Axioms of addition and multiplication of real numbers

The set of real numbers $\mathbb{R}$ is *closed* under addition (denoted by $+$) and multiplication (denoted by $\times$ or simply by juxtaposition) and satisfies:

1. Addition is *commutative.*
$$x + y = y + x$$
for all $x, y \in \mathbb{R}$.

2. Addition is *associative.*
$$(x + y) + z = x + (y + z)$$
for all $x, y, z \in \mathbb{R}$.

3. There is an *additive identity element.* There is a real number 0 with the property that
$$x + 0 = x$$
for all $x \in \mathbb{R}$.

4. Every real number has an *additive inverse.* Given any real number x, there is a real number $(-x)$ so that
$$x + (-x) = 0$$

5. Multiplication is *commutative.*
$$xy = yx$$
for all $x, y \in \mathbb{R}$.

6. Multiplication is *associative.*
$$(xy)z = x(yz)$$
for all $x, y, z \in \mathbb{R}$.

7. There is a *multiplicative identity element.* There is a real number 1 with the property that
$$x.1 = x$$
for all $x \in \mathbb{R}$. Furthermore, $1 \neq 0$.

8. Every non-zero real number has a *multiplicative inverse.* Given any real number $x \neq 0$, there is a real number $\frac{1}{x}$ so that
$$x\frac{1}{x} = 1$$

9. Multiplication *distributes* over addition
$$x(y + z) = xy + xz$$
for all $x, y, z \in \mathbb{R}$.

Miscellaney.

1. **Least Principle.** Every non-empty subset of $\mathbb{N}$ contains a least element.
2. **Theorem. (Division Algorithm)** Let $d \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that
$$a = qd + r$$
where $0 \leq r < d$.
3. **Proposition [Euclidean Algorithm].** Let a and b be integers and b positive. By the Division Algorithm there are unique integers q, r so that
$$a = bq + r \qquad \text{and } 0 \leq r < b.$$
Then
$$\gcd(a, b) = \gcd(b, r).$$
4. **Proposition (Bezout's identity).** Let a, b be integers, not both zero. Then there exist integers l, m such that
$$\gcd(a, b) = la + mb.$$
5. **Corollary (Euclid's Lemma).** Let p, b, c be integers, and p a prime number. If $p \mid bc$ and $p \nmid b$, then $p \mid c$.
6. **Theorem (Fundamental Theorem of Arithmetic).** Every integer a greater than or equal to 2 can be expressed as a product of prime numbers. That is
$$a = p_1 \ldots p_n$$
where the p_j are primes. This includes the special case of $n = 1$ and so a is prime.

   Furthermore, this expression is unique if we require that the primes be listed in non-decreasing order.
$$p_1 \leq p_2 \leq \cdots \leq p_n.$$
7. **Theorem (Fermat's Little Theorem).** Let p be a prime number and let a be a nonzero element of $\mathbb{Z}_p$. Then
$$a^{p-1} \equiv 1 \mod p.$$

Miscellaney.

1. **Chinese Remainder Theorem.** Let $m_1, \ldots, m_k$ be pairwise relatively prime natural numbers. The system of simultaneous linear congruences

$$x \equiv a_1 \mod m_1\,, \quad \ldots \quad, x \equiv a_k \mod m_k$$

has a unique solution $\mod M$, where $M = m_1 \ldots m_k$.

This solution is found as follows. Let $z_i = M/m_i$ and note that for each i the congruence

$$z_i y_i \equiv 1 \mod m_i$$

has a solution y_i (because $\gcd(z_i, m_i) = 1$). Now a solution to the simultaneous congruences is found by

$$x \;=\; a_1 y_1 z_1 + \cdots + a_k y_k z_k$$

2. **Definition (Group).** A *group* consists of a set G and a binary operation $\circ : G \times G \to G : (g, h) \mapsto g \circ h$ which satisfies the following properties.

   (a) **Associativity.** For all $g, h, k \in G$ we have

   $$(g \circ h) \circ k \;=\; g \circ (h \circ k)$$

   (b) **Identity.** There is an element $e \in G$ such that

   $$e \circ g \;=\; g \circ e \;=\; g$$

   for all $g \in G$.

   (c) **Inverses.** For every $g \in G$ there exists $g^{-1} \in G$ such that

   $$g \circ g^{-1} \;=\; g^{-1} \circ g \;=\; e$$

   Note that the *closure* property is included in the definition of a binary operation as being a function from $G \times G$ with values in G.

3. **Cayley's Theorem.** Every group is isomorphic to a subgroup of a group of permutations.

4. **Lagrange's Theorem.** If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.