Tutorial 2

Problem 1.

a) Let G be a cyclic group. Show that G is abelian.

b) Let $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$. For $A, B \subseteq \mathbb{Z}$, define

$$A + B = \{a + b : a \in A, b \in B\}.$$

Show that $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Solution

a) Since every element is of the form g^i, we have

$$g^i \cdot g^j = g^{i+j} = g^{j+i} = g^j \cdot g^i.$$

b) If $x, y \in a\mathbb{Z} + b\mathbb{Z}$, then one can find integers r, r', s, s' such that $x = ar + bs$ and $y = ar' + bs'$.

Thus, $x - y = a(r - r') + b(s - s') \in a\mathbb{Z} + b\mathbb{Z}$. By the subgroup criterion, $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Problem 2. Let G be a group and $H, K \leq G$.

a) Prove that $H \cap K \leq G$.

b) Give an example of G, H, K where $H \cup K \leq G$ and another where $H \cup K \nleq G$.

c) For what H, K, G do we have that $H \cup K \leq G$? Prove your condition.

Solution

a) For all $r, s \in H \cap K$, we note that $r, s \in H, K$, which implies $rs^{-1} \in H$ and $rs^{-1} \in K$. Putting it together, this means

$$rs^{-1} \in H \cap K.$$

By the subgroup criterion, $H \cap K$ is a subgroup of G.

b) Whenever $K \leq H \leq G$ we have $H \cup K = H \leq H$. For a specific example, we may take $K = 4\mathbb{Z}$ and $H = 2\mathbb{Z}$ with $G = \mathbb{Z}$.

An example where $H \cup K \nleq G$ can be given by $K = 3\mathbb{Z}$ and $H = 2\mathbb{Z}$ with $G = \mathbb{Z}$. To see why this example works, see next part.

c) We claim that $H \cup K \leq G$ if and only if $H \leq K$ or $K \leq H$.

The backward direction gives us $H \cup K = K$ or H which is immediately a subgroup of G.

As for the forward direction, suppose $H \cup K \leq G$ and $K \not\subset H$. Then we have $k \in K$ with $k \notin H$.

Now for any $h \in H$, we have $kh \in H \cup K$. Note that $kh \in H \implies khh^{-1} = k \in H$. This contradicts our assumption. Hence, we must have $kh \in K$. But this tells us that $k^{-1}kh = h \in K$.

Since this holds for any element $h \in H$, it follows that $H \subseteq K$ which means $H \leq K$. Thus, $H \cup K \leq G$ if and only if $H \leq K$ or $K \leq H$.

Problem 3. Let G be a finite group of n elements.

a) Show that each row (resp. column) of the Cayley table of G is a permutation of its elements. [Hint: What happens if the row (resp. column) is not a permutation?]

b) Let G be a group of three elements $\{e, a, b\}$. What are the possible Cayley tables of G? What about $G = \{e, a, b, c\}$?

c) What are the possible Cayley tables of $G = \{e, a, b, c, d\}$?

d) Conclude that a group of ≤ 5 elements must be abelian.

Solution

a) If the coloumns of the Cayley table are names $g_1, g_2, ..., g_n$, then the row of a Cayley table corresponding to element g constitutes the tuple

$$gg_1, gg_2, ..., gg_n$$

If this row is not a permutation, then multiplication-by-g will no longer be a bijective function. This cannot happen as multiplication by g has a two-sided inverse function given by multiplication-by-g^{-1}.

b) The following part of the Cayley table for $\{e, a, b\}$ is immutable i.e. has to be as follows.

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

Since every row and column has to be a permutation, the moment we fill in $a \cdot a$, $a \cdot b$ and $b \cdot a$ are fixed. The last place $b \cdot b$ then follows.

If $a \cdot a = e$, we have

$\cdot$	e	a	b
e	e	a	b
a	a	e	b
b	b	b	*

This table is not a Cayley table for a group as the last row is not a permutation. (b occurs twice).

As such, we must have $a \cdot a = b$, which gives rise to the following Cayley table:

$-$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

For $G = \{e, a, b, c\}$, the potential Cayley tables are:

G	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

G	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

c) Same procedure more tedious. we begin by examing the row of a. this row has to be one of

$$(a, P) : P \textit{ is a permutation of } \{e, b, c, d\}.$$

24 possiblities. After eliminating you will get the following 6 permutations will give you a Cayley table.

$$(a, b, c, d, e), (a, b, d, e, c), (a, c, d, b, e), (a, c, e, d, b), (a, d, c, e, b), (a, d, e, b, c)$$

Fixing this permutation will automatically fix the tables.

d) All these Cayley tables are symmetric about the diagonal, so the groups are abelian.

Problem 4 (Hard). Show that if there are 3 consecutive integers i such that for all $a, b \in G$, $a^i b^i = (ab)^i$, then G is abelian. [Hint: Try to rewrite ab using what we have.]

Solution

For any $a, b \in G$, we have

$$(ab)^k = a^k b^k, \tag{1}$$
$$(ab)^{k+1} = a^{k+1} b^{k+1}, \tag{2}$$
$$(ab)^{k+2} = a^{k+2} b^{k+2}. \tag{3}$$

Multiplying (2) by the inverse of (1) on the right gives us

$$ab = a^{k+1} b^{k+1} (b^{-k} a^{-k}) = a^{k+1} b a^{-k}.$$

Multiplying (3) by the inverse of (2) on the right gives

$$ab = a^{k+2} b^{k+2} (b^{-(k+1)} a^{-(k+1)}) = a^{k+2} b a^{-k-1} = a(a^{k+1} b a^{-k}) a^{-1}.$$

Putting the two equations above together, we get

$$ab = a^{k+2} b a^{-k-1} = a(a^{k+1} b a^{-k}) a^{-1} = a(ab) a^{-1}.$$

Left cancellation of a gives

$$b = aba^{-1},$$

and hence $ba = ab$.

Since this holds for all $a, b \in G$, G is abelian.