There are 2 questions for a total of 10 points.

1. (4 points) Let $\Sigma = \{0, 1\}$, and let $L = \{xy \in \Sigma^* \mid \#\text{ of 0's in } x = \#\text{ of 1's in } y\}$. Prove that L is a regular language.

Solution: We claim that $L = \Sigma^*$.

Proof:

Consider any string $x = x[1]x[2]\ldots x[n]$ in Σ^*. Let $o[i]$ = number of ones in $x[1 \ldots i]$, and $z[i]$ = number of zeros in $x[i \ldots n]$. Define $o[0] = z[n+1] = 0$ vacuously (for the case when the prefix/suffix is the empty string).

Also define $f(i) = z[i] - o[i-1]$ for $1 \le i \le n+1$.

We first show that there exists an i such that $f(i) = 0$ and $1 \le i \le n+1$.

For this, we claim the following two things:

Claim 1. $f(i) = z[i]-o[i-1]$ changes by 1 at each step when going from i to $i+1$, i.e., $|f(i)-f(i+1)| = 1$ for all valid i.

Proof: Make two cases on $x[i]$:

1. when $x[i] = 0$, then $o[i] = o[i-1]$ and $z[i+1] = z[i] - 1$, so we have $|f(i) - f(i+1)| = 1$.
2. when $x[i] = 1$, then $o[i] = o[i-1]+1$ and $z[i+1] = z[i]$, so we again have $|f(i) - f(i+1)| = 1$.

Claim 2. $f(1) \ge 0$ and $f(n+1) \le 0$

Proof: Clearly, we have $f(1) = z[1] - o[0] = z[1] \ge 0$ since counts are always non-negative. We also have $f(n+1) = z[n+1] - o[n] = -o[n] \le 0$ by the same reason.

Now we shall implicitly prove and invoke a form of the discrete intermediate value theorem on integers as follows:

Suppose there exists no i such that $f(i) = 0$. Wlog suppose that $f(1) > 0$ (the other case is analogous). Then we show that $f(i) > 0$ for all valid i, which shall contradict Claim 2.

We shall show this using induction. The base case is true. Now suppose that $f(i) > 0$ for some $i \ge 1$. Note that $f(i+1) = f(i)+1$ or $f(i)-1$. If $f(i+1) < 0$, the fact that $f(i) > 0$ implies that $|f(i+1) - f(i)| \ge 2$, which is false, hence it must hold that $f(i+1) > 0$, since it can't be equal to 0 by assumption. Thus, the induction is complete, so $f(n+1) > 0$, which is a contradiction to Claim 2.

Hence our assumption was wrong, and $f(i) = 0$ for some $1 \le i \le n+1$. Consider such an i.

We have $o[i-1] = z[i]$. So we have the number of zeros in $x[1 \ldots i-1]$ equal to the number of ones in $x[i \ldots n]$. This shows that x is in L. Since x was arbitrary, we have $\Sigma^* \subseteq L$. Now by definition of a language, $L \subseteq \Sigma^*$, so $L = \Sigma^*$.

Now it is easy to make a DFA for $L = \Sigma^*$: for instance, consider $(Q, \Sigma, \delta, q_0, A) = (\{q_0\}, \{0, 1\}, \delta, q_0, \{q_0\})$ where δ is defined as $\delta(q_0, 0) = \delta(q_0, 1) = q_0$. (Note: in fact, any DFA with $Q = A$ and $|Q| > 0$ works).

Thus L is indeed a regular language as needed.

2. (6 points) Let $L \subseteq \Sigma^*$ be any regular language. Prove that the language $L' = \{z \mid \exists x, y \in \Sigma^* \text{ such that } z = xy \text{ and } yx \in L\}$ is regular.

Solution: Suppose the $DFAD = (Q, \Sigma, \delta, q_0, A)$ recognizes L.

Consider the following languages:

$$L_q = \{xin\Sigma^* \mid \hat{\delta}(q, x) \in A\}$$

$$M_q = \{xin\Sigma^* \mid \hat{\delta}(q_0, x) = q\}$$

Claim 1: Both L_q and M_q are regular languages.

Proof:

Construct DFAs as follows:

1. L_q: consider the DFA $D_q = (Q, \Sigma, \delta, q, A)$.
2. M_q: consider the DFA $D'_q = (Q, \Sigma, \delta, q_0, \{q\})$

The fact that these DFAs correspond to these languages follows from the very definition of these languages.

So $L_q M_q$ is a regular language (closure under concatenation).

So, $L'' = \bigcup_{q \in Q} L_q M_q$ is a regular language due to closure under finite union.

Now we claim that $L'' = L'$; this shall complete the proof since we have already shown L'' is regular.

For that we shall need the following claims:

1. Any string in L'' is in L':

   Consider any string x in L''. Then for some state $q \in Q$, $x \in L_q M_q$. So there exist two strings x' and x'' in L_q and M_q such that $x = x'x''$ by definition of language concatenation. So we have $\hat{\delta}(q_0, x''x') = \hat{\delta}(\hat{\delta}(q_0, x''), x') = \hat{\delta}(q, x')$ which is in A, by the definition of L_q and M_q. So $x''x'$ is accepted by D, and hence belongs to L. Thus x is in L' (since $x = x'x''$ and $x''x'$ is in L).

2. Any string in L' is in L''.

   Consider any string x in L'. Then there exist strings $x', x'' \in \Sigma^*$ such that $x = x'x''$ and $x''x'$ is in L. Consider $q = \hat{\delta}(q_0, x'')$. Then since $x''x'$ is in L, we have $A \ni \hat{\delta}(q_0, x''x') = \hat{\delta}(\hat{\delta}(q_0, x''), x') = \hat{\delta}(q, x')$. By definition of q, x'' is in M_q, and by the result we just obtained (that $\hat{\delta}(q, x') \in A$), we have x' is in L_q. Hence, $x = x'x''$ is in $L_q M_q$, which is a subset of L''. This establishes the fact that any string x in L' is in L''.

Using the first claim, we have $L'' \subseteq L'$ and using the second claim, we have $L' \subseteq L''$, so combining these we have $L' = L''$, and we are done.