Homework Six

- (3.1.2) Let $\phi : G \to H$ be a homomorphism of groups with kernel K, and let $a, b \in \phi(G)$. Let $X \in G/K$ be the fiber above a and $Y \in G/K$ be the fiber above b. Fix an element u of X. Prove that if $XY = Z$ in G/K and $w \in Z$ then there is some $v \in Y$ such that $uv = w$.

  Note that Z must be the fiber above ab, so $\phi(w) = ab$. Then $\phi(u^{-1}w) = a^{-1}ab = b$, and hence $u^{-1}w \in Y$, so there is some $v \in Y$ such that $u^{-1}w = v$. Multiplying on both sides by u we obtain $w = uv$, with $v \in Y$ as desired.

- (3.2.6) Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals *some* left coset aH of H in G then it equals the left coset gH.

  If $Hg = aH$ for some a, then $1g = g \in aH$, so there is some $h \in H$ such that $g = ah$. But then $a^{-1}g = h \in H$, so $aH = gH$, whence $Hg = gH$.

- (3.2.8) Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = \{1_G\}$.

  We note that $(H \cap K) \leq H$ and $(H \cap K) \leq K$. Thus by Lagrange, we have that $|H \cap K|$ divides both $|H|$ and $|K|$. But since $gcd(|H|, |K|) = 1$ we have $|H \cap K| = 1$, from which the result immediately follows.

- (3.2.16) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ to prove *Fermat's Little Theorem*: If p is prime then $a^p \cong a(modp)$ for all $a \in \mathbb{Z}$.

  Note that $|(\mathbb{Z}/p\mathbb{Z})^{\times}|$ is $p-1$, since all $p-1$ non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ are relatively prime to the prime number p. Thus we have $a^{p-1} = 1(modp)$. Multiplying by a on both sides we have $a^p = a(modp)$.

- Let $f : G \to H$ be a group epimorphism with kernel K. Prove that there is a one-to-one correspondence between subgroups of H and subgroups of G that contain K such that $K \leq A \leq B$ if and only if $f(A) \leq f(B)$.

  First we describe the correspondence ϕ between $subGK = \{A \leq G | K \leq H\}$ and $subH = \{X \leq H\}$. For $A \leq G$ containining K define $\phi(A) = f(A)$, which we've already shown is a subgroup of H. Now define $\psi : subH \to subGK$ by $\psi(X) = f^{-1}(X) = \{g \in G | f(g) \in X\}$. We have already established that this is a subgroup of G, and note that for any $k \in K$, $f(k) = 1_H \in X$ so $K \leq f^{-1}(X)$.

  Now we show that $\psi \circ \phi = id_{subGK}$ and $\phi \circ \psi = id_{subH}$, from which it follows that both ψ and ϕ are one-to-one and onto. Let $A \leq G$ with $K \leq A$. Then $\phi(A) = f(A)$, and

  $$\psi(f(A)) = f^{-1}(f(A)) = \{g \in G | f(g) \in f(A)\}.$$

  Now if $g \in G$ is such that $f(g) = h \in f(A)$, since $h \in f(A)$ there is some $a \in A$ with $f(a) = h$, and we then have $f(g) = f(a)$, and so $f(g^{-1}a) = 1_H$, so $g^{-1}a \in K \leq A$. Thus $gA = aA = A$, so $g \in A$, and $\psi \circ \phi(A) = A$ as desired. Considering $\phi(\psi(X))$ we see $\phi(f^{-1}(X)) = f(f^{-1}(X)) = X$, so $\phi \circ \psi(X) = X$.

Finally we suppose that $K \leq A \leq B$. Then for $h \in f(A)$ we have some $a \in A$ with $f(a) = h$, and since $A \leq B$, $a \in B$, so $h \in f(B)$, and $f(A) \leq f(B)$. Conversely let $X \leq Y \leq H$. Then for $g \in f^{-1}(X)$ we have $f(g) = x \in X$, and $X \leq Y$ implies $x \in Y$, so $f(g) \in Y$, so $g \in f^{-1}(Y)$, and we have $f^{-1}(X) \leq f^{-1}(Y)$.