Разрешимость уравнений в радикалах

При помощи теории Галуа можно дать ответ на вопрос о том, когда корни многочлена могут быть выражены в радикалах. Начнём с простейшего хорошо известного случая квадратных уравнений.

Решим уравнение $x^2 + px + q = 0$, где p, q лежат в поле k характеристики, не равной 2. Пусть α, β – корни, а $K = \mathsf{k}[\alpha] = \mathsf{k}[\alpha, \beta]$ – поле, порождённое корнями. Это нормальное сепарабельное расширение поля k, его группа Галуа переставляет корни и потому изоморфна $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ или тривиальна. Будем считать, что $G = Gal(K, \mathsf{k}) \cong \mathbb{Z}/2\mathbb{Z}$. Имеется действие G на k-векторном пространстве K.

Для любого представления группы $\mathbb{Z}/2\mathbb{Z} = \langle 1, \sigma\rangle$ в векторном пространстве V имеем разложение $V = V_0 \oplus V_1$, где σ на V_0 действует тривиально, а на V_1 – умножением на -1. Для вектора $v \in V$ компоненты $v_i \in V_i$ имеют вид $v_0 = \frac{v+\sigma(v)}{2}$ и $v_1 = \frac{v-\sigma(v)}{2}$.

Возвращаясь к квадратному уравнению, получаем разложение $K = K_0 \oplus K_1$ для действия группы Галуа на поле K. При этом умножение в K согласовано с разложением: $K_0 \cdot K_0 \subset K_0$, $K_0 \cdot K_1 \subset K_1$, $K_1 \cdot K_1 \subset K_0$. По основной теореме теории Галуа $K_0 = K^G = \mathsf{k}$.

Для того, чтобы найти корень α, отыщем его чётную и нечётную части α_0 и α_1. По теореме Виета, $\alpha_0 = \frac{\alpha+\sigma(\alpha)}{2} = \frac{\alpha+\beta}{2} = \frac{-p}{2}$. Выразить α_1 многочленом через p и q не удастся, так как $\alpha_1 \in K_1$. Однако $\alpha_1^2 \in K_0 = \mathsf{k}$, и его можно выразить: $\alpha_1^2 = (\frac{\alpha-\sigma(\alpha)}{2})^2 = \frac{(\alpha-\beta)^2}{4} = \frac{(\alpha+\beta)^2-4\alpha\beta}{4} = \frac{p^2-4q}{4}$ по теореме Виета. Извлекая корень и правильно выбирая знак, получаем:

$$\alpha, \beta = \frac{-p}{2} \pm \sqrt{\frac{p^2-4q}{4}}.$$

Мы говорим, что элемент $\alpha \in \bar{\mathsf{k}}$ *выразим в радикалах* (над k), если существует конечная формула из знаков арифметических действий, знаков радикалов разных степеней и элементов поля k, выражающая α (при правильном выборе значений радикалов). На языке полей это означает, что имеется последовательность расширений полей $\mathsf{k} = K_0 \subset K_1 \subset \ldots \subset K_n$ такая, что $\alpha \in K_n$ и каждое поле K_i получается присоединением к K_{i-1} корня некоторой степени из некоторого элемента $a_i \in K_{i-1}$.

Оказывается, что такая башня полей на языке групп отвечает последовательности подгрупп группы Галуа $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$, в которой все факторгруппы G_i/G_{i+1} циклические. Такие группы G называются разрешимыми. Тем самым, вопрос о разрешимости уравнения в радикалах сводится к вопросу о разрешимости группы Галуа этого уравнения. Деталям этого соответствия и посвящена сегодняшняя лекция.

Определение 1. (Конечная) группа G называется *разрешимой*, если существует последовательность подгрупп $G = G_0 \supset G_1 \supset \ldots \supset G_{m-1} \supset G_m = \{e\}$ (называемая *фильтрацией*) такая, что при всех i подгруппа G_{i+1} нормальна в G_i и факторгруппа G_i/G_{i+1} абелева.

Замечание 2. Разрешимость конечной группы равносильна существованию фильтрации с циклическими (а не просто абелевыми) факторгруппами. Действительно, пусть имеется фильтрация $\ldots G_i \supset G_{i+1} \supset \ldots$ с абелевым фактором G_i/G_{i+1}. Её можно уплотнить до фильтрации с циклическими факторами следующим образом. Пусть $A = G_i/G_{i+1}$ – конечная абелева группа, она изоморфна прямой сумме циклических. Поэтому для A существует фильтрация $A = A_0 \supset \ldots \supset A_m = \{e\}$ с циклическими факторами A_j/A_{j+1}. Пусть $p\colon G_i \to A$ – отображение факторизации, тогда последовательность $G_i = p^{-1}(A_0) \supset p^{-1}(A_1) \supset \ldots \supset p^{-1}(A_m) = G_{i+1}$ будет уплотнением исходной фильтрации и факторы $p^{-1}(A_j)/p^{-1}(A_{j+1}) \cong A_j/A_{j+1}$ – циклические.

Нам понадобятся следующие свойства:

Предложение 3. *1. Подгруппа и факторгруппа разрешимой группы разрешима.*

2. Если $H \subset G$ – нормальная подгруппа и группы H и G/H разрешимы, то и G разрешима.

Доказательство. 1. Пусть $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ – фильтрация с абелевыми факторами, а $H \subset G$ – подгруппа. Тогда фильтрация $H_i = H \cap G_i$ будет искомой для H, так как факторы $(H \cap G_i)/(H \cap G_{i+1}) \subset G_i/G_{i+1}$ абелевы. Если $H \lhd G$ и $p\colon G \to G/H$ – проекция на фактор, то фильтрация $p(G_i)$ – искомая для G/H, так как $p(G_i)/p(G_{i+1})$ – факторгруппа G_i/G_{i+1} и потому абелева.

2. Если $H = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$ и $G/H = \bar{G}_0 \supset \bar{G}_1 \supset \ldots \supset \bar{G}_l = \{e\}$ – фильтрации с абелевыми факторами, то в качестве фильтрации с абелевыми факторами для G можно взять

$$G = p^{-1}(\bar{G}_0) \supset p^{-1}(\bar{G}_1) \supset \ldots \supset p^{-1}(\bar{G}_l) = H = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\},$$

где $p\colon G \to G/H$ – проекция на факторгруппу. □

Определение разрешимой группы неконструктивно, изложим критерий, позволяющий проверять разрешимость на практике. Напомним, что коммутантом группы G называется подгруппа $[G, G] \subset G$, порождённая всеми элементами вида $ghg^{-1}h^{-1}$. Это нормальная подгруппа, фактор по ней абелев. Причём коммутант – наименьшая подгруппа с такими свойствами: если $H \lhd G$ и факторгруппа G/H абелева, то $[G, G] \subset H$. Определим производный ряд группы: $G' = [G, G]$, $G'' = [G', G']$, …, $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$,…

Предложение 4. *Группа разрешима тогда и только тогда, когда найдётся N, для которого $G^{(N)} = \{e\}$.*

Доказательство. Очевидно, факторгруппы $G^{(i)}/G^{(i+1)}$ абелевы, и если $G^{(N)} = \{e\}$, то производный ряд образует нужную фильтрацию и G разрешима.

Обратно, покажем, что производный ряд убывает быстрее всех фильтраций с абелевыми факторами. Пусть $G = G_0 \supset G_1 \supset G_2 \supset \ldots$ – фильтрация с абелевыми факторами. Тогда G/G_1 – абелева группа, и значит $G_1 \supset G'$. Далее: так как группа G_1/G_2 абелева, получаем, что $G_2 \supset G_1' \supset G''$. Продолжая, по индукции доказываем, что $G_i \supset G^{(i)}$. Если $G_m = \{e\}$, то и $G^{(m)} = \{e\}$. □

Пример 5. Пусть $G = S_4$, тогда $G' = S_4' = A_4$, $G'' = A_4' = V_4$, $G''' = V_4' = \{e\}$. Значит, группа S_4 разрешима.

Пример 6. Пусть $G = S_n, n \geqslant 5$, тогда $G' = S_n' = A_n$, $G'' = A_n' = A_n$, и далее все $G^{(k)} = A_n$. Значит, группа S_n не разрешима при $n \geqslant 5$.

Эти два примера являются причиной того, что уравнения степени $\leqslant 4$ разрешимы в радикалах, а уравнения степени $\geqslant 5$ – как правило, нет.

Определение 7. Расширение полей $\mathsf{k} \subset K$ называется *абелевым* (соотв. *циклическим*), если оно является расширением Галуа и группа $Gal(K, \mathsf{k})$ абелева (соотв. циклическая).

Связь между разрешимыми группами и разрешимыми уравнениям основана на том факте, что расширения полей, полученные присоединением радикала, соответствуют циклическим группам Галуа. Для того, чтобы этот факт был верен, необходимо, чтобы в исходном поле было достаточно много корней из единицы.

Предложение 8. *Пусть* k *– поле характеристики* p *и число* n *не делится на* p*. Предположим, что в* k *содержится первообразный корень из единицы степени* n*, а также элемент* a*. Положим* $K = \mathsf{k}[\sqrt[n]{a}]$*. Тогда* K *– расширение Галуа поля* k*, и группа Галуа* $Gal(K, \mathsf{k}) \cong \mathbb{Z}/m\mathbb{Z}$*, где* $n = md$*. При этом* $\sqrt[d]{a} = b \in \mathsf{k}$ *и* $K = \mathsf{k}[\sqrt[m]{b}]$*.*

Доказательство. Обозначим первообразный корень из единицы в k степени n через ξ_n. Все корни из a степени n получаются из одного корня умножением на корни из единицы, которые все лежат в k. Поэтому K содержит все корни многочлена $x^n - a$ и является его полем разложения. Этот многочлен взаимно прост со своей производной nx^{n-1}, поэтому он сепарабелен и значит, K/k – расширение Галуа. Пусть $\sigma \in G = Gal(K, \mathsf{k})$ – автоморфизм, он однозначно задаётся образом $\sqrt[n]{a}$. Этот образ – также корень n-й степени из a, поэтому $\sigma(\sqrt[n]{a}) = \xi_n^s \cdot \sqrt[n]{a}$ для некоторого s. Так как корень ξ_n первообразный, s определено однозначно по модулю n. Получаем вложение $G \to \mathbb{Z}/n\mathbb{Z}\colon \sigma \mapsto s$. Его образ – подгруппа в $\mathbb{Z}/n\mathbb{Z}$, она изоморфна $\mathbb{Z}/m\mathbb{Z}$ для некоторого m – делителя n, пусть $n = md$. Тогда орбита $\sqrt[n]{a}$ относительно G состоит из $\sqrt[n]{a}$, $\sqrt[n]{a}\cdot\xi_n^d$, $\sqrt[n]{a}\cdot\xi_n^{2d}, \ldots, \sqrt[n]{a}\cdot\xi_n^{(m-1)d}$. Значит, произведение этих элементов лежит в $K^G = \mathsf{k}$. Так как $\xi_n \in \mathsf{k}$, получаем, что $b = \sqrt[n]{a}^m \in \mathsf{k}$. Отсюда $b^d = a$, $\sqrt[n]{a} = \sqrt[m]{b}$ и $K = \mathsf{k}[\sqrt[m]{b}]$. □

Для доказательства аналогичного предложения в другую сторону нам понадобится вспомнить теорию представлений. Пусть k – поле характеристики p и n не делится на p. Предположим, что в k содержится первообразный корень из единицы степени n. Мы покажем, что тогда все представления группы $\mathbb{Z}/n\mathbb{Z}$ над k разбиваются в прямую сумму одномерных. Это известно в случае алгебраически замкнутого поля, нам же понадобится для незамкнутого поля.

Фиксируем образующую σ группы $\mathbb{Z}/n\mathbb{Z}$, обозначим через $\xi_n \in \mathsf{k}$ первообразный корень из единицы степени n. Пусть $\rho_i\colon \mathbb{Z}/n\mathbb{Z} \to \mathsf{k}^*$ – одномерное представление, которое на σ равно ξ_n^i, $i = 0 \ldots n-1$.

Лемма 9. *Любое представление* $\mathbb{Z}/n\mathbb{Z}$ *над полем* k *разлагается в прямую сумму представлений, изоморфных* ρ_i*.*

Доказательство первое, понятное. Пусть V – некоторое представление $\mathbb{Z}/n\mathbb{Z}$ над полем k. Обозначим через V_i подпредставление в V, образованное векторами v такими, что $\sigma(v) = \xi_n^i v$, оно изоморфно прямой сумме ρ_i. Очевидно, что $\oplus V_i \subset V$. Нужно показать, что любой вектор $v \in V$ представляется виде $\sum_{i=0}^{n-1} v_i$, где $v_i \in V_i$. Положим

$$v_i = \frac{1}{n}\sum_{j=0}^{n-1} \xi_n^{-ij}\sigma^j(v).$$

Тогда

$$\sigma(v_i) = \frac{1}{n}\sum_{j=0}^{n-1} \xi_n^{-i(j+1)}\sigma^{j+1}(v)\xi_n^i = v_i\xi_n^i,$$

поэтому $v_i \in V_i$. С другой стороны,

$$\sum_{i=0}^{n-1} v_i = \frac{1}{n}\sum_{i,j=0}^{n-1} \xi_n^{-ij}\sigma^j(v).$$

Суммируя по i геометрическую прогрессию, получаем: $\sum_i \xi_n^{-ij} = 0$ при $j \neq 0$ и $\sum_i \xi_n^{-ij} = n$ при $j = 0$. Отсюда $\sum_i v_i = \sigma^0(v) = v$. □

Доказательство второе, простое. Представления $\mathbb{Z}/n\mathbb{Z}$ над k – это всё равно, что модули над групповой алгеброй $\mathsf{k}[\mathbb{Z}/n\mathbb{Z}] \cong \mathsf{k}[\sigma]/(\sigma^n - 1)$. Как мы знаем, любое представление раскладывается в прямую сумму неприводимых (потому что $n \neq 0$ в k), следовательно эта алгебра полупроста. Все простые модули над ней содержатся в разложении модуля $\mathsf{k}[\mathbb{Z}/n\mathbb{Z}]$ на простые слагаемые. По китайской теореме об остатках,

$$\mathsf{k}[\sigma]/(\sigma^n - 1) \cong \mathsf{k}[\sigma] \Bigg/ \left(\prod_{i=0}^{n-1}(\sigma - \xi_n^i)\right) \cong \prod_{i=0}^{n-1} \mathsf{k}[\sigma]/(\sigma - \xi_n^i).$$

Это и есть разложение алгебры $\mathsf{k}[\mathbb{Z}/n\mathbb{Z}]$ в прямое произведение простых алгебр и соответствующего модуля на простые модули. Модуль $\mathsf{k}[\sigma]/(\sigma - \xi_n^i)$ одномерный, он соответствует представлению ρ_i. Значит, других неприводимых представлений, кроме ρ_i, нет. □

Предложение 10. *Пусть k – поле характеристики p и число n не делится на p. Предположим, что в k содержится первообразный корень из единицы степени n. Пусть K/k – циклическое расширение Галуа степени n. Тогда K получено присоединением к k радикала степени n, т.е. $\exists \alpha \in K$ такое, что $K = \mathsf{k}[\alpha]$ и $\alpha^n \in K$.*

Доказательство. Имеется представление G в векторном пространстве K над k. Разложим его на неприводимые, пользуясь леммой 9: $K = \oplus_{i=0}^{n-1} K_i$. Это разложение согласовано с умножением: $K_i \cdot K_j \subset K_{i+j}, (K_i \setminus 0)^{-1} \subset K_{-i}$. Действительно, если $x_i \in K_i, x_j \in K_j$, то $\sigma(x_i x_j) = \sigma(x_i)\sigma(x_j) = \xi_n^i x_i \xi_n^j x_j = \xi_n^{i+j} x_i x_j$, поэтому $x_i x_j \in K_{i+j}$. По основной теореме теории Галуа $K_0 = K^G = \mathsf{k}$. Если $x \in K_i$, $x \neq 0$, то умножение на x и на x^{-1} устанавливает взаимно обратные изоморфизмы между K_0 и K_i. Поэтому $\dim_{\mathsf{k}} V_i = 0$ или 1. При этом $\sum_{i=0}^{n-1} \dim_{\mathsf{k}} K_i = \dim_{\mathsf{k}} K = n$, поэтому все V_i одномерны. В частности, $K_1 \neq 0$. Возьмём в качестве α любой ненулевой элемент K_1. Тогда $\alpha^i \in K_i, \alpha^i \neq 0$. Значит, $\alpha^n \in K_n = K_0 = \mathsf{k}$ и степени α порождают все K_i и значит, всё K. □

Теперь мы можем доказать критерий разрешимости уравнения в радикалах.

Теорема 11. *Пусть k – поле характеристики ноль, $f \in \mathsf{k}[x]$ – неприводимый многочлен, а α – его корень. Тогда α выразим в радикалах, если и только если группа Галуа многочлена f разрешима.*

Доказательство в одну сторону. Пусть α выразим в радикалах при помощи некоторой формулы Φ, а K – поле разложения f. Заметим, что при правильном выборе значений радикалов в формуле Φ можно получить, помимо α, все другие корни многочлена f (и не только их). Пусть N – натуральное число, делящееся на степени всех радикалов, встречающихся в формуле Φ. Присоединим первообразный корень из единицы: $L_0 = \mathsf{k}[\sqrt[N]{1}]$, пусть L – поле, полученное последовательным присоединением к L_0 всех значений всех радикалов, встречающихся в формуле Φ. Тогда $K \subset L$. Очевидно, K, L_0 и L – расширения Галуа поля k.

Покажем, что группа Галуа $Gal(L, L_0)$ разрешима. Отсюда при помощи предложения 3 будет следовать, что и группа $Gal(L, \mathsf{k})$ разрешима, так как её фактор по разрешимой подгруппе $Gal(L, L_0)$ есть абелева группа $Gal(L_0, \mathsf{k}) = Gal(\mathsf{k}[\sqrt[N]{1}], \mathsf{k})$. Действительно, любой автоморфизм $\mathsf{k}[\sqrt[N]{1}]$ над k действует на первообразном корне возведением в степень, взаимно простую с n, поэтому $Gal(\mathsf{k}[\sqrt[N]{1}], \mathsf{k}) \subset (\mathbb{Z}/N\mathbb{Z})^*$. Но группа $Gal(K, \mathsf{k})$ тогда также будет разрешимой как факторгруппа разрешимой группы $Gal(L, \mathsf{k})$.

Итак, нужно показать, что $Gal(L, L_0)$ разрешима. Поле L получается из L_0 последовательным присоединением радикалов, т.е. существует последовательность $L_0 \subset L_1 \subset \ldots \subset$

$L_m = L$ полей, где $L_i = L_{i-1}[\sqrt[d_i]{a_i}]$ для $a_i \in L_{i-1}$. При этом все d_i делят N (по выбору N), поэтому в L_0 (и значит в L_{i-1}) есть все корни из единицы степени d_i. Значит, все расширения $L_{i-1} \subset L_i$ нормальны. Положим $G_i = Gal(L, L_i)$, тогда G_i – нормальная подгруппа в G_{i-1} и $G_{i-1}/G_i = Gal(L_i, L_{i-1})$ – циклическая группа по предложению 8. Таким образом, у группы $Gal(L, L_0)$ есть фильтрация $Gal(L, L_0) = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ с абелевыми факторами, значит она разрешима. $\square$

Доказательство в другую сторону. Пусть K – поле разложения многочлена f над k и группа Галуа $Gal(K, \mathsf{k})$ разрешима. Пусть $n = [K, \mathsf{k}]$, присоединим корни из единицы: $L_0 = \mathsf{k}[\sqrt[n]{1}]$ и $L = K[\sqrt[n]{1}]$. Очевидно, K, L_0 и L – расширения Галуа поля k.

Покажем, что n делится на $[L, L_0]$. Так как $[L, L_0][L_0, \mathsf{k}] = [L, \mathsf{k}] = [L, K][K, \mathsf{k}]$, это равносильно тому, что $[L_0, \mathsf{k}]$ делится на $[L, K]$. Заметим: $[L_0, \mathsf{k}]$ равно числу элементов в орбите $\sqrt[n]{1}$ относительно действия $Gal(L, \mathsf{k})$, а $[L, K]$ равно числу элементов в орбите $\sqrt[n]{1}$ относительно действия нормальной подгруппы $Gal(L, K) \subset Gal(L, \mathsf{k})$. Таким образом, утверждение вытекает из леммы 12, см. ниже.

Поле L порождено над K корнем из единицы степени n, поэтому группа Галуа $Gal(L, K)$ вложена в $(\mathbb{Z}/n\mathbb{Z})^*$ и, следовательно, абелева. Фактор группы $Gal(L, \mathsf{k})$ по разрешимой подгруппе $Gal(L, K)$ есть $Gal(K, \mathsf{k})$, эта группа разрешима по условию. Значит, по предложению 3, группа $Gal(L, \mathsf{k})$ разрешима, и её факторгруппа $Gal(L, L_0)$ – тоже.

Рассмотрим фильтрацию с циклическими факторами $Gal(L, L_0) = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$. Положим $L_i = L^{G_i}$. Тогда $L_0 = L_0$ и $L_m = L$. Нормальность G_i в G_{i-1} означает, что расширение $L_{i-1} \subset L_i$ нормально и при этом $Gal(L_i, L_{i-1}) = G_{i-1}/G_i$ – циклическая группа. Её порядок $[L_i : L_{i-1}]$ делит $[L : L_0]$, что делит n. Поэтому в L_0 (и, значит, в L_{i-1}) содержатся все корни из единицы степени $|Gal(L_i, L_{i-1})|$. По предложению 10, поле L_i получено присоединением к L_{i-1} радикала из некоторого элемента L_{i-1}. При этом L_0 также получено из k присоединением радикала, а именно $\sqrt[n]{1}$. Значит, все элементы поля L (в частности, все элементы поля K, и в их числе α) выразимы в радикалах. $\square$

Лемма 12. *Пусть конечная группа G действует на множестве X, пусть $H \lhd G$ – нормальная подгруппа, а $x \in X$ – элемент. Тогда порядок орбиты Hx делит порядок орбиты Gx.*

Доказательство – несложное упражнение.

Из следующего примера видно, что, как правило, уравнения не разрешимы в радикалах.

Пример 13. Корни многочлена $f(x) = x^5 - 6x + 2 \in \mathbb{Q}[x]$ не выразимы в радикалах. Действительно, этот многочлен неприводим по критерию Эйзенштейна. Его группа Галуа – подгруппа $G \subset S_5$, транзитивно переставляющая корни. Заметим: у f есть три вещественных корня и два комплексно-сопряжённых. Комплексное сопряжение оставляет на месте вещественные корни и меняет местами комплексные, т.е. это транспозиция в G. Покажем, что любая подгруппа G в S_5, транзитивно переставляющая корни и содержащая транспозицию, совпадает с S_5.

Скажем, что i эквивалентно j, если $(ij) \in G$. Это отношение эквивалентности на множестве $\{1, 2, 3, 4, 5\}$. Из-за транзитивности действия во всех классах эквивалентности одинаковое число элементов. Так как 5 – простое число, получаем, что все элементы эквивалентны и, значит, G содержит все транспозиции и поэтому совпадает с S_5.

Группа S_5 не разрешима, поэтому по теореме 11 корни многочлена f не выразимы в радикалах.