CM10311

Lecture Notes 1

1. Propositions

We will be studying elements of the mathematical logic, more precisely, of *propositional calculus*. A basic concept here is a *proposition*, or a statement, which is assumed to be either **true** or **false**, but not both at the same time. In propositional calculus we are not concerned with the content of a statement but only with its true/false value. This approach is similar to the way the arithmetic treats quantities, describing them by numbers. Laws of, say, addition are indifferent to *what* is added up: apples or pounds of sterling.

2. Logical connectives

Logic studies ways of constructing complex statements from simple ones by means of operations called *logical connectives*. The most important connectives are described below. Since we are interested only in true/false values of statements, to define an operation means just to state which of these two values the result of operation obtains depending on values of operands.

In what follows, the value **true** (resp. **false**) will be abbreviated to **t** (resp. **f**).

Conjunction (logical **and**). Let x and y be propositions. *Conjunction* of x and y is the proposition denoted by $x \wedge y$ and defined by the following table.

x	y	$x \wedge y$
t	**t**	**t**
t	**f**	**f**
f	**t**	**f**
f	**f**	**f**

From the table we see that *a conjunction of two propositions is* **true** *if and only if each of these propositions is* **true**.

Disjunction (logical **or**). Let x and y be propositions. *Disjunction* of x and y is the proposition denoted by $x \vee y$ and defined by the following table.

x	y	$x \vee y$
t	**t**	**t**
t	**f**	**t**
f	**t**	**t**
f	**f**	**f**

From the table we see that *a disjunction of two propositions is* **false** *if and only if each of these propositions is* **false**. Note that the disjunction is "inclusive *or*". Sometimes a different connective, called XOR ("exclusive *or*"), is used. XOR differs from $\vee$ only when x and y both have value **t**, in which case the value of XOR is defined as **f**.

Implication (logical **if — then**). Let x and y be propositions. *Implication* from x to y is the proposition denoted by $x \to y$ (sometimes by $x \supset y$) and defined by the following table.

x	y	$x \to y$
t	**t**	**t**
t	**f**	**f**
f	**t**	**t**
f	**f**	**t**

If $x \to y$, then x is called the *assumption* of the implication while y is called its *consequence*. From the table we see that *an implication of two propositions is* **false** *if and only if the assumption is* **true** *while the consequence is* **false**, *in other words, if and only if* **true** *implies* **false**.

Negation (logical **not**). Let x be a proposition. *Negation* of x is the proposition denoted by $\neg x$ and defined by the following table.

x	$\neg x$
t	**f**
f	**t**

From the table we see that *the negation of a proposition is* **true** *if and only if the proposition is* **false**.

3. Boolean formulae

Recall that passing to from primary school mathematics to algebra involves replacing concrete numbers by letters in order to be able to formulate mathematical laws or theorems in their general forms. These letters are called *variables* standing for numbers. Similar reasons lead us to introducing variables standing for propositions. From variables, logical connectives and parenthesis we can construct *Boolean* or *propositional formulae*.

Definition *Let symbols $X_1, \ldots, X_n$ be variables. Boolean formula is a string of symbols from the set*

$$\{X_1, \ldots, X_n, \wedge, \vee, \to, \neg, (,)\}$$

which is organized as follows.
(1) Any variable X_i, $(1 \leq i \leq n)$ is a Boolean formula.
(2) If F and G are two Boolean formulae, then expressions $(F \wedge G)$, $(F \vee G)$, $(F \to G)$ and $\neg F$ are Boolean formulae.

We usually drop the most external parenthesis in a Boolean formula.

Example The following string *is* a Boolean formula:

$$(X \to \neg Y) \vee (\neg Z \wedge Y),$$

while the next one is not:

$$(X \to))$$

(a consequence in the implication is missing, parenthesis unbalanced).

By assigning concrete true/false values to variables in a Boolean formula F and using defining tables for connectives one can compute the concrete true/false value of F. This is like assigning numerical values to variables a, b in the expression $a + b$ and getting the corresponding numerical value of the sum.

Example Assign the following values to variables:

$$\begin{array}{ll} X & \mathbf{t} \\ Y & \mathbf{t} \\ Z & \mathbf{f} \end{array}$$

Then the value of the formula

$$(X \to \neg Y) \vee (\neg Z \wedge Y)$$

becomes $\mathbf{t}$. On the other hand, for the assignment

$$\begin{array}{ll} X & \mathbf{t} \\ Y & \mathbf{t} \\ Z & \mathbf{t} \end{array}$$

the value of that formula is $\mathbf{f}$.

4. Tautologies

Definition *A Boolean formula F with variables $X_1, \ldots, X_n$ is called* identically true *or* tautology *if for* any *assignment of true/false values to variables the value of F is* $\mathbf{t}$.

Examples The following Boolean formulae are tautologies (very useful in everyday mathematical reasoning).

$$X \vee \neg X$$

$$\neg\neg X \to X$$

$$X \to \neg\neg X$$

$$\neg(X \wedge \neg X)$$

$$((\neg X \to Y) \wedge (\neg X \to \neg Y)) \to X.$$

Clearly, one can generate many other tautologies by replacing variables in these formulae by arbitrary Boolean formulae.

It is convenient to use the abbreviation $F \equiv G$ for the Boolean formula $(F \to G) \wedge (G \to F)$, where F and G are some Boolean formulae. It is easy to see that $F \equiv G$ has value $\mathbf{t}$ if and only if F and G have the same truth value (i.e., either both have value $\mathbf{t}$ or both have value $\mathbf{f}$). Thus, the second and the third formulae in the previous example can be combined in a single tautology

$$\neg\neg X \equiv X.$$

CM10311

Lecture Notes 2

1. Commutative laws

Commutative law for conjunction. *Let x, y be propositions. Then $x \wedge y$ is true if and only if $y \wedge x$.*

Equivalent formulation. *For variables X, Y the Boolean formula*

$$(X \wedge Y) \equiv (Y \wedge X)$$

is identically true.

Proof. Straightforward check of tables defining $\wedge$ and $\equiv$.

Commutative law for disjunction. *Let x, y be propositions. Then $x \vee y$ is true if and only if $y \vee x$.*

Equivalent formulation. *For variables X, Y the Boolean formula*

$$(X \vee Y) \equiv (Y \vee X)$$

is identically true.

Proof. Straightforward check of tables defining $\vee$ and $\equiv$.

2. Associative laws

In what follows we will formulate each law only in a form of identically true Boolean formula.

Associative law for conjunction. *For variables X, Y, Z the Boolean formula*

$$((X \wedge Y) \wedge Z) \equiv (X \wedge (Y \wedge Z))$$

is identically true.

Associative law for disjunction. *For variables X, Y, Z the Boolean formula*

$$((X \vee Y) \vee Z) \equiv (X \vee (Y \vee Z))$$

is identically true.

Proof. Straightforward check of tables.

3. Distributive laws

Conjunction over disjunction. *For variables X, Y, Z the Boolean formula*

$$(X \wedge (Y \vee Z)) \equiv ((X \wedge Y) \vee (X \wedge Z))$$

is identically true.

Disjunction over conjunction. *For variables X, Y, Z the Boolean formula*

$$(X \vee (Y \wedge Z)) \equiv ((X \vee Y) \wedge (X \vee Z))$$

is identically true.

Proof. Straightforward check of tables.

4. De Morgan's laws

For variables X, Y, Z the Boolean formulae

$$\neg(X \wedge Y) \equiv (\neg X \vee \neg Y),$$

$$\neg(X \vee Y) \equiv (\neg X \wedge \neg Y).$$

are identically true.

Proof. Straightforward check of tables.

5. Some other laws of logic

(i) $\neg\neg X \equiv X$;
(ii) $(X \to Y) \equiv (\neg X \vee Y)$.

Observe that De Morgan's laws combined with (i) allow to express $\wedge$ via $\vee$ and vice versa. For example, (i) implies that a disjunction $Y \vee Z$, where Y, Z are variables, can be replaced by an equivalent formula $\neg(\neg(Y \vee Z))$, which in turn, by the first of De Morgan's laws is equivalent to $\neg(\neg Y \wedge \neg Z)$.

Also, (ii) provides a way of replacing $\to$ by $\vee$ and vice versa.

It follows that *every Boolean formula is equivalent to a formula having only one of the following pairs of connectives:*

(a) $\neg$, $\wedge$ *or*
(b) $\neg$, $\vee$ *or*
(c) $\neg$, $\to$.

6. Reductio ad absurdum. Direct and inverse theorems

The tautology

$$((\neg X \to Y) \wedge (\neg X \to \neg Y)) \to X$$

(formula (iv) from Section 5) is often used for proving mathematical statements by "leading to contradiction". To prove a proposition x it's sufficient to assume the negation $\neg x$ of x and deduce from $\neg x$ two contradictory statements, say, y and $\neg y$. The the above tautology implies that x is true.

Many mathematical theorems can be formally described by as implications $x \to y$. Call this implication *direct theorem.* Then the proposition $y \to x$ is known as *inverse*

theorem. Even if the direct theorem is true, the inverse may or may not be true. The proposition $\neg x \to \neg y$ is called *opposite theorem*. The proposition $\neg y \to \neg x$ is, therefore, *opposite to inverse theorem*. Observe, that an opposite to inverse theorem is true if and only if the direct theorem is true, because of the tautology

$$(X \to Y) \equiv (\neg Y \to \neg X).$$

In some cases it's easier to prove opposite to inverse theorem than the direct theorem.

If a theorem has a structure of an implication $x \to y$, then x is called the *sufficient condition* of the theorem, while y is its *necessary condition*. If a theorem has a form "x is necessary and sufficient for y" it means that two statements are true at the same time: $x \to y$ and $y \to x$.

7. Disjunctive normal form of a Boolean formula

Let $X_1, X_2, \ldots, X_n$ be variables. Y_i is called a *literal* if Y_i is either X_i or $\neg X_i$ for any i.

A *conjunctive term* is a conjunction of the kind $Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_m}$, where i_j is one of the numbers $1, 2, \ldots, n$ for $1 \leq j \leq m$, and each Y_{i_j} is a literal.

Definition *A Boolean formula F is in* disjunctive normal form (DNF) *if F is of the form*

$$F_1 \vee F_2 \vee \cdots \vee F_k,$$

where F_i is a conjunctive term for any i.

Theorem *For each Boolean formula G with variables $X_1, X_2, \ldots, X_n$ there exists a Boolean formula F in DNF, with variables from $\{X_1, X_2, \ldots, X_n\}$, such that $G \equiv F$.*

We don't prove this theorem in this course.

Examples

(1) Let G be the formula $X \to Y$. From (ii), Section 5 it follows that $G \equiv \neg X \vee Y$. The righthand side of the latter equivalence is a formula in disjunctive normal form with conjunctive terms $\neg X$ and Y.

(2) Let G be the formula

$$((\neg X \to Y) \wedge (\neg X \to \neg Y)) \to X.$$

Using again (ii), Section 5 and De Morgan's laws we can write a following string of equivalent formulae:

$((\neg X \to Y) \wedge (\neg X \to \neg Y)) \to X$
$\neg((X \vee Y) \wedge (X \vee \neg Y)) \vee X$
$\neg(X \vee Y) \vee \neg(X \vee \neg Y) \vee X$
$(\neg X \wedge \neg Y) \vee (\neg X \wedge Y) \vee X.$

The last formula in this list is equivalent to G and is in DNF.

8. Conjunctive normal form of a Boolean formula

Conjunctive normal form (CNF) of a Boolean formula is a representation dual to its representation in DNF.

A *disjunctive term* (or *clause*) is a disjunction of the kind $Y_{i_1} \vee Y_{i_2} \vee \cdots \vee Y_{i_m}$ where i_j is one of the numbers $1, 2, \ldots, n$ for $1 \leq j \leq m$.

Definition *A Boolean formula F is in* conjunctive normal form (CNF) *if F is of the form*

$$F_1 \wedge F_2 \wedge \cdots \wedge F_k,$$

where F_i is a disjunctive term for any i.

Theorem *For each Boolean formula G with variables $X_1, X_2, \ldots, X_n$ there exists a Boolean formula F in CNF, with variables from $\{X_1, X_2, \ldots, X_n\}$, such that $G \equiv F$.*

We don't prove this theorem.

CM10311

Lecture Notes 3

1. Sets

The concept of a *set* is so basic that it's hard to define it in a way different from just listing synonyms: *collection, family, totality.* A set consists of elements, e.g. the set of all students in this class, a set of all integer numbers.

A set containing a finite number of elements (possibly zero) is called *finite*. If that number is small, a usual way to describe a set is by listing all its elements in braces. For example,

$$S = \{a, b, c\}$$

is a set S consisting of elements a, b, and c. If the number of elements in a set S is large or infinite we describe this set by the property which is satisfied exactly by elements of S. For example,

$$\mathbf{Z} = \{x |\ x \text{ is an integer number}\}.$$

Here the symbol | is read "such that".

To express the fact that an element a belongs to a set S, we write $a \in S$. If an element z is not in S, we write $z \notin S$.

An important set is the *empty set*, containing no elements, denoted by $\emptyset$. So, $\emptyset = \{\ \}$.

2. Universal quantifier

Consider the following proposition:

For all numbers x from the set $A = \{-1, 0, 1\}$ the inequality $x + 1 > x$ is true.

Note it contains the construction *"For all ..."*. We can rewrite the proposition using just conjunctions:

$$(-1 + 1 > -1) \wedge (0 + 1 > 0) \wedge (1 + 1 > 1).$$

A larger set A would lead to a longer conjunction. On the other hand, the proposition makes sense also for infinite sets A, for example for the set $\mathbf{Z}$ of all integer numbers. In the latter case, we are unable to express it in a finite form just by using logical connectives. This prompts us to extend the language of logic by adding *quantifiers*. Now the original proposition obtains the form $\forall x \in \{-1, 0, 1\}(x + 1 > x)$ for the small set, and of the form $\forall x \in \mathbf{Z}(x + 1 > x)$ for the set of all integers. Here the symbol $\forall$ is called the *universal quantifier*. The expression $x+1 > x$ is an example of a *predicate*, the "variable" proposition depending on one or more variables whose values belong to a set. Replacing variables in a predicate by specific elements of that set turns the predicate into a proposition. Likewise, placing $\forall x$ in front of a predicate depending on x turns it into a proposition.

Example.
"Person x is intelligent"

is a predicate.

"$\forall x \in$ (set of all Bath students) (person x is intelligent)"

is a proposition.

3. Existential quantifier

Consider a following proposition.

There exists a number x from the set $A = \{-1, 0, 1\}$ such that $x \leq 0$.

We can rewrite the proposition using disjunctions:

$$(-1 \leq 0) \vee (0 \leq 0) \vee (1 \leq 0).$$

As in the case of the universal quantifier, a larger set A would lead to a larger disjunction. For infinite sets, like $\mathbf{Z}$, interpretation of this proposition as a disjunction is not possible. Instead, we write it in the following form:

$$\exists x \in A(x \leq 0),$$

where the symbol $\exists$ is the *existential quantifier*. As with the universal quantifier, adding $\exists x$ to a predicate depending on a variable x turns this predicate into a proposition.

Example.
"$\exists x \in$ (set of all Bath students) (person x is intelligent)"

is a proposition.

4. $\forall$ and $\exists$ in the same formula

If a predicate contains several variables, it can be reduced to a proposition by adding the same number of quantifiers.

Example. Formula

$$\forall x \in \{-1, 0, 1\} \exists y \in \{-1, 0, 1\}(x + y = 0)$$

describes the same proposition as

$$((-1 + (-1) = 0) \vee (-1 + 0 = 0) \vee (-1 + 1 = 0)) \wedge$$

$$\wedge((0 + (-1) = 0 \vee (0 + 0 = 0) \vee (0 + 1 = 0)) \wedge$$

$$\wedge((1 + (-1) = 0) \vee (1 + 0 = 0) \vee (1 + 1 = 0)).$$

Note that $\exists y \in \{-1, 0, 1\}(x + y = 0)$ is a predicate, not a proposition.

5. Negation of quantifiers

Laws for negation of quantifiers are generalizations of De Morgan's laws. For example,

$$\neg(\forall x \in \{-1, 0, 1\}(x + 1 > x))$$

can be rewritten in the form:

$$\neg((-1 + 1 > -1) \wedge (0 + 1 > 0) \wedge (1 + 1 > 1)).$$

By De Morgan's law, the latter proposition is equivalent to

$$\neg(-1 + 1 > -1) \vee \neg(0 + 1 > 0) \vee \neg(1 + 1 > 1)$$

which is the same as

$$(-1 + 1 \leq -1) \vee (0 + 1 \leq 0) \vee (1 + 1 \leq 1).$$

But, by the definition of $\exists$, the last formula is exactly

$$\exists x \in \{-1, 0, 1\}(x + 1 \leq x).$$

General rule: Let M be a set and $P(x)$ be a predicate Then

$$(\neg\forall x \in M\ P(x)) \equiv (\exists x \in M\ (\neg P(x))),$$

$$(\neg\exists x \in M\ P(x)) \equiv (\forall x \in M\ (\neg P(x))).$$

Examples.

$$(\neg\forall x \in \mathbf{Z}\ (x + 1 > x)) \equiv (\exists x \in \mathbf{Z}\ (x + 1 \leq x)),$$

$$(\neg\exists x \in \mathbf{Z}\ (x < 0)) \equiv (\forall x \in \mathbf{Z}\ (x \geq 0)).$$

$$(\neg\forall x \in M\ \exists y \in N\ P(x, y)) \equiv (\exists x \in M\ \neg(\exists y \in N\ P(x, y))) \equiv (\exists x \in M\ \forall y \in N\ \neg P(x, y)).$$

CM10311

Lecture Notes 4

1. Equal sets, subsets

Two sets A and B are called *equal*, and we write $A = B$, if they consist of the same elements. Let us formulate this in a slightly different way.

Definition. *A set A is a subset of a set B (notation: $A \subset B$), if every element from A is also an element of B, i.e. $\forall x \in A(x \in B)$.*

Definition. *Two sets A and B are equal (notation: $A = B$), if $(A \subset B) \wedge (B \subset A)$.*

For each particular application of the set theory, is convenient to consider all sets occurring in this application as subsets of one large set U, called the *universe*. The precise nature of the universe depends on the context. If $A \subset U$ and $B \subset U$, then obviously $A \subset B$ if and only if

$$\forall x \in U((x \in A) \to (x \in B)). \tag{1}$$

Note, that $A \subset A$ and $\emptyset \subset A$ for any set A. Also, for any three sets A, B and C, if $A \subset B$ and $B \subset C$, then $A \subset C$ (*transitivity* of $\subset$).

2. Union of sets

Definition. *For two sets A and B, the set $A \cup B = \{x | \, (x \in A) \vee (x \in B)\}$ is called their union.*

Examples.

(1) Let E denote the set of all even integer numbers and O denote the set of all odd numbers. Then $E \cup O = \mathbf{Z}$.

(2) Recall that a number $n \in \mathbf{Z}$, such that $n > 1$, is called *prime* if its only positive divisors are 1 and n itself. Let P denote the set of all prime numbers. Then $O \cup P = O \cup \{2\}$.

3. Intersection of sets

Definition. *For two sets A and B, the set $A \cap B = \{x | \, (x \in A) \wedge (x \in B)\}$ is called their intersection.*

Examples.

(1) $E \cap O = \emptyset$.

(2) $E \cap \mathbf{Z} = E$.

(3) Let A be the set of all dog owners, B be the set of all cat owners, then $A \cap B$ is the set of all people owning a cat and a dog. $A \cup B$ is the set of all people owning either a cat or a dog or both.

4. Properties of $\cup$ and $\cap$

Commutative laws

For union: $A \cup B = B \cup A$.

Proof. Because $\vee$ is commutative, we have, $A \cup B = \{x|\ (x \in A) \vee (x \in B)\} = \{x|\ (x \in B) \vee (x \in A)\} = B \cup A$.

For intersection: $A \cap B = B \cap A$.

Proof. Follows from commutativity of $\wedge$.

Associative laws

For union: $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof. Follows from associativity of $\vee$.

For intersection: $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof. Follows from associativity of $\wedge$.

Distributive laws

Intersection over union: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Union over intersection: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. Follows from distributive laws for conjunction and disjunction.

5. Difference of sets

Definition. *For two sets A and B, the set $A \setminus B = \{x|\ (x \in A) \wedge (x \notin B)\}$ is called difference of A and B.*

Suppose again that sets A, B, C, etc., are subsets of the universe U. Then $U \setminus A$ has a special name, it's called *complement* of A and denoted by A'.

Properties of the complement

$A \cap A' = \emptyset$;
$A \cup A' = U$;
De Morgan laws:
$(A \cup B)' = A' \cap B'$;
$(A \cap B)' = A' \cup B'$.

Proof of De Morgan laws.
$x \in (A \cup B)'$ is equivalent to
$x \notin A \cup B$ is equivalent to
$\neg(x \in A \cup B)$ is equivalent to
$\neg((x \in A) \vee (x \in B))$ is equivalent (by De Morgan laws in logic) to
$\neg(x \in A) \wedge \neg(x \in B)$ is equivalent to

$(x \notin A) \wedge (x \notin B)$ is equivalent to
$(x \in A') \wedge (x \in B')$ is equivalent to
$x \in A' \cap B'$.
Proof of the second law is similar.

6. Cartesian product of sets

Definition. *For two sets A and B the set $A \times B = \{(x, y) |\, (x \in A) \wedge (y \in B)\}$ is called their Cartesian product.*

Examples.

(1) If $A = \{x_1, x_2\}$, $B = \{y_1, y_2\}$, then $A \times B = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2)\}$.

(2) If $A = \{x |\, x \text{ is real number, } 0 \leq x \leq 1\}$, $B = \{x |\, x \text{ is real number, } 1 \leq x \leq 2\}$, then $A \times B$ can be represented as a rectangle on the plane with vertices in points with coordinates: $(0, 1)$, $(0, 2)$, $(1, 1)$, $(1, 2)$.

7. Sets of sets

Sets can serve as elements of other sets. For example, if we consider a tutorial group of students as a set of students, then the set of tutorial groups will become a set of sets.

Other examples:

(1) $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$;
(2) $\{\emptyset\}$ (not to confuse with $\emptyset$);
(3) $\{\emptyset, \{\emptyset\}\}$.

8. Power set

Definition. *Let A be a set. Then $\{B |\, B \subset A\}$ is called power set and denoted by 2^A.*

Examples.

(1) $2^{\emptyset} = \{\emptyset\}$;
(2) $2^{\{a\}} = \{\emptyset, \{a\}\}$;
(3) $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$;
(4) $2^{\{a,b,c\}} = 2^{\{a,b\}} \cup \{\{c\}, \{c, a\}, \{c, b\}, \{c, a, b\}\}$.

9. Cardinality

Let A be a finite set consisting of n elements. Then n is called *cardinality* of A. Notation: $n = |A|$.

In the following theorems A and B are arbitrary finite sets.

Theorem $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof. Let us count elements from A and then count elements from B. As a result, each element from $A \cup B$ will be counted at least once. Hereby, each element from $A \cap B$ will be

counted twice: once as an element from A, then as an element from B. All other elements (from $(A \cup B) \setminus (A \cap B)$) are counted exactly once each. The formula follows.

Theorem. $|A \times B| = |A||B|$.

Proof. Recall that $|A \times B|$ is the set of all pairs (x, y), where $x \in A$, $y \in B$. For each of $|A|$ elements $x \in A$ there exist exactly $|B|$ pairs of the kind (x, y) from $A \times B$. It follows that the total number of pairs (elements) in $A \times B$ is $|A||B|$.

Theorem. $|2^A| = 2^{|A|}$.

Proof. Let $A = \{a_1, \ldots, a_n\}$. For a subset B of A, there are two contrary possibilities: either $a_1 \in B$ or $a_1 \notin B$. The same is true for element a_2, hence there are $2 \times 2 = 2^2 = 4$ possibilities for inclusion/exclusion of elements a_1, a_2 in B. Continuing in this fashion, we conclude that there are $2^n = 2^{|A|}$ possibilities for inclusion/exclusion of elements $a_1, a_2, \ldots, a_n$ in B. Each of the possibilities gives a different subset B of A.

Here is a more formal (rigorous) proof, to be read after we study the method of proof by induction. Let $A_n = \{a_1, \ldots, a_n\}$, $A_{n+1} = \{a_1, \ldots, a_n, a_{n+1}\}$, so, in particular, $|A_n| = n$, $|A_{n+1}| = n + 1$. We conduct the proof by induction on n.

Base of the induction, for $n = 0$, is obvious, since from Example (1) we have $2^{|\emptyset|} = |\{\emptyset\}| = 1$.

Inductive hypothesis: $|2^{A_n}| = 2^{|A_n|} = 2^n$.

Represent $2^{A_{n+1}}$ in the form (cf. Example (4)):

$$2^{A_{n+1}} = 2^{A_n} \cup \{\{a_{n+1}\}, \{a_{n+1}, a_1\}, \ldots, \{a_{n+1}, a_n\}, \{a_{n+1}, a_1, a_2\}, \ldots, \{a_{n+1}, a_{n-1}, a_n\},$$

$$\ldots, \{a_{n+1}, a_1, \ldots, a_n\}\} = 2^{A_n} \cup \{\{a_{n+1}\} \cup X |\, X \subset A_n\}.$$

Since the sets 2^{A_n} and $\{\{a_{n+1}\} \cup X |\, X \subset A_n\}$ are disjoint (have empty intersection), the cardinality

$$|2^{A_{n+1}}| = |2^{A_n}| + |\{\{a_{n+1}\} \cup X |\, X \subset A_n\}|.$$

By *inductive hypothesis* each of two terms in the right-hand side is equal to 2^n, thus $|2^{A_{n+1}}| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} = 2^{|A_{n+1}|}$. Theorem is proved.

CM10311

Lecture Notes 5

1. Proof by induction: examples

Geometric progression. We illustrate the use of the induction method by proving the formula for the sum of *geometric progression*:

$$1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - 1}{q - 1} \tag{1}$$

for all integer $q \neq 1$ and $n \geq 0$. We will conduct induction on the parameter n.

Base. For $n = 0$ the formula (1) is true since both sides of (1) are equal to 1.

Inductive hypothesis. Assume that (1) is true.

Inductive step. We need to prove that

$$1 + q + q^2 + \cdots + q^n + q^{n+1} = \frac{q^{n+2} - 1}{q - 1}. \tag{2}$$

By inductive hypothesis, the sum of first $n + 1$ terms in the left-hand side of (2) equals to $\frac{q^{n+1}-1}{q-1}$. Therefore, the left-hand side of (2) can be re-written as

$$\frac{q^{n+1} - 1}{q - 1} + q^{n+1},$$

which, is obviously equal to right-hand side of (2). This completes the proof of (1).

Squares grow faster than linear functions. Our next example is proving the inequaluty $n + 2 \leq n^2$ for all integer numbers $n \geq 2$.

Base For $n = 2$ the inequality is obviously true.

Inductive hypothesis. Assume that $n + 2 \leq n^2$ for some $n \geq 2$.

Inductive step. We need to prove that $n + 1 + 2 \leq (n + 1)^2$. The latter is equivalent to $n^2 - (n + 2) + 2n \geq 0$. By the inductive hypothesis, $n^2 - (n + 2) \geq 0$, but obviously, $2n > 0$, hence the required inequality is true.

2. Maps

Informal Definition. *A map f from a set A to a set B is* a rule *which for every $x \in A$ determines one and only one element $y \in B$*
Notation: $f : A \to B$ (not to confuse $\to$ as a part of map's notation with the implication symbol!!).

Examples.

(1) A computer program (or an algorithm). Here A is the set of all possible inputs on which the program terminates, B is the set of all possible outputs.

(2) $f : \mathbf{Z} \to \mathbf{Z}$, such that to $x \in \mathbf{Z}$ the map f relates $x^2 \in \mathbf{Z}$. The latter condition is usually written as $x \mapsto x^2$, or as $f(x) = x^2$.

(3) Let A be a set of students taking a certain exam, B be a set of all possible marks, e.g. $B = \{0, 1, 2, \ldots, 100\}$. Then the exam is a map from A to B.

Definition. *If $f : A \to B$, then A is called the domain of f, B is called the range (or co-domain) of f. If $x \mapsto y$, then y is called the image of x, x is called the pre-image of y, x is also called the argument of f. We say that f carries x to y.*

If the range B of a map f is a set of numbers, then f is often called a *function*. However, the term *function* is also sometimes used as a synonym for *map*.

IMPORTANT! We re-iterate that the definition of the map $f : A \to B$ requires the following two conditions:

(1) every $x \in A$ is "used", i.e., x is an argument to which a certain image $y \in B$ corresponds;

(2) to every $x \in A$ corresponds *only one* image from B.

Example. Let us list all four possible maps from $A = \{x_1, x_2\}$ to $B = \{y_1, y_2\}$:
$f_1(x_1) = y_1$, $f_1(x_2) = y_2$;
$f_2(x_1) = y_2$, $f_2(x_2) = y_1$;
$f_3(x_1) = y_1$, $f_3(x_2) = y_1$;
$f_4(x_1) = y_2$, $f_4(x_2) = y_2$.

Definition. *Identity map on a set A is defined as $I_A : A \to A$ such that $x \mapsto x$.*

3. Surjective maps

Definition. *A map $f : A \to B$ is called surjective (or surjection) if*

$$\forall y \in B \exists x \in A (f(x) = y).$$

In other words, in a surjective map every element from the range has a pre-image.

Examples.

(1) The map from the set of all humans to the set of all human mothers is surjective (each mother, by the definition, has a child).

(2) The identity map is surjective.

(3) If $\mathbf{R}$ is the set of all real numbers, then $f : \mathbf{R} \to \mathbf{R}$ with $x \mapsto x^2$ is *not* surjective (e.g., -1 has no pre-image). However, over *complex* numbers $f(x) = x^2$ is surjective.

(4) $f(x) = x^3$ is surjective over real numbers.

(5) Let $f : A \to B$ be any map. Let $C \subset B$ be the set of images $f(x)$ for all $x \in A$, i.e., $C = \{f(x) \in B | x \in A\}$. Then the map $g : A \to C$, where $f(x) = g(x)$ for any $x \in A$, is surjective.

4. Injective maps

Definition. *A map $f : A \to B$ is called injective (or injection) if*

$$\forall x_1 \in A \forall x_2 \in A((x_1 \neq x_2) \to (f(x_1) \neq f(x_2)).$$

In other words, in an injective map two different arguments have two different images.

Examples.

(1) The map from the first example in Section 3 *is not* injective, since two persons may have the same mother.

(2) The identity map is injective.

(3) $f(x) = x^2$ is injective neither over real numbers, nor over complex numbers.

(4) $f(x) = 2^x$ over real numbers is injective, but not surjective (-1 has no pre-image).

5. Bijective maps and inverse maps

Definition. *A map $f : A \to B$ which is both surjective an injective is called bijective (or bijection).*

Examples.

(1) Identity map is bijective.

(2) $f(x) = x^3$ over real numbers is bijective.

(3) Correspondence between humans and their fingerprints is apparently bijective.

Definition. *Let $f : A \to B$ be a map. The map $f^{-1} : B \to A$ is called inverse to f, if $f(x) = y$ is equivalent to $f^{-1}(y) = x$.*

Theorem. *A map $f : A \to B$ has an inverse if and only if f is bijective.*

Proof. Assume that f has an inverse. Then, for any $y \in B$ there is $x \in A$ such that $x = f^{-1}(y)$, which is equivalent to $y = f(x)$. This means f is surjective. Also, there can't by two different images $x_1 = f^{-1}(y)$, $x_2 = f^{-1}(y)$ of any argument $y \in B$, which is equivalent to $y = f(x_1)$, $y = f(x_2)$. This means f is injective. We conclude that f is both surjective and injective, i.e f is bijective.

Now assume that f is bijective. Since f is surjective, the function f^{-1} can be defined for any $y \in B$. Since f is injective, for each $y \in B$ there is exactly one image $x = f^{-1}(y)$. It follows that the inverse map exists.

Theorem is proved.

6. Composition of maps

Definition. *Let $f: A \to B$ and $g: B \to C$ be maps. The composition of f and g is a map $g \circ f: A \to C$ such that $g \circ f(x) = g(f(x))$.*

Example. Let $f(x) = x + 1$, $g(y) = y^2$. Then $g \circ f(x) = (x + 1)^2$.

CM10311

Lecture Notes 6

1. Compositions of maps (cont.)

Theorem.
(a) The composition of two injective maps is injective.

(b) The composition of two surjective maps is surjective.

Proof.
(a) Let both maps

$$f:\ A \to B,$$

$$g:\ B \to C$$

be injective. Let $x_1, x_2 \in A$ and $x_1 \neq x_2$. Then $f(x_1) \neq f(x_2)$ since f is injective. Then $g(f(x_1)) \neq g(f(x_2))$ since g is injective. Thus, for $x_1 \neq x_2$ we have $g \circ f(x_1) \neq g \circ f(x_2)$, which means that $g \circ f$ is injective.

(b) Exercise.

Corollary. *The composition of two bijective maps is bijective*

2. Inverse map and identity map

Let $f : A \to B$ be a bijective map. Let $I_A : A \to A$ be the identity map on A. Recall that $I_A(x) = x$ for any $x \in A$.

Theorem. *Composition $f \circ f^{-1}$ coincides with the identity map I_B; composition $f^{-1} \circ f$ coincides with the identity map I_A.*

Proof. Let $x \in A$, $f(x) = y \in B$. By the definition of f^{-1}, we have $x = f^{-1}(y)$. It follows that $f(x) = f(f^{-1}(y)) = y$ and $f^{-1}(f(x)) = x$. The theorem is proved.

Theorem. *Each of the compositions $I_B \circ f$ and $f \circ I_A$ coincides with f.*

Proof. Let $x \in A$, $f(x) = y \in B$. Further on, $I_B(y) = y$. Hence, $I_B \circ f(x) = y$, i.e. values of both maps, f and $I_B \circ f$, coincide at the same argument x. The case of the composition $f \circ I_A$ is proved similarly.

We see that $\circ$ can be considered as an operation on bijective maps from a set A to inself, similar to multiplication of numbers. A significant difference is that $\circ$ is not a commutative operation. The role of the unit is played by the identity map.

3. Map as a subset of Cartesian product

Let us introduce a more precise definition of a map.

Definition. *A map $f : A \to B$ is a subset of $A \times B$ with the following property. For any $x \in A$ there exists one and only one $y \in B$ such that $(x, y) \in f$.*

For familiar functions, like $f(x) = x^2$, the above definition describes their *graphs*, i.e. we define a map via its graph.

4. Relations

Relaxing the definition of the map from Section 3 we obtain the following definition.

Definition. *Let A, B be sets. A relation R between A and B is a subset of $A \times B$. In a special case of $A = B$, we say that $R \subset A \times A$ is a relation on A.*

Examples.

(1) Let A be a set of students, B be a set of available teaching units. Define a relation $R \subset A \times B$ as a set of all pairs (x, y) such that the student x is registered for the unit y.

(2) Let $A = B = \mathbf{Z}$. Define $R = \{(x, y) \in R |\, x < y\}$. In this case, instead of $(x, y) \in R$ the notation $x < y$ is used.

(3) Any map $f : A \to B$ is a relation between A and B.

(4) Let $A = B = \mathbf{Z}$. Define R to be a set of all pairs (x, y) from $\mathbf{Z}^2$ such that x divides y.

(5) Let $A = B = \mathbf{Z}$. Define $R = \{(x, y) \in R |\, x = y\}$. In this case, instead of $(x, y) \in R$ the notation $x = y$ is used.

(6) Let A be a finite set. Any relation R on A is called (or can be interpreted as) a *directed graph*. In this case, A is the set of *vertices* of R and any pair $(x, y) \in A \times A$ is an *arc* from x to y. If for any arc $(x, y) \in R$ there exists the arc $(y, x) \in R$, and we identify these two arcs, then the graph is called *undirected*.

5. Equivalence relations

In the following definition we use the symbol $*$ for a relation, i.e., we write $x * y$ instead of $(x, y) \in R$, like we used $<$ and $=$ in the examples (2) and (5) respectively.

Definition *A relation $*$ on A is called equivalence relation if:*

(a) *$*$ is reflexive, i.e., for any $x \in A$, $x * x$.*

(b) *$*$ is symmetric, i.e., if $x * y$, then $y * x$.*

(d) *$*$ is transitive, i.e., if $x * y$ and $y * z$, then $x * z$.*

Examples.

(1) The relation $=$ is an equivalence relation on $\mathbf{Z}$ (trivial check).

(2) Parity on $\mathbf{Z}$: all even numbers are equivalent, as are all odd numbers.

(3) Let A be a set of people. Define $x * y$ as the predicate which is true if and only if x has the same birthdate as y.

Definition. *Let $*$ be an equivalence relation on a set A, let $x \in A$. The subset $[x] = \{y \in A | \, x * y\}$ is called the equivalence class of the element x.*

Examples.

(1) For the relation "=" on $\mathbf{Z}$ each equivalence class $[i]$ consists of a single element i, i.e. $[i] = \{i\}$.

(2) For the "parity" relation on $\mathbf{Z}$, $[i]$ consists of all even numbers if $i \in \mathbf{Z}$ is even, otherwise $[i]$ is the set of all odd numbers.

6. Partition into equivalence classes

Definition. *A partition of a finite set A is a collection of non-empty subsets*

$$A_1, A_2, \ldots, A_n$$

of A such that
(a) $A = A_1 \cup A_2 \cup \cdots \cup A_n$;
(b) $A_i \cap A_j = \emptyset$ *for* $i \neq j$.

Theorem. *Let $*$ be an equivalence relation on a finite set A. Then the distinct equivalence classes form a partition of A.*

Proof. Let us show that the definition of the partition is satisfied.

Firstly, equivalence classes should be non-empty. Let $x \in A$. Then $x \in [x]$ by reflexiveness, thus $[x] \neq \emptyset$.

Secondly, the union of all equivalence classes should coincide with A. Clearly, that union is a *subset* of A. It remains to show that, conversely, A is a subset of the union. Take any $x \in A$. Then, as before, $x \in [x]$, i.e. x belongs to an equivalence class and therefore to the union of all equivalence classes.

Finally, two distinct equivalence classes should be disjoint. Thus, we need to show that if x is not equivalent to y, then $[x] \cap [y] = \emptyset$. Suppose that is not true, and for some x, y, where x is not equivalent to y, the intersection $[x] \cap [y]$ is non-empty. The latter means that there exists an element $z \in A$ such that $z \in [x] \cap [y]$. By the definition of $\cap$, $z \in [x]$ and $z \in [y]$, that is $z * x$ and $z * y$. By symmetry and transitivity of $*$, it follows that $x * y$, which contradicts to our initial assumption. The theorem is proved.

CM10311

Lecture Notes 7

1. Rational numbers

Let

$$A = \{x/y |\, x, y \in \mathbf{Z}, y \neq 0\},$$

or equivalently,

$$A = \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$$

be the set of ordinary fractions (pairs of integers) with non-zero denominators. Introduce the following relation $\sim$ on A: $x_1/y_1 \sim x_2/y_2$ if and only if $x_1 y_2 = x_2 y_1$. It is easy to check (do it!) that $\sim$ is an equivalence relation.

Definition *The set* $\mathbf{Q}$ *of all rational numbers is the set of all equivalence classes of the relation* $\sim$ *on* A.

Example. The set $\{1/2, 3/6, 27/54, \ldots\}$ consisting of all fractions of the kind $a/(2a)$ for all non-zero $a \in \mathbf{Z}$ is an equivalence class of $\sim$ on A, hence this set is a rational number. A natural representative fraction for this class is $1/2$ ($a = 1$), so we will, sometimes call this rational number $1/2$.

Generally, let $q \in \mathbf{Q}$. Then there exists a unique fraction $x/y \in q$ such that for any fraction $x'/y' \in q$ there exists $a \in \mathbf{Z}$ with $x' = ax$ and $y' = ay$. Let us call this fraction x/y *distinguished representative* of q. It is easy to see that the distinguished representatives are exactly all irreducible fractions, i.e. fractions x/y with x, y having no common divisors over than 1.

Example It is easy to interpret $\mathbf{Z}$ as a subset of $\mathbf{Q}$ by identifying an integer $n \in \mathbf{Z}$ with an equivalence class containing the fraction $n/1$.

2. Arithmetic operations on Q

Definition (arithmetic of fractions). *We define:*

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2},$$

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 x_2}{y_1 y_2}.$$

Definition (arithmetic over $\mathbf{Q}$). *For two rational numbers* $p, q \in \mathbf{Q}$ *their sum* $p + q$ *(respectively, product* pq*) is defined as follows. Choose an arbitrary fraction* $x_1/y_1 \in p$*, an arbitrary fraction* $x_2/y_2 \in q$*. Then* $p + q$ *(respectively,* pq*) is defined the rational number which contains the fraction* $\frac{x_1}{y_1} + \frac{x_2}{y_2}$ *(respectively, the fraction* $\frac{x_1}{y_1} \cdot \frac{x_2}{y_2}$*).*

Theorem. *Arithmetic operations over* $\mathbf{Q}$ *are well defined, that is, the result of an arithmetic operation does not depend on particular choices of fractions* x_1/y_1, x_2/y_2.

Proof. It is sufficient (make sure you understand why) to prove the following proposition. *If*

$$\frac{x}{y} \sim \frac{x'}{y'} \quad \text{and} \quad \frac{z}{w} \sim \frac{z'}{w'}$$

then

$$\frac{x}{y} + \frac{z}{w} \sim \frac{x'}{w'} + \frac{z'}{w'} \quad \text{and} \quad \frac{x}{y} \cdot \frac{z}{w} \sim \frac{x'}{w'} \cdot \frac{z'}{w'}.$$

This proposition can be proved by straightforward computation.

3. Cauchy sequences

Let $\mathbf{N}$ be the set of all *natural numbers*, that is, positive integers.

Definition. *A sequence of rational numbers is a function*

$$a : \mathbf{N} \to \mathbf{Q}.$$

Traditionally, the image $a(n)$ of a at n is denoted by a_n, and the whole sequence by $\{a_n\}$. One can think of a sequence as of an infinite string $a_1, a_2, \ldots, a_n, \ldots$. We will refer to a_n as to the *nth member* of the sequence $\{a_n\}$.

Definition. *Sum and product of two sequences* $\{a_n\}$ *and* $\{b_n\}$ *are defined as follows:*

$$\{a_n\} + \{b_n\} = \{a_n + b_n\},$$

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

We write $\{a_n\} - \{b_n\}$ *for the sequence* $\{a_n\} + \{-b_n\}$.

Recall that for any number x, its *absolute value* $|x|$ is x itself if $x \geq 0$ or $-x$ if $x < 0$. It is easy to see that for any two numbers x, y the absolute values $|x + y| \leq |x| + |y|$ and $|x - y| \leq |x| + |y|$.

Definition. *A sequence* $\{a_n\}$ *of rational numbers is called Cauchy sequence when the following condition is satisfied. For every rational* $\varepsilon > 0$ *there exists* $N \in \mathbf{N}$ *such that for any two natural numbers* $n, m \geq N$ *we have* $|a_n - a_m| < \varepsilon$.

Example. The sequence $\{a_n\}$ where $a_n = 1/n$ is a Cauchy sequence. Indeed, fix any rational number $\varepsilon > 0$. Choose any positive integer N greater than $1/\varepsilon$. Then for any $n, m \geq N > 1/\varepsilon$ we have $1/n, 1/m < \varepsilon$. It follows that $|1/n - 1/m| < \max\{1/n, 1/m\} < \varepsilon$, which means that $\{a_n\}$ is a Cauchy sequence.

4. Arithmetic of Cauchy sequences

Theorem. *If $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, then $\{a_n\}+\{b_n\}$ and $\{a_n\}\cdot\{b_n\}$ are also Cauchy sequences.*

Proof. We will prove the theorem only for addition, for multiplication a proof is similar and is left as a exercise.

Fix any rational number $\varepsilon > 0$. We need to prove that there exists an natural number N such that if $n, m \geq N$ for natural numbers n, m, then $|(a_n + b_n) - (a_m + b_m)| < \varepsilon$.

Since $\{a_n\}$ is a Cauchy sequence, for $\varepsilon > 0$ there exists N' such that if $n, m \geq N'$, then $|a_n - a_m| < \varepsilon/2$. Since $\{b_n\}$ is a Cauchy sequence, for $\varepsilon > 0$ there exists N'' such that if $n, m \geq N''$, then $|b_n - b_m| < \varepsilon/2$. Take $N \geq \max\{N', N''\}$. Then for $n, m \geq N$ we have

$$|(a_n + b_n) - (a_m + b_m)| = |a_n - a_m + b_n - b_m| \leq |a_n - a_m| + |b_n - b_m| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

The theorem is proved for the addition.

5. Null sequences

Definition. *A null sequence is a sequence $\{a_n\}$ of rational numbers with the following property. For any rational number $\varepsilon > 0$ there exists a natural number N such that if a natural number $n \geq N$, then $|a_n| < \varepsilon$.*

Example. The sequence $\{a_n\}$ where $a_n = 1/n$ is a null sequence (for a given ε take $1/\varepsilon + 1$ as N).

From the example in Section 3 we know that $\{1/n\}$ is a Cauchy sequence. A more general fact is true.

Theorem. *Any null sequence $\{a_n\}$ is a Cauchy sequence.*

Proof. We check that the definition of a Cauchy sequence holds for $\{a_n\}$. Fix any rational number $\varepsilon > 0$. By the definition of null sequence, for the number $\varepsilon/2$ one can choose a natural number N such that if $n, m \geq N$ then $|a_n| < \varepsilon/2$ and $|a_m| < \varepsilon/2$. It follows, that $|a_m - a_n| \leq |a_m| + |a_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon$ and the definition of Cauchy sequence is satisfied.

6. Equivalence relations for Cauchy sequences and real numbers

Let C be the set of all Cauchy sequences. Introduce the following relation $\sim$ on C. For $\{a_n\}, \{b_n\} \in C$ let $\{a_n\} \sim \{b_n\}$ if the difference $\{a_n\} - \{b_n\}$ is a null sequence.

Example. $\{1/n\} \sim \{1/n^2\}$ (prove it!).

Theorem. *The relation $\sim$ on C is an equivalence relation.*

Proof. A straightforward check of the reflexivity, symmetry and transitivity of $\sim$.

Definition. *The set* **R** *of real numbers is the set of all equivalence classes of the relation $\sim$ on C.*

CM10311

Lecture Notes 8

1. Arithmetic of real numbers

Definition *Let $x, y \in \mathbf{R}$. The sum $x + y$ and the product xy are defined as follows. Choose an arbitrary Cauchy sequence $\{a_n\} \in x$ and an arbitrary Cauchy sequence $\{b_n\} \in y$. Then $x + y$ is the real number containing (as an equivalence class relative to $\sim$) the sequence $\{a_n\}+\{b_n\}$. Similarly, xy is the real number containing the sequence $\{a_n\} \cdot \{b_n\}$.*

Theorem. *Sum and product of real numbers are defined correctly (do not depend on choices of sequences $\{a_n\}$, $\{b_n\}$ in the above definition).*

Proof. Exercise.
Hint. It is sufficient to prove that if $\{a_n\} \sim \{a'_n\}$ and $\{b_n\} \sim \{b'_n\}$, then $\{a_n\} + \{b_n\} \sim \{a'_n\} + \{b'_n\}$ and $\{a_n\} \cdot \{b_n\} \sim \{a'_n\} \cdot \{b'_n\}$.

2. Partial order and total order

Definition. *Let A be a set. A relation R on A is called antisymmetric if conditions $(x, y) \in R$ and $(y, x) \in R$ imply $x = y$, for all $x, y \in A$.*

Examples.

(1) Relation $\leq$ on $\mathbf{Z}$ is antisymmetric.

(2) Relation $<$ on $\mathbf{Z}$ is also antisymmetric (because the proposition $(x < y) \wedge (y < x)$ is false for all pairs $x, y \in \mathbf{Z}$, hence the implication $((x < y) \wedge (y < x)) \to (x = y)$ is true).

Definition. *A relation R on a set A is called partial order on A, if R is*

(a) reflexive,
(b) antisymmetric,
(c) transitive.

Examples.

(1) Relation $\leq$ on $\mathbf{Z}$ is a partial order.

(2) Relation $\geq$ on $\mathbf{Z}$ is a partial order.

(3) Relation $<$ on $\mathbf{Z}$ is not a partial order (it is antisymmetric and transitive, but not reflexive).

(4) Relation $=$ on $\mathbf{Z}$ is a partial order.

(5) Relation $\subset$ on the set A of all subsets of a universe U is a partial order on A.

(6) Let $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{a, c\}, \{b, c\}\}$. The the relation $\subset$ is a partial order on A.

Definition. *A partial order R on A is called total order if for any $x, y \in A$, either $(x, y) \in R$, or $(y, x) \in R$ is true.*

Examples.

(1) Relation $\leq$ on $\mathbf{Z}$ is a total order.

(2) Let $A = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}, \{a, b, c, d\}\}$. The the relation $\subset$ is a total order on A.

3. Maximal and minimal elements

Definition. *Let R be a partial order on a set A. An element $x \in A$ is called maximal, if $\forall y \in A((x, y) \in R \rightarrow x = y)$. Similarly, an element $x \in A$ is called minimal, if $\forall y \in A((y, x) \in R \rightarrow x = y)$.*

Maximal or minimal element may not exist for some partial orders, for example, for $\leq$ on $\mathbf{Z}$. On the other hand, there may be more than one maximal or minimal element for some partial orders. In example (6), Section 2, elements $\{a, b\}, \{a, c\}, \{b, c\}$ are all maximal.

Exercise. Prove that for a total order on a set A if a maximal element exists, then it's unique. Prove the same for a minimal element.

4. Strict partial order

Definition. *Let A be a set. A relation R on A is called asymmetric if either $(x, y) \notin R$ or $(y, x) \notin R$ for all pairs $x, y \in A$.*

Definition. *A relation R on A is called strict partial order on A if it's asymmetric and transitive.*

Example. The relation $<$ on $\mathbf{Z}$ is a strict partial order.

Theorem. *Let A be a set.*
(a) If $\leq$ be a partial order on A, then a relation $<$ on A defined by

$$x < y \quad \text{if} \quad (x \leq y) \wedge (x \neq y)$$

is a strict partial order.

(b) If $<$ is a strict partial order on A, then a relation $\leq$ on A defined by

$$x \leq y \quad \text{if} \quad (x < y) \vee (x = y)$$

is a partial order on A.

Proof.
(a) We need to prove that $<$ is asymmetric and transitive.

Asymmetric: Suppose that, contrary to what we need, $(x < y) \wedge (y < x)$ for some $x, y \in A$. Then, by the definition of $<$, $(x \leq y) \wedge (y \leq x)$. Since the relation $\leq$ is antisymmetric, it follows that $x = y$, which contradicts to $x < y$ in view of the definition of $<$.

Transitive: Let $(x < y) \wedge (y < z)$ for some $x, y, z \in A$. Then, by the definition of $<$, $(x \leq y) \wedge (y \leq z)$. By the transitivity of $\leq$, we have $x \leq z$. Suppose that $x = z$. Then we can re-write the formula $(x \leq y) \wedge (y \leq z)$ as $(z \leq y) \wedge (y \leq z)$. By the definition of $\leq$,

it follows that $y = z$, which contradicts to $y < z$. We conclude that $x \neq z$, and therefore, $x < z$.

(b) Left as an exercise.

5. Orders on Q and R

We introduce strict partial order on $\mathbf{Q}$ and $\mathbf{R}$ in two steps. Firstly, we will define positive elements in these sets. Secondly, we set $x < y$ if $0 < y - x$, that is, if the difference $y - x$ is positive.

Set of rational numbers $\mathbf{Q}$: We assume that $0 < x$ for $x \in \mathbf{Q}$, if for a fraction $\frac{a}{b} \in x$,

$$((0 < a) \wedge (0 < b)) \vee ((a < 0) \wedge (b < 0)).$$

Theorem. *Strict order on* $\mathbf{Q}$ *is well defined (does not depend on a choice if integers* a *and* b*).*

Proof. Proof is a straightforward routine.

Set of real numbers $\mathbf{R}$: We assume that $0 < x$ for $x \in \mathbf{R}$, if $x \neq 0$ and for a Cauchy sequence $\{a_n\} \in x$ all, except a finite number, terms in $\{a_n\}$, are positive.

Theorem. *Strict order on* $\mathbf{R}$ *is well defined (does not depend on a choice of the sequence* $\{a_n\}$*).*

Proof. Proof is a straightforward routine.

Once strict partial orders on $\mathbf{Q}$ and $\mathbf{R}$ are defined, use the Theorem from Section 4 to define partial orders $\leq$ on $\mathbf{Q}$ and $\mathbf{R}$. Observe that these orders are total.

CM10311

Lecture Notes 9

1. Divisibility of integers

Let $\mathbf{Z}$ denote the set of all integers.

Definition 1. *For $a, b \in \mathbf{Z}$, $a \neq 0$ we say that b is divisible by a (or that a divides b) and write $a|b$ if there exists $q \in \mathbf{Z}$ such that $b = aq$. In that case a is called divisor of b and q is called quotient.*

Remark. In some literature the condition $a \neq 0$ is dropped in this definition. In this case it is assumed that 0 is divisible by 0. We will always assume that $a \neq 0$.

Definition 2. *The number $p \in \mathbf{Z}$, $p > 1$ is called prime if it does not have positive divisors other than 1 and itself. Integers greater than 1 that are not prime are called composite.*

Euclid proved a famous theorem that the set of all prime numbers is infinite.

Definition 3. *Two non-zero integers $a, b \in \mathbf{Z}$ are called relatively prime if their greatest common divisor, $GCD(a, b) = 1$.*

It is well-known that $a, b \in \mathbf{Z}$ are relatively prime if and only if there exist $u, v \in \mathbf{Z}$ such that $au + bv = 1$.

Definition 4. *We say that for $a, b \in \mathbf{Z}$, where $a > 0$, b is divisible by a with the remainder r, if there exist $q, r \in \mathbf{Z}$, with $0 \leq r < a$, such that $b = aq + r$.*

Definition 4. *For $a, b, m \in \mathbf{Z}$, $m > 0$, we say that a is congruent to b modulo m and write $a \equiv b \, mod \, m$, if $a - b$ is divisible by m. Equivalently, $a \equiv b \, mod \, m$ if a is divisible by m with the same remainder as is b divisible by m.*

Examples.

$7 \equiv 1 \, mod \, 3$;

$50 \equiv 175 \, mod \, 25$.

The proofs of the following propositions are trivial.

Proposition 1. *Let for $a, m \in \mathbf{Z}$, $m > 0$, an integer r be the remainder of the division of a by m. Then $a \equiv r \, mod \, m$.*

Proposition 2. *Fix $m \in \mathbf{Z}$. The relation "congruent modulo m" is an equivalence relation. That is:*

(i) $a \equiv a \, mod \, m$;

(ii) *if $a \equiv b \, mod \, m$, then $b \equiv a \, mod \, m$;*

(iii) *if* $a \equiv b \, mod \, m$ *and* $b \equiv c \, mod \, m$, *then* $a \equiv c \, mod \, m$.

As we know, an equivalence relation on a set partitions this set into disjoint *equivalence classes*, i.e., subsets of elements equivalent to each other. Proposition 2 implies that for fixed m the set $\mathbf{Z}$ can be represented as a union of disjoint sets (called *residue classes*) of integers congruent to each other modulo m. By Proposition 1, for every integer a there is an integer r, $0 \leq r < m$ congruent to a modulo m (namely, the remainder of the division of a by m). Therefore, the number of distinct residue classes is not greater than m. On the other hand, every two distinct integers between 0 and $m-1$ are *not congruent* modulo m. It follows that the number of distinct residue classes is exactly m, and the numbers $0, 1, \ldots, m-1$ are representatives of these classes.

The finite family of all residue classes modulo m is denoted by $\mathbf{Z}/m\mathbf{Z}$ or just $\mathbf{Z}_m$.

Example. Let $m = 2$. The condition $a \equiv b \, mod \, 2$ means that $a - b$ is divisible by 2, i.e., a and b have the same parity. It follows that $\mathbf{Z}/2\mathbf{Z}$ consists of two elements: class E of even numbers and class O of odd numbers.

2. More properties of congruences

Proposition 3. *If* $a \equiv b \, mod \, m$ *and* $c \equiv d \, mod \, m$, *then*

$a + c \equiv b + d \, mod \, m$;
$ac \equiv bd \, mod \, m$.

Proposition 3 allows to define arithmetic operations on the family $\mathbf{Z}/m\mathbf{Z}$ of all residue classes.

Definition. *Let* $x, y \in \mathbf{Z}/m\mathbf{Z}$ *and* $a \in x$, $b \in y$. *For an arithmetic operation* $* \in \{+, \cdot\}$ *define* $x * y$ *as the residue class containing* $a * b$.

Due to Proposition 3, arithmetic operations $+$ and $\cdot$ are well-defined, that is, they don't depend on a choice of representatives a and b.

2. Division operation in $\mathbf{Z}/m\mathbf{Z}$

In this unit we introduced various number systems: $\mathbf{Z}$ (integers), $\mathbf{Q}$ (rationals), $\mathbf{R}$ (reals), and, finally, $\mathbf{Z}/m\mathbf{Z}$ (integers modulo m). For each of these systems we defined (in the case of $\mathbf{Z}$ – assumed) operations of addition $(+)$ and multiplication $(\cdot)$. Let us now introduce the inverse operations, subtraction $(-)$ and division $(/)$, respectively. We will do this in two steps. Let A be any of these number systems. Observe that each A contains numbers 0 (the identity element of A with respect to addition) and 1 (the identity element of A with respect to multiplication).

(i) Each number $x \in A$ has the inverse with respect to addition, i.e., number $y \in A$ such that $x + y = 0$. Additive inverse element y is traditionally denoted by $-x$. Similarly, each number $x \in A$, such that $x \neq 0$, has the inverse with respect to multiplication, i.e., number $y \in A$ such that $x \cdot y = 1$. Multiplicative inverse element y is denoted by x^{-1}.

(ii) Subtraction operation $x - z$ for $x, z \in A$ is defined as adding to x the additive inverse of z, i.e., $x - z := x + (-z)$. Division operation x/z for $x, z \in A,\ z \neq 0$, is defined as multiplying x by the multiplicative inverse of z, i.e., $x/z := x \cdot z^{-1}$.

It follows that to define subtraction and division in each of the number sets A it is sufficient to define inverse elements. Additive inverses are defined in a straightforward way, multiplying by (-1).

In $\mathbf{Z}$ the only number with the multiplicative inverse is 1.

For $x \in \mathbf{Q},\ x \neq 0$, let a/b be a fraction in the equivalence class x. Then define x^{-1} as the equivalence class containing b/a.

For $x \in \mathbf{R},\ x \neq 0$, let $\{a_n\}$ be a Cauchy sequence in the equivalence class x. There is only finite number of zero elements in $\{a_n\}$. Remove these elements from the sequence, the result is again a Cauchy sequence, $\{a'_n\}$. Define x^{-1} as the equivalence class containing the Cauchy sequence $\{1/a'_n\}$.

Not every element $x \neq 0$ in $\mathbf{Z}/m\mathbf{Z}$ has multiplicative inverse x^{-1} (such that the class $x \cdot x^{-1}$ contains 1) in $\mathbf{Z}/m\mathbf{Z}$. The following elementary proposition sets the conditions under which inverses exist.

Proposition 5. *An element $x \in \mathbf{Z}/m\mathbf{Z}$ has multiplicative inverse if and only if integers in residue class of x are relatively prime with m.*

Proof. Let x have multiplicative inverse, i.e., there are integers $a \in x$ and $b \in \mathbf{Z}$ such that $ab \equiv 1\ mod\ m$, and let $GCD(a, m) = d$. Then $m|(ab - 1)$ implies $d|(ab - 1)$. Since $d|a$, the integer 1 should also be divisible by d, which is only possible if $d = 1$. Conversely, if $GCD(a, m) = 1$ for $a \in x$, then as was noted above, there exist $u, v \in \mathbf{Z}$ such that $au + mv = 1$, and we can choose as x^{-1} the class containing u.

Corollary. *If $p \in \mathbf{Z}$ is a prime number, then each non-zero element $x \in \mathbf{Z}/p\mathbf{Z}$ has the multiplicative inverse $x^{-1} \in \mathbf{Z}/p\mathbf{Z}$. Therefore, for each two elements $x, z \in \mathbf{Z}/p\mathbf{Z},\ z \neq 0$, there exits the quotient $x/z := x \cdot z^{-1} \in \mathbf{Z}/p\mathbf{Z}$.*