Jennifer Gensler
Calum Shearer
Breeann Wilson

12. Show that if P is a nonabelian group of order p^3, then any automorphism of the center of P extends to an automorphism of P.

Proof. If p is odd, we know that $P \cong U$ or $P \cong L$. So in this case we just need to prove the statement for each of U and L. Firstly, we know that $U \trianglelefteq T$, so conjugation by upper triangular matrices $t \in T$ give automorphisms of U. We aim to show that we can obtain all automorphisms of $Z(U)$ in this way. We can calculate that $Z(U) \cong \mathbb{Z}_p$ is given by matrices of the form:

$$\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $x \in \mathbb{F}_p$. (note that we can argue that $Z(U)$ must be size p: if it's order p^2 then $U/Z(U)$ is cyclic order p, which actually implies that $U = Z(U)$). Then we know that $|\mathrm{Aut}(\mathbb{Z}_p)| = p - 1$. So if we can find $p - 1$ matrices in T that give distinct automorphisms on $Z(U)$ then we are done. Let $a \in \mathbb{Z}_p^*$. Then if:

$$t_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} \in T$$

we find that:

$$t_a^{-1} \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} t_a = \begin{pmatrix} 1 & 0 & ax \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So conjugation by t_a acts like multiplication by a on $Z(U) \cong \mathbb{Z}_p$, so for differing $a \in \mathbb{Z}_p^*$ the map given by conjugation by t_a is a distinct automorphism on $Z(U)$. There are $p-1$ choices of a, so these give all automorphisms of $Z(U)$. As conjugation by t_a is also an automorphism of U by normality of U in T, this shows that each automorphism of $Z(U)$ can be extended to an automorphism of U.

For $P \cong L$, we use the same method as with U. First, note that L is the Sylow p-subgroup of $G := AGL(1, \mathbb{Z}_{p^2}) = \{ax + b \colon a \in \mathbb{Z}_{p^2}^*, b \in \mathbb{Z}_{p^2}\}$. Note that $|\mathbb{Z}_{p^2}^*| = \phi(p^2) = p(p-1)$, so G has size $p^3(p-1)$, while L has size p^3. Then from the Sylow theorems, we know that $[G \colon N_G(L)] \mid (p-1)$ and $[G \colon N_G(L)] \equiv 1(p)$, from which the only choice is that $[G \colon N_G(L)] = 1$, i.e. $L \trianglelefteq G$, so conjugation by elements of G give automorphisms of L. We find that $L = \{ax + b \colon a \equiv 1(p), b \in \mathbb{Z}_{p^2}\}$ (one can check simply by showing that this is indeed a subgroup, for it has the required size and we know that L is the unique subgroup of G of order p^3).

Next, we note that:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ 1 \end{pmatrix}$$

So when doing computations, we can identify the affine linear transformation $ax + b$ with the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Note also, that $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}^{-1}$ i.e. the inverse transformation of $ax+b$ is $a^{-1}x - a^{-1}b$. By the same reasoning we used in the calculation for U, we know that $|Z(L)| = p$. We claim that :

$$Z(L) = \{x + mp \colon 0 \leq m \leq p-1\}$$

(note that all such mp are distinct mod p^2, so this set does indeed have size p). Indeed, given any transformation $g = ax + b \in L$, by writing a as $np + 1$ for some $n \in \mathbb{Z}$, (with inverse mod p^2 given by $1 - np$)we calculate that conjugation of $x + mp$ by g is given by:

$$\begin{aligned}
&\begin{pmatrix} np+1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & mp \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -np+1 & -(-np+1)b \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} np+1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -np+1 & (np-1)b + mp \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (np+1)(np-1)b + (np+1)mp + b \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -b + mp + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & mp \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

So that $(x + mp) \in Z(L)$. Note that there is an isomorphism $Z(L) \cong \mathbb{Z}_p$ given by sending $(x + mp)$ to $m \in \mathbb{Z}_p$. Using this, we will find automorphisms of $Z(L)$ which are equivalent to multiplication by $a \in \mathbb{Z}_p^*$ on $Z(L) \cong \mathbb{Z}_p$, for any possible a, which will then give $p-1$ distinct automorphisms of $Z(L)$ which extend to automorphisms of L (the exact same argument we used for U).

We do so by picking $a \in \{1, 2, \ldots p-1\}$ and consider the transformation $h = ax \in G$ (note that $a \leq p$ and non-zero so is coprime to p^2 and hence in $\mathbb{Z}_{p^2}^*$). Then conjugating by h is an automorphism of L by normality of L in G, and its action on $x + mp \in Z(L)$ is given by:

$$\begin{aligned}
&\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & mp \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a & amp \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & amp \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

So the map $x + mp$ is sent to the map $x + amp$. Using our isomorphism $Z(L) \cong \mathbb{Z}_p$, this is just equivalent to multiplication by a in $\mathbb{Z}_p$. So these $p-1$ automorphisms of L restrict to distinct automorphisms of $Z(L)$. $|\mathrm{Aut}(\mathbb{Z}_p)| = p - 1$, so these are all of the autormorphisms of $Z(L)$. Hence each automorphism of $Z(L)$ can be extended to an automorphism of L.

If $p = 2$ then by the above, $|Z(P)| = 2$, so the center of P must be isomorphic to $\mathbb{Z}_2$. But the only automorphism of $\mathbb{Z}_2$ is the identity, which then extends to P by taking the identity on P. $\square$