1. Arithmetic modulo 2.

Let

\( b = \{0, 1\}. \)

(The \( b \) stands for *bits*.)

We define the binary operations \( + \) and \( \ast \) on \( b \) by the following tables:

\[
\begin{array}{c|c|c}
   a & b & a + b \\
   \hline
   0 & 0 & 0 \\
   0 & 1 & 1 \\
   1 & 0 & 1 \\
   1 & 1 & 0 \\
\end{array}
\quad
\begin{array}{c|c|c}
   a & b & a \ast b \\
   \hline
   0 & 0 & 0 \\
   0 & 1 & 0 \\
   1 & 0 & 0 \\
   1 & 1 & 1 \\
\end{array}
\]

We note that \( b \) is **field** with respect to these operations. One frequently writes

\[ ab \]

instead of \( a \ast b \).

We define the unary operation \( \sim \) on \( b \) by the following table.

\[
\begin{array}{c|c}
   a & \sim a \\
   \hline
   1 & 0 \\
   0 & 1 \\
\end{array}
\]

Note that \( \sim \) is the additive inverse in the field \( b \).

We define the binary operations \( \lor \) and \( \land \) on \( b \) by the following tables:

\[
\begin{array}{c|c|c}
   a & b & a \lor b \\
   \hline
   0 & 0 & 0 \\
   0 & 1 & 1 \\
   1 & 0 & 1 \\
   1 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|c|c}
   a & b & a \land b \\
   \hline
   0 & 0 & 0 \\
   0 & 1 & 0 \\
   1 & 0 & 0 \\
   1 & 1 & 1 \\
\end{array}
\]

Note that \( \land \) equals \( \ast \).

We define the binary operations \( \to \) and \( \leftrightarrow \) on \( b \) by the following tables:

\[
\begin{array}{c|c|c}
   a & b & a \to b \\
   \hline
   0 & 0 & 1 \\
   0 & 1 & 1 \\
   1 & 0 & 0 \\
   1 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|c|c}
   a & b & a \leftrightarrow b \\
   \hline
   0 & 0 & 1 \\
   0 & 1 & 0 \\
   1 & 0 & 0 \\
   1 & 1 & 1 \\
\end{array}
\]

Check that the following hold for \( a, b \in b \):

\[
\begin{align*}
   a \lor b &= ab + a + b; \\
   a \land b &= ab; \\
   \sim a &= a + 1; \\
   a \to b &= ab + a + 1; \\
   a \leftrightarrow b &= a + b + 1;
\end{align*}
\]
and that
\[ a \cdot b = \sim(\sim a \lor \sim b) \]
\[ a + b = \sim((\sim a \lor b) \lor (\sim \sim b \lor a)) \].

2. Truth functions.

Let \( X \) be a set disjoint from the set \( P \) consisting of the symbols
\[ \text{expr} \sim \lor \land \rightarrow \iff \]

**Proposition 2.1.** Suppose \( A \in p(X) \) and \( B \) results by replacing each occurrence of a member of \( X \) in \( A \) by a member of \( p(X) \). Then \( B \in p(X) \).

**Proof.** Just grow the tree parsing \( A \). □

**Theorem 2.1.** There is one and only way to assign to each \( A \in p(X) \) a function \( t_A : 2^X \rightarrow \{0, 1\} \) in such a way that
\[
(1) \quad t_{\sim A} = \sim t_A; \\
t_{A \lor B} = t_A \lor t_B; \\
t_{A \land B} = t_A \land t_B; \\
t_{A \rightarrow B} = t_A \rightarrow t_B; \\
t_{A \iff B} = t_A \iff t_B.
\]

whenever \( A, B \in p(X) \).

**Proof.** This is a straightforward consequence of the uniqueness of the parse tree for any \( A \in p(X) \) and our formulae for arithmetic modulo 2. □

**Definition 2.1.** We say \( A \in p(X) \) is a tautology if \( t_A(A) = 1 \) for all \( A \subset X \).

**Definition 2.2.** Suppose \( \Gamma \subset p(X) \) and \( B \in p(X) \) We write
\[
\Gamma \models B
\]

and say \( B \) is a tautological consequence of \( \Gamma \) if whenever \( T \subset X \)
\[
t_A(T) = 1 \text{ for all } A \in \Gamma \Rightarrow t_B(T) = 1.
\]

**Example 2.1.** Suppose \( A, B \in p(X) \). Then
\[
\{A, (A \rightarrow B)\} \models B.
\]

Indeed, suppose \( T \subset X \), \( t_A(T) = 1 \) and \( t_{(A \rightarrow B)}(T) = 1 \).
To see this, consider the table
Here is another way:

\[ 1 = t_A(T)t_{(A \rightarrow B)}(T) = t_A(T)(t_A(T)t_B(T) + t_A(T) + 1) = t_B(T) + 1 + 1 = t_B(T). \]