Lemma 1.1: For some set X and subsets $A, B \subseteq X$, if $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Proof. By contradiction, assume that $A \neq B$. Then, without loss of generality, there exists $x \in X$ such that $x \in A$ and $x \notin B$. But then it is not true that $A \subseteq B$. The contradiction assumption must therefore be false, i.e. $A = B$. □

Characteristic property

The elements of a subset $A \subseteq X$ can often be characterized by a mathematical property that they satisfy. This property is denoted $p(x)$, and we write

$$A = \{x \in X \mid p(x)\}.$$

For example, if $p(x) =$ 'x is even', then

$$A = \{x \in \mathbb{N} \mid x \text{ is even}\} = \{0, 2, 4, \ldots\} \subseteq \mathbb{N}.$$

Operations on sets

- **Complement**: if $A \subseteq X$ then we define its *complement* to be

$$A^C = \complement A = \{x \in X \mid x \notin A\}.$$

- **Union**: for two sets $A \subseteq X$ and $B \subseteq X$ we define their *union* to be

$$A \cup B = \{x \in X \mid x \in A \text{ or } x \in B\}$$

- **Intersection**: for two sets $A \subseteq X$ and $B \subseteq X$ we define their *intersection* to be

$$A \cap B = \{x \in X \mid x \in A \text{ and } x \in B\}$$

- **Difference**: for two sets $A \subseteq X$ and $B \subseteq X$ we define their *difference* to be

$$A \setminus B = \{x \in X \mid x \in A \text{ and } x \notin B\}$$

- **Symmetric Difference**: for two sets $A \subseteq X$ and $B \subseteq X$ we define their *symmetric difference* to be

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

- **Disjoint Union**: for two sets $A \subseteq X$ and $B \subseteq X$ whose intersection is empty, we often replace the symbol $\cup$ by

$$A \sqcup B \quad \text{or} \quad A \dot{\cup} B$$

Lemma 1.2 (Properties of $\cap$ and $\cup$)**:** For some set X and subsets $A, B, C \subseteq X$ the operations $\cap$ and $\cup$ satisfy:

1. Boolean properties: $A \cap A^C = \emptyset$ and $A \cup A^C = X$.
2. Commutativity: $A \cap B = B \cap A$ and $A \cup B = B \cup A$.
3. Associativity: $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$.
4. Distributivity: $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ and $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
5. De Morgan laws: $(A \cap B)^C = A^C \cup B^C$ and $(A \cup B)^C = A^C \cap B^C$.

Proof. We prove the first of the De Morgan laws. The rest is an exercise.

We want to show that two sets are the same: $(A \cap B)^C = A^C \cup B^C$. To do this, we will show that the set on the left is contained in (or equal to) the set on the right, and vice versa. I.e., we shall show that $(A \cap B)^C \subseteq A^C \cup B^C$ and $(A \cap B)^C \supseteq A^C \cup B^C$.

(i) To show that $(A \cap B)^C \subseteq A^C \cup B^C$, we note the following implications:

$$
\begin{aligned}
& x \in (A \cap B)^C \\
& \quad \Downarrow \\
& x \notin A \cap B = \{y \in X \mid y \in A \text{ and } y \in B\} \\
& \quad \Downarrow \\
& x \notin A \text{ or } x \notin B \\
& \quad \Downarrow \\
& x \in A^C \text{ or } x \in B^C.
\end{aligned}
$$

Since $A^C \subseteq A^C \cup B^C$ and $B^C \subseteq A^C \cup B^C$, we conclude that necessarily $x \in A^C \cup B^C$. Hence $(A \cap B)^C \subseteq A^C \cup B^C$.

(ii) Conversely, we can show $(A \cap B)^C \supseteq A^C \cup B^C$. Assume that $x \in A^C \cup B^C$ and *by contradiction*, assume that $x \notin (A \cap B)^C$. Then we have the implications:

$$
\begin{aligned}
& x \notin (A \cap B)^C \\
& \quad \Downarrow \\
& x \in A \cap B = \{y \in X \mid y \in A \text{ and } y \in B\} \\
& \quad \Downarrow \\
& x \in A \text{ and } x \in B \\
& \quad \Downarrow \\
& x \notin A^C \text{ and } x \notin B^C.
\end{aligned}
$$

But this is in contradiction to the assumption that $x \in A^C \cup B^C$. Therefore the contradiction assumption $x \notin (A \cap B)^C$ is not true, hence $x \in (A \cap B)^C$.

We have shown that $(A \cap B)^C \subseteq A^C \cup B^C$ and that $(A \cap B)^C \supseteq A^C \cup B^C$, so by Lemma 1.1 the two sets must be equal, completing the proof. ◻

Power set

For a given set X, we define its power set $\mathcal{P}(X)$ to be the set of all subsets of X:

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}.$$

In particular, $\emptyset \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$.

1.2 Elements of mathematical logic

The building blocks of mathematical logic are **formulas**, which can be either *true* or *false*. Here are some examples:

$$p = \text{'Blue is a color'}$$
$$q = \text{'15 is the square of a natural number'}$$
$$r = \text{'the number 3 belongs to the set } X\text{'}$$

Then p is true, q is false, and we have no way of knowing whether r is true or false without knowing something about the set X.

1.2.1 Connectives

Connectives are the tools to build new formulas from existing ones. We briefly mention them:

Logical negation $\neg p$ ('not p') is the negation of the formula p

Logical conjunction $p \wedge q$ ('p and q')

Logical disjunction $p \vee q$ ('p or q')

Logical implication $p \Rightarrow q$ ('p implies q' or 'if p, then q')

Logical equivalence $p \Leftrightarrow q$ ('p is logically equivalent to q')

Proof by contradiction

This formalism allows us to understand the notion of a proof by contradiction, which is summed up by the logical equivalence:

$$(p \Rightarrow q) \qquad \Leftrightarrow \qquad (p \wedge \neg q \Rightarrow \neg p)$$

1.2.2 Predicates

A **predicate** is a formula that depends on one or more variables. In fact, we have seen predicates before, when we called them 'characteristic properties'. Here are some more examples:

$$p(x) = \text{'}x\text{ is a prime number'}$$
$$q(y) = \text{'}y\text{ is the square of a natural number'}$$
$$r(x, y) = \text{'}x\text{ is divisible by }y\text{'}$$

1.2.3 Quantifiers

In a set X, for a given predicate $p(x)$ with $x \in X$, we can ask whether p is always true, or perhaps only sometimes. This is expressed mathematically as follows:

Universal quantifier: $\forall x,\ p(x)$ (we say 'for every x, $p(x)$ holds')

Existential quantifier: $\exists x,\ p(x)$ (we say 'there exists x, such that $p(x)$ holds')

Unique existential quantifier: $\exists! x,\ p(x)$ (we say 'there exists one and *only one* x, such that $p(x)$ holds')

Example 1.1: Suppose that, as above, $p(x)$ = 'x is a prime number'. If $X = \mathbb{N}$, then it is true that *there exists* $x \in X$ that is a prime number, i.e. $\exists x,\ p(x)$. However, it is *not true* that *every* $x \in X$ is a prime number. That is, $\neg(\forall x,\ p(x))$.

Example 1.2: Consider the predicate $p(x)$ = '$x^2 = x$'. If $X = \{1, 2, 3, \ldots\}$, then $1 \in X$ is the unique element in X for which $p(x)$ is true. That is, $\exists! x,\ p(x)$. On the set $Y = \{2, 3, 4, \ldots\}$ the predicate $p(x)$ is never true, i.e. $\neg(\exists x,\ p(x))$.

The notions of predicates and quantifiers allow us to formalize the idea of induction:

Theorem 1.3 (Principle of Induction)**:** Let $N \in \mathbb{N}$ and denote by $p(n)$ a predicate defined for every $n \geq N$, $n \in \mathbb{N}$. Suppose that the following hold:

1. $p(N)$ is true,
2. $\forall n \geq N, p(n) \Rightarrow p(n+1)$.

Then $p(n)$ is true for all integers $n \geq N$.

Proof. By contradiction, assume that $\exists n \geq N$ for which $p(n)$ is false. Then the set

$$F = \{n \in \mathbb{N} \mid n \geq N \text{ and } p(n) \text{ is false}\}$$

is not empty. Define $m \in F$ to be the smallest number in F. Then $p(m)$ is false. Therefore $m \neq N$ (recall that we know that $p(N)$ is true). So necessarily $m > N$, and it follows that $m - 1 \geq N$. By our definition of the number m, $p(m-1)$ must be true (otherwise $m - 1$ would have been the smallest number in F). But we know that $\forall n \geq N, p(n) \Rightarrow p(n+1)$. Taking $n = m - 1$ we get that $p(m-1) \Rightarrow p(m)$. But this is not true, since $p(m-1)$ is true while $p(m)$ is false. We have therefore reached a contradiction, so that $\neg(\exists n \geq N$ for which $p(n)$ is false), i.e. $\forall n \geq N, p(n)$ is true. □

Example 1.3 (Bernoulli inequality)**:** We claim that $\forall r \geq -1$, the *Bernoulli inequality*

$$(1+r)^n \geq 1 + nr, \qquad \forall n \in \mathbb{N},$$

holds. We prove this by induction. Here

$$p(n) = \text{`}(1+r)^n \geq 1 + nr\text{'}.$$

1. For $n = 0$, we have $(1+r)^0 = 1$ and $1 + 0 \cdot r = 1$ so that $(1+r)^0 \geq 1 + 0 \cdot r$ and therefore $p(0)$ is true.

2. Now assume that $p(n)$ is true. This is called the **induction assumption**. Let us show that $p(n+1)$ is true. Using the fact that $1 + r \geq 0$, we have

$$\begin{aligned}
(1+r)^{n+1} &= (1+r)(1+r)^n \\
&\geq (1+r)(1+nr) \qquad \textit{(here we use the induction assumption and that } 1 + r \geq 0\textit{)} \\
&= 1 + (n+1)r + nr^2 \\
&\geq 1 + (n+1)r. \qquad \textit{(since } nr^2 \geq 0\textit{)}
\end{aligned}$$

Hence $p(n+1)$ is true, and by the Principle of Induction (we usually just say '*by induction*') the Bernoulli inequality holds for all $n \in \mathbb{N}$.