1 Reading

1. Read section 2.9, start 2.10

2 Problems

1. Let $G$ be a finite group of order $n$, and suppose that $p$ is the smallest prime divisor of $n$. If $H \subseteq G$ is a subgroup of index $p$, prove that $H$ must be normal. (This problem generalizes the statement that an index 2 subgroup is always normal).

**Solution:** Let $S = \{gH|g \in G\}$. Then since $i_G(H) = p$ we have $\#S = p$. In our attempt to generalize Cayley’s theorem we proved the existence of a homomorphism

$$\varphi: G \to A(S)$$

with the property that $K = \ker(\varphi) \subseteq H$. Let $L = \varphi(G)$. Then since $L$ is a subgroup of $A(S)$, Lagrange tells us that $o(L) \mid o(A(S)) = p!$. The isomorphism theorems also tell us that $L \cong G/K$ so $o(L)o(K) = o(G)$ implies that $o(L) \mid o(G) = n$. Thus $o(L) \mid \gcd(n,p!)$. I claim that $\gcd(n,p!) = p$. To see this, suppose $q$ is a prime dividing both $n$ and $p!$. Since $q$ divides $n$ we must have $q \geq p$ as $p$ is the smallest prime divisor of $n$. Since $q$ divides $p!$ we have $q \leq p$ since the only prime factors of $p!$ are all less than or equal to $p$. Thus $q = p$, and since $p^2 \mid p!$ we get $\gcd(n,p!) = p$.

Thus $o(L)$ is either 1 or $p$. It cannot be 1 since $o(K) \leq o(H) < o(G)$ and $o(L)o(K) = o(G)$. Thus $o(L) = p$ which implies that $o(K) = n/p$. But Lagrange says $o(H) = o(G)/i_G(H) = n/p$ as well. Since $K \subseteq H$ we get equality, and hence $H$ is normal in $G$ since $K$, being a kernel, is normal in $G$.

2. In this question we will explore an alternate way to prove that a group of order $p^2$ is abelian. Let $p$ be a prime and let $G$ be a group of order $p^2$.

   (a) Prove that any subgroup $H \subseteq G$ of order $p$ is normal in $G$.

   **Solution:** This is just an application of question 1 since $p$ is the smallest prime divisor of $o(G)$. We can also give a simpler argument in this case. Since $i_G(H) = p$, we have a homomorphism $\varphi: G \to S_p$ whose kernel is contained in $H$. Since $p^2 = o(G) \mid o(S_p) = p!$, we cannot have $\varphi$ one-to-one. Thus $\ker(\varphi)$ is some non-identity subgroup of $H$, but $H$ having only $p$ elements only has trivial subgroups. Thus $\ker(\varphi) = H$ so $H$ is normal in $G$.

   (b) Prove that any subgroup $H \subseteq G$ of order $p$ is contained in the center $Z \subseteq G$.

   **Solution:** Let $H \subseteq G$ be a subgroup of order $p$. Since $p$ is prime we must have $H$ cyclic. That is, $H = \langle x \rangle$ for some $x \in G$. Since $H$ is normal in $G$ we have that $gHg^{-1} = H$ for every $g \in G$. Thus we can define a function $\varphi: G \to \text{Aut}(H)$ given by $\varphi(g) = \tau_g$ where $\tau_g(h) = ghg^{-1}$. It’s easy to check that $\varphi$ is a homomorphism since $\tau_{g_1} \circ \tau_{g_2} = \tau_{g_1g_2}$.

   Now $\varphi(G)$ is a subgroup of $\text{Aut}(H)$ so since $H$ is a cyclic group of size $p$ we have $o(\varphi(G)) \mid o(\text{Aut}(H)) = p - 1$. But $o(\varphi(G)) \mid o(G) = p^2$ as well, which means that $o(\varphi(G)) = 1$ as $\gcd(p^2, p - 1) = 1$. Thus every element of $G$ maps to the identity function on $H$ meaning that $ghg^{-1} = h$ for every $g \in G$ and $h \in H$. This proves that $H$ is contained in the center of $G$.

   (c) Deduce that $G$ must be abelian.
Solution: We just proved that every subgroup of size \( p \) is contained in the center of \( G \). Let \( e \neq x \in G \). Then \( o(x) \) is either \( p \) or \( p^2 \). If \( o(x) = p^2 \) then \( G \) is cyclic hence abelian. Otherwise \( o(x) = p \) so \( (x) \subseteq Z \) by part b). If \( y \in G - (x) \) then again \( o(y) \) is either \( p \) or \( p^2 \). If \( o(y) = p^2 \) then again \( G \) is cyclic hence abelian. Otherwise \( o(y) = p \) so \( (y) \subseteq Z \) as well. In this case we have \( o(Z) > p \) but \( o(Z) | o(G) = p^2 \) implies \( o(Z) = p^2 \) and so \( Z = G \) and therefore \( G \) is abelian.

It is worth remarking that our proof shows us more. It proves for us that up to isomorphism there are exactly two groups of order \( p^2 \). There is the cyclic group \( C_{p^2} \) and there is another group (we will eventually call this other group \( C_p \times C_p \)) which is generated by two commuting elements \( x \) and \( y \) where \( o(x) = o(y) = p \).

3. 2.9.8

Solution: If \( p = 2 \) then there is nothing to prove. We already know all groups of order 4 are abelian and contain elements of order 2. The subgroup this element generated is normal since \( G \) is abelian. Thus we may assume that \( p > 2 \) is an odd prime. For this problem it suffices to prove that \( G \) has an element of order \( p \). This is because if there exists \( g \in G \) of order \( p \), then the subgroup \( \langle g \rangle \) has index 2 and hence is normal by problem 1 above.

Now Lagrange says that every non-identity element of \( G \) has order 2, \( p \) or \( 2p \). If any \( x \in G \) has order \( 2p \) then \( o(x^2) = p \) and we’d be done. Thus we must show why it cannot happen that every non-identity element of \( G \) has order 2.

Thus assume for the sake of contradiction that every non-identity element of \( G \) has order 2. Then necessarily \( G \) is abelian by Herstein exercise 2.3.10. Let \( g \in G \) be any element of order 2. Since \( G \) is abelian we get that \( H = \langle g \rangle \) is an index 2 normal subgroup of \( G \). Thus for any \( y \in G - H \) we have \( o(Hy) = p \) in \( G/H \). This tells us that \( yp \in H \), but we also have by assumption that \( y^2 = e \). Thus

\[
y^p = yy^{p-1} = y(y^2)^{p-1} = y \in H
\]

which is a contradiction.

In class we skipped Applications 1 and 2 of section 2.7 in Herstein. The reason we skipped these is because we will prove more general versions of both of these theorems in the next few days. If you know Application 1 then you can finish off the preceding problem in a single step. After we assume that every non-identity element of \( G \) has order 2 we get that \( G \) is abelian. Then Application 1 proves that there is an element of \( G \) of order \( p \) which is absurd. The ingredients we used in the above proof are more or less the ideas Herstein uses in his proof.

4. 2.9.9

Solution: Let \( G \) be a group of order \( pq \) where \( p \) and \( q \) are distinct prime numbers. Suppose further that \( G \) has subgroups \( H \) and \( K \) of orders \( p \) and \( q \), respectively, which are normal in \( G \). Then there exist elements \( x \in H \) and \( y \in K \) with \( H = \langle x \rangle \) and \( K = \langle y \rangle \). Consider the commutator \( xyx^{-1}y^{-1} \).

On the one hand we have

\[
xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in K
\]

since \( K \) is normal. On the other hand we have

\[
xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in H
\]

since \( H \) is normal. Thus \( xyx^{-1}y^{-1} \in H \cap K \). The group \( H \cap K \) is a subgroup of \( H \) and a subgroup of \( K \) so by Lagrange we know that its order divides both \( p \) and \( q \). Hence it also divides
gcd\(p, q\) = 1 and in fact \(H \cap K = \{e\}\). This proves that \(xyx^{-1}y^{-1} = e\) which in turn says that \(x\) and \(y\) commute. Consider \(z = xy\). Then \(z^p = (xy)^p = x^py^p = y^p \neq e\) since \(q \nmid p\) and similarly \(z^q = (xy)^q = x^qy^q = x^q \neq e\) since \(p \nmid q\). Thus we must have \(o(z) = pq\) which shows that \(G\) is cyclic and is generated by \(z\).

5. 2.10.2

**Solution:**
(a) This permutation equals \((12345)\)
(b) This permutation equals \((1625)(34)\).

6. 2.10.3

**Solution:**
(a) We get \((145678923)\). Notice that in class we multiply permutations right to left. If you multiply left to right you will get a different answer.
(b) We get \((132)\).

7. 2.10.5

**Solution:** We have
\[
\begin{align*}
(12345678)^0 &= () \\
(12345678)^1 &= (12345678) \\
(12345678)^2 &= (1357)(2468) \\
(12345678)^3 &= (14725836) \\
(12345678)^4 &= (15)(26)(37)(48) \\
(12345678)^5 &= (16385274) \\
(12345678)^6 &= (1753)(2864) \\
(12345678)^7 &= (18765432)
\end{align*}
\]

3 For Fun

1. Herstein 2.9: 10

**Solution:**
(a) One can prove this using only Cayley’s theorem and its extension, but such a proof would not be enlightening. Since this homework we have seen Cauchy’s theorem which guarantees the existence of a subgroup of size \(p\) and a subgroup of size \(q\). Notice that by problem 1 above, the subgroup of size \(p\) is automatically normal in \(G\).
(b) Let $y$ be an element of order $p$ in $G$. Then we've seen that $H = \langle y \rangle$ is normal in $G$, so we have a homomorphism $\varphi : G \rightarrow \text{Aut}(H)$ given by $g \mapsto \tau_g$ where $\tau_g(h) = ghg^{-1}$. Now $\text{Aut}(H)$ has size $p - 1$ since $H$ is cyclic of prime size $p$. Thus $o(\varphi(G))$ divides both $p - 1$ and $pq$. By assumption we have $\gcd(q, p - 1) = 1$ and of course $\gcd(p, p - 1) = 1$ so in fact $o(\varphi(G)) = 1$. This proves that $\tau_g$ is the identity on $H$ for every $g \in G$. In particular, if $x \in G$ is an element of order $q$ then $x$ and $y$ commute. Thus $o(xy) = pq$ and so $G$ is cyclic.

(c) Now suppose that $q \mid p - 1$. Let $G = C_p = \langle a \rangle$. Then $\text{Aut}(G)$ is a group of size $p - 1$, isomorphic to $U_p = \{[a] \in J_p | [a] \neq [0]\}$ under multiplication. Since $U_p$ is an abelian group of size $p - 1$ and $q \mid p - 1$, Application 1 in section 2.7 proves that there exists $\varphi \in \text{Aut}(G)$ with $o(\varphi) = q$. The construction of $S$ from homework 8 will then be a non-abelian group of order $pq$.

(d) This question is impossible to do without knowing that $U_p$ is cyclic. We will assume this for now, but prove it in Math 371.

Let $G$ be a non-abelian group of order $pq$ with $p > q$. Then $G$ contains an element $y$ of order $p$ and an element $x$ of order $q$. The subgroup $N = \langle y \rangle$ is normal in $G$ so for $H = \langle x \rangle$ we have that $HN$ is a subgroup of $G$. Since $HN$ contains both $H$ and $N$, its order is a multiple of both $p$ and $q$. This shows that $HN = G$, so we see

$$G = \{x^i y^j | 0 \leq i < q, 0 \leq j < p\}.$$  

Since $N$ is normal in $G$ we have that $x^{-1} y x = y^a$, or equivalently $yx = xy^a$, for some $a$ in the range $2, 3, \ldots, p - 1$ ($a \neq 1$ since $G$ is not abelian). The fact that $o(x) = q$ means that

$$y = x^{-a} y x^a = y^{a^q}$$

meaning that $a^q \equiv 1 \mod p$. Let $G'$ be another non-abelian group of order $pq$. Then by the same argument we see that

$$G' = \{r^i s^j | 0 \leq i < q, 0 \leq j < p\}$$

where $sr = rs^b$ where $b^q \equiv 1 \mod p$. Now $[b], [a] \in U_p$, which is a cyclic group of order $p - 1$. The subgroup of elements of order dividing $q$ in $U_p$ is therefore also cyclic, which shows that $b^{k} \equiv a \mod p$ for some integer $2 \leq k \leq q - 1$. This allows us to construct our isomorphism.

Consider the elements $w = x^k$ and $z = y$ in $G$. Then $w$ and $z$ generate $G$ since $x$ has order $q$ and $k$ is relatively prime to $q$. Also $w^p = z^p = e$ and

$$zw = y x^k = x^k(x^{-k} y x^k) = x^k(y x^k) = x^k y^b = w z^b.$$  

This gives us our isomorphism between $G$ and $G'$. 