October 6, 2025

Problem Set 4

Exercise 1. Let D_n be the dihedral group of rigid symmetries of a regular n-gon, $n \geq 3$:

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle = \{1, r, \dots r^{n-1}, s, sr, \dots sr^{n-1}\}.$$

(a) Show that $sr^i s = r^{-i}$ for all $0 \leq i \leq n-1$.

(b) Identify the element $r^2 sr^{-1} sr^{-4} s \in D_n$ in the list of all elements of D_n.

(c) Find all elements $x \in D_n$ such that $gxg^{-1} = x$ for all $g \in D_n$. The elements with this property are called *central* in the group.

(d) Find the order of the elements $x = sr^2$ and $y = r^2$ in D_n.

Exercise 2. Consider the dihedral group $D_6 = \langle s, r \mid s^2 = 1, r^6 = 1, srs = r^{-1} \rangle$.

(a) Show that $R = \{1, r, r^2, r^3, r^4, r^5\} \subset D_6$ is a normal subgroup.

(b) Show that $H = \{1, r^3\} \subset D_6$ is a normal subgroup.

(c) Show that $T = \{1, sr^3\} \subset D_6$ is a subgroup in D_6 that is not normal.

Exercise 3. (a) Show that if G is such that $a^2 = e$ for all $a \in G$ then G is abelian.

(b) Show that any group of order 4 is abelian.

(b) Let G be an abelian group and $a, b \in G$ two elements of finite order. Suppose that $\mathrm{o}(a)$ and $\mathrm{o}(b)$ are mutually prime. Show that ab is of finite order $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

Exercise 4. Let p be a prime. Show that any group of order p is cyclic.

Exercise 5. Pollard's algorithm for factorizing large integers works as follows:
Suppose you are given an integer n and you want to find its prime factors. Take a small number a and check that $\gcd(a, n) = 1$ (if not, you already have found a nontrivial factor of n). For $m = 2, 3, \dots$, compute $\gcd(a^K - 1, n)$, where $K = \mathrm{lcm}(2, 3, \dots m)$. If $\gcd(a^K - 1, n) > 1$, then you have found a nontrivial factor of n. If $\gcd(a^K - 1, n) = 1$, increase $m \leq \sqrt{n}$ until you get a nontrivial multiple of n.

(a) Explain why Pollard's algorithm works well for finding prime factors p of n in case when $(p-1)$ is a product of small powers of small primes. Use Fermat's little theorem.

(b) Obtain the prime factorization of $n = 15041$ using Pollard's algorithm. You can take $a = 2$ and use the following website to compute the gcd of two integers: `http://www.alcula.com/calculators/math/gcd/`.