List of potentially useful facts and definitions (you may remove this page)

Propositional logic

Basic logical operations:
Negation: $\neg P$ ("not P")
Conjunction: $P \wedge Q$ ("P and Q")
Disjunction: $P \vee Q$ ("P or Q")
Conditional: $P \to Q$ ("if P then Q")

Basic logical equivalences:
$P \to Q \equiv \neg P \vee Q$
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
$P \vee \neg P \equiv T$, $P \wedge \neg P \equiv F$
$P \vee T \equiv T$, $P \wedge T \equiv P$, $P \vee F \equiv P$, $P \wedge F \equiv F$
$P \to Q \equiv \neg Q \to \neg P$

Quantifiers:
Universal ("for all"): $\forall x \in U, P(x)$
Existential ("there exists"): $\exists x \in U : P(x)$
Negtation: $\neg(\forall x \in U, P(x)) \equiv \exists x \in U : \neg P(x)$
$\neg(\exists x \in U : P(x)) \equiv \forall x \in U, \neg P(x)$

Sets and set operations

Membership: $x \in A$ (x belongs to A)
Subset: $A \subseteq B$, if $\forall x \in U, x \in A \to x \in B$.
Equality: $A = B$ if $A \subseteq B$ and $B \subseteq A$
Empty set: the set $\emptyset$ containing no elements.
Power set: $\mathcal{P}(A) = \{B \subseteq U : B \subseteq A\}$
Union: $A \cup B = \{x \in U : x \in A \vee x \in B\}$
Intersection: $A \cap B = \{x \in U : x \in A \wedge x \in B\}$
Complement: $A^c = \{x \in U : x \notin A\}$
Set difference: $A \setminus B = \{x \in A : x \notin B\}$
Product: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

$\bigcup_{\alpha \in I} A_\alpha = \{x \in U \mid \exists \alpha \in I : x \in A_\alpha\}$
$\bigcap_{\alpha \in I} A_\alpha = \{x \in U \mid \forall \alpha \in I, x \in A_\alpha\}$

Basic set equalities:
$(A \cup B)^c = A^c \cap B^c$
$(A \cap B)^c = A^c \cup B^c$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup A^c = U$, $A \cap A^c = \emptyset$
$A \subseteq B$ if and only if $B^c \subseteq A^c$
$A \times (B \cup C) = (A \times B) \cup (A \times C)$
$A \times (B \cap C) = (A \times B) \cap (A \times C)$

Divisibility and congruence

Divides: $m|n$ iff $\exists k \in \mathbb{Z}$ such that $n = mk$.
Congruence: $a \equiv b \pmod{n}$ iff $n|(a - b)$.
Division algorithm: $m = nq + r$, $r \in \{0, 1, \ldots, n-1\}$

Functions

$f : A \to B$ – $\forall a \in A$ get *unique* $b = f(a) \in B$.
Domain: A Codomain: B
Range: $\text{ran}(f) = \{f(a) \mid a \in A\} \subseteq B$
Composition: given $f : A \to B$ and $g : B \to C$ get $g \circ f : A \to C$, $(g \circ f)(a) = g(f(a))$.
One-to-one: for all $a, b \in A$, $f(a) = f(b) \to a = b$.
Onto: $\text{ran}(f) = B$.
Bijection: f is both one-to-one and onto.
Inverse: if $f : A \to B$ is a bijection, define $f^{-1} : B \to A$ by $f^{-1}(b) = a$ if and only if $f(a) = b$.
Cancellation laws: $\forall a \in A, f^{-1}(f(a)) = a$, and $\forall b \in B, f(f^{-1}(b)) = b$.
Image: $f(C) = \{f(c) \mid c \in C\}$.
Preimage: $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.

Cardinality

Equivalence: $A \approx B$, if $\exists$ a bijection $f : A \to B$
Finite sets: $A \approx \{1, 2, \ldots, k\}$ for some $k \in \mathbb{N}$.
Infinite sets: any set that is not finite.
Cardinality: $|A| = k$ iff $A \approx \{1, 2, \ldots, k\}$.
$A \approx B$ iff $|A| = |B|$.
Pigeonhole principle: if $|A| > |B|$, any $f : A \to B$ is not one-to-one.
If A and B are finite and $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.
If A and B are finite then $|A \times B| = |A| \cdot |B|$.
A set A is **countable** if there exists a one-to-one function $f : A \to \mathbb{N}$. (Bijection if A infinite.)
The sets $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ are all countable.
The set $\mathbb{R}$ of real numbers is **uncountable**.

Mathematical induction

Proof by induction: to prove a statement of the form $\forall n \in \mathbb{N}, P(n)$, show that $P(1)$ is true and that for $k \geq 1$, $P(k) \to P(k+1)$.
Strong induction: Instead of only assuming $P(k)$ is true, assume that $P(1), P(2), \ldots, P(k-1), P(k)$ are all true for some k, and use this to show $P(k+1)$ is true. Note that you may need more than one base case.

Equivalence relations

Relation from A to B: a subset $R \subseteq A \times B$.
If $(a, b) \in R$ we write $a\,R\,b$.
Domain: $\{a \in A : a\,R\,b$ for some $b \in B\}$
Range: $\{b \in A : a\,R\,b$ for some $a \in A\}$
Reflexive: $a\,R\,a$ for all $a \in A$
Symmetric: $a\,R\,b \to b\,R\,a$ for all $a, b, \in A$
Transitive: $a\,R\,b \wedge b\,R\,c \to a\,R\,c$ for all $a, b, c \in A$.
Equivalence relation: reflexive, symmetric, and transitive.
Equivalence class: $[a] = \{b \in A \mid b\,R\,a\}$.
An example of an equivalence relation on $\mathbb{Z}$ is congruence modulo n.
Given $n \in \mathbb{N}$, we define $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ to be the set of equivalence classes with respect to congruence modulo n: $[a] = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$.
For any $[a], [b] \in \mathbb{Z}_n$, we define $[a] \oplus [b] = [a + b]$ and $[a] \odot [b] = [a \cdot b]$. These are the operations of **modular arithmetic**.