Homework 4. Cyclotomic polynomials

Problem 1. Let $P \in \mathbb{Z}[X]$ a polynomial with degree $n \geq 1$.

(1) Using the results of Worksheet 2 Problem 1, prove the following :

   (a) If P is irreducible in $\mathbb{Z}[X]$ then it is irreducible in $\mathbb{Q}[X]$.

   (b) If P is a monic polynomial, then all its monic irreducible factors in $\mathbb{Q}[X]$ are in fact in $\mathbb{Z}[X]$.

(2) Verify for yourself the following remark (by writing the division) : let $A, B \in \mathbb{Z}[X]$ and let

$$A = BQ + R$$

be the Euclidean division of A by B in $\mathbb{Q}[X]$. If B is monic then Q and R lie in $\mathbb{Z}[X]$.

Problem 2. Let $n \geq 1$ Let $\mathcal{U}_n$ be the group of n^{th}-root of 1 in $\mathbb{C}$ and ζ_n be a generator of $\mathcal{U}_n$. It is called a primitive n^{th}-root of 1.

(1) Show that ζ_n is of the form $e^{2im\pi/n}$ for $m \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(2) Show that $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois. **We want to compute its degree**.

(3) Show that the action of $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ permutes the primitive n^{th}-root of 1.

(4) Show that there is an injective morphism of groups

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

and deduce that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] \leq \varphi(n)$.

(5) The following polynomial is called the n^{th} cyclotomic polynomial :

$$\Phi_n(X) = \prod_{\zeta \text{ generator of } \mathcal{U}_n} (X - \zeta).$$

Show, using Question (3), that it lies in $\mathbb{Q}[X]$.

(6) Show that $X^n - 1 = \prod_{d|n} \Phi_d$ and prove by induction on n that Φ_n lies in $\mathbb{Z}[X]$ for any $n \geq 1$ (use Problem 1 (2)).

(7) Let $P \in \mathbb{Q}[X]$ be the minimal polynomial of ζ_n.

   (a) Show that $P \in \mathbb{Z}[X]$.

   (b) Show that any root of P is a primitive n^{th} root of 1.

   (c) Let p be a prime number that does not divide n. We want to show that ζ_n^p is a root of P. Suppose that $P(\zeta_n^p) \neq 0$.

      (i) Show that there is $S \in \mathbb{Z}[X]$ such that $X^n - 1 = PS$ and $S(\zeta_n^p) = 0$.

      (ii) Show that P divides $Q := S(X^p)$ in $\mathbb{Z}[X]$.

(iii) For $U \in \mathbb{Z}[X]$ we denote by $\bar{U} \in \mathbb{F}_p[X]$ its reduction mod p. Show that $\bar{P}$ has only simple roots in an algebraic closure of $\mathbb{F}_p$.

(iv) Show that an irreducible factor $a \in \mathbb{F}_p[X]$ of $\bar{P}$ divides $\bar{S}$ and that a^2 divides $\overline{X^n - 1}$ in $\mathbb{F}_p[X]$. Find contradiction and conclude.

(d) Let ζ be a root of P and ζ' a root of Φ_n. Show that there is $m \geq 1$ with $GCD(m, n) = 1$ such that $\zeta' = \zeta^m$. Show, using Question (7)(c), that ζ' is a root of P.

(e) Show that $P = \Phi_n$.

(8) Show that $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. What is the degree of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$?

(9) What is Φ_p when p is prime? Show that the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is cyclic.

Problem 3. Let $n \geq 3$ and $\zeta \in \mathbb{C}$ a primitive n^{th} root of 1.

(1) Show that $\zeta + \zeta^{-1}$ has degree $\varphi(n)/2$ over $\mathbb{Q}$.

(2) Show that $\mathbb{Q}[\zeta + \zeta^{-1}] = \mathbb{R} \cap \mathbb{Q}[\zeta]$.

(3) By the previous problem, there is a isomorphism of groups

$$\chi_n : \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

such that $g(\zeta') = \zeta'^{\chi_n(g)}$ for any $\zeta' \in \mathcal{U}_n$ (check this for yourself). It is called the n^{th} cyclotomic character.

Check that the complex conjugation is an element in $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ and determine its image by the cyclotomic character.

(4) Show that $\mathbb{Q}[\zeta + \zeta^{-1}]/\mathbb{Q}$ is a Galois extension and determine its Galois group (you may use Galois correspondence...)

(5) Let $x \in \mathbb{Q}$. Write $x = a/b$ where $a \in \mathbb{Z}$, $b \in \mathbb{N}_{\geq 1}$ and $gcd(a, b) = 1$. Compute $[\,\mathbb{Q}[\cos(2\pi x)] : \mathbb{Q}]$.

(6) Suppose in this question that $n \neq 4$. Show that

$$[\,\mathbb{Q}[\sin(\frac{2\pi}{n})] : \mathbb{Q}] = \begin{cases} \varphi(n) \text{ if } gcd(8, n) < 4 \\ \varphi(n)/4 \text{ if } gcd(8, n) = 4 \\ \varphi(n)/2 \text{ if } gcd(8, n) > 4 \end{cases}$$

(7) Consider a triangle in $\mathbb{R}^2$ with vertices in $\mathbb{Q}^2$. Show that its area is a rational number.

(8) Suppose that there exists a regular polygon with n sides, with vertices in $\mathbb{Q}^2$ and on the 1-radius circle. Show that $n = 4$.