Things were a little rushed in class today, so here is a more careful proof that the conversion from NFAs to DFAs works.

Recall the basic idea is to store, in the state of the DFA, the set of all possible states the NFA could be in after processing the same string.

We are given an NFA (without ε transitions) $M = (Q, \Sigma, \delta, q_0, F)$ and we constructed a DFA $M' = (Q', \Sigma, \delta', q_0', F')$, where

$$\begin{aligned} Q' &= \mathcal{P}(Q) = \text{the set of all subsets of } Q \\ q_0' &= \{q_0\} \\ F' &= \{S \subseteq Q : S \cap F \neq \emptyset\} = \text{the subsets of } Q \text{ that contain at least one element of } F \\ \delta'(S, a) &= \bigcup_{r \in S} \delta(r, a) = \{q \in Q : \exists r \in S \text{ such that } q \in \delta(r, a)\} \end{aligned}$$

First we want to show that the construction really implements the idea: that the state of M' really is the set of possible states of M after processing the same string. I'll introduce just one piece of notation for this: $\delta^*(x)$ is the state of M' after reading string $x \in \Sigma^*$. Formally, I can define this inductively by:

$$\begin{aligned} \delta^*(\varepsilon) &= q_0', \\ \delta^*(wa) &= \delta'(\delta^*(w), a) \text{ for } w \in \Sigma^*, a \in \Sigma. \end{aligned}$$

(Intuition behind the second equation: when processing wa, M' first processes w, which takes it to state $\delta^*(w)$ and then applies the δ' transition function once more when it processes the last character a.)

If we combine the definition of $\delta^*(wa)$ and the definition of δ', we get:

$$\delta^*(wa) = \delta'(\delta^*(w), a) = \{q \in Q : \exists r \in \delta^*(w) \text{ such that } q \in \delta(r, a)\} \tag{1}$$

Now we're ready to prove the key claim (the invariant of the construction).

Claim: There is a path from q_0 to q in M labelled by string x if and only if $q \in \delta^*(x)$.

Proof by induction on the length of x:

Base case $|x| = 0$. Then $x = \varepsilon$.

There is a path from q_0 to q in M labelled by ε

$\Leftrightarrow$ $q = q_0$ (since a path of length 0 starts and ends at the same place)

$\Leftrightarrow$ $q \in \{q_0\} = q_0' = \delta^*(\varepsilon)$ (by the definition of q_0' and $\delta^*(\varepsilon)$).

Inductive step. Let $k \geq 0$. Assume the claim is true for all strings x of length k. We shall prove the claim is true for all strings x of length $k + 1$.

Let x be any string of length $k + 1$. Then $x = wa$ where w is a string of length k and a is a single character. Then,

There is a path from q_0 to q in M labelled by x

$\Leftrightarrow$ There is a path from q_0 to q in M labelled by wa (since $x = wa$)

$\Leftrightarrow$ There is a state $r \in Q$ such that there is a path from q_0 to r in M labelled by w and $q \in \delta(r, a)$

$\Leftrightarrow$ There is a state $r \in \delta^*(w)$ and $q \in \delta(r, a)$ (by the induction hypothesis)

$\Leftrightarrow$ $q \in \delta^*(wa)$ (by Equation (1)).

This completes the inductive proof of the claim. Now we show that the two machines really accept exactly the same strings.

Claim: M accepts a string x if and only if M' accepts x.

Proof: For any string x,

M accepts x

$\Leftrightarrow$ There is a path in M labelled by x that goes from state q_0 to some state of F

$\Leftrightarrow$ Some state of F is in $\delta^*(x)$ (by the previous claim)

$\Leftrightarrow$ The state of M' after reading x contains an element of F (by the definition of δ^*)

$\Leftrightarrow$ The state of M' after reading x is an accepting state of M' (by the definition of F')
$\Leftrightarrow$ M' accepts x.

This completes the proof that any language accepted by an NFA is also accepted by a DFA. The converse is trivial since a DFA is a special case of an NFA; thus, if a language is accepted by a DFA then it is also accepted by an NFA.

This proves that the class of languages accepted by NFAs is the same as the class of regular languages.