Solution 26

Cyclotomic extensions.

In the following, $\varphi : \mathbb{Z}_{\geqslant 1} \longrightarrow \mathbb{Z}_{\geqslant 0}$ is the Euler function $\varphi(n) = \operatorname{card}((\mathbb{Z}/n\mathbb{Z})^\times)$. For each integer $n \geqslant 1$, we consider the n-th cyclotomic polynomial

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

1. Prove the following properties of the cyclotomic polynomials $\varphi_n \in \mathbb{Z}[T]$

   (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 $n \geqslant 1$.

   Solution:

   (a) Clearly, $\varphi(n) = \deg(\Phi_n)$. Write $\Phi_n(T) = \sum_{j=0}^{\varphi(n)} a_j T^j$. Then

   $$T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right) = T^{\varphi(n)} \sum_{j=0}^{\varphi(n)} a_j T^{-j} = \sum_{j=0}^{\varphi(n)} a_j T^{\varphi(n)-j} \in \mathbb{Z}[T]$$

   is a degree $\varphi(n)$ polynomial as well. Notice that, for each $a \in \mu_n$ we have $a^{-1} \in \mu_n$, so that

   $$a^{\varphi(n)} \Phi_n\left(\frac{1}{a}\right) = 1 \cdot 0 = 0.$$

   Hence $T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)$ has roots $R(T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)) = \mu_n = R(\Phi_n)$ and since they have the same degree and Φ_n has distinct roots they must coincide.

   (b) See Assignment 11, Exercise 4.

   (c) Since μ_n is the disjoint union of the set of primitive d-th roots of 1 for each divisor $d|n$, we obtain the equality

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

This reads, for $n = p^r$, as

$$T^{p^r} - 1 = \prod_{m=0}^{r} \Phi_{p^m}.$$

Hence, by induction on r,

$$\Phi_{p^r}(T) = \frac{T^{p^r} - 1}{\prod_{m=0}^{r-1} \Phi_{p^m}} = \frac{T^{p^r} - 1}{T^{p^{r-1}} - 1} = \frac{(T^{p^{r-1}})^p - 1}{T^{p^{r-1}} - 1} = \Phi_p(T^{p^{r-1}}).$$

(d) Since 2 and n are coprime by assumption, we know that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, so that the two given polynomials have the same degree. If ζ is a primitive $2n$-th root of 1, then $\mathrm{ord}_{\mathbb{C}^\times}(\zeta^n) = 2$, so that $\zeta^n = -1$. In particular, since n is odd, we get $(-\zeta)^n = -\zeta^n = 1$, so that $-\zeta$ is a n-th root of 1. It must be a primitive n-th root of 1, because if $(-\zeta)^m = 1$ for $m < n$, then $zeta^{2m} = (-\zeta)^{2m} = 1$ which contradicts the fact that ζ is a primitive $2n$-th root of 1. Hence $R(\Phi_n) = \{-\zeta, \zeta \in R(\Phi_{2n})\}$, so that

$$\begin{aligned}\Phi_n(T) &= \prod_{\zeta \in R(\Phi_n)} (T - \zeta) = \prod_{\zeta \in R(\Phi_{2n})} (T + \zeta) = (-1)^{\varphi(2n)} \prod_{\zeta \in R(\Phi_{2n})} (-T - \zeta) \\ &= (-1)^{\varphi(2n)} \Phi_{2n}(-T).\end{aligned}$$

In order to conclude, we need to prove that $\varphi(2n)$ is even for n odd. As already noticed, $\varphi(2n) = \varphi(n)$ in this case. Decomposing n into a product of prime powers and using the fact that $\varphi(ab) = \varphi(a)\varphi(b)$ when a and b are coprime[1], we see that it is enough to check that $\varphi(p^r)$ is event for each odd prime p and $r \geqslant 1$, which is clear from the formula $\varphi(p^r) = p^r - p^{r-1}$.

2. Let p be an odd prime number and $r \geqslant 2$ an integer. We want to prove that there is an isomorphism of abelian groups

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

(a) Explain why the statement is equivalent to proving that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.

(b) Prove that there exists $g \in \mathbb{Z}$ which generates $(\mathbb{Z}/p\mathbb{Z})^\times$ and such that $g^{p-1} \not\equiv 1 \mod p^2$ [*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) Prove inductively that there are integers $k_1, k_2, \ldots, k_{r-1} \in \mathbb{Z}$ for which

$$g^{p^{j-1}(p-1)} = 1 + k_j p^j, \ p \nmid k_j$$

[1] By the Chinese Remainder Theorem, $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ as rings, so that they have isomorphic groups of units. Notice that an element $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is invertible if and only if both x and y are invertible, so that we obtain an isomorphism $(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. Then $\varphi(ab) = |(\mathbb{Z}/ab\mathbb{Z})^\times| = |(\mathbb{Z}/a\mathbb{Z})^\times| \cdot |(\mathbb{Z}/b\mathbb{Z})^\times| = \varphi(a)\varphi(b)$.

(d) Deduce that $g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$. Moreover, prove that $\mathrm{ord}_{(\mathbb{Z}/p^r\mathbb{Z})^\times}(g)$ 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 $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

Solution:

(a) Since $p-1$ and p^r are coprime, the group $\mathbb{Z}/p^{r-1}\mathbb{Z}\times\mathbb{Z}/(p-1)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$, a cyclic group. Since this group has cardinality $p^{r-1}(p-1) = p^r - p^{r-1} = \varphi(p^r) = |(\mathbb{Z}/p^r\mathbb{Z})^\times|$, proving that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic is enough to prove the given statement.

(b) As seen in Algebra I, the group $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Let $g \in \mathbb{Z}$ be a representative of a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. If $g^{p-1} \not\equiv 1 \bmod p^2$, then we are done. Else, assume that $g^{p-1} \equiv 1 \bmod p^2$. Expanding the binomial power $(g+p)^{p-1}$ as suggested in the hint, we see that

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + p^2 m, \quad \text{for some } m \in \mathbb{Z}.$$

Hence $(g+p)^{p-1} \equiv g^{p-1} - g^{p-2}p \pmod{p^2}$. Since $g^{p-1} \equiv 1 \bmod p^2$ by assumption, we see that

$$(g+p)^{p-1} \equiv 1 - g^{p-2}p,$$

where $p \nmid g$ so that $p \nmid g^{p-2}$, so that $p^2 \nmid g^{p-2}p$ and $(g+p)^{p-1} \not\equiv 1 \bmod p^2$. Then $g+p$ satisfies the desired property (it is a generator as well, because it represents the same class as g in $\mathbb{Z}/p\mathbb{Z}$.

(c) For $j = 1$, we know by the previous step that

$$g^{1\cdot(p-1)} = 1 + k_1 p, \ \ p \nmid k_1,$$

because $g^{p-1} \equiv 1 \bmod p$ and $g^{p-1} \nmid 1 \bmod p^2$. Now suppose that for $j \geqslant 2$ there exists k_{j-1} such that $g^{p^{j-2}(p-1)} = 1 + k_{j-1}p^{j-1}$ and $p \nmid k_{j-1}$. Then

$$\begin{aligned} g^{p^{j-1}(p-1)} &= (g^{p^{j-2}(p-1)})^p = (1 + k_{j-1}p^{j-1})^p \overset{(*)}{=} 1 + p \cdot k_{j-1}p^{j-1} + p^{2j-1}m_j \\ &= 1 + (k_{j-1} + p^{j-1}m_j)p^j \end{aligned}$$

for some integer m_j. In the equality $(*)$ we used the fact that p divides the binomial coefficients $\binom{p}{k}$ for $0 < k < p$. Then $k_j := k_{j-1} + p^{j-1}m_j$ is not divisible by p because k_{j-1} is not while $p|p^{j-1}m_j$ as $j \geqslant 2$. This proves the induction step and concludes the proof.

(d) For $j = r-1$, we obtain

$$g^{p^{r-2}(p-1)} = 1 + k_{r-1}p^{r-1}$$

where $p \nmid k_{r-1}$. This implies that $g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$. This means that the order of g in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ does not divide $p^{r-2}(p-1)$. On the other hand, this order divides the cardinality of the group, which is $p^{r-1}(p-1)$.

(e) Under the given assumption, reducing modulo p and applying Fermat's little theorem which asserts that $g^p \equiv g \pmod{p}$, we obtain $g^d \equiv 1$ modulo p, which is a contradiction with the fact that g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

(f) By the previous point, the order of g in $(\mathbb{Z}/p^r\mathbb{Z})^\times$, which is a divisor of $p^{r-1}(p-1)$ by part (d), is of the form $p^\varepsilon \cdot (p-1)$. But this order does not divide $p^{r-2}(p-1)$ by part (d), so the only remaining possibility is that $\mathrm{ord}_{(\mathbb{Z}/p^r\mathbb{Z})^\times}(g) = p^{r-1}(p-1) = |(\mathbb{Z}/p^r\mathbb{Z})^\times|$. Hence g is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

3. Prove that for every integer $r \geqslant 2$ there is an isomorphism of abelian groups

$$(\mathbb{Z}/2^r\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}.$$

More specifically, show for $r \geqslant 3$ that

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2 \ldots, 5^{2^{r-2}-1}\}.$$

Solution: First, we prove that $5 \in (\mathbb{Z}/2^r\mathbb{Z})^\times$ has order 2^{r-2} in a way similar to parts (c) and (d) of Exercise 2. Since

$$|(\mathbb{Z}/2^r\mathbb{Z})^\times| = \varphi(2^r) = 2^r - 2^{r-1} = 2^{r-1}(2-1) = 2^{r-1},$$

the order of 5 must be a power of 2. We test the elements 5^{2^ℓ} as follows:

$$\begin{aligned} 5 &= 1 + 2^2 \\ 5^2 &= (1+2^2)^2 = 1 + 2^3 + 2^4 = 1 + k_1 2^3 \quad \text{with } 2 \nmid k_1 \in \mathbb{Z}, \\ 5^{2^2} &= (1 + k_1 2^3)^2 = 1 + k_1 2^4 + k_1^2 2^6 = 1 + k_2 2^4 \quad \text{with } 2 \nmid k_2 \in \mathbb{Z}. \end{aligned}$$

Iterating this, one can prove that there exist $k_1, k_2, k_3, \ldots$ odd numbers such that

$$5^{2^j} = 1 + k_j 2^{2+j}.$$

In particular, for $j = r-3$ and $j = r-2$ we obtain

$$\begin{aligned} 5^{2^{r-3}} &= 1 + k_{r-3}2^{r-1} \not\equiv 1 \pmod{2^r} \\ 5^{2^{r-2}} &= 1 + k_{r-2}2^r \equiv 1 \pmod{2^r}, \end{aligned}$$

letting us conclude that 5 has order 2^{r-2} in $(\mathbb{Z}/2^r\mathbb{Z})^\times$, so that $H = \{1, 5, 5^2 \ldots, 5^{2^{r-2}-1}\}$ is a subgroup of $(\mathbb{Z}/2^r\mathbb{Z})^\times$, of index $2^{r-1}/2^{r-2} = 2$.

In order to prove that $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times H$, it is enough to check that $\mathbb{Z}/2^r\mathbb{Z}$ is a semidirect product of $\{\pm 1\}$ and H (see Assignment 21, Exercise 1), because the action of one subgroup on the other by conjugation is trivial as we are in an abelian group. In particular, both $\{\pm 1\}$ and H are normal subgroups. Let $x \in \{\pm 1\} \cap H$. Then $x = \pm 1$. If $x = -1$, then $-1 \equiv 5^a \pmod{2^r}$ which, reducing modulo 4, gives $-1 \equiv 1 \pmod 4$, contradiction. Hence $x = 1$. This proves that $\{\pm 1\} \cap H = 1$. Moreover, the cardinalities of these two subgroups, multiplied together, give $2^{r-1} = |(\mathbb{Z}/2^r\mathbb{Z})^\times|$, so that by the second isomorphism theorem for groups we can conclude that $\{\pm 1\}H = (\mathbb{Z}/2^r\mathbb{Z})^\times$ and by what we observed above, that

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times H = \{\pm 1\} \times \{1, 5, 5^2 \ldots, 5^{2^{r-2}-1}\}.$$

4. Let n be a positive integer and $p \nmid n$ a prime number. Prove that the irreducible factors of $\Phi_n \in \mathbb{F}_p[X]$ are all distinct and their degree is equal to the order of $p + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. [*Hint:* You may want to prove the following claim: if α is a root of Φ_n, then α is a primitive root of 1.]

   Solution: See Notes 26 from the website.

5. Let n be a positive integer. Prove that there are infinitely many primes p such that $p \equiv 1 \bmod n$. [*Hint:* If one such prime p exists for every n, then one can find a bigger one p' satisfying $p' \equiv 1 \bmod (n \cdot p)$]

   Solution: See Notes 26 from the website.