# MATH 417, HOMEWORK 2

CHARLES ANCEL

**Exercise 1.** Consider the formula $x \star y \overset{\text{def}}{=} 2xy$. Show that $(\mathbb{R}_{>0}, \star)$ is a group.

---

## Solution

To show that $(\mathbb{R}_{>0}, \star)$ is a group under the operation $x \star y = 2xy$, we need to verify the following group axioms:

*Proof.*

**Closure.** Let $x, y \in \mathbb{R}_{>0}$. We need to show that $x \star y = 2xy \in \mathbb{R}_{>0}$.

$$\begin{aligned} x > 0 &\quad \text{and} \quad y > 0 \\ \Rightarrow 2xy > 0 &\quad \text{since } 2 > 0,\ x > 0,\ y > 0. \end{aligned}$$

Thus, $x \star y \in \mathbb{R}_{>0}$, proving closure.

**Associativity.** Let $x, y, z \in \mathbb{R}_{>0}$. We need to show that $(x \star y) \star z = x \star (y \star z)$.

$$\begin{aligned} (x \star y) \star z &= (2xy) \star z \\ &= 2(2xy)z \quad (\text{by definition of } \star) \\ &= 4xyz, \\ x \star (y \star z) &= x \star (2yz) \\ &= 2x(2yz) \quad (\text{by definition of } \star) \\ &= 4xyz. \end{aligned}$$

Thus, $(x \star y) \star z = x \star (y \star z)$, proving associativity.

**Identity Element.** We need to find an element $e \in \mathbb{R}_{>0}$ such that $e \star x = x \star e = x$ for all $x \in \mathbb{R}_{>0}$.

$$\begin{aligned} &e \star x = 2ex = x \quad \Rightarrow e = \frac{1}{2}, \\ &x \star e = 2x \left(\frac{1}{2}\right) = x. \end{aligned}$$

Thus, the identity element is $e = \frac{1}{2}$.

**Inverses.** For each $x \in \mathbb{R}_{>0}$, we need to find an element $y \in \mathbb{R}_{>0}$ such that $x \star y = y \star x = e$, where $e = \frac{1}{2}$.

$$\begin{aligned} x \star y &= 2xy = \frac{1}{2} \\ \Rightarrow y &= \frac{1}{4x}, \\ y \star x &= 2yx = 2\left(\frac{1}{4x}\right)x = \frac{1}{2}. \end{aligned}$$

Thus, the inverse of $x$ is $y = \frac{1}{4x}$.

$\square$

Since the operation $\star$ satisfies closure, associativity, identity, and inverses, we conclude that $(\mathbb{R}_{>0}, \star)$ is a group.

**Exercise 2.** State and prove a formula for the parity of a permutation in terms of its cycle type.

---

## Solution

**Statement of the Formula.** Let $\sigma \in S_n$ be a permutation, and let $c_1, c_2, \ldots, c_k$ be the lengths of the disjoint cycles in the cycle decomposition of $\sigma$. The parity of the permutation $\sigma$ (i.e., whether it is even or odd) can be determined by the formula:

$$\text{parity}(\sigma) = \sum_{i=1}^{k}(c_i - 1) \mod 2.$$

In other words, a permutation is even if the sum of $c_i - 1$ for all cycles is even, and odd if this sum is odd.

**Proof of the Formula.** To prove this formula, we need to show that the sum $\sum_{i=1}^{k}(c_i - 1)$ modulo 2 corresponds to the parity of the permutation $\sigma$.

*Proof.*

**Cycle Decomposition and Transpositions.** Any permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. Let $\sigma = \tau_1\tau_2 \cdots \tau_k$, where each $\tau_i$ is a cycle of length $c_i$.

A $c_i$-cycle $(a_1\, a_2\, \ldots\, a_{c_i})$ can be decomposed into $(c_i - 1)$ transpositions:

$$(a_1\, a_2\, \ldots\, a_{c_i}) = (a_1\, a_{c_i})(a_1\, a_{c_i-1}) \cdots (a_1\, a_2).$$

The number of transpositions in the decomposition of $\tau_i$ is $c_i - 1$.

**Sum of Transpositions.** The total number of transpositions required to express $\sigma$ as a product of transpositions is:

$$\sum_{i=1}^{k}(c_i - 1).$$

**Parity Calculation.** The parity of $\sigma$ is even if this sum is even and odd if this sum is odd. This can be seen as follows: - If the total number of transpositions (2-cycles) used to express $\sigma$ is even, then $\sigma$ is an even permutation. - If the total number of transpositions used to express $\sigma$ is odd, then $\sigma$ is an odd permutation.

Thus, the parity of the permutation $\sigma$ can be calculated as:

$$\text{parity}(\sigma) = \sum_{i=1}^{k}(c_i - 1) \mod 2.$$

**Example for Verification.** Consider the permutation $\sigma = (1\,2\,3)(4\,5)$ in $S_5$:

– The cycle $(1\,2\,3)$ is a 3-cycle and can be decomposed into 2 transpositions: $(1\,3)(1\,2)$.

– The cycle $(4\,5)$ is a 2-cycle and can be decomposed into 1 transposition: $(4\,5)$.

The total number of transpositions is $2 + 1 = 3$. Thus, $\sigma$ is an odd permutation. According to the formula:

$$\text{parity}(\sigma) = ((3-1) + (2-1)) \mod 2 = (2+1) \mod 2 = 1.$$

The parity is 1 (odd), matching our calculation.

$\square$

This proves that the formula for the parity of a permutation in terms of its cycle type is correct.

**Exercise 3.** Suppose $b, c, d, e$ are integers. Show that if $d, e \in I(b, c)$, then $I(d, e) \subseteq I(b, c)$

---

## Solution

Let $I(b, c)$ denote the ideal in $\mathbb{Z}$ generated by $b$ and $c$, and $I(d, e)$ denote the ideal generated by $d$ and $e$. To show that $I(d, e) \subseteq I(b, c)$, we proceed as follows:

*Proof.*

**Definition of Ideals.** The ideal $I(b, c)$ generated by $b$ and $c$ in $\mathbb{Z}$ consists of all linear combinations of $b$ and $c$:

$$I(b, c) = \{xb + yc \mid x, y \in \mathbb{Z}\}.$$

Similarly, the ideal $I(d, e)$ generated by $d$ and $e$ is:

$$I(d, e) = \{ud + ve \mid u, v \in \mathbb{Z}\}.$$

**Given Conditions.** We are given that $d, e \in I(b, c)$. Therefore, there exist integers $x_1, y_1, x_2, y_2$ such that:

$$d = x_1 b + y_1 c,$$
$$e = x_2 b + y_2 c.$$

**Subset Inclusion.** We need to show that any element in $I(d, e)$ is also in $I(b, c)$. Take any element in $I(d, e)$:

$$k = ud + ve \quad \text{for some } u, v \in \mathbb{Z}.$$

Substituting $d = x_1 b + y_1 c$ and $e = x_2 b + y_2 c$:

$$k = u(x_1 b + y_1 c) + v(x_2 b + y_2 c).$$

Expanding and simplifying, we get:

$$k = (ux_1 + vx_2)b + (uy_1 + vy_2)c.$$

Let $x = ux_1 + vx_2$ and $y = uy_1 + vy_2$. Then:

$$k = xb + yc.$$

**Conclusion.** Since $x, y \in \mathbb{Z}$, we have $k = xb + yc$. This shows that $k \in I(b, c)$. Therefore, every element $k \in I(d, e)$ is also in $I(b, c)$, proving that:

$$I(d, e) \subseteq I(b, c).$$

□

**Exercise 4.** Let $a, b, d \in \mathbb{Z}$. Show that if the equation $d = ax + by$ has at least one solution $(x, y) \in \mathbb{Z}^2$, then it has infinitely many such solutions.

---

## Solution

Given the equation $d = ax + by$ with $a, b, d \in \mathbb{Z}$, we aim to show that if there exists at least one integer solution $(x_0, y_0)$, then there are infinitely many integer solutions.

*Proof.*

**Existence of a Particular Solution.** Suppose there exists a solution $(x_0, y_0) \in \mathbb{Z}^2$ such that:

$$d = ax_0 + by_0.$$

**General Solution.** We will derive the general solution to the equation $d = ax + by$.

Consider any integer $t$. Let $x$ and $y$ be parameterized by $t$:

$$x = x_0 + bt, \quad y = y_0 - at.$$

**Verification of the General Solution.** Substitute $x = x_0 + bt$ and $y = y_0 - at$ into the equation $d = ax + by$:

$$\begin{aligned} d &= a(x_0 + bt) + b(y_0 - at) \\ &= ax_0 + abt + by_0 - bat \\ &= ax_0 + by_0 + (abt - bat) \\ &= ax_0 + by_0 + 0 \\ &= d. \end{aligned}$$

Thus, $d = ax + by$ for $x = x_0 + bt$ and $y = y_0 - at$.

**Conclusion.** Since $t$ can be any integer, there are infinitely many pairs $(x, y)$ given by:

$$x = x_0 + bt, \quad y = y_0 - at$$

that satisfy the equation $d = ax + by$.

Therefore, if there is at least one solution to the equation $d = ax + by$, there are infinitely many integer solutions. □

**Exercise 1.6.3.** Suppose that a natural number $p > 1$ has the property that for all nonzero integers $a$, $b$, if $p$ divides the product $ab$, then $p$ divides $a$ or $p$ divides $b$. Show that $p$ is prime. (This is the converse of Proposition 1.6.19 in the book.)

---

## Solution

To prove that $p$ is a prime number, we assume the given property and use a proof by contradiction.

*Proof.*

**Assumption.** Assume $p$ is not prime. Then $p$ can be factored into two positive integers greater than 1:

$$p = mn,$$

where $1 < m < p$ and $1 < n < p$.

**Applying the Property.** Consider the integers $m$ and $n$:

$$p \mid mn \quad \text{(since } p = mn\text{)}.$$

By the given property, since $p$ divides the product $mn$, $p$ must divide either $m$ or $n$.

**Contradiction.** Since $p = mn$:

- If $p \mid m$, then $m = kp$ for some integer $k$, which implies $m \geq p$, contradicting $1 < m < p$.
- If $p \mid n$, then $n = kp$ for some integer $k$, which implies $n \geq p$, contradicting $1 < n < p$.

In both cases, we reach a contradiction. Therefore, our assumption that $p$ is not prime must be false.

**Conclusion.** Since assuming $p$ is not prime leads to a contradiction, we conclude that $p$ must be prime.

□

**Exercise 1.7.1.** Prove that addition and multiplication in $\mathbb{Z}_n$ are both commutative and associative.

---

## Solution

In $\mathbb{Z}_n$, addition and multiplication are defined modulo $n$. We will prove the commutativity and associativity of these operations.

### Addition in $\mathbb{Z}_n$.

*Commutativity.* Let $a, b \in \mathbb{Z}_n$. We need to show that $a + b = b + a$ in $\mathbb{Z}_n$.

*Proof.*

Addition in $\mathbb{Z}_n$ is defined as:

$$a + b \equiv a + b \pmod{n}.$$

Using the commutativity of addition in $\mathbb{Z}$, we have:

$$a + b = b + a.$$

Therefore:

$$a + b \equiv b + a \pmod{n}.$$

Hence, addition in $\mathbb{Z}_n$ is commutative. □

*Associativity.* Let $a, b, c \in \mathbb{Z}_n$. We need to show that $(a + b) + c = a + (b + c)$ in $\mathbb{Z}_n$.

*Proof.*

Addition in $\mathbb{Z}_n$ is defined as:

$$a + b \equiv a + b \pmod{n}.$$

Using the associativity of addition in $\mathbb{Z}$, we have:

$$(a + b) + c = a + (b + c).$$

Therefore:

$$(a + b) + c \equiv a + (b + c) \pmod{n}.$$

Hence, addition in $\mathbb{Z}_n$ is associative. □

**Multiplication in $\mathbb{Z}_n$.**

*Commutativity.* Let $a, b \in \mathbb{Z}_n$. We need to show that $a \cdot b = b \cdot a$ in $\mathbb{Z}_n$.

*Proof.* Multiplication in $\mathbb{Z}_n$ is defined as:

$$a \cdot b \equiv a \cdot b \pmod{n}.$$

Using the commutativity of multiplication in $\mathbb{Z}$, we have:

$$a \cdot b = b \cdot a.$$

Therefore:

$$a \cdot b \equiv b \cdot a \pmod{n}.$$

Hence, multiplication in $\mathbb{Z}_n$ is commutative. □

*Associativity.* Let $a, b, c \in \mathbb{Z}_n$. We need to show that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ in $\mathbb{Z}_n$.

*Proof.* Multiplication in $\mathbb{Z}_n$ is defined as:

$$a \cdot b \equiv a \cdot b \pmod{n}.$$

Using the associativity of multiplication in $\mathbb{Z}$, we have:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Therefore:

$$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}.$$

Hence, multiplication in $\mathbb{Z}_n$ is associative. □

## Conclusion

We have shown that both addition and multiplication in $\mathbb{Z}_n$ are commutative and associative, completing the proof.

**Exercise 1.7.16.** Find an integer $x$ such that $x \equiv 3 \pmod 4$ and $x \equiv 5 \pmod 9$.

---

## Solution

We need to find an integer $x$ that satisfies the following system of congruences:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod 9 \end{cases}$$

To solve this, we can use the method of successive substitutions or apply the Chinese Remainder Theorem.

*Proof.*

**Method of Successive Substitutions.**

1. **Express x in terms of one congruence:** From the first congruence, write $x$ as:

$$x = 4k + 3 \quad \text{for some integer } k.$$

2. **Substitute into the second congruence:** Substitute $x$ in the second congruence:

$$4k + 3 \equiv 5 \pmod 9.$$

   Simplify this to solve for $k$:

$$\begin{aligned} 4k + 3 &\equiv 5 \pmod 9 \\ 4k &\equiv 2 \pmod 9 \\ k &\equiv 2 \cdot 4^{-1} \pmod 9. \end{aligned}$$

3. **Find the inverse of 4 modulo 9:** The multiplicative inverse of 4 modulo 9 is an integer $y$ such that:

$$4y \equiv 1 \pmod 9.$$

   By checking values, we find that $4 \cdot 7 \equiv 28 \equiv 1 \pmod 9$. Thus, the inverse is 7.

4. **Solve for k:** Substitute the inverse back into the equation:

$$k \equiv 2 \cdot 7 \pmod 9 k \equiv 14 \pmod 9 k \equiv 5 \pmod 9.$$

5. **Find x:** Substitute $k$ back into the expression for $x$:

$$x = 4k + 3 = 4 \cdot 5 + 3 = 20 + 3 = 23.$$

   Thus,

$$x \equiv 23 \pmod{36}.$$

**Verification.** To verify:

- Check $x \equiv 3 \pmod 4$:

$$23 \div 4 = 5 \text{ remainder } 3 \quad \Rightarrow \quad 23 \equiv 3 \pmod 4.$$

- Check $x \equiv 5 \pmod 9$:

$$23 \div 9 = 2 \text{ remainder } 5 \quad \Rightarrow \quad 23 \equiv 5 \pmod 9.$$

Both congruences are satisfied.

**Conclusion.** The integer $x$ that satisfies both congruences is:

$$\boxed{23}.$$

$\square$