MATH 71 - ABSTRACT ALGEBRA
FALL 2015
FINAL EXAMINATION

DUE NOVEMBER 24

1. Cyclotomic polynomials

For $n \geq 2$, let μ_n denote the multiplicative group of n^{th} roots of 1: $\mu_n = \{z \in \mathbb{C}\ ,\ z^n = 1\}$ and Π_n the set of generators of μ_n. The *cyclotomic polynomial of order n* is

$$\Phi_n = \prod_{\xi \in \Pi_n} (X - \xi).$$

We recall that the Euler indicator φ satisfies the formula $\sum_{d|n} \varphi(d) = n$.

1. Consider the polynomial $P_n = \prod_{\xi \in \mu_n} (X - \xi)$.

(a) Prove that $P_n = X^n - 1$.

(b) Determine Φ_p for p prime.

2. Let $\omega = e^{\frac{2i\pi}{n}}$ and k an integer such that $0 \leq k \leq n-1$.

(a) Let d be the order of ω^k in μ_n. Prove that $\omega^k \in \Pi_d$

(b) Deduce that $X^n - 1$ divides $\prod_{d|n} \Phi_d$.

(c) Prove that $\prod_{d|n} \Phi_d = X^n - 1$.

3. We will prove by induction that Φ_n has integer coefficients.

(a) Verify the result for $n = 1$.

(b) Assuming the result true up to $n - 1$, find a monic polynomial $P \in \mathbb{Z}[X]$ such that

$$X^n - 1 = P\,\Phi_n.$$

(c) Prove the existence of polynomials Q and R in $\mathbb{Z}[X]$ with $\deg(R) < \deg(P)$, such that

$$X^n - 1 = PQ + R.$$

(d) Prove that the couple (Q, R) is unique and conclude that $\Phi_n \in \mathbb{Z}[X]$.

2. Application: proof of Wedderburn's Theorem

We shall prove that every finite division ring is commutative. Let K be a finite division ring. We argue by induction on the cardinality of K.

0. Prove the following result.

Lemma. *If A is a finite division ring and F a subring of A that is a field, then A is a finite dimensional vector space over F.*

1. Prove that a division ring of cardinality 2 is commutative.

From now on, we assume that every division ring of cardinality $< \#K$ is commutative and that K is noncommutative.

2. Let $\mathcal{Z} = \{x \in K \mid xy = yx \quad \text{for all } y \in K\}$ be the center of K and $q = \#\mathcal{Z}$.

(a) Prove that $\mathcal{Z}$ is a subring of K.

(b) Prove the existence of an integer $n \geq 2$ such that $\#K = q^n$.

3. For $x \in K$, let $K_x = \{y \in K \mid xy = yx\}$.

(a) Verify that either $K_x = K$ or K_x is a field extension of $\mathcal{Z}$ and a subring of K.

(b) Deduce the existence of a divisor d of n such that $\#K_x = q^d$.

4. Recall that the multiplicative group $K^\times = K \setminus \{0\}$ acts on itself by conjugation.

(a) Prove that every stabilizer has a cardinality of the form $q^d - 1$ with d a divisor of n.

(b) Using the class equation, prove the existence of integers λ_d such that

$$\#K^\times = q - 1 + \sum_{d|n\ ,\ d \neq n} \lambda_d \frac{q^n - 1}{q^d - 1}.$$

5. Assume that $d|n$ and $d \neq n$.

(a) Prove that Φ_n divides $\dfrac{X^n - 1}{X^d - 1}$ in $\mathbb{Z}[X]$.

(b) Prove that Φ_n divides $(X^n - 1) - \displaystyle\sum_{d|n\ ,\ d \neq n} \lambda_d \frac{X^n - 1}{X^d - 1}$ in $\mathbb{Z}[X]$.

(c) Deduce that $\Phi_n(q)$ divides $q - 1$.

6. Prove that $|\Phi_n(q)| > \displaystyle\prod_{i=1}^{\varphi(n)} |q - 1| \geq |q - 1|$ and conclude.