6) Suppose that G is a finite group and let p be the smallest prime dividing $|G|$. Let $H \leq G$ be a subgroup with $[G : H] = p$.

a) Prove that H is normal in G.

b) Prove that if G is abelian, $|G| = p(p+2)$ and both p, $p+2$ are primes, then G is cyclic.

Proof: If $\exists x \in G$ with $ord(x) = p(p+2)$, then G is cyclic and we are done.

CASE 1: There exists $x \in G$, $ord(x) = p + 2$.

Then if $H = \langle x \rangle$, we know $[G : H] = p$. Since G is abelian, $H \triangleleft G$, so we have that $G/H \cong \mathbb{Z}_p$. Then $\exists y \in G$ such that yH is a generator for G/H and $ord(yH) = p$. This means that

$$y^p H = (yH)^p = H,$$

and so $y^p \in H$, which implies $\exists q \in \mathbb{N} \cup \{0\}$ with $y^p = x^q$.

Claim: $ord(y) \neq p + 2$.

Suppose $ord(y) = p + 2$. Then $q \neq 0$, and so multiplying both sides by y^2, we have

$$e_G = y^{p+2} = y^p y^2 = x^q y^2.$$

This shows that $y^{-2} = x^q$, and so $y^2 = x^{-q} \in H$. But then

$$(yH)^2 = y^2 H = H,$$

and so $|G/H| = 2$. But $2 + 2 = 4$ which is not prime, contradicting the assumption on p and $p + 2$. Hence $ord(y) \neq p + 2$, which proves the claim.

Now that we know the claim, we may assume $ord(y) = p$ since $ord(y) = p(p + 2)$ implies G is cyclic. Then if $x^n = y^m$ for some $n, m \in \mathbb{Z}$,

$$e_G = (y^p)^m = (y^m)^p = (x^n)^p = x^{np}.$$

Then since $ord(x) = p + 2$, we have that $p + 2$ divides np. As $p + 2$ is prime, $p + 2$ divides n, and so $x^n = e_G = y^m$.

Now consider all elements in G of the form $x^n y^m$ for $0 \leq n \leq p + 1$ and $0 \leq m \leq p - 1$. Suppose that $x^n y^m = x^i y^j$ for some $0 \leq i, n \leq p + 1$ and

$0 \leq j, m \leq p-1$. Then multiplying on the left by x^{-i} and the right by y^{-m}, we have

$$x^{n-i} = y^{j-m}$$

and so by our previous observation, $x^{n-i} = y^{j-m} = e_G$. But by our assumption on the range of i, j, n, m, we must then have $n - i = 0 = j - m$, and so $n = i$ and $j = m$.

Since there are precisely $p(p+2) = |G|$ such elements, we obtain

$$G = \{x^n y^m : 0 \leq n \leq p+1,\ 0 \leq m \leq p-1\}.$$

As G is abelian, we have $G \cong \mathbb{Z}_{p+2} \times \mathbb{Z}_p \cong \mathbb{Z}_{p(p+2)}$ since p and $p+2$ are relatively prime. Hence, G is cyclic.

CASE 2: There exists $x \in G$, $ord(x) = p$.

This is the same argument as Case 1, but switching p and $p+2$.

Now consider arbitrary G. If either $|\mathcal{Z}(G)| = p$ or $|\mathcal{Z}(G)| = p+2$, then $G/\mathcal{Z}(G)$ would be cyclic, which implies that G is abelian by a homework problem. Since then $\mathcal{Z}(G) = G$, we'd have a contradiction, so either $\mathcal{Z}(G) = G$ or $\mathcal{Z}(G) = e_G$. If we can prove the former condition holds, then we'll be done.

If there exists $x \in G$, $ord(x) = p+2$, then by part a), $H = \langle x \rangle$ is normal in G. By exactly the same argument as above (note that we only used the assumption that G is abelian at the very beginning and very end of the argument), we obtain the existence of an element y of order p, that all elements of the form $x^n y^m$ for $0 \leq n \leq p+1$ and $0 \leq m \leq p-1$ are distinct in G, and that

$$G = \{x^n y^m : 0 \leq n \leq p+1,\ 0 \leq m \leq p-1\}.$$

Claim: $K = \langle y \rangle$ is normal in G

Recall the definition of the normalizer of K in G:

$$N_G(K) = \{z \in G : zKz^{-1} = K\}.$$

From the homework, $N_G(K)$ is a subgroup of G, $K \leq N_G(K)$, and $N_G(K) = G$ iff $K \triangleleft G$. By order considerations, we need only show that $\exists z \in N_G(K) \backslash K$ in order to conclude $N_G(K) = G$.

Consider the inner automorphism ϕ_n of G given by $\phi_n(g) = x^n g x^{-n}$ for all $g \in G$. Since $ord(x) = p+2$, there are only $p+2$ distinct $\phi_n's$. Restrict ϕ_n to K for $0 \leq n \leq p+1$. As $x \notin K$, we know that $x^n \notin K$ for all such n. Suppose $\phi_n(K) \neq K$ for all $1 \leq n \leq p+1$. Then again by order considerations, $\phi_n(K) \cap K = e_G$ as the intersection would be a subgroup of K, and $|K| = p$ implies the only possible subgroups of K are $\{e_G\}$ and K itself.

Consider $\phi_n(K) \cap \phi_m(K)$. Order considerations imply either $\phi_n(K) \cap \phi_m(K) = \phi_n(K) = \phi_m(K)$ or $\phi_n(K) \cap \phi_m(K) = e_G$. But if the former case holds, then $K = \phi_{-m}(\phi_n(K)) = \phi_{n-m}(K)$, and hence $n = m$. This implies that for all $0 \leq n, m \leq p+1$,

$$\phi_n(K) \cap \phi_m(K) = e_G.$$

Note that every nonidentity element in $\phi_n(K)$ has order p since ϕ_n is an automorphism for all $0 \leq n \leq p+1$. Since all $p-1$ nonidentity elements in $\phi_n(K)$ are disjoint from $\phi_m(K)$, we have that G possesses $(p-1)(p+2)$ elements of order p. It then follows that the only elements of order $p+2$ in G are the nonidentity elements of H.

From this, we obtain that there exist $1 \leq i \leq p+1$ and $1 \leq j \leq p-1$ with

$$xy = \phi_i(y^j) = x^i y^j x^{-i}.$$

Multiplying on the left by $p-1$, we obtain

$$x = x^i y^j x^{-i} y^{p-1} = x^i (y^j x^{-i} y^{-j}) y^{p-1+j}.$$

As $H \lhd G$, $y^j x^{-i} y^{-j} = x^k$ for some $0 \leq k \leq p+1$. Hence, $x = x^{i+k} y^{p-1+j}$, and so by our assumptions on j, $p-1+j = 0$ mod p. Then $j = 1$, so $xy = x^i y x^{-i}$.

Now since both H and K are normal in G, $xyx^{-1} \in K$ and $y^{-1}xy \in H$. Hence, there are $0 \leq n \leq p+1$ and $0 \leq m \leq p-1$ with $xyx^{-1} = y^m$ and $y^{-1}xy = x^n$. Multiplying the second equation on the left by y, we obtain $xy = yx^n$ and substituting into the first equation, we have

$$y^m = (xy)x^{-1} = (yx^n)x^{-1} = yx^{n-1}.$$

Then multiplying y^{-1} on the left, we get $y^{m-1} = x^{n-1}$, and by our assumptions in n and m, $n = m = 1$. It then follows that both x and y are in $\mathcal{Z}(G)$, and so $\mathcal{Z}(G) \neq \{e_G\}$. By our observation above, it must be true that $\mathcal{Z}(G) = G$, so G is abelian.