Math 562/662 **Spring 2022**
Homework 4 **Drew Armstrong**

---

1. The Fundamental Theorem of Cyclic Groups. Let G be a finite cyclic group of size n and pick a generator $a \in G$ so that $G = \langle a \rangle = \{\varepsilon, a, a^2, \ldots, a^{n-1}\}$. By Lagrange's Theorem, the size of any subgroup divides n. Conversely, we will show that for any positive divisor $d|n$ **there exists a unique subgroup of size** d. Let $n = dd'$ for some integers $d, d' \geq 1$.

(a) Prove that the cyclic subgroup $\langle a^{d'} \rangle \subseteq G$ has size d.

(b) Let $H \subseteq G$ be **any cyclic subgroup** of size d. Prove that $H = \langle a^{d'} \rangle$. [Hint: For any $a^k \in G$ we know from HW3 that $\#\langle a^k \rangle = n/\gcd(k,n)$ and $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$.]

(c) Let $H \subseteq G$ be **any subgroup** of size d. Prove that $H = \langle a^{d'} \rangle$. [Hint: If $d = 1$ then there is nothing to show, so let $d \geq 2$. Let m be the smallest integer $m > 0$ such that $a^m \in H$ and let $b \in H$ be an arbitrary element. We can write $b = a^k$ for some k. Divide k by m to obtain $k = mq + r$ with $0 \leq r < m$. Show that our assumptions imply $r = 0$. It follows that b is a power of a^m and hence $H = \langle a^m \rangle$.]

2. Cyclotomic Polynomials. Let $(\Omega_n, \times, 1)$ be the group of nth roots of unity and consider the subset[1] of *primitive roots*:

$$\Omega'_n = \{\omega^k : 1 \leq k \leq n \text{ and } \gcd(k,n) = 1\}.$$

(a) Prove that the subgroups of Ω_n are just Ω_d for divisors $d|n$.

(b) Prove that Ω'_n is the set of *generators* $\zeta \in \Omega_n$ such that $\langle \zeta \rangle = \Omega_n$. [Hint: We know from HW3 that the cyclic subgroup $\langle \omega^k \rangle \subseteq \Omega_n$ has size $n/\gcd(k,n)$.]

(c) Use (a) and (b) to express Ω_n as a disjoint union:

$$\Omega_n = \coprod_{d|n} \Omega'_d.$$

[Hint: For any $\zeta \in \Omega_n$ we have $\zeta \in \Omega'_d$ if and only if $\langle \zeta \rangle = \Omega_d$.]

(d) We define the *nth cyclotomic polynomial* as follows:[2]

$$\Phi_n(x) := \prod_{\zeta \in \Omega'_n} (x - \zeta) \in \mathbb{C}[x].$$

Prove that $\Phi_n(x)$ actually has **integer coefficients**. [Hint: From part (c) we have

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

Let $f(x)$ be the product of $\Phi_d(x)$ for all divisors $d|n$ except $d = n$, so that $x^n - 1 = \Phi_n(x)f(x)$. By induction we may assume that $f(x)$ has integer coefficients. On the other hand, since $f(x) \in \mathbb{Z}[x]$ has leading coefficient 1 there exist $q(x), r(x) \in \mathbb{Z}[x]$ with $x^n - 1 = q(x)f(x) + r(x)$, such that $r(x) = 0$ or $\deg(r) < \deg(f)$. You don't need to prove this; it follows from the same proof as a the division algorithm over fields.]

---

[1] It is not a subgroup.

[2] We use this notation because the degree of Φ_n is Euler's totient $\phi(n)$.