Group Problems.

1. Let $G$ be a group. Given $a \in G$ define the centralizer $Z(a) := \{b \in G : ab = ba\}$. Prove that $Z(a) \leq G$. For which $a \in G$ is $Z(a) = G$?

2. We say $a, b \in G$ are conjugate if there exists $g \in G$ such that $a = gb^{-1}$. Recall (HW2.8) that this is an equivalence relation. Let $C(a) := \{b \in G : \exists g \in G, a = gb^{-1}\}$ denote the conjugacy class of $a \in G$. Prove that $|C(a)| = [G : Z(a)]$.

3. On HW2 you proved that $\text{Aut}(\mathbb{Z})$ is the group with two elements. Now prove that $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. (Hint: An automorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is determined by $\varphi(1)$. What are the possibilities?) Taking $n = 0$, we recover the fact that $\text{Aut}(\mathbb{Z}) \approx \mathbb{Z}^\times = \{\pm 1\}$.

4. Let $H, K$ be subgroups of $G$. Prove that:
   
   (a) If $H \leq G$ then $HK := \{hk \in G : h \in H, k \in K\}$ is a subgroup of $G$.
   
   (b) Moreover, if $H \cap K = \{1\}$ and if $hk = kh$ for all $h \in H, k \in K$ then $HK$ is isomorphic to the direct product group $H \times K := \{(h, k) : h \in H, k \in K\}$ with the componentwise product. (Hint: What could the isomorphism possibly be? Really?)

5. Let $G$ be a cyclic group of order $n$. Prove that every subgroup of $G$ is cyclic and has order $d$ for some $d|n$. Conversely, prove that for every $d|n$ there exists a subgroup of order $d$. Bonus: Prove that there is exactly one subgroup of order $d|n$.

Ring Problems.

A ring is a tuple $(R, +, \times, 0, 1)$ such that $(R, +, 0)$ is an abelian group, $(R, \times, 1)$ is a semigroup (associative with identity 1, maybe no inverses, maybe not abelian) and for all $a, b, c \in R$ we have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

6. Let $R$ and $S$ be rings. What is the correct definition of a ring homomorphism $\varphi : R \to S$? Hint: You will need $\varphi(1_R) = 1_S$. Suppose that $R$ and $S$ are isomorphic as rings. Prove that the corresponding groups of units $R^\times$ and $S^\times$ are isomorphic as groups.

7. Let $R$ be a (possibly non-commutative) ring. Prove that:

   (a) For all $a \in R$ we have $0a = a0 = 0$.
   
   (b) For all $a, b \in R$ we have $(-a)(-b) = ab$. (Hint: Think about $ab + a(-b)$. Think about $(-a)(-b) + a(-b)$. Now if a child asks you why negative $\times$ negative is positive, you will have an answer.)

8. (Chinese Remainder Theorem) For all $a, b \in \mathbb{Z}$ define the notation $[a]_b = a + b\mathbb{Z}$. Now let $m, n \in \mathbb{Z}$ be coprime. Prove that the map $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi([a]_{mn}) := ([a]_m, [a]_n)$ is a ring isomorphism. (Hint: The hard part is to show surjectivity. Since $m, n$ are coprime we can write $1 = xm + yn$. What does $\varphi$ do to $bxm + ayn$?)

Let $R$ be a ring. We say that $R$ is an integral domain if it is commutative and if for all $a, b \in R$ we have $ab = 0$ implies $a = 0$ or $b = 0$ (i.e. $R$ has no “zero divisors”). We say that $R$ is a field if it is commutative and if every nonzero $a \in R$ has a multiplicative inverse.

9. Prove that a finite integral domain is a field. Give an example to show that an infinite integral domain need not be a field. (Hint: Given $a \in R$ consider the map $R \to R$ defined by $x \mapsto ax$. Is it injective? Surjective?)