MATH 120 PRACTICE FINAL EXAM

Give complete proofs except for problem 1, where answers will suffice. Each problem is worth the same. The final two problems are intended to be more challenging.

1. (a) Let G be a group. The action of G on itself by multiplication on the right by g^{-1} is a left-action or right-action. Which one?
(b) How many elements of S_5 have order 3? How many 3-Sylow subgroups are there? Verify Sylow's theorem in this case.
(c) State the class equation for a group G. The proof involves a group action of G on some set. What is the action?

2. Use Lagrange's theorem on the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove Euler's theorem: if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

3. Let G be a finite group with a normal subgroup K. If $|K|$ and $[G : K]$ are relatively prime, prove that K is the unique subgroup of G having order $|K|$.

4. Show that *every* 2-Sylow subgroup of S_4 is isomorphic to D_8.

5. Let $K_4 = \mathbb{Z}/2 \times \mathbb{Z}/2$. Show that $\mathrm{Aut}(K_4) \cong S_3$. Let $\phi : S_3 \to \mathrm{Aut}(K_4)$ be an isomorphism. Show that $K_4 \rtimes_\phi S_3 \cong S_4$. (*Hint:* Show that S_4 is a semidirect product of K_4 and S_3, and figure out the induced action of S_3 on K_4.)

6. How many ideals does $\mathbb{Z}/(10)$ have? $\mathbb{Z}/(36)$? $\mathbb{Z}/(100)$? For which $n \in \{1, \dots, 100\}$ does $\mathbb{Z}/n$ have an *odd* number of ideals?

7. Show that $\mathbb{Z}[i]/(7)$ is a field. How many elements does it have?

8. Suppose a finite group G acts transitively on a finite set A (i.e. for any a and $a' \in A$, there is some g with $ga = a'$; there is one orbit). Each element of G has a certain number of fixed points in A, i.e. for $g \in G$, there are some $a \in A$ with $ga = a$. What is the average number (over all $g \in G$) of fixed points? (Fancy translation: what is the expected number of fixed points of a random element of G?)

9. Note that $\omega = \frac{-1+\sqrt{-3}}{2}$ is a cube root of 1, and $\omega^2 + \omega + 1 = 0$.
(a) Prove that the subset $\{x + y\omega \in \mathbb{Z}[\omega] : x + y \text{ is divisible by } 3\}$ is an ideal of $\mathbb{Z}[\omega]$. Is it prime?
(b) Show that $\mathbb{Z}[\omega]$ is a Euclidean domain, hence a Unique Factorization Domain. (Hint: recall the proof for the Gaussian integers $\mathbb{Z}[i]$.) There will be a problem on the final following up on this.