# Solution 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 $n > 1$.

*Solution*:

(a) We already know that $\varphi(n) = \deg(\Phi_n)$. Write $\Phi_n(T) = \sum_{j=0}^{\varphi(n)} a_j T^j$. Then

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

is also a polynomial of degree $\varphi(n)$. Let $\mu_n$ denote the set of $n$-th roots of unity. Note that for each $a \in \mu_n$ we have $a^{-1} \in \mu_n$, so

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

Hence the set of roots of $T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)$ is precisely $\mu_n$, which is the set of roots of $\Phi_n$. Since the two polynomials have the same degree and $\Phi_n$ has distinct roots, they must coincide.

(b) See Assignment 11, Exercise 4.

(c) Since $\mu_n$ is the disjoint union of the set of primitive $d$-th roots of unity for each divisor $d \mid n$, we obtain the equality

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

For $n = p^r$ this reads 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 have $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, so the two given polynomials have the same degree. If $\zeta$ is a primitive $2n$-th root of unity, then $\mathrm{ord}_{\mathbb{C}^\times}(\zeta^n) = 2$, so $\zeta^n = -1$. In particular, since $n$ is odd, we get $(-\zeta)^n = -\zeta^n = 1$, so $-\zeta$ is an $n$-th root of unity. It must be a primitive $n$-th root of unity, because if $(-\zeta)^m = 1$ for $m < n$, then $\zeta^{2m} = (-\zeta)^{2m} = 1$ which contradicts the fact that $\zeta$ is a primitive $2n$-th root of unity. Hence the roots of $\Phi_n$ are precisely $\pm$ roots of $\Phi_{2n}$, so

$$\begin{aligned}\Phi_n(T) &= \prod_{\Phi_n(\zeta)=0} (T - \zeta) = \prod_{\Phi_{2n}(\zeta)=0} (T + \zeta) = (-1)^{\varphi(2n)} \prod_{\Phi_{2n}(\zeta)=0} (-T - \zeta) \\ &= (-1)^{\varphi(2n)} \Phi_{2n}(-T).\end{aligned}$$

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 (this product is nonempty for $n > 1$) 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 even for each odd prime $p$ and $r \geqslant 1$. But this is immediate 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. 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 $g + p$.

[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 they have isomorphic groups of units. Moreover, 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. This yields an isomorphism $(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ from which we can deduce that $\varphi(ab) = |(\mathbb{Z}/ab\mathbb{Z})^\times| = |(\mathbb{Z}/a\mathbb{Z})^\times| \cdot |(\mathbb{Z}/b\mathbb{Z})^\times| = \varphi(a)\varphi(b)$.

(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 $\mathrm{ord}_{(\mathbb{Z}/p^r\mathbb{Z})^\times}(g)$ 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 the cyclic group $\mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$. The cardinality of the latter group is $p^{r-1}(p-1) = p^r - p^{r-1} = \varphi(p^r) = |(\mathbb{Z}/p^r\mathbb{Z})^\times|$. Thus to prove the given statement, it suffices to show that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.

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

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

Since $p \nmid g$, we have $p \nmid g^{p-2}$; hence $p^2 \nmid g^{p-2}p$ and $(g+p)^{p-1} \not\equiv 1 \bmod p^2$. Moreover, $g+p$ is also a generator because it represents the same class as $g$ in $\mathbb{Z}/p\mathbb{Z}$. Thus $g+p$ satisfies the desired properties.

(c) For $j = 1$, we know by the previous step that there exists a $k_1$ with

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

because $g^{p-1} \equiv 1 \bmod p$ and $g^{p-1} \not\equiv 1 \bmod p^2$. Now suppose that for $j \geqslant 2$ we have already found $k_{j-1}$ with $g^{p^{j-2}(p-1)} = 1 + k_{j-1}p^{j-1}$ 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 $p \mid p^{j-1}m_j$ for $j \geqslant 2$. This proves the induction step. For $j = r-1$, we thus obtain

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

where $p \nmid k_{r-1}$, which implies that $g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$.

(d) The order of $g$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ divides the cardinality of the group, which is precisely $\varphi(p^r) = p^{r-1}(p-1)$.

(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 $p$, contrary to the fact that $g$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

(f) By Part (d), the order of $g$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is a divisor of $p^{r-1}(p-1)$. Using Part (e), we thus find that it must be of the form $p^\varepsilon \cdot (p-1)$. On the other hand, the fact that $g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r$ from Part (c) means that the order of $g$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ does not divide $p^{r-2}(p-1)$. So the only 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. 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 $\alpha$ is a root of $\Phi_n$, then $\alpha$ is a primitive root of unity.

   *Solution*: See Theorem IV.34 in Prof. Burger's notes on the website.

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 $p' \equiv 1 \bmod (n \cdot p)$.

   *Solution*: See Theorem IV.35 in Prof. Burger's notes on the website.