Н.Г. Чеботарев

Теория Галуа

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Н11

Н.Г. Чеботарев
Н11 Теория Галуа / Н.Г. Чеботарев – М.: Книга по Требованию, 2021. – 153 с.

ISBN 978-5-458-25759-6

Настоящая монография представляет обзор важнейших результатов, полученных в настоящее время по теории Галуа. Теория Галуа, как отдельный комплекс проблем и методов, выделяется в математической литературе, насколько мне известно, впервые (см. также мой обзорный доклад на Цюрихском конгрессе математиков, 1932 г.). Наряду с классической теорией Галуа, посвященной решению уравнений в радикалах (которой посвящена глава II этой монографии), сюда включена проблема построения уравнений с заданной группой (глава III), проблема, для решения которой привлечены теория идеалов, р-адические числа, а также теория рациональных функций многих переменных (проблема Люрота). Далее, глава IV посвящена проблеме резольвент проблеме, поставленной первоначально Ф.Клейном в более узкой формулировке (проблема форм), а затем расширенной Д.Гильбертом 13-я проблема его доклада на Парижском, конгрессе в 1900 г.). Проблема резольвент потребовала привлечения теории непрерывных групп, теории, весьма далекой от алгебры по своим методам. Наконец, глава V содержит ряд обобщений теории Галуа: с одной стороны, распространение теории Галуа на поля более общего типа, а с другой стороны, несколько проблем, решаемых не групповыми методами, но близких к теории Галуа по теме. Сюда относятся: проблема псевдоэллиптических интегралов, проблема Энриквеса понижения степени уравнения с многими неизвестными и др. Эти проблемы, в настоящее время разрозненные, должны в будущем составить главы Науки о рациональном.

ISBN 978-5-458-25759-6

I. ВВЕДЕНИЕ.

§ 1. Поля. Рациональные функции.

1. В теории *Galois* понятие рациональной величины является основным понятием, а потому мы остановимся на нем подробнее. Под рациональным числом в обычном смысле этого слова разумеется дробь вида $\pm\frac{a}{b}$, где a и b суть числа натурального ряда 1, 2, 3, ... Совершая над рациональными числами обычные арифметические операции: сложение, вычитание, умножение и деление по обычным школьным правилам, мы будем опять получать рациональные числа (если считать также число *нуль* рациональным числом).

2. В современной алгебре понятие рационального числа обобщается следующим образом. Совокупность каких-либо предметов называется *группой*, если мы устанавливаем над ними, каким бы то ни было образом, понятие *операции*, т. е. способа сопоставления с каждой парой таких предметов (называемых *элементами* группы), взятых в определенном порядке, определенного третьего предмета той же совокупности [1]), и если при этом соблюдаются следующие правила:

I. Имеет место *ассоциативный* закон $(AB)D=A(BD)$.

II. Группа содержит элемент I (называемый *правой единицей* группы), который для всякого элемента группы удовлетворяет равенству

$$X\cdot I=X. \tag{1. 1}$$

Можно показать, что всякая группа содержит одну единственную правую единицу, которая в то же время является и *левой* единицей, т. е. имеет место

$$I\cdot X=X. \tag{1. 2}$$

III. Каждому элементу A группы соответствует содержащийся в группе *правый обратный элемент* X, для которого имеет место $A\cdot X=I$.

Можно показать, что группа не может содержать несколько различных правых обратных элементов, и что правый обратный элемент является также левым обратным элементом, т. е. наряду с $A\cdot X=I$ имеет место также $X\cdot A=I$[21]. Поэтому принято обозначать элемент, обратный к A, так: A^{-1}.

Если результат операции не зависит от порядка элементов множителей, т. е. если для всех элементов группы имеет место $A\cdot B=B\cdot A$, то группа называется коммутативной или абелевой (в честь знаменитого

---

[1]) Если с элементами A и B сопоставляется элемент C, то мы будем записывать этот факт так: $A\cdot B=C$.

норвежского математика *N. H. Abel'я*, 1802—1829). Легко понять, что все положительные и отрицательные числа вместе с нулем составляют абелеву группу, если под операцией над элементами понимать обыкновенное сложение. При этом единицей группы служит *нуль*. Точно так же совокупность всех рациональных чисел, *кроме нуля*, составляет абелеву группу относительно умножения, причем единицей группы служит обыкновенная единица.

3. Теперь введем понятие *поля* (корпус, тело, область), которое является непосредственным обобщением понятия совокупности рациональных чисел. Мы будем называть полем совокупность каких-либо элементов, над которыми установлено два вида операций. По аналогии со школьной арифметикой мы будем называть первую операцию *сложением* и установим для ее обозначения знак $+$, а вторую *умножением* и записывать ее при помощи знака $\times$ или вовсе без знака. При этом должны соблюдаться следующие правила:

I. Все элементы поля образуют абелеву группу относительно сложения.

Единичный элемент этой группы будем называть и обозначать *нулем поля*.

II. Все элементы поля, кроме нуля, образуют абелеву группу относительно умножения.

Единичный элемент этой группы будем называть и обозначать *единицей поля*.

III. Имеет место *дистрибутивный* (распределительный) закон, а именно $(a+b)c = ac + bc$.

Пользуясь дистрибутивным законом, нетрудно показать, что всякий элемент поля, умноженный на нуль, даст нуль: $a \cdot 0 = 0$.

Кроме того, из свойства II вытекает, что произведение двух элементов поля равно нулю только тогда, если один из множителей равен нулю. Это свойство (отсутствие делителей нуля) играет большую роль при дальнейших обобщениях понятия поля.

4. Нетрудно привести несколько примеров полей. Полем является совокупность всех *действительных* (вещественных) чисел. Совокупность всех *комплексных* чисел также является полем. Присоединяя к какому-нибудь полю величину ξ, не входящую в поле, мы придем к новому полю, содержащему первоначальное поле как часть (будем в дальнейшем говорить: первоначальное поле является *делителем* нового поля). Элементами нового поля являются рациональные функции от величины ξ с коэфициентами из первоначального поля. В классификации полей является существенным, удовлетворяет ли величина ξ алгебраическому уравнению с коэфициентами из первоначального поля или нет. В первом случае присоединение называется *алгебраическим*, во втором — *трансцендентным* [1]).

5. Если первоначальным полем является поле рациональных чисел, то величины поля, расширенного путем алгебраического присоединения, носят название *алгебраических чисел*. Каждая из них удовлетворяет алгебраическому уравнению с рациональными коэфициентами. Будем

[1]) В случае трансцендентного присоединения величину ξ следует представлять себе, как переменную величину, которой не приписывается никакого численного значения.

обозначать такого рода поле так: $K(\xi)$. Обобщим понятие рациональной величины следующим образом: будем называть величину η рациональной в поле $K(\xi)$, если она содержится в этом поле. Например, величина $\frac{1}{\sqrt{2}+3}$ рациональна в поле $K(\sqrt{2})$.

Поле, расширенное путем трансцендентного присоединения, состоит из всевозможных рациональных функций от присоединяемой величины, так что их теория приводится к изучению рациональных функций. Всякая рациональная функция может быть представлена как частное двух *целых рациональных функций* или *полиномов*, которыми мы главным образом и будем заниматься в дальнейшем.

К первоначальному полю можно присоединить не одну, а несколько величин. Если между присоединяемыми величинами $\xi_1, \xi_2, \ldots, \xi_m$ не имеет места никакое алгебраическое соотношение, то поле $K(\xi_1, \xi_2, \ldots, \xi_m)$ является полем рациональных функций от m переменных. Если же между $\xi_1, \xi_2, \ldots, \xi_m$ имеет место одно или несколько алгебраических соотношений, то получаемое поле носит название *поля алгебраических функций*. В дальнейшем мы убедимся, что можно заменить присоединяемые величины $\xi_1, \xi_2, \ldots, \xi_m$ их рациональными функциями $\eta_1, \eta_2, \ldots, \ldots \eta_q$ $(q \leqslant m)$, через которые в свою очередь рационально выражаются $\xi_1, \xi_2, \ldots, \xi_m$, причем между $\eta_1, \eta_2, \ldots, \eta_q$ существует уже не более одного соотношения (теорема *Kronecker'a*).

6. Поля рациональных функций от m независимых переменных имеют несравненно более простую структуру, чем поля рациональных функций от величин, между которыми имеется алгебраическое соотношение. Поэтому является важной задачей найти критерий того, чтобы данное поле алгебраических функций могло быть приведено при помощи замены переменных к полю рациональных функций от независимых переменных. Эта задача окончательно решена только для случая *одной* независимой переменной.

Упомянем еще об одной проблеме: может ли всякий делитель поля рациональных функций быть приведен к полю рациональных функций? Эта проблема носит название проблемы *Lüroth'a* или проблемы *рационального минимального базиса*. Она была решена в 1876 г. *P. Lüroth'ом* в положительном смысле для $m = 1$[40]; *E. Netto*[44] предложил чисто алгебраический вывод ее решения. В 1894 г. *G. Castelnuovo*[6] решил ее для случая $m = 2$. Для случая $m = 3$ *F. Enriques*[45], опираясь на работу *G. Fano*[47], нашел пример делителя поля рациональных функций, который не может быть приведен к полю рациональных функций. Представляет большой интерес разыскание всех типов такого рода полей. К сожалению, все эти вопросы до сих пор трактуются исключительно геометрическим методом, в то время как современная алгебра еще не в состоянии охватить их. В связи с этим упомянутые вопросы еще ждут своего эффективного (при помощи конечного числа действий) разрешения.

§ 2. Полиномы. Их корни. Делимость полиномов. Алгоритм Евклида. Кратные корни. Интерполяция.

1. Каждый элемент поля рациональных функций от одной переменной x может, как мы видели, быть представлен, как частное двух целых рациональных функций или полиномов, т. е. выражений вида

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \qquad (2.1)$$

где $a_0, a_1, \ldots, a_{n-1}, a_n$ суть величины первоначального поля K или, как мы будем говорить, рациональные в поле K величины.

Основной задачей алгебры считается решение уравнений, приведенных к виду $f(x)=0$, где $f(x)$ — полином, другими словами, нахождение значений x, обращающих $f(x)$ в нуль [*корней* полинома $f(x)$]. При этом слово „решение" может быть понимаемо в различных смыслах. Известно, что всякое уравнение имеет корень, лежащий в поле всех комплексных чисел. Доказательство его существования опирается на соображения непрерывности. В теории *Galois*, во всяком случае в ее первоначальном понимании, рассматривается вопрос о выражении корней полиномов в *радикалах*, т. е. при помощи корней *двучленных полиномов* $x^m - A$. Эта задача, как мы увидим ниже, не всегда имеет решение. В данный момент мы, не делая предположений о природе корней, будем рассматривать корни, как вновь вводимые величины, подчиняющиеся обычным арифметическим законам, характеризующим поле.

2. Задача нахождения корней равносильна с задачей разложения полинома на линейные множители. В самом деле, полином $f(x)$ делится на линейный полином $x-a$ тогда и только тогда, если a есть корень полинома $f(x)$ (теорема *Bézout*). Представляя полином $f(x)$ в виде $(x-a)f_1(x)$, находя (или предполагая существующим) корень полинома $f_1(x)$ и продолжая процесс, мы в конце концов придем к следующему представлению полинома в виде произведения линейных полиномов:

$$f(x)=a_0(x-a_1)(x-a_2)\dots(x-a_n), \qquad (2.\ 2)$$

где $a_1, a_2, \dots, a_n$ — корни полинома $f(x)$. Их число равно степени полинома $f(x)$. Из формулы (2. 2) ясно, что $f(x)$ не может иметь других корней, кроме $a_1, a_2, \dots, a_n$. Поэтому всякий полином n-й степени имеет ровно n корней.

3. Впрочем, число корней может быть меньше в том случае, если некоторые из величин $a_1, a_2, \dots, a_n$ равны друг другу. В этом случае говорят, что полином $f(x)$ имеет кратные корни. Точнее: корень a называется корнем k-й кратности, если $f(x)$ делится на $(x-a)^k$.

Существование кратных корней обнаруживается при помощи *производной* $f'(x)$ от полинома $f(x)$, которую можно определить, как коэффициент при первой степени h в разложении выражения $f(x+h)$ по степеням h. (Такое определение не содержит понятий непрерывности и предела, а потому может быть применяемо также в тех случаях, когда рассматриваемое поле не позволяет оперировать с непрерывными величинами. Мы увидим ниже, что такие поля существуют; примером может служить *конечное поле*.) Это определение может быть заменено следующими правилами практического нахождения производной:

$$\text{I.}\quad (x^m)'=m\cdot x^{m-1};$$

$$\text{II.}\quad (c\cdot f(x))'=c\cdot f'(x);$$

$$\text{III.}\quad (f(x)+g(x))'=f'(x)+g'(x),$$

где c — величина, не зависящая от x. Этих правил достаточно для определения производной от любого полинома.

Производная от производной носит название второй производной и обозначается так: $f''(x)$. Аналогично определяются третья, четвертая

и т. д. производные. При их помощи можно представить разложение $f(x+h)$ по степеням h так:

$$f(x+h)=f(x)+h\cdot f'(x)+\frac{h^2}{2!}f''(x)+\ldots+\frac{h^n}{n!}f^n(x) \qquad (2.3)$$

(формула *Taylor'a*). Подставляя сюда $x=a$, $a+h=z$, мы убедимся, что a является k-кратным корнем полинома $f(z)$ тогда и только тогда, если величины $f(a)$, $f'(a)$, $\ldots, f^{k-1}(a)$ обращаются в нуль.

Отсюда же следует, что k-кратный корень полинома $f(x)$ является $(k-1)$-кратным корнем его производной $f'(x)$. Другими словами, при $k>1$ полином $f(x)$ и его производная имеют общий множитель $(x-a)^{k-1}$. Таким образом для нахождения кратных корней надо найти общий наибольший делитель полиномов $f(x)$ и $f'(x)$.

4. Общий наибольший делитель двух полиномов $f(x)$ и $g(x)$ отыскивается путем так называемого *алгоритма Евклида* или *алгоритма последовательного деления*. Пусть степень $f(x)$ больше или равна степени $g(x)$. Разделим $f(x)$ на $g(x)$ и определим таким образом частное $q_1(x)$ и остаток $r_1(x)$. Затем разделим $g(x)$ на остаток $r_1(x)$, и пусть новое частное будет $q_2(x)$, а остаток $r_2(x)$. Разделим $r_1(x)$ на $r_2(x)$ и т. д. При продолжении процесса степени полиномов $r_i(x)$ будут все время уменьшаться, так что мы в конце концов дойдем или до остатка, не зависящего от x, или до того, что предыдущий полином разделится на последующий без остатка. На этом прекратим процесс.

На основании известной связи между делимым, делителем, частным и остатком будем иметь:

$$\left.\begin{aligned} f(x)&=g(x)\cdot q_1(x)+r_1(x),\\ g(x)&=r_1(x)\cdot q_2(x)+r_2(x),\\ &\cdots\cdots\cdots\cdots\cdots\\ r_{m-2}(x)&=r_{m-1}(x)\cdot q_m(x)+r_m(x),\\ r_{m-1}(x)&=r_m(x)\,q_{m+1}(x). \end{aligned}\right\} \qquad (2.4)$$

Я утверждаю, что последний делитель (в данном случае $r_m(x)$) является общим наибольшим делителем полиномов $f(x)$ и $g(x)$. С одной стороны, $r_m(x)$ есть делитель $f(x)$ и $g(x)$, в чем мы убедимся из последовательного рассмотрения равенств (2.4), начиная с предпоследнего и идя снизу вверх. С другой стороны, всякий общий делитель $f(x)$ и $g(x)$ является также делителем $r_m(x)$. В этом мы убедимся из равенств (2.4), начиная с первого и идя сверху вниз.

Из равенств (2.4) можно при помощи последовательного исключения полиномов $r_{m-1}(x)$, $r_{m-2}(x)$, $\ldots$, $r_1(x)$ получить весьма важное для дальнейшего тождество

$$r_m(x)=u(x)\cdot f(x)+v(x)\cdot g(x), \qquad (2.5)$$

где $u(x)$ и $v(x)$ — некоторые полиномы. В частности, если общий наибольший делитель не зависит от x (в этом случае полиномы $f(x)$ и $g(x)$ называются *взаимно простыми*), имеет место тождество

$$u(x)\cdot f(x)+v(x)\cdot g(x)=1. \qquad (2.6)$$

5. *H. Weber*[68] и *O. Perron*[68] предложили для общего наибольшего делителя вполне определенные выражения через коэфициенты полиномов $f(x)$ и $g(x)$. Именно, *Perron*, предполагая, что общий наибольший делитель полиномов

$$f(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m,$$
$$g(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n \quad (a_0 \neq 0,\ b_0 \neq 0)$$

имеет k-ю степень, получил для него выражение в форме определителя. Замечательно, что в случае большего числа переменных невозможно составить подобное выражение для общего наибольшего делителя.

6. Таким образом коэфициенты общего наибольшего делителя получаются из коэфициентов заданных полиномов рациональным путем, т. е. принадлежат тому же полю. Отсюда следует, что в полиноме с кратными корнями можно рациональным путем выделить множители, уже не имеющие кратных корней. Именно, пусть $f(x) = X_1X_2^2 \ldots X_k^k$, где полиномы $X_1, X_2, \ldots, X_k$ не имеют кратных корней и взаимно просты. Обозначая через $f_l(x)$ общий наибольший делитель $f_{l-1}(x)$ и $f'_{l-1}(x)$, мы, очевидно, будем иметь:

$$f_1(x) = X_2X_3^2 \ldots X_k^{k-1},$$

и аналогично

$$f_2(x) = X_3 \ldots X_k^{k-2},$$
$$\ldots\ldots\ldots\ldots$$
$$f_{k-2}(x) = X_{k-1}X_k^2,$$
$$f_{k-1}(x) = X_k.$$

Вводя обозначения

$$g_1(x) = \frac{f(x)}{f_1(x)},\quad g_2(x) = \frac{f_1(x)}{f_2(x)}, \ldots,\quad g_{k-1}(x) = \frac{f_{k-2}(x)}{f_{k-1}(x)},\quad g_k(x) = f_{k-1}(x),$$

мы получим для $X_1, X_2, \ldots, X_k$ следующие выражения:

$$X_1 = \frac{g_1(x)}{g_2(x)},\quad X_2 = \frac{g_2(x)}{g_3(x)}, \ldots,\quad X_{k-1} = \frac{g_{k-1}(x)}{g_k(x)},\quad X_k = g_k(x).$$

7. Доказанное имеет силу, поскольку мы имеем дело с обыкновенными числовыми полями. Существуют, однако, поля, в которых подобное выделение не всегда возможно. Именно, в некоторых полях (например, в так называемых *конечных* полях) любой элемент поля, умноженный на определенное простое число, называемое *характеристикой* поля, обращается в нуль. В этом случае производные полиномов, содержащих x только в степенях, кратных характеристике, тождественно равны нулю (см *E. Steinitz*[65], стр. 258).

8. В заключение упомянем об интерполяционной формуле *Lagrange'a*, которая понадобится нам в дальнейшем. Если мы зададимся целью построить полином $g(x)$ не выше n-й степени, принимающий при заданных значениях $x = x_0, x_1, \ldots, x_n$ переменной x соответственно значения $y_0, y_1, \ldots, y_n$, то этими условиями полином $g(x)$ однозначно определится и может быть представлен в виде следующего выражения:

$$g(x) = f(x)\left\{\frac{y_0}{f'(x_0)(x-x_0)} + \frac{y_1}{f'(x_1)(x-x_1)} + \ldots + \frac{y_n}{f'(x_n)(x-x_n)}\right\}, \quad (2.\ 7)$$

где $f(x) = (x-x_0)(x-x_1)\ldots(x-x_n)$. Если же мы отбросим требо

вание, чтобы степень $g(x)$ не превышала n, то общее решение задачи может быть представлено в виде:

$$g(x)+f(x)\cdot\varphi(x),$$

где $g(x)$ — полином, найденный по формуле (2. 7), а $\varphi(x)$ — произвольный полином.

9. Для решения этой интерполяционной задачи *Newton* [47] предложил другую, более удобную для практических вычислений формулу, которая в том случае, когда значения $x_0, x_1, \ldots, x_n$ взять через равные интервалы, имеет следующий вид:

$$g(x)=y_0+\frac{x-x_0}{h}\Delta y_0+\frac{(x-x_0)(x-x_0-h)}{2!\,h^2}\Delta^2 y_0+\ldots$$
$$\ldots+\frac{(x-x_0)(x-x_0-h)\ldots(x-x_0-(n-1)h)}{n!\,h^n}\Delta^n y_0, \qquad (2.\ 8)$$

где

$$h=x_{i+1}-x_i,\quad \Delta y_i=y_{i+1}-y_i,$$

$$\Delta^2 y_i=\Delta y_{i+1}-\Delta y_i,\ \ldots,\ \Delta^n y_i=\Delta^{n-1}y_{i+1}-\Delta^{n-1}y_i\ (i=0,1,\ldots,n-1).$$

§ 3. Симметрические функции. Результант. Дискриминант.

1. В дальнейшем мы будем полагать в уравнении $a_0=1$. Сравнивая коэфициенты при различных степенях x в формулах (2. 1) и (2. 2), мы получим следующие выражения коэфициентов полиинома через его корни:

$$\left.\begin{aligned}
a_1&=-\alpha_1-\alpha_2-\ldots-\alpha_n,\\
a_2&=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3+\ldots+\alpha_{n-1}\alpha_n,\\
a_3&=-\alpha_1\alpha_2\alpha_3-\alpha_1\alpha_2\alpha_4-\ldots-\alpha_{n-2}\alpha_{n-1}\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
a_{n-1}&=(-1)^{n-1}(\alpha_1\alpha_2\ldots\alpha_{n-1}+\ldots+\alpha_2\alpha_3\ldots\alpha_n),\\
a_n&=(-1)^n\alpha_1\alpha_2\ldots\alpha_n.
\end{aligned}\right\} \qquad (3.\ 1)$$

Обратим внимание на то, что правые части этих формул представляют собой функции от корней $\alpha_1, \alpha_2, \ldots, \alpha_n$, не меняющих своего вида, если мы самым произвольным образом переставим корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ между собой. Такого рода функции носят название *симметрических*. Очевидно, что всякая рациональная функция от коэфициентов $a_1, a_2, \ldots, a_n$ является в силу (3. 1) рациональной симметрической функцией от корней $\alpha_1, \alpha_2, \ldots, \alpha_n$. Справедливо и обратное выражение:

Всякая рациональная симметрическая функция от корней $\alpha_1, \alpha_2, \ldots, \alpha_n$ рационально выражается через коэфициенты $a_1, a_2, \ldots, a_n$ (называемые также *элементарно-симметрическими функциями* от $\alpha_1, \alpha_2, \ldots, \alpha_n$). Если при этом она есть целая рациональная функция от $\alpha_1, \alpha_2, \ldots, \alpha_n$, то и через $a_1, a_2, \ldots, a_n$ она выразится, как целая рациональная функция. Если, кроме того, ее коэфициенты суть целые числа, то и в выражении через $a_1, a_2, \ldots, a_n$ коэфициенты будут целыми числами.

2. Для этой теоремы существует несколько доказательств. Самое замечательное из них в теоретическом отношении принадлежит *Cauchy* [7], который вводит в рассмотрение следующие полиномы (модули *Cauchy*):

В качестве первого полинома X — полином $f(x)$.

В качестве полинома X_1 — частное от деления X на $x - a_1$. Его коэфициенты рационально зависят от a_1, а корнями являются $a_2, a_3, \ldots, a_n$.

В качестве полинома X_2 — частное от деления X_1 на $x - a_2$. Его коэфициенты суть рациональные функции от a_1 и a_2, а корнями являются $a_3, \ldots, a_n$.

Продолжая процесс, придем наконец к полиному X_{n-1}, коэфициенты которого суть рациональные функции от $a_1, a_2, \ldots, a_{n-1}$, а корнем является a_n. Заметим, что степени полиномов $X, X_1, \ldots, X_{n-1}$ убывают с каждым шагом на единицу.

Пусть V будет целая рациональная симметрическая функция от $a_1, a_2, \ldots, a_n$. Подставим в ее выражение вместо a_n переменную x и разделим V на X_{n-1}. Остаток от деления не будет зависеть от x, так как полином X_{n-1} линейный. Этот остаток должен быть численно равен V. Затем заменим в полученном выражении a_{n-1} через x и разделим на X_{n-2}. Получится линейный относительно x остаток, который при подстановке $x = a_{n-1}$ должен давать V. Действительно, $V(x) = X_{n-2}\,Q(x) + R(x)$ при подстановке $x = a_{n-1}$ дает $V = R(a_{n-1})$. Но величина V согласно условию не изменится, если мы поменяем местами a_{n-1} и a_n. Поэтому, если мы в выражении $R(a_{n-1})$ заменим a_{n-1} на a_n [a_n заменять на a_{n-1} не придется, так как в выражение $R(x)$ a_n не входит], то это выражение не изменится. Таким образом уравнение $R(x) - V = 0$, будучи первой степени, имеет два корня: a_{n-1} и a_n, а потому является тождеством, т. е. в $R(x)$ x не входит, и $R = V$.

Таким путем мы постепенно освободим выражение от корней $a_n, a_{n-1}, \ldots, a_2, a_1$ и в конце концов получим рациональную функцию от $a_1, a_2, \ldots, a_n$. Так как во всех встречающихся здесь процессах деления делители имеют единицу при старших членах, то все выражения будут оставаться целыми рациональными, и V будет представлено как целая рациональная функция от $a_1, a_2, \ldots, a_n$.

3. Это доказательство теоретически наиболее совершенно, но для практического вычисления более удобны другие методы. Один из них дает возможность вычислять простейшие симметрические функции, которые получаются, если взять произвольное произведение степеней корней типа $a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n}$ и прибавить к нему все отличные от него члены, полученные от всевозможных перестановок корней. Будем записывать такого рода простейшие симметрические функции так: $\sum a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n}$. Любая целая симметрическая функция является суммой такого рода функций.

Самыми простыми функциями этого типа являются функции

$$\sum a_i^k = a_1^k + a_2^k + \ldots + a_n^k,$$

называемые суммами k-х степеней и обозначаемые символом s_k. *Newton* [48] вывел для них следующие рекуррентные формулы, связывающие

их с коэфициентами $a_1, a_2, \ldots, a_n$ и позволяющие последовательно вычислять $s_1, s_2, s_3, \ldots$:

$$s_1 + a_1 = 0,\ s_2 + a_1 s_1 + 2a_2 = 0,\ s_3 + a_1 s_2 + a_2 s_1 + 3a_3 = 0, \ldots \quad (3.\ 2)$$

Если эти формулы (при вычислении s_k для $k > n$) приведут нас к коэфициентам $a_k (k > n)$, то их следует просто полагать равными нулю.

Waring [67] предложил следующую явную формулу, выражающую s_n через коэфициенты $a_1, a_2, \ldots, a_m$:

$$s_n = \sum \frac{(-1)^{\lambda_1+\lambda_2+\cdots+\lambda_m} \cdot n\,(\lambda_1+\lambda_2+\ldots+\lambda_m-1)!}{\lambda_1!\,\lambda_2!\ldots\lambda_m!}\, a_1^{\lambda_1} a_2^{\lambda_2} \ldots a_m^{\lambda_m}, \quad (3.\ 3)$$

где сумма распространяется на неотрицательные значения $\lambda_1, \lambda_2, \ldots, \lambda_m$, удовлетворяющие равенству:

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + m\lambda_m = n. \quad (3.\ 4)$$

Обратно, коэфициенты $a_1, a_2, \ldots, a_m$ могут быть следующим образом выражены через суммы степеней:

$$a_n = \sum \frac{(-1)^{\lambda_1+\lambda_2+\cdots+\lambda_m}}{1^{\lambda_1} 2^{\lambda_2} \ldots m^{\lambda_m} \lambda_1!\,\lambda_2!\ldots\lambda_m!}\, s_1^{\lambda_1} s_2^{\lambda_2} \ldots s_m^{\lambda_m}, \quad (3.\ 5)$$

где значки суммирования попрежнему удовлетворяют равенству (3. 4). Коэфициент $\frac{1}{1^{\lambda_1} 2^{\lambda_2} \ldots m^{\lambda_m} \lambda_1!\,\lambda_2!\ldots\lambda_m!}$, будучи умножен на $n!$, равняется числу подстановок в симметрической группе n-й степени, состоящих из λ_1 одночленных, λ_2 двучленных, $\ldots, \lambda_m$ m-членных циклов.

4. Формула (3. 5) показывает, что всякая симметрическая функция рационально выражается через $s_1, s_2, \ldots, s_n$, или, как принято говорить, система $s_1, s_2, \ldots, s_n$ является *базисом* поля симметрических функций. Во многих случаях бывает важно определить, какая система n симметрических функций является базисом и какая нет. Этот вопрос ставился по отношению к системам типа $s_{k_1}, s_{k_2}, \ldots, s_{k_n}$ *Borchardt'ом* [4], *Vahlen'ом* [68], *Ludwig'ом* [39] и *S. Kakeya* [26], который доказал, что системы этого типа являются базисами, если система всех натуральных чисел, отличных от $k_1, k_2, \ldots, k_n$, является *аддитивной последовательностью*, т. е. если сумма любых чисел этой последовательности тоже принадлежит к этой последовательности. Результат *Kakeya* содержит результаты предыдущих авторов, как частные случаи.

Nakamura [43] предложил практический прием для нахождения этих выражений.

5. Следующими по простоте при настоящей классификации симметрическими функциями являются суммы вида $\sum a_1^{k_1} a_2^{k_2}$, выражаемые через s_k так:

$$\sum a_1^{k_1} a_2^{k_2} = s_{k_1} s_{k_2} - s_{k_1+k_2}\,(k_1 \neq k_2), \qquad \sum a_1^k a_2^k = \frac{1}{2}\, s_k^2 - \frac{1}{2}\, s_{2k},$$

затем тройные:

$$\sum a_1^{k_1} a_2^{k_2} a_3^{k_3} = s_{k_1} s_{k_2} s_{k_3} - s_{k_1+k_2} s_{k_3} - s_{k_1+k_3} s_{k_2} - s_{k_2+k_3} s_{k_1} + 2s_{k_1+k_2+k_3} (k_1 \neq k_2 \neq k_3),$$

$$\sum a_1^k a_2^k a_3^{k_3} = \frac{1}{2}\,(s_k^2 s_{k_3} - s_{2k} s_{k_3} - 2s_{k+k_3} s_k + 2s_{2k+k_3}) \quad (k \neq k_3),$$

$$\sum a_1^k a_2^k a_3^k = \frac{1}{6}\,(s_k^3 - 3s_{2k} s_k + 2s_{3k})$$

и т. д. Для произвольной функции этого вида *Waring*[67] получил следующее выражение:

$$\sum a_1^{k_1}a_2^{k_2}\dots a_k^{k_k} =$$
$$= \sum (-1)^{k-\lambda_1-\lambda_2-\dots-\lambda_k}(1!)^{\lambda_1}(2!)^{\lambda_2}\dots(\overline{k-1}!)^{\lambda_k}T(\lambda_1, \lambda_2, \dots, \lambda_k), \quad (3.\ 6)$$

где значки суммирования $\lambda_1, \lambda_2, \dots, \lambda_k$ удовлетворяют условию

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \dots + k\lambda_k = k,$$

а $T(\lambda_1, \lambda_2, \dots, \lambda_k)$ обозначают сумму произведений множителей типа

$$s_{\Sigma k_1},\ s_{\Sigma k_2},\ \dots,\ s_{\Sigma k_l},$$

где значок при i-м множителе равен сумме i слагаемых из ряда k_1, $k_2, \dots, k_k$ $(i = 1, 2, \dots, k)$, а суммирование распространяется на все перестановки в этом ряду, дающие различные произведения $s_{\Sigma k_1}, s_{\Sigma k_2}, \dots, s_{\Sigma k_l}$. Здесь, в отличие от обычного допущения $s_0 = n$, приходится принимать $s_0 = 1$. Формула (3. 6) справедлива в предположении, что все k_i различны. В противном случае левая часть уменьшается в некоторое число раз.

6. В том же мемуаре *Waring* предложил другой метод вычисления простейших сумм, который позволяет выражать их непосредственно через коэфициенты уравнения, а не при помощи сумм степеней. Здесь мы будем считать задачу приведенной к более простой, если нам удастся выразить заданную симметрическую функцию $\sum a_1^{k_1}a_2^{k_2}\dots a_k^{k_k}$ через другие симметрические функции, для которых наибольший из показателей k будет меньше. Предположим, что $k_1 \geqslant k_2 \geqslant \dots \geqslant k_k$, и составим произведение $(-1)^{k_1+k_2+\dots+k_k}\cdot a_1^{k_1-k_2}\cdot a_2^{k_2-k_3}\dots a^{k_{k-1}-k_k}\cdot a^{k_k}$. Выражая его через корни, производя перемножение и собирая члены одинакового типа, мы получим сумму $\sum a_1^{k_1}a_2^{k_2}\dots a_k^{k_k}$, а также суммы более „простого" типа. При последних должны стоять некоторые численные коэфициенты, определение которых составляет главную трудность метода. Оно достигается или непосредственно с помощью методов комбинаторики, или путем подстановки вместо корней частных значений. Получаемое равенство устанавливает линейную связь между заданной симметрической функцией и другими функциями более „простого" типа. Производя для последних подобную же редукцию, мы в конце концов выразим все рассматриваемые симметрические функции через такие, в которых показатели при корнях равны единице, т. е. которые являются просто элементарно-симметрическими функциями. Например, чтобы вычислить $\sum a_1^3a_2^2a_3$, мы должны определить $a_1a_2a_3$. Получается:

$$a_1a_2a_3 = \sum a_1\cdot\sum a_1a_2\cdot\sum a_1a_2a_3 = \sum a_1^3a_2^2a_3 + 3\sum a_1^3a_2a_3a_4 +$$
$$+ 3\sum a_1^2a_2^2a_3^2 + 8\sum a_1^2a_2^2a_3a_4 + 22\sum a_1^2a_2a_3a_4a_5 + 60\sum a_1a_2a_3a_4a_5a_6.$$

7. Одним из наиболее важных приложений теории симметрических функций является определение *результанта*. Пусть заданы два полинома:

$$f(x) = a_0x^m + a_1x^{m-1} + \dots + a_m = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_m),$$
$$g(x) = b_0x^n + b_1x^{n-1} + \dots + b_n = b_0(x-\beta_1)(x-\beta_2)\dots(x-\beta_n).$$