D-MATH Algebra II FS19
Prof. Rahul Pandharipande

Assignment 24

Cyclotomic extensions.

1. Let $\varphi : \mathbb{Z}_{\geqslant 1} \longrightarrow \mathbb{Z}_{\geqslant 0}$ be the Euler function $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Prove the following properties of the cyclotomic polynomials

$$\Phi_n := \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(T - e^{\frac{2\pi i}{n} a}\right) \in \mathbb{Z}[T].$$

   (a) $\Phi_n(T) = T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)$ for every integer $n \geqslant 2$.
   (b) $\Phi_p(T) = T^{p-1} + \cdots + 1$ for every prime number p.
   (c) $\Phi_{p^r}(T) = \Phi_p(T^{p^{r-1}})$ for every prime number p and integer $r \geqslant 1$.
   (d) $\Phi_{2n}(T) = \Phi_n(-T)$ for every **odd** integer $n > 1$.

2. Let p be an odd prime number and $r \geqslant 2$ an integer. The goal of this exercise is to show that there is an isomorphism of abelian groups

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

   (a) Explain why the statement is equivalent to proving that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.
   (b) Show that there exists $g \in \mathbb{Z}$ which generates $(\mathbb{Z}/p\mathbb{Z})^\times$ with $g^{p-1} \not\equiv 1 \bmod p^2$.
   Hint. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Look at $(g+p)^{p-1}$ modulo p^2 and eventually replace g with $g+p$.
   (c) For g as in (b), show that $g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$ by proving inductively that there exist integers $k_1, k_2, \ldots, k_{r-1} \in \mathbb{Z}$ for which

$$g^{p^{j-1}(p-1)} = 1 + k_j p^j \quad \text{and} \quad p \nmid k_j.$$

   (d) Explain why $\operatorname{ord}_{(\mathbb{Z}/p^r\mathbb{Z})^\times}(g)$ divides $p^{r-1}(p-1)$.
   (e) Suppose that $g^{p^\varepsilon d} \equiv 1 \bmod p^r$ for some integer $\varepsilon \geqslant 1$ and a proper divisor d of $p-1$. Deduce that $g^d \equiv 1 \bmod p$ and derive a contradiction.
   (f) Conclude that g is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

3. Let n be a positive integer and $p \nmid n$ a prime number. Show that the irreducible factors of $\Phi_n \in \mathbb{F}_p[X]$ are all distinct with degree equal to the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

   Hint. Prove that if α is a root of Φ_n, then α is a primitive root of unity.

4. Show that for any $n \in \mathbb{Z}_{>0}$ there are infinitely many primes p with $p \equiv 1 \bmod n$.

   Hint. If one such prime p exists, then one can find a prime $p' > p$ with $p' \equiv 1 \bmod (n \cdot p)$.