Алгебра 2 2023 Кузнецов

1 Листок 1

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

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

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

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

   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

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

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

   $$a_1 + \ldots + a_k,$$

   $$a_1a_2 + \ldots + a_{k-1}a_k,$$

   $$\ldots$$

   $$a_1 \ldots a_k$$

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

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

— 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 мультипликатиной 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 $f(\frac{1}{\alpha}) = f(\overline{\alpha}) = 0$). Значит, эти многочлены не взаимно просты, и в силу неприводимости f должны иметь все корни общие. То есть эти многолены пропорциональны:

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

Отсюда $c_k = tc_{n-k}$ 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. Воспользуемсяя 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 $3s \vdots p-1$. 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

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

Звдача 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:

- $p \equiv 1 (\mod 8)$. 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.
- $p \equiv -1 (\mod 8)$. Это более сложный случай. По задаче 3a, -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):

$$x^4+1=(x^2-h^2)(x^2-1/h^2),$$
$$x^4+1=(x^2-(h+1/h)x+1)(x^2+(h+1/h)x+1),$$
$$x^4+1=(x^2-(h-1/h)x-1)(x^2+(h-1/h)x-1).$$

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 вариантво реализуется, у нас получится позже. □

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.

- $p \equiv -3(\mod 8)$. Предположим,

$$s^2 \equiv 2(\mod p).$$

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

$$j^2 \equiv -1(\mod p).$$

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

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

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.

- $p \equiv 3(\mod 8)$. Это самый сложный случай. Поначалу можно рассуждать, как в случае $p \equiv -1(\mod 8)$. 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 $\mod p$ (см. утвержение 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 представвить хотя бы один квадратичный невычет $c \in F_p$ — 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, ..., 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. □

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: