Math 3063 Abstract Algebra — Prof. Paul Bailey — Project 3 — April 3, 2009 — **Solutions**

Definition 1. Let G be a group. We say that G is *abelian* if $gh = hg$ for all $g, h \in G$.

Problem 1. Let G be a group such that $g^2 = 1$ for every $g \in G$. Show that G is abelian.

Solution. Let $g, h \in G$. Then $g^2 = 1$, $h^2 = 1$, and $(gh)^2 = 1$. Since $(gh)^2 = ghgh$, we have $1 = ghgh$. Multiplying on the left by g gives $g = gghgh = g^2hg = hgh$. Multiplying on the right by h gives $gh = hghh = hgh^2 = hg$. Since g and h were selected arbitrarily from G, $gh = hg$ for every $g, h \in G$, and G is abelian. $\square$

Definition 2. Let G be a group and let $g \in G$. The *order* of G is $|G|$. The *order* of g is the smallest positive integer k such that $g^k = 1$.

Problem 2. Let G be a group of even order. Show that G has an element of order two.

Solution. Let $A = \{g \in G \mid g^2 = 1\}$. Since $1 \in A$, A is nonempty. If $|A|$ is even, then A contains at least one more element, which is necessarily an element of order two.

Let $B = G \smallsetminus A$. Clearly, $|G| = |A| + |B|$. Now $b \in B$ if and only if $b \neq b^{-1}$. Since inverses are unique, B can be partitioned into sets of the form $\{b, b^{-1}\}$. Each such set contains exactly two elements, so $|B|$ is even. Since $|G|$ is even, $|A| = |G| - |B|$ is also even. Thus A has an element of order two. $\square$

Definition 3. Let G be a group and let $H \subset G$. We say that H is a *subgroup* of G, and write $H \leq G$, if

(S0) H is nonempty;

(S1) $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$;

(S2) $h \in H \Rightarrow h^{-1} \in H$.

Problem 3. Let $V = \mathbb{R}^3$; this is a group under addition. Let $T : V \to \mathbb{R}$ be given by $T(x, y, z) = x + y + z$. Let $W = \{\vec{v} \in \mathbb{R}^3 \mid T(\vec{v}) = 0\}$. Show that $W \leq V$.

Solution. To show that $W \leq G$, we verify the three properties of being a subgroup.

(S0) Let $\vec{0} = (0, 0, 0)$. Since $T(\vec{0}) = 0 + 0 + 0 = 0$, we have $\vec{0} \in W$.

(S1) Let $\vec{v}_1, \vec{v}_2 \in W$, where $\vec{v}_1 = (x_1, y_1, z_1)$ and $\vec{v}_2 = (x_2, y_2, z_2)$. Then

$$T(\vec{v}_1 + \vec{v}_2) = (x_1 + x_2) + (y_1 + y_2) + (z_1 + z_2) = (x_1 + y_1 + z_1) + (x_2 + y_2 + z_2) = T(\vec{v}_1) + T(\vec{v}_2) = 0 + 0 = 0.$$

Since $T(\vec{v}_1 + \vec{v}_2) = 0$, we know that $\vec{v}_1 + \vec{v}_2 \in W$.

(S2) Let $\vec{v} \in W$ where $\vec{v} = (x, y, z)$. Then

$$T(-\vec{v}) = T(-x, -y, -z) = -x - y - z = -(x + y + z) = -T(\vec{v}) = -0 = 0.$$

Since $T(-\vec{v}) = 0$, we have $-\vec{v} \in W$. $\square$

Definition 4. Let G be a group. The *center* of G is

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

Problem 4. Let G be a group with a unique element $g \in G$ of order two. Show that $g \in Z(G)$.

Definition 5. Let G be a group and let $H \leq G$.
The *centralizer of H in G* is

$$C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}.$$

Problem 5. Let G be a group, $g \in G$, and $H \leq G$. The *centralizer* of g in H is

$$C_H(g) = \{h \in H \mid h^{-1}gh = g\}.$$

Show that $C_H(g) \leq G$.

Solution. We verify properties **(S0)**, **(S1)**, and **(S2)**.
(S0) Since $1 \in H$ and $g \cdot 1 \cdot g^{-1} = gg^{-1} = 1$, we have $1 \in C_H(g)$.
(S1) Let $h_1, h_2 \in C_H(g)$. Then

$$g^{-1}h_1h_2g = g^{-1}h_1(gg^{-1})h_2g = (g^{-1}h_1g)(g^{-1}h_2g) = h_1h_1.$$

Thus $h_1h_2 \in C_H(g)$.
(S2) Let $h \in C_H(g)$. Then $g^{-1}hg = h$, so $(g^{-1}hg)^{-1} = h^{-1}$. But $(g^{-1}hg)^{-1} = g^{-1}h^{-1}g$, so $g^{-1}h^{-1}g = h^{-1}$, and $h^{-1} \in C_H(g)$. □

Definition 6. Let G be a group and let $g, h \in G$. The *conjugate* of h by g is $g^{-1}hg$.

Problem 6. Let G be a group and let $g, h \in G$.

(a) Show that g and h commute if and only if $g^{-1}hg = h$.

(b) Show that $(g^{-1}hg)^n = g^{-1}h^ng$ (use induction).

(c) Show that if $\text{ord}(h) = n$, then $\text{ord}(g^{-1}hg) = n$.

Solution.
(a) Clearly, $hg = gh \Leftrightarrow g^{-1}hg = g^{-1}gh$, so $hg = gh \Leftrightarrow hg = gh$.
(b) For $n = 1$, we have $(g^{-1}hg)^1 = g^{-1}hg = g^{-1}h^1g$.
Let $n > 1$. By induction, $g^{-1}hg)^{n-1} = g^{-1}h^{n-1}g$. Multiplying both sides by $g^{-1}hg)$ gives

$$g^{-1}hg)^n = g^{-1}h^{n-1}gg^{-1}hg = g^{-1}h^{n-1}hg = g^{-1}h^ng.$$

(c) Suppose $\text{ord}(h) = n$, and let $k = \text{ord}(g^{-1}hg)$. Since $(g^{-1}hg)^n = g^{-1}h^ng = g^{-1} \cdot 1 \cdot g = g^{-1}g = 1$, we have $n \mid k$. Also, $h^k = g(g^{-1}h^kg)g^{-1} = g(g^{-1}hg)^kg^{-1} = g \cdot 1 \cdot g^{-1} = 1$, so $k \mid n$. Since n and k are positive, $k = n$. □