Math 295. Summary of Basic Definitions not in the Text.

If A and B are sets, a **function** $f : A \to B$ with domain (or source) A and range (or target) B is a subset $f \subseteq A \times B$ such that for all $a \in A$, there is a *unique* $b \in B$ (denoted $f(a)$) with (a, b) in the subset $f \subseteq A \times B$. If $A = B = \mathbb{R}$, this is just a description of a "graph" which meets every vertical line exactly one. We denote the effect of the function f by the notation $a \mapsto f(a)$ for a specific $a \in A$.

We say that $f : A \to B$ is **injective** (or one-to-one) if $a \neq a' \Rightarrow f(a) \neq f(a')$ (or equivalently, whenever $f(a) = f(a')$ then necessarily $a = a'$). If $A = B = \mathbb{R}$, this says that the graph of f meets every horizontal line at most once. We say that f is **surjective** (or onto) if every $b \in B$ can be expressed in the form $b = f(a)$ for some (perhaps many) $a \in A$. If f is both surjective and injective, we say f is **bijective**. Explicitly, f is bijective iff for all $b \in B$ the equation $f(x) = b$ has a unique solution in A.

If S is a set, a **binary operation** is a function $\oplus : S \times S \to S$, described by the notation $(s, s') \mapsto s \oplus s'$. We say that $\oplus$ is **associative** if $s \oplus (s' \oplus s'') = (s \oplus s') \oplus s''$ for all $s, s', s'' \in S$. We say that $\oplus$ is **commutative** if $s \oplus s' = s' \oplus s$ for all $s, s' \in S$. Using the method of induction, one can then establish similar identities for forming $\oplus$'s of any finite set of elements in S.

We say that $e \in S$ is an **identity element** for $\oplus$ if $s \oplus e = e \oplus s$ for all $s \in S$. Such an element is uniquely determined by this condition if it exists. If $\oplus$ is associative and has a (necessarily unique) identity element e, then for a fixed element $s \in S$ we say that $s' \in S$ is an **$\oplus$-inverse** of s if $s \oplus s' = s' \oplus s = e$. Thanks to associativity, such an element s' is uniquely determined by this condition if it exists.

A set F equipped with associative binary operations $+, \cdot$ is called a **field** if

- there exists an identity element (denoted 0) for $+$ and $+$-inverses for all elements,
- there exists an identity element (denoted 1) for $\cdot$ and $\cdot$-inverses for all $x \in F$, $x \neq 0$,
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$
- $1 \neq 0$

An **order structure** on a field F is a subset $P \subseteq F$ such that P is stable under $+$, $\cdot$ and the **trichotomy property** is satisfied (for all $x \in F$ exactly one of the following holds: $x = 0$, $x \in P$, or $-x \in P$). We then say (for $a, b \in F$) that $a > b$ when $a - b \in P$. We define $|a|$ for $a \in F$ as follows: $|a| = a$ when $a \in P$, $|a| = -a$ when $-a \in P$, and $|a| = 0$ when $a = 0$. When an order structure is speficied, we call the data (F, P) an **ordered field** (and usually abbreviate this by suppressing explicit mention of P). For an ordered field F, the positive elements are stable under formation of multiplicative inverses and the **triangle inequality** holds: $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

A subset $S \subseteq F$ is **bounded above** if there exists $b \in F$ such that $s \leq b$ for all $s \in S$ (and then we call such b an **upper bound** for S). The notions of **bounded below** and **lower bound** are defined similarly with reverse inequalities. A **supremum** for a subset $S \subseteq F$ is a least upper bound for S (if it exists); it is denoted $\sup(S)$. An **infimum** for a subset $S \subseteq F$ is a greatest lower bound for S (if it exists); it is denoted $\inf(S)$. We say that F is **complete** if every *non-empty* bounded-above subset of F has a supremum (in F, of course). In this case, every non-empty bounded-below subset has an infimum.

A subset N of an ordered field F is said to be **inductive** if $1 \in N$ and if $n + 1 \in N$ whenever $n \in N$. There is a unique inductive set $\mathbb{N}_F \subseteq F$ which is contained inside of all other inductive sets in F. It is stable under addition and multiplication, $n \geq 1$ for all $n \in \mathbb{N}_F$, and whenever $m, n \in \mathbb{N}_F$ then $m < n$ iff $n = m + r$ for some $r \in \mathbb{N}_F$ (in particular, $m < n$ iff $m + 1 \leq n$). Moreover, $\mathbb{N}_F$ satisfies the **weak induction property**: if $S \subseteq \mathbb{N}_F$ is an inductive subset then $S = \mathbb{N}_F$.

The subset $\mathbb{N}_F \subseteq F$ satisfies two additional properties: the **strong induction** property (if $S \subseteq \mathbb{N}_F$ and $n \in S$ whenever $\{k \in \mathbb{N}_F \mid k < n\} \subseteq S$, then $S = \mathbb{N}_F$) and the **well-ordering principle** (every *non-empty* subset of $\mathbb{N}_F$ contains a minimal element).

We define $\mathbb{R}$ to be a complete ordered field (and will later prove it to be "unique" in a very precise sense). When $F = \mathbb{R}$, we write $\mathbb{N}$ rather than $\mathbb{N}_F$. We define $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$. This is stable under addition, multiplication, and additive inversion. Moreover, we define

$$\mathbb{Q} = \{x \in \mathbb{R} \mid x = m/n \text{ for some } m, n \in \mathbb{Z}, n \neq 0\}.$$

This is an *ordered field* inside of $\mathbb{R}$. The order structures on $\mathbb{Q}$ and $\mathbb{R}$ are unique.

The completeness of $\mathbb{R}$ implies that $\mathbb{N}$ is *not* bounded above. Using this, one shows that the ordered field $\mathbb{R}$ satisfies the **archimedean property** (for every $\varepsilon > 0$ and every $x \in \mathbb{R}$ there exists $n \in \mathbb{N}$ such that $n\varepsilon > x$) and that a mild **generalized well-ordering principle** holds: any non-empty subset of $\mathbb{Z}$ which is bounded below in $\mathbb{R}$ contains a minimal element.

Taking $x = 1$ in the archimedean property, we see that for every $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $0 < 1/n < \varepsilon$. For any $x, y \in \mathbb{R}$ with $x < y$ there exists $q \in \mathbb{Q}$ with $x < q < y$ and that for all $\beta \in \mathbb{R}$ there is a unique $m \in \mathbb{Z}$ such that $\beta - 1 < m \leq \beta$; this m is called the **greatest integer less than or equal to** β and is denoted $[\beta]$. We then call $\beta - [\beta] \in [0, 1)$ the **fractional part** of β.

We say that $x \in \mathbb{R}$ is **non-negative** when $x \geq 0$. The equation $x^2 = a$ has a solution in $\mathbb{R}$ iff $a \geq 0$. For such a, this equation has a unique non-negative solution, denoted $\sqrt{a}$, and $\sqrt{a} > 0$ when $a > 0$.

If S is a set, a function $f : S \to \mathbb{R}$ is **bounded above** if there is some $b \in \mathbb{R}$ such that $f(x) \leq b$ for all $x \in S$. Likewise, f is **bounded below** if there is some $b \in \mathbb{R}$ such that $f(x) \geq b$ for all $x \in S$. When both conditions hold, we say f is **bounded**. If $S \subseteq \mathbb{R}$ then we say that f is **increasing** (resp. **decreasing**) if $f(x) < f(y)$ (resp. $f(x) > f(y)$) whenever $x < y$.

The **division algorithm** in $\mathbb{Z}$ states that for every $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ and $a = bq + r$. When $b = 1 + 1$ we say that a is **even** if $r = 0$ and a is **odd** if $r = 1$.

A natural number $n \in \mathbb{N}$ is said to be **prime** if $n > 1$ and whenever $n = ab$ with $a, b \in \mathbb{N}$ then $a = 1$ (or equivalently, $b = n$) or $b = 1$ (or equivalently, $a = n$). Every $n \in \mathbb{N}$ larger than 1 is a product of finitely many primes.