Appendix A Sets

Definition. *Set definitions*

1. ***Set*** *is a collection of objects, called elements of the set.*

2. ***Subset*** $B \subseteq A$ *if every element of* B *is an element of* A

3. ***Proper Subset*** B *is a proper subset of* A *if* $B \subseteq A$ *and* $B \neq A$

4. ***Equality*** *Two sets are equal,* $A = B$*, if and only if* $A \subseteq B$ *and* $B \subseteq A$

5. ***Empty Set*** $\emptyset$ *is a subset of every set.*

6. ***Union, Intersection***

   $A \cup B = \{x : x \in A \text{ or } x \in B\}$ $\quad$ $A \cap B = \{x : x \in A \text{ and } x \in B\}$

   $$\bigcup_{i=1}^{n} A_i = \{x : x \in A_i \text{ for some } i = 1, 2, \cdots, n\} \qquad \bigcap_{i=1}^{n} A_i = \{x : x \in A_i \text{ for all } i = 1, 2, \cdots, n\}$$

   $$\bigcup_{\alpha \in \Lambda} = \{x : x \in A_\alpha \text{ for some } \alpha \in \Lambda\} \qquad \bigcap_{\alpha \in \Lambda} = \{x : x \in A_\alpha \text{ for all } \alpha \in \Lambda\}$$

   where Λ *is an index set and* $\{A_\alpha : \alpha \in \Lambda\}$ *is a collection of sets.*

7. ***Disjoint*** *Two sets are disjoint if their intersection equals the empty set* $A \cap B = \emptyset$

8. ***Relation*** *A relation on* A *is a set* S *of ordered pairs of elements of* A *such that* $(x, y) \in S$ *if and only if* x *stands in the given relationsihp to* y*. For example, is equal to, is less than, .. are relations. If* S *is a relation on a set* A*, we write* $x \sim y$ *in place of* $(x, y) \in S$

9. ***Equivalence Relation*** *A relation* S *on a set* A *is an equivalence relation on* A *if the 3 condition holds*

   (a) *For all* $x \in A$, $x \sim x$ *(reflexivity)*
   (b) *If* $x \sim y$*, then* $y \sim x$ *(symmetry)*
   (c) *If* $x \sim y$ *and* $y \sim z$*, then* $x \sim z$ *(transitivity)*

   If we define $x \sim y$ *to be* $x - y$ *divisible by a fixed integer* n*, then* $\sim$ *is an equivalence relation on the set of integers.*

Appendix B Functions

Definition. *Functions*

1. ***Function*** *A, B are sets, a function f from A to B, $f : A \to B$ is a rule that associates each element $x \in A$ a unique element denoted by $f(x)$ in B.*

2. ***Image and Preimage*** *The element $f(x)$ is the image of x under f; x is the preimage of $f(x)$ under f.*

   (a) *If $S \subseteq A$, then denote by $f(S)$ the set $\{f(x) : x \in S\}$ of all images of elements of S.*

   (b) *Likewise, denote by $f^{-1}(T)$ the set $\{x \in A : f(x) \in T\}$ of all preimages of elements in T.*

   (c) *Preimage of an element in the range need not be unique*

3. ***Domain and Codomain*** *If $f : A \to B$, then A is called the domain of f and B is called the codomain of f.*

4. ***Range*** *The set $\{f(x) : x \in A\}$ is called the range of f. Note the range of f is a subset of B*

5. ***Function Equality*** *Two functions $f : A \to B$ and $g : A \to B$ are equal, $f = g$, if $f(x) = g(x)$ for all $x \in A$*

6. ***One-to-one*** *Functions such that each element of the range has a unique preimage are one-to-one; that is $f : A \to B$ is one-to-one if $f(x) = f(y)$ implies $x = y$, or equivalently, if $x \neq y$ implies $f(x) \neq f(y)$*

7. ***Onto*** *If $f : A \to B$ is a function with range B, that is if $f(A) = B$, then f is called onto. In other words, f is onto if and only if the range of f equals codomain of f*

8. ***Restriction*** *Let $f : A \to B$ be a function and SA. Then a function $f_S : S \to B$, called restriction of f to S, can be formed by defining $f_S(x) = f(x)$ for all $x \in S$. (Note codomain stay unchanged for restriction)*

9. ***Composite*** *Let A, B, C, be sets and $f : A \to B$ and $g : B \to C$ be functions. then $g \circ f : A \to C$ is a composite of g and f, i.e. $(g \circ f)(x) = g(f(x))$ for all $x \in A$.*

   (a) *Usually composites are not associative, i.e. $g \circ f \neq f \circ g$*

   (b) *associative this way, $h \circ (g \circ f) = (h \circ g) \circ f$*

10. ***Invertible Function*** *A function $f : \mathbb{R} \to \mathbb{R}$ is invertible if there exists a function $g : B \to A$ such that $(f \circ g)(y) = y$ for all $y \in B$ and $(g \circ f)(x) = x$ for all $x \in A$. If such a function g exists, then it is unique and is called inverse of f, denoted as f^{-1}.*

11. ***Invertible Function Properties***

(a) f is invertible if and only if f is both one-to-one and onto

(b) If $f : A \to B$ is invertible, then f^{-1} is invertible, $(f^{-1})^{-1} = f$

(c) If $f : A \to B$, $g : B \to C$ are invertible, then $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Appendix C Fields

Definition. *Field*
A field F is a set on which two operations $+$ and $\cdot$ (addition and multiplication) are defined so that, for each pair of elements x, y in F, there are unique elements sum, $x + y$, and products ,$x \cdot y$, in F for which the conditions hold for all elements $a, b, c \in F$

1. *Commutativity of addition and multiplication*

$$a + b = b + a \quad \textit{and} \quad a \cdot b = b \cdot a$$

2. *Associativity of addition and multiplication*

$$(a + b) + c = a + (b + c) \quad \textit{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. *Existence of identity elements for addition and multiplication, i.e. exists distinct identity elements zero, 0, and one, 1, in F such that*

$$0 + a = a \quad \textit{and} \quad 1 \cdot a = a$$

4. *Existence of inverses for addition and multiplication, i.e. for each $a \in F$ and each nonzero element $b \in F$, there exists $c, d \in F$ such that*

$$a + c = 0 \quad \textit{and} \quad b \cdot d = 1$$

   where c is the additive inverse for a and d is a multiplicative inverse for b.

5. *Distributivity of multiplication over addition*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Example.

1. The set of real numbers $\mathbb{R}$ with usual definition of addition and multiplication is a field.

2. The set of integers with usual definition of addition and multiplication is a field, since no inverses exist for addition and multiplication.

Theorem. ***Cancellation Laws***
For arbitrary elements a, b, c in a field, following statements are true,

1. *If $a + b = c + b$, then $a = c$*
2. *If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$*

Proof. Prove second part, If $b \neq 0$, then exists multiplicative inverse d such that $b \cdot d = 0$. Now multiply both sides of equation to by d, by associativity of multiplication and identity of multiplication we have

$$(a \cdot b) \cdot d = (c \cdot b) \cdot d \quad \to \quad a \cdot (b \cdot d) = c \cdot (b \cdot d) \quad \to \quad a \cdot 1 = c \cdot 1 \quad \to \quad a = c$$

□

Corollary. ***Each element in field has unique additive/multiplicative inverse***
The elements 0 and 1 mentioned in condition 3 of definition for field and c and d mentioned in condition 4 are unique

Proof. Suppose eists another zero $0' \in F$ such that $0' + a = a$ for all $a \in F$. Since $0 + a = a$ for all $a \in F$, we have $0' + a = 0 + a$ so $0 = 0'$ □

Additive inverse and multiplicative inverse are denoted by $-b$ and d^{-1}. They are used to represent subtraction and division

$$a - b = a + (-b) \qquad \frac{a}{b} = a \cdot b^{-1}$$

Theorem. *Let a and b be arbitrary elements of a field. Then each of the following statements are true*

1. $a \cdot 0 = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Proof.

1. $$0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$
   so $0 = a \cdot 0$ by cancellation theorem
2. Note $-(a \cdot b)$ is an unique element of F with property $a \cdot b + (-(a \cdot b)) = 0$. To prove $(-a) \cdot b = -(a \cdot b)$, we show $a \cdot b + (-a) \cdot b = 0$
   $$a \cdot b + (-a) \cdot b = (a + -(a)) \cdot b = 0 \cdot b = 0$$
   Similarly for proving $a \cdot (-b) = -(a \cdot b)$

3. Applying 2nd point twice

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

□

Corollary. *The additive identity of a field has no multiplicative inverse.*

Definition. ***Characteristic of Field*** *The smallest positive integer p for which a sum of p 1's equals 0 is called the characteristic of F. If no such p exists, then F is said to have characteristic zero. ($\mathbb{R}$ has characteristic zero)*

Appendix D Complex Number

Definition. ***Complex Number*** *A complex number is an expression of the form $z = a + bi$ where a and b are real numbers called the* ***real part*** *and the* ***imaginary part*** *of z, respectively. The sum and product of 2 complex numbers $z = a + bi$ and $w = c + di$ are defined as*

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

$$zw = (a + bi)(c + di) = (ac - bd) + (bc + ad)i$$

1. *Any real number $c \in \mathbb{R}$ can be regarded as a complex number with $c + 0i$.*
2. *Any complex number of form $bi = 0 + bi$, where b is nonzero real, is called an* ***imainary****. The product of 2 imaginary number is real*

   $$(bi)(di) = (0 + bi)(0 + di) = (0 - bd) + (b \cdot 0 + 0 \cdot d)i = -bd$$

   In particular, for $i = 0 + 1i$, $i \cdot i = -1$
3. *Real number 0 is an additive identity for the complex numbers; Real number 1 is a multiplicative identity element for the set of complex number*
4. *Each complex number $a + bi$ has an additive inverse. Each complex number except 0 has a multiplicative inverse,*

   $$-(a + bi) = (-a) + (-b)i$$

   $$(a + bi)^{-1} = (\frac{a}{a^2 + b^2}) - (\frac{b}{a^2 + b^2})i$$

Theorem. *The set of complex numbers with the operations of addition and multiplication previously defined is a field. (Just verify all the conditions...)*

Definition. ***Complex Conjugate*** *The complex confugate of a complex number $a + bi$ is the complex number $a - bi$. Denote conjugate of a complex number z by $\overline{z}$. As an example,*

$$\overline{-3 + 2i} = -3 - 2i \qquad \overline{6} = \overline{6 + 0i} = \overline{6 - 0i} = 6$$

Theorem. ***Complex Conjugate Properties***
Let z and w be complex numbers. Then the following statement is true

1. $\overline{\overline{z}} = z$
2. $\overline{(z+w)} = \overline{z} + \overline{w}$
3. $\overline{zw} = \overline{z} \cdot \overline{w}$
4. $\overline{(\frac{z}{w})} = \frac{\overline{z}}{\overline{w}}$
5. z *is a real number if and only if* $\overline{z} = z$

Definition. ***Abosolute Value*** *let $z = a+bi$, where $a, b \in \mathbb{R}$. The absolute value (modulus) of z is the real number $\sqrt{a^2+b^2}$. We denote the absolute value of z by $|z|$. Note $z\overline{z} = |z|^2$, follows from*

$$z\overline{z} = (a+bi)(a-bi) = a^2 + b^2$$

gives that product of a complex number with its conjugate is a real number provides an easy method for determining the quotient of 2 complex numbers, if $c + di \neq 0$, then

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\frac{c-di}{c-di} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Also note, $|\overline{z}| = |z|$, and $|z| = |-z|$

Theorem. *Let z and w denote any two complex numbers, then the following are true*

1. $|zw| = |z| \cdot |w|$
2. $|\frac{z}{w}| = \frac{|z|}{|w|}$ *if* $w \neq 0$
3. $|z+w| \leq |z| + |w|$ *(triangular inequality)*
4. $|z| - |w| \leq |z+w|$

Definition. ***Geometric Interpretation*** *In $\mathbb{R}^2$, there are two axes, the real axis and the imaginary axis, the absolute value of z gives the length of the vector z. By a special case of Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, we use $e^{i\theta}$ to represent the unit vector that makes an angle θ with the positive real axis. Any nonzero complex number z can be depicted as a multiple of a unit vector, i.e. $z = |z|e^{i\theta}$*

Theorem. ***The Foundamental Theorem of Algebra*** *Suppose that $p(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ is a polynomial in $P(C)$ of degree $n \geq 1$. Then $p(z)$ has a zero*

Remark. The theorem states that every non-constant single-variable polynomial with complex (or specifically real) coefficients has at least one complex root.

Corollary. *If* $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ *is a polynomial of degree* $n \geq 1$ *with complex coefficients, then there exists complex number* $c_1, c_2, \cdots, c_n$ *such that*

$$p(z) = a_n(z - c_1)(z - c_2)\cdots(z - c_n)$$

In other words, all polynomials can be factored in this case.

Definition. ***Algebraically Closed*** *A field i called algebraically closed if it has the property that every polynomial of positive degree with coefficients from that field factors as a product of polynomial of degree 1.*