GENERAL LINEAR GROUPS AND THE
TECHNICAL LEMMA FOR THE J-THEOREMS

We need the following fact.

**Lemma.** Let $G = GL(2, p)$, where $p$ is an odd prime, and let $P \in \text{Syl}_p(G)$. Suppose that $L \subseteq G$ is normalized by $P$ and that $p$ does not divide $|L|$. If a Sylow 2-subgroup of $L$ is abelian, then $P$ centralizes $L$.

Actually, a slightly stronger result is true since the hypothesis on the Sylow 2-subgroup of $L$ is needed only in the case $p = 3$. We will not bother to prove this refinement, however.

We begin with a discussion of some basic facts about the **General Linear Group** $GL(n, q)$ and related groups. Here, $n$ is a positive integer and $q$ is a power of the prime $p$. The group $G = GL(n, q)$ is the full group of invertible $n \times n$ matrices over the unique field $F$ of order $q$. It is not hard to see that

$$|G| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}),$$

and thus a Sylow $p$-subgroup of $G$ has order $qq^2q^3 \cdots q^{n-1} = q^{n(n-1)/2}$. Now, consider the set $U$ of $n \times n$ matrices over $F$ having all diagonal entries equal to 1 and all below-diagonal entries equal to 0. These matrices have determinant 1, and so they are invertible, and it is easy to see that $U$ is a subgroup of $G$. Each of the $n(n - 1)/2$ above-diagonal entries in each matrix in $U$ is an arbitrary member of $F$ and it follows that $|U| = q^{n(n-1)/2}$. We conclude that $U$ is a Sylow $p$-subgroup of $G$. If $n = 2$ (which is the smallest interesting case) we have $|G| = q(q - 1)^2(q + 1)$ and $|U| = q$.

The determinant defines a group homomorphism from $G$ onto the multiplicative group $F^\times$ of $F$ (which has order $q - 1$). The kernel of this determinant map is the normal subgroup $S = SL(n, q)$, the **Special Linear** group. It follows that $G/S \cong F^\times$, and in particular $|G : S| = q - 1$. In other words, $|S| = |G|/(q - 1)$. Since the matrices in $U$ all have determinant 1, we see that $U \subseteq S$, and thus all Sylow $p$-subgroups of $G$ lie in the normal subgroup $S$. Also, since $G/S \cong F^\times$ is abelian, we see that $G' \subseteq S$. In the case where $n = 2$, we have $|S| = q(q - 1)(q + 1)$.

Let $Z$ be the subgroup of $S = SL(n, q)$ consisting of the scalar matrices in $S$. (These are the matrices of determinant 1 that have the form $\alpha I$, where $\alpha \in F$.) The determinant condition yields that $\alpha^n = 1$, and thus $\alpha$ must lie in the (unique) subgroup of order $d = (q - 1, n)$ of $F^\times$. Thus $|Z| = d$, and clearly $Z \subseteq Z(G)$. It is not too hard to show, in fact, that $Z = Z(S)$. The factor group $S/Z$ is usually denoted $PSL(n, q)$; it is the **Projective Special Linear** group. If $n = 2$ and $q$ is odd, then $d = 2$ and we have $|PSL(2, q)| = q(q - 1)(q + 1)/2$. If $n = 2$ and $q$ is a power of 2, then $d = 1$ and in this case $|Z| = 1$ and $PSL(2, q) = SL(2, q)$ has order $q(q - 1)(q + 1)$.

We mention the following important theorem without proof.
THEOREM. The group $PSL(n,q)$ is simple for $n \geq 2$ except in the cases where $n = 2$ and $q \in \{2, 3\}$.

Note that $|PSL(2,2)| = 6$ and $|PSL(2,3)| = 12$, and so these groups certainly are not simple. We see that $|PSL(2,4)| = 60 = |PSL(2,5)|$, and in fact, each of these groups is isomorphic to the alternating group $A_5$. Also, $|PSL(2,9)| = 360$, and it turns out that this group is isomorphic to $A_6$. It is also true that $PSL(4,2) \cong A_8$, but all of the other simple groups of the form $PSL(n,q)$ are different from alternating groups.

Let us now focus on $S = SL(2,q)$, where $q$ is odd. If $t \in S$ and $t^2 = 1$, then each of the two eigenvalues of $t$ lies in the set $\{1, -1\}$ and the product of these eigenvalues is $\det(t) = 1$. There are just two possibilities therefore: either both eigenvalues are 1 or both are $-1$. The characteristic polynomial of the matrix $t$ is thus either $(X + 1)^2$ or $(X - 1)^2$. But $t^2 = 1$, and so the minimal polynomial of $t$ divides $X^2 - 1$. The minimal polynomial of an arbitrary square matrix, however, divides the characteristic polynomial, and so in this case, we see that there are just two possibilities for the minimal polynomial: $X + 1$ or $X - 1$. (We are using the fact that $1 \neq -1$, which is true because the characteristic is $p \neq 2$.) It follows that $t$ is either the identity matrix 1 or its negative. In particular, this shows that $-1$, the negative of the identity matrix, is the unique involution in $SL(2,q)$ when $q$ is odd.

Proof of the technical lemma. We assume that $P$ does not centralize $L$ and we work toward a contradiction. If there is a proper subgroup of $L$ that is normalized but not centralized by $P$, we can replace $L$ by that subgroup, and so we can assume that $L$ is minimal with the property that it is normalized but not centralized by $P$.

Let $C = C_L(P) < L$ and let $q$ be any prime divisor of $[L : C]$. Choose a $P$-invariant Sylow $r$-subgroup $R$ of $L$. (This is possible since $p$ does not divide $[L, L]$.) Then $R \not\subseteq C$, and so $P$ normalizes but does not centralize $R$. By the minimality of $L$, we see that $R = L$, and so $L$ is an $r$-group.

Now $1 < [L, P] = [L, P, P]$, and thus $[L, P]$ is a $P$-invariant subgroup of $L$ that is not centralized by $P$. By the minimality of $L$, it follows that $L = [L, P] \subseteq G^r \subseteq SL(2,p)$.

If $r = 2$, then $L$ is abelian, by hypothesis. But $SL(2,p)$ contains a unique involution, and thus $L$ is cyclic. This is impossible, however, because a group of order $p \neq 2$ cannot act nontrivially on a cyclic 2-group. (This is because the order of the automorphism group of a cyclic group of order $2^e$ is $\varphi(2^e) = 2^{e-1}$, and this is not divisible by $p$.) We conclude, therefore, that $r$ is odd and $L$ has odd order.

Now $|L|$ is an odd prime power dividing $|SL(2,p)| = p(p+1)(p-1)/2$. Since $p+1$ and $p-1$ have no common odd prime divisor and we know that $(|L|, p) = 1$, it follows that $|L|$ divides $p+1$ or $|L|$ divides $p-1$, and thus $|L| \leq p+1$. But $P$ is not normal in $PL$ (since otherwise $P$ would centralize $L$), and hence the number $n$ of Sylow $p$-subgroups of $PL$ exceeds 1. It follows by Sylow theory that $p+1 \leq n \leq |L|$, and since we already know that $|L| \leq p+1$, we deduce that $|L| = p+1$. But this implies that $|L|$ is even, which is a contradiction. 
