. Нижняя грань $\inf_{z\in B} |p(z)|$ достигается в силу компактности круга B.

Предположим, что $p(a) \neq 0$. Заменяя многочлен $p(z)$ на $p(z+a)/p(a)$, мы сводим дело к случаю, когда $p(0) = 1$ и $|p(z)| \geqslant 1$ при всех z. Пусть $p(z) = 1 + a_k z^k + \dots + a_n z^n$, где $a_k \neq 0$. Сведем дело к случаю, когда $a_k = -1$. Из каждого комплексного числа можно извлечь корень k-й степени (это следует из записи числа в тригонометрической форме). Пусть c — такое число, что $c^k = -1/a_k$. Заменяя многочлен $p(z)$ на $p(cz) = 1 - z^k + \dots$ $\dots + a_n c^n z^n$, мы можем считать, что $a_k = -1$.

Запишем $p(z)$ в виде $p(z) = 1 - z^k + b(z)$. Когда z стремится к нулю, $|b(z)|$ бесконечно мало по сравнению с $|z^k|$. В частности, если x — достаточно малое положительное число, то $|b(x)| < x^k$. При таких x имеем $|p(x)| = |1 - x^k + b(x)| \leqslant 1 - x^k + |b(x)| < 1$ — противоречие. ▶

Комментарий. Это упрощение основной идеи Даламбера принадлежит швейцарскому математику Аргану (1814). Но и он (в начале прошлого века) не смог бы как следует объяснить, почему задача на минимум имеет решение. Ведь тогда еще не родились Вейерштрасс, Дедекинд и Кантор, которые построили теорию действительного числа.

Отметим, что равенство $p(a) = 0$, где a — точка, в которой $|p(z)|$ достигает минимума, вытекает также из *принципа максимума модуля*. Согласно этому принципу, модуль непостоянной голоморфной функции, определенной в связном открытом множестве, не может достигать максимума. В нашем случае надо применить этот принцип к функции $1/p$. Функция $1/p$ фигурирует и в нашем следующем доказательстве.

Восьмое доказательство [14, 16]. ◀ Предположим, что многочлен $p(z)$ степени > 0 не имеет корней. Тогда функция $1/p$ определена при всех $z \in \mathbb{C}$, голоморфна и стремится к нулю на бесконечности. По теореме Лиувилля эта функция должна быть тождественно равна нулю — противоречие. ▶

Комментарий. Теорема Лиувилля утверждает, что ограниченная голоморфная функция, определенная при всех $z \in \mathbb{C}$, постоянна. Есть и более общая формулировка: ограниченная гармоническая функция, определенная на евклидовом пространстве $\mathbb{R}^n$, постоянна. Комплексная функция f, определенная в открытом множестве $U \subset \mathbb{R}^n$, называется *гармонической*, если она дважды непрерывно дифференцируема и удовлетворяет уравнению Лапласа $\sum_{i=1}^n \partial^2 f/\partial x_i^2 = 0$. Непрерывная функция f, определенная в U, является гармонической тогда и только тогда, когда для нее выполняется теорема о среднем значении: для любого шара B, содержащегося в U, значение функции f в центре шара равно ее «среднему по шару», т. е. интегралу $\int_B f$, деленному на объем шара. Каждая голоморфная функция является гармонической.

Докажем теорему Лиувилля об ограниченных гармонических функциях, исходя из теоремы о среднем значении. Пусть f — гармоническая функция, определенная на $\mathbb{R}^n$. Допустим, что $|f(x)| \leqslant M$ при всех $x \in \mathbb{R}^n$, и докажем, что f постоянна. Зафиксируем $a, b \in \mathbb{R}^n$. Пусть A и B — шары одинакового большого радиуса с центрами a и b. Положим $C = A \cap B$. Нетрудно видеть, что отношение $m(A \setminus C)/m(A)$ стремится к нулю, когда радиусы шаров A и B стремятся к бесконечности (через $m(X)$ мы обозначаем объем множества X). Согласно теореме о среднем значении, $f(a) = \int_A f/m(A) = (\int_C f + \int_{A\setminus C} f)/m(A)$. Слагаемое $\int_{A\setminus C} f/m(A) \leqslant m(A \setminus C)M/m(A)$ стремится к нулю с ростом радиуса шара. Следовательно, $f(a)$ равно пределу отношения $\int_C f/m(A)$.

По аналогичным причинам $f(b)$ равно этому же пределу. Таким образом, $f(a) = f(b)$.

Понятие гармонической функции и теорема Лиувилля переносятся на функции со значениями в произвольном банаховом пространстве. Пусть X — комплексное банахово пространство, $B(X)$ — банахово пространство всех ограниченных линейных операторов из X в себя. *Спектром* оператора $A \in B(X)$ называется множество тех $\lambda \in \mathbb{C}$, для которых оператор $A - \lambda \cdot 1_X$ необратим. Мы видели в разделе 2, что алгебраическая замкнутость поля $\mathbb{C}$ равносильна следующему свойству: если E — конечномерное векторное пространство над $\mathbb{C}$ размерности > 0, то всякий линейный оператор $A : E \to E$ имеет непустой спектр. Поэтому следующую теорему, принадлежащую И. М. Гельфанду, можно рассматривать как усиление основной теоремы алгебры: *если X — комплексное банахово пространство, не сводящееся нулю, то всякий оператор $A \in B(X)$ имеет непустой спектр.* Эта теорема вытекает из теоремы Лиувилля. Предположим, что оператор $f(\lambda) = A - \lambda \cdot 1_X$ обратим для всех $\lambda \in \mathbb{C}$. Тогда функция $g : \mathbb{C} \to B(X)$, определенная по формуле $g(\lambda) = f(\lambda)^{-1}$, голоморфна и стремится к нулю на бесконечности. По теореме Лиувилля она должна тождественно равняться нулю — противоречие.

Вернемся к изначальному рассуждению этого пункта, чтобы придать чуть другую форму доказательству.

◀ Пусть по-прежнему p — многочлен степени больше 0, не имеющий корней. Из того, что функция $1/p$ стремится к нулю на бесконечности, вытекает, что

$$\left| \int_{|z|=R} \frac{dz}{zp(z)} \right| \leqslant 2\pi \max_{|z|=R} \frac{1}{p(z)} \underset{R\to\infty}{\to} 0.$$

С другой стороны, функция $1/zp(z)$ имеет единственный полюс в нуле с вычетом $1/p(0)$, и по теореме о вычетах

$$\int_{|z|=R} \frac{dz}{zp(z)} = 2\pi i$$

любого $R > 0$ — противоречие.▶

Идея этого доказательства восходит к Коши.

Девятое доказательство. ◀ Мы показали в разделе 2, что алгебраическая замкнутость поля $\mathbb{C}$ равносильна следующему утверждению: *если E — векторное пространство над $\mathbb{C}$ размерности $n + 1$, то всякий линейный оператор $A : E \to E$ имеет собственный вектор.* Можно предполагать, что оператор A невырожден, так как в противном случае собственные векторы, очевидно, существуют: таковы ненулевые векторы ядра. Пусть $P(E) = \mathbb{C}P^n$ — множество всех одномерных линейных подпространств в E. Это множество называется n-мерным комплексным проективным пространством и имеет естественную структуру компактного гладкого многообразия. Оператор A индуцирует гладкое отображение $\hat{A} : \mathbb{C}P^n \to \mathbb{C}P^n$. Собственные векторы оператора A соответствуют неподвижным точкам отображения $\hat{A}$. Таким образом, нам надо доказать, что отображение $\hat{A}$ имеет неподвижную точку. Это вытекает из теоремы Лефшеца. ▶

Комментарий. *Неподвижная точка* отображения f множества X в себя — это такое $x \in X$, что $f(x) = x$. Теорема Лефшеца утверждает, что отображение $f : X \to X$ компактного полиэдра в себя имеет неподвижную точку, если так называемое *число Лефшеца* $L(f)$ отображения f отлично от нуля [13, 11]. Мы не будем определять это число для произвольного f, а ограничимся случаем, когда f гомотопно тождественному отображению id_X (т. е. f и id_X могут быть соединены непрерывным путем в пространстве $C(X, X)$ отображений X в себя). В этом случае $L(f)$ совпадает с эйлеровой характеристикой пространства X. *Эйлерова характеристика* $\chi(X)$ компактного многообразия X может быть определена следующим образом. Пусть $F_0 \subset F_1 \subset \ldots \subset F_n = X$ — возрастающая последовательность замкнутых подмножеств в X, такая, что каждая разность $F_k \setminus F_{k-1}$ гомеоморфна дизъюнктной сумме конечного числа a_k экземпляров пространства $\mathbb{R}^k$. Мы считаем, что $F_{-1} = \varnothing$, так что F_0 — это конечное множество. Тогда $\chi(X) = \sum_{k=0}^{n}(-1)^k a_k$. Это число не зависит от выбора последовательности $F_0, \ldots, F_n$. Нужный нам вариант теоремы Лефшеца формулируется так: *если X — компактное многообразие ненулевой эйлеровой характеристики, то всякое непрерывное отображение $f : X \to X$, гомотопное тождественному, имеет неподвижную точку.*

Покажем, что эта теорема применима к отображению $\hat{A} : \mathbb{C}P^n \to \mathbb{C}P^n$, индуцированному невырожденным линейным оператором $A : E \to E$. Эйлерова характеристика комплексного проективного пространства $\mathbb{C}P^n$ равна $n+1$. Это вытекает из рассмотрения цепочки подпространств $\mathbb{C}P^0 \subset \mathbb{C}P^1 \subset \ldots \mathbb{C}P^n$, в которой каждая разность $\mathbb{C}P^k \setminus \mathbb{C}P^{k-1}$ гомеоморфна $\mathbb{C}^k$. С другой стороны, группа $\mathrm{GL}(E)$ всех обратимых линейных операторов из E в себя связна. Это легко доказать индукцией по размерности пространства E. Можно также рассуждать следующим образом. Пусть $L = L(E, E)$ — линейное пространство всех линейных отображений из E в себя. Группа $\mathrm{GL}(E)$ служит дополнением в L к алгебраическому множеству $D = \{B \in L : \det B = 0\}$. Множество D имеет в L коразмерность 2 и потому не может разбивать L. Более того, для любых двух точек $x, y \in \mathrm{GL}(E) = L \setminus D$ комплексная прямая $l \subset L$, соединяющая x и y, пересекается с D по конечному множеству, поэтому существует ломаная, соединяющая x с y в l и не пересекающаяся с D. Таким образом, в группе $\mathrm{GL}(E)$ существует путь, соединяющий единичный оператор с A. Отсюда следует, что существует путь, соединяющий $\hat{A}$ в пространстве $C(\mathbb{C}P^n, \mathbb{C}P^n)$ с тождественным отображением, т. е. что отображение $\hat{A}$ гомотопно тождественному.

Проведенное доказательство можно применить в более общей ситуации. Пусть G — связная топологическая группа, H — такая замкнутая подгруппа в G, что факторпространство G/H является компактным многообразием ненулевой эйлеровой характеристики. Тогда каждое $g \in G$ сопряжено с некоторым элементом из H. Действительно, по теореме Лефшеца отображение $xH \mapsto gxH$ пространства G/H в себя имеет неподвижную точку aH. Таким образом, $gaH = aH$, откуда $a^{-1}ga \in H$. Выше мы фактически рассматривали случай, когда $G = \mathrm{GL}(E)$, а H — подгруппа всех преобразований $A \in G$, оставляющих инвариантной некоторую фиксированную прямую в E. В этом случае факторпространство G/H отождествляется с проективным пространством $\mathbb{C}P^n$, где $n = \dim E - 1$. Можно дать еще одно доказательство основной теоремы алгебры, приняв за H подгруппу всех операторов из G, имеющих верхнетреугольные матрицы (т. е. с нулями ниже главной диагонали) относительно некоторого фиксированного базиса в E. В этом случае факторпространство G/H является так называемым «многообразием флагов». Оно компактно и имеет эйлерову характеристику $(n+1)!$. Утверждение, что каждое $g \in G$ сопряжено с некоторым элементом подгруппы H, означает, что каждый оператор $g \in G$ имеет относительно некоторого базиса треугольную матрицу. Это утверждение равносильно основной теореме алгебры.

Укажем еще одно применение сформулированной выше теоремы о топологических группах. Пусть G — связная компактная группа Ли (т. е. топологическая группа, являющаяся гладким многообразием). *Тором* в G называется подгруппа, изоморфная конечной степени группы $\mathbb{R}/\mathbb{Z}$. Если T — максимальный тор в G, то эйлерова характеристика пространства G/H равна порядку так называемой *группы Вейля* группы G и, в частности, отлична от нуля. Следовательно, G покрывается подгруппами, сопряженными с T. Отсюда легко вывести, что все максимальные торы в G сопряжены между собой [1].

Десятое доказательство [9]. Наше последнее доказательство будет алгебраическим. Роль топологии при этом сводится к минимуму. Мы используем лишь связность прямой в следующей форме: *если многочлен с вещественными коэффициентами меняет знак (т. е. принимает как положительные, так и отрицательные значения), то он имеет вещественный корень*. Это свойство упорядоченного поля $\mathbb{R}$ называется *вещественной замкнутостью*. Оно равносильно соединению двух свойств: *всякий многочлен нечетной степени имеет корень, и всякое положительное число является квадратом.*

Каждое комплексное число является квадратом. Выше мы уже пользовались более общим фактом: из каждого комплексного числа можно извлечь корень любой целой степени $n > 0$. При этом мы ссылались на запись комплексных чисел в тригонометрической форме. Однако теперь мы хотим дать доказательство, которое годилось бы для всех вещественно замкнутых полей и не использовало бы трансцендентных функций. Пусть $a, b \in \mathbb{R}$. Нам надо найти такие $x, y \in \mathbb{R}$, что $(x + iy)^2 = a + ib$. Это уравнение равносильно системе уравнений $x^2 - y^2 = a$ и $2xy = b$. Пусть x и y — квадратные корни из положительных чисел $(a + \sqrt{a^2 + b^2})/2$ и $(-a + \sqrt{a^2 + b^2})/2$. Тогда $x^2 - y^2 = a$ и $x^2y^2 = b^2/4$, откуда $2xy = \pm b$. Если $2xy = -b$, изменим знак у x или y.

Из того, что всякий многочлен из $\mathbb{R}[X]$ нечетной степени имеет корень, вытекает, что у поля $\mathbb{R}$ нет собственных конечных расширений нечетной степени. Из того, что всякое $z \in \mathbb{C}$ является квадратом, вытекает, что у поля $\mathbb{C}$ нет расширений степени 2. Покажем, как вывести отсюда, что поле $\mathbb{C}$ алгебраически замкнуто. Идея доказательства восходит к Эйлеру. Эта идея была усовершенствована Лагранжа, а затем совершенно безупречно реализована Гауссом в его втором доказательстве (1815 г.) основной теоремы алгебры. Изложение, основанное на симметрических многочленах, можно найти в [7, 5]. Мы приведем доказательство Артина, основанное на теории Галуа и теореме Силова.

◀ Напомним сперва основные факты теории Галуа. Пусть L — конечное расширение поля K. Обозначим через $G(L/K)$ группу всех автоморфизмов f поля L, таких, что $f(x) = x$ для всех $x \in K$. Эта группа конечна. Для каждой подгруппы $H \subset G = G(L/K)$ пусть L_H — неподвижное поле группы H, т. е. множество всех таких $x \in L$, что $f(x) = x$ для всех $f \in H$. Конечное расширение L называется *расширением Галуа*, если $L_G = K$. Пусть L — расширение Галуа поля K. Тогда существует естественное взаимно-однозначное соответствие между множеством $\mathcal{P}$ всех подполей поля L, содержащих K, и множеством $\mathcal{H}$ всех подгрупп группы G. Каждой группе $H \in \mathcal{H}$ сопоставим поле $L_H \in \mathcal{P}$. Каждому полю $P \in \mathcal{P}$ сопоставим группу $G(L/P) \in \mathcal{H}$. Указанные отображения $\mathcal{H} \to \mathcal{P}$ и $\mathcal{P} \to \mathcal{H}$ взаимно обратны. Если H_1, H_2 — подгруппы группы G и $H_1 \subset H_2$, то для полей P_1 и P_2, соответствующих H_1 и H_2, имеем $P_2 \subset P_1$, и степень $[P_1 : P_2]$ равна индексу $(H_2 : H_1)$.

Согласно теореме 1, нам надо установить, что у поля $\mathbb{C}$ нет собственных конечных расширений. Пусть K — конечное расширение поля $\mathbb{C}$. Существует конечное расширение L поля K, такое, что L — расширение Галуа поля $\mathbb{R}$. Рассмотрим группу Галуа $G = G(L/\mathbb{R})$. Так как у поля $\mathbb{R}$ нет собственных расширений нечетной степени, то в группе G нет собственных подгрупп нечетного индекса. Следовательно, силовская 2-подгруппа группы G совпадает с G, т. е. G является 2-группой. Пусть $H = G(L/\mathbb{C})$ — подгруппа индекса 2 в G, соответствующая полю $\mathbb{C}$. Так как у поля $\mathbb{C}$ нет расширений степени 2, то в группе H нет подгрупп индекса 2. Однако в нетривиальной конечной p-группе всегда есть подгруппа индекса p, поэтому H сводится к единице. Отсюда следует, что $L = K = \mathbb{C}$. ▶

Список литературы

[1] *Адамс Дж.* Лекции по группам Ли. М.: Наука. 1979.

[2] *Бурбаки Н.* Очерки по истории математики. М.: Изд-во иностр. литературы. 1963.

[3] *Бурбаки Н.* Алгебра. Многочлены и поля. Упорядоченные группы. М.: Наука. 1965.

[4] *Клейн Ф.* Лекции о развитии математики в XIX столетии. М.: Наука. 1989.

[5] *Кострикин А. И.* Введение в алгебру. М.: Наука. 1994.

[6] *Курант Р., Роббинс Г.* Что такое математика? М.: Просвещение. 1967.

[7] *Курош А. Г.* Курс высшей алгебры. М.: Наука. 1971.

[8] Сборник задач московских математических олимпиад /*под ред. А.А. Лемана.* М.: Просвещение. 1965.

[9] *Ленг С.* Алгебра. М.: Мир. 1968.

[10] *Милнор Дж.* Топология с дифференциальной точки зрения // *Милнор Дж., Уоллес А.* Дифференциальная топология. М.: Мир. 1972.

[11] *Понтрягин Л. С.* Основы комбинаторной топологии. М.: Наука. 1976.

[12] *Рудин У.* Основы математического анализа. М.: Мир. 1966.

[13] *Спеньер Э.* Алгебраическая топология. М.: Мир. 1971.

[14] *Форстер О.* Римановы поверхности. М.: Мир. 1980.

[15] *Фоменко А. Т., Фукс Д. Б.* Курс гомотопической топологии. М.: Наука. 1989.

[16] *Шварц Л.* Анализ. М.: Мир. 1972.

[17] *Янин В. Л.* Предисловие // *Колмогоров А. Н.* Новгородское землевладение XV века. М.: Наука. 1994.