Поля, расширения полей. Конечные поля.

Задача 1 (трансцендентные расширения). a) Пусть x трансцендентен (т.е. не алгебраичен) над полем F, а $K \subset F(x)$ — подполе, не совпадающее с F. Покажите, что элемент x алгебраичен над K.

b) Пусть x трансцендентен над полем F, а $\sigma : F \to E$ — вложение F в некоторое поле E. При каких условиях и сколькими способами σ продолжается до вложения $F(x)$ в E?

Задача 2 (вложения $\mathbb{R}$ и $\mathbb{C}$). a) Покажите, что всякий гомоморфизм полей из $\mathbb{R}$ в $\mathbb{R}$ биективен.

b) (для знакомых с базисами трансцендентности) Докажите, что $\mathbb{C}$ изоморфно бесконечному числу своих собственных подполей.

c) Покажите, что группа $\mathrm{Aut}(\mathbb{C})$ автоморфизмов поля $\mathbb{C}$ несчётна.

Задача 3° (поля разложения). [1] a) Докажите, что степень поля разложения многочлена степени n делит $n!$.

b) Сколько корней в $\mathbb{F}_{16}$ имеют многочлены $x^3 - 1, x^4 - 1, x^{15} - 1, x^{17} - 1$? Постройте их поля разложения.

c) Разложите на неприводимые множители многочлен $x^4 + 1$ над полями $\mathbb{F}_5$, $\mathbb{F}_{25}$ и $\mathbb{F}_{125}$. Найдите его поле разложения.

d) Постройте поле разложения многочлена $x^5 - 2$ над $\mathbb{Q}$.

e) Покажите, что многочлен $x^p - x - a$ над полем характеристики p либо неприводим, либо разлагается на линейные множители.

f) Найдите поле разложения многочлена $x^{p^m} - 1 \in \mathbb{F}_p[x]$. Какова его степень над $\mathbb{F}_p$?

g) Пусть K — поле, полученное из $\mathbb{F}_p$ присоединением всех корней l-ой степени из 1 для всех простых $l \neq p$. Покажите, что K алгебраически замкнуто.

Задача 4 (кубические многочлены). Пусть $\mathrm{char}\, K \neq 2, 3$.

a°) Докажите, что любой кубический многочлен над K может быть приведен к виду $P(x) = x^3 + px + q$ линейной заменой переменной x.

b°) Пусть $\alpha_1, \alpha_2, \alpha_3$ — корни $P(x)$ в некотором алгебраическом замыкании поля K. Докажите, что дискриминант $D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_3)^2$ лежит в K. Выразите D через p и q.

c°) Пусть L — поле разложение $P(x)$. Покажите, что $L = K(\alpha_1)$, если D — квадрат в K и $L = K(\sqrt{D}, \alpha_1)$ иначе.

d^*) Обобщите утверждение пункта b) на многочлены произвольной степени. Каков в этом случае аналог утверждения из пункта c)?

Задача 5 (построения циркулем и линейкой). Зафиксируем на плоскости единичный отрезок. Множество E состоит из длин всех отрезков, которые можно построить циркулем и линейкой, чисел, противоположных им, и нуля.

a) Покажите, что E — поле и, если $x \in E, x > 0$, то $\sqrt{x} \in E$.

b) Опишите E алгебраически.

c) Верно ли, что $\sqrt[3]{2} \notin E$? Можно ли в общем случае разделить угол на три равные части с помощью циркуля и линейки? Можно ли построить циркулем и линейкой правильный 7-ми угольник?

d^*) При каких значениях n правильный n-угольник можно построить циркулем и линейкой?

---

[1] Задачи со значком $^\circ$ очень рекомендуется научиться решать.

Задача 6 (неприводимые многочлены над конечными полями). Пусть $q = p^f$ — степень простого числа p, $k = \mathbb{F}_q$ — конечное поле из q элементов. Все многочлены рассматриваются над полем $\mathbb{F}_q$.

a°) Покажите, что неприводимый многочлен $f(x)$ делит $x^{q^n} - x$ тогда и только тогда, когда степень $f(x)$ делит n.

b°) Докажите, что

$$x^{q^n} - x = \prod_{d|n} \prod_{f_d - \text{неприводим}} f_d(x),$$

где произведение берется по всем неприводимым над k многочленам степени d со старшим коэффициентом 1. Выведите отсюда, что $q^n = \sum\limits_{d|n} d\psi(d)$, где $\psi(d)$ — число неприводимых многочленов степени d. Это равенство эквивалентно следующему (вычисление дзета-функции аффинной прямой):

$$\frac{1}{1-qt} = \prod_{d=1}^{\infty} (1-t^d)^{-\psi(d)}.$$

c) Получите равенство $n\psi(n) = \sum\limits_{d|n} \mu(d) q^{n/d}$, где $\mu(d)$ — функция Мёбиуса, равная 0, если d делится на квадрат некоторого простого числа и $(-1)^r$, если $n = p_1 \ldots p_r$ — произведение различных простых чисел (это даёт альтернативное доказательство существования конечных полей $\mathbb{F}_{p^r}$ при $r \geq 2$).

Задача 7 (квадратичный закон взаимности). Пусть $q = p^f$ — степень простого числа p, $k = \mathbb{F}_q$. Напомним, что символ Лежандра $\left(\frac{x}{p}\right)$ для простого числа $p \neq 2$ и $x \in \mathbb{F}_p^*$ равен 1, если x — квадрат в $\mathbb{F}_p$, и -1 иначе.

a°) Покажите, что, если $p = 2$, то каждый элемент поля k является квадратом, а, если $p \neq 2$, то квадраты образуют подгруппу индекса 2 в k^*, которая является ядром гомоморфизма $x \mapsto x^{(q-1)/2}$, принимающего значения ± 1. Выведите из этого, что $\left(\frac{x}{p}\right) = x^{(p-1)/2}$.

b) Докажите, что $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Подсказка: воспользуйтесь тем, что $(\alpha + \alpha^{-1})^2 = 2$, *если* α — *примитивный корень* 8-*ой степени из* 1 *в алгебраическом замыкании поля* $\mathbb{F}_p$.

c) Пусть дано нечётное простое число $l \neq p$, а $\omega \neq 1$ — корень степени l из 1 в алгебраическом замыкании поля $\mathbb{F}_p$. Определим сумму Гаусса $y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) \omega^x$. Докажите, что $y^2 = (-1)^{(l-1)/2} l$.

d) Покажите, что $y^{p-1} = \left(\frac{p}{l}\right)$, и получите отсюда *квадратичный закон взаимности Гаусса*:

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{(p-1)(l-1)/4}.$$

Задача 8 (квадратные уравнения над конечными полями).

a) Пусть $f(x,y) = ax^2 + 2bxy + cy^2$ — квадратичная форма с определителем $d = ac - b^2$. Пусть $d \neq 0$ в $\mathbb{F}_p$. Покажите, что число ненулевых решений уравнения $f(x,y) = 0$ в $\mathbb{F}_p$ равно $(p-1)\left(1 + \left(\frac{-d}{p}\right)\right)$.

b^*) Пусть $p \neq 2$— простое, $f(x_1, \ldots, x_n)$ — квадратичная форма с определителем $d \neq 0$ в $\mathbb{F}_p$. Покажите, что число ненулевых решений уравнения $f(x_1, \ldots, x_n) = 0$ в поле $\mathbb{F}_p$ равно $p^{n-1} - 1 + (p-1)\left(\frac{(-1)^{n/2} d}{p}\right) p^{n/2-1}$ при чётном n и $p^{n-1} - 1$ при нечётном n.

Подсказка: приведите форму f *к виду* $y_1 y_2 + g(y_3, \ldots, y_n)$.

c^*) В предположениях предыдущего пункта найдите число решений в поле $\mathbb{F}_p$ уравнения $f(x_1, \ldots, x_n) = a$.