Круговые поля

Задача 1. Пусть A – факториальное кольцо, F – его поле частных.

a) Докажите, что многочлен $f \in A[x]$ неприводим в $A[x]$ тогда и только тогда, когда неприводим в $F[x]$.

b) Докажите критерий Эйзенштейна: если в многочлене $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ все коэффициенты $a_0, \ldots, a_{n-1}$ делятся на простой элемент $p \in A$ и при этом a_0 не делится на p^2, то этот многочлен неприводим.

Задача 2. Пусть $p \in \mathbb{Z}$ – простое число. Докажите, что многочлен $\frac{x^p-1}{x-1} = x^{p-1}+\ldots+x+1$ неприводим над $\mathbb{Q}$.

Подсказка: сделайте замену $y = x - 1$.

Определим круговые многочлены равенством

$$\Phi_n(x) = \prod_{\xi^n=1, \xi^k \neq 1 \text{ при } 0<k<n} x - \xi,$$

где произведение берётся по всем первообразным комплексным корням степени n из 1.

Задача 3. a) Докажите, что степень Φ_n равна $\phi(n)$ – количеству остатков по модулю n, взаимно простых с n.

b) Выпишите явно многочлены Φ_n при $n \leqslant 10$.

c) Докажите, что

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

d) Выведите отсюда, что $\Phi_n \in \mathbb{Z}[x]$.

Задача 4. Пусть поле $\mathbb{Q}[\xi_n] \subset \mathbb{C}$ получено присоединением к $\mathbb{Q}$ какого-либо первообразного комплексного корня ξ_n из 1.

a) Докажите, что $\mathbb{Q}[\xi_n]$ является полем разложения многочлена $x^n - 1$.

b) Докажите, что расширение $\mathbb{Q}[\xi_n]/\mathbb{Q}$ имеет степень $n-1$ при простом n.

c) Докажите, что группа Галуа $\mathbb{Q}[\xi_n]$ над $\mathbb{Q}$ – подгруппа в $(\mathbb{Z}/n\mathbb{Z})^*$.

Задача 5. a) Пусть $f(x)$ – неприводимый множитель в разложении $\Phi_n(x)$ на неприводимые над $\mathbb{Z}[x]$, а p – простое число, не делящее n. Пусть ξ – корень f, покажите, что ξ^p – также корень f.

Подсказка: предположите, что ξ^p – корень другого неприводимого множителя $g(x)$ и перейдите к полю $\mathbb{Z}/p\mathbb{Z}$.

b) То же для произвольного p, взаимно простого с n.

c) Докажите, что многочлен Φ_n неприводим над $\mathbb{Z}$, а значит, и над $\mathbb{Q}$.

d) Выведите отсюда, что $\deg \xi_n = \phi(n)$, а $Gal(\mathbb{Q}[\xi_n], \mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$.

Задача 6. a) Пусть m и n взаимно просты. Докажите, что правильный mn-угольник можно построить циркулем и линейкой тогда и только тогда, когда можно построить правильные m и n-угольники.

b) Докажите, что правильный n-угольник можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^m p_1 \cdot \ldots \cdot p_k$, где p_i – различные простые числа, имеющие вид $2^r + 1$.

c) Докажите, что если число $2^r + 1$ просто, то оно имеет вид $2^{2^s} + 1$. Такие простые числа называются числами Ферма.