Section 6, p66 #1-4,45,46

In Exercises 1 through 4, find the quotient and remainder, according to the division algorithm, where n is divided by n.

1. $n = 42,\ m = 9$

$42 = 4(9) + 6$

2. $n = -42,\ m = 9$

$-42 = -5(9) + 3$

3. $n = -50,\ m = 8$

$-50 = -7(8) + 6$

4. $n = 50,\ m = 8$

$50 = 6(8) + 2$

Theory

45. Let r and s be positive integers. Show that $X = \{nr + ms : n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$

A subgroup is closed under the operation of the group and closed under inverses.

Proof. Consider $a,$ and $b \in X$, where $a = n_1r + m_1s$ and $b = n_2r + m_2s$.

$$\begin{aligned} a + b &= (n_1r + m_1s) + (n_2r + m_2s) \\ &= (n_1r + n_2r) + (m_1s + m_2s) \\ &= (n_1 + n_2)r + (m_1 + m_2)s \end{aligned}$$

Since $n_1 + n_2 \in \mathbb{Z}$ and $m_1 + m_2 \in \mathbb{Z}$, $a + b$ takes the form of elements in X. Now consider $a = nr + ms \in X$. We know a^{-1} exists since a is also in $\mathbb{Z}$.

$$\begin{aligned} a^{-1} &= (nr + ms)^{-1} \\ &= -(nr + ms) && \text{since we are using } \mathbb{Z} \text{ with addition} \\ &= (-n)r + (-m)s \end{aligned}$$

We know $-n$ and $-m \in \mathbb{Z}$, thus $a^{-1} \in X$. Thus X is a subgroup of $\mathbb{Z}$, $X < \mathbb{Z}$ $\square$

46. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n

When we say a has order n, it means that in the cyclic group that $a^n = e$.

Proof. Assume $\langle ab \rangle$ has order n. This means that

$$\begin{aligned} (ab)^n &= e && \text{for some smallest positive integer } n \\ a(ba)^{n-1}b &= e \\ ba(ba)^{-1}ba &= ba \\ (ba)^{n+1} &= ba \\ (ba)^n &= e \end{aligned}$$

Thus, ba has order $\leq n$. Assume that ba has order $< n$, say m. Thus, $(ba)^m = e$. By a similar argument as above, we can show that $(ab)^m = e$. This contradicts our assumption that the order of ab is n.

$\therefore$ the order of ba must be exactly n. $\square$