MATH 113 HOMEWORK 4
DUE MONDAY, JULY 20TH

1. Review

You do not need to submit solutions for these problems.

Problem 1.1. **Memorize** and **understand** the proofs of the following theorems from class:

(1) Every subgroup of a cyclic group is cyclic.
(2) Lagrange's theorem. (A proof of this should constitute: show that the left cosets of H in G form a partition of G, show that gH has the same number of elements as H, and from this deduce Lagrange's theorem).

Problem 1.2. Let ζ be a primitive 15th root of unity (for example, take $\zeta = \mathrm{cis}(\frac{2\pi}{15})$). Draw a picture that shows all of the elements of the subgroup of the circle group C generated by ζ. For each element in this group, calculate its order, and use some colored pencils or otherwise to distinguish elements of each different order. Pictorially represent the various subgroups of this group.

Problem 1.3. Show that the group $(\mathbb{Z}/13\mathbb{Z})^\times$ is cyclic by finding a generator. List off the powers of your generator, and do the same thing as in the last exercise: calculate the order of each element of this group, by using the formula $o(a^k) = \frac{o(a)}{\gcd(k, o(a))}$. Then find all subgroups of this group, and a generator for each subgroup.

Problem 1.4. Review and practice doing computations in S_n and D_n. Specifically, in S_n, practice:

(1) Computing products of cycles,
(2) Decomposing permutations into products of disjoint cycles, and using this to determine the order of a permutation,
(3) Computing the sign of a permutation,
(4) Finding all the cycle types (a.k.a. cycle structures) in S_n, and determining which are cycle types in A_n, and
(5) Writing any cycle as a product of transpositions.

In D_n, practice composing elements and simplifying the result to an expression of the form $r^k s^\ell$, where $0 \leq k < n$ and ℓ is either 0 or 1. Know the basic relations: $srs = r^{-1}, r^n = 1 = s^2$. Be able to show, for example, that $sr^k s = r^{-k}$ by applying these relations.

2. Basic Problems

Problem 2.1. Show that every group of order 4 is isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 2.2. Use Fermat's Little Theorem to show that if $p \in \mathbb{N}$ is prime and $p \equiv 3 (\text{mod } 4)$ then there is no solution to the equation

$$x^2 \equiv -1 (\text{mod } p).$$

Give an example that shows that this equation *can* have solutions if $p \equiv 1 (\text{mod } 4)$.

Problem 2.3. Let G be a group. Recall that an *automorphism* of G is an isomorphism $f : G \to G$.

(1) Show that the set of automorphisms of G forms a group; we denote this group $\text{Aut}(G)$.
(2) Show that $\text{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.
(3) Calculate $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, and show that this group is isomorphic to a group we are already very familiar with.

3. Basic Problems Part 2

Problem 3.1. Do Judson, Ch. 9, Exercise 6.

Problem 3.2. Let G be a group and let H be a normal subgroup of G such that $[G : H]$ is finite. Suppose there is some element $g \in G$ such that $g \notin H$ but $g^2 \in H$. Show that $[G : H]$ is even.

Problem 3.3. Let G be a group and let H be a subgroup of G. Show that H is normal in G if and only if the set of left cosets of H is equal to the set of right cosets of H, i.e.

$$\{gH \mid g \in G\} = \{hG \mid g \in G\}.$$

Use this to give a second proof that if $[G : H] = 2$ then H is normal.

Problem 3.4. Let G be a group. Recall that the *center* $Z(G)$ of G is defined by

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

(1) Show that $Z(G)$ is a normal subgroup of G.
(2) Calculate $Z(D_4)$.

4. Creative Problem

Problem 4.1. Due at office hours on the week of July 20th-23rd: come up with a list of five questions you would like to explore for your final project. Try to make your questions open-ended; an ideal example (which you shouldn't pick) is: "which groups $(\mathbb{Z}/n\mathbb{Z})^\times$ are cyclic?" Come to office hours on the 22nd or 23rd (or arrange a meeting with me outside of class if you can't attend office hours) to discuss your ideas.