Круговые расширения

▷ В этом листке ζ_n — корень степени n из единицы; p и q — нечетные простые числа.

Задача 5.1. Пусть L/K — поле разложения многочлена, x_i — его корни, $d = \prod(x_i - x_j)$.
а) Элемент $D := d^2$ (*дискриминант*) лежит в K.
б) Элемент d лежит в K тогда и только тогда, когда группа $\mathrm{Gal}(L/K)$ состоит только из четных перестановок.

Задача 5.2. Пусть L/K — расширение Галуа, $\mathrm{char}\, K \neq 2, 3$.
а) Если $\mathrm{Gal}(L/K) = \mathbb{Z}/2$, то $L = K(\sqrt{a})$.
б) Если $\mathrm{Gal}(L/K) = \mathbb{Z}/3$ и K содержит кубический корень из единицы, то $L = K(\sqrt[3]{a})$.
Указание. При действии образующей σ группы Галуа элемент $\sqrt[3]{a}$ должен домножаться на ζ_3. Как получить элемент с таким свойством из базиса α, $\sigma\alpha$, $\sigma^2\alpha$?

Задача 5.3. Если у многочлена с целыми коэффициентами старший коэффициент не делится на p, а остальные коэффициенты делятся на p, причем свободный член не делится на p^2, то этот многочлен неприводим (“критерий Эйзенштейна”).

Задача 5.4. Круговой многочлен $\Phi_q(x) = \dfrac{x^q - 1}{x - 1}$ неприводим над $\mathbb{Q}$.
Указание. Полезно сделать замену $t = x - 1$.

Задача 5.5. Правильный q-угольник можно построить циркулем и линейкой тогда и только тогда, когда
а) круговое поле $\mathbb{Q}(\zeta_q) = \mathbb{Q}[\zeta]/\Phi_q(\zeta)$ получается из $\mathbb{Q}$ последовательностью квадратичных расширений;
б) q — “простое число Ферма”, т. е. имеет вид $2^l + 1$.

Задача 5.6. У расширения $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ есть ровно одно квадратичное подрасширение L. Пусть $L = \mathbb{Q}(\sqrt{q^*})$, где q^* — целое число, свободное от квадратов.
а) Представьте $\sqrt{q^*}$ как сумму степеней ζ_q с коэффициентами ± 1 (“сумма Гаусса”).
б) Выразите q^* через q.
в) Любое квадратичное расширение поля $\mathbb{Q}$ содержится в круговом.
(Последнее утверждение можно рассматривать как частный случай *теоремы Кронекера–Вебера* о том, что любое абелево расширение поля $\mathbb{Q}$ содержится в круговом.)

▷ Напомним определение *символа Лежандра*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ квадратичный невычет по модулю } p. \end{cases}$$

Задача 5.7. а) Символ Лежандра мультипликативен: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; б) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Задача 5.8. При действии автоморфизма Фробениуса ($x \mapsto x^p$) поля $\mathbb{F}_p[\zeta]/\Phi_q(\zeta)$ сумма Гаусса $S(\zeta, q)$ домножается на а) $\left(\frac{q^*}{p}\right)$; б) $\left(\frac{p}{q}\right)$.
в) Равенство $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ эквивалентно обычному квадратичному закону взаимности,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

г) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Указание. Рассмотрите поле $\mathbb{F}_p(\zeta_8)$.