Sets and Numbers Notes (2023/2024)

Griffin Reimerink

Contents

1 Symbols

1.1 Logic

$\forall$	for all
$\exists$	there exists
$\neg$	not
$\wedge$	and
$\vee$	or
$\implies$	implies
$\iff$	if and only if (iff)
$\sim$	logically equivalent
$:$	such that (s.t.)

1.2 Number systems

$\mathbb{N}$	set of all natural numbers
$\mathbb{Z}$	set of all integers
$\mathbb{Q}$	set of all rational numbers
$\mathbb{R}$	set of all real numbers
$\mathbb{C}$	set of all complex numbers
$\mathbb{F}$	set of all scalars (real or complex)

1.3 Set theory

$\in$	is an element of
$\notin$	is not an element of
$\subseteq$	subset or equal
$\subset$	subset, not equal
$[n]$	$0, 1, 2...n-1$ for all $n \in \mathbb{N}$
$\emptyset$	empty set $\{\}$
2^X	power set of X
$\#$	cardinality
X^C	complement of X
$\cup$	union
$\cap$	intersection
$\setminus$	difference
$\overline{a}$	equivalence class of a

2 Proofs

A **theorem** is an important statement.
A **lemma** is a less important statement which is often a part of a proof for a theorem.
A **proposition** is a statement that is either true or false without ambiguity.
A **tautology** is a statement that is always true, a **contradiction** is a statement that is always false.

2.1 Proving existence

Proof by construction: provide an example that proves the statement.

2.2 Proving equality

To prove equality of two real numbers a and b with certain properties, one way to go is to prove first $a \leq b$ and then $b \leq a$. Similarly, we can prove two sets A and B are equal by showing $A \subseteq B$ and $B \subseteq A$ and using the definition of a subset.

2.3 Proof by contradiction

To prove a statement, one can assume first that the statement is false and then show this implies a contradiction.

2.4 Proof by exhaustion

The statement

$$\forall\, x \in S,\ p(x)$$

is logically equivalent to

$$(\forall\, x \in S_1,\ p(x)) \land (\forall\, x \in S_2,\ p(x))$$

provided that $S_1 \cup S_2 = S$. Therefore, one can prove the former by proving the latter.

2.5 Mathematical induction

- **Initial step** Show that the statement is true for the minimum value of n.
  ($n = 0$ or $n = 1$ in most cases)
- **Hypothesis** Assume that the statement is true for some $n \in \mathbb{N}$.
  Strong induction: the statement is true for all $q \leq n$
- **Induction** Prove that the statement is true for $n + 1$ by substituting the hypothesis.

Reverse induction can be used to prove by contradiction: Suppose that there exists a counterexample N. Prove that if that is the case, there also exists a lower counterexample. Therefore the base case must also be a counterexample which leads to a contradiction.

2.6 Proving $p \implies q$

One can prove that the statement

$$((p \implies r) \land (r \implies q)) \implies (p \implies q)$$

is a tautology. By repeated application, we can further prove that

$$((p \implies r_1) \land (r_1 \implies r_2) \land ... \land (r_{k-1} \implies r_k) \land (r_k \implies q)) \implies (p \implies q)$$

is also a tautology. This means that we can prove $p \implies q$ by coming up with statements $r_1, r_2, ..., r_k$ such that $p \implies r_1 \implies r_2 \implies ... \implies r_{k-1} \implies r_k \implies q$.

Beside proving $p \implies q$ directly, a **proof by contraposition** can be used:
The **contrapositive** of $p \implies q$ is the statement $\neg q \implies \neg p$ and it is logically equivalent to $p \implies q$. Therefore, one can prove $p \implies q$ by proving the contrapositive $\neg q \implies \neg p$.

2.7 Proving $p \iff q$

$p \iff q$ can also be proven directly in a way similar to $p \implies q$.
We can also rely on the fact that $p \iff q$ is logically equivalent to $(p \implies q) \wedge (q \implies p)$

3 Sets

Sets (with the exception of the **empty set**) contain **elements**.
An element can be anything, for example a number, an object or another set.
Note that in this course, $\mathbb{N}$ starts at 0.

$$\{a, a\} = \{a\} \qquad \{a, b\} = \{b, a\}$$

3.1 Subsets

$X \subset Y$ iff every element of X is also an element of Y.
$X = Y$ iff $X \subseteq Y$ and $Y \subseteq X$. (**Double inclusion lemma**)
If $X \subseteq Y$ and $Y \subseteq Z$ then $X \subseteq Z$ (**Transitivity of subsets**)
$\emptyset$ is a subset of every set.
The **power set** of X is the set of all subsets of X.
Notation for the subset of all x of X for which $P(x)$ is true: $\{x \in X : P(x)\}$

3.2 Set operations

Union, **intersection** and **difference**:

$$X = \{1, 2\}, Y = \{2, 3\}$$
$$X \cup Y = \{1, 2, 3\} \qquad X \cap Y = \{2\} \qquad X \setminus Y = \{1\} \qquad Y \setminus X = \{3\}$$

Lines in 2D geometry are sets $\{(x, y) \in \mathbb{R}^2 : ax + by = c\}$
If $A_0, A_1, ...A_n$ are sets and k is a dummy variable, then:

$$\bigcup_{k=0}^{n} A_k = A_0 \cup A_1 \cup ... \cup A_n \qquad \bigcap_{k=0}^{n} A_k = A_0 \cap A_1 \cap ... \cap A_n$$

De Morgan's Law: If X, Y, Z are sets then $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$

If X, Y are sets, then $X \cap Y = Y \cap X$ and $X \cup Y = Y \cup X$. This is not true for differences.
The complement of a set X is the set of all elements not in X.
Two sets A and B are **disjoint** if $A \cap B = \emptyset$.
$(A \cap B)^C = A^C \cup B^C \quad (A \cup B)^C = A^C \cap B^C$

3.3 Cardinality

A **singleton** is a set with only one element.
The **cardinality** of set A, denoted by card A, is the number of elements it contains. Two sets have equal cardinality if there exists an invertible $f : X \to Y$
A set is **finite** if there exists an $n \in \mathbb{N}$ and an invertible function $f : [n] \to X$ or is **infinite** otherwise.
X is **countably infinite** if there is an invertible $f : \mathbb{N} \to X$
Cantor theorem: There are sets that are not countable.
If A and B are disjoint finite sets then $\#(A \cup B) = \#A + \#B$
If a set X is finite then so is any subset of X.

3.4 Cartesian product

If X and Y are sets then their **Cartesian product** $X \times Y$ is the set of ordered pairs (x, y) where $x \in X$ and $y \in Y$.

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ $\quad$ $A \times B \neq B \times A$ because the pairs are ordered. $\quad$ $(x, y) \neq \{x, y\}$

Projection function:
$\pi_1 : X \times Y \to X$ is defined by $\pi_1((x, y)) = x$ and likewise $\pi_2 : X \times Y \to Y$ is defined by $\pi_2((x, y)) = y$

If X and Y are finite then $\#(X \times Y) = \#X * \#Y$
If X and Y are countably infinite then $X \times Y$ is also countably infinite.

$$(A \cup B) \times Y = (A \times Y) \cup (B \times Y) \quad (A \cap B) \times Y = (A \times Y) \cap (B \times Y) \quad (A \setminus B) \times Y = (A \times Y) \setminus (B \setminus Y)$$

3.5 Equivalence relations

An **equivalence relation** R on a set X is a subset $R \subseteq X^2$ with the following properties for all $x, y, z \in X$:

1. **Reflexivity** $x \sim y$
2. **Symmetry** if $x \sim y$ and $y \sim z$
3. **Transitivity** if $x \sim y$ and $y \sim z$ then $x \sim z$ as well

X/R is the set of **equivalence classes** (not to be confused with $X \setminus R$).
All equivalence classes are disjoint.
If $f : X \to Y$ then introduce equivalence relation $\sim_f$ on X by $x \sim x'$ iff $f(x) = f'(x)$
We say $P \subseteq 2^X$ is a **partition** of X if $\bigcup\limits_{p \in P} p = X$ and for all $p, q \in P$ we have $p \cap q = \emptyset$
Given an equivalence relation R on a set X we say that the equivalence class of $x \in X$ is the set

$$\overline{x} = \{y \in X : y \sim x\}$$

If R is an equivalence relation on X then the set of equivalence classes X/R is a partition of X.
Example:

$$X = \{0, 1, 2\} \qquad R = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 2)\} \qquad X/R = \{\{0, 1\}, \{2\}\} = \{\overline{0}, \overline{2}\}$$

A subset $S \subseteq X$ is called a **system of representatives** iff S contains precisely one element of each equivalence class.

If P is a partition on X then the following $R \in X^2$ is an equivalence relation on X
$x \sim y$ iff $(x, y) \in R$

$$R = \{(a, b) \in X^2 : (\exists \pi \in P : \{a, b\} \in \pi)\}$$

More generally, any subset $R \subseteq X \times Y$ is called a **relation** between X and Y.

4 Functions

$f \circ g$	composition of functions (f on g)
id	identity function
$\mapsto$	maps to

When you have trouble understanding a function, make a diagram of a simple example.

4.1 Definition

Let A and B be sets. With the notation $f : A \to B$, we mean that f is a function whose **domain** is A and **codomain** is B. That is, f assigns a unique value $f(a) \in B$ to each $a \in A$. Therefore, $f(a_1) = f(a_2)$ whenever $a_1 = a_2$. However, it is possible that $a_1 \neq a_2$ and $f(a_1) = f(a_2)$.

The **image** of a subset $A \subseteq X$ is called $f(A) = \{y \in Y : \text{There is some } x \in A \text{ with } f(x) = y\}$.
The **range** of $f : X \to Y$ is $f(X)$.
Two functions $f : X \to Y$ and $g : A \to B$ are **equal** iff

$$X = A \text{ and } Y = B \text{ and for every } x \in X : f(x) = g(x)$$

To denote a function, we sometimes use the shorthand notation $a \mapsto b$ whenever the sets A and B are clear from the context.

For any sets X and Y define the set $Y^X = \{ \text{ functions } f : X \to Y\}$ where $\#(Y^X) = (\#Y)^{\#X}$
Calculus is about $\mathbb{R}^{\mathbb{R}}$, linear algebra is about $\mathbb{R}^{[n]}$

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\} \qquad \mathbb{R}^{[2]} = \{f : X \to \mathbb{R}\} \qquad \mathbb{N}^{\mathbb{N}} = \text{set of all sequences}$$

4.2 Properties of functions

A function $f : A \to B$ is **onto** or **surjective** if the range equals the codomain: $f(X) = Y$.
Therefore, for any $y \in Y$ there exists an $x \in X$ such that $f(x) = Y$.
It is **one to one** or **injective** if f cannot take the same value twice.
In other words: if for some x_1, x_2 we have $f(x_1) = f(x_2)$ then we must have $x_1 = x_2$.
f is bijective if it is both injective and surjective.

The composition of two injective functions is injective.
The composition of two surjective functions is surjective.
Cantor's theorem: If X and Y are sets and Y has at least two distinct elements,
then there is no surjective $f : X \to Y^X$. In particular, $\#X \neq \#Y^X$

4.3 Special functions

Indicator function: For any subset $A \subset X$ of a set define

$$\nVdash_A : X \to [2] \text{ by } \nVdash_A(x) = \begin{cases} 1 \text{ if } X \in A \\ 0 \text{ if } X \notin A \end{cases}$$

$$\nVdash_A * \nVdash_B = \nVdash_{A \cap B}$$

$\nVdash$ can translate set theory into numbers (and back)
The **identity function** outputs the input without changing it.
id_X is defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

4.4 Composition and inverse

$$(f \circ g)(x) = f(g(x))$$

If and only if f is **bijective** we can define its **inverse** $f_{-1} : B \to A$ by

$$f_{-1}(b) = a \text{ where } a \in A \text{ and } b \in B \text{ such that } f(a) = b$$

A function $f : X \to Y$ has an inverse if there exists a function $g : Y \to X$ such that

$$g \circ f = \mathrm{id}_X \text{ and } f \circ g = \mathrm{id}_Y$$

$f(a)$ is **ambiguous** and therefore $f(x)$ has no inverse if there are multiple solutions.
When composing multiple functions, no parentheses are needed.
The order of composed functions matters.
Repeated composition: $f^{(n)} = f \circ f \circ ... \circ f$ (n times)
If h and k are both inverses of f then $h = k$. (**uniqueness of inverse**)
If $f : X \to Y$ and $g : Y \to Z$ are functions then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
$\#f(X) = \#X$ iff f is invertible. $a^{(x^y)} \neq (a^x)^y$
Given $f : X \to Y$ and $B \subseteq Y$ define the **inverse image** of B to be $f^{-1}(B) = \{x \in X : f(x) \in B\}$
When you define an inverse, also prove that it's an inverse.

5 Integers

This class is about the set of positive and negative integers $\mathbb{Z}$.
Because it is ambiguous whether $\mathbb{N}$ starts at 0 or 1, we use $\mathbb{Z}_{>0}$ and $\mathbb{Z}_{\geq 0}$.
Arithmetic operations can be expressed as a function $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

5.1 Divisibility

Notation: for $a, b \in \mathbb{Z}$, we write $a|b$ iff $b = ac$ for some $c \in \mathbb{Z}$. It is a statement, not a number.
The opposite of this is $a \nmid b$, where there does not exist such a number c.

Properties of divisibility for $a, b, c \in \mathbb{Z}$:

- $a|a$, $0|0$, $a|0$, $1|a$
- If $a|b$ then $a|bc$ for any c.
- If $a|b$ and $b|c$ then $a|c$.
- If $a|b$ and $a|c$ then $a|(b - c)$ and $a|(b + c)$.
- If $a|b$ and $a|c$ then $a|(br - cs)$ for every $r, s \in \mathbb{Z}$.
- $\{c \in \mathbb{Z} : a|c\} = a\mathbb{Z}$ is the set of **multiples** of a.
- $\{c \in \mathbb{Z} : c|b\} = \mathrm{Dvs}(b)$ is the set of **divisors** of b.

Properties of the set of divisors:

- $\mathrm{Dvs}(b)$ is a finite set if $b \neq 0$.
- $-b, -1, b, 1 \in \mathrm{Dvs}(b)$
- $\mathrm{Dvs}(b)$ is infinite $\iff b = 0$
- $\#\mathrm{Dvs}(b) = 2 \iff b = \pm 1$
- for $b \neq 0$, $2|\#\mathrm{Dvs}(b)$

A **prime number** is an integer $p > 0$ such that $\#\mathrm{Dvs}(p) = 4$

Take a pair $a, b \in \mathbb{Z}$ such that $(a, b) \neq (0, 0)$. $\mathrm{Dvs}(a) \cap \mathrm{Dvs}(b)$ is a nonempty finite set.
The greatest number in this set is the **greatest common divisor** $\gcd(a, b)$.

5.2 Division with remainder

If $a, b \in \mathbb{Z}$ and $b \neq 0$ then $q, r \in \mathbb{Z}$ exist such that $0 \leq r < |b|$ and $a = q * b + r$.
Moreover, for given a, b these q, r are unique. If $b > a$, then $q = 0$ and $r = a$.
Euclid's Algorithm for calculating gcd's:

1. $\gcd(a, b) = \gcd(|a|, |b|)$
2. $\gcd(|a|, 0) = |a|$
3. if $a = qb + r$ for integers q, r, then $\gcd(a, b) = \gcd(r, b)$

We define the **sum of multiples** as $\mathbb{Z}a + \mathbb{Z}b = \{xa + by : x, y \in \mathbb{Z}\}$
Bézout's theorem: If $a, b, q, r \in \mathbb{Z}$ such that $a = qb + r$ then $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z} = \gcd(a, b)\mathbb{Z}$
If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$. If $a|c$ and $b|c$ and $\gcd(a, b) = 1$, then $ab|c$. $p \in \mathbb{Z}_{\geq 2}$ is prime $\iff$ for all $a, b \in \mathbb{Z}$, if $p|ab$, then $p|a$ or $p|b$
$\gcd(a, b)$ can be written as $ax + by$ where $x, y \in \mathbb{Z}$.
If p is prime, if $p|a$ then $\gcd(p, a) = p$ and if $p \nmid a$ then $\gcd(p, a) = 1$
If $\gcd(a, b) = 1$ we say a and b are **relatively prime** or **coprime**.

The **extended Euclidean algorithm** is used to find x, y and $\gcd(a, b)$ such that $ax+by = \gcd(a, b)$.
Example with $a = 49$ and $b = 10$:

$$\begin{aligned}
0 * 10 + 1 * 49 &= 49 && \textcircled{1} \\
1 * 10 + 0 * 49 &= 10 && \textcircled{2} \\
-4 * 10 + 1 * 49 &= 9 && \textcircled{3} = \textcircled{1} - 4 * \textcircled{2} \\
5 * 10 - 1 * 49 &= 1 && \textcircled{4} = \textcircled{2} - \textcircled{3} \\
1 * 9 - 9 * 1 &= 0 && \textcircled{5} = \textcircled{3} - 9 * \textcircled{4}
\end{aligned}$$

For each step n except the first two, we subtract $n - 1$ from $n - 2$ a certain amount of times to get the positive integer on the right side of the equation as low as possible. The algorithm terminates when it reaches 0, where the second to last equation is $x * a + y * b = \gcd(a, b)$

5.3 Fundamental theorem of arithmetic

P is the set of prime numbers $\{n : n \in \mathbb{Z}_{\geq 0}$ and $\#\,\mathrm{Dvs}(n) = 4\}$
and $\xi = \{e : P \to \mathbb{Z}_{\geq 1} : e(p) = 0$ for all $p \in P$ bigger than some bound$\}$
Given $e \in \xi$, the product $\prod\limits_{p \in P} p^{e(p)}$ is well-defined and it is in $\mathbb{Z}_{\geq 1}$.
Define $\varphi = \xi \to \mathbb{Z}_{\geq 1}$ by $\varphi(e) = \prod\limits_{p \in P} p^{e}(p) \in \mathbb{Z}_{\geq 1}$.
By the **fundamental theorem of arithmetic** the function φ is bijective.
Simple version: every positive integer can be written as a unique product of primes.

6 Modular arithmetic

We construct an equivalence relation on $\mathbb{Z}$ based on a fixed b: $a \sim_b c$ iff $b|a - c$
The set of equivalence classes for $\sim_b$ is called $\mathbb{Z}/b\mathbb{Z}$.
The equivalence class of $a \in \mathbb{Z}$ we denote by $a \bmod b$ or $\overline{a}$.
By definition, $a \bmod b = \{c \in \mathbb{Z} : c \sim_b a\} = \{c \in \mathbb{Z} : b|(c - a)\} = a + b\mathbb{Z}$

Consider $\overline{a}, \overline{c} \in \mathbb{Z}/b\mathbb{Z}$. If $x_1, x_2 \in \overline{a}$ and $y_1, y_2 \in \overline{c}$, then

$$\overline{x_1 y_1} = \overline{x_2 y_2} \qquad \overline{x_1 + y_1} = \overline{x_2 + y_2}$$

Several divisibility tricks can be derived from these properties.
Equations mod b can be simplified by replacing numbers with a simpler representative of their class.
If $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$ is odd, then $(a+b)|(a^n + b^n)$

6.1 Units

Definition: $\overline{a} \in \mathbb{Z}/b\mathbb{Z}$ is called a **unit** if some $\overline{c} \in \mathbb{Z}/b\mathbb{Z}$ exists s.t. $\overline{a} * \overline{c} = \overline{1}$.
There exists precisely 1 such $\overline{c}$. $\overline{a}^{-1}$ denotes the unique $\overline{c}$ such that $\overline{a} * \overline{c} = \overline{1}$.
The subset of $\mathbb{Z}/b\mathbb{Z}$ containing all units is denoted by $(\mathbb{Z}/b\mathbb{Z})^{\times}$.
$\#(\mathbb{Z}/b\mathbb{Z})^{\times}$ we write as $\phi(b)$ (**Euler's totient function**) $(\mathbb{Z}/0\mathbb{Z})^{\times} = \{\overline{1}, \overline{-1}\}$
$\overline{a} \in \mathbb{Z}/b\mathbb{Z}$ is a unit iff a and b are relatively prime. ($\gcd(a,b) = 1$)
Inverses can be computed using $ax + by = 1$ where $\overline{x}^{-1} = \overline{y}$

Fermat's little theorem $a^p \equiv a \mod p$ $a^{p-1} \equiv 1 \mod p$
Euler's theorem Given $n \in \mathbb{Z}$ and $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $\overline{a}^{\Phi(n)} = \overline{1}$ and $n|(a^{\Phi(n)} - 1)$
If n is prime, $n|a^{n-1} - 1$ whenever p does not divide a.
If and only if every prime number $p|n$ divides n only once , $n|a^{\Phi(n)+1} - a$

6.2 Linear equations

In $\mathbb{Z}/n\mathbb{Z}$: given $\overline{a}, \overline{b}$, find (if exists) x such that $\overline{a}x = \overline{b}$
m_a is the map "multiplied by a" m_a is injective $\iff$ m_a is surjective
If $m_{\overline{a}}(\overline{b}) = 1$, $\overline{a}$ is a unit, the map is invertible and $\overline{a}x = \overline{b}$ has a unique solution.
Otherwise, some $\overline{b}$'s have no solutions and some $\overline{b}$'s have multiple solutions.
$ax = b \mod n \iff n|ax - b \iff kn|k(ax - b)$

6.3 Hill cipher

A matrix or vector mod b has all of its entries mod b.
A matrix mod b has an inverse if its determinant is a unit.
Inverse matrix mod b using adjoint: $A^{-1} = A_{adj} * (\det A)^{-1}$

Application: $n = 26$, agree on a secret matrix A s.t. $\det A$ is a unit, and some secret $\boldsymbol{t} \in (\mathbb{Z}/26\mathbb{Z})^k$.
$x \to Ax + \boldsymbol{t}$ is the **Hill cipher** to encode messages.
The Hill cipher can be decoded by solving the system of linear equations $Ax + \boldsymbol{t}$
which may require elementary row operations to turn coefficients into units.

6.4 RSA

1. Take two secret distinct prime numbers p, q.
2. Make $n = pq$ public.
3. $\Phi(n) = (p-1)(q-1)$, which is kept secret.
4. Choose an $e \geq 1$ such that $\gcd(\Phi(n), e) = 1$
5. Compute a secret d which is the inverse of $e \mod \Phi(n)$
6. Encode messages $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ by raising to the power e
7. Decode messages $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ by raising to the power d