Maths Reference Sheet

Manuscript version: *#5fb3f8* - 2024-11-04 17:27:43Z

These pages also include a few symbols and phrases not used in this module but which you might see elsewhere, including words and phrases used in the course of writing proofs. Terms are divided up by topic rather than by lecture, so there are occasional repetitions. Summary definitions are given, consult the lectures or notes for full definitions of the techical terms.

Basic logic and proof terminology

$\forall$	'for all'
$\exists$	'there exists'
$\forall x \in X.$	'for all x which are in the set X'
$\wedge$	'and'
$\vee$	'or'
$\neg$	'not', 'it is not the case that'
$\implies, \to$	'implies'. ' $\implies$ ' is also shorthand for 'which implies' or 'therefore'.
$\impliedby$	'(is) implied by'
$\iff$, iff	'if and only if'. $A \iff B$ is equivalent to $(A \implies B) \wedge (B \implies A)$
necessary condition (for A)	a proposition B such that $A \implies B$
sufficient condition (for A)	a proposition B such that $B \implies A$
necessary and sufficient condition (for A)	a proposition B such that $A \iff B$
$\therefore$	shorthand for 'therefore'.
$\because$	shorthand for 'because'.
WLOG	'without loss of generality' (proving a special case without losing the general case).
RTP	'required to prove' (written before a reminder of what needs to be proved)
STP	'sufficient to prove' (written before stating something which implies what we needed to prove)
s.t.	'such that'
w.r.t.	'with respect to'
$\square$, QED	marks the end of a proof
by hypothesis	'by an assumption given in the statement of the proposition'
induction	Proof method for statements of the form $\forall n \in \mathbb{N}.\Phi(n)$ or similar.

weak induction	Induction with a base case $\Phi(0)$ and inductive step $\Phi(k) \implies \Phi(k+1)$.
strong induction	Induction with only an inductive step $(\forall k < n.\Phi(k)) \implies \Phi(n)$.
IH, induction hypothesis	The assumption made for the inductive step of a proof by induction, so $\Phi(k)$ for weak induction and $\forall k < n.\Phi(k)$ for strong induction.

Sets

$\{x \mid \Phi(x)\}$	The set of all things x such that $\Phi(x)$ is true. So $a \in \{x \mid \Phi(x)\}$ iff $\Phi(a)$ is true.
$\{x \in A \mid \Phi(x)\}$	As above, but only those x which are also in A.
$\{x \subseteq X \mid \Phi(x)\}$	As before, except restricting to those x which are also subsets of X.
$\{x \leq 100 \mid \Phi(x)\}$	Another of many possible variations of the above.
$x \in X$	x is an *element* (or *member*) of the set X.
$A \subseteq B$	A is a *subset* of B: $\forall x.\, x \in A \implies x \in B$.
$A \subsetneq B$	A is a *proper* (or *strict*) subset of B: $A \subseteq B$ but also $A \neq B$.
$A \supseteq B$	A is a *superset* of B. Equivalent to $B \subseteq A$.
$\emptyset$, $\varnothing$, $\{\}$	Notations for the *empty set*.
$X \times Y$	The set of *ordered pairs* (x, y) where $x \in X$ and $y \in Y$.
X^2	$X \times X$ (special case of the above)
X^n	$\underbrace{X \times \ldots \times X}_{n}$, the product of X with itself n times. The elements of this set are the *n-tuples* $(x_1, x_2, \ldots, x_n)$ where all the $x_i \in X$.
Y^X	The set of *functions* $X \to Y$
$X \cup Y$	The *union* of X and Y.
$\bigcup_{i \in I} X_i$	The union of the family of the family of sets $(X_i \mid i \in I)$.
$X \cap Y$	The *intersection* of X and Y.
$\bigcap_{i \in I} X_i$	The intersection of the family of the family of sets $(X_i \mid i \in I)$.
$P(X)$	The *powerset* of X, the set of all subsets of X.
$X \backslash A$	The *set difference*: the set $\{x \in X \mid x \notin A\}$.
$X \triangle Y$	The *symmetric difference*: the set $\{x \mid x \in X \texttt{ XOR } x \in Y\}$.
disjoint	When $A \cap B = \emptyset$.
finite	there is a bijection with a set $\{x \in \mathbb{N} \mid x < n\}$ for some $n \in \mathbb{N}$
infinite	not finite, equivalently, admits an injection from $\mathbb{N}$
countable	finite or there is a bijection with $\mathbb{N}$, equivalently, injects into $\mathbb{N}$
countably infinite	countable and infinite, equivalently, bijects with $\mathbb{N}$
uncountable	not countable
$\lvert X\rvert = \lvert Y\rvert$	when X and Y are sets, means that there is a bijection between them
$\lvert X\rvert \leq \lvert Y\rvert$	when X and Y are sets, means that there is an injection $X \to Y$

cardinality	the ‘equivalence class’ of a set under the ‘equivalence relation’ $\lvert X\rvert = \lvert Y\rvert$.
$\{0,1\}^*$	The set of binary strings, finite lists of 0’s and 1’s.
$\{0,1\}^{\mathbb{N}}$	The set of binary streams, infinite lists of 0’s and 1’s, formally just functions $\mathbb{N} \to \{0,1\}$.

Numbers

$\mathbb{N}$	The set of natural numbers $0, 1, 2, 3, \ldots$
$\mathbb{Z}$	The set of integers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$\mathbb{Z}_m$	The set of residue classes modulo m. Nearly always, working with $\mathbb{Z}_m$ is equivalent to working with $x \equiv y \pmod{m}$
$\mathbb{N}^+$, $\mathbb{Z}_{\neq 0}$, $\mathbb{R}_{\geq 0}$	Non-standard variations on the above sets, should always be explained when they are used.
$x + y$	AKA sum, addition, plus
$x \times y$, xy	AKA product, multiplication, ‘times’, (very occasionally $x.y$ or $x \cdot y$)
$x - y$, $x + (-y)$	AKA difference, subtraction, minus
$x \div y$, x/y, $\frac{x}{y}$	AKA quotient, division, ‘x over y’ (N.B. ‘quotient’ should not be confused with `div`)
associativity	The algebraic property of sum (and product) that allows re-bracketing.
commutativity	The algebraic property of sum (and product) that allows re-ordering.
distributivity of $\times$ over $+$	The algebraic law corresponding to ‘multiplying out’ and ‘factorizing’.
neutral element	(AKA ‘identity element’) e.g. 0 is neutral for $+$ because $0 + x = x = x + 0$, and 1 is neutral for $\times$.
negative, $-x$	defined by $x + (-x) = 0$ (‘additive inverse’), allows defining $a - b = a + (-b)$
reciprocal, x^{-1}, $\frac{1}{x}$	defined by $x \times x^{-1} = 1$ (‘multiplicative inverse’), allows defining $a \div b = a \times b^{-1}$
field	A ‘number system’ with $+$ and $\times$, satisfying the usual algebraic laws, where all elements have a negative, and all non-zero elements have a reciprocal, (and also $0 \neq 1$).
$x \leq y$	x is less than or equal to y
$x < y$	x is less than y. So both $x \leq y$ and also $x \neq y$.
positive	(strictly) greater than 0.
$x = \pm y$	Shorthand for “$x = y$ or $x = -y$”.

Integers

$\mathbb{N}$	The set of natural numbers $0, 1, 2, 3, \ldots$
$\mathbb{Z}$	The set of integers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
$a \mid b$	'a divides b', 'a is a divisor of b', 'b is a multiple of a'. Equivalent to $b \equiv 0 \pmod{a}$.
$a \nmid b$	Negation of the above.
prime number	An integer $p \in \mathbb{N}$ with $p > 1$ and whenever $d \mid p$ then $d = \pm 1$ or $\pm p$.
prime factorization	Writing an integer $n \geq 1$ has a product of prime numbers (the empty product is allowed).
$b \,\mathtt{div}\, a$, $b \,\mathtt{mod}\, a$	When $a \neq 0$, you can write $b = (b \,\mathtt{div}\, a)a + (b \,\mathtt{mod}\, a)$ where $0 \leq (b \,\mathtt{mod}\, a) < a$. (Note the typewriter font to help distinguish `mod` from $(\mathrm{mod}\ m)$).
$x \equiv y \pmod{m}$	'x is congruent to y modulo m'. Equivalent to $x \,\mathtt{mod}\, m = y \,\mathtt{mod}\, m$, and to $m \mid (x - y)$.
residue	'remainder'. $b \,\mathtt{mod}\, a$ is the *residue* of b modulo a.
$[i]_m$	The residue class of i modulo m (a special name and notation for the equivalence class of i under the equivalence relation $(\mathrm{mod}\ m)$).
$\gcd(x, y)$	The *greatest common divisor* of x and y.
coprime	When the greatest common divisor is 1.
$r_0, r_1, \ldots$	Notation used in this module for the residue terms appearing in Euclid's algorithm.
coefficient	A number that multiplies another (more important) number in some expression. E.g. "3 is coefficient of x in $x^2 + 3x + 5$".
Bézout coefficients	The x and y in the expression $xa + yb = \gcd(a, b)$ given by Bézout's Lemma.

Reals and rationals

$\mathbb{Q}$	The set of rational numbers. Numbers which can be written as a fraction (ratio) $\frac{x}{y}$ with $x, y \in \mathbb{Z}$ (and $y \neq 0$).
numerator	The x in $\frac{x}{y}$.
denominator	The y in $\frac{x}{y}$.
reduced fraction	An fraction $\frac{x}{y}$ where x and y are coprime ($\gcd(x, y) = 1$), and moreover $y > 0$ (N.B. many other sources do not include $y > 0$ as part of the definition, but we do in order to get uniqueness of reduced fractions).
$\mathbb{R}$	The set of real numbers. Numbers which are 'on the number line'. Numbers which can be written as a (possibly infinite) decimal expansion such as $3.14159\ldots$.
irrational	A real number which is not a rational number. E.g. $\sqrt{2}$.
square root (of x)	A number y such that $y^2 = x$.
$\sqrt{x}$	The unique non-negative square root of x.
interval	A subset of the reals of the form $[a, b]$, (a, b), $(a, b]$, $[a, b)$, (or a special variant with ∞ or $-\infty$).

$[a, b]$	A *closed* interval (the endpoints a and b are included in the subset).
(a, b)	An *open* interval (the endpoints a and b are *not* included in the subset).
interval bisection	A method of finding (approximations to) a real number α where: you know that $\alpha \in [a_n, b_n]$, then you check whether α is in $[a_n, c_n]$ or $[c_n, b_n]$ where $c_n = \frac{1}{2}(a_n + b_n)$.

Relations

Relation from X to Y	A subset of $X \times Y$.
Relation on X	A relation from X to X. A subset of $X \times X$. This is the default situation when talking about relations rather than functions.
$x\ R\ y$	Notation for $(x, y) \in R$.
reflexive	$x\ R\ x$
symmetric	$x\ R\ y \implies y\ R\ x$
transitive	$x\ R\ y \wedge y\ R\ z \implies x\ R\ z$
equivalence relation	reflexive + symmetric + transitive
$[x]_R$, equivalence class	The equivalence class of x is the set $[x]_R$ of all $y \in X$ such that $x\ R\ y$.
$[x]$	The equivalence class of x, omitting the subscript R is obvious from context.
partition	Dividing X up to into disjoint, non-empty subsets. There is a correspondence between equivalence relations on X and partitions of X.
antisymmetric	$x\ R\ y \wedge y\ R\ x \implies x = y$. Equivalently, $x \neq y \implies \neg(x\ R\ y \wedge y\ R\ x)$.
partial order	reflexive + antisymmetric + transitive
total order	partial order + $\forall x, y \in X.\, x\ R\ y \vee y\ R\ x$.

Functions

function from X to Y	Informally, an assignment of an output in Y to every input in X. Formally, a relation from X to Y (subset of $X \times Y$) satisfying two conditions.
$f : X \to Y$	'f is a function from X to Y'.
$x \mapsto E$	'maps to' arrow. Describes what a function does to an input value x by giving an expression E for the output value.
$\mathsf{id}_X : X \to X$	The *identity* function on X, given by $x \mapsto x$
domain	The X in $f : X \to Y$.
codomain	The Y in $f : X \to Y$.
$f[X]$, image, range	The set of $y \in Y$ which get something in X mapped to them.
$f^{-1}(B)$, preimage	For $B \subseteq Y$, the set of x's sent to an output in B.
$f \restriction_A$, $f\vert_A$	The *restriction* of f to a subset $A \subseteq X$.
$g \circ f$	The *composite* of $f : X \to Y$ and $g : Y \to Z$.

injection	A function which sends different inputs to different outputs.
surjection	A function which hits every possible output in the codomain.
bijection	A function which is both an injection and surjection.
f^{-1}, inverse function	If $f : X \to Y$, then f^{-1} is a function $Y \to X$ with $f(f^{-1}(y)) = y$ and $f^{-1}(f(x)) = x$. There is an inverse function for f iff f is a bijection.
inclusion	When $A \subseteq X$, there is a function $A \to X$ where $x \mapsto x$.
χ_A	The *characteristic function* of a subset $A \subseteq X$. $\chi_A : X \to \{0, 1\}$ sends x to 1 iff $x \in A$.