Math-Net.Ru

Общероссийский математический портал

В. В. Варфоломеев, Группы Галуа полиномов Герона–Сабитова для пятиугольников, вписанных в окружности, *Матем. сб.*, 2004, том 195, номер 2, 3–16

DOI: <https://doi.org/10.4213/sm798>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.181.102

26 апреля 2023 г., 06:33:05

УДК 513.7

В. В. Варфоломеев

Группы Галуа полиномов Герона–Сабитова для пятиугольников, вписанных в окружности

Вычисляются группы Галуа над полями рациональных функций от ребер пятиугольника d -, r - и S -полиномов. Корнями этих полиномов являются диагонали, радиусы описанных окружностей и площади вписанных многоугольников. Группы Галуа оказываются максимально широкими. Даются элементарные геометрические приложения.

Библиография: 3 названия.

Введение

Полиномы Герона–Сабитова (ГС-полиномы) были введены в статье И. Х. Сабитова [1] (естественно, что там они так не назывались), где было показано, что объем многогранника является алгебраической функцией от квадратов длин ребер этого многогранника. Вид полинома зависит только от топологического рода и комбинаторного типа многогранника. В статье [2] были построены аналоги ГС-полиномов для геометрических характеристик вписанных в окружность многоугольников (невыпуклых в том числе). ГС-полиномы многоугольников имеют высокую степень симметрии, поэтому их проще исследовать; кроме того, возможны предсказания “по аналогии” геометрического смысла корней ГС-полиномов многогранников. У ГС-полиномов многоугольников есть интересные особенности. Например, в полях разложений этих полиномов действует бесконечномерная алгебра Ли с конечным числом образующих (группа Галуа представлена в ней автоморфизмами). Эта алгебра порождается бесконечно малыми вращениями вершин многоугольников вдоль описанных окружностей, при этом вращения вдоль разных окружностей не коммутируют (эта алгебра Ли будет предметом изучения в следующей работе автора). Основным объектом изучения настоящей статьи является полином

$$\begin{aligned} P_d(x) = & \left(x^3 + \left(\frac{a_3 a_4}{a_5} + \frac{a_3 a_5}{a_4} + \frac{a_4 a_5}{a_3} \right) x^2 \right. \\ & \left. + (a_3^2 + a_4^2 + a_5^2) x + a_3 a_4 a_5 \right) (x^2 - a_1^2 - a_2^2)^2 \\ & - \frac{1}{a_3 a_4 a_5} (x(x^2 - a_3^2 - a_4^2 - a_5^2) - 2a_3 a_4 a_5)^2 a_1^2 a_2^2 \end{aligned}$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 02-01-00101).

$$\begin{aligned}
&= (x^3 + v_1x^2 + v_2x + v_3)(x^2 - u)^2 - \frac{1}{v_3}(x^3 - v_2x - 2v_3)^2t \\
&= P_0(x)Q_0(x) + F(x)t
\end{aligned} \tag{1}$$

(см. [2; пример к лемме 1], там дано разложение (1) по степеням x). Его геометрический смысл такой: диагональ, соединяющая вершины A_1 и A_3 вписанного в окружность 5-угольника с длинами ребер $a_1, a_2, \dots, a_5$ (см. ниже рис. 1), будет корнем полинома (1). При этом некоторые длины диагоналей могут получаться с отрицательным знаком — это явление объясняется в [2; лемма 13]. Полином (1) неприводим над полем рациональных функций от ребер, а геометрическая причина, по которой он имеет седьмую степень, такова: имеется 7 правильных многоугольников — выпуклый, 5-конечная звезда и пять треугольников с 3-кратным ребром (любая из пяти вершин может быть изолированной); малое шевеление ребер одного из них приводит к расщеплению кратных корней полинома (1) и появлению семи вписанных в разные окружности 5-угольников с одинаковым набором ребер (подробнее см. в [2; § 4]). Необязательно, что все корни (1) будут чьими-то диагоналями; например, 5-угольников с ребрами $(5, 4, 3, 2, 1)$ всего три, хотя действительных корней у полинома (1) пять. Кроме полинома $P_d(x)$ мы рассмотрим полиномы $P_r(x^2) = P_r(y)$ и $P_S(x^2) = P_S(z)$. Их корни — квадраты радиусов описанных окружностей и квадраты площадей 5-угольников соответственно (площадь невыпуклого многоугольника понимается в смысле формулы (6) из [2]). Оба полинома имеют седьмую степень по y или z соответственно, однако их полные степени слишком велики, чтобы имело смысл их выписывать (в [2] вычислен свободный член $P_S(z)$, он имеет 28-ю степень и геометрический смысл).

Основной результат статьи такой: группы Галуа всех трех полиномов над полем $K(a_1, a_2, \dots, a_5)$ рациональных функций от алгебраически независимых переменных $a_1, a_2, \dots, a_5$ (это ребра 5-угольников) изоморфны полной группе подстановок из семи элементов S_7 , и их поля разложений совпадают. Последнее утверждение влечет некоторые элементарно-геометрические следствия, и они приведены в § 2 после доказательства теоремы 2.

В заключение автор выражает благодарность участникам геометрического семинара А. С. Мищенко и А. Т. Фоменко, семинара И. Х. Сабитова на мех.-мат. факультете МГУ им. М. В. Ломоносова, а также алгебраического семинара А. Н. Паршина в Математическом институте им. В. А. Стеклова РАН за готовность выслушать и обсудить старомодную тематику настоящей работы.

§ 1. Группа Галуа d -полинома над полем, порожденным его коэффициентами

Пусть k — поле, порожденное коэффициентами полинома (1). Можно показать, что оно совпадает с полем рациональных функций от v_1, v_2, v_3, u, t . Через k_1 обозначается подполе в k рациональных функций от v_1, v_2, v_3, u . Коэффициенты самих рациональных функций будем сразу считать комплексными.

ТЕОРЕМА 1. *Группа Галуа полинома (1) над полем k изоморфна группе подстановок S_7 .*

ДОКАЗАТЕЛЬСТВО. Нам понадобятся некоторые леммы.

ЛЕММА 1. *Имеет место следующее разложение полинома (1) в произведение формальных степенных рядов по t :*

$$P_0(x)Q_0(x) + F(x)t = \sum_{i=0}^{\infty} P_i(x)t^i \sum_{i=0}^{\infty} Q_i(x)t^i, \quad (2)$$

где $P_i(x)$ и $Q_i(x)$ – полиномы от x с коэффициентами в k_1 , причем

$$\deg P_i(x) \leq 2, \quad \deg Q_i(x) \leq 3$$

при всех $i = 1, 2, \dots$.

ДОКАЗАТЕЛЬСТВО. Для $i = 1$ имеем

$$P_0(x)Q_1(x) + Q_0(x)P_1(x) = F(x). \quad (3)$$

Рассматриваем (3) как систему семи линейных над k_1 уравнений с семью неизвестными коэффициентами полиномов $P_1(x)$ и $Q_1(x)$. Определитель этой системы – это результат полиномов $P_0(x)$ и $Q_0(x)$. Так как они взаимно просты, этот результат отличен от нуля в k_1 . Следовательно, система (3) имеет единственное решение в k_1 . При $i > 1$ коэффициенты полиномов $P_i(x)$ и $Q_i(x)$ вычисляются из линейной системы вида

$$P_0Q_i + Q_0P_i = - \sum_{l+l'=i} P_lQ_{l'}, \quad l > 0, \quad l' > 0,$$

поэтому остается применить индукцию по i .

Заметим теперь, что $P_0(x)$ имеет своими корнями

$$-\frac{a_3a_4}{a_5}, \quad -\frac{a_3a_5}{a_4}, \quad -\frac{a_4a_5}{a_3},$$

поэтому разложение (2) в степенные ряды можно продолжить:

ЛЕММА 2. *Имеют место следующие разложения в формальные степенные ряды по t :*

$$\begin{aligned} \sum_{i=0}^{\infty} P_i(x)t^i &= \left(x + \frac{a_3a_4}{a_5} + \sum_{i=1}^{\infty} A_i t^i \right) \left(x + \frac{a_3a_5}{a_4} + \sum_{i=1}^{\infty} A'_i t^i \right) \\ &\quad \times \left(x + \frac{a_4a_5}{a_3} + \sum_{i=1}^{\infty} A''_i t^i \right), \end{aligned} \quad (4)$$

$$\sum_{i=0}^{\infty} Q_i(x)t^i = \left((x + \sqrt{u})^2 + \sum_{i=1}^{\infty} B_i(x)t^i \right) \left((x - \sqrt{u})^2 + \sum_{i=1}^{\infty} B'_i(x)t^i \right), \quad (5)$$

где A_i, A'_i, A''_i – рациональные функции от $a_3a_4/a_5, a_3a_5/a_4, a_4a_5/a_3, u$; $B_i(x)$ линейны по x , а их коэффициенты – рациональные функции от $v_1, v_2, v_3, \sqrt{u}$.

Доказательство аналогично доказательству леммы 1.

Записав каждый из множителей в правой части (5) по степеням переменной x , получим два квадратных трехчлена:

$$(x + \sqrt{u})^2 + \sum_{i=1}^{\infty} B_i(x) t^i = x^2 + (2\sqrt{u} + \mu_1 t + \mu_2 t^2 + \dots)x + u + \nu_1 t + \nu_2 t^2 + \dots, \quad (6)$$

$$(x - \sqrt{u})^2 + \sum_{i=1}^{\infty} B'_i(x) t^i = x^2 + (-2\sqrt{u} + \mu'_1 t + \mu'_2 t^2 + \dots)x + u + \nu'_1 t + \nu'_2 t^2 + \dots. \quad (7)$$

ЛЕММА 3. *Дискриминанты квадратных трехчленов (6) и (7) имеют вид*

$$\Delta = -\frac{F(-\sqrt{u})}{uP_0(-\sqrt{u})}t + \dots, \quad (8)$$

$$\Delta' = -\frac{F(\sqrt{u})}{uP_0(\sqrt{u})}t + \dots, \quad (9)$$

здесь F обозначает слагаемые старших по t степеней.

ДОКАЗАТЕЛЬСТВО. Вычисляя дискриминанты, получаем

$$\Delta = 4(\sqrt{u} \mu_1 - \nu_1)t + \dots, \quad \Delta' = -4(\sqrt{u} \mu'_1 + \nu'_1)t + \dots.$$

Коэффициенты $\mu_1, \nu_1, \mu'_1, \nu'_1$ линейных функций $B_1 = \mu_1 x + \nu_1$ и $B'_1 = \mu'_1 x + \nu'_1$ находим из уравнения $(x + \sqrt{u})^2 B'_1 + (x - \sqrt{u})^2 B_1 = Q_1(x)$, откуда получаем

$$4(\sqrt{u} \mu_1 - \nu_1)u = -Q_1(-\sqrt{u}), \quad -4(\sqrt{u} \mu'_1 + \nu'_1)u = -Q_1(-\sqrt{u}).$$

Так как $Q_0(\pm\sqrt{u}) = 0$, то из (3) найдем

$$Q_1(\sqrt{u}) = \frac{F(\sqrt{u})}{P_0(\sqrt{u})}, \quad Q_1(-\sqrt{u}) = \frac{F(-\sqrt{u})}{P_0(-\sqrt{u})},$$

что и завершает доказательство леммы.

СЛЕДСТВИЕ 1. *Разложения в формальные ряды по степеням t корней квадратных трехчленов (6) и (7) содержат полуцелые степени t .*

ДОКАЗАТЕЛЬСТВО. По лемме 3 имеем

$$\sqrt{\Delta'} = \sqrt{-\frac{F(\sqrt{u})}{uP_0(\sqrt{u})}} \cdot \sqrt{t} \cdot \sqrt{1 + c_1 t + c_2 t^2 + \dots},$$

остается воспользоваться для последнего множителя в правой части биномиальной формулой.

Пусть $k(\alpha_1, \dots, \alpha_l)$ обозначает расширение поля k , полученное присоединением к нему алгебраических элементов $\alpha_1, \dots, \alpha_l$. Пусть, далее, x_1, x_2, x_3 — корни по-

$$k \subset k(x_1) \subset k(x_1, x_2) \subset k(x_1, x_2, x_3) \subset \cdots \subset k(x_1, \dots, x_7). \quad (10)$$
$$\sum_{i=0}^{\infty} P_i(x) t^i = x^3 + M_2 x^2 + M_1 x + M_0 = \tilde{P}(x), \quad (11)$$

$$\sum_{i=0}^{\infty} Q_i(x)t^i = x^4 + N_3x^3 + N_2x^2 + N_1x + N_0 = \tilde{Q}(x). \quad (12)$$

ДОКАЗАТЕЛЬСТВО. Если (11) приводим, то хотя бы один из его корней, скажем x_1 , будет полиномом над k от $x_4, \dots, x_7$. Перестановка $a_4 \leftrightarrow a_5$ приводит, очевидно, к перестановке корней $x_1 \leftrightarrow x_2$, а остальные корни и само поле k остаются неподвижными. Но (1) неприводим, поэтому его корни простые; получили противоречие. Пусть теперь (12) приводим. Если он распадается на линейный и кубический множители, то один из его корней будет полиномом над k от x_1, x_2, x_3 . Замена $\sqrt{u} \rightarrow -\sqrt{u}$ переводит корни полинома (6) в корни (7) и наоборот. Однако корни x_1, x_2, x_3 и поле k остаются неподвижными – такое же противоречие. Пусть (12) распадается на квадратичные множители (6) и (7). Тогда их коэффициенты являются полиномами от x_1, x_2, x_3 над k . Эти полиномы неподвижны при замене $\sqrt{u} \rightarrow -\sqrt{u}$, но (6) и (7) должны поменяться местами – противоречие. Наконец, если (12) распадается на квадратичные множители $(x - x_4)(x - x_6)$ и $(x - x_5)(x - x_7)$, то к противоречию приводит замена $\sqrt{t} \rightarrow -\sqrt{t}$, которая оставляет поле $k(x_1, x_2, x_3)$ неподвижным, а эти множители переводит друг в друга.

ЛЕММА 5. *Полином (11) неприводим над $k(M_0, M_1, M_2)$, и степень расширения поля $k(x_1, x_2, x_3)$ над $k(M_0, M_1, M_2)$ равна 6.*

ДОКАЗАТЕЛЬСТВО. Коэффициенты M_i рационально над k выражаются через коэффициенты N_j полинома (12), а N_j , в свою очередь, — через $x_4, \dots, x_7$, поэтому $k(M_0, M_1, M_2)$ можно рассматривать как подполе в $k(x_4, x_5, x_6, x_7)$ и неприводимость (11) следует из леммы 4. Расширение $k(M_0, M_1, M_2) \subset k(x_1, x_2, x_3)$ является расширением Галуа с группой S_3 (любая перестановка корней x_1, x_2, x_3 индуцируется соответствующей перестановкой переменных a_3, a_4, a_5), и степень расширения равна порядку этой группы.

$$k \stackrel{7}{\subset} k(x_1) \stackrel{d}{\subset} k(x_1, x_2) \stackrel{d'}{\subset} k(x_1, x_2, x_3)$$
$$\quad \quad \quad \cap^{7.l} \qquad \qquad \qquad 6\subset$$
$$k(M_0, M_1, M_2),$$

здесь над знаками включения стоят соответствующие степени расширений. Имеем $dd' = 6l$ и $d \geq d'$, поэтому для d формально возможны значения 3, 4, 5, 6. Первые три исключаются по лемме 4, значит, $d = 6$. Из формально возможных значений d' (от 1 до 5) значения 2, 3, 4 исключаются по лемме 4; покажем, что $d' = 1$ также невозможно. В противном случае имеем $x_3 = p(x_1, x_2)$ – полином над k . Перестановка $a_4 \leftrightarrow a_5$ оставляет на месте корень x_3 и переставляет x_1 с x_2 , следовательно, p можно считать симметричным (иначе возьмем полусумму $p(x_1, x_2)$ и $p(x_2, x_1)$). По уже доказанному существует автоморфизм σ поля разложения $k(x_1, x_2, \dots, x_7)$, переводящий x_1 в x_4 , а x_2 в x_6 (условимся при этом, что нумерация корней такая, что замена $\sqrt{u} \rightarrow -\sqrt{u}$ переводит x_4 в x_6). По лемме 4 $\sigma(x_3)$ не может быть ни одним из корней x_1 или x_2 , поэтому $\sigma(x_3)$ равно x_5 или x_7 . Предположим, что $\sigma(x_3) = x_5$, тогда $x_5 = \sigma(x_3) = p(\sigma(x_1), \sigma(x_2)) = p(x_4, x_6)$. Замена $\sqrt{u} \rightarrow -\sqrt{u}$ переводит x_5 в x_7 , но $p(x_4, x_6)$ остается неподвижным – противоречие. Аналогично исключается $\sigma(x_3) = x_7$. Итак, $d' = 5$. Заметим еще, что из леммы 4 следует, что степень расширения $k(x_1, x_2, x_3) \subset k(x_1, x_2, x_3, x_4)$ равна четырем. Таким образом, мы вычислили степень расширения в первых четырех этажах башни (10). Для вычисления оставшихся степеней удобно изменить порядок присоединения корней. Рассмотрим теперь башню

$$k \stackrel{7}{\subset} k(x_7) \stackrel{d}{\subset} k(x_7, x_6) \stackrel{d'}{\subset} k(x_7, x_6, x_5) \stackrel{d''}{\subset} k(x_7, x_6, x_5, x_4) \stackrel{6}{\subset} k(x_7, \dots, x_1).$$

В последнем этаже степень расширения равна 6, так как это расширение Галуа с группой S_3 . Из уже доказанного ясно, что произведение $d \cdot d' \cdot d''$ кратно 20, поэтому $d = 5$ или $d' = 5$, но первая возможность исключается леммой 4, поэтому $d' = 5$. Для d'' значения 2 и 3 невозможны по лемме 4, если же $d'' = 1$, то $d = 4$ – вновь противоречие с леммой 4. Итак, $d'' = 4$. Покажем, что $d = 6$: $d \neq 1$, так как замена $\sqrt{u} \rightarrow -\sqrt{u}$ давала бы $d'' = 1$; $d \neq 2$, иначе $d' = 1$; $d \neq 3$, иначе $d'' = 1$; и, наконец, значения 4 или 5 исключены леммой 4. Таким образом, степень расширения $k(x_1, x_2, x_3, \dots, x_7)$ над k равна $7!$ и доказательство теоремы 1 закончено.

§ 2. Группы Галуа d -, r - и S -полиномов над полем рациональных функций от ребер 5-угольника

ТЕОРЕМА 2. *Группа Галуа d -полинома над $K = K(a_1, \dots, a_5)$ изоморфна S_7 .*

ДОКАЗАТЕЛЬСТВО. Сначала докажем некоторые леммы.

ЛЕММА 6. *Поле k , рассматриваемое как подполе в K , состоит из всех элементов, неподвижных относительно следующих автоморфизмов K :*

- а) перестановка переменных a_1 и a_2 ;
- б) замена $a_i \rightarrow -a_i$, $i = 1, 2$;
- в) перестановки переменных a_3, a_4, a_5 ;
- г) одновременная замена $a_j \rightarrow -a_j$, $a_k \rightarrow -a_k$, $j \neq k$, $j, k = 3, 4, 5$.

Доказательство леммы 6 очевидно.

Положим $k' = K \cap k(x_1, x_2, \dots, x_7)$.

ЛЕММА 7. *Поле k' инвариантно относительно автоморфизмов из леммы 6.*

ДОКАЗАТЕЛЬСТВО. Если функция $f(a_1, \dots, a_5) \in k'$, то ее можно представить также в виде

$$f = \sum \alpha_{i_1 \dots i_7} x_1^{i_1} x_2^{i_2} \dots x_7^{i_7}, \quad \alpha_{i_1 \dots i_7} \in k. \quad (13)$$

Из доказательства теоремы 1 следует, что автоморфизмы б) и в) приводят к перестановке корней в правой части (13), при этом замена $a_i \rightarrow -a_i$ соответствует замене $\sqrt{t} \rightarrow -\sqrt{t}$ из леммы 4. Автоморфизмы а) и г) оставляют (13) неподвижным.

Определим гомоморфизм $\varphi: S_3 \times \mathbb{Z}_2 \rightarrow \text{Aut } k'$, при котором элементам S_3 сопоставляются перестановки в), а элементу порядка 2 из $\mathbb{Z}_2$ – замена $a_1 \rightarrow -a_1$. Пусть $G = \varphi(S_3 \times \mathbb{Z}_2)$.

ЛЕММА 8. *Расширение $k \subset k'$ является расширением Галуа с группой G .*

ДОКАЗАТЕЛЬСТВО. По лемме 6 k является множеством элементов в k' , неподвижных относительно G . Остается применить известный результат из теории Галуа (см. [3; гл. VIII, § 1, теорема 2]).

ЛЕММА 9. *Группа G тривиальна.*

ДОКАЗАТЕЛЬСТВО. Предположим, что $G \neq \{e\}$, и рассмотрим башню

$$k \xrightarrow{G} k' \xrightarrow{H} k(x_1, x_2, \dots, x_7). \quad (14)$$

Оба этажа (14) являются расширениями Галуа с группами G и H . Применяя теорему 1, получаем $G \simeq S_7/H$. Нетривиальный нормальный делитель в S_7 только один – это подгруппа $S_7^{\text{чет}}$ четных перестановок, поэтому $G \simeq \mathbb{Z}_2$. В группе $S_3 \times \mathbb{Z}_2$ есть только два нормальных делителя индекса 2 – это $S_3 \times \{e\}$ и $S_3^{\text{чет}} \times \mathbb{Z}_2$. Если ядро $\ker \varphi = S_3 \times \{e\}$, то поле k' неподвижно при всех автоморфизмах, определенных перестановками переменных a_3, a_4, a_5 . Такие перестановки индуцируют всевозможные перестановки корней x_1, x_2, x_3 , оставляя на месте другие корни d -полинома. Это противоречит тому, что поле k' сохраняют только четные перестановки корней. Пусть теперь $\ker \varphi = S_3^{\text{чет}} \times \mathbb{Z}_2$. Рассмотрим расширение

$$k'(x_4, x_5, x_6, x_7) \subset k'(x_4, \dots, x_7, x_1, x_2, x_3) = k(x_4, \dots, x_7, \dots, x_3).$$

Это расширение Галуа, и его группа не может иметь порядок 6, так как тогда H содержала бы и нечетные перестановки корней x_1, x_2, x_3 . Следовательно, дискриминант полинома (4) будет полным квадратом в поле $k'(x_4, x_5, x_6, x_7)$ (см. [3; гл. VIII, § 2, пример 2]). Положим

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = \sum p_{ijkl} x_4^i x_5^j x_6^k x_7^l, \quad p_{ijkl} \in k'. \quad (15)$$

Положим еще

$$\delta' = (x_4 - x_5)(x_4 - x_6)(x_4 - x_7)(x_5 - x_6)(x_5 - x_7)(x_6 - x_7). \quad (16)$$

Заметим теперь, что правая часть в (15) – кососимметрическая форма от корней $x_4, \dots, x_7$ в том смысле, что любая четная перестановка корней сохраняет эту форму, а любая нечетная изменяет только знак. Запишем (15) в виде

$$\delta = \delta' \cdot \sum p'_{ijkl} x_4^i x_5^j x_6^k x_7^l, \quad p'_{ijkl} \in k'. \quad (17)$$

Так как δ' также кососимметрична, то второй множитель в правой части (17) – уже симметричная форма от $x_4, \dots, x_7$ и, следовательно, является рациональной над k' функцией от коэффициентов полинома (5). Напомним, что эти коэффициенты являются формальными степенными рядами от t с коэффициентами, рационально зависящими от $a_3, a_4, a_5, u = a_1^2 + a_2^2$; таков же и δ . Вычисляя δ' , получаем

$$(x_4 - x_5)(x_6 - x_7) = \sqrt{\Delta} \cdot \sqrt{\Delta'} = \sqrt{\frac{F(-\sqrt{u})F(\sqrt{u})}{u^2 P_0(-\sqrt{u})P_0(\sqrt{u})}} t(1 + f_1 t + f_2 t^2 + \dots), \quad (18)$$

где $f_i = f_i(a_3, a_4, a_5, u)$ – рациональные функции (в вычислении использовано следствие 1). Далее,

$$4(x_4 - x_6)(x_4 - x_7)(x_5 - x_6)(x_5 - x_7) = (m - m')^4 - 2(m - m')^2(\Delta + \Delta') + (\Delta - \Delta')^2, \quad (19)$$

где m и m' – коэффициенты при x в (6) и (7), а Δ и Δ' – дискриминанты этих полиномов. Таким образом, (19) также представима степенным рядом от t с рационально зависящими от a_3, a_4, a_5, u коэффициентами. Однако множитель в (18)

$$\sqrt{\frac{F(-\sqrt{u})F(\sqrt{u})}{u^2 P_0(-\sqrt{u})P_0(\sqrt{u})}}$$

не может быть так представлен, поскольку не является рациональной функцией. Этим завершается доказательство леммы 9.

СЛЕДСТВИЕ 2. *Поля k и k' совпадают.*

Завершим доказательство теоремы 2. Рассмотрим для этого башни полей

$$\begin{array}{ccccc} k & \subset & k' & \subset & k'(x_1, x_2, \dots, x_7) \\ \cap & & & & \cap \\ K & \subset & K \cdot k(x_1, \dots, x_7) & = & K(x_1, \dots, x_7), \end{array}$$

здесь $K \cdot k(x_1, \dots, x_7)$ обозначает композит полей. По теореме о композите (см. [3; гл. VIII, § 1, теорема 4]) группа Галуа поля $k'(x_1, \dots, x_7)$ над k' изоморфна группе Галуа поля $K(x_1, \dots, x_7)$ над K . По следствию 2 $k' = k$. Это заканчивает доказательство теоремы 2.

СЛЕДСТВИЕ 3. *Группа Галуа r -полинома $P_r(y)$ изоморфна S_7 . Кроме того, можно считать, что поля разложений полиномов $P_d(x)$ и $P_r(y)$ совпадают.*

Рис. 1

ДОКАЗАТЕЛЬСТВО. Пусть x_i , как и раньше, – корни $P_d(x)$. Для сокращения текста воспользуемся рис. 1.

Положим

$$y_i = \frac{a_1^2 a_2^2 x_i^2}{(x_i + a_1 + a_2)(x_i + a_1 - a_2)(x_i - a_1 + a_2)(-x_i + a_1 + a_2)}, \quad (20)$$

тогда y_i – корни полинома $P_r(y)$. Действительно, (20) – это известная формула, выражающая радиус описанной около треугольника (x_i, a_1, a_2) окружности через его стороны и площадь. Рассмотрим башню полей

$$K \overset{G}{\subset} K(y_1, \dots, y_7) = K_r \overset{H}{\subset} K(x_1, \dots, x_7) = K_d.$$

Оба ее этажа являются расширениями Галуа с группами G и H . Из теоремы 2 следует, что $G \simeq S_7/H$. В S_7 есть только один нетривиальный нормальный делитель $S_7^{\text{чет}}$, и если $H = S_7^{\text{чет}}$, то $G \simeq \mathbb{Z}_2$ и степень расширения K_r над K будет равна двум, но эта степень не может быть меньше семи – противоречие. Так как $H \simeq S_7$, то $K_r = K_d$.

СЛЕДСТВИЕ 4. Формула (20) допускает рациональное обращение, точнее, x_i рационально над K выражается через y_i .

ДОКАЗАТЕЛЬСТВО. По следствию 3 имеем $x_i = \varphi(y_1, \dots, y_i, \dots, y_7)$, где $\varphi \in K_r$. Автоморфизмы из группы Галуа поля K_r , сохраняющие y_i , оставляют на месте и x_i , следовательно, $\varphi \in K(y_i)$. Можно написать и “явную” формулу для φ . Воспользуемся для этого оператором $\mathcal{D}_x = x^2 \mathcal{D}_A + (a_1^2 - a_2^2) \mathcal{D}_S$ (см. [2; § 3, лемма 6]) и положим в нем $x = x_i$, тогда $\mathcal{D}_{x_i} \circ y_i = 0$. Запишем r -полином $P_r(y)$ по степеням y : $P_r(y) = \sum p_k(a_1, \dots, a_5) y^k$, затем положим $y = y_i$ и применим дифференцирование $\mathcal{D}_{x_i}$. Получим

$$x_i^2 = - \frac{(a_1^2 - a_2^2) \sum (\mathcal{D}_S \circ p_k) y_i^k}{\sum (\mathcal{D}_A \circ p_k) y_i^k}. \quad (21)$$

По доказанному правая часть (21) является полным квадратом в поле $K(y_i)$. Остается извлечь квадратный корень.

СЛЕДСТВИЕ 5. *Все пять d -полиномов 5-угольников имеют изоморфные группы Галуа, и можно считать, что поля разложений этих полиномов над K совпадают.*

ДОКАЗАТЕЛЬСТВО сразу вытекает из следствия 3.

Как и в следствии 4, здесь тоже можно указать явные формулы для рациональных выражений одних корней через другие. Например, для выражения x_i через x'_i достаточно заменить в (21) коэффициенты r -полинома на коэффициенты d -полинома для x'_i . Опуская элементарные выкладки, приведем результат:

$$\begin{aligned} x_i &= -\frac{(x'_i{}^3 - (a_1^2 + a_2^2 + a_3^2)x'_i - 2a_1a_2a_3)a_4a_5}{(x'_ia_1 + a_2a_3)(x'^2_i - a_4^2 - a_5^2)}, \\ x'_i &= -\frac{(x_i^3 - (a_3^2 + a_4^2 + a_5^2)x_i - 2a_3a_4a_5)a_1a_2}{(x_ia_3 + a_4a_5)(x_i^2 - a_1^2 - a_2^2)}. \end{aligned}$$

СЛЕДСТВИЕ 6. *Группа Галуа полинома $P_S(z)$ изоморфна S_7 , и поля разложений $K_S = K(z_1, \dots, z_7)$ и K_d можно считать совпадающими.*

ДОКАЗАТЕЛЬСТВО повторяет доказательство следствия 3, нужно только установить включение $K_S \subset K_d$. Оно вытекает из формулы

$$\begin{aligned} 16z_i &= 16(S_{4i} \pm S_{3i})^2 = (x_i + a_1 + a_2)(x_i + a_1 - a_2)(x_i - a_1 + a_2)(-x_i + a_1 + a_2) \\ &\quad + (-x_i + a_3 + a_4 + a_5)(x_i - a_3 + a_4 + a_5)(x_i + a_3 - a_4 + a_5) \\ &\quad \times (x_i + a_3 + a_4 - a_5) \pm 2 \frac{a_1a_2(x_ia_3 + a_4a_5)x'_i}{y_i}. \end{aligned}$$

Геометрический смысл этой формулы простой: площадь 5-угольника является суммой или разностью площадей (знак зависит от вида 5-угольника, как именно — здесь неважно) треугольника (x_i, a_1, a_2) и четырехугольника (x_i, a_3, a_4, a_5) .

С точки зрения элементарной геометрии наши результаты можно сформулировать так:

ГЕОМЕТРИЧЕСКАЯ ТЕОРЕМА. *Любая из величин — квадрат площади, квадрат радиуса описанной окружности или любая диагональ вписанного в окружность 5-угольника является рациональной функцией любой другой из этих величин и ребер 5-угольника. При этом вид этой функции не зависит от самого 5-угольника (речь идет, конечно, о многоугольниках общего положения; для вырожденных, например с кратными ребрами, формулы также могут вырождаться).*

ЗАМЕЧАНИЕ. Упомянутая во введении алгебра Ли порождается операторами $\mathcal{D}_x$ из доказательства следствия 4, когда x пробегает все корни всех d -полиномов 5-угольника.

В завершение статьи вычислим группы Галуа r - и S -полиномов $P_r(x^2)$ и $P_S(x^2)$, рассматривая их уже как полиномы от x , а не от x^2 .

ТЕОРЕМА 3. Группы Галуа полиномов $P_r(x^2)$, $P_S(x^2)$ изоморфны прямому произведению $S_7 \times \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_7$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим только r -полином, так как для S -полинома доказательство аналогично. Как обычно, понадобятся некоторые леммы.

ЛЕММА 10. Пусть Δ_d – дискриминант d -полинома (1). Тогда разложение выражения $\delta_d = \sqrt{\Delta_d}$ в формальный степенной ряд по t имеет вид

$$\delta_d = \sqrt{\frac{F(-\sqrt{u})F(\sqrt{u})}{u^2 P_0(-\sqrt{u})P_0(\sqrt{u})}} \sum_{k=-l}^{\infty} c_k t^k,$$

где $c_k = c_k(v_1, v_2, v_3, u)$ – рациональные функции.

ДОКАЗАТЕЛЬСТВО. Сначала заметим, что δ_d можно представить в виде

$$\delta_d = \delta \cdot \delta' \cdot \tilde{Q}(x_1) \cdot \tilde{Q}(x_2) \cdot \tilde{Q}(x_3),$$

где δ и δ' определены формулами (15) и (16), а произведение $\prod \tilde{Q}(x_i)$ – это результат полиномов (11) и (12) и, следовательно, является симметрической функцией корней $x_1, x_2, \dots, x_7$. Такая функция обязана принадлежать полю $k \subset K$. Остается воспользоваться результатом вычисления δ и δ' из леммы 9 (см. формулу (18)).

ЛЕММА 11. Положим

$$A = \prod_{i=1}^7 (a_1 + a_2 - x_i)(a_1 - a_2 + x_i)(-a_1 + a_2 + x_i)(a_1 + a_2 + x_i). \quad (22)$$

Тогда

- а) $A \in k \subset K$,
- б) разложение $\sqrt{A}$ в формальный степенной ряд по t имеет вид

$$t^2 \sum_{k=0}^{\infty} b_k t^k,$$

- где $b_k = b_k(v_1, v_2, v_3, u)$ – рациональные функции и $b_0 \neq 0$ в k ,
- в) A не является квадратом в K .

ДОКАЗАТЕЛЬСТВО. а) Очевидно, что A – симметричная форма от $x_1, \dots, x_7$, а кроме того, A выдерживает перестановки переменных a_1 и a_2 и замены знаков у этих переменных. Следовательно, A является рациональной функцией от v_1, v_2, v_3, u, t .

б) Заметим, что справедливо равенство

$$-A = P_d(a_1 + a_2)P_d(-a_1 - a_2)P_d(a_2 - a_1)P_d(a_1 - a_2). \quad (23)$$

Из вида (1) полинома P_d заключаем, что $Q_0(\pm(a_1 + a_2)) = Q_0(\pm(a_1 - a_2))$, поэтому выражению (23) можно придать вид

$$-\frac{A}{t^4} = (4P_0(a_1 + a_2) + F(a_1 + a_2))(4P_0(-a_1 - a_2) + F(-a_1 - a_2)) \\ \times (4P_0(a_1 - a_2) + F(a_1 - a_2))(4P_0(a_2 - a_1) + F(a_2 - a_1)). \quad (24)$$

Если положить в правой части (24) $a_1 = 0$, получим произведение

$$[4P_0(a_2) + F(a_2)]^2 [4P_0(-a_2) + F(-a_2)]^2 = g^2(v_1, v_2, v_3, a_2). \quad (25)$$

Коэффициент при нулевой степени t для $-A/t^4$ получается подстановкой в (25) переменной $u = a_1^2 + a_2^2$ вместо a_2^2 . Итак, для $\sqrt{A}$ имеем формулу

$$\sqrt{A} = g(v_1, v_2, v_3, u) t^2 \sqrt{1 + \sum_{k=1}^{\infty} b'_k t^k}.$$

Остается применить биномиальное разложение для радикала в правой части.

в) Приведем явную формулу для A , опуская промежуточные выкладки:

$$A = (u^2 - 4t)^2 \frac{t^4}{v_3^4} (a_1 + a_2 + \dots + a_5) \prod_{i=1}^5 (a_1 + \dots - a_i + \dots + a_5) \\ \times \prod_{i_1 < i_2} (a_1 + \dots - a_{i_1} + \dots - a_{i_2} + \dots + a_5). \quad (26)$$

Перейдем к доказательству собственно теоремы. Покажем сначала, что $\sqrt{y_i}$ не принадлежит полю разложения K_r полинома $P_r(y)$ ни при каком $i = 1, 2, \dots, 7$. Действительно, пусть $\sqrt{y_1} \in K_r$, тогда из теоремы 2 следует, что $\sqrt{y_i} \in K_r$ при любом i . Полагая $\sqrt{y_i} = \varphi_i(y_1, \dots, y_7)$, перемножим все эти равенства:

$$\sqrt{y_1} \sqrt{y_2} \dots \sqrt{y_7} = \varphi(y_1, y_2, \dots, y_7). \quad (27)$$

Ясно, что $\varphi(y_1, \dots, y_7)$ — либо симметрическая, либо кососимметрическая функция корней $y_1, \dots, y_7$. Рассмотрим обе возможности. В первом случае $\varphi \in K$. Заменив y_i через x_i с помощью формулы (20), приходим к выражению

$$y_1 y_2 \dots y_7 = \frac{t^7 x_1^2 x_2^2 \dots x_7^2}{A} = \varphi^2, \quad t = a_1^2 a_2^2. \quad (28)$$

Числитель в левой части является квадратом в K , а знаменатель по лемме 11 не является квадратом — противоречие.

Рассмотрим теперь второй случай. Для этого запишем формулу (27) в виде

$$\sqrt{y_1} \sqrt{y_2} \dots \sqrt{y_7} = \delta_d \psi(y_1, y_2, \dots, y_7). \quad (29)$$

Ясно, что ψ – теперь уже симметрическая функция корней $y_1, \dots, y_7$, а следовательно, и корней $x_1, \dots, x_7$ полинома (1). Поэтому $\psi \in K$. Из (29) получаем, что δ_d представляется степенным рядом по t с рациональными коэффициентами, зависящими от a_3, a_4, a_5, u , но из леммы 10 видно, что δ_d так представлен быть не может.

Рассмотрим теперь поле $K_r(\sqrt{y_1})$ и покажем, что $\sqrt{y_i}$ не принадлежит этому полю ни при каком i . Пусть это не так и, скажем, $\sqrt{y_2} \in K_r(\sqrt{y_1})$. Тогда $\sqrt{y_2} = a + b\sqrt{y_1}$, где $a, b \in K_r$. Согласно доказанному $b \neq 0$ и, возводя $\sqrt{y_2}$ в квадрат, имеем $y_2 = a^2 + 2ab\sqrt{y_1} + b^2y_1$, откуда следует, что $a = 0$. Итак,

$$\sqrt{y_1} \sqrt{y_2} = \varphi(y_1, y_2, \dots, y_7). \quad (30)$$

Ясно, что φ является либо симметрической, либо кососимметрической функцией корней $y_3, \dots, y_7$. Рассмотрим обе возможности. Пусть φ симметрическая. Тогда $\varphi \in K_r(y_1, y_2)$. Положим ребро a_5 равным нулю. Тогда P_r делится на полиномы P_r^+ и P_r^- для 4-угольника с ребрами a_1, a_2, a_3, a_4 (см. [2; лемма 21]). Формула (30) останется справедливой, если считать, что один из корней будет корнем P_r^+ , а другой – корнем P_r^- . Но в этом случае правая часть в (30) будет рациональной функцией переменных $a_1, \dots, a_4$, а левая – нет (см. [2; формула (4) и комментариев к ней]). Пусть теперь φ кососимметрична. Представим (30) в виде

$$\sqrt{y_1} \sqrt{y_2} = \delta_d \psi(y_1, y_2, \dots, y_7).$$

Здесь ψ уже симметрична по $y_3, \dots, y_7$ и, следовательно $\psi \in K(y_1, y_2)$. Переходим к корням x_i , тогда

$$\frac{tx_1x_2}{\sqrt{4t - (x_1^2 - u)^2} \sqrt{4t - (x_2^2 - u)^2}} = \delta_d \theta(x_1, x_2). \quad (31)$$

Оба корня x_1 и x_2 являются формальными рядами по t с рациональными коэффициентами. Коэффициент при нулевой степени t в выражении $4t - (x_1^2 - u)^2$ равен $(a_3^2 a_4^2 / a_5^2 - u)^2$, тот же коэффициент для $4t - (x_2^2 - u)^2$ равен $(a_3^2 a_5^2 / a_4^2 - u)^2$. Следовательно, квадратные корни, стоящие в знаменателе в (31), также выражаются степенными рядами по t с рациональными коэффициентами. Но правая часть в (31) по лемме 10 не может быть так представлена. Итак, $\sqrt{y_2} \notin K_r(\sqrt{y_1})$. Ясно, что $\sqrt{y_1}$ и $\sqrt{y_2}$ можно заменить любыми другими корнями $\sqrt{y_i}$ и $\sqrt{y_j}$, $i \neq j$.

Пусть уже доказаны строгие включения

$$K_r(\sqrt{y_1}, \dots, \sqrt{y_{k-2}}) \subset K_r(\sqrt{y_1}, \dots, \sqrt{y_{k-1}}).$$

Предположим, что $\sqrt{y_k} \in K_r(\sqrt{y_1}, \dots, \sqrt{y_{k-1}})$, тогда

$$\sqrt{y_k} = a + b\sqrt{y_{k-1}}, \quad b \neq 0,$$

где $a, b \in K_r(\sqrt{y_1}, \dots, \sqrt{y_{k-2}})$. Возводя в квадрат последнее равенство, найдем, как и раньше, что $a = 0$. По индукции заключаем, что имеет место формула, подобная формуле (30):

$$\sqrt{y_1} \sqrt{y_2} \cdots \sqrt{y_{k-1}} \sqrt{y_k} = \varphi(y_1, \dots, y_7). \quad (32)$$

Если $k < 7$, то перестановкой можно получить

$$\sqrt{y_1} \sqrt{y_2} \cdots \sqrt{y_{k-1}} \sqrt{y_{k+1}} = \tilde{\varphi}(y_1, \dots, y_7). \quad (33)$$

Перемножая соотношения (32) и (33), найдем, что $\sqrt{y_k} \sqrt{y_{k+1}} \in K_r$ — это противоречит уже доказанному. Если же $k = 7$, то мы оказываемся в уже рассмотренной ситуации формулы (27). Следовательно, степень расширения в каждом этаже башни полей

$$K_r \subset K_r(\sqrt{y_1}) \subset K_r(\sqrt{y_1}, \sqrt{y_2}) \subset \cdots \subset K_r(\sqrt{y_1}, \dots, \sqrt{y_7})$$

будет равна двум, и теорема 3 доказана.

Список литературы

1. *Сабитов И. Х.* Обобщенная формула Герона–Тарталья и некоторые ее следствия // Матем. сб. 1998. Т. 189. № 10. С. 105–134.
2. *Варфоломеев В. В.* Вписанные многоугольники и полиномы Герона // Матем. сб. 2003. Т. 194. № 3. С. 3–24.
3. *Ленг С.* Алгебра. М.: Мир, 1968.

Московский институт радиотехники,
электроники и автоматики

Поступила в редакцию
09.06.2003