FIGURE 3.2 Common propositional-logic tautologies

$$p \vee \neg p$$
$$p \equiv (\neg\neg p)$$
$$p \supset (q \vee p)$$
$$p \supset (q \supset p)$$
$$(p \wedge q) \supset p$$
$$\neg(\neg p \wedge p)$$
$$p \supset (q \supset (p \wedge q))$$
$$(p \wedge q) \supset (p \supset q)$$
$$(p \wedge q) \supset (q \wedge p)$$
$$(p \equiv q) \supset (p \supset q)$$
$$((p \vee q) \wedge \neg p) \supset q$$
$$((p \supset q) \wedge (q \supset r)) \supset (p \supset r)$$

(i.e., *derives*) various formulas on a piece of paper. Each rule states that, if all the premises of an inference rule have already been written down (derived), then the conclusion can also be written down (derived). Axioms can always be written down.

We return to this notion of derivations in Section 3.2, where we introduce *formal proofs*. For now, however, we discuss each of the logical rules in turn.

3.1.1 The *Taut* Rule

The simplest rule is the axiom *Taut*:

$$\textit{Taut} \qquad \frac{}{\varphi} \text{ if } \varphi \text{ is an instance of a prop-logic tautology}$$

This axiom states that any instance of a *tautology* from propositional logic can be introduced at any time as a derivable statement in the access-control logic. To understand what this rule means, first recall that a propositional-logic tautology is a formula that evaluates to *true* under *all* possible interpretations of its propositional variables. For example, the propositional formula $p \vee \neg p$ always evaluates to *true*, independent of whether the propositional variable p is assigned the value *true* or the value *false*. In contrast, the formula $p \supset \neg p$ is not a tautology, because it evaluates to *false* whenever p is assigned the value *true*. Although it does not constitute a complete listing, Figure 3.2 summarizes some common propositional-logic tautologies.

A formula φ is *an instance* of the formula ψ if there exist propositional variables $p_1, \ldots, p_k$ (for some $k \geq 0$) and modal formulas $\varphi_1, \ldots, \varphi_k$ such that φ is obtained by replacing each p_i in ψ by φ_i. For example, the formula

$$(\mathit{Alice} \textsf{ says } \mathit{go}) \vee ((\mathit{sit} \wedge \mathit{read}) \supset (\mathit{Alice} \textsf{ says } \mathit{go}))$$

is an instance of the formula $q \vee (r \supset q)$: it can be obtained by replacing every q by $(\mathit{Alice} \textsf{ says } \mathit{go})$ and every r by $(\mathit{sit} \wedge \mathit{read})$. In contrast, the formula

$$(\mathit{Alice} \textsf{ says } \mathit{go}) \vee ((\mathit{sit} \wedge \mathit{read}) \supset \mathit{stay})$$

is *not* an instance of the formula $q \vee (r \supset q)$, because the two separate occurrences of q were not replaced by the same formula.