Math 493 Fall 2023 HW5

1. **(20 pts)** (Cyclic groups) In parts (a)-(e), let G be a cyclic group of order n, generated by the element a.

   (a) (3 pts) For any integer i, determine the order of a^i in G (in terms of i and n).

   (b) (3 pts) Show that every subgroup of G is cyclic and that for any $d \mid n$, G has a unique (cyclic) subgroup of order d.

   (c) (3 pts) The Euler ϕ function is defined by

   $$\phi(n) = |\{1 \leq a \leq n,\ \gcd(a, n) = 1\}$$

   Give a formula for $\phi(n)$ in terms of the prime factorization of n and show that ϕ is multiplicative, i.e., $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m, n) = 1$.

   (d) (4 pts) Show that for any $d \mid n$, the number of elements of G of order d is exactly $\phi(d)$. Deduce that

   $$\sum_{d|n} \phi(d) = n.$$

   (e) (3 pts) Show that $\mathrm{Aut}(G) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$, where the latter is the multiplicative group of classes mod n that are coprime to n. In particular, $|\mathrm{Aut}(G)| = \phi(n)$.

   (f) (4 pts) Let m and n be positive integers. Show that $C_m \times C_n \simeq C_{mn}$ if and only if m and n are coprime.

2. **(10 pts)** In this problem we will show that any finite subgroup of the multiplicative group of a field is cyclic. In particular, $(\mathbf{Z}/p\mathbf{Z})^\times$, being a multiplicative subgroup of the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, is cyclic of order $p - 1$.

   Let k be a field, and let $G \subset k^\times$ be a finite subgroup with $|G| = n$.

   (a) (5 pts) For any $d \mid n$, let $a(d)$ denote the number of elements of G of order dividing d, and let $b(d)$ denote the number of elements of G of order exactly d. Show that

   $$d = a(d) = \sum_{d'|d} b(d').$$

   Hint: You will want to use that a non-zero polynomial with coefficients in k cannot have more roots in k than its degree.

   (b) (5 pts) Prove that $b(d) = \phi(d)$ for all $d \mid n$. In particular, $b(n) = \phi(n) \geq 1$, so that G is cyclic, and has $\phi(n)$ different generators.

   Hint: Use induction on d and part (d) of the previous problem.

3. **(10 pts)** From the previous two problems, we see that the automorphism group $\mathrm{Aut}(C_p)$ for any prime p is cyclic of order $p - 1$. Use this to classify groups of order pq, where p and q are distinct primes.

4. **(10 pts)** Let p be a prime. How many p-Sylow subgroups does the symmetric group S_p contain? Use your answer to deduce Wilson's theorem from elementary number theory: recall this says that $(p-1)! \equiv -1 \bmod p$.

5. **(15 pts)** (Artin problem 7.7.8) Compute the order of $\mathrm{GL}_n(\mathbf{F}_p)$. Find a p-Sylow subgroup of $\mathrm{GL}_n(\mathbf{F}_p)$ and determine the number of p-Sylow subgroups.

6. **(35 pts)** We have shown in class that the smallest nonabelian simple group has order 60. Show that there are no nonabelian simple groups with order satisfying $60 < |G| < 168$.