Math 561/661 **Fall 2023**
Homework 6 **Drew Armstrong**

---

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 $\#(H * K) \cdot \#(H \cap K) = \#H \cdot \#K$.

(a): Let $H, K \subseteq (G, *, \varepsilon)$ be subgroups and let $K \subseteq G$ be normal. This means that for any $g \in G$ and $k \in K$ there exists some $k' \in K$ such that $k * g = g * k'$. We will use this property to show that $H * K \subseteq G$ is a subgroup.

So consider any two elements $h_1 * k_1$ and $h_2 * k_2$ in $H * K$. Since H and K are subgroups of G we know that $h_1 * h_2^{-1} \in H$, $h_2^{-1} \in H$ and $k_1 * k_2^{-1} \in K$. Putting $g = h_2^{-1}$ and $k = k_1 * k_2^{-1}$ into the previous remark gives
$$\begin{aligned}(h_1 * k_1) * (h_2 * k_2)^{-1} &= h_1 * (k_1 * k_2^{-1}) * h_2^{-1} \\ &= h_1 * h_2^{-1} * k',\end{aligned}$$
for some element $k' \in K$, and hence $(h_1 * k_1) * (h_2 * k_2)^{-1} \in H * K$.

(b): Note that K is a subset of $H*K$ since every element $k \in K$ has the form $k = \varepsilon * k \in H*K$. The fact that K is a normal subgroup of $H * K$ follows trivially from the assumption that K is a normal subgroup of G. Hence the quotient group $H * K/K$ exists.

(c): Define the function $\varphi : H \to (H * K)/K$ by $\varphi(h) := (h * \varepsilon) * K = h * K$. The fact that this is a group homomorphism follows from the definition of coset multiplication:
$$\varphi(h_1) * \varphi(h_2) = (h_1 * K) * (h_2 * K) := (h_1 * h_2) * K = \varphi(h_1 * h_2).$$
To see that φ is surjective, consider any coset $(h * k) * K \in (H * K)/K$, with $h \in H$ and $k \in K$. Recall that for any $a, b \in G$ we have $a * K = b * K$ if and only if $a^{-1} * b \in K$. Taking $a = h$ and $b = h * k$ gives $a^{-1} * b = h^{-1} * h * k = k \in K$ and hence
$$(h * k) * K = h * K = \varphi(h).$$

(d): For any $a \in G$ recall that $a * K = K$ if and only if $a \in K$. Since the coset K is the identity element of the quotient group $(H * K)/K$, we have[1]
$$\ker \varphi = \{h \in H : h * K = K\} = \{h \in H : h \in K\} = H \cap K.$$
It follows from the First Isomorphism Theorem that
$$\frac{H}{H \cap K} = \frac{H}{\ker \varphi} \cong \operatorname{im} \varphi = \frac{H * K}{K}.$$

---

[1]Since kernels are normal, it follows from this that $H \cap K$ is a normal subgroup of H, though this is easy enough to check directly.

(e): If G is a finite group then it follows from part (d) and Lagrange's Theorem that

$$\begin{aligned}
\#\left(H/(H\cap K)\right) &= \#\left((H*K)/K\right) \\
\#H/\#(H\cap K) &= \#(H*K)/\#K \\
\#H\cdot\#K &= \#(H*K)\cdot\#(H\cap K).
\end{aligned}$$

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 $\mathrm{Stab}(K) = H\cap K$.
(c) For the specific coset $K \in X$, show that $\#\mathrm{Orb}(K) = \#(H*K)/\#K$. [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.

(a): Let H and K be subgroups of $(G, *, \varepsilon)$ and consider the set $X = G/K$ of left cosets of K. We do not assume that $K \subseteq G$ is normal, hence $X = G/K$ need not be a group. I claim that the rule $h\cdot(g*K) := (h*g)*K$ defines an action of the group H on the set X. Indeed, for $h=\varepsilon$ we have $\varepsilon\cdot(g*K) = (\varepsilon*g)*K = g*K$, and for any $h_1, h_2 \in H$ we have

$$h_1\cdot(h_2\cdot(g*K)) = h_1\cdot((h_2*g)*K) = (h_1*h_2*g)*K = (h_1*h_2)\cdot(g*K).$$

(b): For the specific coset $K = \varepsilon * K \in X$ we have

$$\begin{aligned}
\mathrm{Stab}(K) &= \{h\in H : h\cdot(\varepsilon*K) = \varepsilon*K\} \\
&= \{h\in H : h*K = K\} \\
&= \{h\in H : h\in K\} \\
&= H\cap K.
\end{aligned}$$

This need not be a normal subgroup of H.

(c): Note that every coset $h\in K$ with $h\in H$ is contained in the product set $H*K$. Furthermore, every element $h*k\in H*K$ is contained in the coset $h*K$. This shows that $H*K$ is equal to the union of cosets in the set $\mathrm{Orb}(K) = \{h*K : h\in H\}$. If G is finite then $n := \#\mathrm{Orb}(K)$ is finite and we can choose some orbit representatives $h_1,\ldots,h_n\in H$ so that

$$H*K = (h_1*K)\sqcup(h_2*K)\sqcup\cdots\sqcup(h_n*K).$$

Then since each coset has size $\#K$ we get

$$\begin{aligned}
\#(H*K) &= \#(h_1*K) + \#(h_2*K) + \cdots + \#(h_n*K) \\
&= \#K + \#K + \cdots + \#K \\
&= n\cdot\#K \\
&= \#\mathrm{Orb}(K)\cdot\#K.
\end{aligned}$$

(d): It follows from the Orbit-Stabilizer Theorem that

$$\begin{aligned}
\#\mathrm{Orb}(K) &= \#H/\#\mathrm{Stab}(K) \\
\#(H*K)/\#K &= \#H/\#(H\cap K) \\
\#(H*K)\cdot\#(H\cap K) &= \#H\cdot\#K.
\end{aligned}$$

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.]

(a): Suppose that the quotient group $G/Z(G)$ is cyclic, generated by some coset $g * Z(G)$. This implies that every coset of $Z(G)$ has the form $g^k * Z(G)$ for some $k \in \mathbb{Z}$. Since G is covered by the cosets of $Z(G)$ is follows that every element of G has the form $g^k * a$ for some $k \in \mathbb{Z}$ and $a \in Z(G)$. Finally, for any two elements $g^{k_1} * a_1$ and $g^{k_2} * a_2$ in G we have

$$\begin{aligned}
(g^{k_1} * a_1) * (g^{k_2} * a_2) &= g^{k_1} * g^{k_2} * a_1 * a_2 && a_1 \in Z(G) \\
&= g^{k_1+k_2} * a_1 * a_2 \\
&= g^{k_2+k_1} * a_1 * a_2 \\
&= g^{k_2} * g^{k_1} * a_1 * a_2 \\
&= (g^{k_2} * a_2) * (g^{k_1} * a_1). && a_2 \in Z(G)
\end{aligned}$$

(b): For any group $(G, *, \varepsilon)$ the class equation says that

$$\#G = \#Z(G) + \sum_i \#K(a_i),$$

where $a_i \in G$ are representatives for the non-trivial conjugacy classes: $\#K(a_i) \geq 2$. By Orbit-Stabilizer we have $\#K(a_i) = \#G/\#Z(a_i)$ and hence each $\#K(a_i)$ divides $\#G$. Now suppose that $\#G = p^k$ is a power of a prime. Since $\#K(a_i)$ is a divisor of $\#G$ and $\#K(a_i) \neq 1$ we see that p divides $\#K(a_i)$ for each i. Finally, since p divides $\#G$ and $\#K(a_i)$ for each i, the class equation tells us that p divides $\#Z(G)$.

(c): Now let $\#G = p^2$. Since the center $Z(G)$ is a subgroup of G, Lagrange's Theorem tells us that $\#Z(G)$ equals 1, p or p^2. Part (b) tells us that $\#Z(G) = 1$ is impossible. If $\#Z(G) = p^2$ then we have $Z(G) = G$ and hence G is abelian. Otherwise, if $\#Z(G) = p$ then the quotient group $G/Z(G)$ has size $p^2/p = p$. In this case, since any group of prime order is cyclic, it follows from part (a) that G is abelian.

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.]

(a): Let $\#G = p^2$ for some prime p and suppose that G is not cyclic. Consider any $\varepsilon \neq a \in G$. By Lagrange, the cyclic subgroup $\langle a \rangle$ has size 1, p or p^2. The first is impossible because $a \neq \varepsilon$ and the last is impossible since $\#\langle a \rangle = p^2$ implies $\langle a \rangle = G$, which contradicts our assumption that G is not cyclic. Hence we must have $\#\langle a \rangle = p$.

(b): Now pick any $b \in G \setminus \langle a \rangle$ and consider the groups $H = \langle a \rangle$ and $K = \langle b \rangle$. By the same argument as in part (a) we know that $\#K = p$. Since $H \cap K$ is a subgroup of H and K, Lagrange's Theorem tells us that $\#(H \cap K) = 1$ or p. The latter implies that $H = H \cap K = K$, which is impossible because $b \in K \setminus H$. Hence we must have $\#(H \cap K) = 1$.

(c): It follows from Problem 2 that[2]

$$\#(H * K) = \#H \cdot \#K / \#(H \cap K) = p^2/1 = p^2$$

and hence $H * K = G$.

(d): Finally, I claim 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. The fact that φ is well-defined follows from the facts that $a^p = \varepsilon$ and $b^p = \varepsilon$. Indeed, if $k_1 \equiv k_2$ and $\ell_1 \equiv \ell_2 \bmod p$ then we have $a^{k_1} = a^{k_2}$ and $b^{\ell_1} = b^{\ell_2}$, hence

$$\varphi(k_1, \ell_1) = a^{k_1} * b^{\ell_1} = a^{k_2} * b^{\ell_2} = \varphi(k_2, \ell_2).$$

The fact that φ is a homomorphism follows from Problem 3, which says that G is abelian. Indeed, for any (k_1, ℓ_1) and (k_2, ℓ_2) we have

$$\begin{aligned}
\varphi(k_1, \ell_1) * \varphi(k_2, \ell_2) &= (a^{k_1} * b^{\ell_1}) * (a^{k_2} * b^{\ell_2}) \\
&= a^{k_1} * a^{k_2} * b^{\ell_1} * b^{\ell_2} && (a * b = b * a) \\
&= a^{k_1 + k_2} * b^{\ell_1 + \ell_2} \\
&= \varphi(k_1 + k_2, \ell_1 + \ell_2).
\end{aligned}$$

The fact that φ is surjective follows from part (c), which implies that

$$G = H * K = \langle a \rangle * \langle b \rangle = \{a^k * b^\ell : k, \ell \in \mathbb{Z}\}.$$

Finally, to see that φ is injective we will use part (b), which says that $H \cap K = \{\varepsilon\}$. Indeed, suppose that we have $\varphi(k_1, \ell_1) = \varphi(k_2, \ell_2)$, so that

$$\begin{aligned}
a^{k_1} * b^{\ell_2} &= a^{k_2} * b^{\ell_2} \\
a^{k_1 - k_2} &= b^{\ell_2 - \ell_1}. && (a * b = b * a)
\end{aligned}$$

Since the left side is in H and the right side is in K we must have $a^{k_1 - k_2} = \varepsilon$ and $b^{\ell_2 - \ell_1} = \varepsilon$. This implies that $k_1 \equiv k_2$ and $\ell_1 \equiv \ell_2 \bmod p$, as desired.

Remark: In summary, we have shown that every group of size p^2 (with p prime) is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. As you see, the proof was not trivial. The hardest part was to show that a group of size p^2 must be abelian. A group of size p^k with $k \geq 3$ need not be abelian. For example, there are two non-abelian groups of size 2^3: the dihedral and quaternion groups. Non-abelian groups of size p^k can be extremely complicated. On the other hand, the Fundamental Theorem of Finite Abelian Groups says that any finite abelian group is isomorphic to a direct product of cyclic groups, which is nice. Maybe we will see that theorem next semester.

[2] We know from Problem 3 that G is abelian, hence we could use Problem 1(e), but it is better not to assume what we don't need.

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.]

(a): If $(g, g, \ldots, g) \in X$ then by definition we have $g^p = gg \cdots g = \varepsilon$. This implies that $\#\langle g \rangle$ divides p, which, since p is prime, implies $\#\langle g \rangle = 1$ or $\#\langle g \rangle = p$. But the first possibility implies $g = \varepsilon$, which contradicts our assumption. Hence $\#\langle g \rangle = p$.

(b): Let $(g_1, g_2, \ldots, g_p) \in X$ so that $g_1 g_2 \cdots g_p = \varepsilon$. Then conjugating by g_1 gives

$$\begin{aligned} g_1 g_2 \cdots g_p &= \varepsilon \\ g_1^{-1} g_1 g_2 \cdots g_p g_1 &= g_1^{-1} \varepsilon g_1 \\ g_2 \cdots g_p g_1 &= g_1^{-1} g_1 \\ g_2 \cdots g_p g_1 &= \varepsilon, \end{aligned}$$

and hence $(g_2, \cdots, g_p, g_1) \in X$. Thus the function $\varphi : G^p \to G^p$ defined by

$$\varphi(g_1, g_2, \ldots, g_p) := (g_2, \cdots, g_p, g_1)$$

sends elements of X to elements of X. Note that the map φ has order p, hence X is acted on by the following cyclic group of size p:

$$\langle \varphi \rangle = \{\mathrm{id}, \varphi, \varphi^2, \ldots, \varphi^{p-1}\}.$$

(c): For any element $x \in X$ the Orbit-Stabilizer Theorem says that

$$\begin{aligned} \#\mathrm{Orb}(x) &= \#\langle \varphi \rangle / \#\mathrm{Stab}(x) \\ \#\mathrm{Orb}(x) &= p / \#\mathrm{Stab}(x) \\ \#\mathrm{Orb}(x) \cdot \#\mathrm{Stab}(x) &= p. \end{aligned}$$

Since p is prime, this tells us that every orbit has size 1 or p.

(d): Note that $\mathrm{Orb}((\varepsilon, \ldots, \varepsilon)) = \{(\varepsilon, \ldots, \varepsilon)\}$ is an orbit of size 1. From part (a) we know that the other orbits of size 1 are in bijection with elements of G of order p. Let n be the number of elements of G of order p. Then since X decomposes as a disjoint union of orbits of size 1 and p we must have

$$\begin{aligned} \#X &= 1 + \underbrace{1 + \cdots + 1}_{n \text{ times}} + p + p + \cdots + p \\ &= 1 + n + p(\text{something}). \end{aligned}$$

Since p divides $\#X$ this implies that $n + 1 \equiv 0 \bmod p$. In particular, $n \neq 0$.

6. The Symmetric Group is Not Solvable[3] (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}.]

(a): This is just a weird observation. The hint says it all.

(b): Suppose for induction that $X \subseteq G_i$. Our goal is to show that $X \subseteq G_{i+1}$. To do this, consider any $c \in X$. From part (a) we can write $c = c_1 c_2 c_1^{-1} c_2^{-1}$ for some $c_1, c_2 \in X$. Since $c, c_1, c_2 \in G_i$ we may consider the corresponding cosets in the quotient group G_i/G_{i+1}. To simplify notation we will write these cosets as $[c]$, $[c_1]$ and $[c_2]$. Then since G_i/G_{i+1} is assumed to be abelian we have

$$\begin{aligned}
[c] &= [c_1 c_2 c_1^{-1} c_2^{-1}] \\
&= [c_1][c_2][c_1^{-1}][c_2^{-1}] \\
&= [c_1][c_1^{-1}][c_2][c_2^{-1}] && G_i/G_{i+1} \text{ is abelian} \\
&= [c_1 c_1^{-1}][c_2 c_2^{-1}] \\
&= [\varepsilon][\varepsilon] \\
&= [\varepsilon\varepsilon] \\
&= [\varepsilon].
\end{aligned}$$

We have shown that the cosets cG_{i+1} and $\varepsilon G_{i+1} = G_{i+1}$ are equal, which implies that $c \in G_{i+1}$. Since this holds for $c \in X$ we have shown that $X \subseteq G_{i+1}$.

Remark: We have shown that the symmetric group S_n is not solvable when $n \geq 5$. Next semester we will prove Galois' Theorem, which says that a polynomial equation is solvable by radicals if and only if its corresponding Galois group is solvable. Since the generic equation of degree n has Galois group S_n, the result of Problem 6 will imply that for $n \geq 5$ there does not exist a "formula" expressing the roots in terms of the coefficients.

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