Contents

I Introduction

In this introductive part of the thesis, we will explain the aims of this work and make a few general comments.

I.1 Aims of the thesis

The main aim of the thesis is to present, in a detailed, complete, rigorous and comparative way, the construction of Dedekind's and Cantor's model of reals numbers, starting from Peano axioms for the natural numbers, with particular attention to:

1. Use of the theory of limits (especially in Dedekind's approach)
2. Use of Axiom of Choice (AC), and its weaker denumerable form (Axiom of Countable Choice (CC)) and, more in general, the role of these principles in theorems of elementary Analysis
3. Comparison between these "constructive approaches" and the "direct axiomatic approach" to $\mathbb{R}$

I.2 Comments and historic reference frame

We apologize with our English readers, but the following section will be in Italian.

Commenti

Negli anni '70 i testi di Analisi, vedi Zwirner [Zv1] o Scorza-Dragoni [SD1], seguivano essenzialmente l'approccio costruttivo alla Dedekind dei numeri reali. L'esposizione di tale approccio presentava, peró, dei limiti. Le conoscenze preliminari di base da cui partire non si delineavano efficacemente o si davano per acquisite nozioni elementari, ma non banali, quali la conoscenza delle proprità aritmetiche dei naturali.
Come esporremo più nel dettaglio successivamente nella parte storica di riferimento, nei testi universitari l'approccio assiomatico diretto ai reali, più rigoroso e astratto, si è graduatamente sostituito a quello costruttivo, vedi Rudin [Ru1] o Giusti [Gi1].
Questa tesi ha voluto riproporre nel dettaglio l'approccio costruttivo ai reali, ripercorrendo formalmente il processo storico di "Aritmetizzazione dell'Analisi", che illustreremo più avanti, giudicando l'assiomatizzazione di Peano per i naturali, il giusto punto di partenza per un approccio costruttivo, astratto, rigoroso e autocontenuto. Un approccio che a nostro parere fornisce un contributo importante all'apprendimento "vero" della natura astratta della retta e della proprietà di continuità dei reali, oltre che un nesso chiave fra la didattica proposta dai primi corsi di Analisi e le relazioni con le tematiche dei primi corsi di Algebra e la Geometria.
Una motivazione che ha dato vita a questo lavoro è la mancanza, se non in testi più avanzati e dedicati quali il Mendelson [Me1], della costruzione dettagliata, "step by step", dei reali. Parziali esposizioni si possono, invece in testi di Analisi anii '70, come già detto

o su testi di Algebra ([PC1], [Fo1] o [Hn1]).

Proprio la chiara componente algebrica che caratterizza l'approccio costruttivo ai reali, ha suggerito una particolare attenzione, specialmente nella versione di Dedekind, a quanta teoria dei limiti occorresse.
Giusti nel testo [Gi2] asserisce che: *la costruzione dei reali secondo Dedekind presuppone solamente la conoscenza delle proprietà fondamentali dei numeri razionali.* Come vedremo non possiamo che condividere la sua teoria, ma la risposta al nostro quesito non sarà del tutto negativa.
Più precisamente è la proprietà Archimedea dei razionali il requisito essenziale che entra in gioco nella cotruzione alla Dedekind. Dimostrando questa proprietà, ci si accorge che il punto chiave è conferire ai naturali la qualità di sottoinsieme illimitato (dato un numero razionale positivo esiste sempre un naturale maggiore di esso), che riformulata in termine di limite: $\lim_{n\to\infty} n = \infty$.
Come si vedrà nella Sezione 1.3, il nostro approccio sarà ancora più attinente all'Analisi, e verranno usate risultati più marcatamente di natura analitica, dell'approccio standard.

Un secondo quesito di indagine è l'occorrenza dell'Assioma di Scelta (AC) e della sua formulazione numerabile (CC), sia nella costruzione dei reali, sia nei teoremi fondamtali dell'Analisi elementare.
Formulazioni standard di tali assiomi sono:

AC: *Data una qualsiasi collezione V non vuota di sottoinsiemi non vuoti di un insieme X, esiste una funzione $f : V \longrightarrow X$ tale che per ogni C elemento di V, $f(C) \in C$*

CC: *Data una collezione V numerabile di sottoinsiemi non vuoti di un insieme X, esiste una funzione $f : V \longrightarrow X$ tale che per ogni C elemento di V, $f(C) \in C$*

Rileggendo CC in formule, si traduce nel seguente modo:
CC: $\{ E_n \}_{n\in\mathbb{N}} \subseteq \mathcal{P}(X)^1 - \{\emptyset\} \implies \exists \{ e_n \}_{n\in\mathbb{N}} \mid e_n \in E_n \ \forall n \in \mathbb{N}$
Si noti come, in questa lettura, CC appaia "così ovvio" e naturale che a fatica ci si rende conto di usare un assunzione in più, di non poterlo provare per Induzione.

Come vedremo AC e CC non intervengono nella costruzione dei modelli di Cantor e Dedekind per i numeri reali.
Viceversa sono diversi i risultati principali di un corso di Analisi 1, quali il teorema dell'unione numerabile (Countable Union Theorem (CUT)), il teorema ponte di Heine-Cantor, il teorema di massimo e minimo di Weierstrass, che necessitano di CC (anche se tale fatto, di solito, non viene menzionato nei libri di testo).
Dall'altra parte, AC sembra non intervenire mai nel programma didattico di un primo corso di Analisi. Per trovare una sua applicazione dobbiamo cercare fra le funzioni

[1] $\mathcal{P}(X)$ insieme delle parti di X, ovvero l'insieme di tutti i sottoinsiemi di X

patologiche (quali le “ugly functions”, ovvero funzioni definite globalmente su $\mathbb{R}$, lineari, identità sui razionali ma non su tutti i reali).

Breve introduzione storica

In questa sezione proporremmo il percorso storico che ha condotto alla ricerca sui fondamenti dei reali.
Le conoscenze attuali della natura dei numeri reali, sono uno dei risultati di un processo intellettuale lungo e complesso che coinvolse l’intera Matematica, che da mero strumento di modellizzazione della realtà, si è evoluta verso l’astratto, con “l’introspezione” delle sue nozioni più basilari, le sue fondamenta concettuali, verso l’impostazione rigorosa che ne caratterizza la logica deduttiva e il suo linguaggio autocontenuto.

It is undeniable that some of the best inspirations in mathematics - in those parts of it which are as pure mathematics as one can image - have come from the natural sciences... J.Von Neumann [2]

In questo passo J.Von Neumann $(1903 - 1957)$ illustra un lato importante della Matematica, la chiara contraddizione fra due facce della stessa medaglia e cioè il conflitto tra Matematica intesa come strumento di indagine dell’uomo sulla natura e Matematica intesa come linguaggio astratto. In questo passo Von Neumann riconosce il fondamentale uso di un processo induttivo che da osservazioni e intuizioni, cerca di risalire ad un concetto generale. Questo procedimento si inverte inevitabilmente all’interno del linguaggio matematico. Di fatti quest’ultimo deve seguire necessariamente la logica deduttiva che lo caratterizza.
La ricerca dei Fondamenti in Matematica è un percorso che si è sviluppato su questo contrasto, affermando l’autonomia del linguaggio dall’intuizione. Un percorso volto a stabilire un maggior rigore concettuale delle nozioni basilari, primitive tentando di fondarle in un contesto astratto.

In questa prima parte dell’introduzione ripercorreremo le principali tappe di questo percorso e cioè:

Il primo prototipo di impostazione assiomatica (Euclide, $IV - III$ sec. a.C.);

“l’era del Rigore” del XVIII secolo che sfociò nella nascita delle Geometrie non Euclidee e nell’Aritmetizzazione dell’Analisi;

l’acceso dibattito tra i programmi per i Fondamenti e il “successo” del programma formalista hilbertiano;

Infine analizzeremo come questo percorso abbia influenzato la didattica e quanto la didattica riporti di questo percorso sulle basi concettuali della Matematica.

[2] [VN1]

I principi base della Matematica nella tradizione Euclidea

Gli “Elementi” di Euclide (circa 300 a.C.) sono forse il trattato più importante della Matematica greca. L'impostazione assiomatica di Euclide rappresenta il primo grande passo verso l'astrazione della Geometria; la caratterizzazione deduttiva dell'impostazione matematica si manifesta in tutta la sua bellezza e funzionalità. Euclide apre il trattato con una serie di definizioni per gli enti fondamentali della Geometria (punto, retta, piano), cinque postulati come regole governanti questi enti e cinque nozioni comuni che postulano i principi logici quali uguaglianza e relazione fra il tutto e le parti. Ovviamente il linguaggio è antico ma questo tipo di impostazione rigorosa influenzerà per sempre il modo di fare Matematica. Nel trattato, composto da tredici volumi, sono presenti anche postulati per l'Aritmetica volti a definire il concetto di numero e quello di proporzionalità. Le ultime definizioni aprono il volume XI dove Euclide definisce i solidi.
La fama degli elementi non fu solo di carattere elogiativo: fra i cinque postulati introdotti nel primo tomo, il V creò da subito diffidenza. A differenza degli altri postulati, il V, o postulato delle parallele, aveva un carattere diverso in quanto conivolgeva indirettamente il concetto di infinità del piano. Questa inquetante presenza contaminava l'intuitività con cui erano stati postulati i restanti, e aveva portato a credere che il V postulato si potesse dedurre come teorema.
I secolari fallimenti si rivelarono conformi alla scoperta che, in effetti, il V postulato era indipendente dagli altri quattro. All'alba del XIX secolo la nascita di modelli di Geometrie non Euclide, portarono la Geometria ad un ulteriore passo verso l'astratto, dimostrando che il postulato delle parallele vincolava l'edificio creato ad essere una rappresentazione della realtà nel senso più intuitivo di essa. Nelle Geometrie non Euclidee modelli più “bizzarri” di punto, retta e piano avrebbero comunque soddisfatto i primi quattro postulati pur rappresentando uno spazio diverso. Lo spazio euclideo aveva così perso la sua assolutezza divenendo una delle tante realizzazioni di un concetto più astratto: lo spazio.
Le vicende della branca madre della Matematica avevano mostrato l'esigenza di un linguaggio matematico più rigoroso e non necessariamente lontano fondato su nozioni intuitive.
L'eco delle scoperte di Geometrie non Euclidee influenzò enormemente l'evolversi della Matematica del XIX secolo e anche il calcolo infinitesimale, così intimamente legato alla fisica e alla meccanica, iniziò un processo analogo di astrazione.

L'Aritmetizzazione dell'Analisi

Agli inizi del XVIII secolo si accese la contesa tra G.Leibniz $(1646 - 1716)$ e I.Newton $(1642 - 1727)$ su chi per primo avesse introdotto il concetto di derivata. Fu uno dei più accesi dibattiti nella storia della Matematica che prese, a volte, toni aspri.
Mentre Leibniz percepiva le grandezze come composizioni di parti infinitesime, il rivale inglese le percepiva come grandezze fluenti impostando il discorso tramite concetti fisici quali spazio, tempo e variazione.

Benchè questi nuovi metodi permettessero la risoluzione di una quantità di problemi prima inimmaginabile, agguerriti critici, fra cui il vescovo Berkeley (1685 1753), denunciavano la dubbia correttezza con cui questi problemi venivano formulati: l'impostazione del problema prevedeva l'uso di queste quantità infinitesime non nulle che al momento di accedere al risultato venivanmo poste uguali a zero ("fantasmi di quantità sparite"[3]). La metafisica che parea avvolgere queste misteriose quantità, era in realtà sintomo della necessità di riformulare il calcolo infinitesimale in maniera più rigorosa.
Nel preparare le sue lezioni alla scuola politecnica di Parigi A.L.Cauchy (1789 − 1857) iniziò un lavoro di rigorizzazione dell'Analisi e basandosi sull'opera di J.B.D'Alembert (1717 − 1783) introdusse la nozione di limite.
Lo storico della Matematica G.Israel, nel suo articolo [Is1], sottolinea come questo rigore non è pura e mera astrazione e neanche una miglioria della convezione stilistica di formulazione, ma piuttosto un riordinamento necessario del linguaggio matematico verso una sempre maggiore autonomia da procedimenti di analogia o da accostamenti intuitivi; intendiamo con ciò evidenziare come si cercasse un'astrazione rimanendo sempre ancorati ad un problema concreto e reale.
Il lavoro di Cauchy fu successivamente completato da K.Weierstrass (1815 − 1897) che introdusse la definizione odierna di limite e di continuità.
La trattazione rigorosa aveva coinvolto i concetti chiave del calcolo, ma si avvertiva la necessità di una trattazione altrettanto rigorosa dei numeri reali sia del concetto di numero irrazionale sia nell'illustrazione della loro fondamentale proprietà strutturale: la continuità. Come le Geometrie non Euclidee avevano mostrato che la nozione di spazio non era necessariamente quella più intuitiva, il movimento del rigore nell'analisi sollevava la necessità di rivisitare un concetto fin ad allora scontato: che la linea retta non avesse buchi.

Questa necessità trovó le definitive risposte verso la fine del XIX secolo con G.Cantor (1845 − 1918) e R.Dedekind (1831 − 1916).
Cosa sono i numeri reali? Come possiamo giustificare la loro esistenza?
Come già detto e come illustreremo nel secondo capitolo della tesi, furono Cantor e Dedekind che, indipendentemente, cominciarono a rispondere, "riducendo" l'insieme dei reali da quello dei razionali ovvero costruendo un modello dei reali basandosi su l'esistenza dell'insieme dei numeri razionali. Seppur pubblicate nello stesso anno (1872) le due risposte sono diverse.
Quella di Cantor identifica un numero reale con una classe di equivalenza di successioni di Cauchy in $\mathbb{Q}$. Questa costruzione non fu originale del tedesco, ma proseguiva le idee di B.Bolzano e Weirstrass[4] già sviluppate alla metà del secolo.
Dall'altra parte Dedekind, uno tra i più famosi specialisti di teoria dei numeri dell'epoca[5] si accostò al problema in maniera diversa, basando i suoi sforzi sul concetto di insieme

[3][MG1] pg.65
[4][Bo1] pg 642 − 643
[5][Frs1] pg 249

continuo ovvero privo di buchi. Dedekind identifica un numero reale con l'unico punto di sezione di una linea continua focalizzando così la vera caratteristica dei reali. La costruzione vera e propria identifica un numero reale con un particolare sottoinsieme non vuto di $\mathbb{Q}$, detto taglio, e il suo metodo usa esclusivamente la proprietà archimedea del campo dei razionali e le sue proprietà algebriche.
A questo punto modelli dei reali erano stati dedotti dai razionali e, come mostreremo nel primo capitolo della tesi, in ultima analisi dai naturali, terminando questo processo comunemente chiamato "Aritmetizzazione dell'Analisi".

I naturali di Cantor, i postulati dell'Aritmetica e l'assiomatica formale di Hilbert

Sebbene molti considerassero l'Aritmetizzazione dell'Analisi un traguardo soddisfacente, lo sviluppo della Teoria "naive" degli Insiemi di Cantor ripromosse il dibattito all'interno della comunità matematica.
Cantor proponeva la deduzione di un modello dei naturali, sulla base della nozione di insieme. Tramite la nozione di numero cardinale, Cantor aveva stabilito una relazione di equivalenza (l'equinumerosità ovvero l'esistenza di una biezione) tra gli insiemi (definiti come una generiche collezioni di elementi). Il relativo insieme quoziente, tramite il principio del Buon Ordinamento (WO), ne risultava, appunto, ben ordinato. Infine si identifica l'insieme dei naturali, come il minimo tra i cardinali non finiti.
Dalla discussione sulla legittimità matematica della teoria di Cantor, si generó un dibattito profondo tra diverse scuole, dibattito che coinvolse, in realtà, la natura della Matematica stessa.

L'alternativa all'approccio alla Cantor, fu la caratterizzazione assiomatica dei naturali, fornita indipendentemente da Dedekind nel 1888 e da G.Peano ($1858 - 1932$) nel 1889.
La caratterizzazione di Dedekind (ben illustrata da Ferreirós nel suo [Frs1]), utilizzando i concetti di insieme semplicemente infinito, mappe e catene, concentrò la sua attenzione nel giustificare più l'uso delle definizioni per recursione sui naturali, piuttosto che nell'illustrare a fondo le loro proprietà aritmetiche e strutturali.
Seppur simili, la caratterizzazione fornita da Peano risultò più convincente, mentre quella del tedesco, anche a causa di un simbolismo poco rigoroso, si fece apprezzare da pochi logici piuttosto che dalla comunità matematica, come invece ci si aspettava[6].
Il modello di approccio assiomatico di Peano ai numeri naturali è un classico esempio di assiomatizzazione formale. Questo nuovo concetto di astrazione, si sviluppó organicamente in un nuovo programma per i Fondamenti (detto programma formalista), dove ,in aggiunta, coinvogliarono i delusi dal programma logicista, reduci dal sostanziale fallimento di fondare la teoria di Cantor nella logica.
Il più grande esponente del programma formalista fu D.Hilbert (1862 1943). Hilbert fu un personaggio molto carismatico e trascinatore, altamente stimato e conosciuto. Il suo celebre discorso al II congresso Internazionale dei matematici di Parigi nel 1900, illustrò una lista di ventitrè problemi insoluti, che a suo parere meritavano maggiore attenzione

[6][Frs1] pg 248

dall'intero mondo matematico. Nel secondo probleme Hilbert illustrava il programma formalista al problema dei Fondamenti dei reali. Hilbert incitava a dare una prova della consistenza degli assiomi dell'Aritmetica, basata su un impostazione assiomatica della Teoria "naive" degli Insiemi di Cantor, analogamente a come aveva fatto, nel 1899, per la Geometria nei suoi "Grundlagen der Geometrie".
La svolta concettuale dell'approccio formale è essenzialmente la seguente: la definizione descrittiva (come quelle scelte da Euclide negli Elementi) degli oggetti presuppone inequivocabilmente l'uso dell'intuizione nella loro formulazione. Viceversa si propone uno svotamento del contenuto descrittivo mostrando in che cosa consista realmente una teoria assiomatica. Proponiamo una citazione dall'articolo di Israel [Is1] che a nostro parere illustra questo ultimo concetto:
una teoria assiomatica consiste in un complesso di teoremi, ricavati per la sola via logico-deduttiva e descriventi le proprietà di un ente matematico astratto definito mediante assiomi. Assiomi e teoremi sono i soli elementi significativi della teoria il cui contenuto "concreto" è irrivelevante rispetto all'armatura logica.
Come Peano non definisce nè uno nè numero, Hilbert non definisce nè punto nè piano nè retta (Hilbert scrisse che poteva sostituirli con sedia, tavolo e boccale di birra) dando un nuovo significato alla funzione dell'assioma. L'approccio assiomatico moderno quindi si distingue da quello che vediamo in Eudlide nella mancanza di definizioni; i concetti primitivi sono definiti implicitamente dai rapporti che li legano esplicitati dagli assiomi; l'assioma non definisce l'oggetto ma ne caratterizza le proprietà, non dice come è fatto ma dice ciò che fa, come si muove. La logica che giace alla base del formalismo hilbertiano propone quindi l'astrazione dagli oggetti alle formule, esortando l'abbandono dell'intuitivitá legata al comune senso di descrivere gli oggetti.

Nel 1931 K.Gödel ($1906 - 1978$) formulò il suo teorema di indecidibilità. Gödel mostró che un sistema sufficentemente grande di assiomi S (come quelli dell'Aritmetica) permette l'insorgere di proposizioni delle quali non si puó stabilire l'indipendenza da S, cioè proposizioni di cui non è provato si possa decidere nel sistema S, indecidibili appunto. Dunque la consistenza di un sistema di assiomi è improvabile all'interno di se stessa. Questo risultato inivetabilmente decretó il fallimento del programma hilbertiano e con questo l'intera ricerca dei Fondamenti ha mostrato i suoi limiti, condannando a interrogarsi sulla legittimità di una sua prosecuzione.

Riflessi sulla didattica

A questo punto, è ancor più legittimo interrogarsi su quanto la didattica, di un primo anno universitario, debba riportare dell'intero percorso. Quale l'approccio migliore ai numeri reali? Assiomatico o costruttivo? Costruttivo da che punto? É giusto illustrare ad uno studente un percorso che ha mostrato i limiti della Matematica? Quanto lo puó interessare o essergli di aiuto? Qual'e il giusto approccio all'Analisi?
Ad un livello universitario, come avviene per l'Algebra e per la Geometria, anche l'Analisi puó essere illustrata ad uno studente in modo rigoroso e tale qualità di approccio è possibile solo mediante la presentazione assiomatica diretta di $\mathbb{R}$. Tra i motivi a sostegno

di questa tesi, se ne possono riscontrare principalmente due.
La prima è che, proprio al livello di interesse ad uno studente, si può comprendere che presentare l'Analisi ad uno studente illustrando l'Aritmetizzazione dell'Analisi possa risultare noioso. Tutt'altro nell'approccio assiomatico: marcare che da poche proprietà date per assiomi si possono derivare tutte le altre, esalta il carattere logico deduttivo della Matematica come in un gioco di strategia.
La seconda, e credo il nostro lavoro in questa tesi lo abbia mostrato, è che solo dopo un'acquisita maturità matematica, si può apprezzare la costruzione dettagliata dei reali da un numero minimale di proprietà.

II Contents of the thesis

Contents

A brief survey of Set Theory and Logic

The thesis begins with this brief survey of set theory and logic notions, we need in this work. Further we give the main standard definitions on set theory that we use (relation, function, operation ...).

The thesis real body is divided in three parts.

Part 1: Chapter 1 and 2

This is the "constructive" part of this work. We prove the following result:

given a Peano System (the triple $(\mathbb{N}, 1, \sigma)$ with Peano axioms) there exists a model of a Complete Ordered Field (COF), namely the quadruple $\left(\mathbb{R}, +_{\mathbb{R}}, *_{\mathbb{R}}, \leq_{\mathbb{R}}\right)$ con 15 algebraic properties and the least upper bound property

Chapter 1

In this Chapter we prove the following result:
Given a Peano Systems $(\mathbb{N}, 1, \sigma)$, there exists a model of an Ordered Field (OF), namely the quadruple $\left(\mathbb{Q}, +_{\mathbb{Q}}, *_{\mathbb{Q}}, \leq_{\mathbb{Q}}\right)$ with 15 algebraic properties, which contains a copy of a Peano System.

As wished, we divided this Chapter into 3 sections.

Section 1.1

The Section starts with: definition of a Peano System; definition of a Peano Ring (the quadruple $\left(\mathbb{N}, +_{\mathbb{N}}, *_{\mathbb{N}}, \leq_{\mathbb{N}}\right)$ with 10 algebraic properties); aim: Given a Peano System we could define two binary inner operations $+_{\mathbb{N}}$, $*_{\mathbb{N}}$ on $\mathbb{N}$, an order relation $\leq_{\mathbb{N}}$ on $\mathbb{N}$ such that

$\left(\mathbb{N}, +_{\mathbb{N}}, *_{\mathbb{N}}, \leq_{\mathbb{N}}\right)$ is a model of a Peano Ring.
First results of this Section (the most significative and meaningful one of the first part) Induction Theorem, to prove by induction, and Recursion Theorem, to justify definition by recursion. The latter one is the Section's hardest and the most fundamental result. In Final two subsections: Isomorphism between Peano Systems and Induction's extension (Strong induction and Minimum principle) of a Peano Ring.

Section 1.2

The Section starts with: definition of an Ordered Integrity Domain (OID), namely the quadruple $\left(\mathbb{Z}, +_{\mathbb{Z}}, *_{\mathbb{Z}}, \leq_{\mathbb{Z}}\right)$ with 14 algebraic properties; aim: Given a Peano Ring there exists a model of an OID which contains a copy of a Peano Ring.

Section 1.3

The Section's start is definition of an OF and its aim: given an OID there exists a model of an OF which contains a copy of on OID. Further, after immersion of OID, we prove Archimedean property of the rational. In final definitions and main properties of rational powers (to prepare Dedekind's construction of the reals).

Chapter 2

Chapter 2 completes the final construction of the real numbers. This Chapter is divided in two independent sections, in each of them we prove the same result: given an OF There exists a model of a COF which contains a copy of an OF

Section 2.1 Construction via Dedekind cuts

Section 2.1 Construction via rational Cauchy sequences

Part 2: Chapter 3

This part represent the "first part's other way round".

Section 3.1

We approach directly to a COF $\big(\mathcal{R}, +_{\mathcal{R}}, *_{\mathcal{R}}, \leq_{\mathcal{R}}\big)$, with its 16 properties. Given a COF, the following sections explore its special subsets and some of its important properties.

Section 3.2

The Section starts showing existence of a proper subset $\mathbb{N}_{\mathcal{R}}$ such that, defining a function σ as $\sigma(x) := (x+1)_{|\mathbb{N}_{\mathcal{R}}}$, $(\mathbb{N}_{\mathcal{R}}, 1, \sigma)$ is a copy of a Peano System. Later on we show as $\mathbb{N}_{\mathcal{R}}$ is a copy of a Peano Ring, restricting to $\mathbb{N}_{\mathcal{R}}$ the binary inner operations $(+, *)$ and the order relation $(\leq)$. Successively we show discreteness of $\mathbb{N}_{\mathcal{R}}$ and its closure for subtraction $n - m$ for $n > m$.
Furthermore special proper subsets $\mathbb{Z}_{\mathcal{R}}$ and $\mathbb{Q}_{\mathcal{R}}$ is showed be copies of, respectively, OID and OF, restricting to them the binary inner operations $(+, *)$ and the order relation $(\leq)$.
The Section ends showing Archimedean property of $\mathcal{R}$ and density of $\mathbb{Q}_{\mathcal{R}}$ in $\mathcal{R}$

Section 3.3

Finite and infinite subsets of a COF $\mathcal{R}$. Sequences in $\mathcal{R}$ and definition of bounded, monotone, convergent and Cauchy sequence.

Section 3.4

Convergence of Cauchy sequences in $\mathcal{R}$

Section 3.5

Theorem of Isomorphism between two models of a COF

Part 3: Chapter 4

Axiom of Choice and elementary Analysis

In this Chapter we show basic Set Theory results and some of elementary Analysis main theorems, in which necessity of infinite arbitrary choices compares, when it is indispensable and when it could be avoided.

Section 4.I General remarks on AC

Section 4.1

Countable Union Theorem (Cantor 1872). Historically it is one of the foremost example of necessity of Axiom of Countable Choice (CC).

Section 4.2

Equivalence between classic definition for infinite subsets and Dedekind definition for infinite subsets, needs CC

Section 4.3

This Section is one of the most significative part of Chapter 4.
We consider $\mathbb{R}$ with its natural topology given by $|\cdot|_{\mathbb{R}}$. After we show how, equivalence between "static" and "dynamic" definition of limit point (and hence definitions of closed sets), needs CC.
We present two proofs of the Bolzano-Weierstrass theorem.The first one, classic, uses CC; the second one, quite similar to the first, avoids it.

Section 4.4

Continuous functions. We propose an example of a use of CC, in elementary Analysis, which does not concern equivalence of definitions: Weierstrass maximum and minimum theorem.

Section 4.5

Some of the most known equivalent principles of AC: Cantor Well-Ordering principle, Zorn Lemma, Hausdorff Maximality Principle

Section 4.6

A powerful pathological application of AC: Existence of an "ugly function" on the reals, namely a linear function on the reals, but non continuous on them.

Characteristic contents

We conclude this introduction underlying some particular choices we have made in our exposition:

- In Chapter 1, conclusion, in both of Sections 1.2 and 1.3, is a remark on arbitrary choices in definitions of operations and order relation in $\mathbb{Z}$ and $\mathbb{Q}$. In each of these sections, models more complex structure E is identified with a quotient set on the cartesian product by given structure e with itself. Order relation $\leq_E$ and operations $+_E$, $*_E$ is defined on equivalence class, as consequence of "well posed" relations on $e \times e$.
  In each of these two remarks, we show a method to choose a determinate representant in $e \times e$ for any element of E., preluding how one could define order relation and operations without selecting arbitrary representant

- Section 2.1, construction via Dedekind cuts. As we told before in section I.1,

Archimedean property of $\mathbb{Q}$ has a fundamental role in this method. Its occurrence appears proving that, a cut ξ_α, previously defined in function of a given positive cut α, is the inverse of α, namely α^{-1}
In this thesis we handle mentioned passage through properties of small positive rational powers. It is specified how this method, do not avoid Archimedean property of the rational numbers, since the latter is required in mentioned rational powers properties owns proofs.

- In Section 3.1, the subset $\mathbb{N}_{\mathcal{R}}$, Peano System copy's framework in un COF $\mathcal{R}$, is deduced by subsets having a particular property, named "property C". This property characterizes finite subset trough least upper bound property (named **Ded**) of $\mathcal{R}$. Appendix A explains, how use of **Ded** is not necessary.

Appendix A

Structures containing Peano Systems

Minimal characteristics for a structure to contained a copy of a Peano System as a proper subset. We generalize standard characterization of a Peano System as intersection of all inductive subsets. In an another point of view, this Appendix represents a Peano axioms's analysis, giving a method to find, in a structure, a subset which satisfies Induction property.

III Notations

- $\forall$, $\exists$ mean respectively "for all" and "exists"
- $|$ means "such that"
- ! means "unique"
- $\Longrightarrow$ means "then" or "hence"
- $\Longleftrightarrow$ means "if and only if"
- In each Chapter the following environments:

  Propositions, Corollaries, Theorems, Definitions, Lemmas, Immersion Theorems, Remarks, Notational remarks

  follow an independent numerations from each other

  Thus Definition $x.y$ indicates the y^{th} definition of Chapter x
- Some Theorems have two Formulation :thus by Formulation $x.y.1$ $(x.y.2)$ we denote the first(second) formulation of Theorem $x.y$
- $A \overset{\text{T}.x.y}{\Longrightarrow} B$ means "by Theorem $x.y$ $A \Longrightarrow B$"
- $A \overset{\text{T}.x.y}{=} B$ means "by Theorem $x.y$ $A = B$"
- $A \overset{\text{T}.x.y}{\Longleftrightarrow} B$ means "by Theorem $x.y$ $A \Longleftrightarrow B$"

  We use these notations as well as theorems also for definition, proposition, corollary which will be denoted respectively with D., P., C.
- More complex proofs need to be divided in steps or in points. So some steps or points will begins with a statement followed by ":". In these cases the rest of that point or step will be the proof of the initial statement

IV A brief survey of elements of Set Theory and Logic

In this thesis we use some elements of naive Set Theory and some elements of Logic, but we do not approach them rigorously. Readers who want to go into more depth in, naive or axiomatic, Set Theory and in Logic, they can see any text of Set Theory like, for example, text of G.Lolli [Lo1] and any text of Logic like, for example, text of J.R.Shoenfield [Sh1]

Sets

A set is a couple $(S, \in_S)$ where: S is a collection of elements and $\in_S$ is the membership relation on S

Sets $(S, \in_S)$ will be denoted as S and the membership relation $\in_S$ only with $\in$

There follows definitions of:

Subset Let S be a set

A subset of S is a sub-collection of some elements of the set S, and this collection could be all the set S

$A \subseteq S$ means that "A is a subset of S"

Proper Subset Let S be a set, $A \subseteq S$

$a \notin A$ means that "a is not an element of A"

$A \subset S$ means that "$A \subseteq S$ and exists $a \notin A$"

Equality

For every Set S, an equality relation $=_S$ between its elements is given.

$=_S$ has the following properties:

$$\begin{cases} \text{(Reflexivity)} \quad x =_S x \quad \forall\, x \in S \\ \text{(Substitutivity)} \quad \text{Let } x, y \in S \\ x =_S y \Longrightarrow F(x,z) =_S F(y,z) \quad \forall\, z \in S \quad \text{where } F \text{ is any formula in } S \end{cases}$$

(Substitutivity) guarantees us that, if two terms x, y are equal, we can replace x in any occurrence of y and viceversa

In any set S its equality relation $=_S$ will be denoted simply as $=$

There follow immediately the following results:

(Symmetry) $x = y \Longrightarrow y = x \quad \forall\, x, y \in S$

(Transitivity) $x = y,\ y = z \Longrightarrow x = z \quad \forall\, x, y, z \in S$

Elements of Set Theory

There follows elements of Set Theory we use in this work

Empty Set Let S be a set.

$\emptyset \subset S \quad | \quad \emptyset$ has no elements

Extensionality Let S, Z two sets

$S = Z \iff (x \in S \Leftrightarrow x \in Z)$

Comprehension Let S be a set and P be a predicate[7] on S

$I_P \subseteq S \quad | \quad x \in I_P \iff x \in S$ and $P(x)$ holds

Power Set Let S be a set

$\mathcal{P}(S)$ is the set of all the subset of S

$A \subseteq S \iff A \in \mathcal{P}(S)$

Union Let S a be set, $A \subseteq \mathcal{P}(S)$

$\cup_{a \in A}\, a \subseteq S \ | \ \cup_{a \in A}\ a := \{x \in S \mid \exists\, a \in A \mid x \in a\}$

Intersection Let S a be set, $A \subseteq \mathcal{P}(S)$

$\cap_{a \in A}\, a \subseteq S \ | \ \cap_{a \in A}\ a := \{x \in S \mid x \in a\ \forall\, a \in A\}$

$A, B \subseteq S$ are disjoint if and only if $A \cap B = \emptyset$

Difference Let S be a set, $A, B \subseteq S$

$A - B := \{x \in S \mid x \in A \text{ and } x \notin B\}$

Cartesian Product Let S_1, S_2 be sets

$S_1 \times S_2$ is the of all the ordered couples (s_1, s_2) where $s_1 \in S_1$, $s_2 \in S_2$.

For ordered couple we mean that if $s_1 \neq s_2$ then the couple $(s_1, s_2)$and the couple (s_2, s_1) are two different elements of $S_1 \times S_2$

Relation Let S a set

R is a Relation on $S \iff R \subseteq S \times S$

[7]By predicate we mean a statement which could be either true or false

Reflexive Relation R is reflexive on $S \iff (x,x) \in R, \quad \forall\, x \in S$

Symmetric Relation R is symmetric on S if and only if :

$(x,y) \in R \implies (y,x) \in R, \quad \forall\, x,y \in S$

Antisymmetric Relation R is antisymmetric on S if and only if:

$$\left.\begin{array}{l}(x,y) \in R\\ (y,x) \in R\end{array}\right\} \implies x = y, \quad \forall\, x,y \in S$$

Transitive Relation R is transitive on S if and only if :

$(x,y) \in R,\ (y,z) \in R \implies (x,z) \in R \quad \forall\, x,y,z \in S$

Total Relation R is total on S if and only if :

$\forall\, x,y \in S \qquad (x,y) \in R \quad \text{or} \quad (y,x) \in R$

Henceforth We use denote $s\,R\,z$ to denote $(s,z) \in R$

Partially Ordered Set Let S be a set and R be a relation on S

$$(S,R) \text{ is a Partially Ordered Set} \iff \begin{cases} R \text{ is reflexive on } S \\ R \text{ is antisymmetric on } S \\ R \text{ is transitive on } S \end{cases}$$

Ordered Set Let S be a set and R be a relation on S

$$(S,R) \text{ is a Partially Ordered Set} \iff \begin{cases} (S,R) \text{ is a Partially Ordered set} \\ R \text{ is Total on } S \end{cases}$$

Well-Ordered Set Let S be a set and R be a relation on S

$$(S,R) \text{ is a Well-Ordered Set} \iff \begin{cases} (S,R) \text{ is a partially ordered set} \\ \forall\, A \subseteq S,\ A \neq \emptyset \implies \exists a \in A \quad | \quad aRx \quad \forall\, x \in A \end{cases}$$

Equivalence Relation Let S be a set and R be a relation on S

$$R \text{ is an Equivalence Relation on } S \iff \begin{cases} R \text{ is reflexive on } S \\ R \text{ is symmetric on } S \\ R \text{ is transitive on } S \end{cases}$$

Equivalence Class Let S a set, R be an equivalence relation on S and $s \in S$

the Equivalence Class generated by s:

$[s]_R \subseteq S \ | \ [s]_R := \{x \in S \ | \ s\,R\,x\}$

Quotient Set Let S be a set and R be an equivalence relation on S

$\frac{S}{R}$ is the set of all the equivalence classes $[s]_R$:

$\frac{S}{R} := \{[s]_R \mid s \in S\}$

Function Let A, B be sets, $A, B \neq \emptyset$.

A function from A to B is a subset $f \subseteq A \times B$ verifying :

$\forall\,(a,b) \in f \quad$ if $\exists\, b_1 \in B \mid (a, b_1) \in f \implies b = b_1$

We use notation $f : A \longrightarrow B$ to denote a function f from A to B

We use notation $b = f(a)$ to denote $(a,b) \in f$

Injective Function $\quad f : A \longrightarrow B$ is injective if and only if:

$a_1 \neq a_2 \implies f(a_1) \neq f(a_2) \quad \forall\, a_1, a_2 \in A$

Surjective Function $\quad f : A \longrightarrow B$ is surjective if and only if:

$\forall\, b \in B \quad \exists\, a \in A \mid b = f(a)$

Bijective Function $\quad f : A \longrightarrow B$ is bijective if and only if:

f is injective and surjective

Image of a function Let $A, B \neq \emptyset$ and $f : A \longrightarrow B$.

$f(A) := \{b \in B \mid \exists\, a \in A \text{ with } b = f(a)\}$

Composition of functions Let $A, B, C \neq \emptyset$ and $f : A \longrightarrow B,\ \ g : B \longrightarrow C$.

$f \circ g := \{(a, g(b)) \in A \times C \mid a \in A,\ b = f(a)\}$

It is not difficult to prove that $f : A \longrightarrow C$

We denote $f \circ g\ (x)$ as $f(g(x)) \quad \forall\, x \in A$

Restriction of a function Let $A, B \neq \emptyset$ be sets and $f : A \longrightarrow B$.

$f(A) := \{b \in B \mid \exists\, a \in A \text{ with } b = f(a)\}$

Collection indexed by a set Let S, I sets, $I \neq \emptyset$

A collection V of subsets of $S\,(V \subseteq \mathcal{P}(S))$ is indexed by I if and only if exist $f : I \longrightarrow V$ bijective

We denote such as V as $\{V_i\}_{i \in I}$

- $\cup_{i \in I} V_i := \{x \in S \mid \exists\, i \in I \mid x \in V_i\}$
- $\cap_{i \in I} V_i := \{x \in S \mid \forall\, i \in I \mid x \in V_i\}$

Binary Inner Operation Let S be a set

A binary inner operation $\star$ on S is a function from $S \times S$ to S

We use notation $z = x \star y$ to denote $z = \star(x, y)$

Chapter 1

From Peano's Naturals to the Rationals

In this Chapter we start from an axiomatic definition of $\mathbb{N}$:

Exist a non-empty set $\mathbb{N}$, an injective and non surjective function σ from $\mathbb{N}$ to $\mathbb{N}$. Further no proper subsets of $\mathbb{N}$ satisfy a particular property. From these Axioms we will show the existence of a model of Rational numbers as we know them.

1.1 Peano Axioms and the Natural Numbers $\mathbb{N}$

Definition 1.1 (Peano Axioms)

$\big($a set $\mathbb{N}$, 1, $\sigma\big)$ is a Peano Sytem if and only if it satisfies the following properties:

(i) $1 \in \mathbb{N}$

(ii) σ is a function from $\mathbb{N}$ to $\mathbb{N}$

(iii) σ is injective

(iv) $1 \neq \sigma(n) \quad \forall n \in \mathbb{N}$

(v) $\forall A \subseteq \mathbb{N}$ which satisfies

- $1 \in A$
- If $n \in A \Longrightarrow \sigma(n) \in A$

$\Longrightarrow A = \mathbb{N}$

Definition 1.2

$\big($ a set $\mathbb{N}$, $+_{\mathbb{N}}$, $*_{\mathbb{N}}$, $\leq_{\mathbb{N}}$ $\big)$ is a Peano Ring if and only if it satisfies the following properties:

(s_1) $n +_{\mathbb{N}} k = k +_{\mathbb{N}} n \qquad \forall\, n, s \in \mathbb{N}$

(s_2) $(n +_{\mathbb{N}} k) +_{\mathbb{N}} m = n +_{\mathbb{N}} (k +_{\mathbb{N}} m) \qquad \forall\, n, k, m \in \mathbb{N}$

(p_1) $n *_{\mathbb{N}} k = k *_{\mathbb{N}} n \qquad \forall\, n, k \in \mathbb{N}$

(p_2) $n *_{\mathbb{N}} (k *_{\mathbb{N}} m) = (n *_{\mathbb{N}} k) *_{\mathbb{N}} m \qquad \forall\, n, k, m \in \mathbb{N}$

(p_3) $\exists\ 1 \in \mathbb{N} \ \mid n *_{\mathbb{N}} 1 = n \qquad \forall\, n \in \mathbb{N}$

(sp) $n *_{\mathbb{N}} (k +_{\mathbb{N}} m) = (n *_{\mathbb{N}} k) \ +_{\mathbb{N}} \ (n *_{\mathbb{N}} m) \qquad \forall\, n, k, m \in \mathbb{N}$

(o_1) $\leq_{\mathbb{N}}$ is a reflexive relation on $\mathbb{N}$

(o_2) $\leq_{\mathbb{N}}$ is an antisymmetric relation on $\mathbb{N}$

(o_3) $\leq_{\mathbb{N}}$ is a transitive relation on $\mathbb{N}$

(o_4) $\leq_{\mathbb{N}}$ is a total relation on $\mathbb{N}$

(so) Let $n, k \in \mathbb{N}$

$$n \leq_{\mathbb{N}} k \iff n +_{\mathbb{N}} m \leq_{\mathbb{N}} n +_{\mathbb{N}} m \quad \forall\, m \in \mathbb{N}$$

Aim of Section 1.1

In this section we will prove the following result:
Given a Peano System $\big(\mathbb{N},\, 1,\, \sigma\big)$ we could define:
two binary inner operations $+_{\mathbb{N}}$, $*_{\mathbb{N}}$ on $\mathbb{N}$, a relation $\leq_{\mathbb{N}}$ on $\mathbb{N}$ such that
$\big(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, \leq_{\mathbb{N}}\ \big)$ is a model of a Peano Ring

---

Proposition 1.1

σ is surjective on $\mathbb{N} - \{1\}$

Proof
By contradiction $\exists\, k \in \mathbb{N} - \{1\}$ such that $k \neq \sigma(n) \ \forall\, n \in \mathbb{N}$
Let $A := \{n \in \mathbb{N} \mid n \neq k\}$

- $1 \neq k \implies 1 \in A$
- If $n \neq k \Longrightarrow \sigma(n) \neq k$ for hypothesis on k i.e.
  If $n \in A \Longrightarrow \sigma(n) \in A$

Then by axiom (v) $A = \mathbb{N}$ which is in contradiction since $k \notin A$
■
It is immediate consequence of proposition 1.1 the following:

Corollary 1.1

$\mathbb{N} = \{1\} \cup \{\sigma(n) \mid n \in \mathbb{N}\}$
And they are disjoints sets

Method of Proving by Induction

Now we want to prove that a property $P(k)$ holds for all $k \in \mathbb{N}$

Axiom **(v)** allow us to enunciate the following result:

Lemma 1.1 (Induction Theorem)

Let $(\mathbb{N}, 1, \sigma)$ a Peano System

Let P be a predicate or a statement on $\mathbb{N} \quad | \quad \begin{cases} P(1) \text{ holds} \\ P(k) \text{ holds} \implies P(\sigma(k)) \text{ holds} \end{cases}$

Then $\quad P(k)$ holds $\quad \forall\, k \in \mathbb{N}$

Proof

Let $A := \{k \in \mathbb{N} \mid P(k) \text{ holds }\}$

- $P(1)$ holds $\implies 1 \in A$
- If $k \in A \implies P(k)$ holds. Then by hypothesis $P(\sigma(k))$ holds $\implies \sigma(k) \in A$

By axiom **(v)** $\implies A = \mathbb{N}$
■

Notational Remark 1.1

Henceforth when we will use Induction we denote the induction hypothesis
"$P(k)$ holds" with $I.S.$

Definition by Recursion

Suppose that we want to define a function $R : \mathbb{N} \longrightarrow \mathbb{N}$ which associate to all the elements k of $\mathbb{N}$ an other element $R(k)$ of $\mathbb{N}$

Suppose that we want R satisfies :

- $R(1) = u \quad$ where $u \in \mathbb{N}$
- $R(\sigma(k)) = g(R(k)) \quad \forall\, k \in \mathbb{N} \quad$ where $g : \mathbb{N} \longrightarrow \mathbb{N}$

The proof of this theorem could appears obvious to someone, since for all Natural number k there exists a finite procedure to value $R(k)$:

- If $k = 1 \quad R(k) = u$
- If $k \neq 1 \overset{\text{C.1.1}}{\Longrightarrow} \exists\, l \in \mathbb{N} \quad | \quad \sigma(l) = k$
  $R(1) = u \implies R(2) = g(R(1)) \ldots \implies R(k) := g(R(l))$

Even if for $k = 4512$ this procedure could be "quite long", none could says it does not exists.

No. The meaning of this theorem is much deeper and to understand it completely we have to think about The definition of function. A function is a subset of the Cartesian Product given by $\{(n, R(n)) \mid n \in \mathbb{N}\}$. It is here the difference.

This theorem want to prove the existence of R as a set, as an object in its totality.The fact that for all k there exists a method to value $R(k)$ is admissible only if it was proved, before, such as R exists.

To prove the existence of such as R an acute reader could hazard this proof:

Let $B := \{k \in \mathbb{N} \mid \exists\, R(k)\}$

- $1 \in B$ since $R(1) = u$
- Suppose $k \in B \implies \exists\, R(k)$ and putting $R(\sigma(k)) := g(R(k))$
  We have proved $R(\sigma(k))$ exists $\implies \sigma(k) \in B$

The by axiom $v \quad \implies B = \mathbb{N}$ i.e. R is defined for all the elements of $\mathbb{N}$

Where does the acute reader wrong using the induction axiom in this way? The error appears at the beginning of the proof
Supposing that $\exists\, k \in B$ implies that R is yet defined on $\mathbb{N}$ and this is a wrong method since one is proving a result using the result itself

Here is a correct method to proceed[1]

Lemma 1.2 (Recursion Theorem)

Let $(\mathbb{N}, 1, \sigma)$ a Peano System

Let $V \subseteq \mathbb{N}, V \neq \emptyset, \quad u \in V \quad g : V \longrightarrow V$

$$\text{Then } \exists! \quad R_{g,u} : \mathbb{N} \longrightarrow V \quad | \quad \begin{cases} R_{g,u}(1) = u \\ R_{g,u}(\sigma(k)) = g(R_{g,u}(k)) \quad \forall\, k \in \mathbb{N} \end{cases}$$

Proof

[1] The proof of the following result is inspired by Mendelson [Me1] pg 56

(R_1) Let $n \in \mathbb{N}$ and define a subset A_n of $\mathbb{N}$ as follows:

$$A_n := \begin{cases} 1 \in A_n \\ n \in A_n \\ \sigma(n) \notin A_n \\ \sigma(k) \in A_n \implies k \in A_n \end{cases}$$

$h : \mathbb{N} \longrightarrow V$ a $n-$piece of $R_{g,u}$ if satisfies following properties:

1. $h(1) = u$
2. $\forall\, \sigma(k) \in A_n \implies h(\sigma(k)) = g(h(k))$

$\mathcal{R}_n := \{h : \mathbb{N} \longrightarrow V \mid h \quad n - \text{piece of } R_{g,u}\}$

(R_2) $\mathcal{R}_n \neq \emptyset \quad \forall\, n \in \mathbb{N}$:

Let $B := \{n \in \mathbb{N} \mid \exists\, h \in \mathcal{R}_n\}$

- $1 \in B$

  $$\left.\begin{array}{l} A_1 = \{1\} \\ \text{Take } h(k) = u \ \ \forall\, k \in \mathbb{N} \end{array}\right\} \implies h \in \mathcal{R}_1$$

- Suppose $n \in B \implies \exists\, h \in \mathcal{R}_n$

  $A_{\sigma(n)} = A_n \cup \{\sigma(n)\}$, and define $\quad \hat{h}(k) := \begin{cases} h(k) & \text{if } k \in A_n \\ g(h(n)) & \text{Otherwise} \end{cases}$

  It's not difficult to prove that $\hat{h} \in \mathcal{R}_{\sigma(n)} \implies \sigma(n) \in B$

By axiom $v \quad \implies B = \mathbb{N}$

(R_3) $h \in \mathcal{R}_{\sigma(n)} \implies h \in \mathcal{R}_n \quad \forall\, n \in \mathbb{N}$:

We omit this part of the proof

(R_4) $\forall\, n \in \mathbb{N}$ If $h_1, h_2 \in \mathcal{R}_n \implies h_1(k) = h_2(k) \quad \forall\, k \in A_n$:

By Induction one proves that calling

$B := \{k \in \mathbb{N} \mid \text{If h, f } \in \mathcal{R}_\text{k} \quad \text{h(l)} = \text{f(l)} \quad \forall\, \text{l} \in \text{A}_\text{k}\} \implies \text{B} = \mathbb{N}$

(R_5) Now fix $n \in \mathbb{N}$ and let

$R^{(n)} := \cap_{h \in \mathcal{R}_n} \{(k, h(k)) \mid k \in A_n\}$

By (R_4) $R^{(n)} \neq \emptyset \quad \forall\, n \in \mathbb{N}$

$R_{g,u} := \cup_{n \in \mathbb{N}} R^{(n)}$

We have to prove that:

1. $R_{g,u}$ is a function from $\mathbb{N}$ to V:

   By induction on n we show that

   $(n, b), (n, b_1) \in R_{g,u} \implies b = b_1 \quad \forall\, n \in \mathbb{N}$

2. $R_{g,u}(1) = u$
3. $R_{g,u}(\sigma(k)) = g(R_{g,u}(k)) \quad \forall\, k \in \mathbb{N}$

(R_6) $R_{g,u}$ is the only function which satisfies the conditions requested by (R_5):

To prove this ,given F_1, F_2 satisfying (R_5),

It suffices show that called $U := \{n \in \mathbb{N} \mid F_1(n) = F_2(n)\} \implies U = \mathbb{N}$

And it is immediate proving it by induction

■

Iterative Construction of subsets

The following Lemma is a useful generalization of Recursion Theorem (Lemma 1.2). It will be useful to build up families of subsets. We will omit the proof since it would be the same as Recursion Theorem's proof

Lemma 1.3 (Iterative Construction Theorem)

Let $\mathfrak{V} \subseteq \mathcal{P}(\mathbb{N}) - \{\emptyset\}, \quad A \in \mathfrak{V}, \quad G : \mathfrak{V} \longrightarrow \mathfrak{V}$

$$\text{Then } \exists! \quad R_{G,A} : \mathbb{N} \longrightarrow \mathfrak{V} \quad | \quad \begin{cases} R_{G,A}(1) = A \\ R_{G,A}(k+1) = G(R_{G,A}(k)) \quad \forall\, k \in \mathbb{N} \end{cases}$$

Remark 1.1 (Recursion in a generic set)

One can says that we prove Recursion Theorem only for $g : V \longrightarrow V$ where $V \subseteq \mathbb{N}$. We could be extend Recursion Theorem for any $V \subseteq X$ where X is any set. Look at the proof of Lemma 1.2 to get sure of it

In the same way we could extend Iterative Construction for any $\mathfrak{V} \subseteq \mathcal{P}(X) - \{\emptyset\}$ where X is any set

Definition 1.3

Fix $n \in \mathbb{N}$.

By Recursion Theorem

$$\exists\ R_{\sigma,\sigma(n)} : \mathbb{N} \longrightarrow \mathbb{N} \quad | \quad \begin{cases} R_{\sigma,\sigma(n)}(1) := \sigma(n) \\ R_{\sigma,\sigma(n)}(\sigma(k)) := \sigma(R_{\sigma,\sigma(n)}(k)) \quad \forall\, k \in \mathbb{N} \end{cases}$$

Fixed $n \in \mathbb{N}$ we will denote $R_{\sigma,\sigma(n)}(k)$ as $\sigma^k(n)$

Then $\sigma^k(n)$ satisfies:

- $\sigma^1(n) := \sigma(n)$
- $\sigma^{\sigma(k)}(n) := \sigma(\sigma^k(n)) \quad \forall\, k \in \mathbb{N}$

Remark 1.2

Henceforth we will omit this passage on definition new function on $\mathbb{N}$
We will simply give the couple of equations which characterize the recursive definition

Proposition 1.2

$\sigma^k(1) = \sigma(k) \quad \forall\, k \in \mathbb{N}$

Proof
Let us proceed by induction on k

- $k = 1$
  $\sigma^1(1) \overset{\text{D.1.3}}{=} \sigma(1)$
- Supposed for k we show it for $\sigma(k)$
  $\sigma^{\sigma(k)}(1) \overset{\text{D.1.3}}{=} \sigma(\sigma^k(1)) \overset{I.S.}{=} \sigma(\sigma(k))$

■

Proposition 1.3

Let $n, m \in \mathbb{N}$
$\sigma^k(n) = \sigma^k(m) \implies n = m \quad \forall\, k \in \mathbb{N}$

Proof
We proceed by Induction on k

- $k = 1$
  $\sigma^1(n) = \sigma^1(m) \overset{\text{D.1.3}}{\implies} \sigma(n) = \sigma(m) \overset{\textbf{(iii)}}{\implies} n = m$
- Supposed for k we show it for $\sigma(k)$
  $\sigma^{\sigma(k)}(n) = \sigma^{\sigma(k)}(m) \overset{\text{D.1.3}}{\implies} \sigma(\sigma^k(n)) = \sigma(\sigma^k(m)) \overset{\textbf{(iii)}}{\implies} \sigma^k(n) = \sigma^k(m) \overset{I.S.}{\implies} n = m$

■

Proposition 1.4

$\sigma^k(\sigma(n)) = \sigma^{\sigma(k)}(n) \quad \forall\, k, n \in \mathbb{N}$

Proof
Fixed n let us proceed by Induction on k

- $k = 1$
  $\sigma^1(\sigma(n)) \overset{\text{D.1.3}}{=} \sigma(\sigma(n)) \overset{\text{D.1.3}}{=} \sigma(\sigma^1(n)) \overset{\text{D.1.3}}{=} \sigma^{\sigma(1)}(n)$
- Supposed for k we show it for $\sigma(k)$
  $\sigma^{\sigma(k)}[\sigma(n)] \overset{\text{D.1.3}}{=} \sigma[\sigma^k(\sigma(n))] \overset{I.S.}{=} \sigma[\sigma^{\sigma(k)}(n)] \overset{\text{D.1.3}}{=} \sigma^{\sigma(\sigma(k))}(n)$

■

Proposition 1.5

$\sigma^k(n) = \sigma^n(k) \quad \forall\, n, k \in \mathbb{N}$

Proof
Fix $n \in \mathbb{N}$ let us proceed by Induction on k

- $k = 1$
  $\sigma^1(n) \overset{\text{D.1.3}}{=} \sigma(n) \overset{\text{P.1.2}}{=} \sigma^n(1)$
- Supposed for k we show it for $\sigma(k)$
  $\sigma^{\sigma(k)}(n) \overset{\text{D.1.3}}{=} \sigma(\sigma^k(n)) \overset{I.S.}{=} \sigma(\sigma^n(k)) \overset{\text{D.1.3}}{=} \sigma^{\sigma(n)}(k)$

■

Definition 1.4

Let $\;+_{\mathbb{N}} \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}\;$ defined as:
$+_{\mathbb{N}} := \{((n,k), \sigma^k(n)) \mid n, k \in \mathbb{N}\}$
It is easy to prove that $+_{\mathbb{N}}$ is a binary inner operation[2] on $\mathbb{N}$

Namely $\quad \begin{array}{rccc} +_{\mathbb{N}}: & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n,k) & \longrightarrow & \sigma^k(n) \end{array}$

In view of proposition 1.5 the following theorem holds

Theorem 1.1

$$n +_{\mathbb{N}} k = k +_{\mathbb{N}} n \qquad \forall\, n, k \in \mathbb{N}$$

Notational Remark 1.2
Henceforth we will denote $+_{\mathbb{N}}$ simply as $+$

[2]See this definition in: A brief survey of elements of Set theory and Logic

Corollary 1.2

Let $n, m \in \mathbb{N}$

$n = m \Longleftrightarrow n + l = m + l \quad \forall\, l \in \mathbb{N}$

Proof

$n = m \overset{\text{P.1.3}}{\Longleftrightarrow} \sigma^l(n) = \sigma^l(k)\ \ \forall\, l \in \mathbb{N} \overset{\text{D.1.4}}{\Longleftrightarrow} n + l = k + l\ \ \forall\, l \in \mathbb{N}$

■

Theorem 1.2

$$(k + n) + m = k + (n + m) \qquad \forall\, n, m, k \in \mathbb{N}$$

Proof

- $(k + n) + m \overset{\text{D.1.4}}{=} \sigma^k(n) + m \overset{\text{D.1.4}}{=} \sigma^m(\sigma^n(k))$

- $k + (n + m) \overset{\text{D.1.4}}{=} k + \sigma^m(n) \overset{\text{D.1.4}}{=} \sigma^{\sigma^m(n)}(k)$

Hence we have to show that

$\sigma^m(\sigma^n(k)) = \sigma^{\sigma^m(n)}(k) \quad \forall\, n, m, k \in \mathbb{N}$

Fixed k, m let us proceed by induction on n

- $n = 1$
  $\sigma^m(\sigma^1(k)) \overset{\text{D.1.3}}{=} \sigma^m(\sigma(k)) \overset{\text{P.1.4}}{=} \sigma^{\sigma(m)}(k) \overset{\text{P.1.2}}{=} \sigma^{\sigma^m(1)}(k)$
- Supposed for n we show it for $\sigma(n)$
  $\sigma^m[\sigma^{\sigma(n)}(k)] \overset{\text{D.1.3}}{=} \sigma^m[\sigma(\sigma^n(k))] \overset{\text{P.1.4}}{=} \sigma^{\sigma(m)}(\sigma^n(k)) \overset{\text{D.1.3}}{=} \sigma[\sigma^m(\sigma^n(k))]$
  $\overset{I.S.}{=} \sigma[\sigma^{\sigma^m(n)}(k)] \overset{\text{D.1.3}}{=} \sigma^{\sigma[\sigma^m(n)]}(k) \overset{\text{D.1.3}}{=} \sigma^{\sigma^{\sigma(m)}(n)}(k) \overset{\text{P.1.4}}{=} \sigma^{\sigma^m\sigma(n)}(k)$

■

Definition 1.5

Fix $n \in \mathbb{N}$ and let $g \subseteq \mathbb{N} \times \mathbb{N}$ defined as $g := \{(k, n + k) \ \mid n \in \mathbb{N}\}$
It easy to prove that $g : \mathbb{N} \longrightarrow \mathbb{N}$

Then by Recursion Theorem we define:
$(n, 1)_* := n$
$(n, \sigma(k))_* := n + (n, k)_* \quad \forall\, k \in \mathbb{N}$

Proposition 1.6

$(1,k)_* = k \quad \forall\, k \in \mathbb{N}$

Proof

- $k = 1$
  $(1,1)_* \overset{\text{D.1.5}}{=} 1$
- Supposed for k we show it for $\sigma(k)$
  $(1,\sigma(k))_* \overset{\text{D.1.5}}{=} (1,k)_* + 1 \overset{I.S.}{=} k + 1 \overset{\text{D.1.4}}{=} \sigma(k)$

■

Proposition 1.7

Let $n \in \mathbb{N}$
$(n+1,k)_* = (n,k)_* + k \quad \forall\, k \in \mathbb{N}$

Proof
We show it by Induction on k

- $k = 1$
  $(n+1,1)_* \overset{\text{D.1.5}}{=} n + 1 \overset{\text{D.1.5}}{=} (n,1)_* + 1$
- Supposed for k we show it for $\sigma(k)$

$$
\begin{aligned}
(n+1,\sigma(k))_* &\overset{\text{D.1.5}}{=} (n+1,k)_* + (n+1) \overset{I.S.}{=} ((n,k)_* + k) + (n+1) \\
&\overset{\text{T.1.2}}{=} (n,k)_* + (k + (n+1)) \overset{\text{T.1.2}}{=} (n,k)_* + ((k+n)+1) \\
&\overset{\text{T.1.1}}{=} (n,k)_* + ((n+k)+1) \overset{\text{T.1.2}}{=} (n,k)_* + (n + (k+1)) \\
&\overset{\text{T.1.2}}{=} ((n,k)_* + n) + (k+1) \overset{\text{D.1.5}}{=} (n,\sigma(k))_* + \sigma(k)
\end{aligned}
$$

■

Proposition 1.8

$(k,n)_* = (n,k)_* \quad \forall\, n,k \in \mathbb{N}$

Proof
Fix n let us proceed by Induction on k

- $k = 1$
  $(1,n)_* \overset{\text{P.1.6}}{=} n \overset{\text{D.1.5}}{=} (n,1)_*$

- Supposed for k we show it for $\sigma(k)$

  $(\sigma(k), n)_* \overset{\text{P.1.7}}{=} (k, n)_* + n \overset{I.S.}{=} (n, k)_* + n \overset{\text{D.1.5}}{=} (n, \sigma(k))_*$

■

Notational Remark 1.3
As in definition 1.4 let

$*_{\mathbb{N}} := \{((n, k), (n, k)_*) \ \mid \ n, k \ \in \mathbb{N}\}$

It is easy to prove that $*_{\mathbb{N}}$ is a binary inner operation[3] on $\mathbb{N}$

Namely $\begin{array}{llll} *_{\mathbb{N}} : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (n, k) & \longrightarrow & (n, k)_* \end{array}$

In view of proposition 1.8 the following theorem holds

Theorem 1.3

$$n *_{\mathbb{N}} k = k *_{\mathbb{N}} n \qquad \forall\, n, k \ \in \mathbb{N}$$

Notational Remark 1.4
Henceforth we will denote $*_{\mathbb{N}}$ simply as $*$

Theorem 1.4

$$n * (l + m) = n * l + n * m \qquad \forall\, n, k, l \ \in \mathbb{N}$$

Proof
I show that fixed n, l then

$n * (l + m) = n * l + n * m \quad \forall\, m \ \in \mathbb{N}$

- $m = 1$

  $n * (l + 1) \overset{\text{D.1.5}}{=} n * l + n \overset{\text{D.1.5}}{=} n * l + n * 1$

- Supposed for m we show it for $\sigma(m)$

  $$\begin{aligned} n * (l + \sigma(m)) &\overset{\text{D.1.4}}{=} n * (l + m + 1) \overset{\text{D.1.4}}{=} n * (\sigma(l + m)) \\ &\overset{\text{D.1.5}}{=} n * (l + m) + n \overset{I.S.}{=} n * l + n * m + n \\ &\overset{\text{T.1.2}}{=} n * l + (n * m + m) \overset{\text{D.1.5}}{=} n * l + n * \sigma(m) \end{aligned}$$

■

[3] See this definition in: A brief survey of elements of Set theory and Logic

Theorem 1.5

$$(n * k) * m = n * (k * m) \qquad \forall n, k, m \in \mathbb{N}$$

Proof
we show that fixed n, k

$(n * k) * m = n * (k * m) \quad \forall m \in \mathbb{N}$

- $m = 1$

  $(n * l) * 1) \stackrel{\text{D.1.5}}{=} n * l \stackrel{\text{D.1.5}}{=} n * (l * 1)$

- Supposed for m we show it for $\sigma(m)$

  $$(n * l) * \sigma(m) \stackrel{\text{D.1.5}}{=} (n * l) * m + (n * l) \stackrel{I.S.}{=} n * (l * m) + n * l$$
  $$\stackrel{\text{T.1.4}}{=} n * (l * m + l) \stackrel{\text{D.1.5}}{=} n * (l * \sigma(m))$$

■

Definition 1.6

Let $n, k \in \mathbb{N}$

$n <_{\mathbb{N}} k \Longleftrightarrow \exists\, l \in \mathbb{N} \quad | \quad n + l = k$

Notational Remark 1.5
Henceforth we denote $<_{\mathbb{N}}$ as $<$ We use notation $n \not< k$ to denote "$n < k$ does not hold"

Proposition 1.9

$k \not< k \quad \forall k \in \mathbb{N}$

Proof
We proceed by Induction on k

- $k = 1$

  By contradiction : $1 < 1 \Longrightarrow \exists\, l$ such that $1 + l = 1$

  $\Longrightarrow \sigma(l) = 1$

  But this is in contradiction with axiom **(iv)** .

- Supposed for k we prove it for $\sigma(k)$

  By contradiction $\sigma(k) < \sigma(k) \Longrightarrow \exists\, l$ such that $\sigma(k) + l = \sigma(k)$

  Then by definition 1.4

  $(k + 1) + l = k + 1 \iff k + (1 + l) = k + 1 \stackrel{\text{C.1.2}}{\Longleftrightarrow} 1 + l = 1 \stackrel{\text{D.1.6}}{\Longleftrightarrow} 1 < 1$

  But this is in contradiction with the first step of this proof .

■

Corollary 1.3

Let $n, k \in \mathbb{N}$

$n < k \Longrightarrow n \neq k$

Proof

By contradiction : $n = k \overset{\text{P.1.9}}{\Longrightarrow} n \not< k$.

But this is in contradiction with the hypothesis . ■

Remark 1.3

Proposition 1.9 and corollary 1.3 may appear not so important, but they begin to illustrate the structure of $\mathbb{N}$.

Furthermore they guarantee that the following definition is not redundant

Definition 1.7

Let $n, k \in \mathbb{N}$

$n \leq_{\mathbb{N}} k \Longleftrightarrow n < k \quad \text{or} \quad n = k$

Notational Remark 1.6

Henceforth we denote $\leq_{\mathbb{N}}$ as $\leq$

An immediate corollary of definition 1.7 is the following

Theorem 1.6

$$n \leq n \quad \forall n \in \mathbb{N}$$

Theorem 1.7

$$\left.\begin{array}{l} n \leq k \\ k \leq n \end{array}\right\} \Longrightarrow n = k$$

Proof

$n \leq k \overset{\text{D.1.7}}{\Longleftrightarrow} n < k \quad \text{or} \quad n = k$

$k \leq n \overset{\text{D.1.7}}{\Longleftrightarrow} k < n \quad \text{or} \quad n = k$

If we suppose $n < k \overset{\text{C.1.3}}{\Longrightarrow} n \neq k$. And since $k \leq n$ and $n \leq k$
Then $k < n$ and $n < k$ i.e

$\exists\, l$ such that $n + l = k$ and $\exists\, l_1$ such that $k + l_1 = n$

And then $n+l=k \Longrightarrow (k+l_1)+l=k \overset{\text{T.1.2}}{\Longrightarrow} k+(l+l_1)=k \Longrightarrow k<k$

But this is a contradiction by proposition 1.9.

And then $n \leq k$, but $n \not< k \overset{\text{D.1.7}}{\Longrightarrow} n=k$

■

Theorem 1.8

$$\left.\begin{array}{l} n \leq n_1 \\ n_1 \leq n_2 \end{array}\right\} \Longrightarrow n \leq n_2$$

Proof

- If $n=n_1$ or $n_1=n_2$ nothing to prove
- If $n \neq n_1$ and $n_1 \neq n_2 \Longrightarrow n<n_1$ and $n_1<n_2$
  $n<n_1 \Longleftrightarrow \exists\, l$ such that $n+l=n_1$
  $n_1<n_2 \Longleftrightarrow \exists\, m$ such that $n_1+m=n_2$
  Then $n+(l+m) \overset{\text{T.1.2}}{=} (n+l)+m=n_1+m=n_2$
  I.e. by definition 1.6 $n<n_2 \overset{\text{D.1.7}}{\Longrightarrow} n \leq n_2$.

■

Corollary 1.4

$1<n \quad \forall\, n \in \mathbb{N}-\{1\}$

Proof
Let $n \neq 1$ then by corollary 1.1 $\exists\, l \in \mathbb{N} \quad n=l+1 \overset{\text{D.1.6}}{\Longleftrightarrow} 1<n$

■

Corollary 1.5

$k<\sigma(k) \quad \forall\, k \in \mathbb{N}$

Proof
$\sigma(k) \overset{\text{D.1.4}}{=} k+1 \Longrightarrow \exists\, l \in \mathbb{N} \quad | \quad k+l=\sigma(k)$ ■

Theorem 1.9

Formulation 1.9.1

$\forall\, n,k \in \mathbb{N}$ one and only one of the following holds : $n=k, \quad n<k, \quad n>k$

Proof
It is clear they are three disjoint options. The heart of the proof is showing that at least one holds for any couple $n, k \in \mathbb{N}$. To show this fix n , and let us proceed by induction on k

- $k = 1$

  By corollary 1.1 we have two possibilities for n

  If $n = 1 \implies n = k$

  If $n \neq 1 \overset{\text{C.1.4}}{\implies} 1 < n$

- Supposed for k we show for $\sigma(k)$.

  By inductive step one and only one of the following holds;

  $n = k \qquad n < k \qquad k < n$

  - If $n = k$

    Applying corollary 1.5 we get $n < \sigma(k)$
  - if $n < k$
    $\overset{\text{C.1.5}}{\implies} k < \sigma(k) \overset{\text{T.1.8}}{\implies} n < \sigma(k)$
  - if $k < n \implies \exists\, l$ with $k + l = n$
    - If $l = 1 \implies \sigma(k) = n$
    - if $l \neq 1 \overset{\text{C.1.1}}{\implies} n = k + (1 + m) \overset{\text{T.1.2}}{=} (k + 1) + m \iff \sigma(k) < n$

■

Formulation 1.9.2

$$\forall\, n, k \in \mathbb{N} \implies n \leq k \text{ or } \; k \leq n$$

Proof
It comes immediately by above formulation ■

Theorem 1.10

Formulation 1.10.1
Let $n, k \in \mathbb{N}$

$$n < k \iff n + l < k + l \qquad \forall\, l \in \mathbb{N}$$

Proof
$\implies$)

- $l = 1$

  Since $n < k \overset{\text{C.1.3}}{\implies} n \neq k \overset{\text{C.1.2}}{\implies} n + 1 \neq k + 1$

  Hence by theorem 1.9 $(n + 1) < (k + 1)$ or $(k + 1) < (n + 1)$.

By contradiction $(k+1) < (n+1) \overset{\text{D.1.6}}{\Longrightarrow} \exists\, g \in \mathbb{N}$ such that $(k+1)+g = (n+1)$.

On the other hand since $n < k \overset{\text{D.1.6}}{\Longrightarrow} n + m = k$. Hence

$$\begin{aligned}((n+m)+1)+g = (n+1) &\overset{\text{T.1.2}}{\Longrightarrow} (n+(m+1))+g = (n+1)\\ &\overset{\text{T.1.1}}{\Longrightarrow} (n+(1+m))+g = (n+1)\\ &\overset{\text{T.1.2}}{\Longrightarrow} ((n+1)+m)+g = (n+1)\\ &\overset{\text{T.1.2}}{\Longrightarrow} (n+1)+(m+g) = n+1\\ &\overset{\text{D.1.6}}{\Longrightarrow} n+1 < n+1.\end{aligned}$$

But this a contradiction by proposition 1.9

- Supposed for l we show it for $\sigma(l)$

  Since $n < k \overset{\text{C.1.3}}{\Longrightarrow} n \neq k \overset{\text{C.1.2}}{\Longrightarrow} n + \sigma(l) \neq k + \sigma(l)$

  Hence by theorem 1.9 $(n+\sigma(l)) < (k+\sigma(l))$ or $(k+\sigma(l)) < (n+\sigma(l))$.

  By contradiction $(k+\sigma(l)) < (n+\sigma(l)) \overset{\text{D.1.6}}{\Longrightarrow} \exists\, g \in \mathbb{N}$ such that $(k+\sigma(l))+g = (n+\sigma(l))$.

  On the other hand since $n < k \overset{\text{D.1.6}}{\Longrightarrow} n + m = k$. Hence

$$\begin{aligned}((n+m)+\sigma(l))+g = (n+\sigma(l)) &\overset{\text{T.1.2}}{\Longrightarrow} (n+(m+\sigma(l)))+g = (n+\sigma(l))\\ &\overset{\text{T.1.1}}{\Longrightarrow} (n+(\sigma(l)+m))+g = (n+\sigma(l))\\ &\overset{\text{T.1.2}}{\Longrightarrow} ((n+\sigma(l))+m)+g = (n+\sigma(l))\\ &\overset{\text{T.1.2}}{\Longrightarrow} (n+\sigma(l))+(m+g) = n+\sigma(l)\\ &\overset{\text{D.1.6}}{\Longrightarrow} n+\sigma(l) < n+\sigma(l).\end{aligned}$$

  But this a contradiction by proposition 1.9

$\Longleftarrow$)

By theorem 1.9 $\Longrightarrow$ $n = k$ or $n < k$ or $n > k$

- If $n = k$

  $\overset{\text{P.1.3}}{\Longrightarrow} \sigma^l(n) = \sigma^l(k) \Longrightarrow n + l = k + l$

- If $n > k$

  By formulation above $n + l > k + l$

And then the only one possible is $n < k$ ■

Formulation 1.10.2

Let $n, k \in \mathbb{N}$

$$n \leq k \Longleftrightarrow n + l \leq k + l \quad \forall\, l \in \mathbb{N}$$

Proof

It comes immediately by above formulation and corollary 1.2 ■

Proposition 1.10

Let $n, k \in \mathbb{N}$

$n < k \Longleftrightarrow n * l < k * l \quad \forall\, l \in \mathbb{N}$

Proof

$\Longrightarrow)$

Proceed by induction on l

- $l = 1$ nothing to prove .
- Supposed for l we show it for $\sigma(l)$

  $n * \sigma(l) \overset{\text{D.1.5}}{=} n * l + n \overset{I.S.}{<} k * l + n \overset{\text{T.1.10}}{<} k * l + k \overset{\text{D.1.5}}{=} k * \sigma(l)$

$\Longleftarrow)$

By theorem 1.9 $\quad \Longrightarrow \quad n = k$ or $n < k$ or $n > k$

- If $n = k \Longrightarrow n * l = k * l$
- If $n > k$

  By formulation above $n * l > k * l$

Then the only one possible is $\quad n < k$

■

1.1.1 Isomorphism between Peano Systems

Let $\big(\mathbb{M},\, u,\, \omega\big)$, $\big(\mathbb{N},\, 1,\, \sigma\big)$,two Peano Systems given by definition 1.1.

Then there exists $\quad R : \mathbb{N} \longrightarrow \mathbb{M}$ such that:

1. $R(1) = u$
2. $R(\sigma(n)) = \omega(R(n)) \qquad \forall\, n \in \mathbb{N}$
3. R is injective
4. R is surjective

Proof

According to remark 1.1 by Recursion Theorem let

$R_{\omega,u} : \mathbb{N} \longrightarrow \mathbb{M}.$

To get easier notations we denote $R_{\omega,u}$ as R

R is the function required

1. Obvious by definition Recursion Theorem (Lemma 1.2)

2. As step 1.
3. We divide this step into two points
   - $R(n) = u \implies n = 1 \quad \forall n \in \mathbb{N}$:
     By contradiction $n \neq 1 \overset{\text{C.1.1}}{\implies} \exists\, l \in \mathbb{N} \quad | \quad \sigma(l) = n$
     $$\left.\begin{array}{ll}\text{By step 2.} & R(n) = \omega(R(l)) \\ \text{By hyphothesis} & R(n) = u\end{array}\right\} \implies \exists\, m \in \mathbb{M} \;|\; u = \omega(m)$$
     Contradiction with axiom **(iv)**
   - $R(n) = R(k) \longrightarrow n = k \quad \forall\, n, m \in \mathbb{N}$:
     Let $n \in \mathbb{N}$ and we proceed by Induction on k
     - $k = 1$ then $n = 1$ by the first point of step 3.
     - Supposed for k we showed for $\sigma(k)$
       $R(n) = R(\sigma(k)) \implies R(n) = \omega(R(k))$ and hence $n \neq 1$, otherwise $R(n) = u$
       Therefore by corollary 1.1 $\quad \exists\, j \in \mathbb{N} \quad | \quad \sigma(j) = n$
       $$\left.\begin{array}{ll}\text{By step 2.} & R(n) = \omega(R(j)) \\ \text{By hyphothesis} & R(n) = R(\sigma(k))\end{array}\right\} \implies \omega(R(j)) = \omega(R(k))$$
       $$\overset{\textbf{(iii)}}{\implies} R(k) = R(j)$$
       $$\overset{I.S.}{\implies} k = j$$
       $$\implies \sigma(k) = n$$
4. By contradiction $\exists\, m_0 \in \mathbb{M} \quad | \quad m_0 \notin R(\mathbb{N})$
   Let $A := \{m \in \mathbb{M} \mid m \neq m_0 \quad \text{and} \quad m \in R(\mathbb{N})\,\}$
   - $u \in A$:
     $u \in R(\mathbb{N})$, since $u = R(1)$ and $u \neq m_0$, otherwise $R(1) = m_0$
   - If $m \in A \implies \omega(m) \in A$:
     $$m \in A \implies m = R(l) \implies \omega(m) = R(\sigma(l)) \implies \omega(m) \in R(\mathbb{N})$$
     $$\implies m\omega(m) \neq m_0 \implies \omega(m) \in A$$

   Then by the axiom $v \quad A = \mathbb{M}$ which is in contradiction since $m_0 \notin A$

■

1.1.2 Remarks and Complements

Strong Induction and Well-Ordering of $\mathbb{N}$

On a Peano Ring $(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, \leq_{\mathbb{N}})$ we are able to give another two principles equivalents to Axiom **(v)**. In particular we are able to introduce Minimum principle on $\mathbb{N}$ which prove that $\leq_{\mathbb{N}}$ is a well-order on $\mathbb{N}$.

Induction and and Minimum principle will be used to prove different kind of results on $\mathbb{N}$. The first, as we know by Induction Theorem(Lemma 1.1), gives us a method to prove statements universally on $\mathbb{N}$.
The second one establish the existence of a privileged element which satisfies a determinate property on $\mathbb{N}$. The existence of the minimum will avoid arbitrary choices on proofs on $\mathbb{N}$, assuring us a constructive method to build a proof on the Natural.

Lemma 1.4 (Strong Induction and Minimum principle)

The following principle of $\mathbb{N}$ are equivalents:

(v) $\forall A \subseteq \mathbb{N} \quad | \quad \begin{cases} 1 \in A \\ n \in A \Longrightarrow \sigma(n) \in A \end{cases} \Longrightarrow A = \mathbb{N}$

Strong(v) $\forall A \subseteq \mathbb{N} \quad | \quad \begin{cases} 1 \in A \\ k \in A \ \forall 1 \leq k \leq n \Longrightarrow \sigma(n) \in A \end{cases} \Longrightarrow A = \mathbb{N}$

(Min) $\forall A \subseteq \mathbb{N} \quad \exists! \quad m \in A \quad | \quad m \leq n \quad \forall n \in A$

(Such as n will be called the minimum of A and it will be denoted by $n = \min\ A$)

Proof

Strong(v)$\Longrightarrow$ (v) It is trivial since If $A \subseteq \mathbb{N}$ satisfies the hypotheses of **Strong(v)**, A satisfies the hypotheses of **(v)**

(v)$\Longrightarrow$(Min) Suppose exists $A \subseteq \mathbb{N}$, $A \neq \emptyset$ such that:

If $m \leq n \quad \forall n \in A \Longrightarrow m \notin A$

Now let $B := \{m \in \mathbb{N} \mid m \leq n \forall n \in A\} \overset{\textbf{(v)}}{\Longrightarrow} B = \mathbb{N}$ And since if $n \in B \Longrightarrow n \notin A$ then $A = \emptyset$

(Min)$\Longrightarrow$Strong(v) Let $A \subseteq \mathbb{N}$ satisfying the hypotheses of **Strong(v)**

By contradiction: $A \subset \mathbb{N} \Longrightarrow \mathbb{N} - A \neq \emptyset \overset{\textbf{Min}}{\Longrightarrow} \exists\, m = \min(\mathbb{N} - A)$

Now $\forall n,\ 1 \leq n < m, \quad n \in A$ since m is the minimum of $\mathbb{N} - A$.

Then By hypotheses on $A \quad m \in A$. Contradiction

■

1.2 Construction of the Integers $\mathbb{Z}$

Definition 1.8

$\big($a set $\mathbb{Z}$, $+_{\mathbb{Z}}$, $*_{\mathbb{Z}}$, $\leq_{\mathbb{Z}}$ $\big)$ is an Ordered Integrity Domain (OID) if and only if satisfies the following properties:

(s_1) $z+s=s+z \quad \forall\, z,s \in \mathbb{Z}$

(s_2) $(z+s)+t=z+(s+t) \quad \forall\, z,s,t \in \mathbb{Z}$

(s_3) $\exists\; 0 \in \mathbb{Z} \mid z+0=z \quad \forall\, z \in \mathbb{Z}$

(s_4) $\forall\, z \in \mathbb{Z} \quad \exists -z \in \mathbb{Z} \mid z+(-z)=0$

(p_1) $z*s=s*z \quad \forall\, z,s \in \mathbb{Z}$

(p_2) $z*(s*t)=(z*s)*t \quad \forall\, z,s,t \in \mathbb{Z}$

(p_3) $\exists\; 1 \in \mathbb{Z} \mid z*1=z \quad \forall\, z \in \mathbb{Z}$

(sp) $z*(s+t)=z*s\,+\,z*t \quad \forall\, z,s,t \in \mathbb{Z}$

(o_1) $\leq$ is a reflexive relation on $\mathbb{Z}$

(o_2) $\leq$ is an antisymmetric relation on $\mathbb{Z}$

(o_3) $\leq$ is a transitive relation on $\mathbb{Z}$

(o_4) $\leq$ is a total relation on $\mathbb{Z}$

(so) let $z,s \in \mathbb{Z}$

$$z \leq s \iff z+t \leq s+t \quad \forall t \in \mathbb{Z}$$

(po) $z \geq 0,\ s \geq 0 \implies z*s \geq 0$

Aim of Section 1.2

In this section we show the following results:

Given a Peano Ring $\big(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, \leq_{\mathbb{N}}\big)$ there exists a model of an Ordered Integrity Domain $\big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, \leq_{\mathbb{Z}}\big)$ which contains a copy of $\big(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, \leq_{\mathbb{N}}\big)$

Notational Remark 1.7
In this Section we will denote

$n +_{\mathbb{N}} m$ simply as $n+m \quad \forall\, n,m \in \mathbb{N}$
$n *_{\mathbb{N}} m$ simply as $nm \quad \forall\, n,m \in \mathbb{N}$
$n \leq_{\mathbb{N}} m$ simply as $n \leq m \quad \forall\, n,m \in \mathbb{N}$
$n <_{\mathbb{N}} m$ simply as $n < m \quad \forall\, n,m \in \mathbb{N}$

Definition 1.9

Let $(n, m), (n_1, m_1) \in \mathbb{N} \times \mathbb{N}$
$(n, m) \equiv_{\mathbb{Z}} (n_1, m_1) \Longleftrightarrow n + m_1 = n_1 + n.$

Proposition 1.11

$\equiv_{\mathbb{Z}}$ is a equivalence relationship on $\mathbb{N} \times \mathbb{N}$

Definition 1.10

$\mathbb{Z} := \frac{\mathbb{N}\times\mathbb{N}}{\equiv_{\mathbb{Z}}}$

Proposition 1.12

Let $(n, m), (n_1, m_1), (k, l), (k_1, l_1) \in \mathbb{N} \times \mathbb{N}$

$$\left.\begin{array}{l}(n, m) \equiv_{\mathbb{Z}} (n_1, m_1)\\ (k, l) \equiv_{\mathbb{Z}} (k_1, l_1)\end{array}\right\} \Longrightarrow (n + k, m + l) \equiv_{\mathbb{Z}} (n_1 + k_1, m_1 + l_1)$$

Proof
On one hand
$(n, m) \equiv_{\mathbb{Z}} (n_1, m_1) \overset{\text{D.1.9}}{\Longleftrightarrow} (n + m_1) = (m + n_1).$

On the other hand
$(k, l) \equiv_{\mathbb{Z}} (k_1, l_1) \overset{\text{D.1.9}}{\Longleftrightarrow} (k + l_1) = (l + k_1).$

If we sum the two equations we get
$(n + m_1) + (k + l_1) = (m + n_1) + (l + k_1).$

Let us apply theorems 1.1 and 1.2 on the two members and hence
$(n + k) + (m_1 + l_1) = (n_1 + k_1) + (m + l) \overset{\text{D.1.9}}{\Longleftrightarrow} (n + k, m + l) \equiv_{\mathbb{Z}} (n_1 + k_1, m_1 + l_1)$
■

In view of proposition 1.12 the following definition is well posed

Definition 1.11

Let $z, s \in \mathbb{Z}$
$z +_{\mathbb{Z}} s := [(n + k, m + l)]$ where $(n, m) \in z$ and $(k, l) \in s$

Proposition 1.13

Let $(n, m), (n_1, m_1), (k, l), (k_1, l_1) \in \mathbb{N} \times \mathbb{N}$

If $(n,m) \equiv_{\mathbb{Z}} (n_1,m_1)$ and $(k,l) \equiv_{\mathbb{Z}} (k_1,l_1)$

Then $[((nk)+(ml),(nl)+(mk))] = [((n_1k_1)+(m_1l_1),(n_1l_1)+(m_1k_1))]$

Proof

On one hand

$(n,m) \equiv_{\mathbb{Z}} (n_1,m_1) \overset{D.1.9}{\Longleftrightarrow} (n+m_1) = (m+n_1)$

Then $(n+m_1)k_1 = (m+n_1)k_1$ and $(n_1+m)l_1 = (m_1+n)l_1$.

On the other hand

$(k,l) \equiv_{\mathbb{Z}} (k_1,l_1) \overset{D.1.9}{\Longleftrightarrow} (k+l_1) = (l+k_1)$

Then $(k+l_1)n_1 = (l+k_1)n_1$ and $(k_1+l)m_1 = (l_1+k)m_1$.

If we apply theorem 1.4 on all the four equation; we sum them and apply theorems 1.1 and 1.2 on the two members we get

$((nk)+(ml)) + ((n_1l_1)+(m_1k_1)) + T = ((n_1k_1)+(m_1l_1)) + ((nl)+(mk)) + T$
where $T = (n+m)(k_1+l_1)$

Then by corollary 1.2

$((nk)+(ml)) + ((n_1l_1)+(m_1k_1)) = ((n_1k_1)+(m_1l_1)) + ((nl)+(mk))$

Then by definition 1.9

$((nk)+(ml),((nl)+(mk)) \equiv_{\mathbb{Z}} ((n_1k_1)+(m_1l_1),(n_1l_1)+(m_1k_1))$

■

In view of proposition 1.13 the following definition is well posed

Definition 1.12

Let $z,s \in \mathbb{Z}$

$z *_{\mathbb{Z}} s := [(nk+ml,nl+mk)]$ where $(n,m) \in z$ and $(k,l) \in s$

Notational Remark 1.8

Henceforth we will denote:

$z +_{\mathbb{Z}} s$ simply as $z+s$ $\forall z,s \in \mathbb{Z}$
$z *_{\mathbb{Z}} s$ simply as $z*s$ $\forall z,s \in \mathbb{Z}$

Theorem 1.11

$$z+s = s+z \qquad \forall z,s \in \mathbb{Z}$$

Proof
Let $z = [(n,m)], \quad s = [(k,l)]$

$$\begin{aligned} z + s = [(n,m)] + [(k,l)] &\overset{\text{D.1.11}}{=} [(n+k, m+l)] \\ &\overset{\text{T.1.1}}{=} [(k+n, l+m)] \overset{\text{D.1.11}}{=} [(k,l)] + [(n,m)] = s + z \end{aligned}$$

■

Theorem 1.12

$$t + (z+s) = (t+s) + z \qquad \forall\, t, z, s \in \mathbb{Z}$$

Proof
Let $t = [(a,b)], \quad z = [(n,m)], \quad s = [(k,l)]$

$$\begin{aligned} t + (z+s) = [(a,b)] + \big([(n,m)] + [(k,l)]\big) &\overset{\text{D.1.11}}{=} [a,b] + [(n+k, m+l)] \\ &\overset{\text{D.1.11}}{=} [(a + (n+k), b + (m+l))] \overset{\text{T.1.2}}{=} [((a+n)+k, (b+m)+l)] \\ &\overset{\text{D.1.11}}{=} [(a+n, b+m)] + [(k,l)] \overset{\text{D.1.11}}{=} \big([(a,b)] + [(n,m)]\big) + [(k,l)] = (t+s) + z \end{aligned}$$

■

Proposition 1.14

$(n,n) \equiv_{\mathbb{Z}} (m,m) \quad \forall\, n, m \in \mathbb{N}$

Definition 1.13

$0_{\mathbb{Z}} := [(1,1)] \overset{\text{P.1.14}}{=} [(n,n)] \quad \forall\, n \in \mathbb{N}$

Notational Remark 1.9
Henceforth we will avoid this heavy notation and we will denote $0_{\mathbb{Z}}$ simply with 0

Proposition 1.15

Let $n, k \in \mathbb{N}$
$(n+c, k+c) \equiv_{\mathbb{Z}} (n,k) \quad \forall\, c \in \mathbb{N}$

Proof
Let $c \in \mathbb{N}$
$(n+c)+k \overset{\text{T.1.2}}{=} n + (c+k) \overset{\text{T.1.1}}{=} n + (k+c) \overset{\text{D.1.9}}{\iff} (n+c, k+c) \equiv_{\mathbb{Z}} (a,b)$ ■

Theorem 1.13

$$z + 0 = z \quad \forall\, z \in \mathbb{Z}$$

Proof
$z+0=[(a,b)]+[(1,1)] \overset{\text{D.1.11}}{=} [(a+1,b+1)] \overset{\text{P.1.15}}{=} [(a,b)]=z$ ■

An immediate corollary is the following

Corollary 1.6

Let $z,s \in \mathbb{Z}$

$z=s \iff z+t=s+t \quad \forall t \in \mathbb{Z}$

Proof
$\Longrightarrow)$

By contradiction $\exists\, t_0 \in \mathbb{Z} \mid z+t_0 \neq s+t_0$

By Extensionality we have two options:

$\exists\,(n,m) \in z+t_0 \mid (n,m) \notin s+t_0 \quad$ or $\quad \exists\,(n,m) \in s+t_0 \mid (n,m) \notin z+t_0$

Suppose the first one holds. Then

$(n,m) \in z+t_0 \overset{\text{D.1.11}}{\iff} \exists\,(a,b) \in z,\ \exists\,(c,d) \in t_0 \ \mid\ [(a+c,b+d)]=[(n,m)]$

But since $z=s \Longrightarrow (a,b) \in s \Longrightarrow [(a+c,b+d)]=s+t_0$

Contradiction. Supposing the second one we will get a contradiction too

$\Longleftarrow)$

By contradiction $z \neq s \overset{\text{T.1.13}}{\Longrightarrow} z+0 \neq s+0$

Contradiction

■

Theorem 1.14

$$\forall\, z \in \mathbb{Z} \quad \exists!\ s \in \mathbb{Z} \quad | \quad z+s=0$$

Proof
Let $z=[(a,b)]$

$\Longrightarrow s_z := [(b,a)]$

$z+s_z=[(a,b)]+[(b,a)] \overset{\text{D.1.11}}{=} [(a+b,b+a)] \overset{\text{D.1.11}}{=} [(a+b,a+b)] \overset{\text{D.1.13}}{=} 0$

Let $s_1 \in \mathbb{Z}, \quad z+s_1=0 \quad$ then

$s_1 \overset{\text{T.1.13}}{=} s_1+0 \ = \ s_1+(z+s_z) \overset{\text{T.1.12}}{=} (s_1+z)+s_z=0+s_z \overset{\text{T.1.13}}{=} s_z$ ■

Definition 1.14

Let $z \in \mathbb{Z}$

We call "the opposite of z" the unique element s, given by theorem 1.14, such that $z+s=0$ and we denote it with $-z$

Corollary 1.7

$-(-z)=z \quad \forall\, z \in \mathbb{Z}$

Proposition 1.16

$-(z+s)=(-z)+(-s) \quad \forall\, z,s \in \mathbb{Z}$

Proof
Let $z=[(a,b)]\, s=[(c,d)]$

Then by theorem 1.14 $-z=[(b,a)],\ \ -s=[(d,c)]$ and
$(-z)+(-s)=[(b+d,a+c)] \overset{\text{T.1.14}}{=} -[(a+c,b+d)] \overset{\text{D.1.11}}{=} -(z+s)$ ■

Proposition 1.17

$-z=[(1,2)]*z \quad \forall\, z \in \mathbb{Z}$

Proof
Let $z=[(n,k)]$

$$z+\big([(1,2)]*z\big)=[(n,k)]+\big([(1,2)]*[(n,k)]\big) \overset{\text{D.1.12}}{=} [(n,k)]+[((n1)+(2k),(2n)+(k1))]$$
$$\overset{\text{D.1.11}}{=} [((2n)+(2k)),((2n)+(2k))] \overset{\text{D.1.13}}{=} 0$$
■

Theorem 1.15

$$z*s=s*z \qquad \forall\, z,s \in \mathbb{Z}$$

Proof
Let $z=[(a,b)],\quad s=[(c,d)]$

$$z*s=[(a,b)]*[(c,d)] \overset{\text{D.1.12}}{=} [(ac+bd,ad+bc)]$$
$$\overset{\text{T.1.3}}{=} [(ca+db,da+cb)] \overset{\text{T.1.1}}{=} [(db+ca,cb+da)] \overset{\text{D.1.12}}{=} [(c,d)]*[(a,b)]=s*z$$

■

Theorem 1.16

$$t*(z*s)=(t*z)*s \qquad \forall\, t,z,s \in \mathbb{Z}$$

Proof
Let $t = [(a,b)], \quad z = [(c,d)], \quad s = [(e,f)]$

$$
\begin{aligned}
t*(z*s) = [(a,b)]*([(c,d)]*[(e,f)]) &\overset{\text{D.1.12}}{=} [(a,b)]*[(ce+df, cf+de)] \\
&\overset{\text{D.1.12}}{=} [(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))] \\
&\overset{\text{T.1.4}}{=} [(ace+adf+bcf+bde, acf+ade+bce+bdf)] \\
&\overset{\text{T.1.1}}{=} [(ace+bde+adf+bcf, acf+bdf+ade+bce)] \\
&\overset{\text{T.1.4}}{=} [((ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e)] \\
&\overset{\text{D.1.12}}{=} [(ac+bd, ad+bc)]*[(e,f)] \overset{\text{D.1.12}}{=} ([(a,b)]*[(c,d)])*[(e,f)] = (t*z)*s
\end{aligned}
$$

■

Theorem 1.17

$$z*(s+t) = z*s + z*t \qquad \forall\, z,s,t \in \mathbb{Z}$$

Proof
Let $z = [(a,b)], \quad s = [(c,d)], \quad t = [(e,f)]$

$$
\begin{aligned}
z*(s+t) = [(a,b)]*([(c,d)]+[(e,f)]) &\overset{\text{D.1.11}}{=} [(a,b)]*[(c+e, d+f)] \\
&\overset{\text{D.1.12}}{=} [a(c+e)+b(d+f), a(d+f)+b(c+e)] \\
&\overset{\text{T.1.4}}{=} [(ac+ae+bd+bf, ad+af+be+bc)] \\
&\overset{\text{T.1.11}}{=} [(ac+bd, ad+bc)]+[(ae+bf, af+be)] \\
&\overset{\text{D.1.12}}{=} [(a,b)]*[(c,d)]+[(a,b)]*[(e,f)] = z*s+z*t
\end{aligned}
$$

■

Proposition 1.18

$z*0 = 0 \quad \forall\, z \in \mathbb{Z}$

Proof
Let $z = [(a,b)]$

By definition 1.13 $\quad 0 = [(1,1)]$. And hence
$z*0 = [(a,b)]*[(1,1)] \overset{\text{D.1.12}}{=} [(a+b, a+b)] \overset{\text{P.1.14}}{=} [(1,1)] \overset{\text{D.1.13}}{=} 0$ ■

Proposition 1.19

$-(z*s) = z*(-s) = (-z)*s \quad \forall\, z,s \in \mathbb{Z}$

Proof

$$
\begin{aligned}
z*s+z*(-s) &\overset{\text{P.1.17}}{=} z*s+z*\big([(1,2)]*s\big)\\
&\overset{\text{T.1.16}}{=} z*s+\big(z*[(1,2)]\big)*s \overset{\text{T.1.15}}{=} z*s+\big([(1,2)]*z\big)*s\\
&\overset{\text{T.1.16}}{=} z*s+[(1,2)](z*s) \overset{\text{P.1.17}}{=} 0
\end{aligned}
$$

Then by theorem 1.14 calling $t := z*s$
then $-t = z*(-s)$, and we get the thesis
■

Corollary 1.8

$(-z)*(-s) = z*s \quad \forall\, z,s \in \mathbb{Z}$

Proof
$-(z*s)+(-z)*(-s) \overset{\text{P.1.19}}{=} (-z)*s+(-z)*(-s) \overset{\text{T.1.17}}{=} (-z)*(s+(-s)) \overset{\text{T.1.13}}{=} -z*0 \overset{\text{P.1.18}}{=} 0$

And then calling $s_1 := (-z)*(-s) \implies -s_1 = z+s$

Hence by corollary 1.7 $\quad s_1 = -(z+s)$ ■

Proposition 1.20

$(n+1,n) \equiv_{\mathbb{Z}} (m+1,m) \quad \forall\, n,m \in \mathbb{N}$

Definition 1.15

$1_{\mathbb{Z}} := [(2,1)] = [(n+1,n)] \quad \forall\, n \in \mathbb{N}$

Remark 1.4

$1_{\mathbb{Z}} \neq 0_{\mathbb{Z}}$

Notational Remark 1.10
Henceforth we will avoid this heavy notation and we will denote $1_{\mathbb{Z}}$ simply with 1 avoiding to confuse the element $1 \in \mathbb{N}$ with $1_{\mathbb{Z}}$

Theorem 1.18

$$z*1 = z \qquad \forall\, z \in \mathbb{Z}$$

Proof
Let $z = [(k,m)]$

$$\begin{aligned} z * 1 = [(k,m)] * [(2,1)] &\overset{\text{D.1.12}}{=} [(2k+m, k+2m))] \\ &\overset{\text{T.1.2}}{=} [(k+(k+m), (k+m)+m)] \\ &\overset{\text{P.1.15}}{=} [(k,m)] = z \end{aligned}$$

■

Proposition 1.21

$$\left.\begin{array}{l} (a,b) \equiv_{\mathbb{Z}} (a_1,b_1) \\ (c,d) \equiv_{\mathbb{Z}} (c_1,d_1) \\ a+d \leq b+c \end{array}\right\} \Longrightarrow a_1+d_1 \leq b_1+c_1$$

Proof
$(a,b) \equiv_{\mathbb{Z}} (a_1,b_1) \Longrightarrow a_1+b = a+b_1$
$(c,d) \equiv_{\mathbb{Z}} (c_1,d_1) \Longrightarrow c+d_1 = c_1+d$
Then by corollary 1.2 $\;(a_1+b)+(c+d_1) = (a+b_1)+(c_1+d)$
Now suppose $a_1+d_1 > b_1+c_1 \overset{\text{T.1.10}}{\Longrightarrow} a_1+d_1+(b+c) > b_1+c_1+(b+c)$
On the other side by theorems 1.1 and 1.2
$a_1+d_1+(b+c) = (a_1+b)+(c+d_1) = (a+b_1)+(c_1+d)$
And so we have $(a+b_1)+(c_1+d) > b_1+c_1+(b+c) \overset{\text{T.1.10}}{\Longleftrightarrow} a+d > b+c$
but this is contradiction since $a+d \leq b+c$ ■

In view of proposition 1.21 the following definition is well posed

Definition 1.16

Let $z, s \in \mathbb{Z}$

$z \leq_{\mathbb{Z}} s \Longleftrightarrow (a+d) \leq (b+c)$ where $(a,b) \in z$ and $(c,d) \in s$

Definition 1.17

Let $z, s \in \mathbb{Z}$

$z <_{\mathbb{Z}} s \Longleftrightarrow z \leq s$ and $z \neq s$

Notational Remark 1.11
Henceforth we will denote:

$z <_{\mathbb{Z}} s$ simply as $z < s \quad \forall z, s \in \mathbb{Z}$
$z \leq_{\mathbb{Z}} s$ simply as $z \leq s \quad \forall z, s \in \mathbb{Z}$

Proposition 1.22

Let $z, s \in \mathbb{Z}$

$z < s \iff (a+d) < (b+c)$ where $(a,b) \in z$ and $(c,d) \in s$

Theorem 1.19

$$z \leq z \quad \forall z \in \mathbb{Z}$$

Theorem 1.20

Let $z, s \in \mathbb{Z}$

$$\left.\begin{array}{l} s \leq z \\ z \leq s \end{array}\right\} \Longrightarrow z = s$$

Proof

Let $z = [(a,b)], \quad s = [c,d]$

$s \leq z \iff c + b \leq d + a$

$z \leq s \iff a + d \leq b + c$

And then calling $n = (a+d)$ and $k = (b+c)$

$\overset{\text{T.1.7}}{\Longrightarrow} n = k \Longrightarrow a + d = b + c \iff z = s$ ■

Theorem 1.21

Let $z, z_1, z_2 \in \mathbb{Z}$

$$\left.\begin{array}{l} z \leq z_1 \\ z_1 \leq z_2 \end{array}\right\} \Longrightarrow z \leq z_2$$

Proof

Let $z = [(a,b)], \quad z_1 = [(c,d)], \quad z_2 = [(e,f)]$

$z \leq z_1 \iff a + d \leq b + c$

$z_1 \leq z_1 \iff c + f \leq d + e$

$a + d \leq b + c \overset{\text{T.1.10}}{\iff} (a+d) + f \leq (b+c) + f$

On one side

$(a+d) + f = (a+f) + d$

And on the other side

$(b+c) + f \overset{\text{T.1.2}}{=} b + (c+f) \overset{\text{T.1.10}}{\leq} b + (d+e) = (b+e) + d$

Then $(a+f) + d \leq (b+e) + d$

$\overset{\text{T.1.10}}{\iff} a + f \leq (b+e) \overset{\text{D.1.16}}{\iff} z \leq z_2$ ■

Theorem 1.22

Formulation 1.22.1

$$\forall\, z, s\, \in \mathbb{Z} \quad \text{one and only one of the following holds :} \quad z = s, \quad z < s, \quad z > s$$

Proof

Let $z = [(a, b)], \quad s = [(c, d)]$

Define $n := a + d, \quad k := b + c$

By Theorem 1.9 one and only one of the following relations holds:

$n = k, \quad n < k, \quad k < n$

Hence one and only one of the following holds

$z = s, \quad z < s, \quad s < z$

■

Formulation 1.22.2

$$\forall\, z, s\, \in \mathbb{Z} \Longrightarrow z \leq s \quad \text{or} \quad s \leq z$$

Proof

We omit the proof because the method is the same as the proof just here above,but using the other formulation of theorem 1.9 ■

Proposition 1.23

Let $z \in \mathbb{Z}$

$z > 0 \Longleftrightarrow\ a > b \quad \forall\, (a, b) \in\, z$

Proof

Let $z = [(a, b)]$

By definition 1.13 $\quad 0 = [(1, 1)]$. And hence

$z > 0 \iff [(a, b)] > [(1, 1)] \overset{D.1.17}{\iff} a + 1 > b + 1 \overset{T.1.10}{\iff} a > b$ ■

Corollary 1.9

$1_{\mathbb{Z}} > 0_{\mathbb{Z}}$

Proof

By definition 1.15 $\ 1_{\mathbb{Z}} = [(2, 1)]$ and hence by proposition above it holds ■

Theorem 1.23

Formulation 1.23.1
Let $z, s \in \mathbb{Z}$

$$z < s \Longleftrightarrow z + t < s + t \qquad \forall t \in \mathbb{Z}$$

Proof
$\Longrightarrow$)
Let $z = [(a, b)], \quad s = [(c, d)], \quad t = [(e, f)]$

$$\begin{aligned} z < s &\overset{D.1.17}{\Longleftrightarrow} a + d < b + c \\ &\overset{T.1.10}{\Longleftrightarrow} a + d + (e + f) < b + c + (e + f) \\ &\Longleftrightarrow (a + e) + (d + f) < (c + e) + (b + f) \\ &\overset{D.1.17}{\Longleftrightarrow} [(a + e, b + f)] < [(c + e, d + f)] \overset{D.1.11}{\Longleftrightarrow} z + t < s + t \end{aligned}$$

■

Formulation 1.23.2
Let $z, s \in \mathbb{Z}$

$$z \leq s \Longleftrightarrow z + t \leq s + t \quad \forall t \in \mathbb{Z}$$

Proof
It comes immediately by the first formulation and by corollary 1.6 ■

Corollary 1.10

Let $z \in \mathbb{Z}$

$z > 0 \Longrightarrow -z < 0$

$z < 0 \Longrightarrow -z > 0$

Proof

- $z > 0 \overset{T.1.23}{\Longrightarrow} z + (-z) > 0 + (-z) \overset{T.1.14}{\Longrightarrow} 0 > 0 + (-z) \overset{T.1.13}{\Longrightarrow} 0 > -z$
- $z < 0 \overset{T.1.23}{\Longrightarrow} z + (-z) < 0 + (-z) \overset{T.1.14}{\Longrightarrow} 0 < 0 + (-z) \overset{T.1.13}{\Longrightarrow} 0 < -z$

■

Proposition 1.24

$$(n + 1) + (m + 1) < (n + 1)(m + 1) + 1 \quad \forall n, m \in \mathbb{N}$$

Proof

- $m = 1$
  $(n+1)+1+1 \overset{\text{C.1.4}}{<} n+1+(n+1)+1 \overset{\text{D.1.5}}{=} (n+1)*1+(n+1)*1+1 \overset{\text{T.1.4}}{=} (n+1)*(1+1)+1$
- Supposed for m we show it for $m+1$
  $(n+1)+((m+1)+1) \overset{\text{T.1.2}}{=} ((n+1)+(m+1))+1 \overset{I.S.}{<} ((n+1)(m+1)+1)+1$
  $\overset{\text{C.1.4}}{<} ((n+1)(m+1)+(n+1))+1 \overset{\text{T.1.4}}{=} (n+1)((m+1)+1)+1$

■

Proposition 1.25

Let $z \in \mathbb{Z}$

$z \geq 0 \iff \exists! \quad c \in \mathbb{N} \quad | \quad z = [(c,1)]$

Proof

$\Longrightarrow)$

- If $z = 0$
  $\Longrightarrow c = 1$ by definition 1.13
- If $z > 0$
  By proposition 1.23 $z = [(a,b)]$ with $a > b$
  $a > b \overset{\text{D.1.6}}{\iff} \exists l \in \mathbb{N}$ with $b + l = a$
  - if $l = 1 \implies z = [(b+1,b)]$
    $c := 2 \qquad (c > 1)$ and in fact
    $(b+1)+1 \overset{\text{T.1.2}}{=} b+(1+1) = b+c \overset{\text{D.1.9}}{\iff} (b+1,b) \equiv_{\mathbb{Z}} (c,1)$
  - if $l > 1 \overset{\text{C.1.1}}{\Longrightarrow} l = k+1 \implies z = [(b+(k+1),b)]$
    $c := (k+1)+1 \qquad (c > 1)$ and in fact
    $(b+(k+1))+1 \overset{\text{T.1.2}}{=} b+((k+1)+1) = b+c \overset{\text{D.1.9}}{\iff} (b+(k+1),b) \equiv_{\mathbb{Z}} (c,1)$

The uniqueness of c is trivial and we omit to prove it

$\Longleftarrow)$

$z := [(c,1)]$ with $c \in \mathbb{N}$

- if $c = 1$
  $\Longrightarrow z = [(1,1)] \overset{\text{D.1.13}}{=} 0$
- if $c > 1 \overset{\text{P.1.23}}{\Longrightarrow} z > 0$

■

Corollary 1.11

Let $z \in \mathbb{Z}$

$z > 0 \iff z \geq 1$

Proof

$\Longrightarrow)$

By proposition above $z > 0 \Longrightarrow z = [(m, 1)]$ with $m > 1$

$\overset{C.1.1}{\Longrightarrow} m = k + 1 \Longrightarrow z = [(k + 1, 1)]$

- if $k = 1 \Longrightarrow z = [(2, 1)] \overset{D.1.15}{\Longrightarrow} z = 1$
- if $k > 1$
  $k > 1 \overset{T1.10}{\iff} k + 2 > 1 + 2 \overset{T1.2}{\iff} (k + 1) + 1 > 2 + 1 \overset{D.1.17}{\iff} [(k + 1, 1)] > [(2, 1)]$
  Hence $z > 1$

$\Longleftarrow)$

By corollary 1.9 $1 > 0$.

Furthermore if $z > 1 \overset{T.1.21}{\Longrightarrow} z > 0$ ■

Theorem 1.24

Formulation 1.24.1

$$z > 0, \quad s > 0 \Longrightarrow z * s > 0 \qquad \forall\, z, s \in \mathbb{Z}$$

Proof

By proposition 1.25

Let $z = [(a, 1)]$, $s = [(b, 1)]$ with $a,\ b > 1$

$z * s > 0 \overset{D.1.12}{\iff} [(ab + 1, a + b)] > 0 \overset{P.1.23}{\iff} a + b < ab + 1$

But this is true by proposition 1.24 ■

Formulation 1.24.2

$$z \geq 0, \quad s \geq 0 \Longrightarrow z * s \geq 0 \qquad \forall\, z, s \in \mathbb{Z}$$

Proof

- if $z, s > 0$ $\quad z * s > 0$ by the first formulation
- if $z = 0$ or $s = 0$
  by proposition 1.18 $z * s = 0 \Longrightarrow z * s \geq 0$

■

Proposition 1.26

$z > z_1 \quad s > 0 \Longrightarrow z * s > z_1 * s \quad \forall\, z, z_1, s\ \in \mathbb{Z}$

Proof

$$z > z_1 \overset{\text{T.1.23}}{\Longrightarrow} z + (-z_1) > 0 \overset{\text{T.1.24}}{\Longrightarrow} s * (z + (-z_1)) > 0$$
$$\overset{\text{T.1.17}}{\Longrightarrow} s * z + s * (-z_1) > 0 \overset{\text{P.1.19}}{\Longrightarrow} s * z + -(s * z_1) > 0$$
$$\overset{\text{T.1.23}}{\Longrightarrow} z * s > z_1 * s$$

■

Corollary 1.12

Let $z \in \mathbb{Z}$

$z \neq 0 \Longrightarrow z * z > 0$

Proof

- $z > 0 \overset{\text{T.1.24}}{\Longrightarrow} z * z > 0$
- $z < 0 \overset{\text{C.1.10}}{\Longrightarrow} -z > 0 \overset{\text{T.1.24}}{\Longrightarrow} (-z) * (-z) > 0$
  But by corollary 1.8 $(-z) * (-z) = z * z$

■

Immersion Theorem 1.1 ($\mathbb{N} \hookrightarrow \mathbb{Z}$)

We have just built $\Big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, <_{\mathbb{Z}}\Big)$ from $\Big(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, <_{\mathbb{N}}\Big)$.

Now we will show that in $\Big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, <_{\mathbb{Z}}\Big)$ there exists a copy of $\Big(\mathbb{N},\, +_{\mathbb{N}},\, *_{\mathbb{N}},\, <_{\mathbb{N}}\Big)$.
To be more precise we will show that exist $J : \mathbb{N} \longrightarrow \mathbb{Z}$ such that:

1. J is injective
2. $J(n +_{\mathbb{N}} m) = J(n) +_{\mathbb{Z}} J(m) \quad \forall\, n, m \in \mathbb{N}$
3. $J(n *_{\mathbb{N}} m) = J(n) *_{\mathbb{Z}} J(m) \quad \forall\, n, m \in \mathbb{N}$
4. $n <_{\mathbb{N}} m \iff J(n) <_{\mathbb{Z}} J(m) \quad \forall\, n, m \in \mathbb{N}$
5. $z \in J(\mathbb{N}) \iff z > 0$

In this way $\left(J(\mathbb{N}),\ +_{\mathbb{Z}_{|_{J(\mathbb{N})}}},\ *_{\mathbb{Z}_{|_{J(\mathbb{N})}}},\ <_{\mathbb{Z}_{|_{J(\mathbb{N})}}}\right)$ "is a copy" of $\mathbb{N}$ in $\mathbb{Z}$.

In other words in the system $\mathbb{Z}$, $\mathbb{N}$ exists , no more like a construction on a system of Axioms, but like a subset of a builded set $\mathbb{Z}$ .We could say that $\mathbb{N}$ "really exists" in $\mathbb{Z}$. This mechanism of proving the existence of system S_0 in a more complex system S_1 is the most important step in the reduction program we spoke in the Introduction. In the foundational context(talking about rigorization, correctness,systematic clarification) this mechanism is the key.

Let $n \in \mathbb{N}$, $\quad J(n) := [(n+1,1)]$

1. $J(n) = J(m) \iff [(n+1,1)] = [(m+1,1)]$
$$\stackrel{\text{D.1.9}}{\iff} (n+1)+1 = (m+1)+1$$
$$\stackrel{\text{T.1.2}}{\iff} n+(1+1) = m+(1+1)$$
$$\stackrel{\text{C.1.2}}{\iff} n = m$$

2. $J(n +_{\mathbb{N}} m) = [((n+m)+1,1)] \stackrel{\text{P.1.15}}{=} [((n+m)+1+1, 1+1)]$
$$= [(n+1)+(m+1), 1+1] \stackrel{\text{D.1.11}}{=} [n+1,1]+[m+1,1]$$
$$= J(n) +_{\mathbb{Z}} J(m)$$

3. $J(n *_{\mathbb{N}} m) = [((n*m)+1,1)]$
$$\stackrel{\text{P.1.15}}{=} [((n*m)+1+(n+m+1), 1+(n+m+1))]$$
$$= [(((n+1)*(m+1))+1, (n+1)+(m+1))]$$
$$\stackrel{\text{D.1.12}}{=} [(n+1,1)]*[(m+1,1)] = J(n) *_{\mathbb{Z}} J(m)$$

4. $n < m \stackrel{\text{T1.10}}{\iff} n+2 < m+2 \stackrel{\text{T1.2}}{\iff} (n+1)+1 < (m+1)+1$
$$\stackrel{\text{D.1.17}}{\iff} [(n+1,1)] < [(m+1,1)] \iff J(n) < J(m)$$

5. $z \in J(\mathbb{N}) \iff z > 0:$

$\Longrightarrow)$

$z = J(n) \implies z = [(n+1,1)]$

Then calling $c := n+1 \Longrightarrow z = [(c,1)]$ with $c > 1$

and hence looking at proposition 1.25 we get the thesis

$\Longleftarrow)$

$z > 0 \stackrel{\text{P.1.25}}{\Longrightarrow} \exists c \in \mathbb{N},$ such that $z = [(c,1)],$ with $c > 1 \stackrel{\text{C.1.1}}{\Longrightarrow} c = k+1$

Hence $z = [(k+1,1)] = J(k)$

1.2.1 Remarks and Complements

Remark 1.5 About arbitrary choices on building $\mathbb{Z}$

At the begin of this section , we defined $+_{\mathbb{Z}}, *_{\mathbb{Z}}, \leq_{\mathbb{Z}}$ and we proved the results holding for them , choosing an arbitrary element in each equivalence class $z \in \mathbb{Z}$.

As opposite of this method we could select, using only the Minimum principle of $\mathbb{N}$, a privileged representant as follows:

1. Show that $\begin{cases} (n,m) \equiv_{\mathbb{Z}} (n,k) \implies m = k & \forall\, n,m,k \in \mathbb{N} \\ (n,m) \equiv_{\mathbb{Z}} (k,m) \implies n = k & \forall\, n,m,k \in \mathbb{N} \end{cases}$
2. Let $z \in \mathbb{Z}$ We define $\begin{cases} PP(z) := \{n \in \mathbb{N} \mid \exists\, m \in \mathbb{N} \text{ s.t. } (n,m) \in z\} \\ NP(z) := \{m \in \mathbb{N} \mid \exists\, n \in \mathbb{N} \text{ s.t. } (n,m) \in z\} \end{cases}$
3. Define $n_z := \min PP(z)$ and $m_z := \min NP(z)$
4. $\forall\, z \in \mathbb{Z} \quad (n_z, k) \in z \implies k = m_z$
5. We define $CH_{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{N} \times \mathbb{N}$ as follows
   $CH_{\mathbb{Z}} f(z) := (n_z, m_z)$

In this way we could define $+_{\mathbb{Z}}, *_{\mathbb{Z}}, \leq_{\mathbb{Z}}$ and prove all the their results without choosing any arbitrary element as representant of the equivalence classes involved in definitions or in proofs.

Thus no arbitrary choices occur to build $\mathbb{Z}$

1.3 Construction of the Rational Numbers $\mathbb{Q}$

Definition 1.18

$\big($a set $\mathbb{Q}$, $+_{\mathbb{Q}}$, $*_{\mathbb{Q}}\big)$is a Field
if and only if satisfies these properties :

(s_1) $q +_{\mathbb{Q}} p = p +_{\mathbb{Q}} q \qquad \forall\, q, p \in \mathbb{Q}$

(s_2) $(q +_{\mathbb{Q}} p) +_{\mathbb{Q}} t = q +_{\mathbb{Q}} (p +_{\mathbb{Q}} t) \qquad \forall\, q, p, t \in \mathbb{Q}$

(s_3) $\exists\, 0 \in \mathbb{Q} \mid q +_{\mathbb{Q}} 0 = q \qquad \forall\, f \in \mathbb{Q}$

(s_4) $\forall\, q \in \mathbb{Q} \quad \exists -q \in \mathbb{Q} \mid q +_{\mathbb{Q}} (-q) = 0$

(p_1) $q *_{\mathbb{Q}} p = p *_{\mathbb{Q}} q \qquad \forall\, q, p \in \mathbb{Q}$

(p_2) $q *_{\mathbb{Q}} (p *_{\mathbb{Q}} t) = (q *_{\mathbb{Q}} p) *_{\mathbb{Q}} t \qquad \forall\, q, p, t \in \mathbb{Q}$

(p_3) $\exists\, 1 \in \mathbb{Q} \;\mid q *_{\mathbb{Q}} 1 = q \qquad \forall\, q \in \mathbb{Q}$

(p_4) $\forall\, q \in \mathbb{Q},\, q \neq 0 \quad \exists\, q^{-1} \in \mathbb{Q},\, q^{-1} \neq 0 \;\mid q *_{\mathbb{Q}} q^{-1} = 1$

(sp) $q *_{\mathbb{Q}} (p +_{\mathbb{Q}} t) = q *_{\mathbb{Q}} p +_{\mathbb{Q}} q *_{\mathbb{Q}} t \qquad \forall\, q, p, t \in \mathbb{Q}$

Definition 1.19

$\big($a set $\mathbb{Q}$, $+_{\mathbb{Q}}$, $*_{\mathbb{Q}}$, $\leq_{\mathbb{Q}}$ $\big)$is an Ordered Field (OF)
if and only if satisfies these properties:

$\big(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}}\big)$is a Field

(o_1) $\leq_{\mathbb{Q}}$ is a reflexive relation on $\mathbb{Q}$

(o_2) $\leq_{\mathbb{Q}}$ is an antisymmetric relation on $\mathbb{Q}$

(o_3) $\leq_{\mathbb{Q}}$ is a transitive relation on $\mathbb{Q}$

(o_4) $\leq_{\mathbb{Q}}$ is a total relation on $\mathbb{Q}$

(so) Let $q, p \in \mathbb{Q}$

$$q \leq_{\mathbb{Q}} p \iff q +_{\mathbb{Q}} t \leq_{\mathbb{Q}} p +_{\mathbb{Q}} t \quad \forall\, t \in \mathbb{Q}$$

(po) $q \geq_{\mathbb{Q}} 0,\, p \geq_{\mathbb{Q}} 0 \implies q *_{\mathbb{Q}} p \geq_{\mathbb{Q}} 0$

Aim of Section 1.3

In this section we will show the following results:
Given an Ordered Integrity Domain $\big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, \leq_{\mathbb{Z}}\big)$
there exists an OF $\big(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}},\, \leq_{\mathbb{Q}}\big)$ which contains a copy of $\big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, \leq_{\mathbb{Z}}\big)$

Notational Remark 1.12
In this Section we will denote
$z +_{\mathbb{Z}} s$ simply as $z + s \quad \forall\, z, s \in \mathbb{Z}$
$z *_{\mathbb{Z}} s$ simply as $zs \quad \forall\, z, s \in \mathbb{Z}$
$z \leq_{\mathbb{Z}} s$ simply as $z \leq s \quad \forall\, z, s \in \mathbb{Z}$
$z <_{\mathbb{Z}} s$ simply as $z < s \quad \forall\, z, s \in \mathbb{Z}$

Definition 1.20

$\mathbb{Z}_+ := J(\mathbb{N}) = \{z \in \mathbb{Z} \mid z > 0\}$[4]

[4]See Immersion Theorem 1.1

Definition 1.21

Let $(z,s),(z_1,s_1) \in \mathbb{Z}\times\mathbb{Z}_+$
$(z,s) \equiv_{\mathbb{Q}} (z_1,s_1) \Longleftrightarrow zs_1 = z_1 s$

Proposition 1.27

$\equiv_{\mathbb{Q}}$ is an equivalence relationship on $\mathbb{Z}\times\mathbb{Z}_+$

Definition 1.22

$\mathbb{Q} := \frac{\mathbb{Z}\times\mathbb{Z}_+}{\equiv_{\mathbb{Q}}}$

Proposition 1.28

Let $(z,s),(z_1,s_1),(t,w),(t_1,w_1) \in \mathbb{Z}\times\mathbb{Z}_+$

$$\left.\begin{array}{l}(z,s)\equiv_{\mathbb{Q}}(z_1,s_1)\\(t,w)\equiv_{\mathbb{Q}}(t_1,w_1)\end{array}\right\} \Longrightarrow (zw+st,sw)\equiv_{\mathbb{Q}}(z_1w_1+s_1t_1,s_1w_1)$$[5]

Proof
$(z,s)\equiv_{\mathbb{Q}}(z_1,s_1) \overset{\text{D.1.21}}{\Longleftrightarrow} z\,s_1 = s\,z_1 \Longrightarrow (z\,s_1)(w\,w_1) = (s\,z_1)(w\,w_1)$
On the other hand
$(t,w)\equiv_{\mathbb{Q}}(t_1,w_1) \overset{\text{D.1.21}}{\Longleftrightarrow} t\,w_1 = w\,t_1 \Longrightarrow (t\,w_1)(s\,s_1) = (w\,t_1)(s\,s_1)$
If we sum the two equations we get
$(z\,s_1)(w\,w_1) + (t\,w_1)(s\,s_1) = (s\,z_1)(w\,w_1) + (w\,t_1)(s\,s_1)$
Let us apply theorem 1.17 on the two members
$(z\,w + t\,s)(w_1\,s_1) = (z_1\,w_1 + t_1\,s_1)(s\,w) \overset{\text{D.1.21}}{\Longleftrightarrow} (zw+st,sw)\equiv_{\mathbb{Q}}(z_1w_1+s_1t_1,s_1w_1)$ ■

In view of proposition 1.28 the following definition is well posed

Definition 1.23

Let $p,q \in \mathbb{Q}$
$p +_{\mathbb{Q}} q := [(zw+st,sw)]$ where $(z,s)\in p$ and $(t,w)\in q$

Remark 1.6

Let $(z,s),(t,w) \in \mathbb{Z}\times\mathbb{Z}_+$
Since $s,w>0 \overset{\text{T.1.24}}{\Longrightarrow} sw>0$. Hence $(zt,sw) \in \mathbb{Z}\times\mathbb{Z}_+$

[5] Since $s,w>0 \overset{\text{T.1.24}}{\Longrightarrow} sw>0 \Longrightarrow (zw+st,sw) \in \mathbb{Z}\times\mathbb{Z}_+$

Proposition 1.29

Let $(z,s),(z_1,s_1),(t,w),(t_1,w_1) \in \mathbb{Z}\times\mathbb{Z}_+$

$$\left.\begin{array}{l}(z,s)\equiv_{\mathbb{Q}}(z_1,s_1)\\(t,w)\equiv_{\mathbb{Q}}(t_1,w_1)\end{array}\right\}\Longrightarrow (zt,sw)\equiv_{\mathbb{Q}}(z_1t_1,s_1w_1)$$

Proof

$(z,s)\equiv_{\mathbb{Q}}(z_1,s_1)\overset{\text{D.1.21}}{\Longleftrightarrow} z\,s_1 = s\,z_1$

On the other hand

$(t,w)\equiv_{\mathbb{Q}}(t_1,w_1)\overset{\text{D.1.21}}{\Longleftrightarrow} t\,w_1 = w\,t_1 \Longrightarrow (t\,w_1)(z\,s_1) = (w\,t_1)(s\,z_1)$

Let us apply theorems 1.16 and 1.15 on the two members

$(z\,t)(w_1\,s_1) = (z_1\,t_1)(w\,s)\overset{\text{D.1.21}}{\Longleftrightarrow}(zt,sw)\equiv_{\mathbb{Q}}(z_1t_1,s_1w_1)$ ∎

In view of proposition 1.29 the following definition is well posed

Definition 1.24

Let $p,q \in \mathbb{Q}$

$p*q := [(zt,sw)]$ where $(z,s)\in p$ and $(t,w)\in q$

Notational Remark 1.13

Henceforth we will denote:

$p+_{\mathbb{Q}}q$ simply as $p+q \quad \forall\, p,q \in \mathbb{Q}$
$p*_{\mathbb{Q}}q$ simply as $p*q \quad \forall\, p,q \in \mathbb{Q}$

Corollary 1.13

Let $(t,w),(t_1,w_1) \in \mathbb{Z}\times\mathbb{Z}_+$

$$\left.\begin{array}{l}(t,w)\equiv_{\mathbb{Q}}(t_1,w_1)\\t>0\end{array}\right\}\Longrightarrow t_1>0$$

Proof

$(t,w)\equiv_{\mathbb{Q}}(t_1,w_1)\Longrightarrow tw_1 = t_1w$

By theorem 1.24 $tw_1>0$. Hence $t_1w>0$

By contradiction $t_1<0 \overset{\text{C.1.10}}{\Longrightarrow} -t_1>0 \overset{\text{T.1.24}}{\Longrightarrow} -t_1w>0$

Contradiction by corollary 1.10 ∎

Theorem 1.25

$$p+q = q+p \qquad \forall\, p,q \in \mathbb{Q}$$

Proof
Let $p = [(t, w)]$, $q = [(z, s)]$

$$p + q = [(t, w)] + [(z, s)] \overset{\text{D.1.23}}{=} [(ts + wz, ws)] \overset{\text{T.1.15}}{=} [(st + zw, sw)]$$
$$\overset{\text{T.1.11}}{=} [(zw + st, sw)] \overset{\text{D.1.23}}{=} [(z, s)] + [(t, w)] = q + p$$

■

Theorem 1.26

$$p + (q + t) = (p + q) + t \qquad \forall\, p, q, t \in \mathbb{Q}$$

Proof
Let $p = [(t, w)]$, $\quad w = [(z, s)]$, $\quad t = [(a, b)]$

$$\begin{aligned} p + (q + t) &= [(t, w)] + \big([(z + s)] + [(a, b)]\big) \\ &\overset{\text{D.1.23}}{=} [(t, w)] + [(zb + as, sb)] \\ &\overset{\text{D.1.23}}{=} [(t(sb) + w(zb + as), w(sb))] \\ &\overset{\text{T.1.17}}{=} [(t(sb) + w(zb) + q(as), w(sb))] \\ &\overset{\text{T.1.17}}{=} [((ts)b + (wz)b + (ws)a, (ws)b)] \\ &\overset{\text{T.1.17}}{=} [((ts + wz)b + (ws)a, (ws)b)] \\ &\overset{\text{D.1.23}}{=} [(ts + wz, ws)] + [(a, b)] \\ &\overset{\text{D.1.23}}{=} \big([(p, q)] + [(z + s)]\big) + [(a, b)] = (p + q) + t \end{aligned}$$

■

Proposition 1.30

$(0, z) \equiv_{\mathbb{Q}} (0, 1) \quad \forall\, z \in \mathbb{Z}_+$

Proof
By proposition 1.18 $z * 0 = 0 \quad \forall\, z \in \mathbb{Z}$

Hence $0 * z = 0 * 1 \overset{\text{D.1.21}}{\iff} (0, z) \equiv_{\mathbb{Q}} (0, 1) \quad \forall\, z \in \mathbb{Z}$ ■

Definition 1.25

$0_{\mathbb{Q}} := [(0, 1)] \overset{\text{P.1.30}}{=} [(0, z)] \quad \forall\, z \in \mathbb{Z}_+$

Notational Remark 1.14
Henceforth we will avoid this heavy notation and we will denote $0_{\mathbb{Q}}$ simply with 0

Proposition 1.31

Let $(z, s) \in \mathbb{Z} \times \mathbb{Z}_+$

$(zt, st) \equiv_{\mathbb{Q}} (z, s) \quad \forall\, t \in \mathbb{Z}_+$

Theorem 1.27

$$q + 0 = q \qquad \forall\, q \in \mathbb{Q}$$

Proof

Let $q = [(z, s)]$

$$q + 0 = [(z, s)] + [(0, 1)] \overset{\text{D.1.23}}{=} [((z1) + (s0), (s1))] \overset{\text{P.1.18}}{=} [(z1, s1)] \overset{\text{T.1.13}}{=} [(z, s)] = q$$

■

An immediate corollary is the following

Corollary 1.14

Let $p, q \in \mathbb{Q}$

$p = q \Longleftrightarrow p + t = q + t \quad \forall\, t \in \mathbb{Q}$

Proof

$\Longrightarrow$)

By contradiction $\exists\, t_0 \in \mathbb{Q} \mid p + t_0 \neq q + t_0$

By Extensionality we have two options:

$\exists\,(z, s) \in p + t_0 \mid (z, s) \notin p + t_0 \quad$ or $\quad \exists\,(z, s) \in p + t_0 \mid (z, s) \notin q + t_0$

Suppose the first one holds. Then

$(z, s) \in p + t_0 \overset{\text{D.1.23}}{\Longleftrightarrow} \exists\,(a, b) \in p,\ \exists\,(c, d) \in t_0 \mid [(ad + bc, bd)] = [(z, s)]$

But since $p = q \Longrightarrow (a, b) \in q, \Longrightarrow [(ad + bc, bd)] = q + t_0$

Contradiction. Supposing the second one we will get a contradiction too

$\Longleftarrow$)

By contradiction $p \neq q \overset{\text{T.1.27}}{\Longrightarrow} p + 0 \neq q + 0$

Contradiction

■

Theorem 1.28

$$\forall\, q \in \mathbb{Q} \quad \exists!\ p \in \mathbb{Q} - \{0\} \quad \text{such that} \quad q + p = 0$$

Proof
Let $q = [(z,s)]$ Then if we define $p := [(-z,s)]$

$$q + p = [(z,s)] + [(-z,s)] \stackrel{\text{D.1.23}}{=} [((zs) + (s(-z)), ss)] \stackrel{\text{P.1.19}}{=} [((zs) - (sz), sz)]$$
$$\stackrel{\text{T.1.16}}{=} [((zs) - (zs), ss)] \stackrel{\text{T.1.14}}{=} [0, ss)] \stackrel{\text{D.1.25}}{=} 0$$

Furthermore let $w \in \mathbb{Q}$ with $q + w = 0$
$w \stackrel{\text{T.1.13}}{=} w + 0 = w + (q + p) \stackrel{\text{T.1.12}}{=} (w + q) + p = 0 + p \stackrel{\text{T.1.13}}{=} p$ ■

Definition 1.26

Let $q \in \mathbb{Q}$
We call "the opposite of q" the unique element p such that $q + p = 0$
given by this theorem and we denote it by $-q$

Proposition 1.32

$-(p+q) = (-p) + (-q) \quad \forall\, p, q \in \mathbb{Q}$

Proof
Let $p = [(a,b)],\ q = [(c,d)] \stackrel{\text{T.1.14}}{\Longrightarrow} -p = [(-a,b)],\ -q = [(-c,d)]$

$$(-p) + (-q) = [(((-a)d) + (b(-c)), bd)] \stackrel{\text{P.1.19}}{=} [((-(ad)) - (bc), bd)]$$
$$\stackrel{\text{P.1.16}}{=} [(-((ad) + (bc)), bd)]$$
$$\stackrel{\text{T.1.28}}{=} -[((ad) + (bc), bd)] \stackrel{\text{D.1.23}}{=} -(p+q)$$

■

Notational Remark 1.15
We use notation $p - q$ instead of $p + (-q)$
Thus we could extend notation $-p - q$ instead of $(-p) + (-q)$

Theorem 1.29

$$q * p = p * q \qquad \forall\, q, p \in \mathbb{Q}$$

Proof
Let $q = [(a,b)], \quad p = [(c,d)]$

$$q * p = [(a,b)] * [(c,d)] \stackrel{\text{D.1.24}}{=} [(ac, bd)] \stackrel{\text{T.1.15}}{=} [(ca, db)] \stackrel{\text{D.1.24}}{=} [(c,d)] * [(a,b)] = s * q$$

■

Theorem 1.30

$$p * (q * h) = (p * q) * h \quad \forall\, p, q, h \in \mathbb{Q}$$

Proof
Let $q = [(a,b)], \quad p = [(c,d)], \quad h = [(e,f)]$

$$p * (q * h) = [(a,b)] * \big([(c,d)] * [(e,f)]\big) \overset{\text{D.1.24}}{=} [(a,b)] * [(ce,df)]$$
$$\overset{\text{D.1.24}}{=} [(a(ce), b(df))] \overset{\text{T.1.16}}{=} [((ac)e, (bd)f)]$$
$$\overset{\text{D.1.24}}{=} [(ac,bd)] * [(e,f)] \overset{\text{D.1.24}}{=} \big([(a,b)] * [(c,d)]\big) * [(e,f)] = (p * q) * h$$

■

Proposition 1.33

$$-(p * q) = p * (-q) = (-p) * q \quad \forall\, p, q \in \mathbb{Q}$$

Proof
Let $p = [(a,b)], \quad q = [(c,d)]$

$$p * q + p * (-q) = [(a,b)] * [(c,d)] + [(a,b)] * [(-c,d)]$$
$$\overset{\text{D.1.24}}{=} [(ac,bd)] + [(a(-c),bd)]$$
$$\overset{\text{P.1.19}}{=} [(ac,bd)] + [(-(ac),bd)]$$
$$\overset{\text{D.1.23}}{=} [((ac)(bd) + -(ac)(bd), (bd)(bd))]$$
$$\overset{\text{P.1.19}}{=} [((ac)(bd) - ((ac)(bd)), bdbd)] \overset{\text{T.1.14}}{=} [(0, bdbd] \overset{\text{D.1.25}}{=} 0$$

■

Proposition 1.34

$$q * 0 = 0 \quad \forall\, q \in \mathbb{Q}$$

Proof
Let $q = [(a,b)]$
By definition 1.25 $\quad 0 = [(0,1)]$
$q * 0 = [(a,b)] * [(0,1)] \overset{\text{D.1.24}}{=} [(a0, b1)] \overset{\text{P.1.18}}{=} [(0,b)] \overset{\text{P.1.30}}{=} [(0,1)] \overset{\text{D.1.25}}{=} 0$ ■

Corollary 1.15

$$(-p) * (-q) = p * q \quad \forall\, p, q \in \mathbb{Q}$$

Proof
$-(p * q) + (-p) * (-q) \overset{\text{P.1.33}}{=} (-p) * q + (-p) * (-q) \overset{\text{T.1.37}}{=} (-p) * (q + (-q)) \overset{\text{T.1.27}}{=} -q * 0 \overset{\text{P.1.34}}{=} 0$
Thus calling $t := (-p) * (-q)$ then $-t = p * q$
and by uniqueness of the opposite $t = p * q$ ■

Proposition 1.35

$$[(z,z)] \equiv_{\mathbb{Q}} [(s,s)] \quad \forall\, z, s > 0$$

After this proposition,and reminding that $1_{\mathbb{Z}} > 0_{\mathbb{Z}}$, we are allowed to define

Definition 1.27

$1_{\mathbb{Q}} := [(1,1)] \overset{\text{P.1.35}}{=} [(z,z)] \quad \forall\, z\, > 0$

Remark 1.7

$1_{\mathbb{Q}} \neq 0_{\mathbb{Q}}$

Henceforth we will denote $1_{\mathbb{Q}}$ simply with 1

Theorem 1.31

$$q * 1 = q \qquad \forall\, q\, \in \mathbb{Q}$$

Proof

Let $q = [(z,s)]$

$q * 1 = [(z,s)] * [(1,1)] \overset{\text{D.1.24}}{=} [(z1, s1)] \overset{\text{T.1.18}}{=} [(z,s)] = q$ ■

Theorem 1.32

$$\forall\, q \in \mathbb{Q} - \{\, 0\,\} \quad \exists !\; p \in \mathbb{Q} - \{\, 0\,\} \quad \text{such that} \quad q * p = 1$$

Proof

Let $q = [(a,b)]$ $\qquad$ ($a \neq 0$ otherwise $q = 0$ for proposition 1.30)

Hence by theorem 1.22 we have to cases for a : $a > 0$ or $a < 0$

- $a > 0$

  $\Longrightarrow p := [(b,a)]$ $\qquad$ (since $b > 0 \implies p \neq 0$)

  $q * p = [(a,b)] * [(b,a)] \overset{\text{D.1.24}}{=} [(ab, ba)]$

  On the other hand

  $b > 0$ hence by theorem 1.24 $\quad ab > 0$

  Hence $[(ab, ba)] \overset{\text{D.1.27}}{=} 1$

- $a < 0$

  $\Longrightarrow p := [(-b, -a)]$ $\qquad$ (since $(-b) > 0 \implies p \neq 0$)

  $q * p = [(a,b)] * [(-b,-a)] \overset{\text{D.1.24}}{=} [(a(-b), b(-a))] \overset{\text{P.1.19}}{=} [(-ab, -ba)]$

  On the other hand

  $b > 0$ hence by theorem 1.24 $\quad (-a)b > 0$

  Hence $[((-a)b, (-a)b)] \overset{\text{P.1.19}}{=} [(-ab, -ba)] \overset{\text{D.1.27}}{=} 1$

Furthermore let $w \in \mathbb{Q} - \{0\}$ with $q * w = 1$

$w \overset{T.1.31}{=} w * 1 = w * (q * p) \overset{T.1.30}{=} (w * q) * p = 1 * p \overset{T.1.31}{=} p$ ■

Definition 1.28

Let $q \in \mathbb{Q} - \{0\}$

We call "the inverse of q" the unique element p such that $q * p = 1$ given by theorem 1.14 and we denote it q^{-1}

Proposition 1.36

Let $(a, b), (a_1, b_1), (c, d), (c_1, d_1) \in \mathbb{Z} \times \mathbb{Z}_+$

$$\left.\begin{array}{l} (a, b) \equiv_{\mathbb{Q}} (a_1, b_1) \\ (c, d) \equiv_{\mathbb{Q}} (c_1, d_1) \\ ad \leq bc \end{array}\right\} \Longrightarrow a_1 d_1 \leq b_1 c_1$$

Proof

$(a, b) \equiv_{\mathbb{Q}} (a_1, b_1) \Longrightarrow ab_1 = a_1 b$

$(c, d) \equiv_{\mathbb{Q}} (c_1, d_1) \Longrightarrow cd_1 = c_1 d$

Looking now this elements of $\mathbb{Z}$

$z := ((a_1 d_1) - (b_1 c_1))(aa)(bb)(cc)(dd)$

A few of considerations :

$$\left.\begin{array}{l} bb_1 > 0 \quad \text{By theorem 1.24} \\ (aa), (cc_1), (dd) \geq 0 \quad \text{By corollaries 1.13 and 1.12} \\ ad \leq bc \overset{T.1.23}{\Longrightarrow} (ad) - (bc) \leq 0 \end{array}\right\} \overset{T.1.24}{\Longrightarrow} z \leq 0$$

Using theorems 1.15 , 1.16 and 1.17 it follows that

$z = ((ad) - (bc))(aa)(bb_1)(cc_1)(dd)$

But since corollary 1.12 $(aa), (bb), (cc), (dd) \geq 0$

by theorem 1.24 we obtain $((a_1 d_1) - (b_1 c_1)) \leq 0$

■

In view of proposition 1.36 the following definition is well posed

Definition 1.29

Let $p, q \in \mathbb{Q}$

$p \leq_{\mathbb{Q}} q \Longleftrightarrow ad \leq bc$ where $(a, b) \in p$ and $(c, d) \in q$

Definition 1.30

Let $p, q \in \mathbb{Q}$

$p <_{\mathbb{Q}} q \iff p \leq_{\mathbb{Q}} q$ and $p \neq q$

Notational Remark 1.16
Henceforth we will denote:

$p \leq_{\mathbb{Q}} q$ simply as $p \leq q \quad \forall\, p, q \in \mathbb{Q}$
$p <_{\mathbb{Q}} q$ simply as $p < q \quad \forall\, p, q \in \mathbb{Q}$

Theorem 1.33

$$q \leq q \qquad \forall\, q \in \mathbb{Q}$$

Theorem 1.34

$$\left.\begin{array}{l} p \leq q \\ q \leq p \end{array}\right\} \Longrightarrow p = q$$

Proof
Let $p = [(a, b)], \quad q = [c, d]$

$p \leq q \iff ad \leq bc$

$q \leq p \iff bc \leq ad$

And then calling $z = ad$ and $s = bc$

$\overset{\text{T.1.20}}{\Longrightarrow} z = s \Longrightarrow ad = bc \iff p = q$ ■

Theorem 1.35

$$\left.\begin{array}{l} q \leq q_1 \\ q_1 \leq q_2 \end{array}\right\} \Longrightarrow q \leq q_2$$

Proof
Let $q = [(a, b)], \quad q_1 = [c, d], \quad q_2 = [(e, f)]$

$q \leq q_1 \iff ad \leq bc$

$q_1 \leq q_1 \iff cf \leq de$

$ad \leq bc \overset{\text{P.1.26}}{\Longrightarrow} (ad)f \leq (bc)f.$ (because $f > 0$)

By theorems 1.15 and 1.16 $(ad)f = (af)d$ and furtheremore
$(bc)f \overset{\text{T.1.16}}{=} b(cf) \overset{\text{P.1.26}}{\leq} b(de) \overset{\text{T.1.16}}{=} (be)d$

Hence $(af)d \leq (be)d \overset{\text{T.1.23}}{\iff} ((af)d) - ((be)d) \leq 0 \overset{\text{T1.17}}{\iff} (af - be)d \leq 0$

And since $d > 0$ then by theorem 1.24
$(af - be) \leq 0 \overset{\text{T1.23}}{\iff} af \leq be \iff [(a, b)] \leq [(e, f)] \iff q \leq q_2$ ■

Theorem 1.36

Formulation 1.36.1

$$\forall\, q, p\, \in \mathbb{Q} \quad \text{one and only one of the following holds :} \quad p = q, \quad p < q, \quad q < p$$

Proof

Let $q = [(a, b)], \quad p = [(c, d)]$

We define $z := ad, \quad s := bc$

By Theorem 1.22 one and only one of the following relations holds:

$z = s, \quad z < s, \quad s < z$

Hence one and only one of the following holds

$p = q, \quad p < q, \quad q < p$

■

Formulation 1.36.2

$$\forall\, q, p\, \in \mathbb{Q} \implies q \leq p \quad \text{or} \quad p \leq q$$

Proof

We omit the proof because the method is the same as the proof just here above,but using the other formulation of theorem 1.22 ■

Proposition 1.37

$$\begin{matrix} q > 0 & & z > 0 & \\ q = 0 & \overset{\text{Respectively}}{\iff} & z = 0 & \forall\,(z, s) \in\, q \\ q < 0 & & z < 0 & \end{matrix}$$

Proof

By theorem 1.36 we know that

$q > 0, \;\; q = 0, \;\; q < 0$ are three options disjoints for q.

Furthermore reminding that $0 = [(0, 1)]$ let $q = [(z, s)]$:

- $q > 0 \iff [(z, s)] > 0 \overset{\text{D.1.30}}{\iff} z1 > s0 \iff z > 0$
  using that $z1 = z$ by theorem 1.18 and $s0 = 0$ by proposition 1.18
- $q = 0 \iff [(z, s)] = 0 \overset{\text{D.1.21}}{\iff} z1 = s0 \iff z = 0$
- $q < 0 \iff [(z, s)] < 0 \overset{\text{D.1.30}}{\iff} z1 < s0 \iff z > 0$

■

Corollary 1.16

$1_{\mathbb{Q}} > 0_{\mathbb{Q}}$

Theorem 1.37

$$q * (p + t) = q * p + q * t \quad \forall\, q, p, t \,\in \mathbb{Q}$$

Proof
Let $q = [(a, b)]$, $p = [(c, d)]$, $t = [(e, f)]$

$$\begin{aligned} q * (p + t) &= [(a, b)] * \big([(c, d)] + [(e, f)]\big) \overset{\text{D.1.23}}{=} [(a, b)] * [((cf) + (de), (df))] \\ &\overset{\text{D.1.24}}{=} [(a(cf + de), b(df))] \overset{\text{T.1.17}}{=} [((acf) + (ade), (bdf))] \\ &\overset{\text{P.1.31}}{=} [((acf) + (ade)(bdf), (bdf)(bdf))] \\ &\overset{\text{T.1.17}}{=} [((acf)(bdf) + (ade)(bdf), (bdf)(bdf))] \\ &\overset{\text{T.1.23}}{=} [((ac)f, (bd)f)] + [((ae)d, (bf)d)] \overset{\text{P.1.31}}{=} [(ac, bd)] + [(ae, bf)] \\ &\overset{\text{D.1.24}}{=} q * p + q * t \end{aligned}$$

■

Theorem 1.38

Formulation 1.38.1
Let $p, q \,\in \mathbb{Q}$

$$q < p \Longleftrightarrow q + t < p + t \qquad \forall\, t \in \mathbb{Q}$$

Proof
Let $q = [(a, b)]$, $\quad p = [(c, d)]$

$$\begin{aligned} q < p &\overset{\text{D.1.30}}{\Longleftrightarrow} ad < bc \overset{\text{T.1.24}}{\Longleftrightarrow} (ad)(ff) < (bc)(ff) \\ &\overset{\text{T.1.23}}{\Longleftrightarrow} (ad)(ff) + bdef < (bc)(ff) + bdef \\ &\overset{\text{T.1.17}}{\Longleftrightarrow} (af + be)(df) < (cf + de)(bf) \\ &\overset{\text{D.1.30}}{\Longleftrightarrow} [(af + be, bf)] < [(cf + de, df)] \overset{\text{D.1.23}}{\Longleftrightarrow} z + t < s + t \end{aligned}$$

■

Formulation 1.38.2
Let $p, q \,\in \mathbb{Q}$

$$q \leq p \Longleftrightarrow q + t \leq p + t \quad \forall\, t \in \mathbb{Q}$$

Proof
By first formulation we know that
$q < p \Longleftrightarrow q + t < p + t \qquad \forall\, p, q, t \,\in \mathbb{Q}$

Furthermore by corollary 1.14 we know that
$q = p \Longleftrightarrow q + t = p + t \qquad \forall\, p, q, t \,\in \mathbb{Q}$

and hence putting together both the results we get the thesis ■

Corollary 1.17

Let $q \in \mathbb{Q}$

$q > 0 \Longrightarrow -q < 0$

$q < 0 \Longrightarrow -q > 0$

Proof

- $q > 0 \overset{\text{T.1.38}}{\Longrightarrow} q + (-q) > 0 + (-q) \overset{\text{T.1.28}}{\Longrightarrow} 0 > 0 + (-q) \overset{\text{T.1.27}}{\Longrightarrow} 0 > -q$
- $q < 0 \overset{\text{T.1.38}}{\Longrightarrow} q + (-q) < 0 + (-q) \overset{\text{T.1.28}}{\Longrightarrow} 0 < 0 + (-q) \overset{\text{T.1.27}}{\Longrightarrow} 0 < -q$

■

Theorem 1.39

Formulation 1.39.1

$$p > 0\,,\ q > 0 \Longrightarrow\ p * q > 0 \qquad \forall\, p, q\ \in \mathbb{Q}$$

Proof

Let $q = [(a, b)], \quad p = [(c, d)]$

Then by proposition 1.37 $\quad a, c > 0 \overset{\text{T.1.24}}{\Longrightarrow} ac > 0$

Hence $\quad p * q > 0 \overset{\text{D.1.24}}{\Longleftrightarrow} [(ac, bd)] > 0 \overset{\text{P.1.37}}{\Longleftrightarrow} ac > 0$ ■

Formulation 1.39.2

$$p \geq 0\,,\ q \geq 0 \Longrightarrow\ p * q \geq 0 \quad \forall\, p, q\ \in \mathbb{Q}$$

Proof

- If $p = 0$ or $q = 0$

  By proposition 1.34 $\quad q * p = 0 \Longrightarrow q * p \geq 0$
- If $p, q > 0$ then by first formulation $\quad p * q > 0 \Longrightarrow p * q \geq 0$

■

Proposition 1.38

$q > p,\ \ t > 0 \Longrightarrow\ q * t > p * t \quad \forall\, p, q, t\ \in \mathbb{Q}$

Proof

$$q > p \overset{T.1.38}{\iff} q - p > 0 \overset{T.1.39}{\iff} (q-p) * t > 0 \overset{T.1.37}{\iff} q * t + (-p) * t > 0$$
$$\overset{P.1.33}{\iff} q * t - p * t > 0 \overset{T.1.38}{\iff} q * t > p * t$$
■

Proposition 1.39

Let $p \in \mathbb{Q}$

$p > 0 \Longrightarrow p^{-1} > 0$

$p < 0 \Longrightarrow p^{-1} < 0$

Proof

Let $p = [(a, b)]$

$p > 0 \overset{P.1.37}{\Longrightarrow} a > 0 \overset{T.1.32}{\Longrightarrow} p^{-1} = [(b, a)] \overset{P1.37}{\Longrightarrow} p^{-1} > 0$ ■

Proposition 1.40

Let $p, q \in \mathbb{Q}$

$p > q > 0 \implies 0 < p^{-1} < q^{-1}$

Proof

By proposition just above $p^{-1}, q^{-1} > 0$

$$p > q \overset{P.1.38}{\Longrightarrow} p^{-1} * p > q * p^{-1} \overset{T.1.31}{\Longrightarrow} 1 > q * p^{-1} \overset{P.1.38}{\Longrightarrow} 1 * q^{-1} > q * p^{-1} * q^{-1}$$
$$\overset{T.1.31}{\Longrightarrow} q^{-1} > q^{-1} * q * p^{-1} \overset{T.1.31}{\Longrightarrow} q^{-1} > p^{-1}$$
■

Proposition 1.41

Let $p \in \mathbb{Q}$

$(-q)^{-1} = -(q^{-1}) \quad \forall q \in \mathbb{Q} - \{0\}$

Proof

Let $q = [(a, b)]$

- $q > 0$ ($a > 0$ by proposition 1.37)

  On one hand

  $q > 0 \overset{T.1.32}{\Longrightarrow} q^{-1} = [(b, a)]$

  On the other hand

  $q > 0 \overset{T.1.28}{\Longrightarrow} -q = [(-a, b)] < 0 \overset{T.1.32}{\Longrightarrow} (-q)^{-1} = [(-b, a)]$

Hence

$$(q)^{-1} + (-q)^{-1} = [(b,a)] + [(-b,a)] \overset{\text{D.1.23}}{=} [(ba + (-b)a, aa)]$$
$$\overset{\text{P.1.19}}{=} [(ba - ba, aa)] = [(0, aa)] \overset{\text{D.1.25}}{=} 0$$

- $q < 0 \quad (a < 0)$

  On one hand

  $q < 0 \overset{\text{T.1.32}}{\Longrightarrow} q^{-1} = [(-b, -a)]$

  On the other hand

  $q < 0 \overset{\text{T.1.28}}{\Longrightarrow} -q = [(-a, b)] > 0 \overset{\text{T.1.32}}{\Longrightarrow} (-q)^{-1} = [(b, -a)]$

  Hence

$$(q)^{-1} + (-q)^{-1} = [(-b,-a)] + [(b,-a)] \overset{\text{D.1.23}}{=} [((-b)(-a) + b(-a), (-a)(-a))]$$
$$\overset{\text{C.1.8}}{=} [(ba + b(-a), aa)] \overset{\text{P.1.19}}{=} [(ba - ba, aa)] = [(0, aa)] \overset{\text{D.1.25}}{=} 0$$

Hence $(-q)^{-1}$ is the opposite of q^{-1} and by uniqueness of the opposite given by theorem 1.28 we get the thesis ■

Remark 1.8

$2_{\mathbb{Q}} := 1_{\mathbb{Q}} + 1_{\mathbb{Q}}$ and we have the following properties[6]:

- $2 > 1$
- $0 < 2^{-1} < 1$
- If $k > 0 \Longrightarrow 0 < k * 2^{-1} < k$
- If $p < q \Longrightarrow p < (p + q) * 2^{-1} < q$
- $p * 2^{-1} + p * 2^{-1} = p \quad \forall\, p \in \mathbb{Q}$

Definition 1.31 (Powers)[7]

Let $q > 0$

- $q^1 := q$
- $q^{n+1} := q^n * q \quad \forall\, n \in \mathbb{N}$

Proposition 1.42

$(q * p)^n = q^n * p^n \quad \forall\, q, p > 0 \quad \forall\, n \in \mathbb{N}$

[6] From this point forward we denote $2_{\mathbb{Q}}$ simply as 2

[7] See Remark 1.1

Proof
Let $q, p > 0$. Let us proceed by induction on n

- $n = 1$
  $(q * p)^1 \overset{\text{D.1.31}}{=} q * p = q^1 * p^1$
- Supposed for n we show it for $n + 1$
  $$(q * p)^{n+1} \overset{\text{D.1.31}}{=} (q * p)^n * (q * p) \overset{I.S.}{=} (q^n * p^n) * (q * p)$$
  $$= ((q^n) * q) * (p^n * p) \overset{\text{D.1.31}}{=} q^{n+1} * p^{n+1}$$

■

Corollary 1.18

$q^n > 0 \quad \forall\, q > 0 \quad \forall\, n \in \mathbb{N}$

Proof
Let $q > 0$. Let us proceed by induction on n

- $n = 1$
  $q^1 \overset{\text{D.1.31}}{=} q \implies q^1 > 0$
- Supposed for n we show it for $n + 1$
  $q^{n+1} \overset{\text{D.1.31}}{=} q^n * q$
  $$\left.\begin{array}{ll} q^n > 0 & \text{by inductive step} \\ q > 0 & \text{by hypothesis} \end{array}\right\} \overset{\text{T.1.39}}{\implies} q^{n+1} > 0$$

■

Remark 1.9

$1^n = 1 \quad \forall\, n \in \mathbb{N}$

Corollary 1.19

$(q^{-1})^n = (q^n)^{-1} \quad \forall\, q > 0 \quad \forall\, n \in \mathbb{N}$

Proof
Let $q > 0, \ n \in \mathbb{N}$
$1 = 1^n = (q * q^{-1})^n \overset{\text{P.1.42}}{=} q^n * (q^{-1})^n$
Hence calling $t := q^n \quad t^{-1} = (q^{-1})^n$ and by uniqueness of the inverse given by theorem 1.32 we get the thesis
■

Proposition 1.43

$q^n > 1 \quad \forall\, q > 1 \quad \forall\, n \in \mathbb{N}$

Proof
Let $q > 1$. Let us proceed by induction on n

- $n = 1$
  $q^1 \overset{\text{D.1.31}}{=} q \implies q^1 > 1$
- Supposed for n we show it for $n+1$
  $q^{n+1} \overset{\text{D.1.31}}{=} q^n * q$

$$\left.\begin{array}{ll} q^n > 1 & \text{by inductive step} \\ q > 1 & \text{by hypothesis} \end{array}\right\} \overset{\text{T.1.39}}{\Longrightarrow} q^{n+1} > 1$$

■

Immersion Theorem 1.2 ($\mathbb{Z} \hookrightarrow \mathbb{Q}$)

We have just built $\Big(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}},\, <_{\mathbb{Q}}\Big)$ from $\Big(\mathbb{Z},\, +_{\mathbb{Z}},\, *_{\mathbb{Z}},\, <_{\mathbb{Z}}\Big)$.
As in Immersion Theorem 1.1 we will show that exist $J_1 : \mathbb{Z} \longrightarrow \mathbb{Q}$ such that:

1. J_1 is injective
2. $J_1(z +_{\mathbb{Z}} s) = J_1(z) +_{\mathbb{Q}} J_1(s) \qquad \forall\, z, s \in \mathbb{Z}$
3. $J_1(z *_{\mathbb{Z}} s) = J_1(z) *_{\mathbb{Q}} J_1(s) \qquad \forall\, z, s \in \mathbb{Z}$
4. $z <_{\mathbb{Z}} s \iff J_1(z) <_{\mathbb{Q}} J_1(s) \qquad \forall\, z, s \in \mathbb{Z}$
5. $q \in J_1(\mathbb{Z}) \iff \exists\, z \in \mathbb{Z} \quad | \; q = [(z, 1)]$
6. $q \in J_1(J(\mathbb{N})) \iff \exists\, z \in \mathbb{Z}, \quad z > 0 \quad | \; q = [(z, 1)]$

Proof
Let $z \in \mathbb{Z}, \qquad J_1(z) := [(z, 1)]$

1. $J_1(z) = J_1(s) \iff [(z, 1)] = [(s, 1)] \overset{\text{D.1.21}}{\iff} z1 = s1 \overset{\text{T.1.18}}{\iff} z = s$
2. $$\begin{aligned} J_1(z +_{\mathbb{Z}} s) &= [(z + s, 1)] \overset{\text{T.1.18}}{=} [(z1 + s1, 11)] \\ &\overset{\text{D.1.23}}{=} [(z, 1)] + [(s, 1)] = J_1(z) +_{\mathbb{Q}} J_1(s) \end{aligned}$$
3. $J_1(z *_{\mathbb{Z}} s) = [(zs, 1)] \overset{\text{D.1.24}}{=} [(z, 1)] * [(s, 1)] = J_1(z) *_{\mathbb{Q}} J_1(s)$
4. $z < s \overset{\text{T1.18}}{\iff} z1 < s1 \overset{\text{D.1.30}}{\iff} [(z, 1)] < [(s, 1)] \iff J_1(z) <_{\mathbb{Q}} J_1(s)$

5. It is immediate by definition of J_1
6. It is immediate by definition of J in Immersion Theorem 1.1

■

Notational Remark 1.17
With a strong abuse of notations, henceforth we will denote $J_1(\mathbb{Z}) \subset \mathbb{Q}$ as $\mathbb{Z} \subset \mathbb{Q}$ and $J_1(J(\mathbb{N})) \subset \mathbb{Q}$ as $\mathbb{N} \subset \mathbb{Q}$
So in the following Lemmas with $n \in \mathbb{N}$ we denote a rational $q \mid q = J_1(J(n))$

Lemma 1.5 (Bernoulli)

$q > 1 \implies \forall n \in \mathbb{N} \quad q^n \geq 1 + (n * (q-1))$

Proof
Let $r := q - 1 \implies q = 1 + r$

We proceed by induction on n

- $n = 1$
  $(1+r)^1 = 1 + r = 1 + (r * 1)$
- Supposed for n we show it for $n+1$
  $(1+r)^{n+1} = (1+r)^n * (1+r)$
  $q^n \geq 1 + n * r$ by inductive step
  Then by theorem 1.39 $(1+r)^{n+1} \geq (1 + (n*r)) * (1+r) \overset{\text{T.1.37}}{=} 1 + (n+1) * r + n * r^2$
  And since $n * r^2 > 0$ by theorem 1.38 $(1+r)^{n+1} \geq 1 + (n+1) * r$

■

Lemma 1.6 (Archimedean Property of $\mathbb{Q}$)

$$\forall p, q \in \mathbb{Q}, \quad q > 0 \implies \exists n \in \mathbb{N} \quad | \quad n * q > p$$

Proof
Proofing this result we will proceed by steps

1. $\forall q \in \mathbb{Q},\ q > 0 \quad \exists n \in \mathbb{N}$ such that $n > q$:
   - $q > 1$
     By proposition 1.37 $q = [(a, b)]$ with $a > 0$
     And hence both $a, b > 0$
     Then by corollary 1.11 $\implies a \geq 1$ and $b \geq 1$.
     On the other hand
     $b \geq 1 \overset{\text{P.1.26}}{\implies} ab \geq a$

By corollary 1.12 $(bb) > 0$ And hence $bb + ab \geq bb + a > a$.

Furthermore
$bb + ab \overset{\text{T.1.17}}{=} b\,(a+1) \overset{\text{T.1.15}}{=} (a+1)b \Longrightarrow (a+1)b > a1 \overset{\text{D.1.30}}{\Longleftrightarrow} [(a+1,1)] > [(a,b)]$

And hence calling $n_q := [(a+1,1)]$

$\Longrightarrow n_q > q$ and by Immersion Theorem 1.2 $n_q \in \mathbb{N}$

- $0 < q \leq 1$

  Let $p > 1$ then $p > 1 \geq q$ and from the point above :

  $\exists\, n_p$ such that $n_p > p \overset{\text{T.1.35}}{\Longrightarrow} n_p > q$

2. $\forall\, p, q \in \mathbb{Q}, \quad q > 0, p > 0 \Longrightarrow \exists\, n \in \mathbb{N}$ such that $n * q > p$:

   Let $p, q > 0$.
   By proposition 1.39 $q^{-1} > 0$.

   We define $t := q^{-1} * p \overset{\text{T.1.39}}{\Longrightarrow} t > 0$

   By the first step let $n_t \in \mathbb{N}$ such that $n_t > t$

   Then by proposition 1.38 $n_t * q > t * q \Longrightarrow n_t * q > p$

3. $\forall\, p, q \in \mathbb{Q}, \quad q > 0 \Longrightarrow \exists\, n \in \mathbb{N}$ such that $n * q > p$:

   - $p > 0$ It follows by step 2.
   - $p \leq 0$

     Let $t := 1_{\mathbb{Q}}$. Then $t > 0 \geq p$, and by step 2.

     $\exists\, n \in \mathbb{N}$ such that $n * q > t \overset{\text{T.1.35}}{\Longrightarrow} n * q > p$

■

Proposition 1.44

$$0 < q < 1 \Longrightarrow \forall\, r > 0 \quad \exists\, n \in \mathbb{N} \quad | \quad q^n < r$$

Proof

Let $0 < q < 1$

On one hand by lemma 1.6
$\exists\, n$ such that $r > n^{-1} * (q^{-1} - 1)^{-1}$

On the other hand by proposition 1.40 since $q < 1 \Longrightarrow q^{-1} > 1$
Then by lemma 1.5 $(q^{-1})^n \geq 1 + (n * (q^{-1} - 1)) > (n * (q^{-1} - 1))$

Furthermore by corollary 1.19
$(q^{-1})^n = (q^n)^{-1}$

Hence

$$(q^{-1})^n > (n * (q^{-1} - 1)) \Longrightarrow (q^n)^{-1} > (n * (q^{-1} - 1))$$
$$\overset{\text{P.1.40}}{\Longrightarrow} q^n < n^{-1} * (q^{-1} - 1)^{-1} < r$$

■

1.3.1 Remarks and Complements

Remark 1.10 About arbitrary choices on Building $\mathbb{Q}$

In the same way as the precedent section, we could avoid to define $+_{\mathbb{Q}}, *_{\mathbb{Q}}, \leq_{\mathbb{Q}}$ and all the results holding for them, choosing an arbitrary couple $(z,s) \in \mathbb{Z} \times \mathbb{Z}_+$ of each equivalence class .

Thus, for any $q \in \mathbb{Q}$ we could select a privileged representant as follow:

1. Let $q \in \mathbb{Q}$

   If $(z,s) \in q$, $(z_1,s) \in q \implies z = z_1 \quad \forall\, s \in \mathbb{Z}_+ = J(\mathbb{N})$

2. Recalling definition of J as in Immersion Theorem 1.1,

   we define $CH_{\mathbb{Q}} : \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{Z}_+$ as follows

   $$CH_{\mathbb{Q}}(q) := (z_q, J(n_q)) \quad \text{where} \quad n_q = \min\{n \in \mathbb{N} \mid \exists\, z \in \mathbb{Z} \text{ s.t.} (z, J(n)) \in q\}$$
   $$\text{and} \quad (z_q, J(n_q)) \in q \;\; (z_q \text{ is unique by step 1})$$

Defining $+_{\mathbb{Q}}, *_{\mathbb{Q}}, \leq_{\mathbb{Q}}$ on these representant we could prove all the results without arbitrary choices

Thus arbitrary choices do not occur in building $\mathbb{Q}$

Chapter 2

Constructions of the Reals Numbers

Definition 2.1

Let $\mathcal{F}$ an Ordered Set[1], $A \subset \mathcal{F}$ and $\gamma \in \mathcal{F}$

γ is an upper bound of $A \iff \forall \alpha \in A \quad \alpha \leq \gamma$

A is bounded above $\iff \exists \gamma$ upper bound for A

Definition 2.2

Let $\mathcal{F}$ an Ordered Set, $A \subset \mathcal{F}, \quad \gamma \in \mathcal{F}$

$$\gamma \text{ is the Least Upper Bound of } A \iff \begin{cases} S_1) & \gamma \text{ is upper bound for } A \\ S_2) & \text{if } \gamma_1 \text{ is upper bound for } A \implies \gamma \leq \gamma_1 \end{cases}$$

We call γ the L.U.B. of A and we denote it $\gamma = \sup A$

Remark 2.1

The L.U.B. (whenever it exists) is unique

Proof

Suppose $\gamma_1, \gamma = \sup A$

Since $\mathcal{F}$ is an Ordered Set we have three options : $\gamma_1 < \gamma$ or $\gamma < \gamma_1$ or $\gamma = \gamma_1$

if $\gamma_1 < \gamma$ it's a contradiction since

$\gamma = \sup A$ and then if γ_1 is upper bound for $A \implies \gamma \leq \gamma_1$

The same if we placed $\gamma < \gamma_1$ ■

Definition 2.3

Let $\mathcal{F}$ an Ordered Set, $A \subset \mathcal{F}$ and $\gamma \in \mathcal{F}$

[1] See definition of Ordered Set in Preliminary Set Theory notions

γ is a lower bound of $A \iff \forall\, \alpha \in A \quad \gamma \leq \alpha$

A is bounded below $\iff \exists\, \gamma$ lower bound for A

Definition 2.4

Let $\mathcal{F}$ an Ordered Set, $A \subset \mathcal{F}, \quad \gamma \in \mathcal{F}$

$$\gamma \text{ is the Great Lower Bound of } A \iff \begin{cases} I_1) & \gamma \text{ is lower bound for } A \\ I_2) & \text{if } \gamma_1 \text{ is lower bound for } A \Longrightarrow \gamma \geq \gamma_1 \end{cases}$$

We call γ the G.L.B. of A and we denote it $\quad \gamma = \inf A$

Remark 2.2

The G.L.B. (whenever it exists) is unique

Proof

Look at remark 2.1 ∎

Definition 2.5

Let $A \subset \mathbb{R}$

$$A \text{ is bounded} \iff \begin{cases} A \text{ is bounded above} \\ A \text{ is bounded below} \end{cases}$$

Definition 2.6

$\big(\text{a set}\, \mathbb{R},\, +_{\mathbb{R}},\, *_{\mathbb{R}},\, \leq_{\mathbb{R}}\big)$ is a Complete Ordered Field (COF)
if and only if satisfies the following properties:

- $\big(\mathbb{R},\, +_{\mathbb{R}},\, *_{\mathbb{R}},\, \leq_{\mathbb{R}}\big)$ is an OF[2]

- **(Ded)** $$\left.\begin{array}{l} A \subset \mathcal{R},\ A \neq \emptyset \\ A \text{ bounded above} \\ (A \text{ bounded below}) \end{array}\right\} \Longrightarrow \exists\, \gamma \in \mathbb{R} \quad | \quad \gamma = \sup A \ \ (\gamma = \inf A)$$

Aim of Chapter 2.

In this Chapter we show the following results:

Given an OF $\big(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}},\, \leq_{\mathbb{Q}}\big)$ there exists a model of COF $\big(\mathbb{R},\, +_{\mathbb{R}},\, *_{\mathbb{R}},\, \leq_{\mathbb{R}}\big)$ which contains a copy of $\big(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}},\, \leq_{\mathbb{Q}}\big)$

[2]See definition 1.19

Remark 2.3

We will arrive at this result in two different ways. Thus the two sections which divide this Chapter are uncorrelated. We suggest the reader to do not read them sequentially, but to read them in parallel noting as these different methods conduce to the same results

---

2.1 Construction of $\mathbb{R}$ via Dedekind cuts

Notational Remark 2.1
In this Section we will denote

$p +_{\mathbb{Q}} q$ simply as $p + q \quad \forall\, p, q \in \mathbb{Q}$
$p *_{\mathbb{Q}} q$ simply as $pq \quad \forall\, p, q \in \mathbb{Q}$
$p \leq_{\mathbb{Q}} q$ simply as $p \leq q \quad \forall\, p, q \in \mathbb{Q}$
$p <_{\mathbb{Q}} q$ simply as $p < q \quad \forall\, p, q \in \mathbb{Q}$

Definition 2.7

Let $T \subset \mathbb{Q}$, $T \neq \emptyset$

T is a cut of $\mathbb{Q} \iff T$ satisfy this two conditions

- $c_1) \quad p \in T,\, q \leq p \Longrightarrow q \in T$
- $c_2) \quad p \in T \Longrightarrow \exists\, r > p$ and $r \in T$

Corollary 2.1

Let T cut of $\mathbb{Q}$, $q \in \mathbb{Q}$

$q \notin T \Longrightarrow q > p \quad \forall\, p \in T$

Proof
If $\exists\, p_0 \in T$ with $q \leq p_0 \overset{c_1}{\Longrightarrow} q \in T$.

But $q \notin T$ ■

Corollary 2.2

Let T cut of $\mathbb{Q}$, $q, p \in \mathbb{Q}$

$p \notin T,\, q \geq p \Longrightarrow q \notin T$

Proof
If $q \in T \overset{\text{C.2.1}}{\Longrightarrow} q < p$, but $q \geq p$ ■

Definition 2.8

Let $q \in \mathbb{Q}$
$q^* := \{t \in \mathbb{Q} \mid t < q\}$

Proposition 2.1

q^* is a cut of $\mathbb{Q}$ $\quad \forall\, q \in \mathbb{Q}$

Proof

- $\left.\begin{array}{l} q-1<q \\ q \notin q^* \end{array}\right\} \Longrightarrow q^* \subset \mathbb{Q},\, q^* \neq \emptyset$
- Let $t \in q^*$ and $h < t \overset{\text{T.1.35}}{\Longrightarrow} h < q \Longrightarrow h \in q^*$
- Let $t \in q^*$
  Then $t < q$ and using remark 1.8
  Let $h := (q+t)2^{-1} \implies t < h < q \implies h > t$ and $h \in q^*$

■

Remark 2.4

From Proposition 2.1 there follows that 0^*, 1^* are cuts of $\mathbb{Q}$

Definition 2.9

$\mathbb{R} := \{\alpha \subset \mathbb{Q},\, \alpha \neq \emptyset \mid \alpha \text{ is a cut of } \mathbb{Q}\}$

Definition 2.10

Let $\alpha, \beta \in \mathbb{R}$
$(\alpha, \beta)_+ := \{p+q \mid p \in \alpha,\, q \in \beta\}$

Proposition 2.2

$(\alpha, \beta)_+ \in \mathbb{R}$

Proof
- $\alpha, \beta \neq \emptyset \Longrightarrow \exists\, p \in \alpha,\, q \in \beta$
  Hence $p+q \in (\alpha, \beta)_+ \Longrightarrow (\alpha, \beta)_+ \neq \emptyset$

- $\alpha, \beta \neq \mathbb{Q} \Longrightarrow \exists p_0 \notin \alpha,\, q_0 \notin \beta \overset{\text{C.2.1}}{\Longrightarrow} \forall p \in \alpha \;\; p_0 > p, \quad \forall q \in \beta \;\; q_0 > q$

$$\overset{\text{T.1.39}}{\Longrightarrow} \; p_0 + q_0 > p + q \quad \forall p \in \alpha,\, q \in \beta$$

$$\Longrightarrow p_0 + q_0 \notin (\alpha, \beta)_+ \Longrightarrow (\alpha, \beta)_+ \subset \mathbb{Q}$$

- Let $p \in (\alpha, \beta)_+$ ($p = a + b$ with $a \in \alpha,\, b \in \beta$) and let $q \leq p$

$$\left.\begin{array}{l} q \leq p \Longrightarrow (q-a) \leq b \overset{c_1}{\Longrightarrow} (q-a) \in \beta \\ a + (q-a) \overset{\text{T.1.25}}{=} (q-a) + a \overset{\text{T.1.26}}{=} q + 0 \overset{\text{T.1.27}}{=} q \end{array}\right\} \Longrightarrow q \in (\alpha, \beta)_+$$

- Let$p \in (\alpha, \beta)_+ \Longrightarrow p = a + b$ with $a \in \alpha,\, b \in \beta$

$$\overset{c_2}{\Longrightarrow} \exists\, a_1 \in \alpha, \quad b_1 \in \beta \text{ with } a < a_1, \quad b < b_1$$

$$\Longrightarrow a_1 + b_1 > a + b = p \text{ and } a_1 + b_1 \in (\alpha, \beta)_+$$

■

Proposition 2.3

$(\alpha, \beta)_+ = (\beta, \alpha)_+ \quad \forall\, \alpha, \beta \in \mathbb{R}$

Proof
It comes immediately by the commutativity of sum in $\mathbb{Q}$
■

Notational Remark 2.2
Let $+_{\mathbb{R}} := \{((\alpha, \beta), (\alpha, \beta)_+) \;\mid\; \alpha, \beta \in \mathbb{R}\}$

It is easy to prove that $+_{\mathbb{R}}$ is a binary inner operation[3] on $\mathbb{R}$

Namely $\begin{array}{rccc} +_{\mathbb{R}}: & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & (\alpha, \beta) & \longrightarrow & (\alpha, \beta)_+ \end{array}$

In view of proposition 2.3 the following theorem holds

Theorem 2.1

$$\alpha +_{\mathbb{R}} \beta = \beta +_{\mathbb{R}} \alpha \quad \forall\, \alpha, \beta \in \mathbb{R}$$

Notational Remark 2.3
Henceforth we will denote $\alpha +_{\mathbb{R}} \beta$ simply as $\alpha + \beta \quad \forall\, \alpha, \beta \in \mathbb{R}$

Theorem 2.2

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \quad \forall\, \alpha, \beta, \gamma \in \mathbb{R}$$

[3]See this definition in: A brief survey of elements of Set theory and Logic

Proof
By Extensionality we have to show that

$p \in \alpha + (\beta + \gamma) \Longleftrightarrow p \in (\alpha + \beta) + \gamma$

$\Longrightarrow)$

$$p \in \alpha + (\beta + \gamma) \overset{\text{D.2.10}}{\Longleftrightarrow} p = a + t,\, a \in \alpha,\, t \in (\beta + \gamma)$$

$$p = a + (b + c),\ a \in \alpha,\, b \in \beta,\, c \in \gamma$$

$$\overset{\text{T1.26}}{\Longleftrightarrow} p = (a + b) + c$$

$$\Longrightarrow p \in (\alpha + \beta) + \gamma$$

$\Longleftarrow)$

We omit the proof since its method is the same as above ■

Theorem 2.3

$$\alpha + 0^* = \alpha \quad \forall \alpha \in \mathbb{R}$$

Proof
By Extensionality we have to show that

$p \in \alpha + 0^* \Longleftrightarrow p \in \alpha$

$\Longrightarrow)$

Let $p \in \alpha + 0^* \Longrightarrow p = a + t$ with $a \in \alpha$, $c \in 0^*$
Since $t < 0 \overset{\text{T.1.39}}{\Longrightarrow} p = a + t < a \overset{c_1}{\Longrightarrow} p \in \alpha$

$\Longleftarrow)$

Let $p \in \alpha$

$$\left.\begin{array}{l} p \in \alpha \overset{c_2}{\Longrightarrow} \exists\, r \in \alpha \ \mid r > p \Longrightarrow p - r \ \in 0^* \\ p = r + (p - r) \end{array}\right\} \Longrightarrow p \in \alpha + 0^*$$

■

Remark 2.5

Recalling Notational remark 1.17 with $n \in \mathbb{N}$ and $z \in \mathbb{Z}$ we refer to a rational q such that $q \in J_1(J(\mathbb{N}))$ or $q = J_1(\mathbb{Z})$ respectively

Proposition 2.4

$$\alpha \in \mathbb{R}, \quad w \in \mathbb{Q},\, w > 0 \Longrightarrow \begin{cases} 1. \quad \exists\, n \in \mathbb{N} \ \mid \ nw \notin \alpha \\ 2. \quad \exists\, m \in \mathbb{N} \ \mid \ -mw \in \alpha \\ 3. \quad \exists\, z \in \mathbb{Z}, \quad -(m+1) \leq z \leq n - 1 \quad \mid \\ \qquad\qquad zw \in \alpha,\ (z+1)w \notin \alpha \end{cases}$$

Proof

1. $\alpha \neq \mathbb{Q} \implies \exists\, y \notin \alpha$.
   By Archimedean property of $\mathbb{Q}$ (Lemma 1.6)
   $\exists\, n \in \mathbb{N} \quad | \quad nw > y \overset{\text{C.2.1}}{\implies} nw \notin \alpha$.

2. $\exists\, p \in \alpha$.
   Like above using lemma 1.6
   $\exists\, m \in \mathbb{N}$ such that $mw > (-p)$
   $\implies -mw < p \overset{c_1}{\implies} -mw \in \alpha$

3. $z := (n-1)w$
   If $zw \in \alpha$ we have done since $(z+1)w = nw \notin \alpha$
   if $zw \notin \alpha \implies \quad z := (n-2)$
   If $zw \in \alpha$ we have done since $\quad (z+1)w = (n-1)w \notin \alpha$
   If $zw \notin \alpha \implies \; z := (n-3)\ldots$

   If we continued in this way for all $-(m+1) \leq z \leq n-1$
   it will be a contradiction because surely
   for $z = -(m+1) \implies (z+1)w = -mw \in \alpha$.

■

Definition 2.11

Let $\alpha \in \mathbb{R}$

$\widetilde{\alpha} := \{p \in \mathbb{Q} \;|\; \exists\, A > 0 \;|\; -p - A \notin \alpha\}$

Proposition 2.5

$$\alpha \in \mathbb{R} \quad \implies \begin{cases} \widetilde{\alpha} \in \mathbb{R} \\ \alpha + \widetilde{\alpha} = 0^* \\ \text{If } \; \gamma \in \mathbb{R} \quad \alpha + \gamma = 0^* \implies \gamma = \widetilde{\alpha} \end{cases}$$

Proof

- $\widetilde{\alpha} \in \mathbb{R}$:
  - $\alpha \neq \mathbb{Q} \implies \exists\, q \notin \alpha \overset{\text{C.2.2}}{\implies} q + 1 \notin \alpha$
    Hence if $p := -(q+2) \implies -p - 1 \notin \alpha \implies p \in \widetilde{\alpha} \implies \widetilde{\alpha} \neq \emptyset$

- By contradiction $\widetilde{\alpha} = \mathbb{Q} \Longrightarrow \forall q \in \mathbb{Q} \quad \exists A > 0 \mid -q - A \notin \alpha$

  $\alpha \neq \emptyset \Longrightarrow \exists a \in \alpha$

  Let $b := -a$

  By hypothesis $\exists B > 0 \quad | \quad -b - B \notin \alpha \overset{\text{C.2.1}}{\Longrightarrow} -b - B > a \Longrightarrow B < 0$

  Contradiction

- Let $p \in \widetilde{\alpha}, \quad q \leq p$

  $p \in \widetilde{\alpha} \Longrightarrow \exists A > 0 \mid -p - A \notin \alpha$

  Furthermore $p - q \geq 0 \overset{\text{T.1.38}}{\Longrightarrow} A + (p - q) \geq A > 0 \overset{\text{T.1.35}}{\Longrightarrow} A + (p - q) > 0$

  We define $A_1 := A + (p - q)$ and then

  $-q - A_1 = -q - (A + (p - q)) = -p - A \notin \alpha$

  $\Longrightarrow \exists A_1 > 0 \mid -q - A_1 \notin \alpha \overset{\text{D.2.11}}{\Longrightarrow} q \in \widetilde{\alpha}$

- Let $p \in \widetilde{\alpha} \Longrightarrow \exists A > 0 \mid -p - A \notin \alpha$

  Let $A_1 := (2)^{-1}A$ and according to remark 1.8 we get

  $A_1 < A$ and $A_1 > 0$

  Defining $q := p + A_1 \overset{\text{T.1.38}}{\Longrightarrow} q > p$ and

  $-q - A_1 = -p - A \notin \alpha$

  $\Longrightarrow \exists A_1 > 0$ with $-q - A_1 \notin \alpha \overset{\text{D.2.11}}{\Longrightarrow} q \in \widetilde{\alpha}$

- $\alpha + \widetilde{\alpha} = 0^*$:

  By Extensionality $p \in \alpha + \widetilde{\alpha} \Longleftrightarrow p \in 0^*$

  $\Longrightarrow)$

  Let $p \in \alpha, \quad q \in \beta$

  $\Longrightarrow \exists A > 0$ with $-q - A \notin \alpha \overset{\text{C.2.1}}{\Longrightarrow} -q - A > p \overset{\text{T.1.38}}{\Longrightarrow} p + q < -A < 0 \Longrightarrow p + q \in 0^*$

  $\Longleftarrow)$

  Let $v \in 0^* \Longrightarrow v < 0 \overset{\text{C.1.17}}{\Longrightarrow} -v > 0$

  Hence calling $w := (2)^{-1}(-v)$ by remark 1.8 we know that $w > 0$

  Now by proposition 2.4

  Let be $z \in \mathbb{Z}$ with $zw \in \alpha, \quad (z+1)w \notin \alpha.$

  $(z+1)w = (z+2)w - w = -(-(z+2)w) - w$

  Hence calling $q := -(z+2)w$

  $-q - w \notin \alpha \Longrightarrow q \in \widetilde{\alpha}$

  $$v = -2w \overset{\text{T.1.27}}{=} -2w + 0 \overset{\text{T.1.28}}{=} -2w + (-zw + zw) \overset{\text{T.1.26}}{=} (-2w - zw) + zw$$
  $$\overset{\text{T.1.37}}{=} -w(2+z) + zw = q + zw$$

  With $zw \in \alpha, \quad q \in \widetilde{\alpha} \Longrightarrow zw + q = v \in \alpha + \beta$

- Let $\gamma \in \mathbb{R}$ and $\alpha + \gamma = 0^*$:

$$\gamma \overset{T.2.3}{=} \gamma + 0^* = \gamma + (\alpha + \widetilde{\alpha}) \overset{T.2.2}{=} (\gamma + \alpha) + \widetilde{\alpha} = 0^* + \widetilde{\alpha} \overset{T.2.3}{=} \widetilde{\alpha}$$

■

An immediate corollary of proposition 2.5 is the following

Theorem 2.4

$$\forall \alpha \in \mathbb{R} \quad \exists!\, \widetilde{\alpha} \in \mathbb{R} \;\text{ such that }\; \alpha + \widetilde{\alpha} = 0^*$$

Definition 2.12

Let $\alpha \in \mathbb{R}$ we call "the opposite of α" the unique element $\widetilde{\alpha}$ such that $\alpha + (\widetilde{\alpha}) = 0^*$ given by theorem 2.4 and we denote $\widetilde{\alpha}$ as $-\alpha$

Proposition 2.6

Let $\alpha, \beta \in \mathbb{R}$

$\alpha = \beta \Longleftrightarrow \alpha + \gamma = \beta + \gamma \quad \forall \gamma \in \mathbb{R}$

Proof

$\Longrightarrow$)

By contradiction $\exists\, \gamma_0 \in \mathbb{R} \mid \alpha + \gamma_0 \neq \beta + \gamma_0$

By Extensionality we have two options:

$\exists\, p \in \alpha + \gamma_0 \mid p \notin \beta + \gamma_0$ or $\exists\, p \in \beta + \gamma_0 \mid p \notin \alpha + \gamma_0$

Suppose the first one holds. Then

$p \in \alpha + \gamma_0 \overset{D.2.10}{\Longleftrightarrow} \exists\, a \in \alpha, \exists\, c \in \gamma_0 \mid p = a + c$

But since $\alpha = \beta \Longrightarrow a \in \beta \Longrightarrow p \in \beta + \gamma_0$

Contradiction. Supposing the second one we will get a contradiction too

$\Longleftarrow$)

By contradiction $\alpha \neq \beta \overset{T.2.3}{\Longrightarrow} \alpha + 0^* \neq \beta + 0^*$

Contradiction

■

Definition 2.13

Let $\alpha, \beta \in \mathbb{R}$

$\alpha <_{\mathbb{R}} \beta \Longleftrightarrow \alpha \subset \beta$

Corollary 2.3

$1^* >_{\mathbb{R}} 0^*$

Definition 2.14

Let $\alpha,\ \beta\ \in \mathbb{R}$

$\alpha \leq_{\mathbb{R}} \beta \iff \alpha < \beta$ or $\alpha = \beta \iff \alpha \subseteq \beta$

Notational Remark 2.4
Henceforth we will denote:

$\alpha <_{\mathbb{R}} \beta$ simply as $\alpha < \beta \quad \forall\, \alpha, \beta\ \in \mathbb{R}$
$\alpha \leq_{\mathbb{R}} \beta$ simply as $\alpha \leq \beta \quad \forall\, \alpha, \beta\ \in \mathbb{R}$

We will omit proofs of the following three theorems since they descend directly by definitions 2.13 and 2.14

Theorem 2.5

$$\alpha \leq \alpha \quad \forall\, \alpha \in \mathbb{R}$$

Theorem 2.6
Let $\alpha,\ \beta\ \in \mathbb{R}$

$$\left.\begin{array}{l} \beta \leq \alpha \\ \alpha \leq \beta \end{array}\right\} \Longrightarrow \alpha = \beta$$

Theorem 2.7
Let $\alpha, \alpha_1, \alpha_2\ \in \mathbb{R}$

$$\left.\begin{array}{l} \alpha \leq \alpha_1 \\ \alpha_1 \leq \alpha_2 \end{array}\right\} \Longrightarrow \alpha \leq \alpha_2$$

Theorem 2.8

Formulation 2.8.1

$$\forall\, \alpha, \beta\ \in \mathbb{R} \quad \text{one and only one of the following holds :} \quad \alpha = \beta, \quad \alpha < \beta, \quad \alpha > \beta$$

Proof
It is clear that at most one of the three relations holds for a couple α, β

We will show that at least one of them holds.
Let $\alpha, \beta\ \in \mathbb{R}$
Suppose that $\alpha \neq \beta \iff \alpha \nsubseteq \beta$ or $\beta \nsubseteq \alpha$

- If $\alpha \nsubseteq \beta$

  Then $\exists\, p \in \alpha,\ p \notin \beta$

  $$\text{Let } q \in \beta \implies \left.\begin{array}{l} \text{If } q \geq p \overset{\text{C.2.2}}{\implies} q \notin \beta \text{ Contradiction since } q \in \beta \\ \text{If } q < p \overset{c_1}{\implies} q \in \alpha \end{array}\right\} \implies q \in \alpha$$

  Hence $\beta \subset \alpha \overset{\text{D.2.13}}{\implies} \beta < \alpha$

- If $\beta \nsubseteq \alpha$

  Repeating the same reasoning as above we get the opposite inequality

Then $\forall\, \alpha, \beta \in \mathbb{R} \implies \alpha < \beta$ or $\beta < \alpha$ and these are two disjoint options ■

Formulation 2.8.2

$$\forall\, \alpha, \beta \in \mathbb{R} \implies \alpha \leq \beta \quad \text{or} \quad \alpha \leq \beta$$

Proof

We omit the proof it is an immediate consequence of the first formulation of this theorem ■

Theorem 2.9

Formulation 2.9.1

Let $\alpha, \beta \in \mathbb{R}$

$$\alpha < \beta \iff \alpha + \gamma < \beta + \gamma \quad \forall\, \gamma \in \mathbb{R}$$

Proof

$\implies$)

Let $p \in \alpha + \gamma \implies p = a + c$ with $a \in \alpha$, $c \in \gamma$

$\alpha \subset \beta \implies a \in \beta \implies p = a + c$ with $a \in \beta$, $c \in \gamma$

$\implies p \in \beta + \gamma$

$\impliedby$)

Using what we said above we call $\alpha_1 := (\alpha + \gamma)$, $\beta_1 := (\beta + \gamma)$

$$\begin{aligned} \alpha_1 + (-\gamma) < \beta_1 + (-\gamma) &\iff (\alpha + \gamma) + (-\gamma) < (\beta + \gamma) + (-\gamma) \\ &\overset{\text{T.2.2}}{\iff} \alpha + (\gamma + (-\gamma)) < \beta + (\gamma + (-\gamma)) \\ &\overset{\text{T.2.4}}{\iff} \alpha + 0^* < \beta + 0^* \overset{\text{T.2.3}}{\iff} \alpha < \beta \end{aligned}$$

■

Formulation 2.9.2

Let $\alpha, \beta \in \mathbb{R}$

$$\alpha \leq \beta \iff \alpha + \gamma \leq \beta + \gamma \quad \forall\, \gamma \in \mathbb{R}$$

Proof
It comes immediately by formulation above and using proposition 2.6 ■

Corollary 2.4

Let $\alpha \in \mathbb{R}$

$\alpha > 0^* \Longrightarrow -\alpha < 0^*$

$\alpha < 0^* \Longrightarrow -\alpha > 0^*$

Proof

- $\alpha > 0^* \overset{\text{T.2.9}}{\Longrightarrow} \alpha + (-\alpha) > 0^* + (-\alpha) \overset{\text{T.2.4}}{\Longrightarrow} 0^* > 0^* + (-\alpha) \overset{\text{T.2.3}}{\Longrightarrow} 0^* > -\alpha$
- $\alpha < 0^* \overset{\text{T.2.9}}{\Longrightarrow} \alpha + (-\alpha) < 0^* + (-\alpha) \overset{\text{T.2.4}}{\Longrightarrow} 0^* < 0^* + (-\alpha) \overset{\text{T.2.3}}{\Longrightarrow} 0^* < -\alpha$

■

Proposition 2.7

$-(\alpha + \beta) = (-\alpha) + (-\beta) \quad \forall\, \alpha, \beta \in \mathbb{R}$

Proof

$$\begin{aligned}(\alpha + \beta) + (-\alpha) + (-\beta) &\overset{\text{T.2.1}}{=} (\alpha + \beta) + (-\beta) + (-\alpha) \\ &\overset{\text{T.2.2}}{=} \alpha + (\beta + (-\beta)) + (-\alpha) \overset{\text{T.2.4}}{=} \alpha + 0^* + (-\alpha) \\ &\overset{\text{T.2.3}}{=} \alpha + (-\alpha) \overset{\text{T.2.4}}{=} 0^*\end{aligned}$$

Hence $(-\alpha) + (-\beta)$ is the opposite of $\alpha + \beta$ and for uniqueness given by theorem 2.4 we get the thesis
■

Proposition 2.8

Let $\alpha \in \mathbb{R}$

$\alpha > 0^* \Longleftrightarrow 0 \in \alpha$

Proof
$\Longleftarrow)$

$0 \in \alpha \overset{c_1}{\Longrightarrow}$ if $q < 0 \Longrightarrow q \in \alpha \Longleftrightarrow \forall\, q \in 0^* \Longrightarrow q \in \alpha$

$\Longrightarrow)$

By contradiction $0 \notin \alpha \overset{\text{C.2.1}}{\Longrightarrow} p < 0 \quad \forall\, p \in \alpha \Longleftrightarrow \forall\, p \in \alpha, \quad p \in 0^*$

Contradiction since $\alpha \supset 0^*$
■

Proposition 2.9

Let $\alpha \in \mathbb{R}$

$\alpha > 0^* \iff \exists\, A \in \alpha$ and $A > 0$

Proof

$\Longrightarrow)$

$\alpha > 0^* \overset{\text{P.2.8}}{\Longrightarrow} 0 \in \alpha \overset{c_2}{\Longrightarrow} \exists\, A \in \alpha$ and $A > 0$

$\Longleftarrow)$

$\exists\, A \in \alpha$ and $A > 0 \overset{c_1}{\Longrightarrow} 0 \in \alpha \overset{\text{P.2.8}}{\Longrightarrow} \alpha > 0^*$

■

Proposition 2.9 guarantees that the following definition is well posed

Definition 2.15

Let $\alpha, \beta > 0^*$

$(\alpha, \beta)_* := \{p \in \mathbb{Q} \mid \exists\, A \in \alpha, A > 0, \quad B \in \beta, B > 0 \mid p < AB\}$

Proposition 2.10

Let $\alpha, \beta > 0^* \Longrightarrow (\alpha, \beta)_* \in \mathbb{R}$

Proof

- Trivially $0 \in (\alpha, \beta)_*$ and furthermore since $\alpha, \beta \in \mathbb{R}$

  $\exists\, y_a \notin \alpha,\ y_b \notin \beta \Longrightarrow y_a, y_b > 0$ since $0 \in \alpha$ and $0 \in \beta$

  $q := y_a y_b \Longrightarrow q \notin (\alpha, \beta)_* \Longrightarrow (\alpha, \beta)_* \subset \mathbb{Q}$

- Let $p \in (\alpha, \beta)_*$ and let $t \leq p$

  $p \in (\alpha, \beta)_* \Longrightarrow \exists\, A \in \alpha, A > 0, \quad B \in \beta, B > 0 \mid p < AB$

  $\overset{\text{T.1.35}}{\Longrightarrow} t < AB \Longrightarrow t \in (\alpha, \beta)_*$

- Let $p \in (\alpha, \beta)_* \Longrightarrow \exists\, A \in \alpha, A > 0, \quad B \in \beta, B > 0 \mid p < AB$

  $A \in \alpha,\ B \in \beta$ hence applying c_2 we find

  $A_1 > A, \quad A_1 \in \alpha$ and $B_1 > B, \quad B_1 \in \beta$

  Then $p < AB < A_1 B_1 \Longrightarrow (AB) > p$ and $(AB) \in (\alpha, \beta)_*$

■

Proposition 2.11

$(\alpha, \beta)_* = (\beta, \alpha)_* \quad \forall\, \alpha, \beta > 0*$

Proof
It comes immediately by commutativity of product in $\mathbb{Q}$ ■

Proposition 2.12

$$(\alpha,(\beta,\gamma)_*)_* = ((\alpha,\beta)_*,\gamma)_* \quad \forall\, \alpha,\beta,\gamma\ > 0*$$

Proof
It is trivial
■

Definition 2.16

Let $\alpha,\ \beta\ \in \mathbb{R}$

$$\alpha *_{\mathbb{R}} \beta := \begin{cases} 0^* & \text{if } \alpha = 0^* \text{ or } \beta = 0^* \\ (\alpha,\beta)_* & \text{if } \alpha > 0^*, \beta > 0^* \\ (-\alpha,-\beta)_* & \text{if } \alpha < 0^*, \beta < 0^* \\ -((-\alpha,\beta)_*) & \text{if } \alpha < 0^*, \beta > 0^* \\ -((\alpha,-\beta)_*) & \text{if } \alpha > 0^*, \beta < 0^* \end{cases}$$

Notational Remark 2.5
Henceforth we will denote:

$\alpha *_{\mathbb{R}} \beta$ simply as $\alpha * \beta \quad \forall\, \alpha,\beta\ \in \mathbb{R}$

Theorem 2.10

Formulation 2.10.1
Let $\alpha,\ \beta\ \in \mathbb{R}$

$$\alpha > 0^*,\ \beta > 0^* \implies \alpha * \beta > 0^*$$

Proof
We show in the first point of proposition 2.10 that $0 \in (\alpha,\beta)_* \overset{\text{P.2.8}}{\Longrightarrow} (\alpha,\beta)_* > 0^*$
■

Formulation 2.10.2
Let $\alpha,\ \beta\ \in \mathbb{R}$

$$\alpha \geq 0^*,\ \beta \geq 0^* \implies \alpha * \beta \geq 0^*$$

Proof
$\alpha > 0^*,\ \beta > 0^* \implies \alpha * \beta > 0^*$
$\alpha = 0^* \quad \text{or} \quad \beta = 0^* \implies \alpha * \beta \overset{\text{D.2.16}}{=} 0^*$ ■

Theorem 2.11

$$\alpha * \beta = \beta * \alpha \quad \forall\, \alpha, \beta \in \mathbb{R}$$

Proof

- $\alpha = 0^*$ or $\beta = 0^*$ ok
- $\alpha > 0^*, \beta > 0^*$ follows by proposition 2.11
- $\alpha < 0^*, \beta < 0^*$ follows by proposition 2.11
- $\alpha < 0^*, \beta > 0^*$
  $\alpha * \beta \overset{\text{D.2.16}}{=} -((-\alpha, \beta)_*) \overset{\text{P.2.11}}{=} -((\beta, -\alpha)_*) \overset{\text{D.2.16}}{=} \beta * \alpha$
- $\alpha > 0^*, \beta < 0^*$ like above

■

Proposition 2.13

$\alpha * (-\beta) = (-\alpha) * \beta = -(\alpha * \beta) \quad \forall\, \alpha, \beta \in \mathbb{R}$

Proof

- $\alpha = 0^*$
  Nothing to prove
- $\alpha > 0^*$
  - $\beta = 0^*$ nothing to prove
  - $\beta > 0^*$
    $\alpha * (-\beta) \overset{\text{D.2.16}}{=} -(\alpha * (-(-\beta))) = -(\alpha * \beta)$
    On the other hand $(-\alpha) * \beta \overset{\text{D.2.16}}{=} -((-(-\alpha)) * \beta) = -(\alpha * \beta)$
  - $\beta < 0^*$
    $(\alpha * \beta) \overset{\text{D.2.16}}{=} -(\alpha * (-\beta)) \Longrightarrow -(\alpha * \beta) = \alpha * (-\beta)$
    On the other hand
    $(-\alpha) * \beta \overset{\text{D.2.16}}{=} (-(-\alpha)) * (-\beta) = \alpha * (-\beta)$
- $\alpha < 0^*$
  The proof is equal as the case $\alpha > 0^*$

■

Theorem 2.12

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma \qquad \forall\, \alpha, \beta, \gamma\, \in \mathbb{R}$$

Proof

- $\alpha = 0^*$ or $\beta = 0^*$ or $\gamma = 0^*$
  nothing to prove
- $\alpha > 0^*$
  - $\beta > 0^*, \qquad \gamma > 0^*$
    look at proposition 2.12
  - $\beta > 0^*, \qquad \gamma < 0^*$
    $\beta * \gamma \overset{\text{D.2.16}}{=} -(\beta * (-\gamma))$
    Defining $\delta := (\beta * (-\gamma)) \implies \alpha * (\beta * \gamma) = \alpha * (-(\beta * (-\gamma))) = \alpha * (-\delta) \overset{\text{P.2.13}}{=} -(\alpha * \delta)$
    On the other hand
    $(\alpha * \beta) * \gamma \overset{\text{D.2.16}}{=} -((\alpha * \beta) * (-\gamma)) \overset{\text{P.2.12}}{=} -(\alpha * (\beta * (-\gamma))) = -(\alpha * \delta)$
  - $\beta < 0^*, \qquad \gamma > 0^*$
    The proof is the same ,just use theorem 2.1 with $(\beta * \gamma)$
  - $\beta < 0^*, \qquad \gamma < 0^*$
    $\beta * \gamma \overset{\text{D.2.16}}{=} (-\beta) * (-\gamma)$
    Then $\alpha * (\beta * \gamma) = \alpha * ((-\beta) * (-\gamma)) \overset{\text{P.2.12}}{=} (\alpha * (-\beta)) * (-\gamma)$
    On the other hand
    $(\alpha * \beta) \overset{\text{D.2.16}}{=} -(\alpha * (-\beta)$
    $\implies (\alpha * \beta) * \gamma \overset{\text{D.2.16}}{=} (-(\alpha * (-\beta)) * (-\gamma))$
    Defining $-\delta := (\alpha * (-\beta))$ we get
    $$\begin{aligned}(\alpha * \beta) * \gamma = (-\delta) * (-\gamma) &\overset{\text{P.2.13}}{=} -((-\delta) * \gamma) \\ = -((\alpha * (-\beta)) * \gamma) &\overset{\text{P.2.13}}{=} (\alpha * (-\beta)) * (-\gamma)\end{aligned}$$
- $\alpha < 0^*$
  The proof is the same as $\alpha > 0^*$

■

Theorem 2.13

$$\alpha * 1^* = \alpha \qquad \forall\, \alpha\, \in \mathbb{R}$$

Proof

- $\alpha = 0^*$
  Nothing to prove
- $\alpha > 0^*$
  By Extensionality we will show that $p \in \ \alpha * 1^* \iff p \in \alpha$
  $\Longrightarrow)$
  Let $p \in \alpha * 1^*$
  $$\left.\begin{array}{l} p \in \alpha * 1^* \Longrightarrow \exists\, A \in \alpha, A > 0,\ B \in 1^*, B > 0 \mid p < AB \\ B < 1 \overset{\text{P.1.38}}{\Longrightarrow} AB < A \overset{\text{T.1.35}}{\Longrightarrow} p < A \end{array}\right\} \overset{c_1}{\Longrightarrow} p \in \alpha$$
  $\Longleftarrow)$
  Let $p \in \alpha$
  Applying two times c_2 let $r_1 > r > p \quad r_1, r \ \in \alpha$
  Since $\alpha > 0^* \overset{\text{P.2.9}}{\Longrightarrow} \exists\, q > 0, \quad q \in \alpha \overset{c_2}{\Longrightarrow} \exists\, q_1 > q \quad q_1 \in \alpha$
  $$m := \begin{cases} q_1 & \text{if } q_1 \geq r_1 \\ r_1 & \text{if } q_1 < r_1 \end{cases}$$
  Then $m > 0, \quad m > r, \quad m > q$
  Now a few of considerations:
  On one hand $r \overset{\text{T.1.31}}{=} r1 \overset{\text{T.1.32}}{=} r(mm^{-1}) \overset{\text{T.1.30}}{=} (rm^{-1})m$
  On the other hand $r < m \overset{\text{P.1.38}}{\Longrightarrow} rm^{-1} < 1 \Longrightarrow (rm^{-1}) \ \in 1^*$
  And hence calling $A := m, \quad B := (rm^{-1})$ then
  $\exists\, A \in \alpha,\ A > 0, \quad B \in 1^*, B > 0$ and $p < AB \Longrightarrow p \in \alpha * 1^*$
- $\alpha < 0^*$
  $\alpha * 1^* \overset{\text{D.2.16}}{=} -(-\alpha, 1^*) = -(-\alpha) = \alpha$

■

Definition 2.17

Let $\alpha > 0^*$
$\xi_\alpha := \{p \in \mathbb{Q} \ \mid \ \exists\, R \notin \alpha \ \mid \ pR < 1\}$

Proposition 2.14

$$\alpha > 0^* \quad \Longrightarrow \begin{cases} \xi_\alpha \in \mathbb{R} \\ \xi_\alpha > 0 \\ \alpha * \xi_\alpha = 1^* \\ \text{if} \gamma \in \mathbb{R},\ \gamma > 0^*,\ \alpha * \gamma = 1^* \Longrightarrow \gamma = \xi_\alpha \end{cases}$$

Proof

- $\xi_\alpha \in \mathbb{R}$:
  - $\alpha \neq \mathbb{Q} \Longrightarrow \exists\, A \notin \alpha$
    $0 = 0A \ < 1 \Longrightarrow 0 \in \xi_\alpha \Longrightarrow \xi_\alpha \neq \emptyset$
  - $\alpha \neq \mathbb{Q} \Longrightarrow \exists\, A \notin \alpha$ and $A > 0$ (since $0 \in \alpha$)
    Then by theorem 1.28 $\exists\, A^{-1}$ and $AA^{-1} = 1 \Longrightarrow A^{-1} \notin \xi_\alpha$
  - Let $p \in \xi_\alpha$ $(\exists\, R \notin \alpha \mid pR < 1)$ and let $q < p$
    Since $R > 0 \overset{\text{P.1.38}}{\Longrightarrow} qR < pR < 1 \Longrightarrow q \in \xi_\alpha$
  - Let $p \in \xi_\alpha$ $(\exists\, R \notin \alpha \mid pR < 1)$
    Since $R > 0,\ pR < 1 \Longrightarrow p < R^{-1}$
    Then if we define $r := (p + R^{-1})2^{-1}$, by remark 1.8 $p < r < R^{-1}$
    Then $rR < 1 \Longrightarrow r \in \xi_\alpha$
- $\xi_\alpha > 0^*$:
  $\forall\, R > 0,\ R \notin \alpha \quad R0 = 0 < 1 \Longrightarrow 0 \in \xi_\alpha \overset{\text{P.2.8}}{\Longleftrightarrow} \xi_\alpha > 0^*$
- $\alpha * \xi_\alpha = 1^*$:
  By Extensionality $p \in \alpha * \xi_\alpha \Longleftrightarrow p \in 1^*$
  $\Longrightarrow$)
  Let $p \in \alpha * \xi_\alpha \Longrightarrow \exists\, A \in \alpha, A > 0, \quad B \in \xi_\alpha, B > 0 \mid p < AB$
  $B \in \xi_\alpha \overset{\text{D.2.17}}{\Longrightarrow} \exists\, R \notin \alpha \mid BR < 1$
  $R \notin \alpha \overset{\text{C.2.1}}{\Longrightarrow} A < R \Longrightarrow AB < RB \Longrightarrow p < AB < RB < 1 \overset{\text{T.1.35}}{\Longrightarrow} p < 1 \Longrightarrow p \in 1^*$
  $\Longleftarrow$)
  Let $p \in 1^*$
  If $p \leq 0$
  $\xi_\alpha > 0^*,\ \alpha > 0^* \overset{\text{T.2.9}}{\Longrightarrow} \alpha * \xi_\alpha > 0^* \overset{\text{P.2.8}}{\Longrightarrow} 0 \in \alpha * \xi_\alpha \overset{c_1}{\Longrightarrow} p \in \alpha * \xi_\alpha$
  Hence suppose $0 < p < 1$
  This part of the proof is quite long and we proceed by steps[4]:

[4] There is another way to prove this result which uses directly Archimedean property of $\mathbb{Q}$(Lemma

1. $\exists\, C \notin \alpha$ such that $(pC) \in \alpha$:

   On one hand

   $\alpha \subset \mathbb{Q} \implies \exists\, q \notin \alpha$

   $q > 0$ since $0 \in \alpha \overset{\text{P.1.39}}{\implies} q^{-1} > 0$

   On the other hand

   $\alpha > 0^* \overset{\text{P.2.9}}{\implies} \exists\, r \in \alpha$ and $r > 0$

   Hence $rq^{-1} > 0$ and by proposition 1.44 since $p < 1$

   $\exists\, m \in \mathbb{N} \;\;|\;\; p^m < rq^{-1} \implies p^m q < r \overset{c_1}{\implies} p^m q \in \alpha$

   Now let $k_1 := pq = p^1 q$

   If $k_1 \in \alpha$ we have done since $q \notin \alpha$

   if $k_1 \notin \alpha \implies$ $k_2 := pk_1 = p^2 q$

   If $k_2 \in \alpha$ we have done since $k_1 \notin \alpha$

   If $k_2 \notin \alpha \implies k_3 := pk_2 = p^3 q \ldots$

   If we continued in this way until defining $k_{m+1} := p^{m+1} q$

   it will be a contradiction since surely $k_m = p^m q \in \alpha$

   Hence $\exists\, n \;\;|\;\; p^n q \notin \alpha$ and $p^{n+1} q = pp^n q \in \alpha$

   Hence calling $C := p^n q$ we get the thesis

2. $\exists\, A \in \alpha,\, A > 0 \;\;|\;\; pA^{-1} < C^{-1}$:

   $pC \in \alpha \overset{c_2}{\implies} \exists\, A \in \alpha \;\;|\;\; A > pC$

   Since $pC > 0 \implies A > 0$ And hence we get the thesis

3. $\exists\, B \in \xi_\alpha,\, B > 0$ such that $p < AB$:

   Recalling remark 1.8 let $B \;\;|\;\; pA^{-1} < B < C^{-1}$

   $$\left.\begin{array}{l} A > 0 \implies A^{-1} > 0 \\ p > 0 \end{array}\right\} \overset{\text{T.1.39}}{\implies} pA^{-1} > 0 \implies B > 0$$

   On one hand

   $B < C^{-1} \implies BC < 1 \overset{\text{D.2.17}}{\implies} B \in \xi_\alpha$ since $C \notin \alpha$

   On the other hand

   $pA^{-1} < B \overset{\text{P.1.38}}{\implies} p < AB$

Hence by definition 2.15 $p \in \alpha * \xi_\alpha$

- $\gamma \in \mathbb{R},\, \gamma > 0^*,\, \alpha * \gamma = 1^* \implies \gamma = \xi_\alpha$:

  $\gamma \overset{\text{T.2.13}}{=} \gamma * 1^* = \gamma * (\alpha * \xi_\alpha) \overset{\text{T.2.12}}{=} (\gamma * \alpha) * \xi_\alpha = 1^* * \xi_\alpha \overset{\text{T.2.13}}{=} \xi_\alpha$

1.6) and does not use Powers. Although we use Powers of rational numbers, it is essentially the same since in the following proof we will proposition 1.44 proved by Bernoulli's Lemma(Lemma 1.5) that we have proved through Archimedean Property of $\mathbb{Q}$. To understand this alternative way we recommend to see [La1] and [SD1]

■

Definition 2.18

Let $\alpha \neq 0^*$

$$\alpha^{-1} := \begin{cases} \xi_\alpha & \text{if } \alpha > 0^* \\ -(\xi_{-\alpha}) & \text{if } \alpha < 0^* \end{cases}$$

Proposition 2.15

$\alpha > 0^* \Longrightarrow \alpha^{-1} > 0^*$
$\alpha < 0^* \Longrightarrow \alpha^{-1} < 0^*$

Proof

$\alpha > 0^* \overset{\text{D.2.18}}{\Longrightarrow} \alpha^{-1} = \xi_\alpha \overset{\text{P.2.14}}{\Longrightarrow} \xi_\alpha > 0^*$

$\alpha < 0^* \overset{\text{C.2.4}}{\Longrightarrow} -\alpha > 0^* \overset{\text{P.2.14}}{\Longrightarrow} \xi_{-\alpha} > 0^* \overset{\text{C.2.4}}{\Longrightarrow} -(\xi_{-\alpha}) < 0^*$ ■

Theorem 2.14

$$\forall \alpha \in \mathbb{R},\, \alpha \neq 0^*, \quad \exists!\ \alpha^{-1} \in \mathbb{R} \quad \text{such that} \quad \alpha * \alpha^{-1} = 1^*$$

Proof

- $\alpha > 0^*$
  $\alpha * \alpha^{-1} \overset{\text{D.2.18}}{=} \alpha * \xi_\alpha \overset{\text{P.2.14}}{=} 1^*$
- $\alpha < 0^*$
  $\alpha * \alpha^{-1} = -\alpha * (-(-\xi_{-\alpha})) = -\alpha * \xi_{-\alpha} \overset{\text{P.2.14}}{=} 1^*$

■

Proposition 2.16

$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma \quad \forall \alpha > 0^*,\, \beta > 0^*,\, \gamma > 0^*$

Proof

We will show that $p \in \alpha * (\beta + \gamma) \Longleftrightarrow p \in \alpha * \beta + \alpha * \gamma$

$\Longrightarrow)$

Let $p \in \alpha * (\beta + \gamma) \Longleftrightarrow \exists A \in \alpha, A > 0, \quad K \in (\beta + \gamma), K > 0$ and $p \leq AK$.

$K \in (\beta + \gamma) \Longleftrightarrow K = b + c, \quad b \in \beta,\, c \in \gamma$

Since $\beta > 0^* \overset{\text{P.2.9}}{\Longrightarrow} \exists B \in \beta$ and $B > 0$

We define $B_1 := \begin{cases} b & \text{if } b \geq B \\ B & \text{if } B > b \end{cases}$

Then $B_1 > 0, \quad B_1 \geq b$

Repeating the same reasoning for γ we defined C_1 and then

$AB_1 \in \alpha * \beta, \qquad AC_1 \in \alpha * \gamma, \qquad p \leq AB_1 + AC_1$

Let $q := p - AC_1 \overset{\text{T.1.38}}{\Longrightarrow} q \leq AB_1 \overset{c_1}{\Longrightarrow} q \in \alpha * \beta$

Hence $p \overset{\text{T.1.27}}{=} p + 0 \overset{\text{T.1.28}}{=} p + (-AC_1 + AC_1) \overset{\text{T.1.26}}{=} q + AC_1 \Longrightarrow p \in \alpha * \beta + \alpha * \gamma$

$\Longrightarrow)$

Let $p \in \alpha * \beta + \alpha * \gamma \iff p = H + K$ with $H \in \alpha * \beta, \qquad K \in \alpha * \gamma$

Since $H \in \alpha * \beta \Longrightarrow \exists\, A \in \alpha, A > 0, \quad B \in \beta, B > 0$ and $H \leq AB$

Repeating the same reasoning for K we get:

$p = H + K \leq AB + AC$

$\overset{\text{T.1.37}}{=} A(B + C)$ with $A \in \alpha, A > 0, \ (B + C) \in (\beta + \gamma), (B + C) > 0$

$\overset{\text{D.2.15}}{\Longrightarrow} p \in \alpha * (\beta + \gamma)$

■

Theorem 2.15

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma \quad \forall\, \alpha, \beta, \gamma \in \mathbb{R}$$

Proof

- $\alpha = 0^* \quad$ or $\quad \beta = 0^* \quad$ or $\quad \gamma = 0^*$

  Nothing to prove

- $\alpha > 0^*$

  - $(\beta + \gamma) = 0^* \Longrightarrow \alpha * (\beta + \gamma) = 0^*$

    By proposition 2.6 $\quad \beta = -\gamma$

    $\alpha * \beta = \alpha * (-\gamma) \overset{\text{P.2.13}}{=} -(\alpha * \gamma)$

    And then we got the result

  - $(\beta + \gamma) > 0^*, \quad \gamma < 0^* \qquad (\beta > 0^*$ since if $\beta < 0^* \Longrightarrow (\beta + \gamma) < 0^*)$

    Let $\beta_1 := (\beta + \gamma), \quad \gamma_1 := -\gamma$

    $\beta_1 > 0^*, \gamma_1 > 0^* \overset{\text{P.2.16}}{\Longrightarrow} \alpha * (\beta_1 + \gamma_1) = \alpha * \beta_1 + \alpha * \gamma_1$

    On the other hand

    $\alpha * (\beta_1 + \gamma_1) = \alpha * \beta \quad$ and $\alpha * \gamma_1 = \alpha * (-\gamma) \overset{\text{P.2.13}}{=} -(\alpha * \gamma)$

    And then

    $\alpha * (\beta + \gamma) - (\alpha * \gamma) = \alpha * \beta \overset{\text{P.2.6}}{\Longrightarrow} \alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$

- $(\beta+\gamma) > 0^*, \quad \beta < 0^*$

  The proof is the same as the point just above

- $(\beta+\gamma) < 0^*, \quad \gamma > 0^* \qquad (\beta < 0^*$ because if $\beta > 0^* \Longrightarrow (\beta+\gamma) > 0^*)$

  Let $\beta_1 := -(\beta+\gamma)$

  $\beta_1 > 0^*, \gamma > 0^* \overset{\text{P.2.16}}{\Longrightarrow} \alpha * (\beta_1 + \gamma) = \alpha * \beta_1 + \alpha * \gamma$

  On one hand

  $\alpha * (\beta_1 + \gamma_1) = \alpha * (-\beta) \overset{\text{P.2.13}}{=} -(\alpha * \beta)$

  On the other hand

  $\alpha * \beta_1 = \alpha * (-(\beta+\gamma)) \overset{\text{P.2.13}}{=} -(\alpha * (\beta+\gamma))$

  Hence

  $-(\alpha * (\beta+\gamma)) + (\alpha * \gamma) = -(\alpha * \beta)$

  $\overset{\text{P.2.6}}{\Longrightarrow} -(\alpha * (\beta+\gamma)) = -(\alpha * \beta) - (\alpha * \gamma) \overset{\text{P.2.7}}{=} -((\alpha * \beta) + (\alpha * \gamma))$

- $(\beta+\gamma) < 0^*, \quad \beta > 0^*$

  The proof is the same as the point just above

- $\alpha < 0^*$

  The proof is the same as the case $\alpha > 0^*$

■

Theorem 2.16 (Least Upper Bound Property)

$$\left.\begin{array}{l} A \subset \mathbb{R},\, A \neq \emptyset \\ A \ \text{bounded above} \end{array}\right\} \Longrightarrow \exists \quad \gamma \ = \ \sup A$$

Proof

$\gamma := \cup_{\alpha \in A}\, \alpha = \{p \in \mathbb{Q} \mid \exists\, \alpha \in A \quad | \quad p \in \alpha\}$

- $\gamma \in \mathbb{R}$:

  - $\left.\begin{array}{ll} A \neq \emptyset & \Longrightarrow \exists\, \alpha \in A \\ \alpha \in \mathbb{R} & \Longrightarrow \exists\, p \in \alpha \end{array}\right\} \Longrightarrow \exists\, p \in \gamma \Longrightarrow \gamma \neq \emptyset$

  - A bounded above $\overset{\text{D.2.1}}{\Longrightarrow} \exists\, \beta$ upper bound of A

    Hence by definition 2.1 $\quad \forall\, \alpha \in A \Longrightarrow \alpha \leq \beta \overset{\text{D.2.14}}{\Longleftrightarrow} \alpha \subseteq \beta$

    On the other hand

    $\beta \subset \mathbb{Q} \Longrightarrow \exists\, y \notin \beta \Longrightarrow y \notin \alpha \quad \forall\, \alpha \in A \Longrightarrow y \notin \gamma \Longrightarrow \gamma \neq \mathbb{Q}$

  - Let $p \in \gamma, \quad q < p$

    $p \in \gamma \Longrightarrow \exists\, \alpha \in A$ such that $p \in \alpha \overset{c_1}{\Longrightarrow} q \in \alpha \Longrightarrow q \in \gamma$

  - Let $p \in \gamma \Longrightarrow \exists\, \alpha \in A$ such that $p \in \alpha \overset{c_2}{\Longrightarrow} \exists\, r > p, \quad r \in \alpha \Longrightarrow r > p, \quad r \in \gamma$

- $S_1)$ γ is an upper bound for A:
  It 's clear that
  $\forall\, \alpha \in A, \quad \text{if } p \in \alpha \implies p \in \gamma \implies \forall\, \alpha \in A \implies \alpha \leq \gamma$
- $S_2)$ If γ_1 is upper bound for $A \implies \gamma \leq \gamma_1$:
  Suppose $\gamma_1 < \gamma \iff \gamma_1 \subset \gamma \iff \exists\, p \in \gamma, \quad p \notin \gamma_1$
  Now $p \in \gamma \implies \exists\, \alpha \in A$ such that $p \in \alpha$
  $\exists\, p \in \alpha, \quad p \notin \gamma_1 \implies \gamma_1 \subset \alpha \overset{\text{D.2.13}}{\implies} \alpha < \gamma_1$
  But this is a contradiction since γ_1 is an upper bound for A

■

2.2 Construction of $\mathbb{R}$ via Rational Cauchy sequences

This section will be as rigorous as the precedent one,but we will omit the proofs of many propositions, corollary and theorems. Anyway this sections will builds, step by step, the Real Numbers system as precisely as the precedent ones.

It would be a good exercise proving all the results
Notational Remark 2.6
In this Section we will denote

$p +_{\mathbb{Q}} q$ simply as $p + q \quad \forall\, p, q \in \mathbb{Q}$
$p *_{\mathbb{Q}} q$ simply as $pq \quad \forall\, p, q \in \mathbb{Q}$
$p \leq_{\mathbb{Q}} q$ simply as $p \leq q \quad \forall\, p, q \in \mathbb{Q}$
$p <_{\mathbb{Q}} q$ simply as $p < q \quad \forall\, p, q \in \mathbb{Q}$

Definition 2.19

Let $p \in \mathbb{Q}$

$$|\, p \,|_{\mathbb{Q}} := \begin{cases} p & \text{If } p \geq 0 \\ -p & \text{If } p < 0 \end{cases}$$

Proposition 2.17

The following properties holds

- $|\, p \,|_{\mathbb{Q}} \geq 0 \quad \forall\, p \in \mathbb{Q}$
- $|\, p \,|_{\mathbb{Q}} = 0 \iff p = 0$
- $|\, p + q \,|_{\mathbb{Q}} \leq |\, p \,|_{\mathbb{Q}} + |\, q \,|_{\mathbb{Q}} \quad \forall\, p, q \in \mathbb{Q}$
- $|\, pq \,|_{\mathbb{Q}} = |\, p \,|_{\mathbb{Q}} |\, q \,|_{\mathbb{Q}} \quad \forall\, p, q \in \mathbb{Q}$

Definition 2.20

A sequence in $\mathbb{Q}$ is a function $f : \mathbb{N} \longrightarrow \mathbb{Q}$
And we denote it as $\{ f_n \}_{n\in\mathbb{N}}$

Remark 2.6

We recommend the reader not confusing $\{ f_n \}_{n\in\mathbb{N}}$ which is a set in $\mathbb{N} \times \mathbb{Q}$ with $\{f_n \mid n \in \mathbb{N}\}$ which is a set $\mathbb{Q}$

Definition 2.21

Let $\{ a_n \}_{n\in\mathbb{N}}$ sequence in $\mathbb{Q}$
$\{ a_n \}_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q} \iff \forall\, r > 0\, \exists\, n \in \mathbb{N}$ such that

$$|\, a_k - a_m \,|_{\mathbb{Q}} < r \quad \forall\, k, m \geq n$$

Definition 2.22

Let $q \in \mathbb{Q}$
Let $f_q := \{(n, q) \mid n \in \mathbb{N}\}$.
Then f_q is a sequence in $\mathbb{Q}$ and we denote it as $C(q)$

Definition 2.23

$\mathbb{Q}_{Cs} := \{\{ a_n \}_{n\in\mathbb{N}} \;\mid\; \{ a_n \}_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}\,\}$
$\mathbb{Q}_{Cs} \neq \emptyset$ since $C(q) \in \mathbb{Q}_{Cs} \quad \forall\, q \in \mathbb{Q}$

We define an equivalence relation on $\mathbb{Q}_{Cs}$ in this way:
Let $\{ a_n \}_{n\in\mathbb{N}}, \{ b_n \}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs}$
$\{ a_n \}_{n\in\mathbb{N}} \equiv \{ b_n \}_{n\in\mathbb{N}} \iff \forall\, r \in \mathbb{Q}\, r > 0 \quad \exists\, n \in \mathbb{N}$ such that

$$|\, a_k - b_k \,|_{\mathbb{Q}} < r \quad \forall\, k \geq n$$

It easy to verify that $\equiv$ is an equivalence relation on $\mathbb{Q}_{Cs}$.

Definition 2.24

$\mathbb{R} := \frac{\mathbb{Q}_{Cs}}{\equiv}$

Definition 2.25

Let $\{ a_n \}_{n\in\mathbb{N}}$ sequence in $\mathbb{Q}$

$\{\,a_n\,\}_{n\in\mathbb{N}}$ is Bounded in $\mathbb{Q} \iff \exists\, K \in \mathbb{Q}, K > 0 \quad | \quad |\,a_n\,|_{\mathbb{Q}} \leq K \quad \forall\, n \in \mathbb{N}$

Proposition 2.18

Let $\{\,a_n\,\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \implies \{\,a_n\,\}_{n\in\mathbb{N}}$ is Bounded in $\mathbb{Q}$

Proposition 2.19

Let $\{\,a_n\,\}_{n\in\mathbb{N}}, \{\,b_n\,\}_{n\in\mathbb{N}}, \{\,A_n\,\}_{n\in\mathbb{N}}, \{\,B_n\,\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs}$

$$\left.\begin{array}{l} \{\,a_n\,\}_{n\in\mathbb{N}} \equiv \{\,A_n\,\}_{n\in\mathbb{N}} \\ \{\,b_n\,\}_{n\in\mathbb{N}} \equiv \{\,B_n\,\}_{n\in\mathbb{N}} \end{array}\right\} \implies \begin{cases} \{a_n + b_n\}_{n\in\mathbb{N}}, \{A_n + B_n\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \\ \{a_n + b_n\}_{n\in\mathbb{N}} \equiv \{A_n + B_n\}_{n\in\mathbb{N}} \\ \{a_n\, b_n\}_{n\in\mathbb{N}}, \{A_n\, B_n\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \\ \{a_n\, b_n\}_{n\in\mathbb{N}} \equiv \{A_n\, B_n\}_{n\in\mathbb{N}} \\ \{\,-a_n\,\}_{n\in\mathbb{N}}, \{\,-A_n\,\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \\ \{\,-a_n\,\}_{n\in\mathbb{N}} \equiv \{\,-A_n\,\}_{n\in\mathbb{N}} \end{cases}$$

In virtue of proposition 2.19 the following definitions are well posed

Definition 2.26

Let $\alpha, \beta \in \mathbb{R}$

- $\alpha +_{\mathbb{R}} \beta := [\{a_n + b_n\}_{n\in\mathbb{N}}]$ where $\{\,a_n\,\}_{n\in\mathbb{N}} \in \alpha$ and $\{\,b_n\,\}_{n\in\mathbb{N}} \in \beta$
- $\alpha *_{\mathbb{R}} \beta := [\{a_n + b_n\}_{n\in\mathbb{N}}]$ where $\{\,a_n\,\}_{n\in\mathbb{N}} \in \alpha$ and $\{\,b_n\,\}_{n\in\mathbb{N}} \in \beta$

Notational Remark 2.7
Henceforth we will denote

$\alpha +_{\mathbb{R}} \beta$ *as* $\alpha + \beta$
$\alpha *_{\mathbb{R}} \beta$ *as* $\alpha * \beta$

Theorem 2.17

$$\alpha + \beta = \beta + \alpha \quad \forall\, \alpha, \beta \in \mathbb{R}$$

Theorem 2.18

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \quad \forall\, \alpha, \beta, \gamma \in \mathbb{R}$$

Definition 2.27

$\mathbf{0} := [C(0)]$

Theorem 2.19

$$\alpha + \mathbf{0} = \alpha \quad \forall \alpha \in \mathbb{R}$$

Theorem 2.20

$$\forall \alpha \in \mathbb{R} \quad \exists! \beta \in \mathbb{R} \quad \text{such that} \;\; \alpha + \beta = \mathbf{0}$$

Theorem 2.21

$$\alpha * \beta = \beta * \alpha \quad \forall \alpha, \beta \in \mathbb{R}$$

Theorem 2.22

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma \qquad \forall \alpha, \beta, \gamma \in \mathbb{R}$$

Theorem 2.23

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{R}$$

Definition 2.28

$\mathbf{1} := [C(1)]$

Theorem 2.24

$$\alpha * \mathbf{1} = \alpha \qquad \forall \alpha \in \mathbb{R}$$

Proposition 2.20

Let $\{ a_n \}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs}$, $\{ a_n \}_{n\in\mathbb{N}} \notin \mathbf{0}$

Then exists $\{ \widehat{a}_n \}_{n\in\mathbb{N}}$ such that $\begin{cases} \{ \widehat{a}_n \}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \\ \{ \widehat{a}_n \}_{n\in\mathbb{N}} \equiv \{ a_n \}_{n\in\mathbb{N}} \\ \widehat{a}_n \neq 0 \quad \forall n \in \mathbb{N} \\ \{(\widehat{a}_n)^{-1}\}_{n\in\mathbb{N}} \in Q_{Cs} \\ \{a_n \cdot (\widehat{a}_n)^{-1}\}_{n\in\mathbb{N}} \equiv C(1) \end{cases}$

Theorem 2.25

$$\forall \alpha \in \mathbb{R}, \alpha \neq \mathbf{0}, \quad \exists! \; \alpha^{-1} \in \mathbb{R} \quad \text{such that} \quad \alpha * \alpha^{-1} = \mathbf{1}$$

Definition 2.29

Let $\{ a_n \}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs}$

- $\{ a_n \}_{n\in\mathbb{N}}$ is Definetely negative (Dn) $\iff \exists\, q \in \mathbb{Q},\ q < 0, \quad \exists\, n \in \mathbb{N} \ |$
  $a_m \le q \quad \forall\, m \ge n$
- $\{ a_n \}_{n\in\mathbb{N}}$ is Definetely positive (Dp) $\iff \{ -a_n \}_{n\in\mathbb{N}}$ is Dn

Proposition 2.21

Let $\{ a_n \}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs}$
One and only one of the following statements holds:

- $\{ a_n \}_{n\in\mathbb{N}} \in \mathbf{0}$
- $\{ a_n \}_{n\in\mathbb{N}}$ is Dp
- $\{ a_n \}_{n\in\mathbb{N}}$ is Dn

Proposition 2.22

Let $\alpha \in \mathbb{R}$, $\alpha \ne \mathbf{0}$

- If $\exists \{ a_n \}_{n\in\mathbb{N}} \in \alpha$, $\{ a_n \}_{n\in\mathbb{N}}$ Dp $\implies \forall \{ b_n \}_{n\in\mathbb{N}} \in \alpha \quad \{ b_n \}_{n\in\mathbb{N}}$ is Dp
- If $\exists \{ a_n \}_{n\in\mathbb{N}} \in \alpha$, $\{ a_n \}_{n\in\mathbb{N}}$ Dn $\implies \forall \{ b_n \}_{n\in\mathbb{N}} \in \alpha \quad \{ b_n \}_{n\in\mathbb{N}}$ is Dn

In virtue of proposition 2.22 the following definition is well posed

Definition 2.30

Let $\alpha, \beta \in \mathbb{R}$
$\alpha <_{\mathbb{R}} \beta \iff \exists \{ a_n \}_{n\in\mathbb{N}} \in \alpha - \beta \ | \ \{ a_n \}_{n\in\mathbb{N}}$ is Dn

Definition 2.31

Let $\alpha, \beta \in \mathbb{R}$
$\alpha \le_{\mathbb{R}} \beta \iff \alpha <_{\mathbb{R}} \beta$ or $\alpha = \beta$

Notational Remark 2.8
Henceforth we will denote

$\alpha <_{\mathbb{R}} \beta$ as $\alpha < \beta$
$\alpha \le_{\mathbb{R}} \beta$ as $\alpha \le \beta$

Theorem 2.26

$$\alpha \leq \alpha \quad \forall\, \alpha \in \mathbb{R}$$

Theorem 2.27

$$\left.\begin{array}{l} \beta \leq \alpha \\ \alpha \leq \beta \end{array}\right\} \Longrightarrow \alpha = \beta$$

Theorem 2.28

$$\left.\begin{array}{l} \alpha \leq \alpha_1 \\ \alpha_1 \leq \alpha_2 \end{array}\right\} \Longrightarrow \alpha \leq \alpha_2$$

Theorem 2.29

Formulation 2.29.1

$$\forall\, \alpha, \beta \in \mathbb{R} \quad \text{one and only one of the following holds :} \quad \alpha = \beta, \quad \alpha < \beta, \quad \alpha > \beta$$

Formulation 2.29.2

$$\forall\, \alpha, \beta \in \mathbb{R} \Longrightarrow \alpha \leq \beta \quad \text{or} \quad \alpha \leq \beta$$

Theorem 2.30

Formulation 2.30.1

$$\alpha > \mathbf{0},\, \beta > \mathbf{0} \;\Longrightarrow\; \alpha * \beta > \mathbf{0}$$

Formulation 2.30.2

$$\alpha \geq \mathbf{0},\, \beta \geq \mathbf{0} \;\Longrightarrow\; \alpha * \beta \geq \mathbf{0}$$

Theorem 2.31

Formulation 2.31.1
Let $\alpha, \beta \in \mathbb{R}$

$$\alpha < \beta \Longleftrightarrow \alpha + \gamma < \beta + \gamma \quad \forall\, \gamma \in \mathbb{R}$$

Formulation 2.31.2
Let $\alpha, \beta \in \mathbb{R}$

$$\alpha \leq \beta \Longleftrightarrow \alpha + \gamma \leq \beta + \gamma \quad \forall\, \gamma \in \mathbb{R}$$

Theorem 2.32 (Least Upper Bound Property)

$$\left.\begin{array}{l} A \subset \mathbb{R},\ A \neq \emptyset \\ A \text{ bounded above} \end{array}\right\} \Longrightarrow \exists \quad \gamma = \sup A$$

Proof

We divide this proof in eight steps

1. $A \neq \emptyset \Longrightarrow \exists\, \alpha \in A$

   Let $\{ a_n \}_{n\in\mathbb{N}} \in \alpha \overset{\text{P.2.18}}{\Longrightarrow} \exists\, K \in \mathbb{Q}, K > 0 \quad | \quad |\, a_n\,|_{\mathbb{Q}} \leq K \quad \forall\, n \in \mathbb{N}$

   On the other hand according to definition 2.23 used with $\varepsilon = 1$

   If $\{ b_n \}_{n\in\mathbb{N}} \equiv \{ a_n \}_{n\in\mathbb{N}} \Longrightarrow \exists\, N \in \mathbb{N} \quad | \quad |\, b_n - a_n\,|_{\mathbb{Q}} \leq 1 \quad \forall\, n \geq N$

   $\Longrightarrow \exists\, N \in \mathbb{N} \quad | \quad -\,|\, b_n - a_n\,|_{\mathbb{Q}} \geq -1 \quad \forall\, n \geq N$

   Hence $\quad b_n \geq -|\, b_n\,|_{\mathbb{Q}} \geq -|\, b_n - a_n\,|_{\mathbb{Q}} - |\, a_n\,|_{\mathbb{Q}} \geq -(1+K) \quad \forall\, n \geq N$

   Hence $\quad b_n \geq -(1+K) \quad \forall\, n \geq N \Longrightarrow b_n + (K+2) \geq 1 \quad \forall\, n \geq N$

   $\Longrightarrow b_n + (K+2) > (2^{-1}) \quad \forall\, n \geq N$

   $\overset{\text{D.2.29}}{\Longrightarrow} \{b_n + (K+2)\}_{n\in\mathbb{N}}$ is Dp

   $\overset{\text{D.2.30}}{\Longrightarrow}$ Calling $L := -(K+2) \quad \alpha > [C(L)]$

2. $\exists\, U \in \mathbb{Q} \quad | \quad [C(U)]$ is upper bound for A:

   A is bounded above $\Longrightarrow \exists\, \beta$ upper bound for A

   As we did in the first step of this proof

   we can find $U \quad | \quad [C(U)] > \beta \Longrightarrow [C(U)]$ is upper bound for A

3. Recalling Remark 1.8 we define $m(a,b) := (a+b)\cdot 2^{-1} \quad \forall\, a, b \in \mathbb{Q}$

   According to Remark 1.1 let us apply Recursion Theorem (Lemma 1.2) with:

   $V := (\mathbb{Q}\times\mathbb{Q}) \quad u := (L, U)$ and

   $$g((a,b)) := \begin{cases} (a, m(a,b)) & \text{If } C(m(a,b)) \text{ is an upper bound for } A \\ (m(a,b), b) & \text{Otherwise} \end{cases}$$

   Then $\quad \exists! \quad R_{g,u} : \mathbb{N} \longrightarrow V \quad | \quad \begin{cases} R_{g,u}(1) = u \\ R_{g,u}(k+1) = g(R_{g,u}(k)) \quad \forall\, k \in \mathbb{N} \end{cases}$

   Let $p_1(a,b) := a,\ \ p_2(a,b) := b \quad \forall\,(a,b) \in \mathbb{Q}\times\mathbb{Q}$

4. Define $\{ l_n \}_{n\in\mathbb{N}}, \{ u_n \}_{n\in\mathbb{N}}$ sequences in $\mathbb{Q}$ as follows:

   $l_n := p_1(R_{G,A}(n))\ \forall\, n \in \mathbb{N}, \quad u_n := p_2(R_{G,A}(n))\ \forall\, n \in \mathbb{N}$

5. $\left.\begin{array}{l}\{\, l_n \,\}_{n\in\mathbb{N}}, \{\, u_n \,\}_{n\in\mathbb{N}} \in \mathbb{Q}_{Cs} \\ \{\, u_n \,\}_{n\in\mathbb{N}} \equiv \{\, l_n \,\}_{n\in\mathbb{N}}\end{array}\right\} \Longrightarrow$ Let $\gamma := [\{\, u_n \,\}_{n\in\mathbb{N}}]$

6. γ satisfies $\begin{cases} S_1) & \gamma \text{ is an upper bound for } A \\ S_2) & \text{If } \gamma_1 \text{ is upper bound for } A \Longrightarrow \gamma_1 \geq \gamma \end{cases}$

■

Immersion Theorem 2.1

We have just built a COF $\left(\mathbb{R},\, +_{\mathbb{R}},\, *_{\mathbb{R}},\, <_{\mathbb{R}}\right)$ from an OF $\left(\mathbb{Q},\, +_{\mathbb{Q}},\, *_{\mathbb{Q}},\, <_{\mathbb{Q}}\right)$ in two different ways.

As in Immersion Theorem 1.2 there exists $J_2 : \mathbb{Q} \longrightarrow \mathbb{R}$ such that

1. J_2 is injective
2. $J_2(q +_{\mathbb{Q}} p) = J_2(q) +_{\mathbb{R}} J_2(p) \qquad \forall\, q, p \in \mathbb{Q}$
3. $J_2(q *_{\mathbb{Q}} p) = J_2(q) *_{\mathbb{R}} J_2(p) \qquad \forall\, q, p \in \mathbb{Q}$
4. $q <_{\mathbb{Q}} p \Longleftrightarrow J_2(q) <_{\mathbb{R}} J_2(p) \qquad \forall\, q, p \in \mathbb{Q}$

Proof

According to which construction of $\mathbb{R}$ we use J_2 can be defined as $\begin{cases} J_2(q) = q^* \\ J_2(q) = [C(q)] \end{cases}$

■

Chapter 3

Complete Ordered Fields (COF) and the Real Numbers

3.1 Axioms of a COF

In this chapter we change point of view. A COF $\mathcal{R}$ is given in an axiomatic way. Sixteen theorems we proved in previous chapter for a COF, now they hold as axioms. This kind of approach, to the real numbers, is the standard didactic one. In this chapter, one of the main scopes is finding copies of a Peano System $\mathbb{N}$, OID $\mathbb{Z}$, OF $\mathbb{Q}$, as proper subsets of $\mathcal{R}$. Further we will explore other structural properties of a COF and of their subset. In final we prove isomorphism between two COF.

Remark 3.1

Recalling definition 2.6 a COF $\left(\mathcal{R}, +, *, \leq\right)$ satisfies the following algebraic proprieties:

$s_1 \quad x + y = y + x \quad \forall\, x, y \in \mathcal{R}$

$s_2 \quad x + (y + z) = (x + y) + z \quad \forall\, x, y, z \in \mathcal{R}$

$s_3 \quad \exists\, 0 \in \mathcal{R} \quad | \quad x + 0 = x \quad \forall\, x \in \mathcal{R}$

$s_4 \quad \forall\, x \in \mathcal{R} \quad \exists\, y \in \mathcal{R} \quad | \quad x + y = 0$

$p_1 \quad x * y = y * x \quad \forall\, x, y \in \mathcal{R}$

$p_2 \quad x * (y * z) = (x * y) * z \qquad \forall\, x, y, z \in \mathcal{R}$

$p_3 \quad \exists\, 1 \in \mathcal{R},\, 1 \neq 0 \quad x * 1 = x \qquad \forall\, x \in \mathcal{R}$

$p_4 \quad \forall\, x \in \mathcal{R},\, x \neq 0, \quad \exists\, y \in \mathcal{R},\, y \neq 0 \quad | \quad x * y = 1$

$sp \quad x * (y + z) = x * y + x * z \quad \forall\, x, y, z \in \mathcal{R}$

$o_1 \quad x \le x \quad \forall x \in \mathcal{R}$

$$o_2 \quad \left.\begin{array}{l}\text{If } x \le y\\ \text{If } y \le x\end{array}\right\} \Longrightarrow x = y$$

$$o_3 \quad \left.\begin{array}{l}\text{If } x \le y\\ \text{If } y \le z\end{array}\right\} \Longrightarrow x \le z$$

$o_4 \quad \forall x, y \in \mathcal{R} \quad x \le y$ or $y \le x$

so Let $x, y \in \mathcal{R}$

$x \le y \Longleftrightarrow x + z \le y + z \quad \forall z \in \mathcal{R}$

po $x \ge 0,\ y \ge 0 \Longrightarrow x * y \ge 0$

Remark 3.2

Suppose property p_3 of a COF $\mathcal{R}$ changed in:

$\exists 1 \in \mathcal{R} \quad x * 1 = x \qquad \forall x \in \mathcal{R}$

$$\left.\begin{array}{l}\text{Then let } R \text{ a set with one element}\\ x + x := x \quad \forall x \in R\\ x * x := x \quad \forall x \in R\\ x \le y \Longleftrightarrow x = y \quad \forall x, y \in R\end{array}\right\} \Longrightarrow (R, +, *, \le) \text{ is a COF}$$

Hence condition $1 \neq 0$ is necessary to obtain non banal COF

Notational Remark 3.1

In this Chapter with $\mathcal{R}$ we denote a COF

Proposition 3.1

- Let $x \in \mathcal{R} \Longrightarrow \exists! -x \in \mathcal{R} \mid x + (-x) = 0$
- Let $x \in \mathcal{R}$, $x \neq 0 \Longrightarrow \exists!\, x^{-1} \in \mathcal{R} \mid x * x^{-1} = 1$

Proof

- Let y, z which satisfy s_4 for x
  $z \overset{s_3}{=} z + 0 \overset{s_4}{=} z + (x + y) \overset{s_2}{=} (z + x) + y = 0 + y \overset{s_3}{=} y$
- Let $y, z \neq 0$ which satisfy p_4 for x
  $z \overset{p_3}{=} z * 1 \overset{p_4}{=} z * (x * y) \overset{p_2}{=} (z * x) * y = 1 * y \overset{p_3}{=} y$

■

Notational Remark 3.2
Let $x \in \mathcal{R}$
We denote the only $y \quad | \quad x + y = 0 \quad$ as $-x$ ("The opposite of x")

Let $x \in \mathcal{R}$, $x \neq 0$

We denote the only $y \quad | \quad x * y = 1 \quad$ as x^{-1} ("The inverse of x")

An immediate consequence of the algebraic properties of $\mathcal{R}$ is the following

Corollary 3.1

- $-0 = 0$
- $-(-x) = x$
- $x \geq 0 \iff -x \leq 0$
- $1^{-1} = 1$
- $(x^{-1})^{-1} = x$

Definition 3.1

Let $x, y \in \mathcal{R}$

$x < y \iff x \leq y \quad$ and $\quad x \neq y$

Properties which involve $\leq$ are reformulated with $<$ in the following proposition

Proposition 3.2

$o_1 \qquad x \not< x \quad \forall x \in \mathcal{R}$

$o_2 \qquad x < y \quad$ or $\quad y < x \Longrightarrow x \neq y$

$$o_3 \qquad \left.\begin{array}{c} x < x_1 \\ x_1 < x_2 \end{array}\right\} \Longrightarrow x < x_2$$

$o_4 \qquad \forall x, y \in \mathcal{R}$ one and only one of the following holds :

$x < y, \quad y < x, \quad x = y$

$so \qquad$ Let $x, y \in \mathcal{R}$

$x < y \iff x + z < y + z \quad \forall z \in \mathcal{R}$

$po \qquad x > 0,\ y > 0 \Longrightarrow x * y > 0$

Remark 3.3

Recalling definitions 2.1, 2.2, 2.3, 2.4, 2.5 and recalling remarks 2.1, 2.2

- Let $A \subset \mathcal{R}$ and $z \in \mathcal{R}$

  z is an upper bound of $A \iff \forall x \in A \quad x \leq z$

- Let $A \subset \mathcal{R}$

  A is bounded above $\iff \exists\, z$ upper bound for A

- Let $A \subset \mathcal{R}, \quad A$ bounded above, $\quad \gamma \in \mathcal{R}$

  $$\gamma \text{ is the least upper bound of } A \iff \begin{cases} S_1 & \gamma \text{ is upper bound for } A \\ S_2 & \text{if } \gamma_1 \text{ is upper bound for } A \Longrightarrow \gamma \leq \gamma_1 \end{cases}$$

  We call γ the L.U.B. of A and we denote it $\quad \gamma = \sup A$

- The L.U.B. (whenever it exists) is unique

- Let $A \subset \mathcal{R}$ and $z \in \mathcal{R}$

  z is a lower bound of $A \iff \forall\, x \in A \quad z \leq x$

- Let $A \subset \mathcal{R}$

  A is bounded below $\iff \exists\, z$ lower bound for A

- Let $A \subset \mathcal{R}, \quad \gamma \in \mathcal{R}$

  $$\gamma \text{ is the Great Lower Bound of } A \iff \begin{cases} I_1) & \gamma \text{ is lower bound for } A \\ I_2) & \text{if } \gamma_1 \text{ is lower bound for } A \Longrightarrow \gamma \geq \gamma_1 \end{cases}$$

  We call γ the G.L.B. of A and we denote it $\quad \gamma = \inf A$

- The G.L.B. (whenever it exists) is unique

- Let $A \subset \mathcal{R}$

  $$A \text{ is bounded} \iff \begin{cases} A \text{ is bounded above} \\ A \text{ is bounded below} \end{cases}$$

Remark 3.4

Recalling definition 2.6 the following property is the last one which holds in COF $\mathcal{R}$

$$\textbf{Ded} \qquad \left.\begin{array}{l} A \subset \mathcal{R},\ A \neq \emptyset \\ A \text{ bounded above} \\ (A \text{ bounded below}) \end{array}\right\} \Longrightarrow \exists\, \gamma \in \mathbb{R} \quad | \quad \gamma = \sup A \ \ (\gamma = \inf A)$$

An immediate corollary of **Ded** is the following

Corollary 3.2

$$\left.\begin{array}{l} A \subset \mathcal{R},\ A \neq \emptyset \\ A \text{ bounded above} \\ x > 0 \end{array}\right\} \Longrightarrow \exists\, y \in A \quad | \quad \sup A - x < y$$

Proof
Let $\gamma = \sup A$

By contradiction suppose that

$$\forall\, p \in A \quad \gamma - x \geq p \Longrightarrow \left\{\begin{array}{l} \gamma - x \text{ is an upper bound for } A \\ \gamma - x < \gamma \end{array}\right. \Longrightarrow \gamma - x = \sup A$$

Contradiction ■

Proposition 3.3

$$\text{Let } x \in \mathcal{R} \Longrightarrow x * 0 = 0 * x = 0$$

Proof
$x * 0 \overset{s_3}{=} x * (0 + 0) \overset{sp}{=} x * 0 + x * 0$

Then by s_3 $\quad x * 0 = 0$ ■

Proposition 3.4

$$\text{Let } x \in \mathcal{R} \Longrightarrow -x = (-1) * x$$

Proof
$x + ((-1) * x) \overset{p_3}{=} 1 * x + ((-1) * x) \overset{sp}{=} x * (1 - 1) \overset{s_3}{=} x * 0 \overset{\text{P.3.3}}{=} 0$

Then by proposition 3.1 $\quad (-1) * x = -x$ ■

Proposition 3.5

$$\text{Let } x, y \in \mathcal{R} \Longrightarrow -(x * y) = (-x) * y = x * (-y)$$

Proof
$(x*y)+((-x)*y) \overset{\text{P.3.4}}{=} (x*y)+(((-1)*x)*y) \overset{p_2}{=} (x*y)+((-1)*(x*y)) \overset{\text{P.3.4}}{=} (x*y)-(x*y) = 0$

Then by proposition 3.1 $\quad$ we get the thesis ■

Proposition 3.6

$$\text{Let } x, y \in \mathcal{R} \Longrightarrow x * y = (-x) * (-y)$$

Proof
$((-x)*(-y))-(x*y) \overset{\text{P.3.5}}{=} ((-x)*(-y))+((-x)*y) \overset{sp}{=} (-x)*(-y+y) \overset{s_4}{=} (-x)*0 \overset{\text{P.3.3}}{=} 0$

Then by proposition 3.1 we get the thesis ■

Corollary 3.3

Let $x \neq 0 \implies x^2 := x*x > 0$

Proof
By o_4 we have to cases for x

- $x > 0 \overset{po}{\implies} x*x > 0$
- $x < 0 \overset{\text{C.3.1}}{\implies} -x > 0 \overset{po}{\implies} 0 < (-x)*(-x) \overset{\text{P.3.6}}{=} x*x$

■

Corollary 3.4

$1 > 0$

Proof
Since $1^2 = 1$. By corollary 3.3 we get the thesis ■

Corollary 3.5

$\forall x \in \mathcal{R} \qquad x+1 > x$

Proof
By corollary 3.4 $1 > 0 \overset{so}{\implies} x+1 > x+0 \overset{s_3}{=} x$ ■

Proposition 3.7

$-x-y = -(x+y) \quad \forall x, y \in \mathcal{R}$

Proof
$$(x+y)+(-x-y) \overset{s_2}{=} x+(y+(-x-y)) \overset{s_2}{=} x+((y-x)-y) \overset{s_1}{=} x+((-x+y)-y)$$
$$\overset{s_2}{=} x+(-x+(y-y)) \overset{s_4}{=} x+(-x+0) \overset{s_3}{=} x-x \overset{s_4}{=} 0$$
Then by proposition 3.1 we get the thesis ■

3.2 Naturals, Integers and Rational Numbers of a COF

Remark 3.5

In this section we are going to show that in a COF there exist models of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ as proper subsets.

In this section we define our copy of $\mathbb{N}$ using the structural axiom **Ded** of $\mathcal{R}$ but it would not be a necessary property. To understand necessary properties to have a model of the Natural Numbers as a proper subset and for a simpler way to define copies of Naturals Numbers see Appendix A.

Definition 3.2

$N \subseteq \mathcal{R}$ has the "property C." if and only if satisfies

n_1 $1 \in N$

n_2 $\forall\, x \in N \quad x \geq 1$

n_3 N is bounded above (Then by $Ded \quad \exists \sup N$)

n_4 $x \in N,\ x < \sup N \implies x + 1 \in N$

$\mathfrak{N} := \{N \subseteq \mathcal{R} \mid N \text{ has the "property C."}\}$

Proposition 3.8

$$\text{Let } N \in \mathfrak{N} \implies \begin{cases} \sup N \in N \\ \text{Calling } N_1 := N \cup \{(\sup N) + 1\} \implies \begin{cases} N_1 \in \mathfrak{N} \\ \sup N_1 = (\sup N) + 1 \end{cases} \end{cases}$$

Proof

Let $n := \sup N$

According to n_2 we have two cases

- $n \in N$
  - If $n = 1 \overset{n_1}{\implies} n \in N$
  - If $n > 1$

    By contradiction $n \notin N$

    By corollary 3.2 $\quad \exists\, x \in \mathbb{N} \mid n - 1 < x < n$

    Then $x < n \quad$ but $x + 1 \notin N$ Contradiction since $N \in \mathfrak{N}$

- $N_1 \in \mathfrak{N}$

  It is obvious

■

Definition 3.3

$$\mathbb{N}_{\mathcal{R}} := \{x \in \mathcal{R} \ \mid \exists\, N \in \mathfrak{N} \quad \mid \quad x = \sup N\}$$

Theorem 3.1

Let $f(x) := x + 1 \quad \forall\, x \in \mathcal{R}$. Let $\sigma := f_{|\mathbb{N}_{\mathcal{R}}}$

Recalling Peano System (definition 1.1) we have the following result

$$(\mathbb{N}_{\mathcal{R}},\, 1,\, \sigma) \quad \text{is a Peano System}$$

Proof

We have to prove the following five properties

(i) $1 \in \mathbb{N}_{\mathcal{R}}$:

Let $A := \{\, 1 \,\} \implies A \in \mathfrak{N}, \quad 1 = \sup A \implies 1 \in \mathbb{N}_{\mathcal{R}}$

(ii) $n \in \mathbb{N}_{\mathcal{R}} \implies \sigma(n) \in \mathbb{N}_{\mathcal{R}}$:

It comes immediately by second result of proposition 3.8.

(iii) $1 \notin \sigma(\mathbb{N}_{\mathcal{R}})$:

$x + 1 = 1 \iff x = 0$ but $\forall\, N \in \mathfrak{N},\ 0 \notin N \implies \ n + 1 \neq 1 \quad \forall\, n \in \mathbb{N}_{\mathcal{R}}$

(iv) σ is injective: It is obvious

(v) Induction property:

By contradiction $\exists\, A \subset \mathbb{N}_{\mathcal{R}}$, with $1 \in A,\ x \in A \implies x + 1 \in A$

Thus $\quad \exists\, N \in \mathfrak{N} \mid \ \sup N \notin A$

Now let $n := \sup N \qquad B := A \cap N$

- B satisfies $\ n_1,\, n_2,\, n_3$
- B is bounded above and since $B \subset N \implies \sup B =: b \leq n$

  $$\text{Let } x \in B,\, x < b \implies \left.\begin{array}{l} x < b \overset{o_3}{\implies} x < n \overset{n_4}{\implies} x + 1 \in N \\ x \in A \implies x + 1 \in A \end{array}\right\} \longrightarrow x + 1 \in B$$

Then $B \in \mathfrak{N} \overset{\text{P.3.8}}{\implies} b \in B$ and since $n \notin A \implies b < n$ Then

$$\left.\begin{array}{l} b < n \overset{n_4}{\implies} b + 1 \in N \\ b \in B \implies b \in A \implies b + 1 \in A \end{array}\right\} \implies b + 1 \in B$$

Contradiction since $b = \sup B$

■

Remark 3.6

To build a Peano Ring[1], in Section 1.1, through Recursion Theorem (Lemma 1.2), we constructed suitable inner operations for $\mathbb{N}$.

Now defining them as subsets of $\mathcal{R}$, theorems proofed in Chapter 1. are given as Axioms of $\mathcal{R}$.

Now, the only thing we should prove is that operations $+, *,$ restricted at $\mathbb{N}_{\mathcal{R}}$, are inner operations. We will omit these results since they are immediate by Induction

An immediate corollary is the following:

Theorem 3.2

$$(\mathbb{N}_{\mathcal{R}}, +, *, \leq) \quad \text{is a Peano Ring}$$

Now we are going to see some structural properties of $\mathbb{N}_{\mathcal{R}}$ as a subset of a COF $\mathcal{R}$

Proposition 3.9

$k \neq 1 \implies \exists\, l \in \mathbb{N}_{\mathcal{R}} \quad | \quad n = l + 1 \quad \forall\, k \in \mathbb{N}_{\mathcal{R}}$

Proof

By contradiction $\exists\, k \in \mathbb{N}_{\mathcal{R}} - \{1\} \quad | \quad k \neq n + 1 \quad \forall\, n \in \mathbb{N}_{\mathcal{R}}$

Let $A := \{n \in \mathbb{N}_{\mathcal{R}} \mid n \neq k\}$

- $1 \neq k \implies 1 \in A$
- $m \neq k \Longrightarrow m + 1 \neq k$ by hypothesis on k i.e.
  $m \in A \Longrightarrow m + 1 \in A$

Then by Induction property $A = \mathbb{N}_{\mathcal{R}}$

Contradiction since $k \notin A$

■

An immediate of proposition 3.9 is the following:

Corollary 3.6

$k > 1 \implies k - 1 \geq 1 \quad \forall\, k \in \mathbb{N}_{\mathcal{R}}$

[1] See definition 1.2

Proposition 3.10

$$n > m \implies n - m \in \mathbb{N}_{\mathcal{R}} \quad \forall n, m \in \mathbb{N}_{\mathcal{R}}$$

Proof
Fix $n \in \mathbb{N}_{\mathcal{R}}$ and let $A := \{m \in \mathbb{N}_{\mathcal{R}} \mid n > m \implies n - m \in \mathbb{N}_{\mathcal{R}}\}$

- Let $n \in \mathbb{N}_{\mathcal{R}}$, $n > 1$

  $$\left.\begin{array}{l} n \in \mathbb{N}_{\mathcal{R}} \overset{\text{D.3.3}}{\implies} \exists N \in \mathfrak{N} \quad | \quad n = \sup N \\ n > 1 \overset{\text{C.3.6}}{\implies} n - 1 \geq 1 \end{array}\right\} \implies \{x \in N \mid 1 \geq x \geq n - 1\} \neq \emptyset$$

  Let $N_1 := \{x \in N \mid 1 \geq x \geq n - 1\}$

  It is not difficult to prove that $\left\{\begin{array}{l} N_1 \in \mathfrak{N} \\ \sup N_1 = n - 1 \end{array}\right. \overset{\text{D.3.3}}{\implies} n - 1 \in \mathbb{N}_{\mathcal{R}} \implies 1 \in A$

- Suppose $m \in A$ and $n > m + 1$

  1) $n > m + 1 \overset{o_3}{\implies} n > m \overset{m \in A}{\implies} n - m \in \mathbb{N}_{\mathcal{R}}$

  $\overset{\text{D.3.3}}{\implies} \exists N \in \mathfrak{N} \quad | \quad n - m = \sup N$

  2) $n > m + 1 \overset{so}{\implies} n - m > 1$

  Hence putting together 1) and 2) by corollary 3.6 $\quad n - m - 1 \geq 1$

  Then $\{x \in N \mid 1 \geq x \geq n - m - 1\} \neq \emptyset$

  and repeat the same reasoning as the first point we get the thesis

Then by Induction $A = \mathbb{N}_{\mathcal{R}}$
■

An immediate consequence of proposition 3.10 is the following

Proposition 3.11

$$\left.\begin{array}{l} x \in \mathbb{N}_{\mathcal{R}} \\ n < x \leq n + 1 \end{array}\right\} \implies x = n + 1 \quad \forall n \in \mathbb{N}_{\mathcal{R}}$$

Proof
It is immediate by Induction on n ■

Proposition 3.12 (Archimedean property of $\mathcal{R}$)

$$\forall x, y \in \mathcal{R},\ x > 0 \implies \exists n \in \mathbb{N}_{\mathcal{R}} \quad | \quad n * x > y$$

Proof
Let $x > 0$

$X := \{n * x \mid n \in \mathbb{N}_{\mathcal{R}}\}$

By contradiction $\exists\, y$ upper bound for $X \overset{Ded}{\Longrightarrow} \exists\, \alpha := \sup X$

By corollary 3.2 $\quad \exists\, m * x \in X \quad | \quad \alpha - x < m * x$
Then by $so \quad \alpha < m * x + m \overset{sp}{=} (m+1) * x$

Contradiction since α is an upper bound for X ■

Remark 3.7

In Chapter 1. we constructed $\mathbb{Z}$ and $\mathbb{Q}$ with suitable inner operations and order relations for them.

Now defining them as subsets of $\mathcal{R}$, theorems proofed in Chapter 1. are given as Axioms of $\mathcal{R}$.

Moreover we decided for two special elements , as in $\mathbb{Z}$ as in $\mathbb{Q}$, and we proved they were neutral elements for the operations defined.

Now 0, 1 are given like neutral elements for $\mathcal{R}$.

Thus in this section we have to show that the operations $+$, $*$, restricted at $\mathbb{Z}$, $\mathbb{Q}$, are inner operations for them and also that $0, 1 \in \mathbb{Z}$ and since $\mathbb{Z} \subset \mathbb{Q} \implies 0, 1 \in \mathbb{Q}$

Definition 3.4

$$\mathbb{Z}_{\mathcal{R}} := \{\, x \in \mathcal{R} \mid \exists\, n, m \in \mathbb{N}_{\mathcal{R}} \quad \text{such that} \quad x = (n - m)\}$$

Definition 3.5

$$\mathbb{Z}^{+}_{\mathcal{R}} := \{\, x \in \mathbb{Z}_{\mathcal{R}} \mid x > 0\}$$

Proposition 3.13

$\mathbb{Z}_{\mathcal{R}}$ satisfies these properties

- $x, y \in \mathbb{Z}_{\mathcal{R}} \Longrightarrow x + y \in \mathbb{Z}_{\mathcal{R}}$
- $0 \in \mathbb{Z}_{\mathcal{R}}$
- $x \in \mathbb{Z}_{\mathcal{R}} \implies -x \in \mathbb{Z}_{\mathcal{R}}$
- $x, y \in \mathbb{Z}_{\mathcal{R}} \implies x * y \in \mathbb{Z}_{\mathcal{R}}$
- $\mathbb{N}_{\mathcal{R}} \subset \mathbb{Z}_{\mathcal{R}}$. In particular $\mathbb{N}_{\mathcal{R}} = \mathbb{Z}^{+}_{\mathcal{R}}$

Proof

- Let $x, y \in \mathbb{Z}_{\mathcal{R}} \implies x = (n-m), \quad y = (k-l) \quad n, m, k, l \in \mathbb{N}_{\mathcal{R}}$

  $$\begin{aligned} x + y &= (n-m) + (k-l) \overset{s_2}{=} n + (-m + (k-l)) \overset{s_2}{=} n + ((-m+k) - l) \\ &\overset{s_1}{=} n + ((k-m) - l) \overset{s_2}{=} n + (k + (-m-l)) \\ &\overset{s_2}{=} (n+k) + (-m-l) \overset{\text{P.3.7}}{=} (n+k) - (m+l) \end{aligned}$$

  And since $(n+k), (m+l) \in \mathbb{N}$ we get the thesis

- Just take $n = m$

- Let $x \in \mathbb{Z}_{\mathcal{R}} \implies x = (n-m)$

  Then by proposition 3.7 $\quad -x = -(n-m) = -n + m \overset{s_1}{=} m - n \implies -x \in \mathbb{Z}_{\mathcal{R}}$

- Let $x, y \in \mathbb{Z}_{\mathcal{R}} \implies x = (n-m), \quad y = (k-l) \quad n, m, k, l \in \mathbb{N}_{\mathcal{R}}$

  $$\begin{aligned} x + y &= (n-m) * (k-l) \overset{sp}{=} (n-m) * k + (n-m) * (-l) \overset{\text{P.3.5}}{=} (n-m) * k - ((n-m) * l) \\ &\overset{sp}{=} (n * k + (-m) * k) - (n * l + (-m) * l) \overset{\text{P.3.5}}{=} n * k - (m * k) - (n * l - (m * l)) \\ &\overset{\text{P.3.7}}{=} (n * k) - (m * k) - (n * l) + (m * l) \overset{s_1}{=} (n * k) + (m * l) - (m * k) - (n * l) \\ &\overset{\text{P.3.7}}{=} (n * k) + (m * l) - ((m * k) + (n * l)) \end{aligned}$$

  And since $((n * k) + (m * l)), ((m * k) + (n * l)) \in \mathbb{N}_{\mathcal{R}}$ we got the thesis

- Let $k \in \mathbb{N}_{\mathcal{R}} \overset{\text{T.3.1}}{\implies} \begin{cases} k + 1 \in \mathbb{N}_{\mathcal{R}} \\ 1 \in \mathbb{N}_{\mathcal{R}} \end{cases} \implies k = (k+1) - 1 \in \mathbb{Z}_{\mathcal{R}}$

  Furthermore if $k \in \mathbb{N}_{\mathcal{R}} \implies k \geq 1 \implies k > 0$

  Let $z \in \mathbb{Z}^+_{\mathcal{R}} \implies \exists n, m \in \mathbb{N}_{\mathcal{R}} \quad | \quad z = (n-m)$

  $z > 0 \implies n - m > 0 \overset{\text{P.3.10}}{\implies} n - m \in \mathbb{N}_{\mathcal{R}}$

■

An immediate corollary of proposition 3.13 is the following:

Theorem 3.3

$$(\mathbb{Z}_{\mathcal{R}}, +, *, \leq) \quad \text{is an Ordered Integrity Domain}^2$$

Proposition 3.14

$$\text{Let } x, y \neq 0 \implies \begin{cases} x * y \neq 0 \\ (x * y)^{-1} = x^{-1} * y^{-1} \end{cases}$$

Proof

[2] See definition 1.8

- $x * y \neq 0$

  Since $x \neq 0 \overset{o_4}{\Longrightarrow} x < 0 \quad \text{or} \quad x > 0$

  Thus it's the same for y and then there are four cases

  - $x, y > 0 \overset{po}{\Longrightarrow} x * y > 0$
  - $x, y < 0 \overset{\text{C.3.1}}{\Longrightarrow} -x,\ -y > 0 \overset{po}{\Longrightarrow} (-x) * (-y) > 0$

    And since by proposition 3.6 $\quad (-x) * (-y) = x * y$

    Then we got the result
  - $x > 0,\ y < 0 \overset{\text{C.3.1}}{\Longrightarrow} x,\ -y > 0 \overset{po}{\Longrightarrow} x * (-y) > 0$

    And since by proposition 3.5 $\quad x * (-y) = -(x * y)$

    Then by corollary 3.1 $\quad x * y < 0$
  - $x < 0,\ y > 0$ Like above

- $(x * y)^{-1} = x^{-1} * y^{-1}$

  $$\begin{aligned}(x * y) * (x^{-1} * y^{-1}) &\overset{p_2}{=} x * (y * (x^{-1} * y^{-1})) \overset{p_2}{=} x * ((y * x^{-1}) * y^{-1}) \\ &\overset{p_1}{=} x * ((x^{-1} * y) * y^{-1}) \overset{p_2}{=} x * (x^{-1} * (y * y^{-1})) \\ &\overset{p_4}{=} x * (x^{-1} * 1) \overset{s_3}{=} x * x^{-1} \overset{p_4}{=} 1\end{aligned}$$

  Then by proposition 3.1 we got the thesis

■

Definition 3.6

$$\mathbb{Q}_{\mathcal{R}} := \{\, x \in \mathcal{R} \mid \exists\, z \in \mathbb{Z}_{\mathcal{R}},\ n \in \mathbb{N}_{\mathcal{R}} \quad | \quad x = z * n^{-1}\}$$

Proposition 3.15

$\mathbb{Q}_{\mathcal{R}}$ satisfies these properties

- $x, y \in \mathbb{Q}_{\mathcal{R}} \Longrightarrow x + y \in \mathbb{Q}_{\mathcal{R}}$
- $\mathbb{Z}_{\mathcal{R}} \subset \mathbb{Q}_{\mathcal{R}}$
- $x \in \mathbb{Q}_{\mathcal{R}} \Longrightarrow -x \in \mathbb{Q}_{\mathcal{R}}$
- $x, y \in \mathbb{Q}_{\mathcal{R}} \Longrightarrow x * y \in \mathbb{Q}_{\mathcal{R}}$
- $x \in \mathbb{Q}_{\mathcal{R}},\ x \neq 0 \Longrightarrow x^{-1} \in \mathbb{Q}_{\mathcal{R}}$

Proof

- Let $x, y \in \mathbb{Q}_{\mathcal{R}} \implies x = z * n^{-1}, \quad y = z_1 * n_1^{-1}$
  On one hand applying in order p_3, p_4 and Prop. 3.14
  $x = (z * n_1) * (n * n_1)^{-1}$ and $y = (z_1 * n) * (n_1 * n)^{-1}$
  Thus
  $x + y = ((z * n_1) + (z_1 * n)) * (n * n_1)^{-1}$
- $\forall\, t \in \mathbb{Z}_{\mathcal{R}}$ just take $z = t$, $n = 1$,
- Let $x \in \mathbb{Q}_{\mathcal{R}} \implies x = z * n^{-1}$
  Then by proposition 3.5 $\quad -x = (-z) * n^{-1} \implies -x \in \mathbb{Q}_{\mathcal{R}}$
- We omit to prove that $\mathbb{Q}_{\mathcal{R}}$ is closed under multiplication since its proof is very similar at the first step of this proposition.
- Let $x \in \mathbb{Q}_{\mathcal{R}}$, $x \neq 0 \implies x = z * n^{-1}$ with $z \neq 0$
  - $z > 0 \overset{\text{P.3.13}}{\implies} z \in \mathbb{N}_{\mathcal{R}}$
    Let $y := n * z^{-1} \implies y \in \mathbb{Q}_{\mathcal{R}}$ and $x * y = 1$
    Then by the uniqueness of the opposite we got the thesis
  - $z < 0 \overset{\text{P.3.13}}{\implies} -z \in \mathbb{N}_{\mathcal{R}}$ since $-z > 0$
    Let $y := (-n) * (-z)^{-1} \implies y \in \mathbb{Q}_{\mathcal{R}}$ and $x * y = 1$
    Then by the uniqueness of the opposite we got the thesis

■

An immediate corollary of proposition 3.15 is the following:

Theorem 3.4

$$(\mathbb{Q}_{\mathcal{R}},\, +,\, *,\, \leq) \quad \text{is an Ordered Field}^3$$

Proposition 3.16 ($\mathbb{Q}_{\mathcal{R}}$ is dense in $\mathcal{R}$)

$\forall\, x, y \in \mathcal{R},\, x < y \quad \exists\, q \in \mathbb{Q}_{\mathcal{R}} \quad | \quad x < q < y$

Proof
Since $(y - x) > 0 \overset{\text{P.3.12}}{\implies} \exists\, n \in \mathbb{N}_{\mathcal{R}} \quad | \quad n * (y - x) > 1 \overset{sp+so}{\implies} 1 + n * x < n * y$

Applying again this result we find $m_1, m_2. \in \mathbb{N}_{\mathcal{R}} \quad | \quad \begin{cases} m_1 > n * x \\ m_2 > -n * x \end{cases}$

Then we get $-m_2 < n * x < m_1$

Repeating reasoning as in proposition 2.4

[3] See definition 1.19

There exists $z \in \mathbb{Z}_{\mathcal{R}}$, $-(m_2 - 1) \leq z \leq m_1 \quad | \quad (z-1) \leq n * x < z$

Hence $n * x < z \leq 1 + n * x < n * y$ and multiplying all the terms for n^{-1}, calling $q := z * n^{-1}$

Then $q \in \mathbb{Q}_{\mathcal{R}}$ and $x < q < y$

■

Corollary 3.7

Let $x, y \in \mathcal{R}$

$x < y + \varepsilon \quad \forall \varepsilon > 0 \implies x \leq y$

Proof

It is immediate by contradiction

■

3.3 Finite and infinite subsets of a COF

Notational Remark 3.3

From this point forward, in this chapter we indicate $\mathbb{N}_{\mathcal{R}}$ as $\mathbb{N}$

Definition 3.7

Let $A \subseteq \mathcal{R}$

Let $n \in \mathbb{N}$ and let $I^{(n)} := \{1, \ldots, n\}$

An $n-$map in A is a function $f : I^{(n)} \longrightarrow A$ bijective

We denote it as $\left\{ f_k \right\}_{k \leq n}$

Definition 3.8

Let $A \subseteq \mathcal{R}$

A is Finite $\iff A = \emptyset \quad$ or

$$\exists\, n \in \mathbb{N}, \quad f \ \ n\text{-map in } A$$

Otherwise we say that A is Infinite

Corollary 3.8

Let $A \subseteq \mathcal{R}$

A is Infinite $\implies \forall\, n \in \mathbb{N} \quad \exists\, f : I^{(n)} \longrightarrow A$ injective

Proof

Let $B := \{n \in \mathbb{N} \mid \forall\, f : I^{(n)} \longrightarrow X \ \ f \text{ is no injective}\}$

By contradiction $B \neq \emptyset$

By Minimum principle $\exists\, N := \min\, B$

Since surely $N > 1 \implies N-1 \in A \implies \exists\, f : I^{(N-1)} \longrightarrow A$ injective

Since A is Infinite f is no surjective[4] $\implies \exists\, y \in A,\ y \notin f(I^{(N-1)})$

Then defining $g : I^{(N)} \longrightarrow A$ as $g(k) := \begin{cases} f(k) & k \in I^{(N-1)} \\ y & k = N \end{cases} \implies g$ is injective $\implies N \notin B$

Contradiction

■

Definition 3.9

Let $A \subseteq \mathcal{R},\ A \neq \emptyset$

A is Countable $\iff \quad \exists\, f : \mathbb{N} \longrightarrow A$ bijective

3.3.1 Sequences in a COF

Definition 3.10

Let $A \subset \mathcal{R},\ A \neq \emptyset$

A sequence in $A,$ is a function $f : \mathbb{N} \longrightarrow A$

We denote the set $\{(n, f(n)) \mid n \in \mathbb{N}\}$ as $\{\, f_n \,\}_{n \in \mathbb{N}}$

Remark 3.8

We recommend the reader not confusing $\{\, f_n \,\}_{n \in \mathbb{N}}$
with $\{f_n \mid n \in \mathbb{N}\}$ which is non-empty subset of $\mathcal{R}$

Definition 3.11

Let $x \in \mathcal{R}$

$$|\, x \,|_{\mathcal{R}} := \begin{cases} x & \text{If}\, x \geq 0 \\ -x & \text{If}\, x < 0 \end{cases}$$

Proposition 3.17

The following properties holds

- $|\, x \,|_{\mathcal{R}} \geq 0 \quad \forall\, x \in \mathcal{R}$:
  Trivial

[4]Otherwise f would be an $N-1-$map

- Let $x \in \mathcal{R}$
  $|\,x\,|_{\mathcal{R}} = 0 \iff x = 0$:
  Trivial

- Let $x \in \mathcal{R}$
  $x, -x \;\leq |\,x\,|_{\mathcal{R}}$:
  Trivial

- Let $x \in \mathcal{R}$
  $|\,x\,|_{\mathcal{R}} = |\,-x\,|_{\mathcal{R}}$:
  Trivial

- Let $x, y \in \mathcal{R}$
  $|\,x+y\,|_{\mathcal{R}} \leq |\,x\,|_{\mathcal{R}} + |\,y\,|_{\mathcal{R}}$:

  $$|\,x+y\,|_{\mathcal{R}} \overset{\text{D.3.11}}{=} \begin{cases} x+y & \text{If}\, x+y \geq 0 \\ -(x+y) & \text{If}\, x+y < 0 \end{cases}$$

  - If $x+y \geq 0$
    $|\,x+y\,|_{\mathcal{R}} = x+y$
    $$\begin{cases} x \leq |\,x\,|_{\mathcal{R}} \\ y \leq |\,y\,|_{\mathcal{R}} \end{cases} \overset{so}{\Longrightarrow} x+y \leq |\,x\,|_{\mathcal{R}} + |\,y\,|_{\mathcal{R}}$$
  - If $x+y < 0$
    $|\,x+y\,|_{\mathcal{R}} = -(x+y) \overset{\text{P.3.7}}{=} -x-y$
    $$\begin{cases} -x \leq |\,-x\,|_{\mathcal{R}} \\ -y \leq |\,-y\,|_{\mathcal{R}} \end{cases} \overset{so}{\Longrightarrow} -x-y \leq |\,-x\,|_{\mathcal{R}} + |\,-y\,|_{\mathcal{R}} = |\,x\,|_{\mathcal{R}} + |\,y\,|_{\mathcal{R}}$$

- $|\,\alpha * \beta\,|_{\mathcal{R}} = |\,\alpha\,|_{\mathcal{R}} * |\,\beta\,|_{\mathcal{R}} \quad \forall\, \alpha, \beta \in \mathcal{R}$:
  This proof is very simple but we omit it since it is tiresome

- Let $\varepsilon > 0$
  $|\,\alpha\,|_{\mathcal{R}} < \varepsilon \iff -\varepsilon < \alpha < \varepsilon$:
  Trivial

Definition 3.12

Let $\{\,\alpha_n\,\}_{n\in\mathbb{N}}$ sequence in $\mathcal{R}$

$\{\,\alpha_n\,\}_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathcal{R} \iff \forall\, \varepsilon > 0 \quad \exists\, n \in \mathbb{N}$ such that

$$|\,\alpha_k - \alpha_m\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k, m \geq n$$

Definition 3.13

Let $\{\, a_n \,\}_{n\in\mathbb{N}}$ sequence in $\mathcal{R}$

$\{\, a_n \,\}_{n\in\mathbb{N}}$ is a Up-Bounded sequence in $\mathcal{R} \iff \{a_n \mid n \in \mathbb{N}\}$ is bounded above

$\{\, a_n \,\}_{n\in\mathbb{N}}$ is a Down-Bounded sequence in $\mathcal{R} \iff \{a_n \mid n \in \mathbb{N}\}$ is bounded below

Definition 3.14

Let $\{\, a_n \,\}_{n\in\mathbb{N}}$ sequence in $\mathcal{R}$

$\{\, a_n \,\}_{n\in\mathbb{N}}$ is a Bounded sequence in $\mathcal{R} \iff \{a_n \mid n \in \mathbb{N}\}$ is bounded

Definition 3.15

Let $\{\, a_n \,\}_{n\in\mathbb{N}}$ sequence in $\mathcal{R}$

$\{\, a_n \,\}_{n\in\mathbb{N}}$ is a Up-Monotone sequence in $\mathcal{R} \iff a_n \leq a_{n+1} \quad \forall\, n \in \mathbb{N}$

$\{\, a_n \,\}_{n\in\mathbb{N}}$ is a Down-Monotone sequence in $\mathcal{R} \iff a_n \geq a_{n+1} \quad \forall\, n \in \mathbb{N}$

Definition 3.16

Let $\{\, \alpha_n \,\}_{n\in\mathbb{N}}$ sequence in $\mathcal{R}$

$$\{\, a_n \,\}_{n\in\mathbb{N}} \text{ is a Convergent sequence in } \mathcal{R} \iff \exists\, x \in \mathcal{R} \mid \forall\, \varepsilon > 0 \quad \exists\, n \in \mathbb{N} \quad | \quad |\,\alpha_k - x\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k \geq n$$

An immediate corollary of definition 3.16 is the following

Corollary 3.9

$$\{\, a_n \,\}_{n\in\mathbb{N}} \text{ is a Convergent sequence in } \mathcal{R} \Longrightarrow \exists!\ x \in \mathcal{R} \mid \forall\, \varepsilon > 0 \quad \exists\, n \in \mathbb{N} \quad | \quad |\,\alpha_k - x\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k \geq n$$

Proof

By contradiction there exist $z, y \in \mathcal{R},\ z \neq y$ satisfying definition 3.16 in place of x

It comes immediately that $|\,z - y\,|_{\mathcal{R}} < \varepsilon \quad \forall\, \varepsilon > 0$

According to proposition 3.17

$$\left.\begin{array}{l} |\,z - y\,|_{\mathcal{R}} < \varepsilon \Longrightarrow z < y + \varepsilon \overset{\text{C.3.7}}{\Longrightarrow} z \leq y \\ |\,z - y\,|_{\mathcal{R}} < \varepsilon \Longrightarrow y < z + \varepsilon \overset{\text{C.3.7}}{\Longrightarrow} y \leq z \end{array}\right\} \overset{o_3}{\Longrightarrow} y = z$$

Contradiction $\blacksquare$

Notational Remark 3.4
According to corollary 3.9 the unique x satisfying definition 3.16 will be denoted as $x = \lim\, a_n$

3.4 Convergence of Cauchy sequences in a COF

Proposition 3.18

$$\{\,\alpha_n\,\}_{n\in\mathbb{N}} \text{ a Cauchy sequence in } \mathcal{R} \implies \{\,\alpha_n\,\}_{n\in\mathbb{N}} \text{ Bounded sequence in } \mathcal{R}$$

Proof

$$\{\,\alpha_n\,\}_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathcal{R} \overset{\text{D.3.12}}{\iff} \forall\,\varepsilon > 0 \quad \exists\, n \in \mathbb{N} \quad \text{such that}$$

$$|\,\alpha_k - \alpha_m\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k, m \geq n$$

$$\implies \exists\, n \in \mathbb{N} \quad | \quad |\,\alpha_k - \alpha_n\,|_{\mathcal{R}} < 1 \quad \forall\, k > n$$

Define $K := |\,\alpha_1 - \alpha_n\,|_{\mathcal{R}} + |\,\alpha_2 - \alpha_n\,|_{\mathcal{R}} + \ldots + |\,\alpha_{n-1} - \alpha_n\,|_{\mathcal{R}} + |\,\alpha_n\,|_{\mathcal{R}}$

$$\left.\begin{array}{lll} \text{If} & k \leq n & |\,\alpha_k\,|_{\mathcal{R}} \leq |\,\alpha_k - \alpha_n\,|_{\mathcal{R}} + |\,\alpha_n\,|_{\mathcal{R}} < K \\ \text{If} & k > n & |\,\alpha_k\,|_{\mathcal{R}} \leq |\,\alpha_k - \alpha_n\,|_{\mathcal{R}} + |\,\alpha_n\,|_{\mathcal{R}} < 1 + |\,\alpha_n\,|_{\mathcal{R}} \end{array}\right\} \implies |\,a_n\,|_{\mathcal{R}} \leq K + 1 \quad \forall\, n \in \mathbb{N}$$

$$\implies \{a_n \mid n \in \mathbb{N}\} \text{ is bounded}$$

■

Proposition 3.19

Let $\{\,\phi_n\,\}_{n\in\mathbb{N}}$ be a sequence in $\mathcal{R}$

$$\left.\begin{array}{l} \{\,\phi_n\,\}_{n\in\mathbb{N}} \text{ Up-Monotone in } \mathcal{R} \\ \{\,\phi_n\,\}_{n\in\mathbb{N}} \text{ Up-Bounded in } \mathcal{R} \end{array}\right\} \implies \left\{\begin{array}{l} \{\,\phi_n\,\}_{n\in\mathbb{N}} \text{ Convergent sequence in } \mathcal{R} \\ \lim\, \phi_n = \sup\{\phi_n \mid n \in \mathbb{N}\} \end{array}\right.$$

Proof

According to definition 3.13 $\quad \{\phi_n \mid n \in \mathbb{N}\}$ is bounded above

Then by **Ded** there exists $\phi \in \mathcal{R} \mid \phi = \sup\{\phi_n \mid n \in \mathbb{N}\}$

Let $\varepsilon > 0$

By corollary 3.2 $\exists\, n \in \mathbb{N} \quad | \quad \phi - \phi_n < \varepsilon$

Now let $m \geq n$

$|\,\phi - \phi_m\,|_{\mathcal{R}} \leq |\,\phi - \phi_n\,|_{\mathcal{R}} + |\,\phi_n - \phi_m\,|_{\mathcal{R}}$

$$\left.\begin{array}{l} \phi_n \leq \phi_m \implies |\,\phi_n - \phi_m\,|_{\mathcal{R}} \leq 0 \\ \phi \geq \phi_n \implies |\,\phi - \phi_n\,|_{\mathcal{R}} = \phi - \phi_n \end{array}\right\} \implies |\,\phi - \phi_m\,|_{\mathcal{R}} \leq \phi - \phi_n < \varepsilon$$

■

Definition 3.17

Let $\{ a_n \}_{n \in \mathbb{N}}$ be a sequence in $\mathcal{R}$
Let $\{ g_n \}_{n \in \mathbb{N}}$ sequence in $\mathbb{N}$ $\;|\;$ $g_n < g_{n+1} \quad \forall\, n \in \mathbb{N}$
$\{a_{g_n}\}_{n \in \mathbb{N}}$ is a subsequence of $\{ a_n \}_{n \in \mathbb{N}}$

The following Theorem is one of the most important and useful in Analysis. We will divide its proof in three steps and the third one will be showed in two different ways that we will denote as $3a$ and $3b$: $3a$ is the usual method to achieve the result and there is an evident use of denumerable dependent arbitrary choices. $3b$ avoids infinite arbitrary choices

Theorem 3.5

$$\{ a_n \}_{n \in \mathbb{N}} \text{ Bounded sequence in } \mathcal{R} \implies \exists \text{ Convergent subsequence of } \{ a_n \}_{n \in \mathbb{N}}$$

Proof

1. Let $n \in \mathbb{N}$
   Let $A_n := \{a_k \mid k \geq n\}$
   By definition 3.14 $\quad A_1$ is a bounded set of $\mathbb{R}$
   $A_n \subseteq A_1 \;\forall\, n \in \mathbb{N} \implies A_n$ is bounded $\quad \forall\, n \in \mathbb{N} \overset{\textbf{Ded}}{\implies} \exists\; i_n := \inf(A_n)$
   Hence $\{ i_n \}_{n \in \mathbb{N}}$ is a sequence in $\mathbb{R}$ and
   $$\left.\begin{array}{l} \{ i_n \}_{n \in \mathbb{N}} \text{ Up-Monotone sequence in } \mathcal{R} \\ \{ i_n \}_{n \in \mathbb{N}} \text{ Up-Bounded sequence in } \mathcal{R} \end{array}\right\} \overset{\text{P.3.19}}{\implies} \left\{\begin{array}{l} \{ i_n \}_{n \in \mathbb{N}} \text{ Convergent sequence in } \mathcal{R} \\ \lim\, i_n = \sup\{i_n \mid n \in \mathbb{N}\} \end{array}\right.$$
2. Let $\varepsilon > 0$ and let $L := \sup\{i_n \mid n \in \mathbb{N}\}$.
   Defined $N_\varepsilon := \{n \in \mathbb{N} \mid |\, a_n - L\,|_{\mathbb{R}} < \varepsilon\} \implies N_\varepsilon$ is an Infinite subset of $\mathbb{N}$[5]:
   By Contradiction $\quad \exists\, \delta > 0 \quad | \quad N_\delta$ is Finite
   N_δ is Finite $\iff N_\delta = \emptyset \quad$ or
   $\qquad\qquad\qquad\exists\, n \in \mathbb{N},\; f\;\; n$-map in N_δ
   - If $N_\delta = \emptyset$ then we have two possibilities:
     $a_n \leq L - \delta \quad \forall\, n \in \mathbb{N} \quad$ or $\quad a_n \geq L + \delta \quad \forall\, n \in \mathbb{N}$

[5] See definition 3.8

Suppose $a_n \leq L - \delta \quad \forall n \in \mathbb{N} \Longrightarrow i_n \leq L - \delta \quad \forall n \in \mathbb{N}$

$$\Longrightarrow \begin{cases} L - \delta < L \\ L - \delta \text{ is an upper bound for } \{i_n \mid n \in \mathbb{N}\} \end{cases}$$

$$\Longrightarrow L \neq \sup\{i_n \mid n \in \mathbb{N}\}$$

$\Longrightarrow$ Contradiction

Suppose $a_n \geq L + \delta \quad \forall n \in \mathbb{N}$

By definition of i_n $\exists\, m \geq n \mid a_m < i_n + \delta \Longrightarrow \exists\, m \mid a_m < L + \delta$

$\Longrightarrow$ Contradiction

- If $\exists\, n \in \mathbb{N},\ f$ n-map in $N_\delta \Longrightarrow f : I^{(n)} \longrightarrow N_\delta$ bijective

  Let $M := \max\{f(k) \mid k \in I^{(n)}\}$

  Then $n > M \Longrightarrow a_n \notin N_\delta$ then we have two possibilities:

  $a_n \leq L - \delta \quad \forall n > M \quad \text{or} \quad a_n \geq L + \delta \quad \forall n > M$

  But whatever we suppose it follows a contradiction, ever according to the reasoning used in first point of this step

3*a*. By step 2. $N_{\frac{1}{m}}$ is an Infinite subset of $\mathbb{N} \quad \forall m \in \mathbb{N}$

Then $\forall k \in N_{\frac{1}{m}} \quad \exists K \in N_{\frac{1}{m+1}} \quad \mid \quad K > k$

Hence $\forall k \in \mathbb{N}$ let $g_k \in N_{\frac{1}{k}} \quad \mid \quad g_{k+1} > g_k \quad \forall k \in \mathbb{N}$

$$\begin{cases} \{a_{g_n}\}_{n\in\mathbb{N}} \text{ is a subsequence of } \{a_n\}_{n\in\mathbb{N}} \\ L = \lim a_{g_n} \end{cases}$$

3*b*.
- Recalling definition 3.7 let $n \in \mathbb{N}$ and define a subset of $n-$map in $\mathbb{N}$ as follows:

  $$\{b_k\}_{k\leq n} \in A_n \Longleftrightarrow \begin{cases} b_1 = \min N_1 \\ \text{If } n > 1 \quad b_{k+1} = \min\{n \in N_{\frac{1}{k+1}} \mid n > b_k\} \quad \forall k < n \end{cases}$$

- $A_n \neq \emptyset \quad \forall n \in \mathbb{N}$

  It is immediate by Induction

- $\exists!\ \{b_k\}_{k\leq n} \in A_n \quad \forall n \in \mathbb{N}$:

  It is immediate by induction

- Define a sequence $\{g_n\}_{n\in\mathbb{N}}$ as follows:

  $\forall n \in \mathbb{N} \quad g_n := b_n$ where $\{b_k\}_{k\leq n}$ is the only element of A_n

- $\begin{cases} \{a_{g_n}\}_{n\in\mathbb{N}} \text{ is a subsequence of } \{a_n\}_{n\in\mathbb{N}} \\ L = \lim a_{g_n} \end{cases}$

■

The following proposition is trivial and it is a direct consequence of the definitions of Cauchy and Convergent sequence

Proposition 3.20

$$\{\alpha_n\}_{n\in\mathbb{N}} \text{Convergent sequence in } \mathcal{R} \quad \Longrightarrow \quad \{\alpha_n\}_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathcal{R}$$

Viceversa the following theorem characterizes Complete Ordered Fields

Theorem 3.6 (Convergence of Cauchy sequences in $\mathcal{R}$)

$$\{\alpha_n\}_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathcal{R} \quad \Longrightarrow \quad \{\alpha_n\}_{n\in\mathbb{N}} \text{ Convergent sequence in } \mathcal{R}$$

Proof

Let $\varepsilon > 0$

$$\{\alpha_n\}_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathcal{R} \overset{\text{D.3.12}}{\Longleftrightarrow} \exists\, n \in \mathbb{N} \quad \text{such that}$$
$$|\,\alpha_k - \alpha_m\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k, m \geq n$$

$$\{a_n\}_{n\in\mathbb{N}} \text{ Cauchy sequence in } \mathcal{R} \overset{\text{P.3.18}}{\Longrightarrow} \{a_n\}_{n\in\mathbb{N}} \text{ Bounded sequence in } \mathcal{R}$$
$$\overset{\text{T.3.5}}{\Longrightarrow} \exists\, \{a_{g_n}\}_{n\in\mathbb{N}} \text{ Convergent subsequence of } \{a_n\}_{n\in\mathbb{N}}$$
$$\overset{\text{D.3.16}}{\Longleftrightarrow} \exists\, L \in \mathcal{R} \mid \forall \varepsilon > 0 \quad \exists\, N \in \mathbb{N} \quad \text{such that}$$
$$|\,a_{g_k} - L\,|_{\mathcal{R}} < \varepsilon \quad \forall\, k \geq N$$

Now let $m \geq n + N$

$$|\,a_m - L\,|_{\mathcal{R}} \leq |\,a_m - a_{g_m}\,|_{\mathcal{R}} + |\,a_{g_m} - L\,|_{\mathcal{R}} < 2\varepsilon \overset{\text{D.3.16}}{\Longrightarrow} L = \lim \alpha_n$$

■

3.5 Theorem of Isomorphism between COF

This theorem is the core of all these three chapter.we could say that this result “close our circle” and it gives the wished result on our review on Reals Numbers.

Suppose ones proceeds with the construction of the COF $\mathbb{R}_{\mathcal{R}}$ from the OF $\mathbb{Q}_{\mathcal{R}}$ as in Chapter 2.

Then $\mathbb{R}_{\mathcal{R}}$, $\mathcal{R}$ are two Complete Ordered Fields (COF). And we have the following result:

Theorem 3.7

Let $\Big(\mathcal{K},\, +,\, \cdot,\, \leq\Big)$, $\Big(\mathcal{F},\, \dagger,\, *,\, \preceq\Big)$ Complete Ordered Fields
Exists a function $W\,:\,\mathcal{K}\;\longrightarrow\;\mathcal{F}$ such that

1. $W(x) \preceq W(y) \Longleftrightarrow x \leq y \quad \forall\, x, y \in \mathcal{K}$
2. W is injective
3. W is surjective
4. $W(x + y) = W(x) \dagger W(y) \quad \forall\, x, y\, \in \mathcal{K}$
5. $W(x \cdot y) = W(x) * W(y) \quad \forall\, x, y\, \in \mathcal{K}$

First we have to show the following

Proposition 3.21

Let $\Big(\mathcal{K},\, +,\, \cdot,\, \leq\Big)$, $\Big(\mathcal{F},\, \dagger,\, *,\, \preceq\Big)$ Complete Ordered Fields
Let $\Big(\mathbb{Q}_{\mathcal{K}},\, +,\, \cdot,\, \leq\Big)$, $\Big(\mathbb{Q}_{\mathcal{F}},\, \dagger,\, *,\, \preceq\Big)$ copies of an OF respectively of $\mathcal{K}$ and $\mathcal{F}$ given by theorem 3.4 in Section 3.1
Then there exists $f : \mathbb{Q}_{\mathcal{K}}\;\longrightarrow\;\mathbb{Q}_{\mathcal{F}}$ such that:

- f is injective
- f is surjective
- $f(p + q) = f(p) \dagger f(q) \qquad \forall\, p, q\, \in \mathbb{Q}_{\mathcal{K}}$
- $f(p \cdot q) = f(p) * f(q) \qquad \forall\, p, q\, \in \mathbb{Q}_{\mathcal{K}}$
- $f(q) \preceq f(p) \Longleftrightarrow q \leq p \qquad \forall\, p, q \in \mathbb{Q}_{\mathcal{K}}$

Proof
We give a sketch of proof
Let $\Big(\mathbb{N}_{\mathcal{K}},\, u,\, \sigma\Big)$, $\Big(\mathbb{N}_{\mathcal{F}},\, v,\, \omega\Big)$ copies of Peano Systems respectively of $\mathcal{K}$ and $\mathcal{F}$ given by theorem 3.1 in Section 3.1

- Recalling Subsection 1.1.1 let $R : \mathbb{N}_{\mathcal{K}}\;\longrightarrow \mathbb{N}_{\mathcal{F}}$ such that:
  - $R(1) = u$
  - $R(\sigma(n)) = \omega(R(n)) \qquad \forall\, n \in \mathbb{N}$
  - R is injective

- R is surjective

It is easy to prove that R satisfies:

- $R(n+m) = R(n) \dagger R(m) \qquad \forall\, n, m \in \mathbb{N}_{\mathcal{K}}$
- $R(n \cdot m) = R(n) * R(m) \qquad \forall\, n, m \in \mathbb{N}_{\mathcal{K}}$
- $R(n) \preceq R(m) \iff n \leq m \qquad \forall\, n, m \in \mathbb{N}_{\mathcal{K}}$

- Let $J : \mathbb{N}_{\mathcal{K}} \longrightarrow \mathbb{Z}_{\mathcal{K}}$, $\tilde{J} : \mathbb{N}_{\mathcal{F}} \longrightarrow \mathbb{Z}_{\mathcal{F}}$ as in Immersion theorem 1.1

  Let $T : \mathbb{Z}_{\mathcal{K}} \longrightarrow \mathbb{Z}_{\mathcal{F}}$ defined as $T(z) := \begin{cases} \tilde{J} \circ R \circ J^{-1}(z) & \text{If } z > 0 \\ 0_{\mathcal{F}} & \text{If } z = 0_{\mathcal{K}} \\ -(\tilde{J} \circ R \circ J^{-1}(-z)) & \text{If } z < 0 \end{cases}$

  Then T satisfies:

  - T is injective
  - T is surjective
  - $T(z+s) = T(z) \dagger T(s) \qquad \forall\, z, s \in \mathbb{Z}_{\mathcal{K}}$
  - $T(z \cdot s) = T(z) * T(s) \qquad \forall\, z, s \in \mathbb{Z}_{\mathcal{K}}$
  - $T(z) \preceq T(s) \iff z \leq s \qquad \forall\, z, s \in \mathbb{Z}_{\mathcal{K}}$

- Let $T^2 : \mathbb{Z}_{\mathcal{K}} \times J(\mathbb{N}_{\mathcal{K}}) \longrightarrow \mathbb{Z}_{\mathcal{F}} \times \tilde{J}(\mathbb{N}_{\mathcal{F}})$ defined as
  $T^2(z, s) = (T(z), T(s))$

- According to remark 1.10 in Subsection 1.3.1 (About arbitrary choices on Building $\mathbb{Q}$) we recall definitions of $CH_{\mathbb{Q}_{\mathcal{K}}} : \mathbb{Q}_{\mathcal{K}} \longrightarrow \mathbb{Z}_{\mathcal{K}} \times J(\mathbb{N}_{\mathcal{K}})$, $CH_{\mathbb{Q}_{\mathcal{F}}} : \mathbb{Q}_{\mathcal{F}} \longrightarrow \mathbb{Z}_{\mathcal{F}} \times \tilde{J}(\mathbb{N}_{\mathcal{F}})$

  Let $f : \mathbb{Q}_{\mathcal{K}} \longrightarrow \mathbb{Q}_{\mathcal{F}}$ defined as $f(q) := CH^{-1}_{\mathbb{Q}_{\mathcal{F}}} \circ T^2 \circ CH_{\mathbb{Q}_{\mathcal{K}}}(q)$

  f is the function required

■

Now let us return proving theorem 3.7

Proof

Let $f : \mathbb{Q}_{\mathcal{K}} \longrightarrow \mathbb{Q}_{\mathcal{F}}$ as in proposition 3.21

Now fixed $y \in \mathcal{K}$

Let $A_y := \{q \in \mathbb{Q}_{\mathcal{K}} \mid q < y\}$

Let $B_y := f(A_y)$

By proposition 3.12 $\quad \exists\, n \in \mathbb{N}_{\mathcal{K}} \mid n > y$

Then if $p \in A_y \implies f(p) < f(n)$

Thus $f(n)$ is an upper bound for $B_y \overset{Ded}{\Longrightarrow} \exists \sup B_y$

Let $W(y) := \sup B_y$[6]

[6] The reader should remind that if $q \in A_x \implies f(q) \in B_x \implies f(q) \preceq W(x)$

1. $x \leq y \iff W(x) \preceq W(y)$:

   $\Longrightarrow)$

   If $x = y$ there is nothing to prove

   Then suppose $x < y$.

   By proposition 3.16 $\quad \exists\, q \in \mathbb{Q}_{\mathcal{K}} \quad x < q < y$

   Applying again this result we find $\quad q < q_1 < y$

   On one hand

   If $p \in A_x \overset{o_3}{\Longrightarrow} p < q \Longrightarrow f(p) \prec f(q) \Longrightarrow f(q)$ is an upper bound for B_x

   Then $W(x) \preceq f(q)$

   On the other hand

   $q_1 \in A_y \Longrightarrow f(q_1) \preceq W(y)$

   Then $\quad W(x) \preceq f(q) \prec f(q_1) \preceq W(y) \overset{o_3}{\Longrightarrow} W(x) \prec W(y)$

   $\Longleftarrow)$

   By Contradiction suppose $x \not\leq y \overset{o_4}{\Longrightarrow} y < x$.

   Then, by what we have just proved, $W(y) \prec W(x)$

   Contradiction

2. W is injective: It comes immediately by step 1.

3. W is surjective $\quad (\forall\, T \in \mathcal{F} \quad \exists\, x \in \mathcal{K} \quad | \quad T = W(x))$:

   Let $T \in \mathcal{F}$

   Let $R_T := \{q \in \mathbb{Q}_{\mathcal{F}} \mid q \prec T\} \Longrightarrow T = \sup R_T$

   Then defining $D_T := \{p \in \mathbb{Q}_{\mathcal{K}} \mid f(p) \in R_T\}$

   Since D_T is bounded above $\overset{Ded}{\Longrightarrow} \exists \sup D_T =: x$

   We claim that $W(x) = T$

   $\preceq \quad$ Let $t \in B_x \Longrightarrow t = f(p)$ with $p \in A_x \Longrightarrow p \in D_T$

   $\Longrightarrow t \in R_T \Longrightarrow W(x) \preceq T$

   $\succeq \quad$ By contradiction $W(x) \prec T$

   Now by proposition 3.16 $\quad$ let $\; W(x) \prec k \prec T \quad$ with $\; k \in \mathbb{Q}_{\mathcal{F}}$

   Since $k \in R_T \Longrightarrow f^{-1}(k) \in D_T \Longrightarrow f^{-1}(k) \in A_x$

   $\Longrightarrow k \in B_x \Longrightarrow k \preceq W(x)$

   Then $W(x) \prec k \preceq W(x) \overset{o_3}{\Longrightarrow} W(x) \prec W(x)$ Contradiction

4. $W(x + y) = W(x) \dagger W(y)$:

   $\preceq \quad$ Let $p \in A_{x+y} \Longrightarrow p < x + y \Longrightarrow p - x < y$

   By proposition 3.16 $\quad$ let $p - x < r_1 < y \quad$ and define $r_2 = p - r_1$

   Then $r_1 < y, \quad r_2 < x, \quad p = r_1 + r_2 \quad$ and

$f(p) = f(r_1 + r_2) = f(r_1) \dagger f(r_2) \preceq W(y) \dagger W(x)$

Then $W(x+y) \preceq W(x) \dagger W(y)$

$\succeq$ Let $n \in \mathbb{N}_{\mathcal{F}}$ $\quad t := (2 * n)^{-1}$

By corollary 3.2 $\quad \exists\, q_1 \in A_x \mid W(x) \prec f(q_1) \dagger t$

Let q_2 the same for A_y then

$W(x) \dagger W(y) \prec f(q_1) \dagger f(q_2) \dagger 2t = f(q_1 + q_2) \dagger 2t \preceq W(x+y) \dagger 2t$

Then by corollary 3.7 $\quad W(x) \dagger W(y) \preceq W(x+y)$

5. $W(x \cdot y) = W(x) * W(y)$:

- $x = 0$ or $y = 0$

  There is nothing to prove.

- $x, y > 0$

  $\preceq$ Let $p \in A_{x \cdot y}$, $p > 0 \implies 0 < p < x \cdot y$

  Since $x > 0 \implies 0 < p \cdot x^{-1} < y$

  By proposition 3.16 let $p \cdot x^{-1} < r_1 < y$ and define $r_2 = p \cdot (r_1)^{-1}$
  Then $r_1 < y,\ r_2 < x,\ p = r_1 \cdot r_2$ and

  $f(p) = f(r_1 \cdot r_2) = f(r_1) * f(r_2) \preceq W(x) * W(y) \implies W(x \cdot y) \preceq W(x) * W(y)$

  $\succeq$ Since $x, y > 0 \implies W(x), W(y) \succ 0 \implies W(x)^{-1}, W(y)^{-1} \succ 0$

  Let $n \in \mathbb{N}_{\mathcal{F}}$, and let $t := 2 * n$.

  Let $m \in \mathbb{N}_{\mathcal{F}} \mid m \succ \max\{t,\ W(x) \dagger W(y)\}$

  By corollary 3.2 $\quad \exists\, q_1 \in A_x \mid W(x) \prec f(q_1) \dagger m^{-1}$
  Let q_2 the same for A_y then

  $W(x) * W(y) \prec (f(q_1) \dagger m^{-1}) * (f(q_2) \dagger m^{-1}) \preceq W(x \cdot y) \dagger n^{-1}$

  Then by corollary 3.7 $\quad W(x) * W(y) \preceq W(x \cdot y)$

- $x < 0$, $y < 0$

  $$W(x \cdot y) \overset{\text{P.3.6}}{=} W((-x) \cdot (-y)) = W(-x) * W(-y) = (-W(x)) * (-W(y))$$
  $$\overset{\text{P.3.4}}{=} (-1)^2 * W(x) * W(y) = W(x) * W(y)$$

- $x > 0$, $y < 0$

  $$W(x \cdot y) \overset{\text{P.3.6}}{=} W((-x) \cdot (-y)) = W(-(x) \cdot (-y)) = -W(x \cdot (-y))$$
  $$\overset{\text{P.3.4}}{=} W(x) * (-W(-y)) = W(x) * W(y)$$

- $x < 0$, $y > 0$

  It's the same at the point above

■

Chapter 4

The Axiom of Choice (AC) and elementary Analysis

4.I General remarks on the AC

The axiom of choice is problably the most interesting and, in spite of its late appearance, the most discussed axiom of mathematics, second only to Euclid's axiom of parallel which was introduced more than two thousand years ago

Fraenkel and Bar-Hillel [1]

Una dimostrazione puó essere criticata per la sua estetica; puó essere più o meno funzionale al suo scopo; giusta o totalmente sbagliata
Ma la prova di E.Zermelo $(1871-1953)$ del 1904 in cui introdusse l'Assioma della Scelta (AC), generò una reazione ben più profonda e intricata nella coscienza del mondo matematico.
Zermelo fú uno dei più significativi esponenti del programma formalista di Hilbert, la formulazione di AC lo condusse proprio verso la teoria assiomatica degli insiemi in una pubblicazione del 1908. Se osservato più intuitivamente, cioè non solo in un contesto puramente assiomatico, AC sembra giustificare l'intervento dell'uomo nel mondo platonico degli insiemi, come una legge che permette l'infinito intervento umano di inferenza.

Any argument where one supposes an arbitrary choice to be made an infinite number of times ... [is] outside the domain of mathematics

Borel [2]

Dal 1905 al 1908 eminenti matematici di tutta europa e degli stati uniti dibatterono sulla validita della dimostrazione di Zermelo. In questa prima sezione di questo capitolo, ripercorreremo alcuni tratti della disputa. Per una completa e accurata storia di questo

[1] A.Fraenkel and Y.Bar-Hillel: Foundations of Set Theory (1958 Amsterdam:North Holland)
[2] E.Borel: Quelques remarques sur les principes de la theorie des ensembles (1905 Matematische Annalen)

dibattito vi consigliamo il libro di Moore [Mo1]. Diamo comunque, per in nostri lettori, un breve flash delle critiche più significative alla validità di AC e delle ragioni storiche che ne portarono alla formulazione.
Nel 1883 Cantor propone il famoso Well Ordering Principle (WO): "Every set can be well ordered". Questo risultato fu sviluppato dal medesimo in contemporanea ad un altro risultato potente di teoria "naive" degli insiemi: La Tricotomia dei numeri Cardinali. Cantor non diede dimostrazione di nessuno dei due risultati, credendo comunque che il WO si potesse facilmente dedurre dalla Tricotomia. Questa affermazione non convinse il mondo matematico che bramava una dimostrazione. Nel 1904 Zermelo pubblicò una dimostrazione del WO. Compare per la prima volta la seguente assunzione

Data una qualsiasi collezione V non vuota di sottoinsiemi non vuoti di un insieme X, esiste una funzione $f : V \longrightarrow X$ tale che per ogni C elemento di V, $f(C) \in C$

Personalmente a prima vista questa asserzione mi sembro una tautologia in quanto:

se C è non vuoto $\Longrightarrow \exists\, x_c \in C$ quindi $\begin{array}{rcl} f : V & \longrightarrow & X \\ C & \longmapsto & x_c \end{array}$ soddisfa le ipotesi

No non è così banale e come spiegheremo in seguito la sua non banalità nasce proprio nella definizione di funzione. L'esistenza di tale funzione serve a giustificare, non la possibiltà di sciegliere un elemento da ogni sottoinsieme non vuoto, ma piuttosto a giustificare l'esistenza della "lista delle scelte nella sua totalità".
Vorremmo ancora insistere su questo passaggio. Una funzione è un sottinsieme del prodotto cartesiano, quindi è un insieme. In una visione di platonico esistere di un insieme, del suo esistere nella sua totalità, è un assunzione che precede la possiblità di stabilire la procedura che associa ad ogni sottoinsieme non vuoto un suo elemento. Per ogni C parlare della coppia (C, x_c) come elemento dell'insieme f presuppone la preesistenza dello stesso insieme.
Le critiche provenivano in gran parte dagli esponenti di una corrente chiamata: Construttivismo. La logica costruttivista proponeva l'abbandono del "principio del terzo escluso": A è B o non B, negando l'esistenza di enti tramite dimostrazioni per contraddizione. La contestazione costruttivista coinvolgeva la chiara non costruttività di AC. Inoltre Zermelo aveva, a questo punto, dimostrato un implicazione di un equivalenza in quanto l'implicazione WO $\Longrightarrow$ AC è immediata: Zermelo aveva solamente riformulato il problema con un suo equivalente.
Nonostante le critiche ad AC va riconosciuto il merito di aver sollevato un velo su un "Assunzione" che soggiaceva nelle prove di molti tra i più importanti risultati. Dal 1904 AC impose sempre più il suo peso sulla coscienza del mondo matematico e riveló che la logica aveva bisogno di un altro assioma per inferire nell'universo degli insiemi, costringendo alla rivisitazione di una enorme quantità di risultati dimostrati, specialmente nella teoria degli insiemi di Cantor.
Storicamente le prime dimostrazioni inequivocabilmente legate all'uso di infinte scelte arbitrarie sono quelle relative al concetto di insieme infinito e al suo legame con la numerabilità.

Ed è proprio su questo concetto che si riscontrano i riflessi filosofici di AC più interessanti. Come illustreremo nella seconda Sezione di questo capitolo, affinche un insieme infinito contenga un insieme numerabile, occorre l'assunzione di CC.
In quest ottica, in modelli di Teoria degli Insiemi che rifiutano formulazioni di AC, possiamo dimostrare l'esistenza di insiemi infiniti che non contengono alcun sottoinsieme numerabile, chiamati Cardinali di Dedekind. É chiaro come il concetto di numerabile sia intuitivamente legato al concetto di tempo; la possibilità di contare è la prova del controllo che l'uomo ha sull'infinito. I Cardinali di Dedekind escono dalle potenzialità di controllo dell'uomo sull'infinito, rappresentando la linea di confine tra l'infinito potenziale Aristotelico e il concetto di infinito platonico, cioè tra un infinito comprensibile dalla razionalità e l'infinito come idea.

Many mathematicians still stand opposed to the Axiom of Choice. With the increasing recognition that there are questions in mathematics which cannot be decided without this axiom, the resistance to it must increasingly diseappear.

Steinitz [3]

Ripercorrendo il ruolo della scelta nelle dimostrazioni possiamo individuare tre stadi di scelte che ci guidano su questo sentiero.
Il primo è selezionare un elemento da un insieme non vuoto in maniera non determinata, per estendere il risultato a tutti gli elementi del medesimo insieme. Sebbene AC non intervenga in questa procedura, è qui la prima forma di scelta in una prova.
Il secondo stadio raggruppa quelle prove di esistenza di un particolare oggetto, che conseguono il loro scopo mediante l'uso di infinite scelte seguendo un criterio logico. Come vedremo in questo stadio sono presenti molte prove dell'analisi elementare e l'Assunzione si presenterà nella versione numerabile (CC) principalmente nell'estrazione di una successione convergente all'oggetto suddetto.
Nel terzo stadio ci infiliamo le prove che estendono il primo stadio a un numero infinito di insiemi. Si scelgono casualmente i rappresentanti da infiniti insiemi, soprattutto classi di equivalenza, e si prova un risultato sull'insieme delle scelte estendendolo poi universalmente su ogni classe per arbitrarietà delle selezioni.
É straordinario anche solo avere un idea della quantità dei risultati, sviluppati principalmente dai grandi matematici del XIX secolo, che hanno fatto uso di questa Assunzione, magari incosciamente, prima che Zermelo la formulasse come assioma. L'Assioma della Scelta.
Nel resto del Capitolo noi esploreremo una parte dei risultati più noti nella teoria elementare degli insiemi e, soprattutto, nell'analisi elementare che necessitano l'uso di AC o di CC, sottolineando il passaggio della dimostrazione in cui occorre questa assunzione, e dove possibile forniremo delle prove che sviano l'uso di infinite scelte.
Per una rivisitazione più formale dei risultati legati ad AC vi consigliamo il testo di Jech

[3] E.Steinitz: Algebraische Theorie der Körper(1910 Journal für die reine und angewandte Mathematik)

[Je1]. Molto simile ma meno tecnico e pi u scorrevole illustrazione ai risultati connessi vi rimandiamo al testo di Herrlich [He1].

4.1 Countable Union Theorem

Countable Union Theorem(Cantor 1872) is one of the most meaningful and historically important use of CC[4]. The following theorem show as, proof involved countability, needs infinite arbitrary choices.

Theorem 4.1 (Countable Union Theorem)

Let X a set

$$\{A_n\}_{n\in\mathbb{N}} \text{ sequence in } \mathcal{P}(X) \mid \begin{cases} A_n \,\text{Countable} & \forall\, n \in \mathbb{N} \\ A_n \cap A_k = \emptyset & \text{If}\, n \neq k \end{cases} \implies A := \cup_{n\in\mathbb{N}} A_n \text{ is Countable}$$

Proof

$$A_n \text{ is Countable} \overset{\text{D.3.9}}{\Longrightarrow} \forall\, n \in \mathbb{N} \,\text{Let}\, f^{(n)} : \mathbb{N} \longrightarrow A_n$$
$$f^{(n)} \text{ bijective}$$

$$\text{Defining} \begin{cases} C_1 := \{f^{(1)}(1)\} \\ C_{n+1} := \{f^{(k)}(i) \mid i + k = n + 2\} \end{cases} \implies \begin{cases} C_n \,\text{is Finite} & \forall\, n \in \mathbb{N} \\ A = \cup_{n\in\mathbb{N}} C_n \\ C_n \cap C_k = \emptyset & \text{If}\, n \neq k \end{cases}$$

$$\text{Let } x \in A \implies \exists!\, n_x \mid \begin{cases} x \in C_{n_x} \\ x = f^{(k_x)}(i_x) \quad \text{with } i_x + k_x = n_x \end{cases}$$

$$\text{Hence let us define } \phi(x) := \begin{cases} 1 & \text{If}\, n_x = 1 \\ (n_x \cdot (n_x - 1) \cdot 2^{-1}) + i_x & \text{If}\, n_x > 1 \end{cases}$$

Such as $\phi : A \longrightarrow \mathbb{N}$ is bijective

■

4.2 Dedekind-Finiteness

Our account does not rob the mathematicians of their science, by disproving the actual existence of the infinite.... In point of fact they do not need the infinite and do not use it. They only postulate that the finite straight line may be produced as far as they wish

Aristotle [5]

There are two different definitions for finite set. The classic one (X is finite if and only if there exists a bijective function on $\{1, 2, \dots n\}$) and Dedekind definitions, called

[4] Axioms of Countable Choices

[5] R.McKeon: The Basic Works of Aristotle(1941 New York: Random House)

D-finiteness. In this section we show how equivalence between these two formulations require Axiom of Countable Choice CC.

Definition 4.1

Let X a set , $X \neq \emptyset$

X is D-infinite $\Longleftrightarrow$ $\exists\, B \subset X,\ B \neq \emptyset$ and $f : X \longrightarrow B$ bijective

Otherwise we say that X is D-Finite

Proposition 4.1

Let X a set, $X \neq \emptyset$

X is D-infinite $\Longleftrightarrow \exists\, B \subseteq X,\ B$ Countable

Proof

$\Longrightarrow$

$X$is D-infinite $\Longrightarrow \exists\, B \subset X,\ B \neq \emptyset$ and $f : X \longrightarrow B$ bijective

Let $y \in X - B$

By Recursion Theorem (Lemma 1.2) exists

$$R_{f,y} : \mathbb{N} \longrightarrow X \quad \text{such that} \quad \begin{cases} R_{f,y}(1) = y \\ R_{f,y}(n+1) = f(R_{f,y}(n)) \end{cases}$$

Such as $R_{f,y}$ is injective

To prove this statement fix $k \in \mathbb{N}$ and prove by induction on n the following:

$\forall\, n, k \in \mathbb{N} \quad R_{f,y}(n) = R_{f,y}(l) \implies n = l \quad \forall\, l \leq k$

Let $k \in \mathbb{N}$ and let $l \leq k$ and proceed by induction on n

- $n = 1$

  $R_{f,y}(1) = R_{f,y}(l) \implies R_{f,y}(l) = y \implies l = 1$ since if $l > 1,\ R_{f,y}(l) \in B$

- Supposed for n we show it for $n+1$

$$\begin{aligned} R_{f,y}(n+1) = R_{f,y}(l) &\implies l > 1 \text{ since } R_{f,y}(n+1) \in B \quad \forall\, n \in \mathbb{N} \\ &\implies l = m+1 \text{ and } R_{f,y}(n+1) = R_{f,y}(m+1) \\ &\implies f(R_{f,y}(n)) = f(R_{f,y}(m)) \\ &\implies R_{f,y}(n) = R_{f,y}(m) \text{ since } f \text{ is injective} \\ &\overset{I.S.}{\implies} n = m \implies n+1 = l \end{aligned}$$

Thus $h(\mathbb{N}) := \{h(n) \mid n \in \mathbb{N}\}$ is a Countable subset of X

$\Longleftarrow$

$\exists\, B \subseteq X,\ B$ Countable $\Longrightarrow \exists\, g : \mathbb{N} \longrightarrow B$ Bijective

Let $g_1 : \mathbb{N} \longrightarrow B - \{g(1)\}$ defined as $g_1(n) := g(n+1)$
Such as g_1 is bijective

Let $h : B \longrightarrow B - \{g(1)\}$ defined as $h(x) := g_1(g^{-1}(x))$
Such as h is bijective

Now let $f(x) := \begin{cases} h(x) & \text{If}\, x \in B \\ x & \text{If}\, x \notin B \end{cases}$

Clearly such as $f : X \longrightarrow X - \{g(1)\}$ is bijection of X with one its proper subset ■

Remark 4.1

This is the touchy step, which will needs arbitrary choices in results involving Countability.

If X is Countable there are many function $f : \mathbb{N} \longrightarrow X$ bijective.

Given one f defining $g(n) := \begin{cases} f(2) & \text{If}\, n = 1 \\ f(1) & \text{If}\, n = 2 \\ f(n) & \text{Otherwise} \end{cases}$

Then $g : \mathbb{N} \longrightarrow X$ bijective.

Corollary 4.1

Let X a set $, X \neq \emptyset$

X Countable $\Longrightarrow X$ is Infinite

X Countable $\Longrightarrow X$ is D-Infinite

Proof
Trivial ■

Theorem 4.2
Let X a set $, X \neq \emptyset$

$$X \text{ is Finite} \Longleftrightarrow X \text{ is D-Finite}$$

Proof
$\Longrightarrow$

Trivial

$\Longleftarrow$

By contradiction X is Infinite $\overset{\text{C.3.8}}{\Longrightarrow} \forall\, n \in \mathbb{N}$ let $f^{(n)} : I^{(n)} \longrightarrow X$ injective

Let $\begin{cases} k_1 := f^{(1)}(1) \\ k_{n+1} := \min\{i \leq n+1 \mid f^{(n+1)}(i) \notin f^{(n)}(I^{(n)})\,\} \quad \forall\, n \in \mathbb{N} \end{cases}$

$\forall n \in \mathbb{N} \qquad \text{define } F(n) := f^{(n)}(k_n)$

$$F : \mathbb{N} \longrightarrow X \text{ is injective} \Longrightarrow f(\mathbb{N}) \text{ is a Countable subset of } X$$

$$\overset{\text{P.4.1}}{\Longrightarrow} X \text{is D-Infinite}$$

Contradiction ■

Corollary 4.2

Every Infinite set X has a Countable subset

Proof
X Infinite $\overset{\text{T.4.2}}{\Longrightarrow}$ X D-infinite $\overset{\text{P.4.1}}{\Longrightarrow}$ $\exists B \subset X$ Countable
■

4.3 Point Topology of $\mathbb{R}$ and AC

Modulo $|\cdot|_{\mathbb{R}}$ induces a natural topology on the real numbers. According to this topology, there are two kind of definitions for its basic notions as closed sets and limit point. the first one $(\varepsilon - \delta)-$definition, we could say it is "static" definition. The second one, "dynamic" definition, uses convergent sequences.
In this Section we will show how equivalence between these two definition, needs the countable formulation CC of AC.
Moreover we will go deep in analyzing Bolzano-Weierstrass theorem, one of the most important theorems in first course of Analysis. We will propose two proofs of this theorem. The first one is standard and there is clearly use of CC. Second one will avoid it.
Definition 4.2

Let $A \subseteq \mathbb{R}$

$$A \text{ is Open} \Longleftrightarrow \forall x \in A \quad \exists \varepsilon > 0 \quad |$$
$$\text{If } y \in \mathbb{R},\ |x - y|_{\mathbb{R}} < \varepsilon \Longrightarrow y \in A$$

Definition 4.3

Let $A \subseteq \mathbb{R}$

A is Closed $\Longleftrightarrow$ $\mathbb{R} - A$ is Open

Definition 4.4

Let $X \subseteq \mathbb{R},\ x \in \mathbb{R}$

$$x \text{ is a limit point for } X \Longleftrightarrow \forall \varepsilon > 0 \quad \exists y \in X - \{x\} \quad \text{such that}$$
$$|x - y|_{\mathbb{R}} < \varepsilon$$

Proposition 4.2

$$A \text{ is Closed} \iff \text{If } x \text{ limit point for } A \Rightarrow x \in A$$

Proof
We omit this proof sice it is very simple[6] ■

Definition 4.5

Let $A \subseteq \mathbb{R}$

$$A \text{ is a Sequentially Closed} \iff \left.\begin{array}{l}\{\,a_n\,\}_{n\in\mathbb{N}} \subseteq A\\ x = \lim a_n\end{array}\right\} \Rightarrow x \in A$$

Definition 4.6

Let $X \subseteq \mathbb{R},\ x \in \mathbb{R}$

$$x \text{ is a sequential limit point for } X \iff \exists\,\{\,a_n\,\}_{n\in\mathbb{N}} \subseteq X - \{x\} \quad \text{such that} \quad x = \lim a_n$$

Proposition 4.3

$$A \text{ is Sequentally Closed} \iff \text{If } x \text{ squential limit point for } A \Rightarrow x \in A$$

Proof
Trivial by definitions 4.5 and 4.6 ■

Theorem 4.3
Let $X \subseteq \mathbb{R},\ x \in \mathbb{R}$

$$x \text{ is a limit point for } X \iff x \text{ is a sequential limit point for } X$$

Proof
$\Longleftarrow$

Trivial

$\Longrightarrow$

$$x \text{ is a limit point for } X \iff \forall\,\varepsilon > 0 \quad \exists\, y \in X - \{x\} \quad \text{such that} \quad |\,x - y\,|_{\mathbb{R}} < \varepsilon$$

Let $n \in \mathbb{N}$ We define $B_n(x) := \{y \in X - \{x\} \ \mid\ |\,x - y\,|_{\mathbb{R}} < \frac{1}{n}\}$

Since x is limit point for $X \implies B_n(x) \neq \emptyset$

[6] See [Gi1] pg 25

$\forall n \in \mathbb{N}$ let $y_n \in B_n(x)$

$$\left.\begin{array}{l} \{\, y_n \,\}_{n\in\mathbb{N}} \text{ is a sequence in } X - \{x\} \\ x = \lim\, y_n \end{array}\right\} \overset{\text{D.4.6}}{\Longrightarrow} x \text{ is sequential limit point for} X \quad \blacksquare$$

Theorem 4.4 (Bolzano-Weierstrass Theorem)

Every Infinite Bounded set X has a limit point

Proof

Since X is bounded there exist $a, b \in \mathbb{R} \mid X \subseteq [a, b]$[7]

$[a, b] = [a, \frac{a+b}{2}] \cup [\frac{a+b}{2}, b]$ and since X is infinite at least one of the following holds;

$X \cap [a, \frac{a+b}{2}]$ is Infinite, $\quad X \cap [\frac{a+b}{2}, b]$ is Infinite

$$\text{Define} \begin{cases} a_1 := \begin{cases} a & \text{If } X \cap [a, \frac{a+b}{2}] \text{ is Infinte} \\ \frac{a+b}{2} & \text{Otherwise} \end{cases} \\ b_1 := \begin{cases} \frac{a+b}{2} & \text{If } X \cap [a, \frac{a+b}{2}] \text{ is Infinte} \\ b & \text{Otherwise} \end{cases} \end{cases}$$

$$\forall n \in \mathbb{N} \quad \text{we define} \quad \begin{cases} a_{n+1} := \begin{cases} a_n & \text{If } X \cap [a_n, \frac{a_n+b_n}{2}] \text{ is Infinte} \\ \frac{a_n+b_n}{2} & \text{If } X \cap [\frac{a_n+b_n}{2}, b_n] \text{ is Infinte} \end{cases} \\ b_{n+1} := \begin{cases} \frac{a_n+b_n}{2} & \text{If } X \cap [a_n, \frac{a_n+b_n}{2}] \text{ is Infinte} \\ b_n & \text{If } X \cap [\frac{a_n+b_n}{2}, b_n] \text{ is Infinte} \end{cases} \end{cases}$$

$$\text{These two sequences } \{\, a_n \,\}_{n\in\mathbb{N}}, \{\, b_n \,\}_{n\in\mathbb{N}} \text{ satisfy: } \begin{cases} a \le a_n \le a_{n+1} & \forall n \in \mathbb{N} \\ b \ge b_n \ge b_{n+1} & \forall n \in \mathbb{N} \\ [a_n, b_n] \cap X \text{ is Infinte} & \forall n \in \mathbb{N} \\ b_n - a_n = \frac{a+b}{2^n} & \forall n \in \mathbb{N} \end{cases}$$

By proposition 3.19 we have :
$A := \sup\{a_n \mid n \in \mathbb{N}\} = \lim\, a_n$ and $B := \inf\{b_n \mid n \in \mathbb{N}\} = \lim\, b_n$

On one hand
given $k, m \in \mathbb{N}$ and $n > k, m \implies a_k \le a_n \le b_n \le b_m$
Then by definition of sup $\quad A \le b_m \quad$ Hence Applying the same reasoning we get $B \ge A$

On the other hand
$0 \le B - A \le b_n - a_n = \frac{a+b}{2^n} \quad \forall n \in \mathbb{N} \Longrightarrow A = B$

A is a limit point for X $\blacksquare$

Proof
We divide this proof into steps

1. Suppose $X \subseteq [1, c]$ with $c > 1$

[7] $[a, b] := \{x \in \mathbb{R} \mid a \le x \le b\}$

$\exists\, N \in \mathbb{N} \quad | \quad [1, c] \subseteq \cup_{j=1}^{N} [j, j+1]$

Let $k := \min\{n \in \mathbb{N} \mid [n, n+1] \cap X \text{ is Infinite}\}$

$\rho_1 := \min\{i \in \{0,1\} \mid [k + \frac{i}{2}, k + \frac{i+1}{2}] \cap X \text{ is Infinite}\}$

2. Recalling definition 3.7 let $n \in \mathbb{N}$ and define a subset of $n-$map in $\mathbb{R}$ as follows:

$$\{\, b_k \,\}_{k \leq n} \in A_n \iff \begin{cases} b_1 = k + \frac{\rho_1}{2} \\ [b_k, b_k + \frac{1}{2^k}] \cap X \text{ is Infinite} \quad \forall\, k \leq n \\ \text{If } n > 1 \quad b_{k+1} = b_k \text{ or } b_{k+1} = b_k + \frac{1}{2^{k+1}} \quad \forall\, k < n \end{cases}$$

3. $A_n \neq \emptyset \quad \forall\, n \in \mathbb{N}$:

   One proves by induction that called $I = \{n \in \mathbb{N} \mid \exists \{\, a_k \,\}_{k \leq n} \in A_n\} \implies I = \mathbb{N}$

4. Let $n \in \mathbb{N}$ and define $f(n) := \inf\{b_n \mid \{\, b_k \,\}_{k \leq n} \in A_n\}$

   $\{(k, f(k)) \quad | \quad k \in \mathbb{N}\}$ is a sequence in $\mathbb{R}$ and we denote it as $\{\, f_n \,\}_{n \in \mathbb{N}}$

   It easy prove by induction that $\{\, f_n \,\}_{n \in \mathbb{N}}$ satisfies:

$$\begin{cases} \{\, f_n \,\}_{n \in \mathbb{N}} \in A_m \quad \forall\, m \in \mathbb{N} \\ f_n \leq f_{n+1} \quad \forall\, n \in \mathbb{N} \\ [f_n, f_n + \frac{1}{2^n}] \cap X \text{ is Infinte} \quad \forall\, n \in \mathbb{N} \end{cases}$$

5. Let $k \in \mathbb{N}$. $\quad f_{k+n} \in [f_k, f_k + \frac{1}{2^k}] \quad \forall\, n \in \mathbb{N}$:

   It is immediate by induction on n

   Then $\quad \exists \, \sup\{f_n \mid n \in \mathbb{N}\} \overset{\text{P.3.19}}{=} \lim f_n$

6. Defining $F := \{f_n \mid n \in \mathbb{N}\}$, then F is a limit point for X:

   On one hand, by step 5., we have $F \in [f_k, f_k + \frac{1}{2^k}] \quad \forall\, k \in \mathbb{N}$

   Let $\varepsilon > 0$

   $F = \lim f_n \implies \exists\, n \in \mathbb{N} \quad | \quad F - \varepsilon \leq f_k \leq F + \varepsilon \quad \forall\, k \geq n$

   On the other hand let $m \in \mathbb{N} \quad | \quad \frac{1}{2^m} < \varepsilon \implies f_m + \frac{1}{2^m} < F + \varepsilon$

   Hence if $N \geq \max\{n, m\}$

$$F - \varepsilon \leq f_N \leq F \leq f_N + \frac{1}{2^N} < F + \varepsilon \implies \begin{cases} [f_N, f_N + \frac{1}{2^N}] \cap X \text{ is Infinte} \\ [f_N, f_N + \frac{1}{2^N}] \subset [F - \varepsilon, F + \varepsilon] \end{cases}$$

$$\implies F \text{ is a limit point for } X$$

■

4.4 Continuity and AC

Ever according to the natural topology, given by $|\cdot|_{\mathbb{R}}$, there are two definitions of continuity for a function $f : \mathbb{R} \longrightarrow \mathbb{R}$.

The first is the standard $(\varepsilon - \delta)$-definition. The second one is the dynamic definitions by sequences. They are equivalents if one supposes CC holds.

Choosing, as proper definitions for closed set and continuity, the dynamic ones, all the elementary program Analysis could be proved.

However, as we see in the following section, CC do not intervenes only in results concerting equivalence by definitions. In the matter of this, we propose a "dynamic" formulation of Weierstrass maximum and minimum theorem.

Definition 4.7

$$\begin{aligned}
&\text{Let } A \subseteq \mathbb{R},\ A \neq \emptyset,\ \ f : A \longrightarrow \mathbb{R} \text{ and let } x \in A \\
&f \text{ is sequentially continuous in } x \Longleftrightarrow \forall \left\{ x_n \right\}_{n\in\mathbb{N}} \subseteq A \ \mid\ \lim x_n = x \\
&\qquad\qquad\qquad\qquad\qquad\qquad \Longrightarrow \lim f(x_n) = f(x)
\end{aligned}$$

Definition 4.8

$$\begin{aligned}
&\text{Let } A \subseteq \mathbb{R},\ A \neq \emptyset,\ \ f : A \longrightarrow \mathbb{R} \\
&f \text{ is sequentially continuous in } A \Longleftrightarrow \forall x \in \mathbb{R} \\
&\qquad\qquad\qquad\qquad\qquad\qquad x \in A \Longrightarrow\ f \text{ is sequentially continuous in } x
\end{aligned}$$

Theorem 4.5 (Weierstrass theorem)

$$\left.\begin{array}{l} A \subseteq \mathbb{R},\ \ A \text{ sequentially closed and bounded} \\ f : A \longrightarrow \mathbb{R} \text{ sequentially continuous in } A \end{array}\right\} \Longrightarrow \exists\, y \in A \ \mid\ f(x) \leq f(y) \quad \forall\, x \in A$$

Proof

1. $f(A)$ is bounded above:

   By contradiction, called $A_n := \{x \in A \mid f(x) > n\},\ \ A_n \neq \emptyset \quad \forall\, n \in \mathbb{N}$

   $$\begin{aligned}
   &\forall\, n \in \mathbb{N} \text{ let } x_n \in A_n \Longrightarrow \left\{ x_n \right\}_{n\in\mathbb{N}} \subseteq A \text{ bounded} \\
   &\qquad \overset{\text{T.3.5}}{\Longrightarrow} \exists \left\{ x_{g_n} \right\}_{n\in\mathbb{N}} \text{ Convergent subsequence of } \left\{ x_n \right\}_{n\in\mathbb{N}} \\
   &\qquad \overset{\text{D.4.5}}{\Longrightarrow} \text{called } x := \lim x_{g_n} \Longrightarrow x \in A
   \end{aligned}$$

   By definition of $f \Longrightarrow \lim f(x_{g_n}) = f(x)$

   But this is a contradiction since $x_{g_n} \in A_{g_n}$

2. Let $F := \sup f(A) \Longrightarrow \exists\, y \in A \ \mid\ f(y) = F$:

   By definition of L.U.B. (definition 2.2)

   called $B_n := \{x \in A \mid |\, f(x) - F\,|_{\mathbb{R}} < \frac{1}{n}\},\ \ B_n \neq \emptyset \quad \forall\, n \in \mathbb{N}$

$$\forall n \in \mathbb{N} \text{ let } x_n \in B_n \Longrightarrow \{x_n\}_{n\in\mathbb{N}} \subseteq A \text{ bounded}$$

$$\overset{\text{T.3.5}}{\Longrightarrow} \exists \{x_{g_n}\}_{n\in\mathbb{N}} \text{ Convergent subsequence of } \{x_n\}_{n\in\mathbb{N}}$$

$$\overset{\text{D.4.5}}{\Longrightarrow} \text{called } y := \lim x_{g_n} \Longrightarrow y \in A$$

Since f is sequentially continuous on $A \Longrightarrow \lim f(x_{g_n}) = f(y) \Longrightarrow f(y) = F$

■

4.5 Equivalent formulations of AC

Although first intrust and perplexity, today AC is commonly accepted in mathematical community in large and uses of AC became to appear in many mathematical branches. Increasing comprehension of AC brought to equivalent formulations, more complex formulations which conclusions are very powerful and meaningful. Today more than 100 principles are recognized how equivalent principles of AC. For more equivalent formulation see H.Rubin and J.Rubin [RR1].

Remark 4.2

Let us recall some preliminary Set Theory notions:

Let S be a set and R be a relation on S

$$(S,R) \text{ is a Partially Ordered Set } \Longleftrightarrow \begin{cases} R \text{ is reflexive on } S \\ R \text{ is antisymmetric on } S \\ R \text{ is transitive on } S \end{cases}$$

$$(S,R) \text{ is a Totally Ordered Set } \Longleftrightarrow \begin{cases} (S,R) \text{ is a partially ordered set} \\ R \text{ is Total on } S \end{cases}$$

$$(S,R) \text{ is a Well-Ordered Set } \Longleftrightarrow \begin{cases} (S,R) \text{ is a partially ordered set} \\ \forall A \subseteq S,\ A \neq \emptyset \Longrightarrow \exists a \in A \quad | \quad aRx \quad \forall x \in A \end{cases}$$

Definition 4.9

Let $(X, \leq)$ a partially ordered set

$C \subseteq X$ is a $\leq$-chain $\Longleftrightarrow$ $(C, \leq)$ is totally ordered

Definition 4.10

Let $(X, \leq)$ a partially ordered set

$M \in X$ is $\leq$-maximal for X $\Longleftrightarrow$ If $a \in X,\ M \leq a \Longrightarrow a = M$

Notational Remark 4.1
Let X be a set and let $C \subseteq \mathcal{P}(X)$

From this point forward, in this section we use to denote $(\cup_{c \in C} c)$ as $\cup C$

And we adopt the same notation also for $\cap$

(**Axioms of Choice**)(**AC**)
Let X a set

If $T \subseteq \mathcal{P}(X) - \{\emptyset\} \implies \exists f : T \longrightarrow X \mid \forall A \in T \quad f(A) \in A$

(**Well ordering Principle**)(**WO**)
Let X a set, $X \neq \emptyset$

Then exists a relation R on X such that (X, R) is a well-ordered set

(**Zorn's Lemma**)(**Zorn**)
Let $(X, \leq)$ a partially ordered set
Let $V := \{C \subseteq X \mid C \ \leq\text{-chain}\}$

If $\forall\, C \in V \quad \exists\, N \in X$ upper bound for $C \implies \exists\, M \ \leq$-maximal element for X

(**Hausdorff's Maximal Principle**)(**HMP**)
Let $(X, \leq)$ a partially ordered set
Let $V := \{C \subseteq X \mid C \ \leq\text{-chain}\}$

Then $\exists\, M \in V \quad \subseteq -$maximal element for V

Theorem 4.6
Let X a set

$$\textbf{(WO)} \iff \textbf{(AC)} \iff \textbf{(Zorn)} \iff \textbf{(HMP)}$$

Proof
(WO)$\implies$ **(AC)**:

Trivial

(AC)$\implies$ **(HMP)**[8]:

Let $(X, \leq)$ a partially ordered set
Let $V := \{C \subseteq X \mid C \ \leq\text{-chain}\}$

We divide this proof into two steps

1. Let $g : V \longrightarrow V \mid \forall A \in V \begin{cases} A = g(A) \\ \text{or} \\ \exists x \in X \mid A \cup \{x\} = g(A) \end{cases}$

[8]This proof is inspired by [Ru2] pg 430

Then $\exists\, B \in V \mid g(B) = B$:

We divide step 1. in three points

- Let $b \in V$

  $$W \subseteq V \text{ is a } b\text{-tower} \iff \begin{cases} (t_1) & b \in W \\ (t_2) & C \subseteq W,\ C \ \subseteq\text{-chain} \implies \cup C \ \in W \\ (t_3) & A \in W \implies g(A) \in W \end{cases}$$

  $\mathfrak{T}_b := \{W \subseteq V \ \mid \ W \text{ is } \ b\text{-tower}\}$

  $\mathfrak{T}_b \neq \emptyset \quad$ since $\{A \in V \mid b \subseteq A\} \in \mathfrak{T}_b$

  Defining $T := \cap\, \mathfrak{T}_b$, it is easy to prove that $\ T \in \mathfrak{T}_b$

  Let $O_T := \{A \in T \mid \forall\, B \in T \quad A \subseteq B \ \text{ or } \ B \subseteq A\}$

  $O_T \neq \emptyset \quad$ since $\cup T \ \in O_T$

- $T = O_T$:

  It suffices to prove that $O_T \ \in \mathfrak{T}_b$

  (t_1) Immediate

  (t_2) Immediate

  (t_3) Let $C \in O_T$, we define $O_{g(C)} := \{A \in T \mid A \subseteq g(C) \text{ or } g(C) \subseteq A\}$

  It is straightforward to prove that $O_{g(C)}$ is a $b-$tower

  Then $O_{g(C)} = T$ and it follows immediately that $C \in O_T \implies g(C) \in O_T$

- $\exists\, A_0 \in V \ \mid \ g(A_0) = A_0$:

  $$\cup T \ \in T \overset{(t_3)}{\implies} g(\cup T) \in T$$
  $$\implies g(\cup T) \subseteq \cup T \iff \cup T = g(\cup T)$$

2. $\exists\, M \in V \quad \subseteq$-maximal element for V:

   Let $A \in V \quad$ We define $A^* := \{x \in X \ \mid \ x \notin A,\ A \cup \{x\} \ \in V\}$

   $V^* := \{A^* \mid A \in V\}$

   $V_1^* := \{A^* \in V^* \mid A^* \neq \emptyset\}$

   By **(AC)** let $f : V_1^* \ \longrightarrow \ X \ \mid \ \forall\, A^* \in V_1^* \quad f(A^*) \in A^*$

   We define $g : V \ \longrightarrow \ V \ \mid g(A) := \begin{cases} A \cup \{f(A^*)\} & \text{if } A^* \in V_1^* \\ A & \text{if } A^* \notin V_1^* \end{cases}$

   By step 1 exists $M \in V \ \mid \ g(M) = M \implies M^* = \emptyset$

   Let $A \in V \ \mid \ M \subseteq A$

   By contradiction $M \subset A \implies M^* \neq \emptyset$. Contradiction

(HMP)$\Longrightarrow$(Zorn):

Let $(X, \leq)$ a partially ordered set
Let $V := \{C \subseteq X \ \mid \ C \ \ \leq\text{-chain}\,\}$

By **(HMP)** exists $K \in V \quad \subseteq -$maximal element for V

By **(Zorn)** hypothesis $\exists\ N \in X \quad | \quad N$ upper bound for K

Let $x \in X \ | \ N \leq x$ and, by contradiction, suppose $N < x \implies k < x \ \forall k \in K$
Defining $K' := K \cup \{x\} \implies K' \in V$ (since$K \in V$), $K \subset K'$

Contradiction by $\subseteq$-maximality of K

(Zorn)$\Longrightarrow$(WO)[9]:

Let X a set, $X \neq \emptyset$

We define a subset P of $\mathcal{P}(X) \times \mathcal{P}(X \times X)$ as follows[10]:

$$(A, r) \in P \iff \begin{cases} A \neq \emptyset \\ r \text{ is a well-order of } A \end{cases}$$

Since $X \neq \emptyset \implies \exists x \in X \implies (\{x\}, \{(x, x)\}) \in P$

We define a relation $\leq_P$ on P as follows:

$$(A, r) \leq_P (B, t) \iff \begin{cases} A \subseteq B \\ t_{|_A} = r \quad (t \text{ is an extension of } r) \end{cases}$$

$(P, \leq_P)$ is a partial ordered set and if $C \subseteq P$ is a $\leq_P$-chain :

$$\begin{cases} ((\cup_{(A,r)\in C} A), (\cup_{(A,r)\in C} r)) \in P \\ ((\cup_{(A,r)\in C} A), (\cup_{(A,r)\in C} r)) \text{ is upper bound for } C \end{cases} \overset{\textbf{(Zorn)}}{\Longrightarrow} \exists\,(M, R) \quad \leq_p\text{-maximal for } P$$

Suppose exists $z \in X - M$

We define $M_1 := M \cup \{z\}$ and $R_1 := R \cup \{(x, z) \ | \ x \in M\}$

$$\left.\begin{matrix} (M_1, R_1) \in P \\ (M, R) \leq_p (M_1, R_1) \end{matrix}\right\} \overset{\text{D.4.10}}{\Longrightarrow} (M_1, R_1) = (M, R) \implies R \text{ is a well-order of } X \quad \blacksquare$$

4.6 An "ugly" application of AC

Definition 4.11

Let $(K, \star, \cdot)$ a Field [11]

$(V, +)$ is a $K-$ Space Vector if and only if satisfies

sv1 $+$ is a associative commutative binary inner operation of V and exists a neutral element 0 for it

sv2 $\forall k \in K$ exists a function $g_k : V \longrightarrow V$

[9] An inspiration for this proof is [RR1] pg 16
[10] See definition of $\mathcal{P}(X)$ in: A brief survey of Set theory and logic
[11] see definition 1.18

sv3 $g_k(u+v) = g_k(u) + g_k(v) \quad \forall\, u, v \in V, \forall\, k \in K$

sv4 $g_{k \star + t}(u) = g_k(u) + g_t(u) \quad \forall\, v \in V, \forall\, k, t \in K$

sv5 $g_{k \cdot t}(u) = g_k(g_t(u)) \quad \forall\, u \in V, \forall\, k, t \in K$

sv6 $u + g_{-1}(u) = 0 \quad \forall\, u \in V$

sv7 $g_1(u) = u \quad \forall\, u \in V$

Henceforth we will denote $k\, v := g_k(v) \quad \forall\, u \in V, \forall\, k \in K$

Remark 4.3

$\mathbb{R}$ is a $\mathbb{Q}-$Space Vector

Definition 4.12

Let $(V, +)$ a $K-$Space Vector
Let $A \subset V$
A is linearly independent $\Longleftrightarrow \forall\, n \geq 1, \quad \forall\, v_1, \ldots, v_n \in V$

$$\text{if} \quad \sum_{i=1}^{n} k_i\, v_i = 0 \Longrightarrow k_i = 0 \quad \forall\, 1 \leq i \leq n$$

Definition 4.13

Let $(V, +)$ a $K-$Space Vector
Let $B \subset V$ linearly independent
B is an Hamel Basis (HB) for $V \iff \forall\, v \in V \quad \exists\, n \in \mathbb{N}$,
$v_1, \ldots, v_n \in B$ and $k_1, \ldots, k_n \in K$
(all depending on v) such that

$$v = \sum_{i=1}^{n} k_i\, v_i$$

and this rapresentation is unique

Theorem 4.7

$$\textbf{(Zorn)} \implies \exists\, f : \mathbb{R} \longrightarrow \mathbb{R} \quad | \quad \begin{cases} f(1) = 1 \\ f(x+y) = f(x) + f(y) \quad \forall\, x, y \in \mathbb{R} \\ f \text{ is not continuous on } \mathbb{R} \end{cases}$$

Proof

We divide the proof in steps

1. **Zorn** $\Longrightarrow \; \exists \quad$ HB for $\quad \mathbb{R}$

2. $$\left.\begin{array}{l} f(1)=1 \\ f(x+y)=f(x)+f(y) \quad \forall\, x,y\, \in \mathbb{R} \\ f \text{ continuous on } \mathbb{R} \end{array}\right\} \Longrightarrow f(x)=x \quad \forall\, x \in \mathbb{R}$$

3. $\exists\; HB$ for $\mathbb{R} \;\Longrightarrow\; \exists f \quad$ such that $$\left\{\begin{array}{l} f(1)=1 \\ f(x+y)=f(x)+f(y) \quad \forall\, x,y\, \in \mathbb{R} \\ f \text{ is not continuous on } \mathbb{R} \end{array}\right.$$

1. Let $B_1 := \{1, \sqrt{2}\}$. Surely B_1 is linearly independent

   Let $\mathcal{V} := \{A \subset \mathbb{R} \;\mid\; B_1 \subseteq A,\;\; A \text{ is linearly independent}\}$

   $(\mathcal{V}, \subseteq)$ is a partially ordered family of subsets of $\mathbb{R}$

   Let C a $\subseteq$-chain in $\mathcal{V}$

   Defining $N := \cup\, C \;\Longrightarrow\; N$ is upper bound for C and $N\,\mathcal{V}$

   Then by **Zorn** there exists a $\subseteq$-maximal element $B \in \mathcal{V}$

   B is an HB for $\mathbb{R}$:

   Let $x \in \mathbb{R}$

   - if $x \in B \;\Longrightarrow\; n=1,\, v_1 = x,\, k_1 = 1$ is a representation for x
     Suppose exists another representation for $x \;\Longrightarrow\; x = \sum q_i\, v_i$
     Hence $\sum q_i\, v_i \; - x = 0$
     Since B is linear independent, all the rational coefficients must be 0
     Since x has coefficient -1 we surely claim that, calling $A := \{i \in \mathbb{N} \;\mid\; v_i = x\}$
     $A \neq \emptyset, \quad , \sum_{i \in A} q_i = 1, \quad q_j = 0$ if $j \notin A$
     Hence $x = \sum_{i \in A} q_i\, v_i = \sum_{i \in A} q_i\, x = x$
     And this prove the uniqueness of the representation for any $x \in B$
   - if $x \notin B$
     By maximality of $B \Longrightarrow B \cup \{x\}$ is linearly dependent
     Hence $\exists \quad n \in \mathbb{N}, \quad v_1, \ldots, v_n \;\in B, \quad k, k_1, \ldots, k_n \;\in Q,\, k \neq 0,\, k_i \neq 0 \quad \mid$
     $k\, x + \sum_{i=1}^{n} \, k_i\, v_i = 0$
     Then $\; x = \sum_{i=1}^{n} p_i\, v_i \;$ (where $p_i := k_i \cdot (-k)^{-1}$) is a representation for x
     Suppose there exists another representation for $x \quad x = \sum_{i=1}^{m} q_i\, w_i$
     Let $A := \{i \in \mathbb{N} \mid v_i = w_i\}$
     Then $\quad \sum_{i \in A} (k_i - q_i)\, v_i + \sum_{i \notin A} k_i\, v_i + \sum_{i \notin A} q_i\, w_i = 0$
     By linear independence of $B \Longrightarrow \left\{\begin{array}{l} k_i - q_i = 0 \quad \text{if } i \in A \\ k_i, q_j = 0 \quad \text{if } i, j \;\notin A \end{array}\right.$

And this prove the uniqueness of the representation for any $x \notin B$

2. We omit this proof because it is very simple [12]

3. Let $\phi(x) := \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{if } x \in B,\ x \neq 1 \end{cases}$

   Let $f(x) := \begin{cases} \phi(x) & \text{if } x \in B \\ \sum r_i\, \phi(v_i) & \text{if } x \notin B \quad (\text{Hence } x = \sum r_i\, v_i) \end{cases}$

   - $f(1) = 1$
   - Let $\quad x = \sum_{i=1}^{n} r_i\, v_i, \quad y = \sum_{i=1}^{m} q_i\, w_i$

     By uniqueness of the representation

     $x + y = \sum r_i\, v_i + \sum q_i\, w_i$ is the only representation for $x + y$

     Defining $r_{n+j} := q_j,\ \ v_{n+j} := w_j \quad \forall j \leq m$

$$x + y = \sum_{i=1}^{n+m} r_i\, v_i \implies f(x+y) = \sum_{i=1}^{n+m} r_i\, \phi(v_i)$$
$$= \sum_{i=1}^{n} r_i\, \phi(v_i) + \sum_{i=1}^{m} r_{n+i}\, \phi(w_{n+i})$$
$$= \sum_{i=1}^{n} r_i\, \phi(v_i) + \sum_{i=1}^{m} q_i\, \phi(w_i) = f(x) + f(y)$$

   - f is not continuous on $\mathbb{R}$:

     For $x = \sqrt{2}\quad$ since $x \in B - \{1\} \implies 0 = f(x) \neq x$

     By step 2. we get the thesis

■

[12] Moore attributes this proof to Cauchy [Mo1] pg 112

Appendix A

Structures containing Peano Systems

In Chapters 1. and 2. we showed the following result:

Given a Peano System[1] exists a model of a Complete Ordered Field[2] which contains a copy of a Peano System as a proper subset

In this Appendix we try to do the other way round, reasoning according minimal conditions on a "structure" suffice to contain a model of a Peano System as a proper subset. We do not want neither to explain accurately what we mean for "structure" nor to try to give a hierarchy of conditions on a structure trying to establish the weakest ones, since it would be to long and we prefer a more cautious approach.

Definition A.1

A Primitive System (P, f) is a nonempty set P and a function $f : P \longrightarrow P$

Definition A.2

A D-Primitive System (P, f) is Primitive System (P, f) such that
f injective and non surjective

Aim of Appendix A

In this Appendix we will show the following results:

$$\text{Given a D-Primitive System } (P, f) \Longrightarrow \exists \begin{cases} \mathbb{N}_P \subset P, \ \mathbb{N}_P \neq \emptyset \\ a \in P \\ \sigma : \mathbb{N}_P \longrightarrow \mathbb{N}_P \end{cases} \Big| \quad (\mathbb{N}_P, a, \sigma) \text{ is a Peano system}$$

[1]See definition 1.1
[2]See definition 2.6

Definition A.3

Let (P, f) a D-Primitive System, then by definition A.2 $f(P) \subset P$

Let $a \in (P - f(P)),\ \ I \subseteq P$

$$I \text{ is } a\text{-Inductive} \iff \begin{cases} a \in I \\ p \in I \implies f(p) \in I \quad \forall\, p \in P \end{cases}$$

For example P is a-Inductive

Definition A.4

Let $\mathfrak{I} := \{I \subseteq P \mid I\ a\text{-Inductive}\}$

Let $\mathbb{N}_P := \cap_{I \in \mathfrak{I}}\ I$

The following theorem guaranties us result's achievement

Theorem A.1

Let (P, f) a D-Primitive System, let $\mathbb{N}_P$ as in definition A.4, let $\sigma := f_{|\mathbb{N}_\mathcal{R}}$

$$(\mathbb{N}_P,\ a,\ \sigma) \text{ is a Peano System}$$

Proof

We have to prove that:

1. $\mathbb{N}_P$ is a-Inductive:

   $a \in I \quad \forall\, I\ a\text{-Inductive} \overset{\text{D.A.4}}{\implies} a \in \mathbb{N}_P$

   $p \in \mathbb{N}_P \overset{\text{D.A.4}}{\implies} p \in I \quad \forall\, I\ a\text{-Inductive}$

   $\overset{\text{D.A.3}}{\implies} f(p) \in I \quad \forall\, I\ a\text{-Inductive} \overset{\text{D.A.4}}{\implies} f(p) \in \mathbb{N}_P$

2. $\left.\begin{array}{l} a \notin f(P) \\ f(\mathbb{N}_P) \subseteq f(P) \end{array}\right\} \implies a \notin f(\mathbb{N}_P)$

3. Obvious since f is injective

4. Immediate by definition A.4

■

Theorem A.2

$$\text{In a COF } (\mathcal{R}, +, *, \leq) \quad \exists\, \mathbb{N} \subset \mathcal{R},\ \mathbb{N} \neq \emptyset \quad | \quad (\mathbb{N}, +, *, \leq) \text{ is a Peano Ring}^3$$

Proof
Let $(\mathcal{R},\, +,\, *,\, \leq)$ a Complete Ordered Field[4]

- Let $P := \{x \in \mathcal{R} \mid x \geq 1\}$ and $f(x) := x + 1 \quad \forall\, x \in \mathcal{R}$.
- It is immediate to see that $(P,\, f)$ is a D-Primitive System[5].
- Hence using results of this Appendix let $(\mathbb{N}_P,\, 1,\, f_{|_P})$ a Peano System1.1.
- Using results of Section 1.1[6] we could define two binary inner operations $+_{\mathbb{N}_P}$, $*_{\mathbb{N}_P}$ on $\mathbb{N}_P$, a relation $\leq_{\mathbb{N}_P}$ on $\mathbb{N}_P$ such that $\left(\mathbb{N}_P,\, +_{\mathbb{N}_P},\, *_{\mathbb{N}_P},\, \leq_{\mathbb{N}_P}\right)$ is a Peano Ring
- By Induction it is simple to show that
  - operations $+$ and $*$ of $\mathcal{R}$ restricted on $\mathbb{N}_P$ coincide with $+_{\mathbb{N}_P}$ and $*_{\mathbb{N}_P}$
  - $n \leq k \iff n \leq_{\mathbb{N}_P} k \quad \forall\, n, k \in \mathbb{N}_P$
- Namely $(\mathbb{N}_P,\, +,\, *,\, \leq)$ is a Peano Ring

■

[4]See definition 2.6
[5]See definition A.2
[6]See Aim of section 1.1

Bibliography

[Bo1] Boyer C.B. (1968), "History of Mathematics", John Wiley & Sons

[Co1] Courant R. and Robbins H. (1941), "What is Mathematics", Oxford University Press

[De1] Dedekind R. (1901), "Essay on the theory of numbers", Open Court Publishing Company

[Di1] Dieudonnè J. (1967), "Elements d'Analyse tome I", Gauthiers-Villars

[Fe1] Feferman S. (1993), "The development of programs for the foundations of Mathematics in the first third of 20th century"

[Frs1] Ferreiròs J. (2007), "Labyrinth of Thought", Birkäuser

[Fo1] Fontana M. (1989), "Insiemi, numeri e polinomi : primo ciclo di lezioni del corso di algebra con esercizi svolti" CISU

[Gi1] Giusti E. (2002), "Analisi Matematica 1. terza edizione", Bollati-Boringhieri

[Gi2] Giusti E. (2007), "Piccola storia del calcolo infinitesimale dall antichità al novecento", Istituti editoriali e poligrafici internazionali

[He1] Herrlich H. (2006), "Axiom of Choice", Springer-Verlag

[Hn1] Hungerford T.W. (1974), "Algebra", Springer-Verlag

[Is1] Israel G. (1980) "Rigore e Assiomatica nella Matematica Moderna, in Scienza e Storia. Analisi critica e problemi attuali", Editori Riuniti

[Je1] Jech T.J. (1973), "The Axiom of Choice", North-Holland Publishing Company

[La1] Landau E. (1951), "Foundations of Analysis", Chelsea Publishing & Co.

[Lo1] Lolli G. (1973), "Teoria assiomatica degli insiemi", Boringhieri

[Me1] Mendelson E. (1973), "Number Systems and the Foundations of Analysis", Paperback

[MG1] Millàn Gasca A. (2004), "All'inizio fu lo scriba", Mimesis

[Mo1] Moore G. (1982), "Zermelo's Axiom of Choice. its origin developments and influence", Springer-Verlag

[PC1] Piacentini Cattaneo G.M. (1996), "Algebra", Zanichelli

[RR1] Rubin J.E. and Rubin H. (1961), "Equivalence of the Axiom of Choice", North-Holland Publishing Company

[Ru1] Rudin W. (1976), "Principles of Mathematical Analysis third edition", McGraw-Hill

[Ru2] Rudin W. (1986), "Real and Complex Analysis", McGraw-Hill

[SD1] Scorza Dragoni G. (1967), "Elementi di Analisi Matematica", Cedam

[Sh1] Shoenfield J.R. (1967), "Matematical Logic", Addison-Wesley Publishing Company

[Th1] Thurston H.A. (1956), "The Number System", Blackie & Son

[Tr1] Troelstra A.S. (1991), "History of constructivism in the 20th century"

[VN1] Von Neumann J. (1947), "The Mathematician", University of Chicago Press

[Zv1] Zwirner G. (1972), "Elementi di analisi matematica", CEDAM