UNIVERSITY OF SOUTH CAROLINA

MATH-546 Algebraic Structures I — Homework 4

Problem 1:

Let G be a group and H, K subgroups of G.

a. Prove that $H \cap K$ is also a subgroup of G.

b. Assume that $H \cup K$ is a subgroup of G. Prove that $H \subseteq K$ or $K \subseteq H$.

Answer 1:

a. $\forall a, b \in H \cap K$:

$$\begin{aligned} b \in H \cap K &\Rightarrow (b^{-1} \in H) \wedge (b^{-1} \in K) && \text{closure} \\ &\Rightarrow b^{-1} \in (H \cap K) \\ &\Rightarrow (ab^{-1} \in H) \wedge (ab^{-1} \in K) && \text{closure} \\ &\Rightarrow ab^{-1} \in (H \cap K) \\ &\Rightarrow H \cap K \leq G && \text{TP 1} \end{aligned}$$

b. Given $H \leq G, K \leq G, (H \cup K) \leq G$:

$$\neg((H \subseteq K) \vee (K \subseteq H)) \Rightarrow \exists h \in (H \setminus K) \wedge \exists k \in (K \setminus H)$$

So consider hk:

$$\begin{aligned} hk &\in H \cup K && \text{closure of } H \cup K \\ hk \in H \cup K &\Rightarrow (hk \in H) \vee (hk \in K) \\ hk \in H &\Rightarrow h^{-1}hk \in H && \text{closure of } H \\ &\Rightarrow k \in H \\ hk \in K &\Rightarrow hkk^{-1} \in K && \text{closure of } K \\ &\Rightarrow h \in K \end{aligned}$$

Problem 2:

Let G be a group and $a \in G$ a fixed element. Let

$$H = \{x \in G \mid ax = xa\}.$$

Prove that H is a subgroup of G.

Answer 2:

Associativity: inherited

Identity: $ae = ea \Rightarrow e \in H$

Inverses: WTS: $x \in H \Rightarrow x^{-1} \in H$:

$$\begin{aligned} xx^{-1} &= x^{-1}x \\ axx^{-1} &= ax^{-1}x \\ xax^{-1} &= ae \\ x^{-1}xax^{-1} &= x^{-1}a \\ ax^{-1} &= x^{-1}a \end{aligned}$$

Closure: $\forall x, y \in H : a(xy) = xay = (xy)a$

Problem 3:

Let G be a group. The center of G is defined as

$$Z(G) = \{x \in G \mid ax = xa \ \ \forall a \in G\}.$$

a. Prove that $Z(G)$ is a subgroup of G.

b. Let $G = GL_2(\mathbb{R})$ (the group of 2×2 invertible matrices with matrix multiplication as operation). Prove that

$$Z(G) = \left\{ \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \middle| \ c \neq 0 \right\}.$$

Answer 3:

a. Let $H_a = \{x \in G \mid ax = xa\}$ then H_a is a subgroup of G (by Problem 2). Then by problem 1a:

$$Z(G) = \{x \in G \mid ax = xa \ \ \forall a \in G\} = \bigcap_{a \in G} H_a$$

is a group.

b. Clearly $\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} = c \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in Z(G)$ since scalars and the identity commute with matrices in $GL_2(\mathbb{R})$.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(G)$ and using invertible matrix $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a & -b \\ c & -d \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ -c & -d \end{bmatrix}$$

so $b = -b$ and $c = -c$ and $b = c = 0$.

Using invertible matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ with $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ d & 0 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & d \\ a & 0 \end{bmatrix}$$

and $a = d$.

Therefore the only matrices in $Z(G)$ are of the form $\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$ where $c \neq 0$.

Problem 4:

For each of the following groups, decide whether the group is cyclic or not. Justify your answers.

a. $\mathbb{Z}_{10}^*$

b. $\mathbb{Z}_{12}^*$

c. $\mathbb{Q}$ (with addition as operation)

d. $\mathbb{R}^*$ (with multiplication as operation)

Answer 4:

a. $\mathbb{Z}_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$: is cyclic
$\langle [3]_{10} \rangle = \{[1]_{10}, [3]_{10}, [9]_{10}, [27]_{10}\} = \{[1]_{10}, [3]_{10}, [9]_{10}, [7]_{10}\} = \mathbb{Z}_{10}^*$

b. $\mathbb{Z}_{12}^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$: not cyclic, each $x \in \mathbb{Z}_{12}^*$ squares to the identity.

c. $\mathbb{Q}$: not cyclic: no integer multiple of $q \in \mathbb{Q}$ is in the interval $(0, |q|)$

d. $\mathbb{R}^*$: not cyclic: a positive generator r can't produce negative numbers, a negative generator can't produce $-r^2$.

Theoretical Problem 1:

Let G be a group and $H \subset G$ a subset. Assume that for all $a, b \in H$, ab^{-1} is also in H. Prove that H is a subgroup of G (satisfies closure, identity and inverses).

Answer 1:

Associativity: inherited

Identity: $a \in H \Rightarrow aa^{-1} = e \in H$

Inverse: $e \in H \wedge a \in H \Rightarrow ea^{-1} = a^{-1} \in H$

Closure: $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$

Theoretical Problem 2:

Prove that every subgroup of $\mathbb{Z}$ is cyclic.

Answer 2:

The two trivial subgroups of $\mathbb{Z}$ are cyclic.

Let G be another subgroup of $\mathbb{Z}$ and let n be the smallest positive integer in G. We assert that $G = n\mathbb{Z}$. If not, then there exists $k \in G$ with $k > n$ such that n does not divide k. But that means that $d = \gcd(n, k) \in G$ as $\gcd(n, k)$ is a linear combination of n and k. Either $d < n$ which contradicts definition of n or $d = n$ and $n \mid k$, another contracdiction.

Theoretical Problem 3:

Let G be a group with $|G| = n$. Prove that G is cyclic if and only if there exists $x \in G$ with $o(x) = n$.

Answer 3:

Lemma: $o(a) = k \iff |\langle a \rangle| = k$
Proof:

- $\Rightarrow$ $|\langle a \rangle| > k$ is impossible since the sequence of a^i repeats at $a^k = e$. $|\langle a \rangle| < k$ means $a^i = a^j$ for $i < j < k$ and $a^{j-i} = e$ with $j - i \neq k$.
- $\Leftarrow$ $|\langle a \rangle| = k$ means $\langle a \rangle$ has k distinct elements and so $a^k = a^i$ for some $i < k$. But then $a^{k-i} = e$ and so $i = 0$ and $o(a) = k$.

G is cyclic means $G = \langle x \rangle$ for some $x \in G$ and $|\langle x \rangle| = n$ therefore $o(x) = n$.

If $o(x) = n$ then $|\langle x \rangle| = n$ and any element of G must be in $\langle x \rangle$ and vice-versa and $\langle x \rangle = G$ and G is cyclic.