MATH2050C Assignment 1

Section 2.1. no 3, 9, 10, 16, 17, 23. Section 2.4. no 1, 2, 5, 8, 9, 10, 13, 14.

Hand in: 2.1 no 3b, 10b, 17 ; 2.4 no 2, 14, by Jan 14, 2025.

Supplementary Problems

Let S be an ordered field in (1)-(3). You may use (A1)-(A4), (M1)-(M4), (D), and (O1)-(O3) in the following problems.

1. Prove for $m, n, p, q \in \mathbb{N},\ p, q \neq 0$,
$$\frac{n}{m} + \frac{p}{q} = \frac{nq + mp}{mq} \ .$$
2. Prove $ab > 0$ iff $a, b > 0$ or $a, b < 0$.
3. Prove $2ab \leq a^2 + b^2$.
4. (Optional) Let p be a prime number. Show that $\mathbb{Z}_p$ is a field but it does not admit an ordering satisfying (P1)-(P3).
5. Is $\mathbb{C}$ an ordered field?

See next page for notes on real numbers.

The Real Number System I

We postulate the existence of a number system called the real number system and denote it by $\mathbb{R}$. In one sentence, it is an order-complete field. We will describe it in three steps.

The algebraic structure of the real number system is a field. It is defined as follows. Let S be a nonempty set with two algebraic operations. The first one is called the addition. Given two elements a and b in S, its sum is an element $a+b \in S$ and the followings hold:

- (A1) $a+b=b+a$. (commutative)
- (A2) $(a+b)+c=a+(b+c)$. (associative)
- (A3) There is an element 0 satisfying $a+0=0+a=a$ for all $a \in S$.
- (A4) For each $a \in S$, there is some $b \in S$ satisfying $a+b=b+a=0$.

It is easy to prove that both additive identity 0 and the additive inverse are unique. The additive inverse of a will be denoted by $-a$ and we write $a+(-b)$ as $a-b$ for simplicity. Also we write $(a+b)+c$ and $a+(b+c)$ as $a+b+c$ since the order of addition is irrelevant.

The second operation is the multiplication which assigns any two elements a and b in S an element $a \cdot b$ in S and the followings hold:

- (M1) $a \cdot b=b \cdot a$. (commutative)
- (M2) $(a \cdot b) \cdot c=a \cdot(b \cdot c)$. (associative)
- (M3) There is an element 1 satisfying $1 \cdot a=a \cdot 1$ for all $a \in S$.
- (M4) For each $a \neq 0$ in S, there is some $b \in S$ satisfying $a \cdot b=b \cdot a=1$.

It is easy to prove that both multiplicative identity 1 and the multiplicative inverse are unique. We will simplify the notation by writing $a \cdot b$ as ab. The multiplicative inverse of a will be denoted by $1/a$ or a^{-1}. In particular, a/b means $a \cdot 1/b, a \cdot b^{-1}$, or ab^{-1}. Also we write abc instead of $(ab)c$ or $a(bc)$.

The addition and multiplication are related by the distribution laws:

- (D) For $a, b, c \in S, \quad a \cdot(b+c)=a \cdot b+a \cdot c, \quad (b+c) \cdot a=b \cdot a+c \cdot a$.

Examples of fields include $\mathbb{Z}_p, (p \text{ prime }), \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

We deduce the following rules which have been used since primary school days.

Proposition 1.1

(a) $z + a = a$ implies $z = 0$.

(b) $ua = a, a \neq 0$, implies $u = 1$.

(c) $a0 = 0, \forall a \in S$.

Proposition 1.2

(a) For $a \neq 0, ab = 1$ implies $b = a^{-1}$.

(b) $ab = 0$ implies $a = 0$ or $b = 0$.

Proofs of these propositions can be found in our text, but it is nice to do it by yourself without looking up the book.

Now we describe the order structure on a field. It is defined in an indirect way.

We postulate that there is a nonempty subset P of the field S called positive set which satisfies the following properties:

- (O1) $a, b \in P$ implies $a + b \in P$.
- (O2) $a, b \in P$ implies $ab \in P$.
- (O3) Let $N = \{a : -a \in P\}$. Then we have the disjoint decomposition $S = P \bigcup N \bigcup \{0\}$.

The ordering in S is defined by $a < b$ or $b > a$ iff $b - a \in P$ or $a - b \in N$, and $a \leq b$ or $b \geq a$ if and only if $a < b$ or $a = b$.

Proposition 1.3 For $a, b, c \in S$,

(a) $a < b, b < c$ implies $a < c$.

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

(c) $a < b, c > 0$ implies $ac < ab$ and $a < b, c < 0$ implies $ac > bc$.

Proposition 1.4

(a) For $a \neq 0$, $a^2 > 0$.

(b) $1 > 0$.

(c) $n \geq 1$.

Here we define $2 = 1 + 1, 3 = 2 + 1 = 1 + 1 + 1, \cdots$.

Now we show that an ordered field contains a copy of rational numbers. To be precise, define the natural numbers to be the set $\mathbb{N} = \{1, 2, 3, \cdots\}$ and the set of integers $\mathbb{Z}$ by $\mathbb{Z} = \mathbb{N} \bigcup \{-n : n \in \mathbb{N}\} \bigcup \{0\}$. Furthermore, define the set of rational numbers $\mathbb{Q}$ to be all numbers of the form $\{n/m = nm^{-1} : \ n \in \mathbb{Z}, m \in \mathbb{N}\}$. It is easy to establish

$$\frac{n}{m} + \frac{p}{q} = \frac{nq + mp}{mq} \ ,$$

so that this set $\mathbb{Q}$ is just a copy of the usual set of rational numbers.

Among our previous examples of fields, $\mathbb{Z}_p$ and $\mathbb{C}$ are not ordered fields, see exercises.

Before stating the last property of $\mathbb{R}$, we introduce the notion of the supremum and infimum of a set. Let E be nonempty set in the ordered field S. It is called bounded below if there is some number a such that $a \leq s$ for all $s \in E$. In this case, a is called a lower bound of E. It is called bounded above if there is some $b \in S$ such that $s \leq b$ for all $s \in E$. The number b is called an upper bound of E. A lower bound a is called the infimum or glb (greatest lower bound) of E if $a \geq a'$ for all lower bounds a' of E. An upper bound b is called the supremum or lub (least upper bound) of E if $b \leq b'$ for all upper bounds b' of E. It is clear that the infimum and supremum of a set (if exist) are unique. The following proposition is self-evident.

Proposition 1.5 Let E be a set in the ordered field S.

(a) Let b be the supremum of E. For $\varepsilon > 0$, there is some $x \in E$ such that $b < x + \varepsilon$ or $b - \varepsilon < x$.

(b) Let a be the infimum of E. For $\varepsilon > 0$, there is some $y \in E$ such that $y - \varepsilon < a$ or $y < a + \varepsilon$.

Proof. (a) By definition, $b - \varepsilon$ is no longer an upper bound for E. In other words, there is some $x \in E$ such that $b - \varepsilon < x$. The proof of (a) is similar.

The last assumption on $\mathbb{R}$ is the order completeness property.

Order Comopleteness A nonempty set in the ordered field S bounded above (resp. bounded below) admits a supremum (resp. infimum) in S.

Be careful that it does not necessarily mean that this supremum belongs to the set itself.

We will see that $\mathbb{Q}$ is an ordered field but it is not order-complete.

Summarizing, the real number system is a set satisfying

- The algebraic properties (A1)-(A4), (M1)-(M4), and (D).
- It has an order structure derived from (O1)-(O3).
- The Order Completeness Property holds.

Through our discussion, you will see that these three assumptions completely characterize $\mathbb{R}$. In other words, an order-complete field is necessarily a copy of $\mathbb{R}$.

Proposition 1.6 (Archimedean Property)

(a) For each $x \in \mathbb{R}$, there is a natural number n such that $x < n$.

(b) For each $x > 0$, there is a natural number n such that $1/n < x$.

Proof. (b) follows from (a). It suffices to prove (a). First of all, it suffices to consider $x > 0$. Suppose $n < x$ for all $n \in \mathbb{N}$, that is, x is an upper bound for the set $\mathbb{N}$. By Order Completeness, let z be the supremum of $\mathbb{N}$. By Proposition 1.5, we can find some $m \in \mathbb{N}$ such that $z - 1 < m$ (taking $\varepsilon = 1$ in Proposition 1.5). But it means $z < m + 1 \in \mathbb{N}$, contradicting the fact that z is an upper bound of $\mathbb{N}$.

Sometimes, a rather trivial fact is used instead of the Archimedean property.

Proposition 1.7

(a) For each $x \in \mathbb{R}$, there is a number M such that $x < M$.

(b) For each $x > 0$, there is a number y such that $0 < y < x$.

Unlike the Archimedean principle, it is not required M and y are of the form n and $1/n$ respectively. The proof follows by taking $M = x + 1$ in (a) and $y = x/2$ and in (b). We point out that this proposition is based on the ordering property of $\mathbb{R}$. Indeed, this proposition does not hold in $\mathbb{Z}_p$ and $\mathbb{C}$.

We has pointed out that an ordered field contains $\mathbb{Q}$. Now we show that a complete ordered field contains more than $\mathbb{Q}$.

Proposition 1.8 There is a positive real number x which is not rational satisfying $x^2 = 2$.

Proof. First we show there is no rational number $x = p/q$ such that $x^2 = 2$. Suppose not, let $(p/q)^2 = 2$ where p and q have no common factor greater than 1. We have $p^2 = 2q^2$, so 2 divides p^2. It means p^2 and p are even numbers. Writing $p = 2m$, $4m^2 = p^2 = 2q^2$ implies $q^2 = 2m^2$, that is, q^2 and q are also even numbers. However, we have assumed p and q are reduced, so they cannot have a common factor 2, contradiction holds.

Let $S = \{y > 0 : y^2 < 2\}$. Clearly, every y in S satisfies $y^2 < 4$. As $y^2 - 4 = (y + 2)(y - 2) < 0$, $y < 2$ shows that S is bounded above by 2. By Order Completeness its supremum z exists. We shall prove that $z^2 = 2$ by excluding the cases $z^2 > 2$ and $z^2 < 2$.

First, assume $z^2 > 2$. As $z = \sup S$, by Proposition 1.5, for $\varepsilon > 0$, there is some $y \in S$ such that $y > z - \varepsilon$. By Proposition 1.7, we can choose ε so that $z - \varepsilon > 0$. It implies $y^2 > (z - \varepsilon)^2$, that is, $y^2 > z^2 - 2\varepsilon z + \varepsilon^2$, and $y^2 > (z^2 - 2) + 2 - 2\varepsilon z$. Now, if we choose ε satisfying $0 < \varepsilon < \min\{z, (z^2 - 2)/2z\}$, then $y^2 > 2$, contradicting the fact that $y \in S$.

Next, assume $z^2 < 2$. For $\varepsilon > 0$, $(z+\varepsilon)^2 = z^2+2\varepsilon z+\varepsilon^2 = (z^2-2)+2+\varepsilon z+\varepsilon^2$. Choose $0 < \varepsilon < 1$ such that $0 < \varepsilon < (2 - z^2)/(1 + z)$, that is, $0 < \varepsilon < \min\{1, (2 - z^2)/(1 + z)\}$. The number $z+\varepsilon$ satisfies $(z+\varepsilon)^2 < 2$ hence belongs to S, contradicting the fact that z is the supremum of S.