Naive Set theory

$\boxed{\textit{Definition } 1.}$ A binary relation between two sets A and B is a subset R of $A \times B$ - i.e., is a set of ordered pairs $(x, y) \in A \times B$.

If $A = B$, so that the relation R is a subset of $A \times A$, we say that R is a relation on A.

If R is a relation between A and B (i.e., if $R \subseteq A \times B$), we often write xRy or $x \sim y$ instead of $(x, y) \in R$.

Examples.

1.) Let $A = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$, and take the binary relation on A consisting of all (x, y) such that $x \leq y$.

2.) Let $A = \mathbb{Z}$, and take the binary relation on A consisting of all ordered pairs (x, y) such that $x - y$ is even. In this case x and y are related if and only if either both are even or both are odd.

3.) Let $A = \mathbb{Z}_{>0}$, and take the binary relation on A consisting of all pairs (x, y) such that the quotient $\frac{y}{x}$ is a positive integer (in other words, x evenly divides y with no remainder).

4.) Given a set A, take the binary relation on the set $\mathcal{P}(A)$ of all its subsets defined by BRC if and only if B is a subset of C.

5.) (Graph) Let $f : A \to B$ be a function. Define R as follows: $R = \{(x, y) \in A \times B | y = f(x)\}$.

6.) Let n be a positive integer, $A = \mathbb{Z}$, and take the binary relation on A consisting of all ordered pairs (x, y) such that $x - y$ is divisible by n. (Notation: $x = y(mod\ n)$).

Let's define some of the most important types of relations:

$\boxed{\textit{Definition } 2.}$ Let R be a binary relation on a set A :

- R is reflexive if $a \sim a$ for all $a \in A$.
- R is symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$.
- R is transitive if $a \sim b$ and $b \sim c$ imply $a \sim c$ for all $a, b, c \in A$

We say that R is an **equivalence relation** if it satisfies all of the three properties defined above.

Examples.
1.) If $A = \mathbb{R}$, consider the binary relation $a \sim b$ if and only if $a - b$ is an integer.

2.) Example 6 above (mod n).

3.) Let $A = \{1, 2, 3, 4\}$ and
$R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)\}$.

If two objects in the set A are related by an equivalence relation, it generally means that they have certain properties in common.

Given $a \in A$ and an equivalence relation R on A, it is natural to consider all members of A which have a given common property. The remainder of this lecture is devoted to considering such subsets of A.

$\boxed{\textit{Definition 3.}}$ If A is a set, $a \in A$, and R is an equivalence relation on A, then the equivalence class of a, written $[a]$, is the set of all $x \in A$ such that $x \sim a$.

If C is an equivalence class for R and $x \in C$, then one frequently says that x is a representative for the equivalence class C.

Since equivalence classes for R are subsets of A, we have the following elementary observation.

Remark. If A is a set and R is an equivalence relation on A, then the collection of all $R-$ equivalence classes is a set.

The equivalence classes of an equivalence relation have the following fundamentally important property:

Theorem 1.

Let A be a set, suppose that $x, y \in A$, and let R be an equivalence relation on A. Then either the equivalence classes $[x]$ and $[y]$ are disjoint or they are equal.

Proof.Suppose that the equivalence classes in question are not disjoint, and let z belong to both of them. Then we have $x \sim z$ and $y \sim z$. By symmetry, the second of these implies $z \sim y$, and one can combine the latter with $x \sim z$ and transitivity to conclude that $x \sim y$. ■

Corollary 2.

The equivalence classes of an equivalence relation on A form a family of pairwise disjoint subsets whose union is all of A.

Definition 4.

Let $\sim$ be an equivalence relation on a set A. The quotient set, denoted $A/\sim$, is the set of all $\sim$ $-$equivalence classes - i.e., $A/\sim = \{[x] \mid x \in A\}$. The map $\pi : A \to A/\sim$ given by $\pi(x) = [x]$ is called quotient projection.

Examples.

1.) Consider again in $\mathbb{Z}$, congruence modulo $n \in \mathbb{Z}$. We have that the congruence class of each $a \in \mathbb{Z}$ is simply $a + n\mathbb{Z} = \{a + nk | k \in \mathbb{Z}\}$. The quotient set, denoted by $\{\mathbb{Z}/n\mathbb{Z}$, is the set $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1)\mathbb{Z}\}$

2.) $A = [0,1)$, consider again the binary relation $a \sim b$ if and only if $a - b$ is an integer. Then $A/\sim = \{a + \mathbb{Z} \mid a \in [0,1)\}$

3.) Let K be a field, V be a $K-$vector space, and W be a subspace of V. Let's say that two vectors $v \sim v' \in V$ are congruent modulo W, if $v - v' \in W$. Then $V/\sim$, usually denoted as V/W, is $\{v + W \mid v \in V\}$. V/W is called the quotient space.

A converse to the preceding corollary also plays an important role in the study of equivalence relations:

Proposition 3.

Let A be a set, and let $\mathcal{C} = (C_i)_{i\in I}$ be a family of subsets of A such that
(i) the subsets in $\mathcal{C}$ are pairwise disjoint
(ii) the union of the subsets in $\mathcal{C}$ is equal to A
Then there is an equivalence relation $\sim$ on A whose equivalence classes are the sets in the family $\mathcal{C}$. In other words, $A/\sim = \mathcal{C}$.

Proof. Let $x \sim y$ if there is $i \in I$ such that $x, y \in C_i$. This $\sim$ is reflexive because each $x \in A$ is in some C_i. It is symmetric because $x \sim y$ says that x and y are in some C_i, so y and x are in this same C_i, leading to $y \sim x$. Finally, it is transitive because if $x \sim y$ and $y \sim z$, there are $i, j \in I$ with $x, y \in C_i$ and $y, z \in C_j$ - in particular $y \in C_i \cap C_j$ means that $C_i = C_j$, so that $x, z \in C_i$ leads to $x \sim z$. The rest is clear. ■

Proposition 4.

Let A be a set equipped with a equivalence relation $\sim$, B be a second set, and $f : A \to B$. If f is constant along equivalence classes of $\sim$, there is a unique function $\tilde{f} : A/\sim \to B$ such that $\tilde{f} \circ \pi = f$, where π is the quotient projection. In particular, we have the equality $Im(f) = Im(\tilde{f})$ between images.

Proof. Define $\tilde{f}([x]) = f(x)$. This is well-defined as we assume that f is constant along equivalence classes of $\sim$, and it satisfies $\tilde{f} \circ \pi = f$ by construction. Such relation implies that $Im(f) = Im(\tilde{f})$ since π is surjective.■

Corollary 5.

Let A and B be sets and $f : A \to B$ be a function. If $\sim$ is defined via f (i.e., $x \sim y$ iff $f(x) = f(y)$), then there is a unique injective function $f : A/\sim \to B$ such that $\tilde{f} \circ \pi = f$, where is the quotient projection. In particular, we have the equality $Im(f) = Im(\tilde{f})$.

Remark. When f is surjective, this establishes that $A/\sim$ is in bijection with B.

Proof. The function $\tilde{f}$ exists and is unique in view of the previous theorem because f is constant on the equivalence classes of $\sim$, by definition of the latter. If we start from $\tilde{f}([x]) = \tilde{f}([y])$, then $f(x) = f(y)$, which means that $x \sim y$, so $[x] = [y]$. Hence $\tilde{f}$ is injective. ∎

Additional examples.

1.) $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, where $(m_1, n_1) \sim (m_2, n_2)$ iff $m_1 + n_2 = m_2 + n_1$

2.) $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N} \setminus \{0\})/\sim$, where $(m_1, n_1) \sim (m_2, n_2)$ iff $m_1 n_2 = m_2 n_1$

Definition 5.

(i) A relation $\preceq$ on a set X is called a partial order, if it is reflexive, antisymmetric (i.e., if $a \preceq b$ and $b \preceq a$, then $a = b$), and transitive.

(ii) A relation $\prec$ on a set X is called a strict partial order, if it is irreflexive (NOT $a \prec a$), asymmetric (i.e., if $a \prec b$ then not $b \prec a$), and transitive.

A set X together with a partial ordering $\preceq$ is called a partially ordered set, or poset, and is denoted by $(X, \preceq)$.

Examples.

1.) $(\mathbb{N}, <), (\mathbb{Q}, <), (\mathbb{R}, <), (\mathcal{P}(X), \subsetneq)$ - strict partial orders.

2.) $(\mathbb{N}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq), (\mathcal{P}(X), \subseteq)$ - partial orders.

Definition 6.

- The elements a and b of a poset $(X, \preceq)$ are comparable if either $a \preceq b$ or $b \preceq a$ holds. When a and b are elements of X so that neither $a \preceq$ nor $b \preceq a$ holds, then a and b are called incomparable.
- If any two elements of X are comparable, then X is called a linearly ordered set (the term chain are also used).

Examples.

(i) $(\mathbb{Z}, \leq)$ is a linearly ordered set.

(ii) $(\mathbb{Z}, |)$ is a partially ordered but not linearly ordered set.

Definition 7. Given two partially ordered sets $(X_1, \preceq_1)$ and $(X_2, \preceq_2)$, the lexicographic ordering on $X_1 \times X_2$ is defined by specifying when (a_1, a_2) is less than (b_1, b_2), written, $(a_1, a_2) \prec (b_1, b_2)$, which holds either if $a_1 \prec_1 b_1$ or if $a_1 = b_1$ and $a_2 \prec_1 b_2$ holds.

This definition can be easily extended to a lexicographic ordering on strings.

Example. Consider strings of lowercase English letters. A lexicographic ordering can be defined using the ordering of the letters in the alphabet. This is the same ordering as that used in dictionaries.

discreet $\prec$ discrete, because these strings differ in the seventh position and $e \prec t$.

discreet $\prec$ discreetness, because the first eight letters agree, but the second string is longer.

Definition 8.

Let A be a poset.

- We say that an element $a \in A$ is a least element of A if $a \preceq b$ for all $b \in A$.
- We say that a is a minimal element of A if $b \preceq a$ implies $b = a$.
- We say that $a \in A$ is a greatest element if $b \preceq a$ for all $b \in A$.
- We say that $a \in A$ is a maximal element if $a \preceq b$ implies $b = a$.

Let A be a poset. If A has a least element a, then a is unique, and is also a minimal element of A. However, the converse fails: a minimal element of A is generally not a least element of A, and a poset A can have many minimal elements (in which case none of them can be least elements).

Example. Let A be an arbitrary set. For $a, b \in A$, write $a \leq b$ if $a = b$. Then $\leq$ is a partial ordering on A, which is called the discrete ordering. Every element of A is minimal (and maximal). However, A has no least (or greatest) element unless it has only a single element.

Lemma 6.

Let A be a finite partially ordered set. If A is nonempty, then A has at least one minimal element.

Proof. Since A is nonempty, we can choose an element $a_0 \in A$. If a_0 is minimal, then we are done. Otherwise, there exists an element a_1 such that $a_1 \leq a_0$ and $a_1 \neq a_0$. If a_1 is minimal, then we are done. Otherwise we can choose an element a_2 such that $a_2 \leq a_1$ and $a_2 \neq a_1$. Proceeding in this way, we produce a sequence

$$a_0 \geq a_1 \geq a_2 \geq \dots$$

Since A is finite, this sequence must have some repeated terms: that is, we must have $a_i = a_j$ for some $j \neq i$. Without loss of generality we may assume that $j > i$. Then $a_i = a_j \leq a_{i+1}$ and $a_{i+1} \leq a_i$. Using antisymmetry we deduce that $a_{i+1} = a_i$, which contradicts our choice of a_{i+1}. ∎

Remark. If A is a linearly ordered set, then every minimal element of A is a least element of A. Using Lemma 6, we deduce that if A is finite and nonempty, then it contains a least element. The same argument shows that A has a greatest element.

Proposition 7.

Let A be a finite linearly ordered set. Then there is a unique order-preserving bijection $\epsilon : \{1, 2, \ldots, n\} \to A$, for some $n \in \mathbb{N}$.

Proof. Take n to be the number of elements of A, and work by induction on n. If $n > 0$, then A has a greatest element a by the Remark above, and the bijection ϵ must clearly satisfy $\epsilon(n) = a$. Now apply the inductive hypothesis to the set $A \setminus \{a\}$. ■

Proposition 8.

Let A be a partially ordered set. Then A is isomorphic (as a partially ordered set) to a subset of $\mathcal{P}(X)$, for some set X.

Proof. For each $a \in A$, let $A_{\leq a} = \{b \in A : b \leq a\}$. The construction $a \mapsto A_{\leq a}$ determines a map $\phi : A \to \mathcal{P}(A)$. We claim that ϕ is an isomorphism of partially ordered sets from A onto a subset of $\mathcal{P}(A)$. In other words, we claim that :
(i) The map ϕ is injective.
(ii) For $a, b \in A$, we have $a \leq b$ if and only if $\phi(a) \subseteq \phi(b)$.
Note that (i) is just a special case of (ii): if (ii) is satisfied and $\phi(a) = \phi(b)$, then $a \leq b$ and $b \leq a$ so that $a = b$ by antisymmetry.
To prove (ii), we first note that if $aleqb$ and $c \in A_{\leq a}$, then $c \leq a$. By transitivity we get $c \leq b$ so that $c \in A_{\leq b}$. This proves that $\phi(a) \subseteq \phi(b)$.
Conversely, suppose that $a, b \in A$ are arbitrary and that $A_{\leq a} \subseteq A_{\leq b}$. Since $a \in A_{\leq a}$, we deduce that $a \in A_{\leq b}$, which means that $a \leq b$. ■

Definition 9. Let $(A, \preceq_A)$ and $(B, \preceq_B)$ be posets. We say that a map $\phi : A \to B$ is order-preserving, or monotone, if $a \preceq_A a'$ implies $\phi(a) \preceq_B \phi(a')$.

Proposition 9.

Let A be a finite poset. Then there exists an order-preserving bijection $\phi : A \to B$, where B is a linearly ordered set.

Proof. Let $n = |A|$, and proceed by induction on n. The case $n = 0$ is trivial. Assume therefore that $n > 0$, so that A is nonempty. Let $a \in A$ be a maximal element (guaranteed by Lemma 6). The inductive hypothesis (together with Proposition 7) imply that there exists an order-preserving bijection $\epsilon : A \setminus \{a\} \to \{1, 2, \ldots, n-1\}$. We now extend ϵ to a map $\phi : A \to \{1, \ldots, n\}$ by setting $\phi(a) = n$. Since a was chosen maximal, this map is order-preserving. ■

Axiom of Choice, Zorn's Lemma and the Well-ordering Principle

Axiom of Choice A choice function on a set X is a function $f : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ such that $f(S) \in S$ for every non-empty $S \subset X$. The **Axiom of Choice** asserts that on every set there is a choice function.

Informally, the axiom of choice says that it is possible to choose an element from every set.

We say that an element u is an upper bound for a linearly ordered C if $x \preceq u$ for each $x \in C$.

Zorn's lemma asserts that if P is a non-empty poset in which each chain has an upper bound, then P has a maximal element.

Well-ordering principle A linearly ordered P is called **well-ordered** if every non-empty subset $S \subset P$ has a minimum. The well-ordering principle asserts that every set can be well-ordered by a suitable relation.

Theorem 10.

Zorn's lemma implies Axiom of Choice.

Proof. Let X be any non-empty set. Aided by Zorn's lemma, we will construct a choice function on X. Consider pairs (Y, f) consisting of a subset $Y \subseteq X$ and a choice function f on Y. We introduce a partial order on the set of all such pairs by defining $(Y, f) \preceq (Y', f')$ whenever $Y \subseteq Y'$ and $f = f`|_Y$.

The poset is non-empty because for every $x \in X$, there is an (obvious) partial choice function on $\{x\}$. If C is alinearly subset in this poset, then we can define $\tilde{Y} = \bigcup_{(Y,f) \in C} Y$ and $\tilde{f}(S) = f(S)$ for any S such that f is defined on S. Then $(\tilde{Y}, \tilde{f})$ is an upper bound for C.

Hence, by Zorn's lemma there is some maximal element, which we call (Y, f). If $x \in X \setminus Y$, then we can extend f from Y to $Y \cup \{x\}$ by defining $f(S)$ to be equal to x for any S containing x. This contradicts maximality, and so $X \setminus Y = \varnothing$, and so f is a choice function for X. ■

Theorem 11.

Zorn's lemma implies well-ordering principle.

Proof. We may assume that the set X is non-empty, for the empty set is trivially well-ordered.
An initial segment of a linearly ordered C is linearly ordered subset C' such that $x \in C$, $y \in C'$ and $x \prec y$ imply that $x \in C'$.
Consider pairs $(Y, \leq_Y)$, consisting of a subset $Y \subseteq X$ and a well-ordering $\leq_Y$ on Y. We define a partial order on the set of all such pairs in the similar manner to the preceding proof. Namely, $(Y, \leq_Y) \preceq (Y', \leq_{Y'})$ whenever $Y \subseteq Y'$, the set Y is an initial segment of Y' in $\leq_{Y'}$, and the two orderings $\leq_Y$ and $\leq_{Y'}$ agree on the set Y.

Since X is non-empty, the poset is non-empty. Furthermore, if C is a linearly ordered in this poset, we can define $\tilde{Y} = \bigcup_{(Y,f)\in C} Y$ and $x \leq_{\tilde{Y}} y$ whenever $x \leq_Y y$ for some $(Y, \leq_Y) \in C$. Then $\leq_{\tilde{Y}}$ is a well-ordering on $\tilde{Y}$. Indeed, suppose that a set $S \subseteq \tilde{Y}$ is non-empty and $(Y, \leq_Y) \in C$ is any pair in the chain such that $S \cap Y \neq \varnothing$. Let $u = min_{\leq_Y}(S \cap Y)$, where the minimum is with respect to $\leq_Y$. Then u is a minimum for S with respect to $\leq_{\tilde{Y}}$, for if $s \in S$ is arbitrary, then either $s \in Y$ in which case $u \leq_{\tilde{Y}} s$ follows from $u \leq_Y s$, or $s \notin Y$, in which case $u \leq_{\tilde{Y}} s$ follows from the fact that Y is an initial segment of $\tilde{Y}$. Hence, the pair $(\tilde{Y}, \leq_{\tilde{Y}})$ is an upper bound for C.

So, by Zorn's lemma the poset contains a maximal element $(Y, \leq_Y)$. If $Y \neq X$ and $x \in X \setminus Y$, then we can extend $(Y, \leq_Y)$ to a set $Y \cup \{x\}$ by defining x to be greater than every element of Y. This contradicts maximality, and so $Y = X$, i.e., X can be well-ordered. ■

Theorem 12.

Well-ordering principle implies Axiom of Choice.

Proof. Suppose X is a set, and $\leq$ is a well-ordering of X. Then $f(S) = min\ S$ defines a choice function on X. ■

Theorem 13.

Axiom of Choice implies Zorn's Lemma.

Proof. Let P be any non-empty poset such that every chain has an upper bound. Assume for contradiction's sake that P has no maximal element. Let f be a choice function on P , and let $x_0 = f(P)$. If C is chain, let $Upp(C) = \{u \notin C \mid \forall x \in C, x \prec u\}$ be set of all strict upper bounds for C.

Observation 1. For any chain C, the set $Upp(C)$ is non-empty: Let u be an upper bound for C (which exists by the assumption on P). If C has no maximum element, then $u \notin C$, and so $u \in Upp(C)$. Suppose next that C contain a maximum element, which we call m. Since P has no maximal element, there is u that is greater than m. Then $x \preceq m \prec u$ for each $x \in C$, and so $u \in Upp(C)$.

For any chain C, let $g(C) = f(Upp(C))$.
For purpose of this proof, an attempt is a well-ordered set $A \subset P$ satisfying the following:
(i) $min\ A = x_0$
(ii) For every proper initial segment $C \subset A$, we have $min\ A \setminus C = g(C)$.

Observation 2. If A and A' are two attempts, then either $A \subseteq A'$ or $A' \subseteq A$: Suppose the opposite, and let $z = min\ A \setminus A'$ and $z' = min\ A' \setminus A$. These are well-defined since A and A' are well-ordered, respectively. Since $z \neq z'$, we cannot have both $z \preceq z'$ and $z' \preceq z$. Without loss of generality, suppose $z' \npreceq z$. Let $C = \{x \in A | x \prec z\}$. From the definition of z it follows that $C \subseteq A'$. It is clear that $z = min\ A \setminus C$, and so $z = g(C)$.
If $C = A'$, then $A' \subset A$, and we are done. So, suppose that $C \neq A'$. If $z' \preceq x$ for some $x \in C$, then transitivity would have implied that $z' \prec z$, contrary to our assumption. So, since A' is chain, $x \preceq z'$ for every $x \in C$. Therefore C is a proper initial segment of A', and so $g(C) \in A'$. However, $g(C) = z \notin A'$. The contradiction completes the proof.$\blacksquare$

A consequence of the preceding Observation is that union of any set of attempts is an attempt. So, let $\mathcal{A}$ be the set of all attempts, and put $B = \cup_{A \in \mathcal{A}} A$. Then B is an attempt. However, $B \cup \{g(B)\}$ is an attempt that contains B. The contradiction shows P does have a maximal element after all. ■

Remark. It follows from the Axiom of choice that the result of Proposition 9 is also true for the infinite set A.

Exercises

It would be good to solve them by the next lecture (Nevertheless, we will cover these exercises next time.)

Exercises.

1.) Given the relation

the relation is reflexive

$$\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(3,4),(4,3)\}$$

is an equivalence relation on $\{1,2,3,4\}$, find [3] (the equivalence class containing 3). How many distinct equivalence classes are there?

2.) Give an example of a relation on $\{1,2,3,4\}$ that is reflexive, not antisymmetric, and not transitive. $(1,2).(2,3) \in R$. $(1,3) \notin R$.

3.) Find the equivalence relation (as a set of ordered pairs) on $\{a,b,c,d,e\}$, whose equivalence classes are $\{a\},\{b,d,e\},\{c\}$.

4.) Give an example of a set bounded from above that has no greatest element.

5.) Let $S = \{x \in \mathbb{R} : x^2 \leq (\sqrt{2}+1)x - \sqrt{2})\}$, and $T = S \setminus \mathbb{Q}$.
- a.) S has a greatest element and S has a least element.
- b.) S is bounded above and below in $\mathbb{R}$.
- c.) T has a greatest element, and T has no least element.
- d.) T is bounded above and below in $\mathbb{R}$.

6.) Every vector space V has a basis B (Hint: Zorn's Lemma).

$\leq := \subseteq$. A - poset of linear independent subset of V.

$\exists$ maximal (set) B $V = \text{span}\langle B\rangle$

If $\text{span}\langle B\rangle \subsetneq V$. $\exists v \in V \setminus \text{span}\langle B\rangle$

$\Rightarrow$ $B \cup \{v\} \supsetneq \text{span}\langle B\rangle \Rightarrow$ Contradict with B is maximal.