MATH 111A HOMEWORK 1 SOLUTIONS

---

5) Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Solution. Suppose the contrary that $\mathbb{Z}/n\mathbb{Z}$ is a group. Then its identity element must be $\overline{1}$ since

$$\overline{1} \cdot \overline{m} = \overline{m} = \overline{m} \cdot \overline{1} \quad \text{for all residue classes } \overline{m} \in \mathbb{Z}/n\mathbb{Z}$$

and the identity is unique. Now, let $\overline{m}$ be the inverse of $\overline{0}$, which exists by definition of a group. Then,

$$\overline{0} \cdot \overline{m} = \overline{1} = \overline{m} \cdot \overline{0}$$

which implies $\overline{1} = \overline{0}$. This is a contradiction since $n > 1$. Thus, $\mathbb{Z}/n\mathbb{Z}$ is not group under multiplication.

Alternative solution. Suppose the contrary that $\mathbb{Z}/n\mathbb{Z}$ is a group under multiplication. Then the cancellation law holds (Proposition 2 on o. 20). But $\overline{0} \cdot \overline{1} = \overline{0} = \overline{0} \cdot \overline{0}$ and $\overline{0} \neq \overline{1}$ for $n > 1$. We have a contradiction and so $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group.

---

6) Determine which of the following sets are groups under addition:

a) the set of rational numbers (including $0 = 0/1$) in the lowest terms whose denominators are odd

Solution. Let H be the set. Since $(\mathbb{Q}, +)$ is a group clearly $H \neq \emptyset$, by Problem 26, it suffices to show that H is closed under multiplication and inverses. So let $x, y \in H$. By definition of H, we can write

$$x = \frac{m}{n} \quad \text{and} \quad y = \frac{p}{q}$$

in their lowest terms with $m, n, p, q \in \mathbb{Z}$ and n, q odd. Then

$$x + y = \frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}.$$

Since nq is odd, when reduced to the lowest term, the denominator of this fraction must remain odd. Thus, $x + y \in H$ and so H is closed under multiplication. On the other hand, the inverse of x is

$$-x = -\frac{m}{n} = \frac{-m}{n},$$

which is already in its lowest term by assumption. Since n is odd, we see that $-x \in H$ and so H is closed under inverses also. We hence conclude that $(H, +)$ is a group.

b) the set of rational numbers in the lowest terms whose denominators are even together with 0

Solution. Let H be the set in question. Notice that $\frac{1}{2} \in H$ but $\frac{1}{2} + \frac{1}{2} = \frac{1}{1} \notin H$. It follows that H is not closed under addition and hence is not a group.

---

26) Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e. for all $h, k \in H$ we have $hk, h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

Solution. Since it is already given that H is closed under $\star$ (so $\star$ is a binary operation on H) and inverses, in order to show that $(H, \star)$ is a group, there are only two more things to check.

(1) H is associative: This is clear since $H \subset G$ and $(G, \star)$ is associative.

(2) H has an identity element: Let e be the identity element in G. It will suffice to show that $e \in H$ (so the identity in H is the same as that in G). To that end, first let $h \in H$, which exists since $H \neq \emptyset$ by hypothesis. Since H is closed under inverses, we have $h^{-1} \in H$. Now, H is closed under $\star$ also, which implies that $e = h \star h^{-1} \in H$.

Thus, we conclude that $(H, \star)$ is indeed a group.

---

27) Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

Solution. Let $H = \{x^n \mid n \in \mathbb{Z}\}$ (see p. 20 for the notation x^n). Clearly $H \neq \emptyset$ since $x \in H$. Hence, by Problem 26, it suffices to show that H is closed under multiplication and inverses. So suppose that $x^n, x^m \in H$ with $n, m \in \mathbb{Z}$.

First we show that $x^n x^m = x^{n+m}$ so H is closed under multiplication. There are three cases to consider.

(1) $n, m \geq 0$: Then we have

$$x^n x^m = \underbrace{(x \cdots x)}_{n \text{ times}} \underbrace{(x \cdots x)}_{m \text{ times}} = \underbrace{x \cdots x}_{n+m \text{ times}} = x^{n+m}.$$

(2) $n, m \leq 0$: Then we have

$$x^n x^m = \underbrace{(x^{-1} \cdots x^{-1})}_{|n| \text{ times}} \underbrace{(x^{-1} \cdots x^{-1})}_{|m| \text{ times}} = \underbrace{x^{-1} \cdots x^{-1}}_{|n|+|m| \text{ times}} = x^{-(|n|+|m|)} = x^{n+m}.$$

(3) $n \geq 0, m \leq 0$: Then we have

$$x^n x^m = \underbrace{(x \cdots x)}_{n \text{ times}} \underbrace{(x^{-1} \cdots x^{-1})}_{|m| \text{ times}}.$$

If $n \geq |m|$ then

$$\underbrace{(x \cdots x)}_{n \text{ times}} \underbrace{(x^{-1} \cdots x^{-1})}_{|m| \text{ times}} = \underbrace{x \cdots x}_{n-|m| \text{ times}} = x^{n-|m|} = x^{n+m}.$$

If $n \leq |m|$ then

$$\underbrace{(x \cdots x)}_{n \text{ times}} \underbrace{(x^{-1} \cdots x^{-1})}_{|m| \text{ times}} = \underbrace{x^{-1} \cdots x^{-1}}_{|m|-n \text{ times}} = x^{-(|m|-n)} = x^{m+n}.$$

In either case we obtain the desired result $x^n x^m = x^{n+m}$.

Next we show that $(x^n)^{-1} = x^{-n}$ so H is closed under inverses. Indeed, using the above, we have

$$x^{-n} x^n = x^n x^{-n} = x^{n+(-n)} = x^0 = 1$$

and so $(x^n)^{-1} = x^{-n}$. Therefore, we have proved that H is a group.
