Notes 1

Math 214, Fall 2017

A **field** is a set F together with two operations, usually called addition and multiplication, and denoted "$+$" and "$\cdot$" respectively, such that the following axioms hold.

(A1) $\forall a, b \in F$, $a + b \in F$ and $a \cdot b \in F$.

(A2) $\forall a, b, c \in F$, $a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(A3) $\forall a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(A4) There exists an element $0 \in F$, such that $\forall a \in F$, $a+0 = a$. Likewise there exists an element 1, such that $\forall a \in F$, $a \cdot 1 = a$. 1 is required not to equal 0.

(A5) $\forall a \in F$, $\exists(-a) \in F$, such that $a + (-a) = 0$. Similarly, $\forall a \in F$ and $a \neq 0$, $\exists a^{-1} \in F$, such that $a \cdot a^{-1} = 1$.

(A6) $\forall a, b, c \in F$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

An **ordered field** is a field which also satisfies the following axioms about an order structure $\leq$.

(B1) For any $a, b \in F$, either $a \leq b$ or $b \leq a$.

(B2) If $a \leq b$ and $b \leq a$, then $a = b$.

(B3) If $a \leq b$ and $b \leq c$, then $a \leq c$.

(B4) If $a \leq b$, then $a + c \leq b + c$.

(B5) If $a \leq b$ and $0 \leq c$, then $ac \leq bc$.

We also define $a < b$ if $a \leq b$ and $a \neq b$; moreover we define $a \geq b$ if and only if $b \leq a$, and $a > b$ if and only if $b < a$.

Theorem 1. *Let F be a field, and let $a, b, c \in F$. Then*

1. *$a + b = b + c$ implies $a = b$;*
2. *$\forall a \in F$, $a \cdot 0 = 0$;*
3. *$(-a) \cdot b = -(ab)$;*
4. *$(-a) \cdot (-b) = ab$;*
5. *$ac = bc$ and $c \neq 0$ imply $a = b$;*
6. *$ab = 0$ implies that $a = 0$ or $b = 0$.*

Theorem 2. *Let F be an ordered field with order $\leq$, and let $a, b, c \in F$. Then*

1. *If $a \leq b$, then $-b \leq -a$;*
2. *If $a \leq b$ and $c \leq 0$, then $bc \leq ac$;*
3. *If $0 \leq a$ and $0 \leq b$, then $0 \leq ab$;*
4. *$\forall a \in F$, $0 \leq a^2 = a \cdot a$;*
5. *$0 < 1$;*
6. *If $0 < a$, then $0 < a^{-1}$;*
7. *If $0 < a < b$, then $0 < b^{-1} < a^{-1}$.*

Common sets of numbers

$\mathbb{N}$ is the set of all natural numbers; $\mathbb{Z}$ is the set of all integers; $\mathbb{Q}$ is the set of rational numbers; and $\mathbb{R}$ is the set of of all real numbers. For $x \in \mathbb{R}$, $|x| = x$ if $x \geq 0$, and $|x| = -x$ if $x < 0$.

$\mathbb{Q}$ and $\mathbb{R}$ are both ordered fields. Therefore $\mathbb{Q}$ and $\mathbb{R}$ satisfy axioms (A1)-(A6), and also (B1)-(B5).

$\mathbb{Z}$ is not a field, but it satisfies all (A1)-(A6) and (B1)-(B5) except the existence of a^{-1} for each $a \in \mathbb{Z}$.

Basic Number Theory

For $a, b \in \mathbb{Z}$, $a|b$ (a *divides* b) if $b = ak$ for some $k \in \mathbb{Z}$. In this case, b is a *multiple* of a, and a is a *divisor* of b. An integer a is *even* if $2|a$, and a is *odd* if $2 \nmid a$. Or an integer p is an *even* number if there exists $q \in \mathbb{Z}$ such that $p = 2q$, and an integer p is an odd number if if there exists $q \in \mathbb{Z}$ such that $p = 2q - 1$.

For each $x \in \mathbb{Q}$, there exist $p, q \in \mathbb{Z}$ and $q \neq 0$, and p, q have no common positive divisors other than 1, such that $x = \dfrac{p}{q}$.

A *prime* number is an integer $p \geq 2$ whose only positive divisors are 1 and p. An integer $p \geq 2$ that is not prime is a *composite* number.

Theorem 3.12: Let $x \in \mathbb{Z}$. Then x^2 is even if and only if x is even; and x^2 is odd if and only if x is odd.

Result 4.1-4.3: Let $a, b, c, d \in \mathbb{Z}$ and $a \neq 0$, $b \neq 0$. (4.1) If $a|b$ and $b|c$, then $a|c$; (4.2) If $a|c$ and $b|d$, then $ab|cd$; (4.3) If $a|c$ and $a|d$, then $a|(cx+dy)$ for $x, y \in \mathbb{Z}$.

Result 5.15: Let a be a rational number, and let b be an irrational number. Then (i) $a + b$ is irrational; (ii) If $a \neq 0$, then $a \cdot b$ is irrational.

Axioms for rational numbers (special case of axiom (A1)): Let a, b be rational numbers. Then (i) $a + b$ is rational; (ii) $a \cdot b$ is rational.

$\mathbb{N}$ is *well-ordered*, that is, every non-empty subset of $\mathbb{N}$ has a smallest element. (**Well-Ordering Principle**)