

Алгебра 2 2023 Кузнецов

1 Листок 1

1. Для каких натуральных n многочлен $\frac{x^n-1}{x-1} = 1+x+\dots+x^{n-1}$ неприводим?

По-видимому, имеется в виду неприводимость над полем \mathbb{Q} .

Во-первых, заметим, что при $n = ab$ имеет место равенство

$$1 + x + \dots + x^{n-1} = (1 + x + \dots + x^{a-1})(1 + x^a + \dots + x^{a(b-1)}).$$

Или без разложения:

$$\frac{x^{ab} - 1}{x - 1} = \frac{x^a - 1}{x - 1} \frac{x^{ab} - 1}{x^a - 1}.$$

Отсюда следует, что при составном n многочлен $\frac{x^n-1}{x-1}$ приводим.

Теперь попробуем доказать, что при простом $n = p$ многочлен $\frac{x^n-1}{x-1}$ неприводим. Предположим, что

$$\frac{x^p - 1}{x - 1} = u(x)v(x),$$

где u, v — непостоянные многочлены с рациональными коэффициентами, причём будем считать, что их старшие коэффициенты равны 1, и u — непостоянный многочлен с рациональными коэффициентами наименьшей степени, делящий $\frac{x^p-1}{x-1}$. Тогда, что

$$u(x) = (x - a_1) \dots (x - a_k),$$

где a_1, \dots, a_k — попарно различные неединичные корни степени p из единицы. Поэтому все симметрические многочлены от a_1, \dots, a_k

$$a_1 + \dots + a_k,$$

$$a_1 a_2 + \dots + a_{k-1} a_k,$$

$$\dots$$

$$a_1 \dots a_k$$

рациональны — они являются коэффициентами многочлена u . Но тогда для любого натурального s

$$u_s(x) = (x - a_1^s) \dots (x - a_k^s)$$

— тоже многочлен с рациональными коэффициентами (поскольку все симметрические многочлены выражаются через элементарные), и он должен быть взаимно прост с u либо совпадать с u , ибо иначе наибольший общий делитель этих многочленов будет степени меньше степени u и будет делить многочлен $\frac{x^p-1}{x-1}$. Рассмотрим множество тех $s \in \{1, \dots, p-1\}$, для которых

$$\{a_1^s, \dots, a_k^s\} = \{a_1, \dots, a_k\}.$$

Это подгруппа мультипликативной группы \mathbb{F}_p . Значит, она циклическая, и есть $h \in \{1, \dots, p-1\}$, таких, что она порождена h . Тогда

$$u(x) = (x-a)(x-a^h)(x-a^{h^2}) \dots (x-a^{h^t}).$$

Дальше я не знаю, как закончить это рассуждение. Поэтому будем решать по-другому. Попробуем применить критерий Эйзенштейна. $q(x) = \frac{x^p-1}{x-1}$ неприводим над \mathbb{Q} тогда и только тогда, когда неприводим

$$q(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + C_p^{p-1} x^{p-2} + \dots + C_p^2 x + p.$$

И применим критерий Эйзенштейна.

2. $x^n f(\frac{1}{x}) = c_0 x^n + c_1 x^{n-1} + \dots + c_{n-1} x + c_n$ имеет с $f(x)$ общий корень — тот, который лежит на единичной окружности (если $|\alpha| = 1$ и $f(\alpha) = 0$, то $f(\frac{1}{\alpha}) = f(\bar{\alpha}) = 0$). Значит, эти многочлены не взаимно просты, и в силу неприводимости f должны иметь все корни общие. То есть эти многочлены пропорциональны:

$$f(x) = t x^n f\left(\frac{1}{x}\right), t \in \mathbb{Q}.$$

Отсюда $c_k = t c_{n-k}$ для всех k . Отсюда $t^2 = 1$. Значит, $t = \pm 1$. Если $t = -1$, то многочлен f имеет корнем 1, что противоречит неприводимости. Значит, $t = 1$. Если n нечётно, $n = 2m+1$, то

$$f(x) = (x^{2m+1} + 1) + c_1(x^{2m} + x) + \dots,$$

и этот многочлен имеет корень -1 , что тоже невозможно в силу его неприводимости. Всё доказано.

3. а) Кажется, это известная теорема. Воспользуемся тем, что мультипликативная группа поля \mathbb{F}_p циклическая. Значит, она порождается неким $g \in \mathbb{F}_p$. Тогда $\left(\frac{-1}{p}\right) = 1$ тогда и только тогда, когда для некоторого $s, 0 < s < p-1$ имеет место

$$g^{2s} = -1.$$

Из этого равенства следует $g^{4s} = 1$, и получаем:

$2s$ не делится на $p-1$, $4s$ делится на $p-1$.

Отсюда следует, что $p-1$ делится на 4. Пусть, напротив, $p-1$ делится на 4. Тогда возьмём $h = g^{\frac{p-1}{2}}$. Отсюда $h^2 = 1$. Поэтому $h = \pm 1$. Но $h = 1$ быть не может, так как g — первообразный корень.

- б) Очевидно, следующие утверждения равносильны:

- $\left(\frac{-3}{p}\right) = 1$
- Многочлен $x^2 + 3$ приводим над \mathbb{F}_p
- Многочлен $(x+1)^2 + 3 = x^2 + 2x + 4$ приводим над \mathbb{F}_p
- Многочлен $(x-2)(x^2 + 2x + 4) = x^3 - 8$ разложим над \mathbb{F}_p
- Существует $\varepsilon \in \mathbb{F}_p, \varepsilon \neq 1$, такое, что $\varepsilon^3 = 1$ (поделить на 2 корни уравнения из предыдущего пункта)

Но мультипликативная группа поля \mathbb{F}_p циклическая. Значит, она порождается неким $g \in \mathbb{F}_p$. Тогда $\varepsilon = g^s, 0 < s < p-1$. Но тогда $g^{3s} = 1$, и $3s \mid p-1$. Если $p-1$ не делится на 3, то s делится на $p-1$, а такое невозможно в силу $0 < s < p-1$. Значит, $p-1$ делится на 3.

И обратно — если $p-1$ делится на 3, то можно положить

$$\varepsilon = g^{\frac{p-1}{3}}.$$

Задача решена.

4. K содержит примитивный корень из 1 степени 8. Пусть это корень g . Ясно, что тогда $g^4 = -1, g^2 = -1/g^2$. Рассмотрев пример поля комплексных чисел, я подобрал такое:

$$(g + 1/g)^2 = g^2 + 2 + 1/g^2 = g^2 + 2 - g^2 = 2.$$

Теперь рассмотрим 4 случая:

- $p \equiv 1 \pmod{8}$. Тогда существует примитивный корень из 1 степени 8. Почему? Как мы помним, мультипликативная группа конечного поля \mathbb{F}_p циклическая. Она порождена элементом $t \in \mathbb{F}_p$. Тогда $t^{\frac{p-1}{8}}$ и есть первообразный корень из 1 степени 8.
- $p \equiv -1 \pmod{8}$. Это более сложный случай. По задаче 3а, -1 является квадратичным невычетом в F_p . Значит, многочлен $x^2 + 1$ неприводим над F_p , и фактор $G = F_p[x]/(x^2 + 1)$ является полем из p^2 элементов. Обозначим в этом поле элемент x как i , $i^2 = -1$. Итак, $G = \{a + bi \mid a, b \in F_p\}$. Пусть g — первообразный корень в G (то есть порождающий элемент мультипликативной группы поля G). Положим

$$h = g^{(p^2-1)/8}.$$

Тогда $h^4 = -1$, h — примитивный корень из 1 степени 8 (но, к сожалению, он лежит не в поле F_p , а в его расширении).

Утверждение 1.1. Или $h + 1/h$, или $h - 1/h$ лежит в F_p .

Proof. h является корнем многочлена $x^4 + 1$. Вот 4 корня этого многочлена: $h, -h, 1/h, -1/h$. Легко видеть, что они все разные (если, например, $h = -1/h$, то $h^2 = -1$, а это противоречит равенству $h^4 = -1$). Итак,

$$x^4 + 1 = (x - h)(x + h)(x - 1/h)(x + 1/h).$$

Но $F_p[h]$ — поле, которое строго больше F_p , но содержится в G . Значит, оно совпадает с G , ведь нет поля характеристики p с количеством элементов между p и p^2 . Значит, любой элемент поля G представляется в виде $\alpha h + \beta, \alpha, \beta \in F_p$. Поэтому

$$h^2 = \alpha h + \beta, \alpha, \beta \in F_p.$$

Значит, многочлены $x^4 + 1$ и $x^2 - \alpha x - \beta$ не взаимно просты. Поэтому $x^4 + 1$ делится на какой-то многочлен степени 2 с коэффициентами в F_p . Возможны лишь такие разложения $x^4 + 1$ в произведение многочленов второй степени (с коэффициентами из F_p):

$$\begin{aligned} x^4 + 1 &= (x^2 - h^2)(x^2 - 1/h^2), \\ x^4 + 1 &= (x^2 - (h + 1/h)x + 1)(x^2 + (h + 1/h)x + 1), \\ x^4 + 1 &= (x^2 - (h - 1/h)x - 1)(x^2 + (h - 1/h)x - 1). \end{aligned}$$

Первый вариант не подходит, поскольку h^2 не может лежать в F_p , ведь его квадрат равен -1 . Во втором и третьем вариантах либо $h + 1/h$, либо $h - 1/h$ лежит в F_p . Выяснить, какой же из этих вариантов реализуется, у нас получится позже. \square

Покажем, что не может быть $h - 1/h \in F_p$. Пусть $g = u + vi, u, v \in F_p$. Тогда

$$\frac{1}{g} = \frac{u - vi}{u^2 + v^2}.$$

Имеем

$$h - 1/h = (u + vi)^{(p^2-1)/8} - \frac{(u - vi)^{(p^2-1)/8}}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Пусть $h = U + Vi = (u + vi)^{(p^2-1)/8}, U, V \in F_p$. Тогда

$$h - 1/h = U + Vi - \frac{U - Vi}{(u^2 + v^2)^{(p^2-1)/8}} = U + Vi + \frac{-U + Vi}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Это может лежать в F_p , только если

$$V + \frac{V}{(u^2 + v^2)^{(p^2-1)/8}} = 0.$$

$V = 0$ быть не может, ведь $U + Vi = h$, а h не лежит в F_p — потому что $h^4 = -1$, а -1 у нас квадратичный невычет. Значит, на V можно сократить, и

$$(u^2 + v^2)^{(p^2-1)/8} = -1.$$

Но у нас $(p^2 - 1)/8$ чётное, и из этого равенства следует, что -1 — квадратичный вычет по модулю p . А это неверно. Итак, $h - 1/h$ не может лежать в F_p , и остаётся $h + 1/h \in F_p$. Поскольку

$$(h + 1/h)^2 = 2,$$

то всё доказано.

- $p \equiv -3 \pmod{8}$. Предположим,

$$s^2 \equiv 2 \pmod{p}.$$

По задаче 3а есть $j \in \mathbb{F}_p$, такое, что

$$j^2 \equiv -1 \pmod{p}.$$

Рассмотрим $z = s^{\frac{1+j}{2}}$. Тогда

$$z^2 = s^{\frac{1+j}{2}} = j.$$

Отсюда ясно, что z — первообразный корень из 1 степени 8. Мультипликативная группа поля \mathbb{F}_p циклическая. Она порождена элементом $t \in \mathbb{F}_p$. Тогда $z = t^k, 0 < k < p-1$. Отсюда $t^{8k} = 1$, $8k$ делится на $p-1$. Но $p-1$ не делится на 8. Значит, $4k$ делится на $p-1$, и $z^4 = 1$. Противоречие с первообразностью p .

- $p \equiv 3 \pmod{8}$. Это самый сложный случай. Поначалу можно рассуждать, как в случае $p \equiv -1 \pmod{8}$. По задаче 3а, -1 — квадратичный невычет в F_p . Поэтому так же рассматриваем расширение $G = F_p[x]/(x^2 + 1)$. В нём выбираем элемент g , порождающий мультипликативную группу G . Полагаем

$$h = g^{(p^2-1)/8}.$$

Как и раньше, $h^4 = -1$. Снова получаем, что либо $h + 1/h$, либо $h - 1/h$ лежит в F_p . И нам надо показать, что в этом случае $h - 1/h \in F_p$ (тогда получается, что -2 — квадратичный вычет в F_p , а раз -1 — невычет, то 2 — невычет).

Итак, покажем, что $h + 1/h \notin F_p$.

Пусть $g = u + vi, u, v \in F_p$. Тогда

$$\frac{1}{g} = \frac{u - vi}{u^2 + v^2}.$$

Имеем

$$h + 1/h = (u + vi)^{(p^2-1)/8} + \frac{(u - vi)^{(p^2-1)/8}}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Пусть $h = U + Vi = (u + vi)^{(p^2-1)/8}, U, V \in F_p$. Тогда

$$h + 1/h = U + Vi + \frac{U - Vi}{(u^2 + v^2)^{(p^2-1)/8}}.$$

Это может лежать в F_p , только если

$$V - \frac{V}{(u^2 + v^2)^{(p^2-1)/8}} = 0.$$

$V = 0$ быть не может, ведь $U + Vi = h$, а h не лежит в F_p — потому что $h^4 = -1$, а -1 у нас квадратичный невычет. Значит, на V можно сократить, и

$$(u^2 + v^2)^{(p^2-1)/8} = 1.$$

На первый взгляд, тут нет никакого противоречия. Но добавим ещё такое замечание: $u^2 + v^2$ должно быть первообразным корнем в F_p . Действительно, в поле G норма $\|a + bi\| = a^2 + b^2 \in F_p$ мультипликативна (легко проверить). Чтобы порождать мультипликативную группу поля G , $g = u + vi$ должно обладать таким свойством, что $(u^2 + v^2)^k, k \geq 0$ должно пробегать все элементы в F_p вида $a^2 + b^2, a, b \in F_p$. Поскольку $a^2 + b^2, a, b \in F_p$ пробегает все вычеты $\bmod p$ (см. утверждение ниже), то $u^2 + v^2$ — порождает мультипликативную группу F_p . А тогда $(u^2 + v^2)^{(p-1)/2} = -1$, и в силу нечётности $\frac{p+1}{4}$

$$(u^2 + v^2)^{(p^2-1)/8} = -1.$$

Противоречие.

Утверждение 1.2. $a^2 + b^2, a, b \in F_p$ пробегает все элементы F_p .

Proof. Ясно, что в виде $a^2 + b^2$ можно представить любой квадратичный вычет в F_p (надо взять $b = 0$). Осталось показать, что в таком виде можно представить хотя бы один квадратичный невычет $s \in F_p$ — ведь любой другой квадратичный невычет представляется в виде $cz^2, z \in F_p$ (потому что частное двух квадратичных невычетов — квадратичный вычет). Ясно, что есть квадратичный вычет s , такой, что $s + 1$ — квадратичный невычет (если бы это было не так, то по индукции бы получили, что $0, 1, 2, \dots, p-1$ — все квадратичные вычеты, что неправда). Тогда $s = a^2, s + 1 = a^2 + 1$, и мы представили квадратичный невычет s в виде суммы двух квадратов. Доказательство окончено. \square

5. Ясно, что $K(\sqrt{a} + \sqrt{b}) \subseteq K(\sqrt{a}, \sqrt{b})$. Покажем, что

$$K(\sqrt{a}, \sqrt{b}) \subseteq K(\sqrt{a} + \sqrt{b}).$$

Имеем

$$\sqrt{a} - \sqrt{b} = \frac{a - b}{\sqrt{a} + \sqrt{b}} \in K(\sqrt{a} + \sqrt{b}).$$

Ну а тогда

$$\sqrt{a} = \frac{1}{2}((\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b})) \in K(\sqrt{a} + \sqrt{b}).$$

И аналогично для \sqrt{b} . А всё потому, что в поле характеристики, отличной от 2, элемент 2 обратим. А если характеристика поля равна 2, то это не обязательно так. Пример:

6. Потом.

7. q — степень простого числа. Сколько неприводимых многочленов степени 42 над F_q ? Решим сначала, когда $q = p$ — простое число. Пусть P_k — произведение всех приведённых неприводимых многочленов степени k над F_p . Имеем тогда

$$x^{p^{42}} - x = P_1 P_2 P_3 P_6 P_7 P_{14} P_{21} P_{42},$$

$$x^{p^{21}} - x = P_1 P_3 P_7 P_{21}.$$

Отсюда

$$\frac{x^{p^{42}} - x}{x^{p^{21}} - x} = P_2 P_6 P_{14} P_{42}.$$

Далее,

$$\begin{aligned} x^{p^{14}} - x &= P_1 P_2 P_7 P_{14}, \\ \frac{x^{p^{42}} - x}{(x^{p^{21}} - x)(x^{p^{14}} - x)} &= \frac{P_6 P_{42}}{P_1 P_7}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^7} - x &= P_1 P_7, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)} &= P_6 P_{42}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^6} - x &= P_1 P_2 P_3 P_6, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= \frac{P_{42}}{P_1 P_2 P_3}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^3} - x &= P_1 P_3, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= \frac{P_{42}}{P_2}. \end{aligned}$$

Далее,

$$\begin{aligned} x^{p^2} - x &= P_1 P_2, \\ \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)(x^{p^2} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)} &= P_{42} P_1. \end{aligned}$$

Но $P_1 = x^p - x$. Итак,

$$P_{42} = \frac{(x^{p^{42}} - x)(x^{p^7} - x)(x^{p^3} - x)(x^{p^2} - x)}{(x^{p^{21}} - x)(x^{p^{14}} - x)(x^{p^6} - x)(x^p - x)}.$$

Приравняем степени. Получаем, что количество многочленов, входящих в произведение P_{42} , равно

$$\frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Это как раз то, что мы искали. Но как быть для случая F_q ?

Итак, решаем задачу в общем случае. Пусть Q_k — количество неприводимых многочленов степени k со старшим коэффициентом 1 над F_q , где q — степень простого числа. Напишем рекуррентные соотношения для Q_k :

$$Q_1 = q,$$

$$Q_k = q^k - \sum_{s=1}^k \sum_{\substack{0 < i_1 \leq i_2 \leq \dots \leq i_s \\ i_1 t_1 + \dots + i_s t_s = k \\ t_1 + \dots + t_s > 1}} \binom{Q_{i_1} + t_1 - 1}{t_1} \dots \binom{Q_{i_s} + t_s - 1}{t_s}, k > 1.$$

Поясним, откуда берётся такая рекуррентная формула. Мы вычитаем из общего количества многочленов степени k со старшим коэффициентом 1 количество приводимых многочленов. Количество приводимых многочленов мы считаем с помощью суммирования по всевозможным разложениям на неприводимые множители. i_r соответствуют степеням неприводимых множителей, t_r — количество неприводимых многочленов степени i_r в разложении. $\binom{Q_{i_r} + t_r - 1}{t_r}$ — это количество сочетаний с повторениями из Q_{i_r} различных неприводимых многочленов степени i_r по t_r .

А теперь определим последовательность многочленов $H_k(x)$:

$$H_1(x) = x,$$

$$H_k(x) = x^k - \sum_{s=1}^k \sum_{\substack{0 < i_1 \leq i_2 \leq \dots \leq i_s \\ i_1 t_1 + \dots + i_s t_s = k \\ t_1 + \dots + t_s > 1}} \frac{(H_{i_1}(x) + t_1 - 1) \dots H_{i_1}(x)}{t_1!} \dots \frac{(H_{i_s}(x) + t_s - 1) \dots H_{i_s}(x)}{t_s!},$$

$$k > 1.$$

Ясно, что $Q_k = H_k(q)$, причём, заметим, H_k не зависит от q . Если $q = p$ — простое, то, как мы видели,

$$Q_{42} = \frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Отсюда для простого p

$$H_{42}(p) = \frac{p^{42} - p^{21} - p^{14} + p^7 - p^6 + p^3 + p^2 - p}{42}.$$

Так как простых чисел бесконечно много, то

$$H_{42}(x) = \frac{x^{42} - x^{21} - x^{14} + x^7 - x^6 + x^3 + x^2 - x}{42}.$$

Значит,

$$Q_{42} = H_{42}(q) = \frac{q^{42} - q^{21} - q^{14} + q^7 - q^6 + q^3 + q^2 - q}{42}.$$

Ответ: количество неприводимых многочленов степени 42 над F_q со старшим коэффициентом 1 есть

$$\frac{q^{42} - q^{21} - q^{14} + q^7 - q^6 + q^3 + q^2 - q}{42}.$$

2 Листок 2

1. Не буду решать.

2. Степень расширения $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}]$ равна произведению степеней $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_{s+1}}] : \mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_s}]]$. А каждая из этих степеней — 1 или 2. Поэтому степень расширения $[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}]$ — это степень двойки. Если бы там был $\sqrt[3]{2}$, то было бы

$$[\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{n_1}, \dots, \sqrt{n_m}] : \mathbb{Q}[\sqrt[3]{2}]] [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}].$$

Но $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ — это 3. А слева степень двойки, она на 3 не делится. Противоречие.

3. Работаем в поле разложения многочлена $x^3 - x - a$. Имеем

$$x^3 - x - a = (x - \alpha)(x - \beta)(x - \gamma).$$

Отсюда, приравнявая коэффициенты, получаем

$$\alpha + \beta + \gamma = 0,$$

$$\alpha\beta + \beta\gamma + \alpha\gamma = -1,$$

$$\alpha\beta\gamma = a.$$

Далее, из предыдущих равенств

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \alpha\gamma) = 2,$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \beta\gamma + \alpha\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = 1.$$

Теперь имеем

$$(3\alpha^2 - 1)(3\beta^2 - 1)(3\gamma^2 - 1) = 27\alpha^2\beta^2\gamma^2 - 9(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3(\alpha^2 + \beta^2 + \gamma^2) - 1 = 27a^2 - 4.$$

Из равенств $\alpha\beta\gamma = a$, $\alpha^3 - \alpha = a$ получаем

$$\alpha\beta\gamma = \alpha^3 - \alpha,$$

$$\beta\gamma = \alpha^2 - 1.$$

Аналогично, $\alpha\beta = \gamma^2 - 1$, $\alpha\gamma = \beta^2 - 1$. Имеем

$$(\alpha - \beta)(\beta - \gamma) = \alpha\beta - \beta^2 - \alpha\gamma + \beta\gamma = (\alpha + \gamma)\beta - \beta^2 - \alpha\gamma = -2\beta^2 - \alpha\gamma = -2\beta^2 - (\beta^2 - 1) = 1 - 3\beta^2.$$

Аналогично, $(\beta - \gamma)(\gamma - \alpha) = 1 - 3\gamma^2$, $(\gamma - \alpha)(\alpha - \beta) = 1 - 3\alpha^2$. Итак,

$$4 - 27a^2 = (1 - 3\alpha^2)(1 - 3\beta^2)(1 - 3\gamma^2) = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

Осталось показать, что $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$ лежит в F_p . Рассмотрим в поле разложения многочлена $x^3 - x - a$, то есть $F_p[\alpha, \beta, \gamma]$, автоморфизм Фробениуса $x \rightarrow x^p$. Как известно, он оставляет на местах элементы F_p и только их. Кроме того, ясно, что корни многочлена $x^3 - x - a$ переходят в его же корни, поэтому α, β, γ переставляются этим автоморфизмом. Но поскольку эти корни не лежат в F_p , ни один из них не переходит в себя. А все перестановки множества из трёх элементов, не оставляющие на месте ни один из них, чётные. Поэтому наш автоморфизм производит чётную перестановку α, β, γ , а значит, переводит $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$ в себя. А кто переходит в себя, тот лежит в F_p . Всё доказано.

4. Существует ли неприводимый над \mathbb{Q} многочлен, который приводим над \mathbb{F}_p для всех p ? Да, существует, и это $x^4 + 1$. Докажем, что он приводим над \mathbb{F}_p для любого p . Для $p = 2$ это легко видеть. Для $p > 2$ имеем несколько вариантов

- 2 — квадратичный вычет по модулю p , $\alpha^2 = 2 \pmod{p}$. Над \mathbb{F}_p

$$\begin{aligned}(x^2 - \alpha x + 1)(x^2 + \alpha x + 1) &= (x^2 + 1)^2 - \alpha^2 x^2 = \\ &= x^4 + 2x^2 + 1 - \alpha^2 x^2 = x^4 + 2x^2 + 1 - 2x^2 = x^4 + 1.\end{aligned}$$

- -2 — квадратичный вычет по модулю p , $\alpha^2 = -2 \pmod{p}$. Над \mathbb{F}_p

$$\begin{aligned}(x^2 - \alpha x - 1)(x^2 + \alpha x - 1) &= (x^2 - 1)^2 - \alpha^2 x^2 = \\ &= x^4 - 2x^2 + 1 - \alpha^2 x^2 = x^4 - 2x^2 + 1 + 2x^2 = x^4 + 1.\end{aligned}$$

- И 2 , и -2 — невычеты по модулю p . Тогда -1 — вычет. $\gamma^2 = -1$. Над \mathbb{F}_p

$$(x^2 - \gamma)(x^2 - 1/\gamma) = x^4 - (\gamma + 1/\gamma)x^2 + 1 = x^4 + 1.$$

Итак, приводимость над \mathbb{F}_p доказана. А как проверить неприводимость над \mathbb{Q} ? Предположим, что для $a_1, a_2, b_1, b_2 \in \mathbb{Q}$

$$x^4 + 1 = (x^2 + a_1x + b_1)(x^2 + a_2x + b_2).$$

Отсюда имеем

$$x^4 + 1 = x^4 + (a_1 + a_2)x^3 + (a_1a_2 + b_1 + b_2)x^2 + (a_1b_2 + a_2b_1)x + b_1b_2.$$

Из сравнения коэффициентов при x^3 имеем

$$a_2 = -a_1.$$

Теперь из коэффициента при x

$$a_1(b_2 - b_1) = 0.$$

Имеем два варианта

- $a_1 = a_2 = 0$. Тогда

$$b_1 + b_2 = 0, b_1b_2 = 1.$$

Этого для рациональных (и потому действительных) b_1, b_2 быть не может.

- $b_1 = b_2$. Пусть $a = a_1 = -a_2, b = b_1 = b_2$. Имеем

$$2b - a^2 = 0, b^2 = 1.$$

Тогда $b = \pm 1, a^2 = \pm 2$, чего в рациональных числах не бывает.

Итак, $x^4 + 1$ не раскладывается над \mathbb{Q} в произведение двух квадратных трёхчленов. Остаётся проверить, что у него нет рациональных корней. Но у него их нет, у него ведь вообще нет действительных корней, тем более рациональных. Всё доказано.

5.

6.

7. Выберем наименьшее нечётное число $k > 1$, для которого существует формально вещественное поле F и его расширение степени k , не являющееся формально вещественным. Рассмотрим такое поле F и соответствующее его расширение. Это расширение простое, то есть получается как $F[x]/(f(x))$ для неприводимого f , потому что иначе мы бы реализовали его как последовательность простых расширений (нечётных степеней), и на каком-то этапе формальная вещественность бы исчезла, а степень такого промежуточного расширения была бы меньше k — противоречие с минимальностью k .

Итак, у нас есть поле F и неприводимый многочлен $f(x)$ нечётной степени k , такие, что F формально вещественно, а $F[x]/(f(x))$ нет. То есть существуют многочлены $f_1(x), \dots, f_n(x)$ степеней меньше k , такие, что $f_1(x)^2 + \dots + f_n(x)^2 + 1$ делится на $f(x)$ (в поле $F[x]$). То есть

$$f_1(x)^2 + \dots + f_n(x)^2 + 1 = h(x)f(x),$$

где $h(x) \in F[x]$ — некоторый многочлен. Но степень многочлена

$$f_1(x)^2 + \dots + f_n(x)^2 + 1$$

меньше $2k$ (так как степень каждого $f_i(x)$ меньше k) и чётна. Отсюда следует, что степень $h(x)$ меньше k и нечётна. Разложим $h(x)$ на неприводимые над $F[x]$ множители:

$$h(x) = h_1(x) \dots h_m(x).$$

Если среди этих множителей есть множитель степени 1, то есть многочлен вида $x - \alpha, \alpha \in F$, то

$$f_1(\alpha)^2 + \dots + f_n(\alpha)^2 + 1 = 0,$$

что противоречит формальной вещественности F . Значит все множители $h_i(x)$ имеют степень больше 1. Но поскольку степень $h(x)$ нечётна, то степень одного из $h_i(x)$ также нечётна. Пусть это $h_s(x)$. Тогда $F(x)/(h_s(x))$ — тоже расширение F нечётной степени, не являющееся формально вещественным. Но его степень меньше k . Противоречие с минимальностью k . Доказательство окончено.

3 Листок 3

1. $\alpha_1, \dots, \alpha_n$ — корни $f(x)$, $p_m = \sum_{i=1}^n \alpha_i^m$. Через $\det(u_1, \dots, u_n)$ мы будем обозначать детерминант матрицы, образованной столбцами u_1, \dots, u_n . Пусть A_i — это матрица

$$A_i = \begin{pmatrix} 1 & \alpha_i & \dots & \alpha_i^{n-1} \\ \alpha_i & \alpha_i^2 & \dots & \alpha_i^n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_i^{n-1} & \alpha_i^n & \dots & \alpha_i^{2n-2} \end{pmatrix}$$

Тогда детерминант, о котором речь в условии, это

$$\det(A_1 + A_2 + \dots + A_n).$$

Его мы сейчас и посчитаем (и покажем, что он равен дискриминанту f). Детерминант суммы матриц можно записать так:

$$\det(A_1 + \dots + A_n) = \sum_{i_1, \dots, i_n} \det(A_{i_1,1}, A_{i_2,2}, \dots, A_{i_n,n}).$$

Здесь $A_{i_s,s}$ — s -ый столбец матрицы A_{i_s} . Ну, то есть сумма всевозможных детерминантов матриц, в которых из одной из суммируемых матриц A_i взят первый столбец и поставлен на место первого столбца, из другой взят второй столбец и поставлен на место второго и т.д. Заметим, что в рассматриваемой сумме

$$\sum_{i_1, \dots, i_n} \det(A_{i_1,1}, A_{i_2,2}, \dots, A_{i_n,n}).$$

слагаемые, в которых некоторые i_s совпадают, обращаются в 0, поскольку любые два столбца каждой матрицы A_i пропорциональны. Значит, сумма на самом деле не по всем последовательностям из $1, \dots, n$, а по всем перестановкам чисел $1, \dots, n$. И эта сумма равна (выносим из столбцов множители вида α_i^k)

$$\begin{aligned} \sum_{i_1, \dots, i_n} \det(A_{i_1,1}, A_{i_2,2}, \dots, A_{i_n,n}) &= \\ &= \sum_{i_1, \dots, i_n} \alpha_{i_2} \alpha_{i_3}^2 \dots \alpha_{i_n}^{n-1} \det(A'_{i_1,1}, \dots, A'_{i_n,n}). \end{aligned}$$

Здесь

$$A'_i = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_i & \alpha_i & \dots & \alpha_i \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_i^{n-1} & \alpha_i^{n-1} & \dots & \alpha_i^{n-1} \end{pmatrix}$$

Ясно, что $\det(A'_{i_1,1}, \dots, A'_{i_n,n})$ равен знаку перестановки i_1, \dots, i_n , который мы обозначим через $s(i_1, \dots, i_n)$, умноженному на детерминант матрицы

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}$$

А детерминант этой матрицы — это определитель Вандермонда

$$V = \prod_{i < j} (\alpha_j - \alpha_i).$$

Итак,

$$\begin{aligned}\det(A_1 + A_2 + \dots + A_n) &= \\ &= \sum_{i_1, \dots, i_n} \alpha_{i_2} \alpha_{i_3}^2 \dots \alpha_{i_n}^{n-1} \det(A'_{i_1,1}, \dots, A'_{i_n,n}) = \\ &= V \times \sum_{i_1, \dots, i_n} s(i_1, \dots, i_n) \alpha_{i_2} \alpha_{i_3}^2 \dots \alpha_{i_n}^{n-1}.\end{aligned}$$

Осталось найти

$$\sum_{i_1, \dots, i_n} s(i_1, \dots, i_n) \alpha_{i_2} \alpha_{i_3}^2 \dots \alpha_{i_n}^{n-1}.$$

Но это есть полное разложение определителя матрицы

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{pmatrix}$$

То есть

$$\sum_{i_1, \dots, i_n} s(i_1, \dots, i_n) \alpha_{i_2} \alpha_{i_3}^2 \dots \alpha_{i_n}^{n-1} = V.$$

В итоге,

$$\det(A_1 + A_2 + \dots + A_n) = V^2 = \text{disc}(f).$$

2. Найдём дискриминант многочлена $\frac{x^n-1}{x-1}, n > 2$. Для этого будем пользоваться формулой из предыдущей задачи. Пусть $\varepsilon_1, \dots, \varepsilon_{n-1}$ — корни $\frac{x^n-1}{x-1}$. Пусть $\varepsilon_0 = 1$.

$$p_m = \varepsilon_1^m + \dots + \varepsilon_{n-1}^m.$$

Найдём p_m . Пусть $S_m = \sum_{i=0}^n \varepsilon_i^m$. Тогда $p_m = S_m - 1$. Умножение на ε_k только переставляет ε_i , поэтому

$$\varepsilon_k^m S_m = S_m.$$

Значит, $S_m = 0$, если только не все $\varepsilon_k^m = 1$. Последнее бывает в случае m делящегося на n , и только. Итак, $p_m = -1$ при m не делящемся на n и $p_m = n - 1$ иначе. Теперь наш определитель для дискриминанта принимает вид определителя матрицы $(n-1) \times (n-1)$

$$\begin{pmatrix} n-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & n-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & n-1 & \dots & -1 \end{pmatrix}$$

Несколько раз переставляя столбцы, можно добиться того, чтобы все $n-1$ стояли на главной диагонали, а все элементы вне главной диагонали были -1 . Для этого надо сделать

$$(n-4) + (n-5) + \dots + 2 + 1 = \frac{(n-4)(n-3)}{2}$$

перестановок столбцов. Итак, наш дискриминант равен

$$(-1)^{\frac{(n-4)(n-3)}{2}} \det \begin{pmatrix} n-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \dots & n-1 \end{pmatrix}$$

Теперь отнимаем второй столбец от всех остальных и получаем

$$(-1)^{\frac{(n-4)(n-3)}{2}} \det \begin{pmatrix} n & -1 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & -1 & n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -1 & 0 & \dots & n \end{pmatrix}$$

Теперь меняем знак у второго столбца и переставляем первый и второй столбцы, получаем

$$(-1)^{\frac{(n-4)(n-3)}{2}} \det \begin{pmatrix} 1 & n & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & n \end{pmatrix}$$

Вынося n из всех столбцов, кроме первого, получаем

$$(-1)^{\frac{(n-4)(n-3)}{2}} n^{n-2} \det \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Теперь от первого столбца отнимаем все остальные столбцы, получаем

$$(-1)^{\frac{(n-4)(n-3)}{2}} n^{n-2} \det \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Ну а оставшийся детерминант равен -1 (можно переставить первые два столбца, будет единичная матрица), поэтому получаем ответ.

Ответ: $\text{disc}\left(\frac{x^n-1}{x-1}\right) = (-1)^{\frac{(n-3)(n-4)}{2}+1} n^{n-2} = (-1)^{\frac{n(n+1)}{2}+1} n^{n-2}$.

3.

4.

5.

6.

7. Автоморфизм поля $\overline{\mathbb{F}}_p$, не являющийся степенью автоморфизма Фробениуса. Алгебраическое замыкание поля \mathbb{F}_p можно представить как объединение последовательности вложенных друг в друга полей $\mathbb{F}_{p^{n!}}$. На каждом из этих полей можно задать какой-то автоморфизм, но он с необходимостью будет степенью автоморфизма Фробениуса. Значит, единственная возможность — задать согласованно на этих подполях степени автоморфизма Фробениуса, но так, чтоб эти степени были разные, но при этом автоморфизмы были согласованы.

Теперь опишем решение формально. Пусть

$$k_n = 1 + p^{1!} + p^{2!} + \dots + p^{(n-1)!}.$$

Зададим на вложенных друг в друга $\mathbb{F}_{p^{n!}}$ полях автоморфизм ϕ так:

$$\phi(x) = x^{p^{k_n}}, x \in \mathbb{F}_{p^{n!}}.$$

Согласованность следует из того, что при $m > n$ $k_m - k_n$ делится на $n!$. Значит, автоморфизм ϕ на $\overline{\mathbb{F}}_p$ определён корректно, а быть фиксированной степенью M автоморфизма Фробениуса он не может, так как на $\mathbb{F}_{p^{n!}}$ при больших n минимальная степень Фробениуса, которой является наш автоморфизм, есть $k_n < p^{n!}$ (то есть наш автоморфизм на $\mathbb{F}_{p^{n!}}$ есть степень k_n автоморфизма Фробениуса, или $k_n + n!$, или $k_n + 2n!$, или \dots , но никак не нечто иное).

4 Листок 4

1.

2.

3. $E \subset F \subset K$ — поля, $[K : E] < \infty$.

а) Если K/E нормально, то и K/F нормально. Итак, пусть K/E нормально. Покажем, что K/F нормально. Пусть f — неприводимый над F многочлен, имеющий корень k в K . Нам надо показать, что все корни f лежат в K . Пусть g — минимальный многочлен k над E . Тогда все корни g лежат в K , поскольку K/E нормально. Но f — минимальный многочлен k над F , а g — это тоже многочлен с коэффициентами из F , такой, что $g(k) = 0$. Значит, g делится на f . Поэтому все корни f лежат среди корней g , и, значит, они все лежат в K .

б) Если K/F нормально и F/E нормально, верно ли, что K/E нормально?

Приведём пример, когда это не так. Пусть $E = \mathbb{Q}$, $F = \mathbb{Q}[\sqrt{2}]$, $K = \mathbb{Q}[\sqrt[4]{2}]$. Тогда F/E нормально, поскольку $\mathbb{Q}[\sqrt{2}]$ — это поле разложения $x^2 - 2$ над \mathbb{Q} . K/F нормально, поскольку $\mathbb{Q}[\sqrt[4]{2}]$ — это поле разложения $x^2 - \sqrt{2}$ над $\mathbb{Q}[\sqrt{2}]$. Но K/E — не нормально, поскольку неприводимый над \mathbb{Q} многочлен $x^4 - 2$ имеет корень $\sqrt[4]{2}$ в поле $\mathbb{Q}[\sqrt[4]{2}]$, но его корень $i\sqrt[4]{2}$ не лежит в этом поле, ведь он мнимый, а поле $\mathbb{Q}[\sqrt[4]{2}]$ вкладывается в \mathbb{R} .

4.

5. Существует конечно много полей K , таких, что $F \subset K \subset F(a, b)$. Рассмотрим для каждого $f \in F$ поле $F(a + fb)$. Таких различных полей конечно много, поэтому для каких-то двух различных $f_1, f_2 \in F$ имеет место $F(a + f_1b) = F(a + f_2b)$. Тогда $a + f_2b \in F(a + f_1b)$. Но тогда $a, b \in F(a + f_1b)$. Вот и всё, $F(a, b) = F(a + f_1b)$.
6. $F(\alpha)$ — конечное расширение F . Покажем, что существует лишь конечное число промежуточных полей $F \subset K \subset F(\alpha)$. Как сказано в указании, рассмотрим для каждого такого поля K минимальный многочлен f_K элемента α над K . Таких многочленов конечно много, поскольку все они делят f_F . Теперь покажем, что многочлен f_K однозначно определяет поле K . Пусть K_1 — расширение F , порождённое коэффициентами многочлена f_K . Тогда K_1 лежит в K . Является ли f_K минимальным многочленом для α над K_1 ? Если нет, то существует многочлен g меньшей степени с коэффициентами в K_1 , такой, что $g(\alpha) = 0$. Но коэффициенты этого многочлена лежат и в K , поскольку K содержит K_1 , а это противоречит тому, что f_K — минимальный многочлен для α над K . Противоречие. Итак, f_K — минимальный многочлен для α над K_1 . Значит,

$$[F(\alpha) : K_1] = \deg f_K = [F(\alpha) : K].$$

Но тогда, применяя лемму о башне, получаем

$$[K_1 : F] = [K : F].$$

А из вложенности K_1 в K следует, что $K_1 = K$. Итак, по минимальному многочлену f_K поле K однозначно восстанавливается как минимальное расширение F , содержащее все коэффициенты f_K . Поэтому и промежуточных полей конечно много, как и минимальных многочленов.

7. Предъявим бесконечно много полей K , таких, что

$$\mathbb{F}_p(x^p, y^p) \subset K \subset \mathbb{F}_p(x, y).$$

Доказательство проведём в несколько этапов.

- Расширение $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$ имеет степень не меньше p^2 . Для этого заметим, что элементы

$$x^k y^l, 1 \leq k \leq p-1, 1 \leq l \leq p-1$$

линейно независимы над $\mathbb{F}(x^p, y^p)$. Действительно, если есть равенство

$$\sum_{1 \leq k, l \leq p-1} \frac{U_{kl}(x^p, y^p)}{V(x^p, y^p)} x^k y^l = 0,$$

где U_{kl}, V — многочлены, то

$$\sum_{1 \leq k, l \leq p-1} U_{kl}(x^p, y^p) x^k y^l = 0,$$

и тогда каждое слагаемое тут равно нулю, потому что разные слагаемые имеют разные остатки степеней коэффициентов по модулю p , и

$$U_{kl} = 0, 1 \leq k, l \leq p-1.$$

- Если $\beta \in \mathbb{F}_p(x^p, y^p)$, то $\mathbb{F}_p(x^p, y^p, x + \beta y)$ не совпадает с $\mathbb{F}_p(x, y)$. Действительно, $(x + \beta y)^p - (x^p + \beta^p y^p) = 0$, и минимальный многочлен для $x + \beta y$ имеет степень p или ниже. Значит, степень расширения

$$\mathbb{F}_p(x^p, y^p, x + \beta y) / \mathbb{F}_p(x^p, y^p)$$

не выше p , и

$$\mathbb{F}_p(x^p, y^p, x + \beta y) \neq \mathbb{F}_p(x, y).$$

Значит, для любых двух различных $\beta_1, \beta_2 \in \mathbb{F}_p(x^p, y^p)$

$$\mathbb{F}_p(x^p, y^p, x + \beta_1 y) \neq \mathbb{F}_p(x^p, y^p, x + \beta_2 y).$$

Действительно, если

$$x + \beta_1 y \in \mathbb{F}_p(x^p, y^p, x + \beta_2 y),$$

то $x, y \in \mathbb{F}_p(x^p, y^p, x + \beta_2 y)$, и

$$\mathbb{F}_p(x^p, y^p, x + \beta_2 y) = \mathbb{F}_p(x, y),$$

а мы выяснили, что это не так. Вот мы и получили бесконечно много различных промежуточных полей:

$$\mathbb{F}_p(x^p, y^p, x + \beta y), \beta \in \mathbb{F}_p(x^p, y^p).$$

- Хотя, надо ещё заметить, что само поле $\mathbb{F}_p(x^p, y^p)$ бесконечно, иначе мы не найдём там бесконечно много различных β . Но вот в нём бесконечно много различных элементов:

$$x^{np}, n \in \mathbb{N}.$$

8. Докажем индукцией по n , что для различных простых p_1, \dots, p_n одновременно выполнены следующие два свойства:

- Степень расширения $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}]$ равна 2^n , то есть $\sqrt{p_{i_1}} \dots \sqrt{p_{i_s}}$ линейно независимы.
- Для любого простого p , отличного от p_1, \dots, p_n , и целого числа $Z \neq 0$, взаимно простого с p , не существует $A \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ со свойством

$$A^2 = \frac{p}{Z}.$$

База индукции: для простого p_1 первое свойство очевидно, докажем второе. Каждый элемент $A \in \mathbb{Q}(\sqrt{p_1})$ единственным образом представляется в виде

$$a + b\sqrt{p_1}, a, b \in \mathbb{Q}.$$

Значит, $A^2 = \frac{p}{Z}$ пишется как

$$(a + b\sqrt{p_1})^2 = \frac{p}{Z},$$

$$a^2 + b^2 p_1 + 2ab\sqrt{p_1} - \frac{p}{Z} = 0.$$

Отсюда получаем

$$a^2 + b^2 p_1 = \frac{p}{Z}, 2ab = 0.$$

Имеем два случая:

- $a = 0, p = b^2 p_1,$
- $b = 0, a^2 = \frac{p}{Z}.$

Ни один из этих случаев не может быть реализован в силу основной теоремы арифметики.

Индукционный переход: от n к $n+1$. Чтобы показать, что степень $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n+1}}) : \mathbb{Q}]$ равна 2^{n+1} , достаточно показать, что $\sqrt{p_{n+1}}$ не содержится в $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ (а дальше просто лемма о башне). Предположим, что это не так, и

$$\sqrt{p_{n+1}} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}).$$

Тогда p_{n+1} представляется как квадрат элемента из $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$, что противоречит предположению индукции (второму свойству).

Осталось показать, что второе свойство также выполнено для $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n+1}})$. Предположим, что это не так, и для некоторого простого p ,

$$p \neq p_i, i = 1, \dots, n+1,$$

и целого Z имеем

$$\frac{p}{Z} = A^2, A \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n+1}}).$$

Тогда по доказанному первому утверждению A однозначно представляется в виде

$$A = R + S\sqrt{p_{n+1}}, R, S \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}).$$

Итак,

$$(R + S\sqrt{p_{n+1}})^2 = \frac{p}{Z},$$

$$R^2 + S^2 p_{n+1} + 2RS\sqrt{p_{n+1}} = \frac{p}{Z},$$

$$2RS\sqrt{p_{n+1}} = \frac{p}{Z} - R^2 - S^2 p_{n+1}.$$

И $2RS$, и $\frac{p}{Z} - R^2 - S^2 p_{n+1}$ лежат в $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. Поэтому, если $RS \neq 0$, $\sqrt{p_{n+1}}$ тоже там лежит, что, как мы уже узнали, неправда. Поэтому

$$RS = 0, \frac{p}{Z} - R^2 - S^2 p_{n+1} = 0.$$

Имеем два случая:

- $R = 0, \frac{p}{Z} = S^2 p_{n+1}$, тогда

$$S^2 = \frac{p}{Z p_{n+1}},$$

и это противоречит предположению индукции.

- $S = 0, \frac{p}{Z} = R^2$. Это тоже противоречит предположению индукции.

Всё доказано.