Math 561/661 **Fall 2018**
Homework 3 **Drew Armstrong**

---

1. Order of a Power. Let G be a group and let $g \in G$ be an element of order n.

(a) For all $k \in \mathbb{Z}$, prove that $\langle g^k \rangle = \langle g^d \rangle$ where $d = \gcd(n, k)$. [Hint: $n\mathbb{Z} + k\mathbb{Z} = d\mathbb{Z}$.]
(b) For any divisor $d|n$ show that g^d has order n/d.
(c) Combine (a) and (b) to prove that for any $k \in \mathbb{Z}$ the element g^k has order $n/\gcd(n, k)$.

2. Multiplication of Subgroups. Let $(G, *, \varepsilon)$ be a group and let $H, K \subseteq G$ be any two subgroups. Consider the Cartesian product of sets

$$H \times K := \{(h, k) : h \in H, k \in K\}$$

and the "multiplication function" $\mu : H \times K \to G$ defined by $\mu(h, k) := h * k$.

(a) Prove that μ is injective if and only if $H \cap K = \{\varepsilon\}$.
(b) We can think of the set $H \times K$ as an abstract group by defining

$$(h_1, k_1) * (h_2, k_2) := (h_1 * h_2, k_1 * k_2) \quad \text{for all } h_1, h_2 \in H \text{ and } k_1, k_2 \in K.$$

In this case we call $(H \times K, *)$ the *direct product* of H and K. Prove that μ is a group homomorphism if and only if we have $h * k = k * h$ for all $h \in H$ and $k \in K$.

(c) The image of $\mu : H \times K \to G$ is the "internal product set"

$$HK := \{h * k : h \in H, k \in K\} \subseteq G.$$

Prove that $HK \subseteq G$ is a subgroup if and only if $HK = KH$.

3. Why Does $AB = I$ Imply $BA = I$? Given a field $\mathbb{F}$ and a positive integer n we define

$$\mathbb{M} := \mathrm{Mat}_n(\mathbb{F}) = \text{the set of } n \times n \text{ matrices with entries in } \mathbb{F}.$$

I claim that this set is a *vector space of dimension* n^2 over the field $\mathbb{F}$. Now consider any two matrices $A, B \in \mathbb{M}$ such that $AB = I$.

(a) Show that the set $B\mathbb{M} := \{BM : M \in \mathbb{M}\}$ is a *vector subspace* of $\mathbb{M}$. In other words, for all matrices $X, Y \in B\mathbb{M}$ and scalars $\alpha, \beta \in \mathbb{F}$, show that $\alpha X + \beta Y \in B\mathbb{M}$.
(b) More generally, for each integer $k \geq 0$ define the set $B^k\mathbb{M} := \{B^k M : M \in \mathbb{M}\}$ and show that $B^{k+1}\mathbb{M}$ is a vector subspace of $B^k\mathbb{M}$.
(c) I claim that a finite-dimensional vector space has no infinite descending chain of subspaces. Use this fact to prove that there exists an integer $k \geq 0$ and a matrix $C \in \mathbb{M}$ satisfying $B^k = B^{k+1}C$.
(d) Let C be as in part (c). Prove that $BC = I$ and hence $C = A$. It follows that $BA = I$.

[Remark: Believe it or not, this is the shortest proof I know.]

4. Conjugation is an Automorphism. Let $(G, *, \varepsilon)$ be a group and let $g \in G$ be any element. Define the function $\varphi_g : G \to G$ by $\varphi_g(a) := g * a * g^{-1}$.

(a) Prove that $\varphi_g : G \to G$ is a bijection.
(b) Prove that $\varphi_g : G \to G$ is a homomorphism, hence it is an *automorphism* of G.
(c) Application: Consider any two elements $a, b \in G$. Prove that the cyclic groups $\langle a * b \rangle$ and $\langle b * a \rangle$ are isomorphic, hence the elements $a * b$ and $b * a$ have the same order.

5. Galois Connection. Let $(P, \leq)$ and $(Q, \leq)$ be posets and let $f : P \to Q$ and $g : Q \to P$ be any functions satisfying

$$p \leq g(q) \iff f(p) \leq q \quad \text{for all } p \in P \text{ and } q \in Q.$$

(a) For all $p \in P$ and $q \in Q$ prove that

$$p \leq g(f(p)) \qquad \text{and} \qquad f(g(q)) \leq q.$$

(b) For all $p_1, p_2 \in P$ and $q_1, q_2 \in Q$ prove that

$$p_1 \leq p_2 \Rightarrow f(p_1) \leq f(p_2) \qquad \text{and} \qquad q_1 \leq q_2 \Rightarrow g(q_1) \leq g(q_2).$$

(c) For all $p \in P$ and $q \in Q$ prove that

$$f(p) = f(g(f(p)) \qquad \text{and} \qquad g(q) = g(f(g(q))).$$

(d) Define the "images" $P' := g[Q] := \{g(q) : q \in Q\}$ and $Q' := f[P] := \{f(p) : p \in P\}$. Prove that these are the same as the sets of "closed elements"

$$P' = \{p \in P : p = g(f(p))\} \quad \text{and} \quad Q' = \{q \in Q : q = f(g(q))\}.$$

(e) Prove that the functions f, g restrict to an isomorphism of posets:

$$f : P' \longleftrightarrow Q' : g.$$

6. Image and Preimage. Let $(G, *, \delta)$ and $(H, \bullet, \varepsilon)$ be groups and let $\varphi : G \to H$ be any group homomorphism. For every subset $S \subseteq G$ we define the *image set*

$$\varphi[S] := \{\varphi(g) : g \in S\} \subseteq H,$$

and for every subset $T \subseteq H$ we define the *preimage set*

$$\varphi^{-1}[T] := \{g \in G : \varphi(g) \in T\} \subseteq G.$$

(a) Show that the function $\varphi^{-1} : H \to G$ exists if and only if $\#\varphi^{-1}[\{h\}] = 1$ for all $h \in H$.
(b) If $S \subseteq G$ is a subgroup prove that the image $\varphi[S] \subseteq H$ is a subgroup.
(c) If $T \subseteq H$ is a subgroup prove that the preimage $\varphi^{-1}[T] \subseteq G$ is a subgroup.
(d) Now you have two functions $\varphi : \mathscr{L}(G) \leftrightarrows \mathscr{L}(H) : \varphi^{-1}$ between the subgroup lattices. Prove that this is a Galois connection.