

## Notations and symbols

$A := B$	$A$ is defined by $B$ ( $B =: A$ as well).
$\forall \dots,$	For any $\dots$ ,
$\exists \dots,$	There exists $\dots$ ,
$P \implies Q$	$P$ implies $Q$ (logical inclusion).
$P \iff Q$	$P$ and $Q$ are equivalent.
s.t.	such that
$\square$	end of proof.
$\mathbb{N} := \{0, 1, 2, \dots\}$ ,	0 and natural numbers.
$\mathbb{N}^+ := \{1, 2, \dots\}$ ,	the set of all positive integers.
$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ ,	the set of all integers.
$\mathbb{R} :=$	the set of all real numbers.
$\mathbb{C} :=$	the set of all complex numbers.
$\lfloor t \rfloor :=$	the largest integer not exceeding real number $t$ (rounding down).
$\lceil t \rceil :=$	the smallest integer no less than real number $t$ (rounding up).
$\mathbf{1}_B(x) :=$	the indicator function of set $B = \begin{cases} 1 & (x \in B), \\ 0 & (x \notin B). \end{cases}$
$\#B :=$	the number of elements of set $B$ .
$2^B :=$	the set of all subsets of $B$ .
$B^c :=$	the complementary set to $B$ .
$A \setminus B := A \cap B^c$ .	
$\emptyset :=$	the empty set.
Pr	probability (when no probability space is explicitly specified).
$\mathbf{E}[X] :=$	the mean (expectation) of random variable $X$ .
$\mathbf{E}[X; B] := \mathbf{E}[X\mathbf{1}_B]$ .	
$\mathbf{V}[X] :=$	the variance of random variable $X$ .
$\mathcal{N}(m, \sigma^2) :=$	the normal (Gaussian) distribution with mean $m$ and variance $\sigma^2$ .
$O(f(n)) :=$	Landau's symbol,
	$g(n) = O(f(n)) \iff \exists c > 0$ s.t. $ g(n)  \leq cf(n)$ .
$\mathbf{0} :=$	zero. This is used mainly in Chapter 6 to distinguish the number “0” from the letter “O”.
$a \bmod N :=$	$a$ modulo $N$ , the remainder, on division of $a$ by $N$ .
	When $N = 1$ , it means the fractional part of $a$ .