Алгебра 6
16.10.97

Симметрические функции

Часть 1. Разрешимые и неразрешимые группы.

Предложение. Группа $\mathfrak{A}_7$ неразрешима.

Пусть $a = (123)$, $b = (14567) \implies ab = (1456723) \implies a^3 = b^5 = (ab)^7 = 1$. Если бы группа $\mathfrak{A}_7$ была разрешима, то и подгруппа G, порожденная a, b тоже была бы разрешима, а тогда у нее была бы нетривиальная абелева факторгруппа G/H. Но в абелевой группе из равенства $\overline{a}^3 = \overline{b}^5 = (\overline{ab})^7 = 1$ вытекает $\overline{a} = \overline{b} = 1$. Противоречие. □

Предложение. Если $\#G = p^n$, то G разрешима.

Лемма. Центр G (обозначается ZG) нетривиален.

Рассмотрим разбиение G на классы сопряженности $G = \bigsqcup C_i$, где C_i являются классами эквивалентности, задаваемыми отношением $a \sim b \iff \exists c \in G \mid a = cbc^{-1}$.

Легко видеть, что $c_1ac_1^{-1} = c_2ac_2^{-1}$ тогда и только тогда, когда $c = c_1c_2^{-1}$ коммутирует с a. Пусть $H = \{\, c \mid ca = ac \,\}$. Тогда существует взаимно-однозначное соответствие между элементами класса сопряженности, содержащего a, и G/H, а именно, $c_1ac_1^{-1} \leftrightarrow \overline{c}_1$. Поэтому порядок каждого класса сопряженности делит порядок группы. Класс $\{\, a \,\}$ состоит из одного элемента тогда и только тогда, когда a коммутирует со всеми элементами G, т.е. когда $a \in ZG$.

Если бы центр G был тривиален, то единственным классом сопряженности, содержащим один элемент, был бы класс $\{1\}$, а порядки всех остальных классов делились бы на p, чего не может быть, так как в сумме они дают p^n. Лемма доказана. □

Теперь доказательство можно вести по индукции. В самом деле, если $\#ZG = \#G$, то G абелева и все доказано. Если же $\#ZG < \#G$, то $\#ZG = p^k$, $0 < k < n$ и $\#G/ZG = p^{n-k}$. По предположению индукции ZG и G/ZG разрешимы, следовательно, G разрешима. □

Следствие. Если $K : L$ — нормальное расширение порядка 2^n, то K поликвадратично.

Часть 2. Симметрические функции.

Пусть есть поле L и неопределенные переменные $u_1, \ldots, u_n$. Тогда поле $L(u_1, \ldots, u_n)$ — это поле рациональных функций от неопределенных переменных $u_1, \ldots, u_n$:

$$F = L(u_1, \ldots, u_n) = \left\{ \frac{P(u_1, \ldots, u_n)}{Q(u_1, \ldots, u_n)} \;\Big|\; P, Q \in L[u_1, \ldots, u_n] \right\}$$

Рассмотрим уравнение $z^n + u_1 z^{n-1} + \ldots + u_n = 0$ над полем F. Обозначим его корни через $\nu_1, \nu_2, \ldots, \nu_n$ и рассмотрим минимальное поле разложения $F(\nu_1, \nu_2, \ldots, \nu_n)$.

Теорема. $\operatorname{Gal}(F(\nu_1,\nu_2,\dots,\nu_n):F)=\mathfrak{S}_n$.

Доказательство. Положим $\mathcal{F}:=L(x_1,\dots,x_n)$, где $x_1,\dots,x_n$ — свободные переменные. Рассмотрим над $\mathcal{F}$ уравнение

$$(z-x_1)\cdot\ldots\cdot(z-x_n)=0 \Leftrightarrow z^n-\sigma_1(x)z^{n-1}+\ldots\pm\sigma_n(x)=0 \qquad (*)$$

В поле $\mathcal{F}$ действует группа $\mathfrak{S}_n=G$, переставляя x_i. Она сохраняет элементарные симметрические функции σ (симметрические функции являются элементами поля $\mathcal{F}$, а не функциями на нем): $\mathcal{F}^G\ni\sigma_1(x),\dots,\sigma_n(x)$.

Лемма о симметрических функциях. Любая симметрическая функция (симметрический многочлен) однозначно выражается через элементарные. Иными словами,

$$\mathcal{F}^G=L(\sigma_1,\dots,\sigma_n)$$

Доказательство. Очевидно,

$$\mathcal{F}\overset{n!}{\supset}\mathcal{F}^G\supset L(\sigma_1,\dots,\sigma_n)\quad\Longrightarrow[\mathcal{F}:L(\sigma_1,\dots,\sigma_n)]\geqslant[\mathcal{F}:\mathcal{F}^G]=n!$$

Поле $\mathcal{F}$ является минимальным полем разложения многочлена $(*)$ над $L(\sigma_1,\dots,\sigma_n)$, то есть оно получается последовательным присоединением $x_1,\dots,x_n$ к $L(\sigma_1,\dots,\sigma_n)$, откуда

$$[\mathcal{F}:L(\sigma_1,\dots,\sigma_n)]\leqslant n!\quad\Longrightarrow\mathcal{F}^G=L(\sigma_1,\dots,\sigma_n).$$

Значит, выражение любой симметрической функции через элементарные существует.

Если бы какая-то симметрическая функция двумя способами выражалась через элементарные, то между $\sigma_1,\dots,\sigma_n$ было бы алгебраическое соотношение $f(\sigma_1,\dots,\sigma_n)=0$. Рассмотрим отображение $L[x_1,\dots,x_n]\to F(\nu_1,\dots,\nu_n)$, $x_i\mapsto\nu_i$, переводящее σ_i в $(-1)^iu_i$. Получаем $f(-u_1,\dots,\pm u_n)=0$, откуда $f\equiv 0$, так как u_i — свободные переменные.

Лемма доказана. $\square$

Отображение из предыдущего абзаца задает коммутативный квадрат

$$\begin{tikzcd}
F(\nu_1,\dots,\nu_n) & F \arrow[l, hook', "\supset"'] \\
\mathcal{F} \arrow[u, "\wr"'] & \mathcal{F}^G \arrow[l, hook', "\supset"'] \arrow[u, "\wr"']
\end{tikzcd}$$

откуда видно, что $\operatorname{Gal}(F(\nu_1,\dots,\nu_n):F)=\operatorname{Gal}(\mathcal{F}:\mathcal{F}^G)=G=\mathfrak{S}_n$. Доказательство теоремы окончено. $\square$

Следствие. Если группа $\mathfrak{S}_n$ неразрешима, то не существует универсальной формулы, выражающей корни уравнения $x^n+u_1x^{n-1}+\ldots+u_n=0$ в радикалах через его коэффициенты.

Часть 3. Результант и дискриминант.

Пусть

$$f(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_n = a_0(z - x_1) \cdot \ldots \cdot (z - x_n)$$
$$g(z) = b_0 z^m + b_1 z^{m-1} + \ldots + a_m = b_0(z - y_1) \cdot \ldots \cdot (z - y_m)$$

Тогда по определению дискриминант f

$$D(f) := a_0^{2n-2} \prod_{i<j} (x_i - x_j)^2,$$

а результант f и g

$$R(f, g) := a_0^m b_0^n \prod_{i,j} (x_i - y_j).$$

Таким образом, дискриминант равен нулю тогда и только тогда, когда у многочлена f есть кратные корни, а результант равен нулю тогда и только тогда, когда у f и g есть общие корни. Дискриминант и результант — это симметрические многочлены от корней, поэтому они должны выражаться через коэффициенты f и g.

Найдем явную формулу для результанта.

$R(f, g) = 0 \Leftrightarrow$ у f и g есть общий делитель $\Leftrightarrow\ \exists\, h(z), k(z) \mid hf = gk,\ \deg h < m,\ \deg k < n$. Пусть

$$h = c_0 z^{m-1} + c_1 z^{m-2} + \ldots + c_{m-1},\ \ k = d_0 z^{n-1} + d_1 z^{n-2} + \ldots + d_{n-1}$$

Тогда

$$\begin{array}{ccl} hf & = & (a_0 z^n + a_1 z^{n-1} + \ldots)(c_0 z^{m-1} + c_1 z^{m-2} + \ldots) \\ \| & & \\ gk & = & (b_0 z^m + b_1 z^{m-1} + \ldots)(d_0 z^{n-1} + d_1 z^{n-2} + \ldots) \end{array}$$
$$\Updownarrow$$
$$\left\{ \begin{array}{rcl} a_0 c_0 & = & b_0 d_0 \\ a_0 c_1 + c_0 a_1 & = & b_0 d_1 + b_1 d_0 \\ a_0 c_2 + a_1 c_1 + a_2 c_0 & = & b_0 d_2 + b_1 d_1 + b_2 d_0 \\ \multicolumn{3}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \end{array} \right.$$

Мы получили систему $m + n$ линейных уравнений на неизвестные $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{n-1}$, которая, как известно, имеет ненулевое решение, если и только если ее определитель равен нулю. Транспонировав матрицу и поменяв знаки у части столбцов, получаем

$$R(f, g) = 0 \quad \Longleftrightarrow \quad \left| \begin{array}{ccccccc} a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_n & \ldots & 0 \\ \multicolumn{7}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_m & 0 & \ldots & 0 \\ \multicolumn{7}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_m \end{array} \right| = \det A = 0$$

Утверждение. $\det A = R(f, g)$.

В самом деле, как легко видеть, степени $\det A$ и $R(f,g)$ как многочленов от x_i, y_j равны, кроме того, у них совпадают множества корней. Поэтому они могут отличаться только умножением на некоторое выражение от a_0, b_0.

Но в $\det A$ входит диагональный член $a_0^m b_m^n$, а в $R(f,g)$ он тоже присутсвует:

$$R(f,g) = a_0^m \prod_i (b_0 \prod_j (x_i - y_j)) = a_0^m \prod_i g(x_i) = a_0^m (\ldots + b_m^n)$$

Утверждение доказано. $\square$

Утверждение. $R(f,f') = \pm a_0 D(f)$.

Как мы только что видели, $R(f,f') = a_0^{n-1} \prod_i f'(x_i)$. Вычисляя производную произведения $f(z) = a_0 \prod_i (z - x_i)$, убеждаемся, что $a_0^{n-1} \prod_i f'(x_i) = a_0^{2n-1} \prod_{i \neq k} (x_i - x_k)$. $\square$.

Кстати, неудивительно, что $R(f,f')$ делится на a_0: первый столбец матрицы A делится на a_0.

Замечание. Если придать каждой из переменных a_i и b_i вес i, то вес $R(f,g)$ будет в точности равен mn — это степень результанта как многочлена от x_i, y_j. Если же придать каждой из переменных a_i, b_i вес 1, то вес (степень) результанта по a будет равен m, а степень по b будет равна n.

Теорема Безу. Две алгебраические кривые на плоскости

$$\begin{aligned} f(x,y) &= 0, \qquad \deg f = n \\ g(x,y) &= 0, \qquad \deg g = m, \end{aligned}$$

имеющие конечное пересечение, имеют не более mn общих точек.

Доказательство. Выберем оси координат t, u так, чтобы все точки пересечения проецировались на разные точки оси абсцисс. При этом степени наших кривых не изменятся.

Рассмотрим f и g как многочлены над кольцом $\mathbb{C}[t]$. Тогда $R(f,g) \in \mathbb{C}[t]$. Если при некотором t_0 многочлены имеют общий корень u_0, то $R(f,g) = 0$ и $R(f,g)$ имеет корень t_0, и наоборот. Значит, число точек пересечения не больше $\deg_t R(f,g)$.

Пусть

$$f(t,u) = a_0(t) u^n + \ldots + a_n(t)$$

Так как $\deg f = n$, то $\deg_t a_i(t) \leqslant i$. Поэтому, в силу последнего замечания, $\deg_t R(f,g) \leqslant mn$.
$\square$

Замечание. Из доказательства видно, что если у наших кривых больше mn общих точек, то $R(f,g) \equiv 0$, а стало быть, при любом значении t наши многочлены имеют общий корень, т.е. пересечение кривых сюръективно проецируется на ось t. Это означает, что у наших кривых есть общая компонента.