Commuting with complement

Consider a function $f\colon X \to Y$. Let $\mathcal{P}(S)$ denote the power set of S (the set of subsets of S), and define the function $\bar{f}\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ by

$$\bar{f}(A) = \{f(a)\colon a \in A\} \qquad \text{for } A \subseteq X.$$

(We often simply write $f(A)$ for this, conflating f and $\bar{f}$ in an admitted slight abuse of notation. In most contexts, this conflation is relatively harmless; in what follows, it will be useful to keep the distinction clear.)

We have:

$$\begin{aligned} f \text{ is injective} &\equiv (\forall A \subseteq X\colon \bar{f}(A^C) \subseteq \bar{f}(A)^C) \\ f \text{ is surjective} &\equiv (\exists A \subseteq X\colon \bar{f}(A)^C \subseteq \bar{f}(A^C)) \end{aligned}$$

Here ^{C} denotes complement with respect to the appropriate set: $\bar{f}(A^C)$ means $\bar{f}(X \setminus A)$ and $\bar{f}(A)^C$ means $Y \setminus \bar{f}(A)$.

These statements may be taken as exercises in symbolic logic; for example, the condition for injectivity may be proved as follows. For convenience, let the variable A be of type $\mathcal{P}(X)$, the variables x, x_1, x_2 be of type X, and the variable y be of type Y (so that $\forall y$ means $\forall y \in Y$ and so on). We compute:

$$\begin{aligned}
&\forall A\colon \bar{f}(A^C) \subseteq \bar{f}(A)^C \\
\equiv\quad &\{\text{definitions of } \subseteq, \bar{f}, {}^C\} \\
&\forall A\colon \forall y\colon (\exists x\colon x \in A^C \text{ and } y = f(x)) \Rightarrow \neg(\exists x\colon x \in A \text{ and } y = f(x)) \\
\equiv\quad &\{(p \Rightarrow q) \equiv (\neg p \text{ or } q) \text{ and De Morgan's laws}\} \\
&\neg\exists A\colon \exists y\colon (\exists x\colon x \in A^C \text{ and } y = f(x)) \text{ and } (\exists x\colon x \in A \text{ and } y = f(x)) \\
\equiv\quad &\{\text{and distributes over } \exists\} \\
&\neg\exists A\colon \exists y\colon \exists x_1, x_2\colon x_1 \in A^C \text{ and } y = f(x_1) \text{ and } x_2 \in A \text{ and } y = f(x_2) \\
\equiv\quad &\{\exists \text{ commutes with itself; and distributes over } \exists\} \\
&\neg\exists x_1, x_2\colon (\exists A\colon x_1 \in A^C \text{ and } x_2 \in A) \text{ and } (\exists y\colon y = f(x_1) \text{ and } y = f(x_2)) \\
\equiv\quad &\{\text{properties of } \in \text{ and } =\} \\
&\neg(\exists x_1, x_2 \in X\colon x_1 \neq x_2 \text{ and } f(x_1) = f(x_2)) \\
\equiv\quad &\{\text{definition of injectivity}\} \\
&f \text{ is injective}
\end{aligned}$$

The condition for surjectivity is left as an exercise.

The "property of $\in$" used above is that, for any a, b,

$$a = b \equiv (\forall S\colon a \in S \equiv b \in S)\,.$$

This property is a kind of dual to the axiom of extensionality: just as sets are equal if they have the same elements, so objects are equal if they are members of the same sets.