1. The Second Isomorphism Theorem. Let H and K be subgroups of $(G,*,\varepsilon)$ and suppose that at least one of these subgroups is normal. Let's say $K\subseteq G$ is normal.

(a) Show that the product set $H*K=\{h*k:h\in H,k\in K\}$ is a subgroup of G.
(b) Show that $K\subseteq H*K$ is a normal subgroup, hence the group $(H*K)/K$ exists.
(c) Show that the function $\varphi:H\to(H*K)/K$ defined by $\varphi(h):=h*K$ is a surjective group homomorphism.
(d) Show that $\ker\varphi=H\cap K$, and then use the First Isomorphism Theorem to show that

$$\frac{H}{H\cap K}\cong\frac{H*K}{K}.$$

(e) If G is finite, use part (d) to show that $\#(H*K)\cdot\#(H\cap K)=\#H\cdot\#K$.

2. Size of a Product Set. Given two subgroups $H,K\subseteq(G,*,\varepsilon)$ you showed on a previous homework that the product set $H*K=\{h*k:h\in H,k\in K\}\subseteq G$ need not be a subgroup, in which case Problem 1(d) makes no sense. Nevertheless, you will show that 1(e) is still true.

(a) Prove that $h(gK):=(h*g)K$ defines an action of H on the set of cosets $X=G/K$.
(b) For the specific coset $K\in X$, show that $\text{Stab}(K)=H\cap K$.
(c) For the specific coset $K\in X$, show that $\#\text{Orb}(K)=\#(H*K)/\#K$. [Hint: Show that the set $H*K$ is a disjoint union of cosets of K.]
(d) Now combine (b) and (c) with the Orbit-Stabilizer Theorem to prove the result.

3. Groups of Size p^2 are Abelian. Let $p\geq 2$ be prime.

(a) For any group $(G,*,\varepsilon)$, the *center* $Z(G)=\{a\in G:\forall b\in G,a*b=b*a\}$ is a normal subgroup. If the quotient group $G/Z(G)$ is cyclic, prove that G must be abelian. [Hint: Suppose that $G/Z(G)$ is generated by the coset $a*Z(G)$. Then every element of G has the form a^k*z for some $z\in Z(G)$.]
(b) For any group $(G,*,\varepsilon)$ with $\#G=p^k$ (for $k\geq 1$), show that $p|Z(G)$. [Hint: The *class equation* says that $\#G=\#Z(G)+\sum_i\#K(a_i)$ where the sum is over the nontrivial conjugacy classes: $\#K(a_i)\geq 2$. Now use Orbit-Stabilizer.]
(c) Finally, let $\#G=p^2$. Use parts (a) and (b) to prove that G is abelian. [Hint: By Lagrange's Theorem the center must have size 1, p or p^2.]

4. There Are Only Two Groups of Size p^2. Let $p\geq 2$ be prime and let $(G,*,\varepsilon)$ be a group with p^2 elements. If $G\not\cong\mathbb{Z}/p^2\mathbb{Z}$, we will show that G must be isomorphic to the direct product $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

(a) Suppose that G is not cyclic and consider any $\varepsilon\neq a\in G$. Show that $\#\langle a\rangle=p$.
(b) Now pick any element $b\in G\setminus\langle a\rangle$ and consider the two groups $H=\langle a\rangle$ and $K=\langle b\rangle$. Prove that $H\cap K=\{\varepsilon\}$. [Hint: Use Lagrange.]
(c) Conclude from Problem 1(e) or 2 that $\#(H*K)=p^2$ and hence $G=H*K$.
(d) Show that the function $\varphi:\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\to G$ defined by $(k,\ell)\mapsto a^k*b^\ell$ is a group isomorphism. [Hint: Problem 3 implies that φ is a homomorphism, part (b) implies that φ is injective and part (c) implies that φ is surjective.]

5. Cauchy's Theorem. Consider a finite group G and a prime factor $p|\#G$. Cauchy's Theorem says that there exists an element $g \in G$ of order p. In order to prove this, we consider the set of p-tuples of group elements whose product (in order) is the identity:

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = \varepsilon\}.$$

Note that $\#X = (\#G)^{p-1}$ because the group elements $g_1, \ldots, g_{p-1}$ can be chosen freely, but then we must have $g_p = g_{p-1}^{-1} \cdots g_1^{-1}$. In particular, since $p|\#G$ and $p \geq 2$ we must have $p|\#X$.

(a) If $g \neq \varepsilon$ and $(g, g, \ldots, g) \in X$, show that g is an element of order p.

(b) Prove that $(g_1, g_2, \ldots, g_p) \in X$ implies $(g_2, \ldots, g_p, g_1) \in X$. This shows that the cyclic group $C_p \subseteq S_p$ generated by the p-cycle $c = (1, 2, \ldots, p)$ acts on the set X.

(c) Use Orbit-Stabilizer to show that every orbit of this action has size 1 or p.

(d) Note that $\{(\varepsilon, \ldots, \varepsilon)\} \subseteq X$ is an orbit of size 1. Show that there is at least one more orbit of size 1, and then use part (a) to show that G contains an element of order p. [Hint: If there were no other orbit of size 1 then by part (c) every other orbit would have size p, which would imply that $\#X - 1$ is divisible by p.]

6. The Symmetric Group is Not Solvable[1] (Optional). Let $n \geq 5$ and consider the symmetric group S_n. Assume for contradiction that there exists a chain of subgroups

$$S_n = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{\text{id}\}$$

with the property that for each i the subgroup $G_{i+1} \subseteq G_i$ is normal and the quotient group G_i/G_{i+1} is abelian. Let $X \subseteq S_n$ be the subset of 3-cycles. We will obtain a contradiction by showing that $X \subseteq \{\text{id}\}$.

(a) Show that every 3-cycle $c \in X$ has the form $c = c_1 c_2 c_1^{-2} c_2^{-1}$ for some 3-cycles $c_1, c_2 \in X$. [Hint: Consider any n-cycle $c = (ijk)$. Since $n \geq 5$ we may choose two more numbers ℓ, m not in the set $\{i, j, k\}$. Check that $(ijk) = (jkm)(i\ell j)(jkm)^{-1}(i\ell j)^{-1}$.]

(b) If $X \subseteq G_i$ for some i, show that we also have $X \subseteq G_{i+1}$. [Hint: Consider any $c \in X$, which from part (a) can be expressed as $c = c_1 c_2 c_1^{-1} c_2^{-1}$ for some $c_1, c_2 \in X$. Use the fact that the group G_i/G_{i+1} is abelian to show that the coset cG_{i+1} equals G_{i+1}.]

[1] This terminology is inspired by Galois' theorem on the solvability of polynomial equations by radicals. We will discuss this next semester.