«Вещественное» доказательство основной теоремы алгебры

А. В. Пухликов

Цель настоящей заметки — доказать теорему об алгебраической замкнутости поля комплексных чисел $\mathbb{C}$, не используя (даже неявно) само понятие комплексного числа. Хорошо известно, что эта теорема эквивалентна следующему, чисто вещественному факту.

Теорема. *Любой вещественный многочлен*

$$p(x) = x^n + a_1 x^{n-1} + \dots + a_n, \qquad a_i \in \mathbb{R},$$

$a_i \in \mathbb{R}$, *раскладывается в произведение линейных и квадратичных (вещественных) сомножителей:*

$$p(x) = \prod (x - \alpha_i) \cdot \prod (x^2 + p_j x + q_j),$$

где $\alpha_i, p_j, q_i \in \mathbb{R}$.

Уже сама эта формулировка позволяет предположить, что доказательство может быть получено средствами вещественного анализа. Это мы и собираемся сделать. Доказательство мы представим в виде серии утверждений-задач, детальная проверка которых оставлена читателю.

Отметим по ходу дела, что значительная часть известных доказательств опирается на следующий простой факт.

Упражнение 1. *Любой (вещественный) многочлен нечетной степени имеет вещественный корень.*

Указание. Воспользуйтесь теоремой о промежуточном значении.

Приводимое ниже доказательство никак *не* связано с четностью степени.

Будем рассуждать индукцией по степени n многочлена p. Для $n = 1, 2$ теорема тривиальна. Считаем поэтому, что $n \geqslant 3$ и для меньших степеней утверждение теоремы справедливо.

Рассмотрим теперь k-мерное аффинное пространство P_k всех (вещественных) многочленов степени k:

$$P_k \ni g = x^k + a_1 x^{k-1} + \dots + a_k.$$

Для удобства всегда полагаем $a_0 = 1$. Коэффициенты a_i задают отождествление

$$P_k \cong \mathbb{R}^k,$$
$$P_k \ni g \mapsto (a_1, \dots, a_k),$$

так что набор коэффициентов $(a_1, \dots, a_k)$ мы можем (и будем) рассматривать как естественную систему координат на P_k.

В основе нашего доказательства лежит анализ *отображения умножения*

$$\mu_k \colon P_k \times P_{n-k} \to P_n,$$
$$\mu_k : (g, h) \mapsto gh,$$

сопоставляющего паре многочленов их произведение. Достаточно показать, что пространство P_n покрывается образами Z_k отображений μ_k, $k = 1, \dots, n-1$, ибо в этом случае можно применить предположение индукции. Итак, положим

$$Z = \bigcup_{k=1}^{n-1} Z_k.$$

Задача 1. *Подмножество $Z \subset P_n$ есть в точности множество всех многочленов степени n, удовлетворяющих утверждению теоремы.*

(Это почти тривиально.)

Нам нужно показать, что $Z = P_n$.

Определение. *Непрерывное отображение называется* собственным, *если прообраз любого компакта есть компакт.*

Упражнение 2. *Проверьте, что соответствие $x \mapsto \sin x$ задает отображение $\varphi : \mathbb{R} \to \mathbb{R}$,* не *являющееся собственным.*

Задача 2. *Отображения умножения μ_k являются собственными.*

Указание. Достаточно показать (почему?), что прообраз любого ограниченного множества относительно μ_k есть ограниченное множество в $P_k \times P_{n-k} \cong \mathbb{R}^n$. Предположим, что это не так. Тогда существуют две последовательности многочленов

$$g_m = a_{m,0}x^k + a_{m,1}x^{k-1} + \dots + a_{m,k}$$

и

$$h_m = b_{m,0}x^{n-k} + b_{m,1}x^{n-k-1} + \dots + b_{m,n-k},$$

$a_{m,0} = b_{m,0} = 1$, такие, что

1) $t_m = \max\limits_{i,j}\{|a_{m,i}|, |b_{m,j}|\} \to \infty$ при $m \to \infty$,

2) коэффициенты многочленов (g_m, h_m) ограничены по модулю константой, не зависящей от m.

Покажите, что, переходя к подпоследовательности, мы можем добиться выполнения следующих свойств «регулярности» поведения коэффициентов:

1) для некоторых индексов s и r $(0 \leqslant s \leqslant k,\ 0 \leqslant r \leqslant n-k)$ абсолютные значения $|a_{m,r}|$ и $|b_{m,s}|$ максимальны для всех m среди $|a_{m,i}|$ и $|b_{m,j}|$ соответственно, причем обе последовательности $|a_{m,r}|$ и $|b_{m,s}|$ не убывают;

2) для любого индекса i или j $(0 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant n-k)$ выполнено в точности одно из двух требований: либо $|a_{m,r}| = O(|a_{m,i}|)$ (соответственно, $|b_{m,s}| = O(|b_{m,j}|)$), в этом случае назовем этот индекс (i или j) *большим*, либо $|a_{m,i}| = o(|a_{m,r}|)$ (соответственно, $|b_{m,j}| = o(|b_{m,s}|)$), и в этом случае назовем этот индекс (i или j) *малым*.

Теперь возьмите два наименьших больших индекса $u \leqslant r$ и $v \leqslant s$. Докажите, что последовательность коэффициентов при x^{n-u-v} в многочленах $g_m h_m$ не может быть ограниченной! Это противоречие завершит доказательство.

Задача 3. *Множества Z_k (и, следовательно, Z) замкнуты в P_n.*

Это следствие собственности отображений умножения. Именно поэтому свойство отображения быть собственным является столь важным.

Итак, Z — замкнутое множество. Хотелось бы, чтобы оно одновременно и открытым: тогда можно было бы воспользоваться связностью $P_n \cong \mathbb{R}^n$ и получить желаемое совпадение $Z = P_n$. Мы установим чуть более слабый факт.

Пусть $f \in Z_k$ — некоторый разложимый многочлен,

$$f = gh,$$
$$g = x^k + b_1 x^{k-1} + \dots + b_k,$$
$$h = x^{n-k} + c_1 x^{n-k-1} + \dots + c_{n-k}.$$

Упражнение 3. *Выпишите явно матрицу дифференциала (якобиан) отображения*

$$\mu_k : P_k \times P_{n-k} \cong \mathbb{R}^n \to P_n \cong \mathbb{R}^n$$

в точке $(g, h) \in P_k \times P_{n-k}$ относительно естественных систем координат — коэффициентов многочленов.

Задача 4. *Докажите, что это линейное отображение $d\mu_k$ невырождено (не имеет ядра) тогда и только тогда, когда многочлены g, h взаимно просты.*

Указание. Фиксируя произвольный многочлен $q \in P_m$, мы превращаем *аффинное* пространство P_m в линейное пространство, записывая произвольный многочлен в виде суммы $q + w$, где w — многочлен степени не превосходящей $m - 1$. *Линейное* пространство многочленов степени, не превосходящей l обозначим через $\mathcal{P}_l$. Отображение μ_k может быть теперь записано так:

$$(g + u, h + v) \mapsto gh + (gv + hu) + uv.$$

Получаем следующий вид якобиана $d\mu_k$:

$$\mathbb{R}^n \cong \mathcal{P}_{k-1} \times \mathcal{P}_{n-k-1} \ni (u, v) \mapsto gv + hu \in \mathcal{P}_{n-1} \cong \mathbb{R}^n.$$

Отсюда утверждение задачи выводится без труда.

Отметим, что задача 4 и упражнение 3 суть классическая теория *результанта* двух многочленов: определитель якобиевой матрицы $d\mu_k$ есть не что иное как результант $R(g, h)$ многочленов g и h.

Задача 5. *Пусть $f \in Z$ допускает представление $f = gh$, $(g, h) = 1$. Тогда Z содержит некоторую окрестность точки f.*

Указание. Примените теорему о неявной функции.

Задача 6. *Пусть $f \in Z$ не допускает представления $f = gh$, $(g, h) = 1$. Тогда либо $f = (x - a)^n$; либо n четно, $n = 2l$, и $f = (x^2 + bx + c)^l$.*

Пусть $Y \subset P_n$ — (замкнутое) множество многочленов, описанных в предыдущей задаче.

Задача 7. $P_n \setminus Y$ *связно.*

Указание. Открытое множество $P_n \setminus Y$ *линейно* связно: постройте явно путь, связывающий две точки.

Итак, мы знаем, что $Z \setminus Y$ открыто в $P_n \setminus Y$ (задача 5) и замкнуто в $P_n \setminus Y$ (задача 3). В силу предыдущей задачи (и непустоты $Z \setminus Y$!) имеем

$$Z \setminus Y = P_n \setminus Y.$$

Стало быть, $Z = P_n$.

Теорема доказана.

Автор благодарен А. И. Кострикину и А. Г. Хованскому за интерес к этому доказательству, а также А. Б. Сосинскому за полезные замечания и предложения по улучшению изложения.