Problem 1. \((C^*, \text{Gallian 7.12 & 7.30})\)

1. Let \(C^*\) be the group of nonzero complex numbers under multiplication and let \(H = \{a + bi \in C^* : a^2 + b^2 = 1\}\). Give a geometric description of the coset \((3 + 4i)H\). Give a geometric description of the coset \((c + di)H\) for arbitrary \(c + di \in C^*\).

2. Determine all finite subgroups \(G\) of \(C^*\). Justify your answer. (Hint: what are the solutions to \(a^n = 1\) in \(C^*\)?)

Problem 2. \((\text{Rotations of regular solids, Gallian 7.48})\) Calculate the order of the group of rotations for each of the following solids (refer to Figure 27.5 in Gallian for illustrations):

1. A regular octahedron (solid with eight congruent equilateral triangles as faces).

2. A regular dodecahedron (a solid with 12 congruent regular pentagons as faces).

3. A regular icosahedron (a solid with 20 congruent equilateral triangles as faces).

Here by “group of rotations” we allow only rotations in 3-dimensional space (no reflections through 2-dimensional planes). Explain your calculations.

Problem 3. \((\text{Cosets Partition } \Leftrightarrow \text{Subgroup})\) Let \(S\) be a subset of a group \(G\) that contains the identity element, and such that the left cosets \(aS\) partition \(G\). That is, for every \(a, b \in G\), either \(aS = bS\) or \(aS \cap bS = \emptyset\). Prove that \(S\) is a subgroup of \(G\). (Hint: first characterize the cosets \(aS\) for \(a \in S\).)
Problem 4. (Gallian 8.20)

1. [AM106-A] Show that if $H$ and $K$ are finite subgroups of a group $G$ such that $|H|$ and $|K|$ are relatively prime, then $H \cap K = \{e\}$.

2. [AM206-A] Let $G$ be a group of order $pq$, where $p$ and $q$ are primes such that $p < q$. Prove that $G$ does not contain two distinct subgroups of order $q$.

Problem 5. (Gallian 8.26) Find a subgroup of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ that is not of the form $H \oplus K$, where $H$ is a subgroup of $\mathbb{Z}_4$ and $K$ is a subgroup of $\mathbb{Z}_2$.

Problem 6. (Testing Squares) For this problem, you may use the fact (which we haven’t proven) that for an odd prime $p$ and every positive integer $n$, $\mathbb{Z}_{p^n}^*$ is cyclic.

1. Provide an efficient (polynomial-time) algorithm that given the prime factorization of an odd number $N$ and an element $x \in \mathbb{Z}_N^*$, decides whether $x$ is a square in $\mathbb{Z}_N^*$ (i.e. whether there exists a $y \in \mathbb{Z}_N^*$ such that $y^2 \mod N = x$). (You may use the solution to Problem 6 on Problem Set 2.)

2. Use your algorithm to determine which of the following elements of $\mathbb{Z}_{315}^*$ are squares: 109, 226, 104, 187. (You don’t need to show all calculations, but enough to indicate that you are using your algorithm.)

There is no known polynomial-time algorithm for testing squareness (aka quadratic residuosity) modulo $N$ without being given the factorization of $N$, and indeed a number of cryptographic protocols are built upon the assumption that this problem is inherently intractable.