0 Foundational material: The appendices

0.1 Appendix A: Sets

Definition 0.1. A set is a collection of objects, called elements.

Example 0.2.

- \{1, 2, 3\} = \{2, 1, 1, 2, 3\} (no notion of “multiplicity”, no notion of order)
- [1, 2] = the interval of reals between 1 and 2, including 1 and 2.
- \(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\) (later)
- \(\begin{bmatrix} 8 \\ 0 \\ -1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}\) = set of two vectors
- \(\emptyset\): the empty set

Given two sets \(A, B\), there are several operations that yield new sets from these. Most important are the following:

- \(A \cup B\) (union of \(A\) and \(B\))
- \(A \cap B\) (intersection of \(A\) and \(B\))
- \(A \times B = \{(a, b) : a \in A, b \in B\}\) (product of \(A\) and \(B\))

Definition 0.3. Let \(A\) be a set. A relation on \(A\) is a subset \(S\) of \(A \times A\). Write \(x \sim y\) if and only if \((x, y) \in S\).

Example 0.4.

- \(A = \{1, 2, 3\}, S = \{(1, 2), (1, 3), (2, 3)\}\). This relation is “<”.
- \(A = \{1, 2, 3\}, S = \{(1, 2), (1, 3), (2, 3), (2, 1), (2, 3), (3, 1), (3, 2)\}\). This relation is “\(\neq\)”.
- \(A = \{1, 2, 3\}, S = \{(1, 1), (2, 2), (3, 3)\}\). This relation is “=”. 

Recall the following symbols. \(\forall\): “for all”, \(\exists\): “there exists”. 

**Definition 0.5.** Let $A$ be a set with a relation $S$. Then $S$ is called an *equivalence relation* if and only if

i. $\forall x \in A : x \sim x$ (reflexive)

ii. $\forall x, y \in A : x \sim y \iff y \sim x$ (symmetric)

iii. $\forall x, y, z \in A : (x \sim y$ and $y \sim z) \Rightarrow x \sim z$ (transitive)

**Example 0.6.** Let $A = \mathbb{Z}$. Let $x \sim y \iff \exists k \in \mathbb{Z} : x - y = 5k$. This defines an equivalence relation.

i. reflexive: Let $x \in \mathbb{Z}$. Then $x - x = 0 = 5 \cdot 0$. Done.

ii. symmetric: Let $x, y \in \mathbb{Z}$ with $x \sim y$. Then $x - y = 5k$ implies $y - x = 5 \cdot (-k)$. Done.

iii. transitive: Let $x, y, z \in \mathbb{Z}$ with $x \sim y$ and $y \sim z$. Then $x - y = 5k_1$ and $y - z = 5k_2$ implies (by adding the two equalities) $x - z = 5 \cdot (k_1 + k_2)$. Done.

### 0.2 Appendix B: Functions

**Definition 0.7.** Let $A, B$ be sets. A function $f : A \to B$ is a rule that associates to each element $x \in A$ a unique element of $B$, denoted $f(x)$. The set $A$ is called the *domain*, the set $B$ is called the *codomain*.

**Definition 0.8.**

- For $S \subseteq A, f(S) = \{f(x) : x \in S\}$ (image of $S$ under $f$). $f(A)$ is called the *range*.
- For $T \subseteq B, f^{-1}(T) = \{x \in A : f(x) \in T\}$ (pre-image of $T$ under $f$)
- $f : A \to B = g : A \to B \iff \forall x \in A : f(x) = g(x)$

**Definition 0.9.**

- $f : A \to B$ is *injective* if and only if $f(x) = f(y) \Rightarrow x = y$.
- $f : A \to B$ is *surjective* if and only if $\forall b \in B \exists a \in A : f(a) = b$.
- For $S \subseteq A$, the restriction of $f$ to $S$ is $f|_S : S \to B, x \mapsto f(x)$.  

3
0.3 Appendix C: Fields

**Definition 0.10.** Let $A$ be a set. A binary operation is any map $A \times A \rightarrow A$. We are very familiar with $\mathbb{Q}$ and $\mathbb{R}$ and the properties that the two binary operations $+$ and $\cdot$ have.

**Definition 0.11.** A field $F$ is a set with two binary operations labelled $+$ and $\cdot$ such that

i. $a + b = b + a$, $a \cdot b = b \cdot a$ (commutativity)

ii. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity)

iii. $\exists 0 \in F : a + 0 = a \forall a$
    $\exists 1 \in F : 1 \cdot a = a \forall a$ (neutral elements)

iv. $\forall a \in A : \exists b \in A : a + c = 0$
    $\forall a \in A \setminus \{0\} : \exists b \in A : a \cdot b = 1$ (inverse elements)

v. $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributive law)

**Theorem 0.12** (Cancellation Laws). Let $F$ be a field and $a, b, c \in F$.

i. $a + b = c + b \Rightarrow a = c$

ii. $a \cdot b = c \cdot b$ and $b \neq 0 \Rightarrow a = c$

**Proof.** Part i. Let $d$ be an additive inverse of $b$. Now, observe that $(a + b) + d = a$ and $(c + b) + d = c$. Done.

Part ii is done in detail in the textbook. \qed

**Proposition 0.13.** The neutral element of addition is unique.

**Proof.** Let $0$ and $0'$ be two neutral elements of addition. Then

$$0 = 0 + 0' = 0'.$$

Fields enjoy several other important properties (not listed here).

**Example 0.14.** Some examples of fields.
• $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
• $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ (see also Homework 1).

0.4 Appendix D: Complex Numbers

Motivation: In $\mathbb{R}$, $x^2 - 1 = 0$ has two solutions, namely $-1, 1$. However, the almost identical equation $x^2 + 1 = 0$ has no solutions. This means that the reals “leave something to be desired.” In response, we introduce the imaginary unit $i$, which has the property $i^2 = -1$.

**Definition 0.15.** A *complex number* is an expression of the form $z = a + bi$ with $a, b \in \mathbb{R}$. Sum and product are defined by

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

and

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

**Remark 0.16.** Memorize the multiplication by multiplying out as one would do naively, and then use $i^2 = -1$. Do some examples!

**Theorem 0.17.** The complex numbers with sum and multiplication as above form a field.

*Proof.* This just involves tedious checking of all the properties—you should try a few yourself at home. \qed

**Remark 0.18.** The multiplicative inverse of $z = a + bi$ is

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

**Definition 0.19.** The complex conjugate of $z = a + bi$ is $\bar{z} = a - bi$.

**Proposition 0.20.**

1. $\bar{\bar{z}} = z$

2. $\bar{z} + w = \bar{\bar{z}} + \bar{w}$

3. $\bar{zw} = \bar{z} \cdot \bar{w}$

4. $\bar{\bar{z}} = \frac{z}{\bar{w}}$
Remark 0.21. It is now clear that there is a bijection $\mathbb{C} \to \mathbb{R}^2$ via $a + bi \mapsto (a, b)$. By Pythagoras' Theorem, the length of a straight line from the origin to the point $(a, b)$ is $\sqrt{a^2 + b^2}$.

Definition 0.22. The absolute value (or modulus) of $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}$.

Remark 0.23. We have

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

Thus,

$$|z| = \sqrt{z\bar{z}}.$$

Properties 0.24. 

i. $|zw| = |z||w|$

ii. $\frac{|z|}{|w|}$

iii. $|z + w| \leq |z| + |w|$

Theorem 0.25 (Fundamental Theorem of Algebra). Let $p(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ be a complex polynomial (i.e., $a_i \in \mathbb{C}$). Then $\exists z_0 \in \mathbb{C} : p(z_0) = 0$.

Proof. No proof is given here. This is a comparatively hard theorem to prove.

Corollary 0.26. For $p$ as above, $\exists r_1, \ldots, r_n \in \mathbb{C}$ such that

$$p(z) = a_n(z - r_1) \ldots (z - r_n).$$

Proof. Long division!

Remark 0.27. The formula often taught in high school to solve quadratic equations still works. For example, to solve $x^2 - 2x + 5 = 0$, write $x = -\frac{-2}{2} \pm \sqrt{1 - 5} = 1 \pm \sqrt{-4} = 1 \pm \sqrt{4(-1)} = 1 \pm 2\sqrt{-1} = 1 \pm 2i$.

1 Vector spaces

1.1 Introduction

Geometrically, a vector in, say, $\mathbb{R}^2$, is the datum of a direction and a magnitude. Thus, it can be represented by an arrow which points in the given
direction and has the given length. Two vector can be added using the parallelogram rule (see the textbook for some nice pictures explaining this).

Physically, the vectors may, e.g., represent forces that are exerted on an object. The result of the addition is the resulting net force that the object experiences when the original two forces are applied.

Algebraically, when \( v = (a_1, a_2) \) and \( w = (b_1, b_2) \), then \( v + w = (a_1 + b_1, a_2 + b_2) \). Scalar multiplication is defined via \( t(a_1, a_2) = (ta_1, ta_2) \).

**Definition 1.1.** The (non-zero) vectors \( v \) and \( w \) are parallel if and only if \( \exists t \in \mathbb{R} : tv = w \).

A vector can be interpreted as the displacement vector between its start and end point. If the start point is \((x_1, x_2)\) and the end point is \((y_1, y_2)\), then the displacement vector is \((y_1 - x_1, y_2 - x_2)\).

**Definition 1.2.** The line through the points \( A = (x_1, x_2) \) and \( B = (y_1, y_2) \) is
\[
\{(x_1, x_2) + t(y_1 - x_1, y_2 - x_2) : t \in \mathbb{R}\}.
\]

**Definition 1.3.** The line through the points \( A = (x_1, x_2, x_3) \) and \( B = (y_1, y_2, y_3) \) is
\[
\{(x_1, x_2, x_3) + t(y_1 - x_1, y_2 - x_2, y_3 - x_3) : t \in \mathbb{R}\}.
\]

**Definition 1.4.** The plane through the points \( A = (x_1, x_2, x_3) \), \( B = (y_1, y_2, y_3) \) and \( C = (z_1, z_2, z_3) \) (not all three on a line) is
\[
\{(x_1, x_2, x_3) + s(y_1 - x_1, y_2 - x_2, y_3 - x_3) + t(z_1 - x_1, z_2 - x_2, z_3 - x_3) : s, t \in \mathbb{R}\}.
\]

**Example 1.5.**

i. The line through \((1, 1, 2)\) and \((0, 3, -1)\) is
\[
\{(1, 1, 2) + t(-1, 2, -3) : t \in \mathbb{R}\}.
\]

ii. The plane through the points \( A = (1, 0, -1) \), \( B = (0, 1, 2) \) and \( C = (1, 1, 0) \) is
\[
\{(1, 0, -1) + s(-1, 1, 3) + t(0, 1, 1) : s, t \in \mathbb{R}\}.
\]

Now, observe that vector addition and scalar multiplication satisfy certain laws, e.g., \( v + w = w + v \), \( 1 \cdot v = v \), \((ab)v = a(bv)\). In Section 1.2, we will distill these obvious properties into an abstract definition.
Quiz 1.

1. (5 points) Let $\mathbb{R}$ be the set of real numbers. Define a relation $R$ on $\mathbb{R}$ by $(x, y) \in R$ if and only if $x - y$ is an integer. Prove that $R$ is an equivalence relation.

2. Let the function $f : \mathbb{Z} \to \mathbb{Z}$ be defined by

   $$f(x) = \begin{cases} 
   2x & \text{if } x \text{ is even} \\
   3x + 1 & \text{if } x \text{ is odd}
   \end{cases}$$

   i. (2.5 points) Is $f$ injective? Prove your answer.

   ii. (2.5 points) Is $f$ surjective? Prove your answer.

Answer to 1.

i. Reflexivity. Let $x \in \mathbb{R}$. Then $x - x = 0 \in \mathbb{Z}$.

ii. Symmetry. Let $(x, y) \in R$. Then there exists an integer $k$ such that $x - y = k$. After multiplying both sides by $-1$, we obtain $y - x = -k \in \mathbb{Z}$, which implies $(y, x) \in R$.

iii. Transitivity. Let $(x, y), (y, z) \in R$. Then there exist integer $k, \ell$ such that $x - y = k$ and $y - z = \ell$. Adding the two equations yields $x - z = k + \ell \in \mathbb{Z}$, which implies $(x, z) \in R$.

Answer to 2.

i. The function $f$ is not injective, because $f(2) = 4 = f(1)$.

ii. The function $f$ is not surjective, because there are no odd numbers in its Range.

1.2 Vector Spaces

Definition 1.6. A vector space (or linear space) $V$ over a field $F$ (think $F = \mathbb{R}$, or $\mathbb{C}$) is a set with a binary operation denoted “+” and a second map $\cdot : F \times V \to V$ such that

   i. $\forall x, y \in V : x + y = y + x$
ii. \( \forall x, y, z \in V : (x + y) + z = x + (y + z) \)

iii. \( \exists 0 \in V : \forall x \in V : x + 0 = x \)

iv. \( \forall x \in V \exists y \in V : x + y = 0 \)

v. \( \forall x \in V : 1x = x \), where 1 is the neutral element of multiplication in \( F \)

vi. \( \forall a, b \in F \forall x \in V : (ab)x = a(bx) \)

vii. \( \forall a \in F \forall x, y \in V : a(x + y) = ax + ay \)

viii. \( \forall a, b \in F \forall x \in V : (a + b)x = ax + bx \)

**Definition 1.7.** The elements of \( F \) are called *scalars*. The elements of \( V \) are called *vectors*. Because of item ii above, sums like \( x + y + z + w \) are well-defined.

**Remark 1.8.** To simplify typing, we will usually not adorn vectors with an arrow, i.e., we will write \( x \) instead of \( \vec{x} \) and 0 instead of \( \vec{0} \). Note that the neutral element of addition in the field is also denoted with 0, but it should always be clear from the context what is meant.

**Example 1.9.**

i. (THE example, see later section on isomorphisms) Take a field \( F \). (We will mostly just take \( \mathbb{R} \), or perhaps \( \mathbb{C} \).) An \( n \)-tuple is \( (a_1, \ldots, a_n) \), where \( a_1, \ldots, a_n \in F \). Note that \( \{n\text{-tuples}\} \cong F^n \) naturally. Define \( (a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) \). Also, \( c(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n) \) for \( c \in F \).

ii. Mat\(_{m,n}(F)\) is a vector space with componentwise addition and scalar multiplication

The following examples of vector spaces are substantially different from the examples above. They are “infinite dimensional,” more about that later.

**Example 1.10.**

i. Let \( S \) be a set of real numbers. Let \( F \) be the set of all real-valued functions on \( S \). Then \( F \) is a vector space (over \( \mathbb{R} \)) with the usual addition and scalar multiplication of real-valued functions.

ii. Let \( S \) now be an interval of reals. Consider in \( F \) only those functions that are continuous. This is also a vector space (use the summation theorem for continuous functions from calculus)

iii. Consider in \( F \) only those functions that are differentiable. This is also a vector space (use the summation theorem for differentiable functions from calculus)
iv. Assume that $x_0 \in S$. Then \( \{ f : S \to \mathbb{R} \mid f(x_0) = 0 \} \) is a vector space. (check it!). \( \{ f : S \to \mathbb{R} \mid f(x_0) = 1 \} \) is not!