# Теорема Кронекера.

**Теорема Кронекера**. Пусть многочлен $f(x) \in \mathbb{Q}[x]$ нечетной простой степени неприводим над $\mathbb{Q}$, и уравнение $f(x) = 0$ разрешимо в радикалах. Тогда многочлен $f(x)$ имеет или ровно один вещественный корень, или все его корни являются вещественными.

**Замечание.** На самом деле мы докажем более сильный факт: если многочлен $f(x) \in \mathbb{Q}[x]$ нечетной простой степени неприводим над $\mathbb{Q}$, и хотя бы один корень уравнения $f(x) = 0$ выражается через радикалы, то многочлен $f(x)$ имеет или ровно один вещественный корень, или все его корни являются вещественными.

**Упр. 1.** Придумайте какой-нибудь неприводимый многочлен $f(x)$ пятой степени, у которого ровно три вещественных корня. Тогда ни один из его пяти корней не будет выражаться через радикалы.

**Упр. 2.** 1) Не существует «радикальной» формулы для решения «общего» уравнений пятой степени $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ (то есть такой формулы, которая давала бы значение хотя бы одного корня многочлена хотя бы при одном выборе значений всех встречающихся в ней радикалов при любых значениях $a, b, c, d, e, f \in \mathbb{Q}$).

2) Аналогичное утверждение верно для многочленов степени $\geqslant 5$.

---

**Лемма 1.** Пусть $q$ – простое число и $x^q - a \in k[x]$. Тогда

1) многочлен $x^q - a$ приводим над $k \iff a = b^q$ для некоторого $b \in k$.

2) если поле $k$ содержит примитивный корень степени $q$ из 1, то многочлен $x^q - a$ или неприводим над $k$, или полностью раскладывается над $k$ на линейные множители.

**Доказательство.** 1) Если $a = b^q$, то приводимость $f(x)$ над $k$ очевидна (и даже есть корень!). Допустим теперь, что $x^q - a = f(x)g(x)$, где $f(x)$ и $g(x)$ – многочлены над $k$, $r = \deg f(x)$, $0 < r < q$. Пусть $\beta$ – один из (комплексных) корней многочлена $f(x)$, $\epsilon$ – примитивный корень степени $q$ из 1. Тогда остальные корни многочлена $f(x)$ имеют вид $\epsilon^{n_i}\beta$. Так как произведение корней многочлена равно $\pm$свободному члену, то для некоторого $n$ выполнено $\beta^r\epsilon^n = c \in k$, где $f(x) = \cdots \pm c$. Тогда $a^r = (\beta^q)^r = (\beta^r)^q = (\beta^r\epsilon^n)^q = c^q$. Так как $(r, q) = 1$, то $1 = rs + qt$ для некоторых целых $s$ и $t$, откуда $a = a^{rs}a^{qt} = c^{qs} \cdot a^{qt} = (c^s a^t)^q$, и $c^s a^t \in k$.

2) Если многочлен $x^q - a$ приводим над $k$, то по части 1 леммы у него есть корень $b \in k$. Тогда все остальные корни имеют вид $\epsilon^i b$, и так как $\epsilon \in k$, то $\epsilon^i b \in k$.

**Лемма 2.** Пусть многочлен $f(x) \in k[x]$ простой степени $p$ неприводим над $k$. Допустим, что многочлен $f(x)$ становится приводимым после присоединения к полю $k$ корня неприводимого многочлена степени $m$ (то есть над полем $k(\beta)$, $[k(\beta) : k] = m$). Тогда $m \vdots p$.

**Доказательство.** Пусть $\alpha$ – (комплексный) корень многочлена $f(x)$. Разложим двумя способами расширение $k \subset k(\alpha, \beta)$ в башню:

$$k \subset k(\alpha) \subset k(\alpha, \beta), \qquad k \subset k(\beta) \subset k(\beta, \alpha).$$

Приравнивая степени расширений, получаем: $p \cdot (\leqslant m) = m \cdot (< p)$. Так как $p$ – простое, то $m \vdots p$.

## Доказательство теоремы Кронекера

0) Один вещественный корень у многочлена $f(x)$ точно есть.

1) Пусть многочлен $f(x) \in \mathbb{Q}[x]$ простой степени $p$ неприводим над $\mathbb{Q}$. Рассмотрим радикальное расширение, в котором $f(x)$ имеет хотя бы один корень:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[q_1]{a_1}) \subset \ldots \mathbb{Q}(\sqrt[q_1]{a_1}, \ldots, \sqrt[q_k]{a_k}), \qquad a_i^{q_i} \in \mathbb{Q}(\sqrt[q_1]{a_1}, \ldots, \sqrt[q_{i-1}]{a_{i-1}}).$$

Понятно, что все числа $q_i$ можно считать простыми [почему?]. В дальнейшем мы будем многократно «уплотнять» эту башню.

Степень расширения $L \subset L(\sqrt[q_i]{a_i})$ равна непонятно чему. Но если в поле $L$ лежит примитивный корень степени $q_i$ из 1, то по лемме 1.2 ситуация гораздо более приятная: эта степень равна 1 (то есть поля $L$ и $L(\sqrt[q_i]{a_i})$ совпадают) или $q_i$. Чтобы можно было воспользоваться леммой 1.2, уплотним каждый этаж башни $L \subset L(\sqrt[q_i]{a_i})$ до $L \subset L(\sqrt[q_i]{1}) \subset L(\sqrt[q_i]{1}, \sqrt[q_i]{a_i})$. Под $\sqrt[q_i]{1}$ подразумевается любой комплексный корень из 1, отличный от 1, который в силу простоты $q_i$ является примитивным корнем.

Эту уплотненную башню будем называть $\mathcal{B}$. Рассмотрим минимальный этаж башни $\mathcal{B}$, над которым $f(x)$ приводим. Меняя обозначения, получаем: $f(x)$ неприводим над $k$, но $f(x)$ приводим над $k(\sqrt[q]{a})$, $q$ – простое.

2) Допустим, что $a \neq 1$. Тогда по леммам 1.2 и 2 $\quad q = p$ (напомним, что примитивный корень степени $q$ из 1 присоединяется на предыдущем шаге). Докажем, что $f(x)$ не просто приводим над $k(\sqrt[p]{a})$, но имеет в этом поле корень, и даже все корни!!! В самом деле, пусть $\beta$ – любой комплексный корень многочлена $f(x)$. Рассмотрим расширение $k \subset k(\sqrt[p]{a}, \beta)$ и двумя способами разложим его в башню:

$$k \subset k(\beta) \subset k(\sqrt[p]{a}, \beta), \qquad\qquad k \subset k(\sqrt[p]{a}) \subset k(\beta, \sqrt[p]{a}).$$

Посмотрим на степени этажей: по лемме 1.2 $[k(\sqrt[p]{a}) : k] = 1$ или $p$, но первый случай невозможен по выбору поля $k$; $[k(\sqrt[p]{a}, \beta) : k(\sqrt[p]{a})] < p$ (так как многочлен $f(x)$ приводим над $k(\sqrt[p]{a})$). Далее, $[k(\beta) : k] = p$ (так как многочлен $f(x)$ неприводим над $k$), и снова по лемме 1.2 $[k(\beta, \sqrt[p]{a}) : k(\beta)] = 1$ или $p$. Приравнивая размерности, получаем, что $p \cdot (< p) = p \cdot (1 \text{ or } p)$, что возможно только в одном случае $[k(\sqrt[p]{a}, \beta) : k(\sqrt[p]{a})] = 1$, что равносильно включению $\beta \in k(\sqrt[p]{a})$. В силу произвольности выбора $\beta$ все корни $f(x)$ лежат в $k(\sqrt[p]{a})$.

Тем самым мы показали, что если один корень $f(x)$ выражается через радикалы, то остальные корни тоже выражаются через радикалы (см. замечание после формулировки теоремы Кронекера). Кроме того, приводимость $f(x)$ над $k(\sqrt[p]{a})$ оказалась равносильна разложимости на линейные множители!

3) Сколько всего замечательного мы уже получили в случае, когда $a \neq 1$, а корень из 1 содержится в предыдущем этаже (а дальше мы докажем еще более замечательные факты)! Случай присоединения примитивного корня степени $q$ из 1 является самым сложным в доказательстве, так как для него практически все эти замечательные вещи не верны.

Но оказывается, что на самом деле корень из 1 можно не присоединять! Доказывается это весьма нетривиально. Сейчас мы сформулируем предложение, которое содержит в себе все идейные и технические сложности этого доказательства.

**Предложение.** Пусть $\epsilon$ – примитивный корень простой степени $q$ из 1. Тогда существует радикальная башня

$$L \subset L(\sqrt[n_1]{a_1}) \subset L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \subset \cdots \subset L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots, \sqrt[n_s]{a_s}), \qquad n_i < q, \qquad (*)$$

такая, что $\epsilon \in L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots, \sqrt[n_s]{a_s})$.

Доказательство предложения временно отложим, а пока поймем, что можно извлечь из этого предложения. В башне $(*)$ заменим присоединение всех радикалов составных степеней на последовательные присоединения радикалов простых степеней. И снова, как мы делали это при уплотнении исходной радикальной башни до башни $\mathcal{B}$, перед присоединенем любого радикала простой степени сначала присоединим примитивный корень этой простой степени из 1. Все эти простые степени строго меньше $q$.

Вернемся к башне $\mathcal{B}$. Этаж $L \subset L(\sqrt[q]{a})$ будем называть *правильным*, если $q$ – простое, и поле $k$ содержит примитивный корень степени $q$ из 1. Требование наличия корня из 1 в $L$ мотивируется

доказанным в пункте 2. По построениею $\mathcal{B}$ неправильными могут быть только этажи $L \subset L(\sqrt[q]{1})$, $q$ – простое. В этом случае каждый неправильный этаж заменим на новую цепочку расширений так, как написано в предыдущем абзаце. Получим новую башню $\mathcal{B}'$. В $\mathcal{B}'$ каждый этаж или является правильным, или имеет вид $L \subset L(\sqrt[p_i]{1})$, $p_i$ – простое. При этом в башне $\mathcal{B}'$ максимальное число $q$, для которого этаж $L \subset L(\sqrt[q]{1})$ – неправильный, строго меньше, чем в башне $\mathcal{B}$. С башней $\mathcal{B}'$ проделаем аналогичную процедуру, и так далее. На некотором шаге получится башня $\mathcal{B}_1$, в которой нет неправильных этажей. Отметим, что в башне $\mathcal{B}_1$ этажей, вообще говоря, много больше, чем в башен $\mathcal{B}$.

Тем самым мы показали, что в башне $\mathcal{B}_1$ каждый этаж $L \subset L(\sqrt[q]{a})$ удовлетворяет свойствам:

– $q$ – простое

– $L$ содержит примитивный корень степени $q$ из 1.

Вернемся к выбору поля $k$: рассмотрим минимальный этаж башни $\mathcal{B}_1$, над которым $f(x)$ приводим. Меняя обозначения, получаем: $f(x)$ неприводим над $k$, но $f(x)$ приводим над $k(\sqrt[q]{a})$, $q$ – простое. Тем самым все то, что мы доказали в пункте 2, верно во всех случаях. А именно:

– $q = p$.

– Степень расширения $k \subset k(\sqrt[p]{a})$ равна $p$.

– $f(x)$ полностью раскладывается над $k(\sqrt[p]{a})$ на линейные множители.

– Все корни $f(x)$ выражаются через радикалы.

4) Пусть $x_0$ – любой корень $f(x)$, $x_0 \in k(\sqrt[p]{a})$. Обозначим для краткости $r = \sqrt[p]{a}$. Тогда по теореме о строении расширения, полученного присоединеним алгебраического элемента,

$$x_0 = \gamma_0 + \gamma_1 r + \gamma_2 r^2 + \cdots + \gamma_{p-1} r^{p-1}, \gamma_i \in k,$$

причем такое представление единственно. Сейчас мы сделаем очень хитрую вещь: найдем, как именно выглядят остальные корни $f(x)$, которые, напомним, тоже лежат в $k(\sqrt[p]{a})$. Обозначим через $\epsilon$ примитивный корень степени $p$ из 1 и положим

$$x_i = \gamma_0 + (\gamma_1 \epsilon^i) r + (\gamma_2 (\epsilon^i)^2) r^2 + \cdots + (\gamma_{p-1} (\epsilon^i)^{p-1}) r^{p-1}, \qquad i = 0, 1, 2, \ldots, p-1.$$

Оказывается, что $x_0, \ldots, x_{p-1}$ – все различные [почему различные?] корни $f(x)$, что совершенно неочевидно! Мы приведем два доказательства этого факта.

**Первое доказательство – автоморфизмы.** Изучим автоморфизмы поля $k(\sqrt[p]{a})$, которые оставляют элементы поля $k$ на месте. Пусть $\varphi$ – такой автоморфизм. Куда при этом автоморфизме переходит корень какого-нибудь неприводимого над $k$ многочлена? Только в корень того же самого многочлена (в тот же корень или в другой корень) [почему?]. Поэтому элемент $\sqrt[p]{a}$ – корень *неприводимого* многочлена $x^p - a$ переходит в другой корень этого же многочлена, то есть $\varphi(\sqrt[p]{a}) = \epsilon^s \sqrt[p]{a}$ для некоторого $s$. При этом значение $\varphi(\sqrt[p]{a})$ полностью определяет, куда переходят *все* элементы поля $k(\sqrt[p]{a})$ [почему?]. С другой стороны, если мы определим отображение $\varphi_s : k(\sqrt[p]{a}) \to k(\sqrt[p]{a})$ по формуле $\varphi_s(\sum_{i=0}^{p-1} \gamma_i r^i) = \sum_{i=0}^{p-1} \gamma_i (\epsilon^s r)^i$, то оно будет корректно определено и будет автоморфизмом (разумеется, это все надо проверить). Чтобы $\varphi_s$ было определено, нужно, чтобы в поле $k$ лежал элемент $\epsilon^s$. Но он там лежит, ведь мы рассматриваем правильные расширения! [Упражнение на понимание: если многочлен $x^p - a$ неприводим над $k$, а в поле $k$ нет примитивного корня степени $p$ из 1, то сколько автоморфизмов (над $k$) будет у поля $k(\sqrt[p]{a})$?]

Осталось заметить, что $\varphi_i(x_0) = x_i$. Так как моногочлен $f(x)$ с корнем $x_0$ неприводим над $k$, по по вышеупомянутому факту его корень $x_0$ переходит под действием $\varphi_i$ в другой корень. Поэтому $x_i$ – корень $f(x)$.

**Второе доказательство – симметрические многочлены.** Рассмотрим многочлен $g(x) = (x - x_0)(x - x_1) \ldots (x - x_{p-1})$ и покажем, что он лежит в $k[x]$. Из этого будет следовать, что оба многочлена $f(x)$ и $g(x)$ лежат в $k[x]$, имеют общий корень $x_0$, откуда из неприводимости $f(x)$ будет вытекать, что $g(x) \vdots f(x)$, а из сравнения степеней будет вытекать, что $f(x) = \mathrm{const} \cdot g(x)$.

Для доказательства того, что все коэффициенты многочлена $g(x)$ лежат в поле $k$, необходимо показать, что все элементарные симметрические функции от $x_0, \dots, x_{p-1}$ $\sigma_t = \sum_{i_1<\dots<i_t} x^{i_1} \dots x^{i_t}$ лежат в $k$. А в силу формул Ньютона [напоминание: если $p_t = x_0^t + \dots + x_{p-1}^t$, то при $k \leqslant p$

$$p_k - p_{k-1}\sigma_1 + p_{k-2}\sigma_2 - \dots + (-1)^{k-1}p_1\sigma_{k-1} + (-1)^k k\sigma_k = 0]$$

достаточно доказать, что элементы $x_0^t + \dots + x_{p-1}^t$ лежат в $k$ для всех $t$. Это достаточно рутинное упражнение «на раскрытие скобочек». Однако в нем где-то надо использовать, что $r$ – это не просто корень какого-то многочлена, а именно корень двучлена $x^p - a$!

Не поленимся, и проделаем это упражнение. По формуле полинома Ньютона

$$x_i^t = \Big(\gamma_0 + (\gamma_1\epsilon^i)r + (\gamma_2(\epsilon^i)^2)r^2 + \dots + (\gamma_{p-1}(\epsilon^i)^{p-1})r^{p-1}\Big)^t =$$

$$= \sum_{t_0+t_1+\dots t_{p-1}=t} C_t^{t_0,t_1,\dots,t_{p-1}} \gamma_0^{t_0}\gamma_1^{t_1}\dots\gamma_{p-1}^{t_{p-1}} (\epsilon^i)^{t_1+2t_2+\dots+(p-1)t_{p-1}} r^{t_1+2t_2+\dots+(p-1)t_{p-1}} =$$

$$= \sum_l \theta_l (\epsilon^i)^l r^l, \qquad \theta_l \in k.$$

Просуммируем по $i = 0, 1, \dots, p-1$, с учетом того, что $\theta_l$ не зависят от $i$:

$$x_0^t + \dots + x_{p-1}^t = \sum_l \theta_l r^l \Big(1 + \epsilon^l + (\epsilon^l)^2 + (\epsilon^l)^3 + \dots + (\epsilon^l)^{p-1}\Big).$$

Если $l \not\vdots p$, то выражение в скобках равно 0. Если $l \vdots p$, то выражение в скобках равно $p$, но при этом $r^l = a^{l/p} \in k$. В итоге $x_0^t + \dots + x_{p-1}^t \in k$.

5) Мы исследуем вещественность/невещественность корней многочлена. Вещественность комплексного числа означает, что оно инвариантно относительно комплексного сопряжения. Поэтому необходимо посмотреть, как соотносится операция комплексного сопряжения с нашей башней радикальных расширений. Пока никак не соотносится. Поэтому уплотним башню $\mathcal{B}_1$: каждый этаж $L \subset L(\sqrt[q_i]{a_i})$ заменим на два этажа $L \subset L(\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}}) \subset L(\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}},\ \sqrt[q_i]{a_i}) = L(\sqrt[q_i]{a_i},\ \overline{\sqrt[q_i]{a_i}})$. Получим новую башню $\mathcal{B}_2$. Заметим, что каждый этаж башни $\mathcal{B}_2$ замкнут относительно сопряжения, что доказывается индукцией по числу этажей башни $\mathcal{B}_2$. При этом используется вещественность числа $\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}}$.

Расширение $L(\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}}) \subset L(\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}},\ \sqrt[q_i]{a_i})$, очевидно, радикально, так как $a_i^{q_i} \in L$. Необходимо проверить, что расширение $L \subset L(\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}})$ радикально. Это легко вытекает из того, что поле $L$ замкнуто относительно сопряжения.

Легко понять, что в башне $\mathcal{B}_2$ каждый этаж получится правильным [почему?]. Поэтому все то, что мы делали для башни $\mathcal{B}_1$, можно проделать и для $\mathcal{B}_2$ (начиная от выбора поля $k$). Итого, в результате рассуждений этого пункта мы можем считать, что поле $k$ замкнуто относительно комплексного сопряжения.

6) Так как все корни $f(x)$ лежат в $k(\sqrt[p]{a})$, то будем считать, что $x_0$ – это вещественный корень. Рассмотрим два случая: число $a$ вещественное и невещественное.

**Первый случай.** Пусть $a$ – вещественное. Тогда $r$ тоже можно считать вещественным, так как все корни степени $p$ из 1 лежат в $k$. Из равенства $x_0 = \overline{x}_0$ получаем, что

$$\gamma_0 + \gamma_1 r + \gamma_2 r^2 + \dots + \gamma_{p-1}r^{p-1} = \overline{\gamma}_0 + \overline{\gamma}_1 r + \overline{\gamma}_2 r^2 + \dots + \overline{\gamma}_{p-1}r^{p-1},$$

откуда в силу ЛНЗ $1, r, r^2, \dots, r^{p-1}$ над $k$ заключаем, что $\gamma_0, \gamma_1, \dots, \gamma_{p-1}$ – вещественны. Здесь мы воспользовались пунктом 5 – замкнутостью поля $k$ относительно сопряжения. Вот зачем это было нужно. Далее рутинной проверкой устанавливается, что все остальные корни полинома $f(x)$ невещественны. Для доказательства надо предположить, что $x_i = \overline{x}_i$ при $i > 0$ (а по пункту 4 корнями $f(x)$ являются $x_0, \dots, x_{p-1}$), и извлечь из этого, что $\gamma_1 = \gamma_2 = \dots = \gamma_{p-1} = 0$, то есть $x_0 \in k$, что противоречит выбору поля $k$.

**Второй случай.** Пусть $a$ – невещественное, $c = r\overline{r} \in \mathbb{R}$. Из равенств $x_0 = \overline{x}_0$ и $r^p = a$ получаем, что

$$\gamma_0 + \gamma_1 r + \gamma_2 r^2 + \cdots + \gamma_{p-1} r^{p-1} = \overline{\gamma}_0 + \overline{\gamma}_1 \overline{r} + \overline{\gamma}_2 \overline{r}^2 + \cdots + \overline{\gamma}_{p-1} \overline{r}^{p-1} =$$

$$= \overline{\gamma}_0 + \overline{\gamma}_1 (c/r) + \overline{\gamma}_2 (c/r)^2 + \cdots + \overline{\gamma}_{p-1} (c/r)^{p-1} = \frac{r^p}{a}\Big(\overline{\gamma}_0 + \overline{\gamma}_1 (c/r) + \overline{\gamma}_2 (c/r)^2 + \cdots + \overline{\gamma}_{p-1} (c/r)^{p-1}\Big) =$$

$$= \overline{\gamma}_0 + (\overline{\gamma}_1 c/a) r^{p-1} + (\overline{\gamma}_2 c^2/a) r^{p-2} + \cdots + (\overline{\gamma}_{p-1} c^{p-1}/a) r.$$

Но просто так мы не можем воспользоваться тем же приемом, что и в первом случае — приравнять коэффициенты при соответствующих степенях $r$. Дело в том, что эти коэффициенты (за счет наличия множителя $c$) могут, вообще говоря, не лежать в $k$. Здесь надо вспомнить про построение башни $\mathcal{B}_2$: до присоединения к очередному этажу элемента $\sqrt[q_i]{a_i}$ мы присоединяли к нему элемент $\sqrt[q_i]{a_i} \cdot \overline{\sqrt[q_i]{a_i}}$. Поэтому элемент $c$ на самом деле лежит в $k$. Поэтому можно приравнять коэффициенты при соответствующих степенях $r$, и получить $p$ равенств. Далее прямой проверкой убеждаемся, что эти $p$ равенств влекут $x_i = \overline{x}_i$, $i = 1, \ldots, p-1$, то есть все корни многочлена $f(x)$ оказываются вещественными.

Теорема Кронекера доказана.

**Задача.** Докажите, что если все три корня неприводимого над полем $\mathbb{Q}$ многочлена $ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ вещественны, то их нельзя выразить посредством вещественных радикалов.

## Доказательство предложения

Для удобства сформулируем доказываемое предложение еще раз, изменив обозначения. Его доказательство связано с именем Гаусса.

**Предложение.** Пусть $\alpha$ – примитивный корень простой степени $p$ из 1. Тогда существует радикальная башня

$$L \subset L(\sqrt[n_1]{a_1}) \subset L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \subset \cdots \subset L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots, \sqrt[n_s]{a_s}), \qquad n_i < p, \qquad (*)$$

такая, что $\alpha \in L(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots, \sqrt[n_s]{a_s})$.

**Доказательство.** Докажем утверждение при помощи индукции по $p$ для любых, не обязательно простых, $p$. Если $p$ составное, то $p = ab$ для некоторых $a$ и $b$. Поэтому $\sqrt[p]{1} = \sqrt[a]{\sqrt[b]{1}}$. Пусть теперь $p$ простое. Пусть $g$ — первообразный корень по модулю $p$. Обозначим $\alpha := \varepsilon_p$, $\varepsilon := \varepsilon_{p-1}$ и,

$$\text{для} \quad r = 0, 1, 2, \ldots, p-2, \quad T_r(x) := x + \varepsilon^r x^g + \varepsilon^{2r} x^{g^2} + \cdots + \varepsilon^{(p-2)r} x^{g^{p-2}} \in \mathbb{Q}(\varepsilon)[x].$$

Тогда $\alpha = \dfrac{(T_0 + T_1 + \cdots + T_{p-2})(\alpha)}{p-1}$. Имеем $T_0(\alpha) = -1$. Поэтому достаточно доказать, что число $T_r(\alpha)$ выражается через радикалы степени меньше $p$ для каждого $r = 1, 2, \ldots, p-2$.

Так как

$$T_r(x^g) \equiv \varepsilon^{-r} T_r(x) \mod (x^p - 1), \quad \text{то} \quad T_r^{p-1}(x^g) \equiv T_r^{p-1}(x) \mod (x^p - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1}$ с коэффициентами в $\mathbb{Q}(\varepsilon)$, сравнимый с $T_r^{p-1}(x)$ по модулю $x^p - 1$. Тогда $a_k = a_{kg \bmod p}$ для любого $k = 1, 2, \ldots, p-1$ [почему?]. Значит, $a_1 = a_2 = \cdots = a_{p-1}$. Поэтому $T_r^{p-1}(\alpha) = a_0 - a_1 \in \mathbb{Q}(\varepsilon)$. Таким образом, число $T_r(\alpha)$ выражается через радикалы степени меньше $p$.