MATH2050C Assignment 1

Deadline: Jan 16, 2017.

Hand in: no. 3, 13, 16, 23.

Section 2.1 no. 1, 2, 3, 6, 8, 12, 13, 16, 18, 20, 21, 23.

Supplementary Exercises

These two problems are optional.

1. (a) Show that every natural number $n > 1$ can be written uniquely as

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \ ,$$

   where p_j's are prime numbers $p_1 < p_2 < \cdots < p_k$ and $n_j \geq 1$. Suggestion: Use induction on n.

   (b) Show that for every natural numbers n, m, there exist n', m' with no common factor greater than 1 such that $\dfrac{n}{m} = \dfrac{n'}{m'}$.

2. Denote $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ and define addition and multiplication on $\mathbb{Z}_p$ by modulo p, that is, $a + b$ and $a \cdot b$ is equal to the reminder of ordinary $a + b$ and $a \cdot b$ after divided by p respectively. Show that $\mathbb{Z}_p$ satisfies all algebraic properties of the real number system. You may try $p = 5$ first.

The Real Number System: Algebraic Properties

The real number system $\mathbb{R}$ satisfies the following algebraic properties. There are two binary operations defined on $\mathbb{R}$ whose first is called addition " $+$ " and second multiplication " $\cdot$ ". The followings hold: For all $a, b, c \in \mathbb{R}$,

- (A1) $a + b = b + a$,
- (A2) $(a + b) + c = a + (b + c)$,
- (A3) There is a number denoted by 0 such that $a + 0 = a$,
- (A4) To each a there is a number denoted by $-a$ such that $a + (-a) = 0$.

- (M1) $a \cdot b = b \cdot a$,
- (M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (M3) There is a number denoted by 1 not equal to 0 such that $1 \cdot a = a$,
- (M4) To each non-zero a, there is a number denoted by $\frac{1}{a}$ such that $a \cdot \frac{1}{a} = 1$.

These two operations are related by

- (D) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Some remarks are in order.

1. By (A2), addition is independent of order. Consequently, $a + b + c$ is well-defined. In general, $a_1 + a_2 + \cdots + a_n$ is well-defined.
2. By (A1) and (A2), $0 + a = a$ also holds.
3. By (A1) and (A3), $(-a) + a = 0$. The additive inverse is unique in the following sense: If $a + b = 0$, then $b = -a$. (Proof: $a + b = 0 \Rightarrow (-a) + a + b = (-a) + 0 \Rightarrow 0 + b = -a$, that is, $b = -a$.)
4. By (M2), multiplication is independent of order. Consequently, $a \cdot b \cdot c$ is well-defined. In general, $a_1 \cdot a_2 \cdots a_n$ is well-defined.
5. By (M1) and (M3), $a \cdot 1 = a$ also holds.
6. By (M1) and (M4), $\frac{1}{a} \cdot a = 1$. The multiplicative inverse is unique in the following sense: If $a \cdot b = 1$, then $b = \frac{1}{a}$. (Proof: $a \cdot b = 1 \Rightarrow \frac{1}{a} \cdot a \cdot b = \frac{1}{a} \Rightarrow 1 \cdot b = \frac{1}{a} \Rightarrow b = \frac{1}{a}$.)
7. From (D) and (M1), $(b + c) \cdot a = b \cdot +c \cdot a$.

Conventions: (a) Write ab instead $a \cdot b$ for short. I will do this later. (b) Define subtraction by setting $a - b = a + (-b)$. (c) Define division by setting $\frac{a}{b} = a \cdot \frac{1}{b}$.

Corollary 1.

(a) For every $a \in \mathbb{R}$, $0 \cdot a = 0$.

(b) $a \cdot b = 0$ implies a or b is 0.

Proof of (a): $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$ by (D). Adding $-(0 \cdot a)$ to both side yields $0 \cdot a = 0$.

Proof of (b): In case $a \neq 0$, we claim that $b = 0$. Multiply both side of $a \cdot b = 0$ by $\frac{1}{a}$ to get $b = 1 \cdot b = \frac{1}{a} \cdot a \cdot b = \frac{1}{a} \cdot 0 = 0$ by (a).

Corollary 2 (Cancelation Laws).

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

(b) $\dfrac{ab}{ac} = \dfrac{b}{c}$.

Proof of (a). Add $-a$ to both side.

Proof of (b). First show that

$$\frac{1}{ac} = \frac{1}{a} \cdot \frac{1}{c}, \quad a, c \neq 0 \ .$$

From the uniqueness of inverse it suffices to check $\dfrac{1}{a}\dfrac{1}{c}ac = 1$. But this is trivial: $\dfrac{1}{a}\dfrac{1}{c}ac = \dfrac{1}{a}a\dfrac{c}{c} = 1 \cdot 1 = 1$.

Define $2 = 1+1, 3 = 2+1, 4 = 3+1, \ldots$ to get the set of all natural numbers denoted by $\mathbb{N}$. The set of all integers $\mathbb{Z}$ is given by $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The set of all rational numbers $\mathbb{Q}$ is given by $\{\frac{a}{b} : \ a, b \neq 0, \in \mathbb{Z}\}$.

Classroom Exercise. Establish the following properties:

1. $-(-a) = a$,
2. $(-1) \cdot a = -a$,
3. $-(a+b) = -a - b$,
4. $-\dfrac{a}{b} = \dfrac{-a}{b} = \dfrac{a}{-b}$,
5. $\dfrac{a_1}{b_1} + \dfrac{a_2}{b_2} = \dfrac{a_1 b_2 + a_2 b_1}{b_1 b_2}$.

I provide proofs for the first two properties.

Proof of (1): Due to the uniqueness of additive inverse, it suffices to show $-(-a) - a = 0$. Indeed, we have $-(-a) - a = -(-a) + (-a) = 0$ since the inverse of $-a$ is $-(-a)$.

Proof of (2): We have $(-1+1) \cdot a = (-1) \cdot a + 1 \cdot a = (-1) \cdot a + a$. On the other hand, $(-1+1) \cdot a = 0 \cdot a = 0$. Therefore, $(-1) \cdot a + a = 0$ which shows that the inverse of a is $(-1) \cdot a$, in other words, $(-1) \cdot a = -a$.