Коммутирующие многочлены

В. О. Бугаенко

Над функциями, как и над числами, можно производить арифметические операции — сложение и умножение. Однако, кроме этих двух привычных операций, на множестве функций, в отличие от множества чисел, существует еще одна — операция композиции. Напомним: композицией двух функций f и g называется функция $f \circ g$ такая, что

$$f \circ g(x) \stackrel{\text{def}}{=} f(g(x)).$$

Будем придерживаться следующих обозначений.

Тождественную функцию будем обозначать id (тождественная функция определяется равенством $\mathrm{id}(x) \equiv x$). Операцию возведения в степень будем рассматривать относительно операции композиции, а не умножения, как это обычно делается, именно $f^n \stackrel{\text{def}}{=} \underbrace{f \circ \cdots \circ f}_{n \text{ раз}}$ для любого натурального числа n. Мы будем обозначать f^{-1} *обратную функцию* к функции f, т. е. такую, что $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}$ (если она существует). Естественно, $f^{-n} \stackrel{\text{def}}{=} \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{n \text{ раз}}$, $\quad f^0 \stackrel{\text{def}}{=} \mathrm{id}$. Возведение функции $f(x)$ в n-ю степень в обычном смысле мы будем обозначать $f(x)^n$.

Операция композиции обладает естественным свойством ассоциативности, т. е. для любых функций f, g и h справедливо равенство $(f \circ g) \circ h = f \circ (g \circ h)$. Однако привычное свойство коммутативности для композиции в общем случае не выполняется; композиции $f \circ g$ и $g \circ f$, как правило, являются различными функциями. Например, если $f(x) = x + 1$, а $g(x) = x^2$, то $f(g(x)) = x^2 + 1$, а $g(f(x)) = x^2 + 2x + 1$.

Для некоторых пар функций равенство

$$f \circ g = g \circ f \tag{1}$$

выполняется. В таком случае функции f и g называют *коммутирующими*.

Очевидно, функции f и g являются коммутирующими в каждом из следующих случаев:

а) $f(x) = g(x)$;

б) $f(x) = x + a$, $g(x) = x + b$ для произвольных чисел a и b;

в) $f(x) = ax$, $g(x) = bx$ для произвольных чисел a и b;

г) $f(x) = x^\alpha$, $g(x) = x^\beta$ для произвольных чисел α и β;

д) $f(x) = h^m(x)$, $g(x) = h^n(x)$ для некоторой функции h и целых (если функция h необратима, то положительных) чисел m и n.

Бывает так, что заметить коммутирование двух функций без непосредственной проверки непросто. Примером таких функций являются многочлены $x^2 - 2$ и $x^3 - 3x$.

Явление коммутирования встречается достаточно редко, и естественным является вопрос описания всех таких случаев, хотя бы для многочленов. Эта задача была сформулирована еще в начале века и полностью решена Дж. Риттом [1]. Позднее появилось множество работ [2, 3, 4], где предлагались различные доказательства этой классификации. Однако все они неэлементарны. Так, исходное доказательство Ритта использовало топологические свойства римановых поверхностей, а работа Дорея и Уэйплса [2] основана на теории нормирований полей.

Элементарное доказательство классификации коммутирующих многочленов не известно до сих пор. В 1977 году школьникам — участникам XI Всесоюзной олимпиады по математике — было предложено разобрать несколько частных случаев этой классификации. Вот как формулировалась задача, предложенная участникам олимпиады.

> *Мы будем рассматривать многочлены от одного переменного x со старшим коэффициентом 1. Будем говорить, что два таких многочлена P и Q коммутируют, если многочлены $P(Q(x))$ и $Q(P(x))$ тождественно равны (т. е. после раскрытия скобок и приведения к стандартному виду все коэффициенты этих многочленов совпадают).*
>
> *а) Для каждого числа α найдите все многочлены Q степени не выше трех, коммутирующие с многочленом $P(x) = x^2 - \alpha$.*
>
> *б) Пусть P — многочлен степени 2, k — натуральное число. Докажите, что существует не более одного многочлена степени k, коммутирующего с P.*
>
> *в) Найдите многочлены степеней 4 и 8, коммутирующие с данным многочленом степени 2.*

г) Многочлены Q и R коммутируют с одним и тем же многочленом P степени 2. Докажите, что они коммутируют между собой.

д) Докажите, что существует бесконечная последовательность многочленов $P_2, P_3, P_4, \ldots, P_k, \ldots$, где P_k — многочлен степени k, в которой любые два многочлена коммутируют и $P_2(x) = x^2 - 2$.

В 1979 году в журнале «Квант» была опубликована статья И. Янтарова (псевдоним И. Н. Бернштейна) [5]. В ней решалась полностью задача Всесоюзной олимпиады, и предлагалось несколько вопросов, элементарные ответы на которые были неизвестны. Одним из таких вопросов был: при каких значениях α существует многочлен нечетной степени (выше первой), коммутирующий с многочленом $x^2 - \alpha$? Фактически, этот вопрос равносилен классификации всех пар коммутирующих многочленов, один из которых имеет степень 2.

Общую задачу можно сформулировать так.

Задача классификации коммутирующих многочленов. *Для данного многочлена P найти все коммутирующие с ним многочлены.*

Мы (не делая специальных оговорок) будем рассматривать лишь многочлены ненулевой степени.

Автор настоящей статьи занялся решением этой задачи, будучи школьником, под руководством А. К. Толпыго и И. Н. Бернштейна. В результате появилось элементарное решение задачи классификации для многочленов второй степени. Ключевая идея, завершившая эту классификацию, принадлежит И. Н. Бернштейну. Изложение этого результата и является основной целью настоящей статьи. Кроме того, задача классификации решается для некоторого достаточно широкого класса кубических многочленов, а также рассматриваются известные примеры коммутирующих многочленов и рациональных функций. Результаты, изложенные в параграфах 4, 6 и 7, принадлежат автору, а изложенные в параграфе 8 — И. Н. Бернштейну. Они были получены в 1979 году, однако публикуются впервые.

В первом параграфе показано, как свести задачу классификации коммутирующих многочленов к более узкому классу так называемых приведенных многочленов. Приведенные многочлены второй степени имеют вид $x^2 - \alpha$; всюду в дальнейшем, кроме параграфов 7 и 9, задача классификации будет рассматриваться только для таких многочленов.

Второй параграф посвящен доказательству единственности многочлена фиксированной степени с данным старшим коэффициентом, коммутирующего с данным многочленом.

Основным результатом третьего параграфа является предложение: *«если два многочлена коммутируют с некоторым многочленом второй степени, то они коммутируют между собой»* и его следствие.

В четвертом параграфе доказывается, что многочлен, коммутирующий с приведенным многочленом второй степени является либо четным, либо нечетным. Как следствие выводится, что для нахождения всех многочленов, коммутирующих с данным многочленом второй степени, достаточно рассмотреть лишь многочлены нечетной степени.

Пятый параграф — самый «конструктивный». Здесь приводятся нетривиальные примеры — цепочки попарно коммутирующих многочленов всевозможных степеней.

В шестом параграфе приводится достаточно эффективный метод исследования коммутирующих многочленов, использующий понятие неподвижной точки. С помощью него решается задача классификации для «большинства» (в определенном смысле) многочленов второй степени.

В седьмом параграфе, используя метод неподвижных точек, решается задача классификации для многочленов вида $x^3 + \alpha$.

В восьмом параграфе задача классификации для многочленов второй степени решается полностью.

Рациональные функции — следующий после многочленов класс функций, для которого естественно поставить вопрос о классификации коммутирующих функций. Есть основания считать, что для рациональных функций явление коммутирования встречается «чаще», чем для многочленов. Один из способов построения примеров коммутирующих рациональных функций приводится в девятом параграфе.

1. Сопряженные многочлены

Если $H(x) = ax + b$ $(a \neq 0)$ — многочлен первой степени, то для него существует обратный многочлен $H^{-1}(x) = \dfrac{1}{a}x - \dfrac{b}{a}$. (Нетрудно доказать, что многочлены первой степени — единственные, для которых существует обратная функция, также являющаяся многочленом.) С любым многочленом H первой степени можно связать отображение множества всех многочленов в себя, действующее по следующему правилу. Каждый многочлен P отображается в многочлен $P_H = H \circ P \circ H^{-1}$. Такое отображение называется *сопряжением* многочлена P многочленом H.

Два многочлена, один из которых может быть получен из другого сопряжением, называются *сопряженными*. Легко заметить, что сопряженные многочлены имеют одинаковую степень.

Нетрудно проверить следующие свойства:

1. $P = P_{\mathrm{id}}$;

2. Если $Q = P_H$, то $P = Q_{H^{-1}}$;

3. Если $Q = P_{H_1}$, а $R = Q_{H_2}$, то $R = P_{H_2 \circ H_1}$.

Иными словами, сопряженность является отношением эквивалентности на множестве многочленов. Это позволяет разбить множество многочленов на классы сопряженности так, что любые два сопряженных многочлена попадают в один класс, а любые два многочлена, не являющиеся сопряженными, — в разные классы.

Сопряжение обладает важным свойством — любую пару коммутирующих многочленов оно переводит в пару коммутирующих многочленов.

Предложение 1. *Если многочлены P и Q коммутируют, а H — произвольный многочлен первой степени, то многочлены P_H и Q_H тоже коммутируют.*

Доказательство.

$$\begin{aligned}
&(H \circ P \circ H^{-1}) \circ (H \circ Q \circ H^{-1}) = \\
&= H \circ P \circ (H^{-1} \circ H) \circ Q \circ H^{-1} = H \circ P \circ Q \circ H^{-1} = H \circ Q \circ P \circ H^{-1} = \\
&\qquad = H \circ Q \circ (H^{-1} \circ H) \circ P \circ H^{-1} = (H \circ Q \circ H^{-1}) \circ (H \circ P \circ H^{-1}).
\end{aligned}$$

Из предложения 1 следует, что если мы умеем находить все многочлены, коммутирующие с некоторым данным многочленом P, то мы умеем также находить и все многочлены, коммутирующие с любым сопряженным с P многочленом. Иными словами, задачу нахождения всех многочленов, коммутирующих с данным, достаточно решить для одного представителя каждого класса сопряженности.

Естественно выяснить, насколько можно упростить общий вид многочлена с помощью сопряжения.

Лемма 1. *Для любого многочлена степени $n \geqslant 2$ существует сопряженный ему многочлен со старшим коэффициентом единица и нулевым коэффициентом при $(n-1)$-й степени.*

Доказательство. Сопряжем многочлен

$$P(x) = Ax^n + Bx^{n-1} + \dots,$$

где многоточие означает члены степени ниже $n-1$, линейным двучленом $H(x) = ax + b$. Имеем

$$\begin{aligned} P_H(x) &= a\left(A\left(\frac{1}{a}x - \frac{b}{a}\right)^n + B\left(\frac{1}{a}x - \frac{b}{a}\right)^{n-1} + \dots\right) + b = \\ &= \frac{A}{a^{n-1}}x^n + \left(-\frac{nAb}{a^{n-1}} + \frac{B}{a^{n-2}}\right)x^{n-1} + \dots \end{aligned}$$

Приравнивая старший коэффициент полученного многочлена единице, получаем уравнение $a^{n-1} = A$, откуда находим a. Далее, приравнивая следующий коэффициент нулю, получаем линейное уравнение на b, из которого находим $b = \dfrac{aB}{nA}$.

Замечание. Мы предполагаем, что коэффициенты рассматриваемых многочленов — комплексные числа. Если рассматривать многочлены с действительными коэффициентами, то предложение остается справедливым лишь для четных n; при нечетных n верно несколько более слабое утверждение относительно старшего коэффициента — сопряжением его можно сделать равным 1 или -1.

Следствие. *Любой многочлен ax^2+bx+c второй степени сопряжен многочлену $x^2 - \alpha$, где $\alpha = \dfrac{3}{4}b^2 - \dfrac{1}{2}b - ac$.*

2. Единственность коммутирующего многочлена данной степени

Предложение 2. *Для данного целого положительного числа существует не более одного многочлена Q степени n, коммутирующего с данным многочленом P степени 2.*

Доказательство. Согласно предложению 1 и лемме 1, достаточно привести доказательство для случая $P(x) = x^2 - \alpha$. Пусть

$$Q(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n, \text{ где } a_0 \neq 0.$$

Тогда композиции многочленов P и Q (в одном и другом порядке) суть многочлены степени $2n$

$$P \circ Q(x) = b_0x^{2n} + b_1x^{2n-1} + b_2x^{2n-2} + \dots + b_{2n-1}x + b_{2n},$$

$$Q \circ P(x) = c_0 x^{2n} + c_1 x^{2n-1} + c_2 x^{2n-2} + \dots + c_{2n-1} x + c_{2n},$$

их коэффициенты b_i и c_i являются функциями от коэффициентов α и a_i многочленов P и Q. Будем приравнивать коэффициенты этих многочленов начиная со старшего члена. Нетрудно найти явные выражения для старших коэффициентов: $b_0 = a_0^2$, $c_0 = a_0$. Получаем $a_0^2 = a_0$, откуда $a_0 = 1$. Таким образом, старший коэффициент многочлена Q определен однозначно. Применим метод математической индукции. Предположим, что все коэффициенты a_i с номерами $i < k$ для некоторого $0 < k \leqslant n$ уже определены. Докажем, что коэффициент a_k определяется при этом однозначно. Выражение для коэффициента b_k имеет вид $b_k = a_k a_0 + \dots$, где многоточие заменяет выражение, зависящее только от коэффициентов a_i с номерами $i < k$. Коэффициент же c_k зависит только от коэффициентов a_i с номерами $i \leqslant [k/2]$ (тем самым, $i < k$) и, быть может, от α. Тем самым, уравнение $b_k = c_k$ представляет собой линейное соотношение на a_k, из которого этот коэффициент однозначно выражается через α и уже выраженные коэффициенты a_i $(i < k)$.

Таким образом, из системы уравнений $b_i = c_i$ при $0 \leqslant i \leqslant n$ мы однозначно определим числа $a_0, a_1, \dots, a_n$. Если полученные числа будут удовлетворять соотношениям $b_i = c_i$ при $n+1 \leqslant i \leqslant 2n$, то они и будут коэффициентами единственного многочлена Q степени n, коммутирующего с P. В противном случае такого многочлена не существует.

Следствие 1. *Пусть P — многочлен степени 2. Тогда для любого целого неотрицательного числа k существует единственный многочлен степени 2^k, коммутирующий с P.*

Доказательство. Многочлен P^k будет, очевидно, обладать требуемыми свойствами. Единственность непосредственно вытекает из предложения 2.

Следствие 2. *Многочлены, коммутирующие с x^2, — это многочлены x^n $(n = 1, 2, \dots)$ и только они.*

Доказательство. Очевидно, что любой многочлен вида x^n коммутирует с x^2. Поскольку степени таких многочленов составляют все множество натуральных чисел, отсутствие других коммутирующих с x^2 многочленов следует из предложения.

Приведенное доказательство предложения 2 без труда переносится и на случай, если P — многочлен степени выше второй, всюду, кроме однозначности определения старшего коэффициента многочлена Q. Точнее, справедливо следующее утверждение.

Предложение 3. *Пусть P — многочлен степени $m \geqslant 2$. Существует не более одного многочлена Q данной степени n с данным старшим коэффициентом a, коммутирующего с P. Старший член многочлена Q может принимать не более чем $m-1$ значение.*

Доказательство. Пусть

$$P(x) = A_0x^m + A_1x^{m-1} + \dots + A_{m-1}x + A_m,$$

$$Q(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n.$$

Приравнивая старшие коэффициенты многочленов $P \circ Q$ и $Q \circ R$, получаем $A_0a_0^m = a_0A_0^n$, откуда $a_0^{m-1} = A_0^{n-1}$, следовательно, a_0 может принимать не более $m-1$ различных значений.

Каждый следующий коэффициент a_k $(1 \leqslant k \leqslant n)$ многочлена $Q(x)$ выражается однозначно через ранее определенные коэффициенты a_i $(0 \leqslant \leqslant i < k)$ и коэффициенты A_i многочлена $P(x)$ из сравнения коэффициентов при $(mn-k)$-й степени многочленов $P \circ Q$ и $Q \circ P$. Действительно, коэффициент при x^{mn-k} многочлена $P \circ Q(x)$ зависит от a_k линейно (и не зависит от a_i с номерами $i > k$), а коэффициент при x^{mn-k} многочлена $Q \circ P(x)$ не зависит от a_i при $i \geqslant k$.

Предложение 4. *Пусть P — многочлен с действительными (рациональными) коэффициентами, Q — коммутирующий с ним многочлен. Пусть при этом выполнено одно из двух условий:*
а) $\deg P = 2$;
б) старший коэффициент многочлена Q является действительным (рациональным) числом.
Тогда все коэффициенты многочлена Q действительны (рациональны).

Доказательство. Формулы, выражающие коэффициенты многочлена Q в доказательствах предложений 2 и 3, не выводят за рамки действительных (рациональных) чисел.

3. Транзитивность коммутирования

Начнем с простого, но очень важного свойства, позволяющего, имея примеры коммутирующих многочленов, строить новые.

Предложение 5. *Если многочлены Q и R коммутируют с одним и тем же многочленом P, то композиция $Q \circ R$ тоже коммутирует с P.*

Доказательство. Доказательство следует из цепочки равенств

$$(Q\circ R)\circ P = \\ = Q\circ(R\circ P) = Q\circ(P\circ R) = (Q\circ P)\circ R = (P\circ Q)\circ R = \\ = P\circ(Q\circ R).$$

Предложение 6. *Если многочлены Q и R коммутируют с многочленом P второй степени, то они коммутируют между собой.*

Доказательство. Из предложения 5 следует, что многочлены $Q\circ R$ и $R\circ Q$ коммутируют с P. Поскольку эти многочлены имеют одинаковую степень, из предложения 2 следует, что они равны.

Замечание. Если степень многочлена выше второй, то предложение перестает быть справедливым. Так, многочлены x^2 и $-x$ коммутируют с x^3, но не коммутируют между собой. Однако, если дополнительно предположить, что все три многочлена P, Q и R *унитарны*, т. е. имеют старший коэффициент единица, то предложение останется в силе для многочлена P любой степени выше первой.

4. Четные и нечетные многочлены

Напомним, что функция $f(x)$ называется *четной*, если для любого x выполняется равенство $f(-x)=f(x)$ и *нечетной*, если выполняется равенство $f(-x)=-f(x)$. Нетрудно доказать, что для многочлена условие четности равносильно тому, что все коэффициенты при нечетных степенях равны нулю, а условие нечетности тому, что все коэффициенты при четных степенях равны нулю. Это означает, что любой четный многочлен может быть представлен в виде $Q(x^2)$, где Q — некоторый многочлен. Аналогично, нечетный многочлен может быть представлен в виде $xQ(x^2)$.

Напомним также одно простое, но очень важное свойство многочленов, которое будет использоваться нами неоднократно.

Лемма 2. *Если значения двух многочленов совпадают при бесконечно многих значениях аргумента, то эти многочлены тождественно равны.*

Доказательство. Разность рассматриваемых многочленов имеет бесконечно много корней. Так как ненулевой многочлен может иметь различных корней не больше, чем его степень, то эта разность является нулевым многочленом. Значит, рассматриваемые многочлены равны.

Предложение 7. *Любой многочлен $Q(x)$, коммутирующий с многочленом $P(x) = x^2 - \alpha$, является либо четным, либо нечетным.*

Доказательство. Поскольку многочлен $P(x)$ является четным, имеем

$$P(Q(-x)) = P \circ Q(-x) = Q \circ P(-x) = Q \circ P(x) = P \circ Q(x) = P(Q(x)).$$

Равенство $P(x_1) = P(x_2)$ означает $x_1^2 - \alpha = x_2^2 - \alpha$, откуда следует $x_1 = \pm x_2$. Взяв $x_1 = Q(-x)$, $x_2 = Q(x)$, получаем $Q(-x) = \pm Q(x)$. Последнее равенство справедливо для любого x. Значит, для бесконечно многих значений x имеет место либо равенство $Q(-x) = Q(x)$, либо равенство $Q(-x) = -Q(x)$. Согласно лемме 2, если первое из этих равенств выполняется для бесконечно многих значений x, то $Q(-x) \equiv Q(x)$, значит многочлен $Q(x)$ четный, а если второе, то $Q(-x) \equiv -Q(x)$, и многочлен $Q(x)$ нечетный.

Предложение 8. *Пусть Q — многочлен степени $2n$, коммутирующий с многочленом $P(x) = x^2 - \alpha$. Тогда многочлен Q можно представить в виде $Q = Q' \circ P$, где Q' — многочлен степени n, коммутирующий с P.*

Доказательство. Из предложения 7 следует, что многочлен $Q(x)$ может быть представлен как многочлен от x^2. Сделав линейную замену переменных, получаем $Q(x) = Q'(P(x))$, где Q' — многочлен степени n. Докажем, что многочлен $Q'(x)$ коммутирует с $P(x)$. Пусть $y = P(x)$. Тогда

$$P \circ Q'(y) = P \circ Q' \circ P(x) = P \circ Q(x) = Q \circ P(x) = Q' \circ P \circ P(x) = Q' \circ P(y).$$

Значения многочленов $P \circ Q'$ и $Q' \circ P$ совпадают при всех значениях аргумента из области значений многочлена $P(x)$, значит, согласно лемме 2, они тождественно равны.

Таким образом, для решения задачи классификации многочленов, коммутируюших с данным многочленом второй степени, достаточно найти все коммутируюшие с ним многочлены нечетной степени.

5. Цепочки коммутирующих многочленов. Многочлены Чебышёва

Предложение 9. *Для любого натурального числа n существует многочлен $P_n(x)$ степени n такой, что справедливо тождество*

$$P_n(t+t^{-1}) = t^n + t^{-n}.$$

Многочлены $P_n(x)$ $(n = 1, 2, \ldots)$ попарно коммутируют.

Доказательство. Существование таких многочленов будем доказывать индукцией по n. Нетрудно проверить, что при $n = 1$ и 2 многочлены $P_1(x) = x$ и $P_2(x) = x^2 - 2$ являются искомыми. Предположим, что мы нашли такие многочлены $P_n(x)$ для всех $n \leqslant k$. Тогда, воспользовавшись тождеством

$$t^{k+1} + t^{-(k+1)} = (t+t^{-1})(t^k + t^{-k}) - (t^{k-1} + t^{-(k-1)}),$$

получаем, что многочлен $P_{k+1}(x) = xP_k(x) - P_{k-1}(x)$ будет искомым при $n = k+1$.

Докажем теперь, что многочлены P_n попарно коммутируют. Пусть $x = t + t^{-1}$. Тогда

$$P_m \circ P_n(x) = P_m(t^n + t^{-n}) = t^{mn} + t^{-mn} = P_n(t^m + t^{-m}) = P_n \circ P_m(x).$$

Поскольку чисел, представимых в виде $t+t^{-1}$, бесконечно много, согласно лемме 2, многочлены $P_m \circ P_n$ и $P_n \circ P_m$ равны.

Следствие. *Все многочлены, коммутирующие с многочленом x^2-2, суть многочлены $P_n(x)$ из предложения 9.*

Доказательство. Среди многочленов P_n имеется по одному многочлену каждой степени. Значит, согласно предложению 2, других коммутирующих с $x^2 - 2$ многочленов нет.

Еще одну цепочку попарно коммутирующих многочленов можно получить следующим образом. При любом натуральном n существует такой многочлен T_n, что справедливо тождество

$$\cos nx = T_n(\cos x). \tag{2}$$

Эти многочлены называют *многочленами Чебышёва*. Из формулы (2) легко вывести, что эти многочлены попарно коммутируют. Известные тригонометрические формулы дают явные выражения для нескольких первых многочленов Чебышёва:

$$\begin{aligned} T_1(x) &= x, \\ T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 3x^3 - 4x. \end{aligned}$$

Однако цепочки многочленов P_n и многочленов Чебышёва фактически являются одним примером — одна получается из другой с помощью сопряжения многочленом $2x$. Доказать это можно многими способами, самый простой из них, пожалуй, — воспользоваться известной формулой

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}.$$

При нечетных n, аналогично приведенным выше многочленам P_n и T_n, можно построить многочлены P'_n и T'_n, определяемые равенствами

$$P'_n(t - t^{-1}) = t^n - t^{-n}$$

и

$$\sin nx = T'_n(\sin x).$$

Однако, и эти серии многочленов отличаются от своих «родственников» P_n и T_n лишь применением сопряжения. Правда, в этом случае сопрягать нужно многочленом $H(x) = ix$ с комплексными коэффициентами. Тем не менее для нечетных n полученный при сопряжении многочлен будет иметь только действительные коэффициенты.

Фактически, не существует примеров коммутирующих многочленов, отличных от приведенных. Основной классификационный результат [1, 2, 3, 4] утверждает, что любая пара унитарных коммутирующих многочленов сопряжением приводится либо к виду (P^n, P^m) для некоторого многочлена P и целых неотрицательных чисел n и m, либо к виду (x^n, x^m) для некоторых целых неотрицательных чисел n и m, либо к паре многочленов Чебышёва. Для случая, когда степень одного из многочленов равна двум, элементарное доказательство этого факта будет приведено в параграфе 8.

6. Неподвижные точки

В этом параграфе изучается важный инструмент для исследования коммутирующих многочленов — метод неподвижных точек. И хотя формально полученные здесь результаты, касающиеся задачи классификации для многочленов второй степени, перекрываются результатами восьмого параграфа, изучение неподвижных точек многочленов позволяет яснее понять ситуацию. Кроме того, в следующем параграфе этот метод применяется для решения задачи классификации коммутирующих многочленов для некоторого класса кубических многочленов.

Корни уравнения $P(x) = x$ мы называем *неподвижными точками* многочлена P. Связь неподвижных точек с коммутирующими многочленами видна из следующего утверждения.

Предложение 10. *Пусть λ — неподвижная точка многочлена P, многочлен Q коммутирует с P. Тогда $Q(\lambda)$ — тоже неподвижная точка многочлена P.*

Доказательство. $P(Q(\lambda)) = P \circ Q(\lambda) = Q \circ P(\lambda) = Q(P(\lambda)) = Q(\lambda)$.

Число x_0 будем называть *периодическим* относительно многочлена $P(x)$, если последовательность, заданная рекуррентным соотношением

$$x_{n+1} = P(x_n) \ (n = 1, 2, \ldots), \tag{3}$$

периодическая.

Многочлен будем называть *периодическим*, если нуль — периодическое относительно него число.

Предложение 11. *Пусть $P(x) = x^2 - \alpha$ — непериодический многочлен. Не существует коммутирующих с ним многочленов нечетной степени, кроме тождественного.*

Доказательство. Пусть $Q(x)$ — многочлен нечетной степени, коммутирующий с $P(x)$. Из предложения 7 следует, что $Q(x)$ является нечетным многочленом, значит, его свободный член равен нулю, поэтому нуль является его неподвижной точкой. Из предложения 10 следует, что любой член последовательности (3) при $x_0 = 0$ является неподвижной точкой многочлена $Q(x)$. Это означает, что многочлен $Q(x) - x$ имеет бесконечно много корней, что возможно только для $Q(x) \equiv x$.

Следующее простое утверждение позволяет во многих случаях доказывать непериодичность.

Лемма 3. *Если последовательность имеет строго монотонную подпоследовательность (в частности, если она сама монотонна), то она не может быть периодической.*

Доказательство. Действительно, периодическая последовательность может принимать лишь конечное число различных значений, а монотонная последовательность принимает бесконечное число различных значений.

Предложение 12. *Многочлен $x^2-\alpha$ является непериодическим в каждом из следующих трех случаев (в пунктах а) и в) α считается действительным числом, а в пункте б) — комплексным):*

а) $\alpha < 0$;

б) $|\alpha| \geqslant 2$, $\alpha \neq 2$;

в) $0 < \alpha < 1$.

Доказательство. Докажем непериодичность последовательности x_n, заданной формулами $x_0 = 0$, $x_{n+1} = x_n^2 - \alpha$. Будем пользоваться при этом утверждением леммы 3.

а) Последовательность x_n монотонно возрастает. Действительно, $x_0 = 0 < -\alpha = x_1$. Если $0 \leqslant x_{k-1} < x_k$, то неравенство $x_k < x_{k+1}$ следует из монотонности многочлена $x^2 - \alpha$ на множестве положительных чисел.

б) Нам достаточно доказать непериодичность последовательности $|x_n|$, поскольку если последовательность периодична, то последовательность модулей ее членов тоже периодична. Докажем по индукции, что последовательность $|x_n|$ строго возрастает.

База индукции. Воспользуемся неравенством треугольника и неравенством $\alpha \geqslant 2$. Имеем $|\alpha - 1| \geqslant |\alpha| - 1 \geqslant 1$. Равенство в первом случае выполняется, если α — положительное действительное число, а во втором — если $|\alpha| = 2$. Поэтому мы имеем строгое неравенство $|\alpha - 1| > 1$. Умножив его на $|\alpha|$, получаем $|\alpha^2 - \alpha| > |\alpha|$ или $|x_2| > |x_1|$.

Шаг индукции. Из предположения индукции ($x_k > x_{k-1}$) нам нужно воспользоваться лишь тем, что $|x_k| > |\alpha|$. Тогда $|x_k| - 1 > 1$. Перемножив два последних равенства, получаем $|x_k|^2 - |x_k| > |\alpha|$ или $|x_k^2| - |\alpha| > |x_k|$. Применив неравенство треугольника, имеем $|x_k^2 - \alpha| > |x_k|$, что и означает $|x_{k+1}| > |x_k|$.

в) Последовательность x_n распадается на две монотонные подпоследовательности — возрастающую подпоследовательность с нечетными номерами и убывающую с четными. Неравенства $x_{n+2} < x_n$ (при четном n) и $x_{n+2} > x_n$ (при нечетном n) доказываются индукцией по n одновременно.

База индукции ($n = 0$). Неравенство $x_2 = \alpha(\alpha - 1) < 0 = x_0$ следует из того, что $0 \leqslant \alpha \leqslant 1$.

Шаг индукции. Поскольку $x_n \leqslant 0$ для всех n, а на множестве неотрицательных чисел многочлен $x^2 - \alpha$ монотонно убывает, из неравенства

$x_{k+2} > x_k$ следует $x_{k+3} < x_{k+1}$, и наоборот, из неравенства $x_{k+2} < x_k$ следует $x_{k+3} > x_{k+1}$.

Предложение 13. *Если α — периодическое рациональное число, то оно целое.*

Доказательство. Если число α рационально, то, очевидно, вся последовательность x_n, определенная по формулам (3) при $x_0 = 0$, состоит из рациональных чисел. Знаменатель каждого члена последовательности, начиная с x_1 (если представить его в виде несократимой дроби), равен квадрату знаменателя предыдущего члена. Значит, если α нецелое, то последовательность знаменателей строго возрастает, поэтому последовательность не может быть периодической.

Периодичность многочлена $x^2 - \alpha$ является достаточным, но не необходимым, условием отсутствия коммутирующих с ним многочленов нечетной степени (кроме тождественного).

Предложение 14. *Не существует многочленов нечетной степени выше первой, коммутирующих с $x^2 - 1$.*

Доказательство. Пусть $Q(x)$ — многочлен нечетной степени выше первой, коммутирующий с $P(x) = x^2 - 1$. Рассмотрим уравнение

$$Q(x) = P(x) \tag{4}$$

и некоторый его корень λ. Из равенства

$$Q(P(\lambda)) = P(Q(\lambda)) = P(P(\lambda))$$

следует, что $P(\lambda)$ — тоже его корень. Значит, λ — периодическое число относительно многочлена P. Опишем все такие числа. Обозначим $\varphi_{1,2} = \dfrac{1 \pm \sqrt{5}}{2}$ — корни многочлена $x^2 - x - 1$ (неподвижные точки многочлена P).

Если $|x_0| > \varphi_1$, то последовательность (3) монотонно возрастает. Действительно, $x_{n+1} = P(x_n) > |x_n|$, так как

$$P(x_n) - |x_n| = x_n^2 - |x_n| - 1 = (|x_n| - \varphi_1)(|x_n| - \varphi_2) > 0.$$

Поэтому числа, большие φ_1, не являются периодическими относительно P.

Пусть теперь $|x_0| < \varphi_1$. Если $x_0 < 0$, то изменим его знак (при этом остальные члены последовательности не изменятся), поэтому можно считать, что $0 < x_0 < \varphi_1$. Начиная с некоторого номера, последовательность x_n попадет внутрь отрезка $[-1, 0]$, поскольку если бы все члены последовательности были положительны, то она была бы монотонно убывающей. Действительно, $x_{n+1} = P(x_n) < x_n$, так как $\varphi_2 < x_n < \varphi_1$, и поэтому

$$P(x_n) - x_n = x_n^2 - x_n - 1 = (x_n - \varphi_1)(x_n - \varphi_2) < 0.$$

Но тогда по теореме Больцано–Вейерштрасса последовательность x_n имела бы предел, принадлежащий полуинтервалу $[0, \varphi_1)$. Однако пределом последовательности, определенной рекуррентным соотношением (3), может быть только корень уравнения $P(x) = x$, а его на указанном полуинтервале нет.

Если член x_k последовательности, лежащий в интервале $[-1, 0]$ не является его концом или не совпадает с φ_2, то последовательность x_n непериодична, так как ее подпоследовательности с четными и нечетными номерами (начиная с k-го) монотонны. Действительно, $x_{n+2} = P^2(x_n)$. Так как

$$P^2(x) - x = (x+1)(x-\varphi_2)x(x-\varphi_1),$$

то $P^2(x) < x$ при $-1 < x < \varphi_2$ и $P^2(x) > x$ при $-1 < x < \varphi_2$. Поэтому если $x_n \in [-1, \varphi_2]$, то $x_{n+2} \in [-1, \varphi_2]$ и $x_{n+2} < x_n$, а если $x_n \in [\varphi_2, 0]$, то $x_{n+2} \in [\varphi_2, 0]$ и $x_{n+2} > x_n$.

Поэтому действительными корнями уравнения (4) могут быть только те числа, которые при многократном применении многочлена P переходят в φ_1 или φ_2 (числа, переходящие в 0 или -1, не подходят, так как 0 не является корнем (4)). Пусть x_n — первый член последовательности, равный φ_i ($i = 1$ или 2). Тогда $x_{n-1} = -\varphi_i$, так как $P(x) = \varphi \Leftrightarrow x = \pm\varphi$. Однако равенства $P(\varphi_i) = Q(\varphi_i)$ и $P(-\varphi_i) = Q(-\varphi_i)$ одновременно выполняться не могут, поскольку P — четный многочлен, Q — нечетный, а $P(\varphi_i) \neq 0$. Поэтому φ_1 и φ_2 — единственные возможные корни (4).

По предложению 4 уравнение (4) имеет рациональные коэффициенты, поэтому корни φ_1 и φ_2 должны иметь одинаковую кратность. Последнее противоречит тому, что уравнение нечетной степени должно иметь нечетное количество действительных корней.

В восьмом параграфе будет доказано, что единственные приведенные многочлены второй степени, для которых существуют нетождественные коммутирующие многочлены нечетной степени, — это x^2 и $x^2 - 2$.

7. Кубические многочлены

В этом параграфе мы перечислим все многочлены, коммутирующие с многочленом вида $x^3+\alpha$. (Напомним, что сопряжением любой кубический многочлен приводится к виду $x^3+\beta x+\alpha$.)

Предложение 15. *Пусть $P(x) = x^3+\alpha$ (α — ненулевое действительное число). Все коммутирующие с $P(x)$ многочлены суть $P^n(x)$.*

Доказательство. Аналогично предложению 7 докажем, что любой коммутирующий с $P(x)$ многочлен $Q(x)$ содержит ненулевые коэффициенты только при степенях x, дающих при делении на 3 одинаковые остатки. Иными словами, $Q(x)$ имеет один из видов $Q'(x^3)$, $xQ'(x^3)$ или $x^2Q'(x^3)$. Пусть ξ — отличный от единицы (комплексный) кубический корень из единицы. Тогда $P(\xi x) = P(x)$ для любого x. Имеем

$$P(Q(\xi x)) = Q(P(\xi x)) = Q(P(x)) = P(Q(x)),$$

откуда $Q(\xi x)^3 = Q(x)^3$, значит,

$$0 = Q(x)^3 - Q(\xi x)^3 = (Q(\xi x) - Q(x))(Q(\xi x) - \xi Q(x))(Q(\xi x) - \xi^2 Q(x)).$$

Тем самым справедливо одно из равенств:

$$Q(\xi x) = Q(x), \tag{5}$$
$$Q(\xi x) = \xi Q(x), \tag{6}$$
$$Q(\xi x) = \xi^2 Q(x). \tag{7}$$

Поскольку одно из этих равенств справедливо для бесконечно многих значений x, оно справедливо при всех x. Представим $Q(x)$ в виде

$$Q(x) = Q_0(x^3) + xQ_1(x^3) + x^2Q_2(x^3).$$

Тогда

$$Q(\xi x) = Q_0(x^3) + \xi x Q_1(x^3) + \xi^2 x^2 Q_2(x^3).$$

Если справедливо равенство $Q(\xi x) = Q(x)$, то $Q_1 = Q_2 \equiv 0$, и многочлен $Q(x)$ имеет ненулевые коэффициенты лишь при степенях, делящихся на 3. Если справедливо равенство $Q(\xi x) = \xi Q(x)$, то $Q_0 = Q_2 \equiv 0$, и многочлен $Q(x)$ имеет ненулевые коэффициенты лишь при степенях, дающих при делении на 3 остаток 1. Соответственно, равенство $Q(\xi x) = \xi x^2 Q(x)$ означает, что $Q_0 = Q_1 \equiv 0$ и многочлен $Q(x)$ имеет ненулевые коэффициенты лишь при степенях, дающих при делении на 3 остаток 2.

Далее так же, как и в предложении 8, показывается, что любой многочлен Q степени $3n$, коммутирующий с P, имеет вид $Q' \circ P$, где Q' — многочлен степени n, тоже коммутирующий с P.

Задача свелась к нахождению многочленов степени не кратной трем, коммутирующих с P. Непосредственно проверяется, что тождественный многочлен является единственным таким многочленом первой степени (проверка здесь необходима, поскольку теорема 3 утверждает лишь, что таких многочленов не больше двух), значит, $P^n(x)$ — единственный коммутирующий многочлен степени 3^n. Из этого следует, что если мы найдем все многочлены степени n, коммутирующие с P, то мы тем самым найдем все многочлены степеней $3^k n$, коммутирующие с P.

Осталось доказать, что многочлен P не имеет коммутирующих многочленов степени выше первой и не кратной трем.

Пусть Q — такой многочлен. Тогда его свободный член равен нулю (действительно, его ненулевые коэффициенты могут быть только при степенях, дающих одинаковые остатки при делении на 3, а старшая степень на 3 не делится), поэтому нуль является корнем уравнения $Q(x) = x$. Из предложения 10 следует, что многочлен P должен быть периодическим. С другой стороны, из монотонности многочлена P следует монотонность последовательности x_n, определенной по формуле (3) при $x_0 = 0$ (она убывающая при $\alpha < 0$ и возрастающая при $\alpha > 0$). Из леммы 3 следует, что эта последовательность непериодична, а значит, непериодичен и многочлен P. Получаем противоречие.

Предложение 16. *Все многочлены, коммутирующие с x^3, — это $\pm x^n$ ($n = 1, 2, \ldots$).*

Доказательство. Легко проверить, что все эти многочлены коммутируют с x^3. Этих многочленов имеется по два каждой степени. Согласно предложению 3, других коммутирующих с x^3 многочленов нет.

8. Классификация многочленов, коммутирующих с квадратными многочленами

Лемма 4. *Существует единственный (с точностью до умножения на -1) многочлен F данной степени n такой, что многочлен $(x+1)F(x)^2 - 1$ является нечетным.*

Доказательство. Пусть $F(x) = ax^n + bx^{n-1} + \ldots$ ($a \neq 0$) — многочлен степени $n \geqslant 1$, удовлетворяющий условиям леммы. Тогда

$$(x+1)F(x)^2 - 1 = a^2 x^{2n+1} + (2ab + a^2)x^n + \ldots$$

Приравниваем нулю коэффициент при $2n$-й степени, получаем $a = -2b$, в частности, $b \neq 0$.

Разложим F в сумму четной и нечетной компонент:

$$F(x) = U(x^2) + xV(x^2),$$

тогда условие леммы можно записать в виде

$$U(t)^2 + 2tU(t)V(t) + tV(t)^2 = 1 \tag{8}$$

(мы обозначили $t = x^2$). Обозначим старший коэффициент многочлена $U(t)$ через u_0, а многочлена $V(t)$ — через v_0. Тогда если n четно, то $u_0 = a$, $v_0 = b$, значит, $u_0 = -2v_0$ и $\deg U = \deg V + 1 = n/2$; а если n нечетно, то $u_0 = b$, $v_0 = a$, значит, $v_0 = -2u_0$ и $\deg U = \deg V = (n-1)/2$.

Непосредственно проверяется, что если (U, V) — решение уравнения (8), то $(U + 2tV, -2U + (1-4t)V)$ и $((1-4t)U - 2tV, 2U + V)$ — тоже решения. Таким образом, мы имеем два отображения Φ_+ и Φ_- соответственно на множестве всех многочленов. Эти отображения переводят многочлены, удовлетворяющие условию леммы, в многочлены, также ему удовлетворяющие. Поэтому будем их рассматривать только на множестве таких многочленов.

Если степень многочлена четна (и не равна нулю), то отображение Φ_+ понижает ее. Действительно, из условий $u_0 = -2v_0$ и $\deg U = \deg V + 1$ следует, что $\deg(U + 2tV) < \deg U$ и $\deg(-2U + (1-4t)V) \leqslant \deg V$. Аналогично, отображение Φ_- понижает степень многочлена, если она нечетна.

На самом деле эти отображения (при $n \geqslant 2$) понижают степень многочлена на 2. Действительно, легко проверить, что описанные отображения Φ_+ и Φ_- являются взаимно обратными. Пусть F — многочлен нечетной степени (напомним, что мы рассматриваем только многочлены, удовлетворяющие условию леммы). Тогда $\Phi_-(F)$ — тоже многочлен нечетной степени. В противном случае получаем противоречие

$$\deg F = \deg \Phi_+(\Phi_-(F)) < \deg \Phi_+(F) < \deg F.$$

Поэтому отображение Φ_- понижает степень многочлена по крайней мере на 2. Больше, чем на 2 степень понизится не может, поскольку обратное отображение Φ_+ не может повысить степень многочлена более, чем на 2 (это следует из явного выражения для Φ_+). Аналогично рассматривается случай многочлена F четной степени.

Таким образом, применяя многократно к многочлену F, удовлетворяющему условию леммы, преобразования Φ_+ или Φ_- (в зависимости от четности его степени), мы получим многочлен, удовлетворяющий условию леммы, первой или нулевой степени. Значит, любой такой многочлен F может быть получен из многочлена первой или нулевой степени многократным применением обратного преобразования. Непосредственное вычисление показывает, что искомые многочлены нулевой и первой степени — это только ± 1 и $\pm(2t-1)$. Значит, для любой степени такой многочлен единствен с точностью до умножения на -1.

Предложение 17. *Для любого (комплексного) числа $\alpha \neq 0$ или 2 не существует многочлена нечетной степени выше первой, коммутирующего с $P(x) = x^2 - \alpha$.*

Доказательство. Пусть $Q(x)$ — многочлен степени $2n+1$ ($n \geqslant 1$), коммутирующий с $P(x)$. Из предложения 7 следует, что

$$Q(x) = xQ'(x^2),$$

где $Q'(x)$ — многочлен степени n со старшим коэффициентом 1. Условие коммутирования многочленов запишем в виде

$$x^2 Q'(x^2)^2 = P(x)Q'(P(x)^2) + \alpha.$$

Предположим, что $\alpha \neq 0$, и введем обозначение $y = \dfrac{P(x)}{\alpha}$, тогда $x^2 = \alpha(y+1)$. Имеем

$$(y+1)Q'(\alpha y + \alpha)^2 = yQ'((\alpha y)^2) + 1.$$

Обозначим далее $F(y) = Q'(\alpha y + \alpha)$ и $G(y) = Q'(\alpha y)$. Степень многочлена F равна n, а старший коэффициент равен α^n. Получаем

$$(y+1)F(y)^2 = yG(y^2) + 1. \tag{9}$$

Возьмем в качестве $Q(x)$ многочлен $P_n(x)$, коммутирующий с $x^2 - 2$, из предложения 9. В этом случае старший коэффициент многочлена F равен 2^n. Поскольку в силу (9) многочлен F удовлетворяет условиям леммы 4, для любого другого многочлена $Q(x)$ мы получим тот же самый многочлен F, быть может, умноженный на -1. Это возможно только если $\alpha^n = \pm 2^n$. Значит, $|\alpha| = 2$. Однако в этом случае воспользуемся предложением 12 б) — многочлен $x^2 - \alpha$ является непериодическим, значит, не имеет коммутирующих нечетной степени выше первой.

Объединяя результаты следствия 2, предложения 2, предложения 9 и его следствия и предложений 8 и 17, получаем основную классификационную теорему.

Теорема. *Пусть $P(x) = x^2 - \alpha$. Тогда все многочлены, коммутирующие с $P(x)$, суть многочлены вида (n — целое неотрицательное число):*

- x^n, *если* $\alpha = 0$;
- $P_n(x)$, *определенные в предложении 9, если* $\alpha = 2$;
- $P^n(x)$ *в остальных случаях.*

С учетом предложения 1 и леммы 1, эта теорема полностью классифицирует все многочлены, коммутирующие с данным многочленом второй степени.

9. Коммутирующие рациональные функции

Как мы видели, случаи коммутирования многочленов очень редки. Приведем один способ построения примеров коммутирующих рациональных функций. Рассмотрим для этого кривую G, задаваемую соотношением $y^2 = x^3 + px + q$. График этой кривой для случая $p = 1$, $q = 0$ изображен на рис. 1.

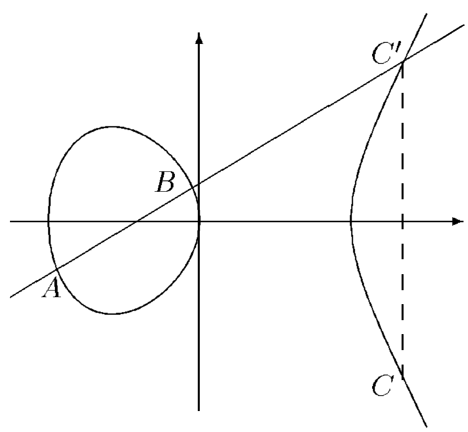

Рис. 1.

На кривой G введем операцию «сложения точек» следующим образом. Пусть две (не симметричные относительно оси абсцисс) точки A и B лежат на кривой G. Проведем через них секущую (или касательную в случае совпадения точек A и B). Она пересекает кривую G в точках A, B и в некоторой третьей точке C'. Действительно, уравнение этой (невертикальной) кривой будет иметь вид $y = kx + b$. Точки пересечения этой прямой с кривой G суть решения системы

$$\begin{cases} y^2 &= x^3 + px + q, \\ y &= kx + b. \end{cases}$$

Подставив в первое уравнение системы вместо y его значение из второго уравнения, получаем кубическое уравнение относительно x. Два (быть может, совпадающих) его корня — это абсциссы точек A и B. Третий корень будет абсциссой искомой точки C'. Ордината точки C' однозначно находится из второго уравнения системы. Суммой точек A и B называется точка C, симметричная точке C' относительно оси абсцисс.

Если точки A и B симметричны относительно оси абсцисс, то их суммой считается добавленная к кривой G бесконечно удаленная точка. Суммой любой точки A и бесконечно удаленной точки считается сама точка A.

Лемма 5. *Введенная операция сложения точек на кривой G является ассоциативной.*

Мы не будем приводить доказательства этой леммы, его можно найти во многих книгах, в частности [6, 7]. Как следствие леммы 5 получаем, что для любой точки A корректно определена точка $nA = \underbrace{A + A + \dots + A}_{n \text{ слагаемых}}$. Рассмотрим множество функций F_n определенных равенствами $F_n(x_A) = x_{nA}$ (через x_A и x_{nA} обозначены абсциссы точек A и nA соответственно).

Предложение 18. *Функции F_n являются попарно коммутирующими рациональными функциями.*

Доказательство. Коммутирование функций F_i доказывается просто. Пусть $x = x_A$ для некоторой точки $A \in G$. Тогда

$$F_m \circ F_n(x) = F_m(x_{nA}) = x_{mnA} = F_n(x_{mA}) = F_n \circ F_m(x).$$

Рациональность будем доказывать индукцией по n. Одновременно будем доказывать, что квадрат углового коэффициента k_n прямой, проходящей через точки x_A и x_{nA}, является рациональной функцией от x_A.

База индукции. Очевидно, что $F_1 = \mathrm{id}$ — рациональная функция, а $k_1(x)$ — это производная $\dfrac{dy}{dx}$ функции, задающей кривую G. Поэтому

$$k_1(x) = \frac{(x^3 + px + q)'}{(y^2)'} = \frac{3x^2 + p}{2y},$$

$$k_1^2(x) = \frac{(3x^2 + p)^2}{4(x^3 + px + q)}.$$

Шаг индукции. Пусть $F_n(x)$ и $k_n^2(x)$ являются рациональными функциями от x. Точки A, nA и $-(n+1)A$ лежат на прямой $y = k_n(x_A)x + b$, значит, их абсциссы x_A, $x_{nA} = F_n(x_A)$ и $x_{-(n+1)A} = x_{(n+1)A} = F_{n+1}(x_A)$ являются корнями кубического уравнения $(k_n(x_A)x + b)^2 = x^3 + px + q$.

По теореме Виета $x_A + F_n(x_A) + F_{n+1}(x_A) = k_n(x_A)^2$. Поэтому $F_{n+1}(x) = k_n(x)^2 - F_n(x) - x$. Так как функции $F_n(x)$ и $k_n(x)^2$ рациональны по предположению индукции, то $F_{n+1}(x)$ — тоже рациональная функция.

Поскольку точки A, nA и $-(n+1)A$ лежат на одной прямой с угловым коэффициентом $k_n(x_A)$,

$$\begin{aligned} y_A - y_{nA} &= k_n(x_A)(x_A - x_{nA}), \\ y_A + y_{(n+1)A} &= k_n(x_A)(x_A - x_{(n+1)A}). \end{aligned}$$

С другой стороны, точки A и $(n+1)A$ лежат на прямой с угловым коэффициентом $k_{n+1}(x_A)$, поэтому

$$y_A - y_{(n+1)A} = k_{n+1}(x_A)(x_A - x_{(n+1)A}).$$

Перемножив два последних равенства, получаем

$$y_A^2 - y_{(n+1)A}^2 = k_n(x_A)k_{n+1}(x_A)(x_A - x_{(n+1)A})^2,$$

откуда следует

$$\begin{aligned} k_{n+1}(x_A) &= \frac{y_A^2 - y_{(n+1)A}^2}{(x_A - x_{(n+1)A})^2 k_n(x_A)} = \\ &= \frac{(x_A^3 + px_A + q) - (x_{(n+1)A}^3 + px_{(n+1)A} + q)}{(x_A - x_{(n+1)A})^2 k_n(x_A)} = \\ &= \frac{(x_A^2 + x_A x_{(n+1)A} + x_{(n+1)A}^2 + p)}{(x_A - x_{(n+1)A}) k_n(x_A)}. \end{aligned}$$

Значит,

$$k_{n+1}(x) = \frac{x^2 + xF_{n+1}(x) + F_{n+1}(x)^2 + p}{(x - F_{n+1}(x))k_n(x)}.$$

Возведя последнюю формулу в квадрат, из рациональности функций $k_n(x)^2$ (по предположению индукции) и $F_{n+1}(x)$ (доказанной выше) получаем рациональность $k_{n+1}(x)^2$.

В качестве упражнения предлагаем читателю найти явный вид функций $F_n(x)$ для нескольких значений n.

Список литературы

[1] *Ritt J.* Prime and Composite Polynomials // Trans. AMS. V. 23. 1922. P. 51–66.

[2] *Dorey F., Whaples G.* Prime and Composite Polynomials // J. Algebra. V. 28. 1972. P. 88–101.

[3] *Engstrom H. T.* Polynomial substitutions // Amer. J. Math. V. 63. 1941. P. 249–255.

[4] *Levi H.* Composite Polynomials with coeffitients in an arbitrary field of characteristic zero // Amer. J. Math. V. 64. 1942. P. 389–400.

[5] *Янтаров И.* Коммутирующие многочлены // Квант. №4. 1979. С. 19–23.

[6] *Прасолов В. В., Соловьев Ю. П.* Эллиптические функции. Специальный курс. М.: МК НМУ. 1993.

[7] *Рид М.* Алгебраическая геометрия для всех. М.: Мир. 1991.