7. ORDERED FIELDS

In this lecture we define the notion of a field and ordered field, which will allow us to give an axiomatic definition of rationals. We then show that rationals are unique up to a bijection that preserves the ordered field structure which we will later to (similarly) axiomatize the reals and prove their uniqueness. Such statements are necessary to ensure that there is only one real analysis one can build out of Zermelo's axioms.

We start by a definition that is standard in algebra:

Definition 7.1 (A field) *A set F with binary operations $+$ and $\cdot$ and two distinct distinguished elements 0 and 1 is a* field *if*

(F1) *the operations of addition and multiplication obey the commutative and associative laws (each of them separately) as well as the distributive law,*
(F2) *(Zero element)* $\forall a \in F\colon\ 0 + a = a \wedge 0 \cdot a = 0$,
(F3) *(Unit element)* $\forall a \in F\colon\ 1 \cdot a = a$,
(F4) *(Additive inverse)* $\forall a \in F\ \exists(-a) \in F\colon\ a + (-a) = 0$,
(F5) *(Multiplicative inverse)* $\forall a \in F \smallsetminus \{0\}\ \exists a^{-1} \in F\colon\ a \cdot a^{-1} = 1$.

We will write $(F, +, 0, \cdot, 1)$ to denote the field F along with all its important attributes.

One can check that, in every field, the following holds:

- The zero and unit elements are unique. Indeed, assuming 0 and $0'$ are both zero elements, then $0 = 0 + 0' = 0'$. The proof for the unit element is similar.
- The additive and multiplicative inverses are unique. Indeed, focusing on the multiplicative inverse, if $\tilde{a}^{-1}$ and a^{-1} are both inverses to $a \neq 0$, then the associative law for multiplication shows $\tilde{a}^{-1} = \tilde{a}^{-1} \cdot (a \cdot a^{-1}) = (\tilde{a}^{-1} \cdot a) \cdot a^{-1} = a^{-1}$.
- The operations of addition and multiplication by non-zero number are injective. Indeed, we have
$$\forall a, b, c \in F\colon\ \ a + b = a + c \Rightarrow b = c \tag{7.1}$$
and
$$\forall a, b, c \in F\colon\ \ (a \neq 0\ \wedge a \cdot b = a \cdot c) \Rightarrow b = c \tag{7.2}$$
- The product of any two non-zero elements is non-zero,
$$\forall a, b \in F\colon\ (a \neq 0 \wedge b \neq 0) \Rightarrow a \cdot b = 0 \tag{7.3}$$
- For all $a, b \in F$ we have $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ and thus $(-a) \cdot (-a) = a \cdot a$. Similarly, we infer $(-a)^{-1} = -a^{-1}$ for all $a \neq 0$.

Theorem 6.6 shows that $\mathbb{Q}$ endowed with operations (6.16–6.17) is a field. There are other natural examples of fields. For instance, there are many finite fields. (We have yet to define the term "finite" but in these examples this will be clear intuitively.) The simplest non-trivial example is $F_2 := \{0, 1\}$, where addition is defined by

$$0 + 0 := 0, \quad 0 + 1 = 1 + 0 := 1, \quad 1 + 1 := 0 \tag{7.4}$$

and multiplication by

$$0 \cdot 0 := 0, \quad 0 \cdot 1 = 1 \cdot 0 := 0, \quad 1 \cdot 1 := 1, \tag{7.5}$$

In the absence of other elements, F_2 is clearly a field. (Note that, in this field, $-1 = 1$.) This example generalizes for any p prime to $F_p := \mathbb{Z}/(p\mathbb{Z})$ which can be identified with

the set $\{0, 1, \ldots, p-1\}$ and the operations of addition and multiplication as in $\mathbb{Z}$ except taken modulo p. Note that F_p is a field *only if* p is a prime; indeed, otherwise there are two non-zero elements — namely, the divisors of p — that multiply to zero.

The need to rule out the example (7.4–7.5) as well as F_p for p prime from consideration (as good sets of numbers for real analysis) motivates us restrict the concept of a field further by requiring the existence of an ordering relation:

Definition 7.2 (Ordered field) *We say that a field $(F, +, 0, \cdot, 1)$ is an* ordered field *if F admits a binary relation $\leqslant$ that*

(O1) *is a total ordering, i.e., is reflexive, antisymmetric and transitive and is connex in the sense that $\forall a, b \in F\colon\ a \leqslant b \vee b \leqslant a$,*

(O2) *is preserved by addition, i.e.,*

$$\forall a, b, c \in F\colon\ a \leqslant b \ \Rightarrow\ a + c \leqslant b + c \tag{7.6}$$

(O3) *is preserved by multiplication by non-negative numbers, i.e.,*

$$\forall a, b, c \in F\colon \big(a \leqslant b \wedge 0 \leqslant c\big) \ \Rightarrow\ a \cdot c \leqslant b \cdot c. \tag{7.7}$$

We will write $(F, +, 0, \cdot, 1, \leqslant)$ for an ordered field with the ordering relation $\leqslant$.

The properties O1-O3 directly imply:

Lemma 7.3 *$0 \leqslant 1$ holds in any ordered field $(F, +, 0, \cdot, 1, \leqslant)$.*

Proof. Assume, on the way to a contradiction, that $1 < 0$. Then (O2) shows $0 < -1$ and, since -1 is non-negative, (O3) gives $0 = 0 \cdot (-1) \leqslant (-1) \cdot (-1) = 1$, in contradiction with the assumption. Hence $0 \leqslant 1$ by the fact that $\leqslant$ is a total order; see (O1). □

We now list further properties which the reader will find completely standard but which, to get a fully rigorous treatment, now have to be verified from the definition of an ordered field:

Lemma 7.4 *Let $(F, +, 0, \cdot, 1, \leqslant)$ be an ordered field. Then*

(1) $\forall a, b \in F\colon\ 0 \leqslant b \Leftrightarrow a \leqslant a + b$

(2) $\forall a, b \in F\colon\ a \leqslant b \Rightarrow -b \leqslant -a$

(3) $\forall a, b \in F\colon (0 < a\ \wedge a \leqslant b) \Rightarrow b^{-1} \leqslant a^{-1}$

Proof. Left to a homework exercise. □

In order to get to the axiomatic definition of the rationals, we make the following important observation:

Lemma 7.5 *Let $(F, +, 0, \cdot, 1, \leqslant)$ be an ordered field. Set*

$$\mathbb{N}_F := \bigcap \big\{ A \subseteq F\colon 0 \in A \wedge (\forall x \in A\colon x + 1 \in A) \big\} \tag{7.8}$$

and let $S_F(x) := x + 1$. Then $(\mathbb{N}_F, 0, S_F)$ is a system of naturals.

Proof. We need to verify the Peano axioms P1-P5. First note that the set $A := F$ contributes to the intersection, which is thus non-empty. It follows that $\mathbb{N}_F$ is a set which, since every A in (7.8) contains 0, obeys $0 \in \mathbb{N}_F$, thus proving P1. Since every set on the rigth of (7.8) is closed under S_F, we also have that S_F is a map $\mathbb{N}_F \to \mathbb{N}_F$, proving P2.

The map S_F is injective (even on F) because $x+1 = y+1$ implies $x = y$ by (7.1), proving P4. As to the range of S_F omitting zero, here we note that the set $\{x \in F\colon 0 \leqslant x\}$ of non-negative elements contributes on the right of (7.8). Since $0 < 1$ by Lemma 7.3 and the assumption that $0 \neq 1$ (for otherwise F would be just a one-element set) forces $0 < x+1$ for each $x \in \mathbb{N}_F$ and thus $0 \notin S_F(\mathbb{N}_F)$, proving P3.

It remains to prove the Induction Axiom P5. For this, let $A \subseteq \mathbb{N}_F$ such that $0 \in A$ and $S_F(A) \subseteq A$. But then A appears among the sets on the right of (7.8) and so $\mathbb{N}_F \subseteq A$. Hence $A = \mathbb{N}_F$ proving P5 as well. □

We will refer to $\mathbb{N}_F$ as the *naturals of* F. With this concept in hand, we are able to axiomatize the rationals as well:

Definition 7.6 *A system of the rationals is an ordered field* $(F, +, 0, \cdot, 1, \leqslant)$ *such that*

$$\forall x \in F\ \exists m, n, r \in \mathbb{N}_F\colon\ r \neq 0 \wedge x = r^{-1} \cdot (m - n) \tag{7.9}$$

where $\mathbb{N}_F$ *are the naturals of* F.

As we have shown above, there is at least one systems of rationals. (The ordering relation is defined in (6.22). Checking that these satisfy O1-O3 in Definition 7.2 is left to the reader.) It remains to prove that the rationals are, in fact, unique:

Theorem 7.7 (Uniqueness of the rationals) *Let* $(F, +, 0, \cdot, 1, \leqslant)$ *and* $(\widetilde{F}, \mathbin{\widetilde{+}}, \widetilde{0}, \mathbin{\widetilde{\cdot}}, \widetilde{1}, \mathbin{\widetilde{\leqslant}})$ *be two systems of the rationals. Then there exists a bijection* $\phi\colon F \to \widetilde{F}$ *such that*

(1) $\forall a, b \in F\colon \phi(a+b) = \phi(a) \mathbin{\widetilde{+}} \phi(b)$,
(2) $\forall a, b \in F\colon \phi(a \cdot b) = \phi(a) \mathbin{\widetilde{\cdot}} \phi(b)$
(3) $\phi(0) = \widetilde{0}$ *and* $\phi(1) = \widetilde{1}$,
(4) $\forall a, b \in F\colon a \leqslant b \Rightarrow \phi(a) \mathbin{\widetilde{\leqslant}} \phi(b)$.

In particular, a system of the rationals is unique up to an isomorphism.

Proof (sketch). We only give the main steps leaving the details to the reader. The uniqueness of the naturals (see Theorem 4.7) and Lemma 7.5 imply the existence of a bijection $\phi\colon \mathbb{N}_F \to \mathbb{N}_{\widetilde{F}}$ with

$$\phi(0) = \widetilde{0}\ \wedge\ \phi \circ S_F = S_{\widetilde{F}} \circ \phi \tag{7.10}$$

In particular, we have

$$\phi(1) = \phi \circ S_F(0) = S_{\widetilde{F}} \circ \phi(0) = S_{\widetilde{F}}(\widetilde{0}) = \widetilde{1} \tag{7.11}$$

proving (3) above. In light of (7.10), ϕ takes the operation of addition $+$ to $\mathbin{\widetilde{+}}$; i.e.,

$$\forall m, n \in \mathbb{N}_F\colon \phi(m+n) = \phi(m) \mathbin{\widetilde{+}} \phi(n) \tag{7.12}$$

We then check that the same applies to multiplication,

$$\forall m, n \in \mathbb{N}_F\colon \phi(m \cdot n) = \phi(m) \mathbin{\widetilde{\cdot}} \phi(n) \tag{7.13}$$

(Both of these statements are readily proved by induction.)

Next we extend ϕ to F as follows: If $x = r^{-1} \cdot (m-n)$ for some $m, n, r \in \mathbb{N}_F$ with $r \neq 0$, then we set

$$\phi(x) := \phi(r)^{-1} \mathbin{\widetilde{\cdot}} \big(\phi(m) \mathbin{\widetilde{+}} (-\phi(n))\big). \tag{7.14}$$

Using (7.12–7.13) we now verify that the right-hand side is the same regardless of which naturals m, n, r are used to represent x, and so ϕ thus defines a function $F \to \widetilde{F}$. A similar argument proves that the map is injective; using that ϕ is bijective and thus invertible on the naturals then shows that ϕ is also onto. This gives properites (1-3) above. In order to prove (4), by additivity of ϕ it suffices to focus on the cxase $a = 0$. Here we note that, for $x \geqslant 0$, we can take $m \geqslant 0$, $r > 0$ and $n = 0$ in (7.14). The fact that property (4) holds for the naturals then implies $\phi(x) \geqslant 0$ as desired. □

Having proved the uniqueness of the rationals, a natural question whether there are in fact other ordered fields than rationals. We will answer this in the next two lectures.