1.2. Properties of the Real Numbers as an Ordered Field.

Note. In this section we give eight axioms related to the definition of the real numbers, $\mathbb{R}$. All properties of sets of real numbers, limits, continuity of functions, integrals, and derivatives will follow from this definition. we start with some material from Introduction to Modern Algebra (MATH 4127/5127).

Note 1.2.A. If you have already taken Introduction to Modern Algebra, then you have been exposed to the following. (If you have not yet taken it, it is probably in your near future!) These definitions can be found in my online notes for Introduction to Modern Algebra:

Definition 18.1. A *ring* $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, respectively, defined on R such that:

$\mathcal{R}_1$: $\langle R, + \rangle$ is an abelian group.

$\mathcal{R}_2$: Multiplication $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

$\mathcal{R}_3$: For all $a, b, c \in R$, the *left distribution law* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the *right distribution law* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Definition 18.14. A ring in which multiplication is commutative (i.e., $ab = ba$ for all $a, b \in R$) is a *commutative ring.* A ring with a multiplicative identity element is a *ring with unity.*

Definition 18.16. Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a *unit* of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a *division ring*. A *field* is a commutative division ring.

In *this* class, we are interested in the field of real numbers (in Complex Variables [MATH 4337/5337] you are interested in the field of complex numbers), so we abbreviate the above information and give a more concise definition of a field.

Definition. A *field* $\mathbb{F}$ is a nonempty set with two operations $+$ and $\cdot$ called addition and multiplication, such that the following axioms hold:

(A1) If $a, b \in \mathbb{F}$ then $a + b$ and $a \cdot b$ are uniquely determined elements of $\mathbb{F}$ (i.e., $+$ and $\cdot$ are *binary operations*).

(A2) If $a, b, c \in \mathbb{F}$ then $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (i.e., $+$ and $\cdot$ are *associative*).

(A3) If $a, b \in \mathbb{F}$ then $a + b = b + a$ and $a \cdot b = b \cdot a$ (i.e., $+$ and $\cdot$ are *commutative*).

(A4) If $a, b, c \in \mathbb{F}$ then $a \cdot (b + c) = a \cdot b + a \cdot c$ (i.e., $\cdot$ *distributes* over $+$).

(A5) There exists $0, 1 \in \mathbb{F}$ (with $0 \neq 1$) such that $0 + a = a$ and $1 \cdot a = a$ for all $g \in \mathbb{F}$.

(A6) If $a \in \mathbb{F}$ then there exists $-a \in \mathbb{F}$ such that $a + (-a) = 0$.

(A7) If $a \in \mathbb{F}$ $a \neq 0$, then there exists a^{-1} such that $a \cdot a^{-1} = 1$.

0 is the *additive identity*, 1 is the *multiplicative identity*, $-a$ and a^{-1} are *inverses* of a.

Note 1.2.B. As mentioned earlier (see Note 1.1.F in Section 1.1. Sets and Functions), there are "no such things" as subtraction and division! As opposed to subtraction we have the *addition* of additive inverses, and as opposed to division we have the *multiplication* by multiplicative inverses. Evidence for this follows from Note 1.2.A where we see that a ring only has TWO binary operations. This technicality will not stop us from using the terms "subtract" and "divide" or the symbols for these procedures, however.

Example. Some examples of fields include:

1. The rational numbers $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$.
2. The rationals extended by $\sqrt{2}$: $\mathbb{Q}[\sqrt{2}] = \{q_1 + q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\}$.
3. The algebraic numbers $\mathbb{A} = \{x \in \mathbb{R} \mid p(x) = 0$ for some polynomial with integer coefficients$\}$.
4. The real numbers $\mathbb{R}$.
5. The complex numbers $\mathbb{C} = \{r_1 + ir_2 \mid r_1, r_2 \in \mathbb{R}, i^2 = -1\}$.
6. The integers modulo p where p is prime $\mathbb{Z}_p$.

Another "interesting" field is the field of *constructible numbers.* A real number r is *constructible* if, starting with a given line segment which is defined to be of length 1, a line segment of length $|r|$ can be constructed with a compass and straight edge in the plane. For more on compass and straight edge constructions, my History of Mathematics (MATH 3040) notes on Section 4.4. The Euclidean Tools, where compass ans straight edge constructions are tied to Euclid's approach to geometry in his *Elements*. The constructible numbers are shown to form a field in Introduction to Modern Algebra (MATH 4127/5127); see Corollary 32.5 in my online notes for that class on Section VI.32. Geometric Constructions.

Note. In the next two theorems, uniqueness of identities and inverses is shown. A common approach to showing uniqueness of an object is to assume that two such objects exist and then showing that the two objects are equal.

Theorem 1-3. For $\mathbb{F}$ a field, the additive and multiplicative identities are unique.

Theorem 1-4. For $\mathbb{F}$ a field and $a \in \mathbb{F}$, the additive and multiplicative inverses of a are unique.

Note. In the next two theorems, some properties of the interaction of addition and multiplication in a field are proved. Notice that in Theorem 1-6(c) it is shown that an additive inverse of a times an additive inverse of b equals ab. To paraphrase (or, arguably, to oversimplify), “the product of two negatives is positive” (if we overlook the fact that we haven’t yet defined “positive” or “negative”; in fact, such an idea does not hold in all fields).

Theorem 1-5. For $\mathbb{F}$ a field, $a \cdot 0 = 0$ for all $a \in \mathbb{F}$.

Theorem 1-6. For $\mathbb{F}$ a field and $a, b \in \mathbb{F}$:

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

(b) $-(-a) = a$.

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

Note. We add another axiom in our development of the real numbers. As an axiom, it is called "The Axiom of Order." It allows us to to define an idea of greater than and less than in certain fields.

Axiom 8/Definition of Ordered Field. A field $\mathbb{F}$ is said to be *ordered* if there is $P \subset \mathbb{F}$ (called the *positive subset*) such that

(i) If $a, b \in P$ then $a + b \in P$ (closure of P under addition).

(ii) If $a, b \in P$ then $a \cdot b \in P$ (closure of P under multiplication).

(iii) If $a \in \mathbb{F}$ then exactly one of the following holds: $a \in P$, $-a \in P$, or $a = 0$ (this is *The Law of Trichotomy*).

Note. Some examples of ordered fields are $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{A}$, and $\mathbb{R}$. In each case, the positive subset is the set of elements of each field which is greater than 0. Examples of fields that are not ordered fields are $\mathbb{C}$ and $\mathbb{Z}_p$. A proof that $\mathbb{C}$ is not ordered is given in my online notes for Complex Analysis 1 (MATH 5510) on Supplement. Ordering the Complex Numbers. The positive set is used to define an ordering as follows.

Definition. Let $\mathbb{F}$ be a field and P the positive subset. We say that $a < b$ (or $b > a$) if $b - a \in P$. We call $<$ and $>$ the *order* on $\mathbb{F}$.

Exercise 1.2.5. If $\mathbb{F}$ is an ordered field, $a, b \in \mathbb{F}$ with $a \leq b$ and $b \leq a$ then $a = b$.

Note. The next theorem gives several properties concerning the interaction of the order with addition and multiplication. Notice that what is proved here (and much of what has been previously proved) is valid for general fields or ordered fields. We are progressing towards $\mathbb{R}$, but we are currently considering a more general setting. In fact, we have not yet *defined* the real numbers.

Theorem 1-7. Let $\mathbb{F}$ be an ordered field. For $a, b, c \in \mathbb{F}$:

(a) If $a < b$ then $a + c < b + c$.

(b) If $a < b$ and $b < c$ then $a < c$ ("$<$" is *transitive*).

(c) If $a < b$ and $c > 0$ then $ac < bc$.

(d) If $a < b$ and $c < 0$ then $ac > bc$.

(e) If $a \neq 0$ then $a^2 = a \cdot a > 0$.

Note. We can use the order on an ordered field to define an interval. This is done in Precalculus 1 (Algebra) (MATH 1710); see my online notes for Precalculus 1 (Algebra) on Supplement A.9. Interval Notation; Solving Inequalities. It is also covered in Calculus 1 (MATH 1910); see my online Calculus 1 notes on Appendix A.1. Real Numbers and the Real Line and notice Table A.1. We repeat this here in the following definition and note.

Definition. An *interval* of real numbers is a set A containing at least two numbers such that if $r, s \in A$ with $r < s$ and it t is a number such that $t < t < s$, then $t \in A$. A set consisting of a single point is not an interval, but is sometimes called a *degenerate interval.*

Note. Intervals of real numbers fall into the following categories:

$$\mathbb{R} = (-\infty, \infty)$$

$$\begin{array}{rlrl} \textbf{(i)} & (a,b) = \{x \mid a < x < b\} & \textbf{(v)} & (-\infty,a) = \{x \mid x < a\} \\ \textbf{(ii)} & [a,b] = \{x \mid a \le x \le b\} & \textbf{(vi)} & (-\infty,a] = \{x \mid x \le a\} \\ \textbf{(iii)} & [a,b) = \{x \mid a \le x < b\} & \textbf{(vii)} & (a,\infty) = \{x \mid x > a\} \\ \textbf{(iv)} & (a,b] = \{x \mid a < x \le b\} & \textbf{(viii)} & [a,\infty) = \{x \mid x \ge a\} \end{array}$$

where $a < b$. Intervals of types (i), (v), and (vii) are *open intervals*, and intervals of types (ii), (vi), and $(viii)$ are *closed intervals.* The interval $(-\infty, \infty)$ is both open and closed.

Note 1.2.C. We assume the usual laws of arithmetic. The axiomatic justification of the properties of addition of natural numbers (and hence of integers) are based on a set theoretic development of $\mathbb{N}$. This is given in an Introduction to Set Theory class. ETSU has no such class, but I have some preliminary notes posted for an Introduction to Set Theory class. The addition of rational numbers in terms of common denominators is justified in Introduction to Modern Algebra (MATH 4217/5217) in Section IV.21. The Field of Quotients of an Integral Domain. The multiplication of integers and rational numbers is justified in terms of repeated addition. We assume that the usual laws of exponents are valid, such as $x^{a+b} = x^a \cdot x^b$ and $x^{a-b} = x^a/x^b$. For $a, b \in \mathbb{Z}$ this follows from the definition x^a, x^b, x^{a+b}, and x^{a-b} and is established in Modern Algebra 1 (MATH 5410) in Section I.1. Semigroups, Monoids, and Groups (see Theorem I.1.9).

Note. The existence of roots of real numbers is not something that can be proved with the information we have at this stage. The next theorem claims the existence of an nth root of a positive real number. We accept it for now and use it to prove some properties of positive real numbers to a rational power. In Section 1.3. The Completeness Axiom, we add an additional axiom to the definition of the real numbers and use this axiom to justify the next theorem.

Theorem 1-8. Let x be a positive real number and let n be a positive integer. Then there is a unique positive number y such that $y^n = x$.

Note. Theorem 1-8 allows to take nth roots of positive real numbers, where $n \in \mathbb{N}$. We can then use this to define exponentiation of any positive real number, where the exponent is rational. We give this definition formally next, and define exponentiation of positive real numbers with irrational exponents in the next section.

Definition. Let x be a positive real number and $n \in \mathbb{N}$. Then we define $x^{1/n} = \sqrt[n]{x}$ as the unique positive real number y, given in Theorem 1-8, such that $y^n = (x^{1/n})^n = x$. Positive real number $x^{1/n}$ is called the *nth root* of x. If p and q are positive integers, then we define $x^{p/q} = (x^{1/q})^p$.

Note. The next two theorems give the behavior of the interaction of inequalities and exponentiation with rational exponents. The proof of Theorem 1-9 is to be given in Exercise 1.2.10.

Theorem 1-9. Let x be a positive real number, and let s_1 and s_2 be positive rational numbers where $s_1 < s_2$. Then

(a) $x^{s_1} < x^{s_2}$ if $x > 1$.

(b) $x^{s_1} > x^{s_2}$ if $0 < x < 1$.

Theorem 1-10. Let x and y be positive real numbers with $x < y$ and let s be a positive rational number. Then $x^s < y^s$.

Note. The next exercise gives several properties of the order in an ordered field. These properties are then used to prove Theorem 1-10.

Exercise 1.2.7. Prove:

(a) $1 > 0$.

(b) If $0 < a < b$ then $0 < 1/b < 1/a$.

(c) If $0 < a < b$ then $a^n < b^n$ for natural number n.

(d) If $a > 0$, $b > 0$ and $a^n < b^n$ for some natural number n, then $a < b$.

(e) For any real numbers a and b, we have $|a| \leq |b|$ if and only if $a^2 \leq b^2$.

(f) Prove Theorem 1-10.

Note. You are familiar with mathematical induction from Mathematical Reasoning (MATH 3000), and possibly from Calculus 1 (MATH 1910). See my online notes for Calculus 1 on Appendix A.2. Mathematical Induction, and for Mathematical Reasoning on Section 2.10. Mathematical Induction and Recursion. We briefly state the Principle of Mathematical Induction here, for reference.

Principle of Mathematical Induction. Suppose that for each $n \in \mathbb{N}$ there is a statement $P(n)$. Suppose that

(i) $P(1)$ is true.

(ii) For any $k \in \mathbb{N}$, if $P(K)$ is true, then $P(k+1)$ must be true.

Then $P(n)$ is true for every $n \in \mathbb{N}$.

Note. We will prove (by induction) the Binomial Theorem. We need a preliminary result first. It involves the *binomial coefficients* $\binom{m}{j} = \frac{m!}{j!(m-j)!}$.

Theorem 1-11. For $m, j \in \mathbb{N}$ with $j \leq m$ we have

$$\binom{m}{j} + \binom{m}{j-1} = \binom{m+1}{j}.$$

Theorem 1-12. The Binomial Theorem.

Let a and b be real numbers and let $m \in \mathbb{N}$. Then

$$(a+b)^m = \sum_{j=0}^{m} \binom{m}{j} a^j b^{m-j}.$$

Note. We conclude this section by defining the absolute value function on $\mathbb{R}$. This plays a fundamental role in this class (as it did in calculus) since we use it to measure distance in $\mathbb{R}$.

Definition. For $a \in \mathbb{R}$, the *absolute value* of a is

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

Note. The properties of the absolute value function are summarized in the next theorem. Part (h) is particularly important in out use of it to measure distance. The remaining parts are to be proved in Exercises 1.2.13 and 1.2.14.

Theorem 1-13. For all $a, b \in \mathbb{R}$

(a) $|a| \geq 0$ with equality if and only if $a = 0$.

(b) $|a| = |-a|$.

(c) $-|a| \leq a \leq |a|$.

(d) $|ab| = |a| \cdot |b|$.

(e) $1/|b| = |1/b|$ if $b \neq 0$.

(f) $|a/b| = |a|/|b|$ if $b \neq 0$.

(g) $|a| < |b|$ if and only if $-b < a < b$.

(h) $|a + b| \leq |a| + |b|$ (this is the *Triangle Inequality*).

(i) $||a| - |b|| \leq |a - b|$.

Note. We measure the distance between two points in a set using a "metric." A set with a metric on it is a "metric space." These are a central topic in the study of analysis. These topics are covered in Introduction to Topology (MATH 4357/5357) in Section 20. The Metric Topology and Section 21. The Metric Topology (continued), in graduate Real Analysis 2 in Chapter 9, Metric Spaces: General Properties, and Chapter 10, Metric Spaces: Three Fundamental Theorems; see my in online notes for Real Analysis 2, and in graduate Complex Analysis 1 in Chapter II, Metric Spaces and the Topology of $\mathbb{C}$, see my online notes for Complex Analysis 1. We now give a formal definition of a "metric" on a set.

Definition. Let X be a set and d a function $d : X \times X \to \mathbb{R}$ satisfying

(i) $d(a, b) \geq 0$ for all $a, b \in X$ and $d(a, b) = 0$ if and only if $a = b$.

(ii) $d(a, b) = d(b, a)$.

(iii) $d(a, c) \leq d(a, b) + d(b, c)$ (this is the *Triangle Inequality*).

Function d is then called a *metric* on X.

Note. A metric on $\mathbb{R}$ based on absolute value is $d(x, y) = |x - y|$. This is because $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and for all $a, b, c \in \mathbb{R}$ we have:

(i) $d(a, b) = |a - b| \geq 0$, and $d(a, b) = |a - b| = 0$ if and only if $a = b$ by Theorem 1-13(a),

(ii) $d(a, b) = |a - b| = |-(a - b)| = |b - a| = d(b, a)$ by Theorem 1-13(b), and

(iii) by Theorem 1-13(h), the Triangle Inequality of absolute value,

$$d(a, c) = |a - c| = |(a - b) - (b - c)| \leq |a - b| + |b - c| = d(a, b) + d(b, c).$$

Note. Examples of metrics on $X = \mathbb{R}^2$ include the

(a) The Euclidean metric $d_E((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$, and

(b) the taxicab metric $d_t((x_1, y_1), (x_2, y_2)) = |x_1 - x_2| + |y_1 - y_2|$.

Notice that the Euclidean metric on $\mathbb{R}^2$ is simply the distance formula with which you are familiar. It is to be shown that both of these actually are metrics in Exercise 1.2.A.