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 $H = \langle a^m \rangle$.]

(a): We showed in the previous homework that $\#\langle a^k \rangle = n/\gcd(k,n)$ for any integer $k \in \mathbb{Z}$. In this case since $d'|n$ we have $\gcd(d', n) = d'$ and hence

$$\#\langle a^{d'} \rangle = n/\gcd(d', n) = n/d' = d.$$

(b): Any cyclic subgroup $H \subseteq G$ has the form $H = \langle b \rangle$ for some $b \in G$. But any element of G has the form $b = a^k$. Recall from the previous homework that

(i) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$,
(ii) $\#\langle a^k \rangle = n/\gcd(k,n)$.

Now suppose that $\#H = d$. It follows from (ii) that

$$d = n/\gcd(k,n)$$

and hence $\gcd(k,n) = n/d = d'$. Then it follows from (i) that

$$H = \langle a^k \rangle = \langle a^{d'} \rangle.$$

(c): Let $H \subseteq G$ be any subgroup of size d. We will show that H is cyclic and then it will follow from (b) that $H = \langle a^{d'} \rangle$. If $d = 1$ then there is nothing to show, so suppose that $d \geq 2$ and let $m > 0$ be the smallest positive integer such that $a^m \in H$.[1] On the one hand, since $a^m \in H$ and since H is a subgroup we know that any power of a^m is in H, hence $\langle a^m \rangle \subseteq H$. On the other hand, we will show that any element $b \in H$ is a power of a^m and hence $H \subseteq \langle a^m \rangle$. It will follow that $H = \langle a^m \rangle$ and hence H is cyclic.

So consider any element $b \in H$. Since $G = \langle a \rangle$ we can write $b = a^k$ for some $k \in \mathbb{Z}$. Divide k by m to obtain

$$\begin{cases} k = mq + r, \\ 0 \leq r < m. \end{cases}$$

We observe that $a^r \in H$ because $a^{-m} \in H$ and hence

$$a^r = a^{k-mq} = a^k(a^{-m})^q \in H.$$

[1] Such an integer exists because $a^n = \varepsilon$.

If $r = 0$ then this contradicts the definition of m. It follows that $r = 0$ and hence $b = a^k = a^{mq} = (a^m)^q$ is a power of a^m, as desired.

2. Cyclotomic Polynomials. Let $(\Omega_n, \times, 1)$ be the group of nth roots of unity and let $\omega = e^{2\pi i/n}$. We know that $\Omega_n = \langle\omega\rangle$ is a cyclic group. Now consider the subset[2] 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 positive 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:[3]

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

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.]

(a): We know that $\Omega_n = \langle\omega\rangle$. Therefore from Problem 1 the subgroups of Ω_n are just $\langle\omega^{n/d}\rangle$ for positive divisors $d|n$. I claim that

$$\langle\omega^{n/d}\rangle = \Omega_d.$$

Indeed, we know that $\#\langle\omega^{n/d}\rangle = d$, so we will be done if we can show that $\langle\omega^{n/d}\rangle \subseteq \Omega_d$. In other words, we want to show that every power of $\omega^{n/d}$ is a dth root of unity. And this is straightforward:

$$\left(\left(\omega^{n/d}\right)^k\right)^d = \omega^{nk} = (\omega^n)^k = 1^k = 1.$$

(b): Let $\zeta = \omega^k \in \Omega_n$ be an arbitrary nth root of unity. Then we have

$$\#\langle\zeta\rangle = \#\langle\omega^k\rangle = n/\gcd(k, n),$$

so that

$$\langle\zeta\rangle = \Omega_n \quad \iff \quad \#\langle\zeta\rangle = n \quad \iff \quad \gcd(k, n) = 1.$$

[2] It is not a subgroup.

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

(c): Every nth root of unity $\zeta \in \Omega_n$ generates a cyclic subgroup $\langle \zeta \rangle \subseteq \Omega_n$, which must equal Ω_d for some $d|n$. Therefore we have a disjoint union:

$$\Omega_n = \coprod_{d|n} \{\zeta \in \Omega_n : \langle \zeta \rangle = \Omega_d\} = \coprod_{d|n} \Omega'_d.$$

(d): It follows from part (c) that

$$\prod_{d|n} \Phi_d(x) = \prod_{d|n} \prod_{\zeta \in \Omega'_d} (x - \zeta) = \prod_{\zeta \in \Omega_n} (x - \zeta) = x^n - 1.$$

Let $f(x)$ be the product of $\Phi_d(x)$ over all divisors $d|n$ except $d = n$, so that

$$x^n - 1 = \Phi_n(x) f(x).$$

Observe that the polynomial $f(x)$ has leading coefficient 1 because each $\Phi_d(x)$ has leading coefficient 1. Now let us assume for induction that $\Phi_k(x) \in \mathbb{Z}[x]$ for all $k < n$, which implies that $f(x) \in \mathbb{Z}[x]$. Since $f(x) \in \mathbb{Z}[x]$ has leading coefficient 1 there exist $q(x), r(x) \in \mathbb{Z}[x]$ with

$$\begin{cases} x^n - 1 = q(x) f(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < \deg(f). \end{cases}$$

On the other hand, we have $x^n - 1 = \Phi_n(x) f(x) + 0$ in the ring $\mathbb{C}[x]$. By uniqueness of quotient and remainder in $\mathbb{C}[x]$ it follows that $\Phi_n(x) = q(x)$ and hence $\Phi_n(x) \in \mathbb{Z}[x]$.

Remark: It is difficult to predict the coefficients of the polynomials $\Phi_n(x)$. However, part (d) gives a recursive algorithm to compute them. Here are the first few cyclotomic polynomials:

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^5 + x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$
11	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
12	$x^4 - x^2 + 1$

See the course notes for more information.

In particular, this table tells us the factorization of $x^{12} - 1$ over the integers.[4] Since the divisors of 12 are $1, 2, 3, 4, 6, 12$ we obtain

$$\begin{aligned} x^{12} - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) \\ &= (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1). \end{aligned}$$

[4]One can show that each cyclotomic polynomial is prime over $\mathbb{Z}$, so this is the prime factorization in the ring $\mathbb{Z}[x]$. However, the proof is quite difficult (even Gauss had trouble with it) so we won't discuss it in this class.