

# TITLE HERE

AUTHOR NAME HERE  
SEMINAR NAME HERE (SEMESTER HERE)  
DATE HERE

ABSTRACT HERE, i.e., a short summary of your topic.

## 1 A section

Some text in a section.

## An unnumbered section

This section, unlike section 1 is not numbered. This is indicated by the “\*”, i.e., `\section*` instead of `\section`. Such “starred” and “unstarred” variants also exist for many environments (and commands). There are subsections, subsubsections and paragraphs (and subparagraphs) for more fine-grained subdivision.

### A subsection

Some text.

### A subsubsection

More text.

**A paragraph** Even more text.

## 2 Important hint

If you don’t know  $\text{\LaTeX}$ , how to use math mode, environment, and so on, a short tutorial/introduction will be more useful than this document. This document is only a reminder of some basic  $\text{\LaTeX}$  stuff. Not the absolute basics, and nothing advanced.

Furthermore, use a **suitable editor**. This will make using  $\text{\LaTeX}$  *much* easier.

## 3 Basic usage of L<sup>A</sup>T<sub>E</sub>X

### 3.1 \newcommand for shorthands

Using `\newcommand{\cmdname}{output}` you can define shorthands, e.g., `\IN` for natural numbers  $\mathbb{N}$ , and so on. See the preamble. Much more than mere text insertion is possible. See (advanced) L<sup>A</sup>T<sub>E</sub>X introductions.

### 3.2 Lists

Use `itemize`, `enumerate` or `description` for lists. For example `itemize`:

- This is the first item
- Now comes the second item

For example `enumerate`:

1. This is the first item
2. Now comes the second item

For example `description`:

**First item:** This is the first item

**Other stuff:** Now comes the second item

### 3.3 Math environments

Use *inline* math mode (i.e., tex code in  $\$$ 's) for inline math, e.g.,  $\lim_{x \rightarrow 1} e^{2\pi i x} = 1$  or  $\alpha\beta = \Gamma$ . Use the `equation*` environment (or `\[` and `\]`) for math in *display* mode, e.g.,

$$\lim_{x \rightarrow 1} e^{2\pi i x} = 1.$$

If you use `equation` you get numbered equations which you can reference to (see section 3.5).

$$|x| = \begin{cases} -x & \text{if } x < 0 \\ x & \text{otherwise} \end{cases} \quad (1)$$

Proofs, Definition, Lemmata, Propositions, Theorems, Remarks, etc, have their own environments. Environments can be changed/redefined and new ones can be defined.

**Definition 1** (Negligible function). Let  $f: \mathbb{N} \rightarrow \mathbb{R}$  be a function. If for any  $k > 0$ , it holds that  $f(x)x^k \rightarrow 0$  for  $x \rightarrow \infty$ , then we call  $f$  *negligible*.

*Remark 2.* Writing  $g: X \rightarrow Y$  looks good, while  $g: X \rightarrow Y$  treats “:” as a *division*, and looks strange. So use `\colon` if you need a colon in math mode.

**Lemma 3.**  $f(x) = 0$  is a negligible function.

**Proposition 4.** If  $f$  and  $g$  are negligible functions, then  $f + g$  is a negligible function.

The following theorem has a proof included.

**Theorem 5** (The ring of negligible functions). *The set of negligible functions is closed under addition, subtraction and multiplication.*

*Proof.* This is just an application of theorems about limits of series and induction. For example,  $0 = 0 + 0 = \lim_{x \rightarrow \infty} f(x)x^k + \lim_{x \rightarrow \infty} g(x)x^k = \lim_{x \rightarrow \infty} (f(x) + g(x))x^k$  and

$$0 = 0 \cdot 0 = \lim_{x \rightarrow \infty} f(x)x^k \lim_{x \rightarrow \infty} f(x)g(x)x^k = \lim_{x \rightarrow \infty} (f(x)g(x))x^{2k}$$

□

**Corollary 6.** *Working with negligible functions is easy.*

*Remark 7.* If  $f$  is *not* negligible, this does *not* imply that  $|f(x)| \geq x^{-k}$  always. This needs to hold for infinitely many  $x \in \mathbb{N}$  (and  $k > 0$ ). E.g.,  $f(x) = 1 - (-1)^x$  is not negligible.

There are a lot more useful things for math layout, e.g., `align` and `aligned` environments for equations, and so on.

### 3.4 Font choices (for algorithms etc.)

It is important to use math mode “correctly”. Typed letters are interpreted as individual symbols, even if they are not separated by whitespace. For example *CTR* looks strange, so use *CTR* or CTR instead, which treats “CTR” as one word. The command `\mathit` uses italics, while `\mathrm` does not. There are also `\mathcal` for calligraphic (e.g.  $\mathcal{B}$ ), and `\mathsf` for sans-serif (e.g.  $\mathsf{Sans}$ ), and `\mathbb` for blackboard bold (e.g.  $\mathbb{N}$ ), and `\mathtt` for monospaced (e.g. `typewriter`), and so on.

It is a good idea *not to* use these macros everytime, but to define new macros instead, which carry the *semantics*. E.g. defining a macro `\IN` which prints  $\mathbb{N}$ . This is easier to type, read, and change. See the preamble for some predefined examples.

Oftentimes, `\mathsf` is used to typeset algorithms. Following the advice above, the preamble defines a `\mathalgofont` macro, which is used in the definitions of `\Gen`, `\Enc`, `\Dec`. Thus, changing `\mathalgofont`, affects all (three) macros, ensuring consistency.

*Example 8.* This shows the difference suitable macros make:

1.  $(Gen, Enc, Dec)$  is correct if for all  $k \leftarrow Gen()$  and all messages  $m$ , we have  $Dec(k, Enc(k, m)) = m$ .
2.  $(Gen, Enc, Dec)$  is correct if for all  $k \leftarrow Gen()$  and all messages  $m$ , we have  $Dec(k, Enc(k, m)) = m$ .

### 3.5 References

To refer to a section, or any other “referrable” object, use the “ref” command. For example: Section 1 or Definition 1 or Eq. (1). The tilde  $\sim$  is an “unbreakable space”. (There are more advanced ways to do this, which are especially useful for longer documents. For example the “cleveref” package.)

### 3.6 Literature and BibTeX

To refer to literature, use BibTeX (which needs a bib-file) and run it (on the main document). The bibfile is set by `\bibliography{FILENAME}` in the preamble. The literature inserted by the `\printbibliography{}` command. (See the end of the document). A good source of (sample) bibfiles is <https://dblp.uni-trier.de>. Use `\cite{}` (e.g., [DH76] or [RSA78]) or variants (see Section 3.7).

### 3.7 Packages and the Internet

There is a huge supply of useful packages. For almost every problem, there's a package to solve it. Just use the Internet to find them. (Special mention: TikZ, cleveref, cryptocode)

Reading some short introduction/tutorial on L<sup>A</sup>T<sub>E</sub>X is also recommended. Because this document only scratches the surface: It does not have tables, pictures, splitting the document into multiple files, and so on. Good starting points are: Search engines, <https://en.wikibooks.org/wiki/LaTeX>, <https://tex.stackexchange.com>

### 3.8 Miscellaneous

To start a new paragraph, use either an empty line in the source tex file or the command `\par`.

Footnotes work via the `\footnote{}` command.<sup>1</sup>

---

<sup>1</sup>This is a footnote.