Final Notes  
Math 214, Spring 2015

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 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 $2 \not{|} a$. $a \equiv b \pmod{n}$ if $n|(a - b)$.

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 there exists $q \in \mathbb{Z}$ such that $p = 2q - 1$.

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

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 $x = \frac{p}{q}$.

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.

An integer $c \neq 0$ is a common divisor of two integers $a$ and $b$ if $c | a$ and $c | b$. The greatest common divisor $(\text{gcd}(a, b))$ of $a$ and $b$ is the greatest positive integer that is a common divisor of $a$ and $b$. Two integers $a$ and $b$ are relatively prime if $\text{gcd}(a, b) = 1$. 
Theorem 10.13: Let $n \in \mathbb{Z}$. Then $n^2$ is even if and only if $n$ is even. Hence $n^2$ is odd if and only if $n$ 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 $a | (cx + dy)$ where $x, y \in \mathbb{Z}$.

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 a rational numbers. Then (i) $a + b$ is rational; (ii) $a \cdot b$ is rational.

Theorem 8.2-8.3: Let $R$ be an equivalence relation on a nonempty set $A$. (8.2) If $a, b \in A$, then $[a] = [b]$ if and only $a R b$; (8.3) The set $P = \{[a] : a \in A\}$ of equivalence classes of $R$ is a partition of $A$.

Theorem 9.8: Let $A$ and $B$ be finite nonempty sets such that $|A| = |B|$, and let $f : A \rightarrow B$ be a function. Then $f$ is injective if and only if $f$ is surjective.

Theorem 9.11-9.12: Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be two functions. (9.11-a) If $f$ and $g$ are injective, so is $g \circ f$; (9.11-b) If $f$ and $g$ are surjective, so is $g \circ f$; (9.12) If $f$ and $g$ are bijective, so is $g \circ f$.

Theorem 9.15: Let $f : A \rightarrow B$ be a function. Then the inverse relation $f^{-1}$ is a function from $B$ to $A$ if and only if $f$ is bijective. Moreover, if $f$ is bijective, then $f^{-1}$ is also bijective.

Result 10.3: $\mathbb{Z}$ is denumerable.

Theorem 10.4: Every infinite subset of a denumerable set is denumerable.

Result 10.5: $k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$ is denumerable.

Result 10.6: If $A$ and $B$ are denumerable, so is $A \times B$.

Result 10.8: $\mathbb{Q}$ is denumerable.

Theorem 10.9: $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ is uncountable.

Corollary 10.11: $\mathbb{R}$ is uncountable.

Theorem 10.13: If $A$ is denumerable, and $B$ is uncountable, then $|A| < |B|$.

Theorem 10.14: $(0, 1)$ and $\mathbb{R}$ are numerically equivalent.

Theorem 10.16: For every nonempty set $A$, $\mathcal{P}(A)$ and $2^A$ are numerically equivalent.

Theorem 10.17: For every set $A$, $|A| < |\mathcal{P}(A)|$.

Theorem 10.20 (Schröder-Berstein) If $A$ and $B$ are sets such that $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

(If there exist two injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$, then there exists a bijection between $A$ and $B$, that is $|A| = |B|$.)

Theorem 10.21 $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

Result 10.22 (a) Suppose that $f : A \rightarrow B$ is an injection, and $B$ is countable, then $A$ is also countable; (b) Suppose that $f : A \rightarrow B$ is a surjection, and $A$ is countable, then $B$ is also countable. (problem 10.43)

Result 10.23 Let $A_\alpha$ be a countable set for each $\alpha \in I$, and let $I$ be a countable index set. Then $\bigcup_{\alpha \in I} A_\alpha$ is also countable.

Theorem 11.3 Let $a, b \in \mathbb{Z}$ and $a, b \neq 0$. (i) If $a | b$ and $b | a$, then $a = b$ or $a = -b$; (ii) If $a | b$, then $|a| \leq |b|$.

Theorem 11.4 (division algorithm) For $a, b \in \mathbb{N}$, there exist unique $q, r \in \mathbb{Z}$ s.t. $b = aq + r$ and $0 \leq r < a$.

Theorem 11.7 Let $a, b \in \mathbb{Z}$ and $a, b \neq 0$. Then $gcd(a, b) = \min\{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. In particular, there exist $x, y \in \mathbb{Z}$ such that $gcd(a, b) = ax + by$.

Lemma 11.9 For $a, b \in \mathbb{N}$, if $b = aq + r$ for $q, r \in \mathbb{Z}$, then $gcd(a, b) = gcd(r, a)$.

Theorem 11.12 Let $a, b \in \mathbb{Z}$ and $a, b \neq 0$. Then $gcd(a, b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Theorem 11.13 (Euclid’s Lemma) Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$. If $a | bc$ and $gcd(a, b) = 1$, then $a | c$.

Corollary 11.14 Let $b, c \in \mathbb{Z}$ and $p$ a prime. If $p | bc$, then either $p | b$ or $p | c$.

Theorem 11.16 Let $a, b, c \in \mathbb{Z}$ and $gcd(a, b) = 1$. If $a | c$ and $b | c$ then $(ab) | c$.

Theorem 11.17 (Fundamental Theorem of Arithmetic) Every integer $n \geq 2$ is either prime or can be expressed as a product of primes: $n = p_1p_2 \cdots p_m$, where $p_i$ are primes. Furthermore, such factorization is unique except the order in which factors occur.

Corollary 11.18 Every integer exceeding 1 has a prime factor.

Theorem 11.20 Let $n \in \mathbb{N}$. Then $\sqrt{n}$ is a rational number if and only if $\sqrt{n} \in \mathbb{N}$.

Corollary 11.21 If $p$ is a prime, then $\sqrt{p}$ is irrational.

Theorem 11.22 There are infinitely many prime numbers.