Круговые поля

Задача 1. a) Докажите *критерий Эйзенштейна.* Пусть K — факториальное кольцо, $p \in K$ — простой элемент. Тогда всякий многочлен $P = a_n x^n + \cdots + a_0$, такой что $p | a_i$ для $0 \leqslant i < n$, $p \not| a_n$, $p^2 \not| a_0$, неразложим над K.

b) Докажите, что при этом P неразложим и над полем частных $F(K)$.

c) Докажите, что для любого поля F многочлен $x^k - t$ неразложим над полем рациональных функций $F((t))$.

d) Докажите, что для любого простого целого p многочлен $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$ неразложим над $\mathbb{Q}$.

Задача 2. Пусть $\zeta_n = \exp(2\pi i/n)$ — корень из единицы n-той степени.

a) Докажите, что $\mathbb{Q}(\zeta_n) = \mathbb{Q}\{x^n - 1\}$, в частности, оно является расширением Галуа $\mathbb{Q}$.

b) Докажите, что $\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$ изоморфна некоторой подгруппе $(\mathbb{Z}/n\mathbb{Z})^*$ — группы обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.

c) Пусть p — простое целое число. Докажите, что $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, в частности, $\mathrm{Gal}(\mathbb{Q}(\zeta_p), \mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Задача 3. a) Пусть $p > 2$ — простое целое число. Докажите, что подполе, соответствующее подгруппе индекса 2 в $\mathbb{Z}/(p-1)\mathbb{Z}$, порождено над $\mathbb{Q}$ корнем из некоторого целого рационального числа p^*.

b) Найдите p^* (с точностью до умножения на полный квадрат).

Hint: В выражении $p = \Phi_p(1) = \prod_i (1 - \zeta_p^i)$ сгруппируйте сомножитель $1 - \zeta_p^i$ с $1 - \zeta_p^{p-i} = -\zeta_p^{-i}(1 - \zeta_p^i)$.

c^*) Выразите p^* линейной комбинацией $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ с рациональными коэффициентами.

Определение 1 Определим *многочлен деления круга*

$$\Phi_n(x) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (x - \zeta_n^k) \in \mathbb{C}[x].$$

Задача 4. a) Докажите, что $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

b) Докажите, что $\Phi_n(x) \in \mathbb{Q}[x]$.

Hint: Подействуйте группой Галуа.

c) Докажите, что $\Phi_n(x) \in \mathbb{Z}[x]$.

Задача 5*. a^*) Пусть p — простое целое число, не делящее n. Докажите, что если ξ является корнем неразложимого сомножителя $x^n - 1$ над $\mathbb{Q}$, то ξ^p тоже является его корнем.

Hint: Сначала докажите это утверждение над полем $\mathbb{Z}/p\mathbb{Z}$, используя отсутствие кратных корней у $x^n - 1$.

b^*) Докажите, что $\Phi_n(x)$ неразложим над $\mathbb{Q}$. Выведите отсюда, что $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, где $\phi(n) = |\{1 \leqslant a < n | (a, n) = 1\}|$, а также что $\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Задача 6. a) Пусть p — простое целое число. Докажите, что правильный p-угольник можно построить циркулем и линейкой тогда и только тогда, когда p имеет вид $2^l + 1$.

b) Докажите, что такое p — автоматически *простое число Ферма*, то есть имеет вид $2^{2^s} + 1$.

c^*) Докажите, что правильный n-угольник можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^k p_1 \ldots p_s$, где p_i — различные простые числа Ферма.

Задача 7. Запишите, используя целые числа, арифметические операции и квадратные корни, следующие алгебраические числа:

a) $\cos(2\pi/5)$,

b^*) $\cos(2\pi/17)$.