0. Preliminaries: Ordinals and cardinals

This chapter essentially covers §§ 4,6,9 and 10 of ([**?**]) and is designed to give a brief introduction to the main notions of set theory for those who haven't seen them. In order to make it a little bit more interesting for those who have seen them, we include a small application which shall be very important during this lecture course: coding of countable ordinals by real numbers.

We start with several definitions:

0.1 (Binary Relations). Let X be an arbitrary set, $R \subseteq X \times X$. We say R is

- **reflexive** iff $(\forall x \in X)(\langle x, x\rangle \in R)$,
- **irreflexive** iff $(\forall x \in X)(\langle x, x\rangle \notin R)$,
- **symmetric** iff $(\forall x, y \in X)(\langle x, y\rangle \in R \longrightarrow \langle y, x\rangle \in R)$,
- **transitive** iff $(\forall x, y, z \in X)(\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \longrightarrow \langle x, z\rangle \in R)$,
- **antisymmetric** iff $(\forall x, y \in X)(\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R \longrightarrow x = y)$,
- **linear** iff $(\forall x, y \in X)(\langle x, y\rangle \in R \vee \langle y, x\rangle \in R \vee x = y)$,
- **well-founded** iff $(\forall A \subseteq X)(A$ has a smallest R-element$)$,
  i.e., $(\forall A \subseteq X)(\exists a \in A)(\forall b \in A)(\langle a, b\rangle \in R \vee a = x)$,

Combining these properties yields the most familiar binary relations: We say R is

- a **partial order** iff R is reflexive, antisymmetric and transitive,
- a **strict partial order** iff R is irreflexive, antisymmetric and transitive,
- a **preorder** iff R is reflexive and transitive,
- a **strict preorder** iff R is irreflexive and transitive,

If the above relation are also linear we get a **linear order**, a **strict linear order** , a **linear preorder** and a **strict linear preorder**, respectively.

Further we say R is

- a **well-order** iff R is a well-founded linear order,
- a **strict well-order** iff R is well-founded strict linear order.

0.2 (Coding of Pairs). Let X be an infinite set, then there is a bijection between $X \times X$ and X (Hessenberg's Theorem, [[**?**], 10.7]).

In case $X = \mathbb{N}$ we can give such a bijection explicitly:

$$\langle n, m\rangle \mapsto \frac{i^2 + j^2 + 2ij + i + 3j}{2}.$$

For this bijection we fix the notation $\ulcorner \cdot, \cdot \urcorner : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

EXERCISE 1. Show that $\ulcorner \cdot, \cdot \urcorner : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a bijection.

0.3 (The "epsilon"-relation). For any set X we can define the relation E_X as: $E_X \subseteq X \times X; \langle x, y\rangle \in E_X \iff x \in y$. We call this relation the **"epsilon"-relation**.

0.4. DEFINITION. A set X is said to be **transitive** iff $(\forall x, y)(y \in X \wedge x \in y \longrightarrow x \in X)$.

0.5. DEFINITION. We say that a set X is an **ordinal** iff X is transitive and E_X is a well-order.

The ordinals form the backbone of set theory. Their wellordered structure is the spine and fundament of every model of set theory, starting with the natural numbers and then using the process of transfinite induction to reach out in the infinite.

We define the natural numbers by $0 := \emptyset$, $1 := \{0\}$, $2 := \{0, 1\}$, and, in general, $n + 1 = n \cup \{n\}$. The set of all such numbers will be denoted by $\mathbb{N}$ or ω.

From this point onwards we define larger and larger ordinals by transfinite induction, starting with $\omega + 1 = \omega \cup \{\omega\} = \mathbb{N} \cup \{\mathbb{N}\}$, $\omega + 2 := \omega + 1 \cup \{\omega + 1\}$, and continuing into the tramsfinite. All mentioned ordinals are countable sets. Using the axiom of replacement (or the axiom of choice), we can show that there are uncountable ordinals. The first uncountable ordinal is denoted by ω_1 – in general, the αth uncountable ordinal (where α is an ordinal) is denoted by ω_α.

0.6. EXAMPLE. The following sets are transitive: $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$.
Not transitive are: $\{\{\emptyset\}\}$ and $\{\{\emptyset\}, \{\{\{\emptyset\}\}\}\}$.

0.7. LEMMA. Let X be an ordinal, then also is $X \cup \{X\}$.

PROOF. [**?**, ?] q.e.d.

0.8. DEFINITION. **Cardinals [AC]**: We say an ordinal α is a **cardinal** iff there is no $\beta \in \alpha$ such that there is a bijection between β and α.

Usually, from now on, we will denote ordinals with the lower-case greek letters α, β, γ, δ, η, ζ, and ξ, and cardinals with the lower-case greek letters κ, λ, and μ.

We recall that in ZF the Axiom of Choice is equivalent to Zermelo's Well-Ordering Theorem, which says that every set can be well-ordered. [**?**, ...]

Using Zermelo's Well-Ordering Theorem, we can define the following: For every set X there exists a unique cardinal κ, such that there is a bijection between X an κ. We will denote this cardinal $\mathrm{Card}(X)$ (or $\bar{\bar{X}}$ as done in [**?**]).

All ordinals ω_α mentioned above are cardinals. When we want to emphasize the cardinal character of the ordinals ω_α, we write $\aleph_\alpha := \omega_\alpha$.

For every cardinal κ there is a least cardinal greater than κ, which we will denote by κ^+. If $\kappa = \aleph_\alpha$, then $\kappa^+ = \aleph_{\alpha+1}$.

0.9. THEOREM (Mostowski's Isomorphism Theorem). Every well-order is isomorphic to an ordinal and both the ordinal and the isomorphism are unique.

PROOF. See [**?**, ...]. q.e.d.

This ordinal is called the **order-type** of the well-order w and denoted as $\mathrm{otp}(w)$.

0.10 (Coding a relation). Let X be an arbitrary infinite set, $R \subseteq X \times X$ a relation and let $\pi : X \times X \to X$ the bijection as given in (0.2). We then define

$$x \in C_R :\iff \pi^{-1}(x) \in R.$$

We call C_R the **code** for R.

0.11. EXAMPLE. For $X = \mathbb{N}$ we have:

$$\langle i, j\rangle \in R \longleftrightarrow \ulcorner i, j \urcorner = \frac{i^2 + j^2 + 2ij + i + 3j}{2} \in C_R, C_R \subseteq \mathbb{N}.$$

In this way, every subset A of X codes a relation: $\langle x, y\rangle \in R_A :\longleftrightarrow \pi(x, y) \in A$. It is easy to see that in case $S \subseteq X \times X$ is a relation and $A \subseteq X$, then $R_{C_S} = S$ and $C_{R_A} = A$.

0.12 (Special subsets of $\mathbb{N}$). (a) A set $A \subseteq \mathbb{N}$ is said to be a **code for a linear order** iff R_A is linear. We will denote the set of codes for linear orders as **LO** .

(b) A set $A \subseteq \mathbb{N}$ is said to be a **code for a well-order** iff R_A is a well-order. We will denote the set of codes for well-orders as **WO** . If $A \in \mathbf{WO}$, then by Theorem 0.9 there is a unique ordinal isomorphic to R_A. We shall denote this by α_{R_A}.

0.13. DEFINITION. We define a map $d : \mathcal{P}(\mathbb{N}) \to \{\alpha\ ;\ \omega \leq \alpha < \omega_1\}$ as follows: For $A \subseteq \mathbb{N}$ let

$$d(A) := \begin{cases} \alpha_{R_A} & A \in \mathbf{WO}, \\ 0 & A \notin \mathbf{WO}. \end{cases}$$

A set $A \subseteq \mathbb{N}$ such that $d(A) = \alpha$ is called a **code for** α.

0.14. CLAIM. The map d as defined above is surjective.

PROOF. Let $\alpha < \omega_1$ be arbitrary. We want to show $(\exists A \subseteq \mathbb{N})(d(A) = \alpha)$. Since α is countable, ther exists a bijection $f : \alpha \to \omega = \mathbb{N}$. We define an order R_f on $\mathbb{N}$ by $\langle n, m\rangle \in R_f \longleftrightarrow f^{-1}(n) < f^{-1}(m)$.

Clearly, $\langle \mathbb{N}, R_f\rangle$ is isomorphic to $\langle \alpha, <\rangle$ via f, i.e., $\alpha_{R_f} = \alpha$. Let $A := C_{R_f} \subseteq \mathbb{N}$. From the remark after Example 0.11, we know $R_{C_{R_f}} = R_f$ and $R_A = R_f$. Consequently, $\alpha_{R_A} = \alpha_{R_f} = \alpha$. So $d(A) = \alpha$. q.e.d.

EXERCISE 2. Let λ be an arbitrary cardinal. Show that all ordinals $\alpha < \lambda^+$ can be coded by subsets of λ following the proof idea of Claim 0.14:

(a) Define $A \in \mathrm{WO}_\lambda\ :\leftrightarrow\ A$ is a wellorder. Show that for all $A \in \mathrm{WO}_\lambda$ there is a unique $\alpha < \lambda^+$ such that $\langle \alpha, \in\rangle$ and $\langle \lambda, R_A\rangle$ are isomorphic.

(b) For $\lambda \leq \alpha < \lambda^+$ with a bijection $f : \lambda \to \alpha$ define the relation R_f in analogy to the proof of 0.14.

(c) Define the analogue of the function d from Definition 0.13 and show that it is surjective.

0.15 (Coding $\alpha < \omega_1$ by a real). We go one step further: From Definition 0.13 and Claim 0.14 we have a surjective function $d : \mathcal{P}(\mathbb{N}) \to \omega_1$ (note that you have to fix the function d slightly because the actual function d from Definition 0.13 doesn't hit the finite ordinals); this time we are looking for a surjective function $c : \setminus \to \omega_1$.

If we look at the diagram

$$\mathbb{R} \xrightarrow{?} \mathcal{P}(\mathbb{N}) \xrightarrow{d} \omega_1,$$

we are looking for a surjective function from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$.

For $A \subseteq \mathbb{N}$ let $\chi_A : \mathbb{N} \to 2(= \{0,1\})$ be the characteristic function:

$$\chi_A(n) := \begin{cases} 0 & n \notin A, \\ 1 & n \in A. \end{cases}$$

We have to be somewhat careful here. Actually $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ are equipollent, and there is a bijection between these two sets, but because of the peculiarities of the set $\mathbb{R}$ it is not too easy to write one down. Therefore we will restrict ourselves to a subset of $\mathbb{R}$.

The peculiarities we talked about are that the binary (or, in general, p-ary) expansions of real numbers are not unique: because $\sum_{i=1}^{\infty} 2^{-i} = 1$, the real number 1 has two binary expansions.

Let us first look at the function

$$e : \mathcal{P}(\mathbb{N}) \to \mathbb{R}; A \mapsto \sum_{n=0}^{\infty} \chi_A(n)\, 3^{-(n+1)}.$$

For any A, the real number $e(A)$, written in ternary form will never contain any 2s in the binary expansion. Therefore its binary expansion is unique, and thus e is injective.

Let c be the inverse of e, and let $D \subseteq \mathbb{R}$ be the domain of c. With this notation, we get the desired surjection

$$D \xrightarrow{c} \mathcal{P}(\mathbb{N}) \xrightarrow{d} \omega_1.$$

We say a $x \in D$ is a **code for** $\alpha < \omega_1$ iff $d(c(x)) = \alpha$.