Круговые поля

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 1°. Выпишите явно многочлены Φ_n при $n \leqslant 10$.

Задача 2. a) Докажите, что степень Φ_n равна $\phi(n)$ – количеству остатков по модулю n, взаимно простых с n.

b°) Докажите, что

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

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

d) Докажите формулу

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

где функция Мёбиуса μ определяется следующим образом: $\mu(p_1 p_2 \dots p_k) = (-1)^k$ для различных натуральных чисел $p_1, \dots, p_k$, $\mu(x) = 0$ в противном случае.

Задача 3. Пусть поле $\mathbb{Q}[\xi_n] \subset \mathbb{C}$ получено присоединением к $\mathbb{Q}$ какого-либо первообразного комплексного корня ξ_n степени n из 1. Такое поле называется *круговым расширением* поля $\mathbb{Q}$, или *круговым полем*.

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 автоморфизмов поля $\mathbb{Q}[\xi_n]$ – подгруппа в $(\mathbb{Z}/n\mathbb{Z})^*$.

В действительности, группа автоморфизмов поля $\mathbb{Q}[\xi_n]$ совпадает с $(\mathbb{Z}/n\mathbb{Z})^*$. Докажем это.

Задача 4. 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 группа автоморфизмов поля $\mathbb{Q}[\xi_n]$ изоморфна $(\mathbb{Z}/n\mathbb{Z})^*$.

Задача 5. 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 степень кругового поля $\mathbb{Q}[\xi_n]$ над $\mathbb{Q}$ является степенью двойки.

c) 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 $2^r + 1$.

d) Докажите, что если число $2^r + 1$ просто, то оно имеет вид $2^{2^s} + 1$. Такие простые числа называются *числами Ферма*. Их известно всего пять: $3, 5, 17, 257, 65537$.