HOMEWORK 3, DUE THU FEB 18TH

All solutions should be with proofs, you may quote from the book

(1) Let G be a group, H, K subgroups.

(a) If H is normal, show that HK is a subgroup of G.

Solution. Using lemma 2.5.1, suffices to show that $HK = KH$. We will show that $HK \subset KH$, the reverse inclusion being similar. So, let $hk \in HK$, with $h \in H, k \in K$. Then, $hk = (kk^{-1})hk = k(k^{-1}hk)$. But $k^{-1}hk \in H$, since H is normal. □

(b) If H, K are both normal, show that HK is normal.

Solution. Let $a \in G$, $h \in H, k \in K$. Then, $a(hk)a^{-1} = (aha^{-1})(aka^{-1}$ and since $aha^{-1} \in H, aka^{-1} \in K$, we see that the last term is in HK. □

(c) If H, K are both normal and $H \cap K = \{e\}$, show that for any $h \in H, k \in K$, $hk = kh$.

Solution. Let $h \in H, k \in K$. Then $hkh^{-1}k^{-1} = (hkh^{-1})k \in K$, since $hkh^{-1} \in K$. Similarly, $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ since $kh^{-1}k^{-1} \in H$. Thus it is in both H and K and thus it must be the identity. So, $hk = kh$. □

(2) (a) Let G be a group and H a subgroup of G. Define $N(H) = \{g \in G | gHg^{-1} = H\}$. Show that H is a normal subgroup of $N(H)$. ($N(H)$ is called the *Normalizer* of H in G.)

Solution. First we show that $N(H)$ is a subgroup of G. If $g, g' \in N(H)$, then $gg'H(gg')^{-1} = g(g'Hg^{-1})g^{-1} = gHg^{-1} = H$. Equally trivial to show that if $g \in N(H)$, then $g^{-1} \in N(H)$. Thus $N(H)$ is a subgroup of G.
Next we show that H is a normal subgroup of $N(H)$. iLet $g \in N(H)$ and then by definition, $gHg^{-1} = H$ and this proves what we need. □

(b) Let G be a group and let $Z(G) = \{g \in G | gx = xg \text{ for all } x \in G\}$, called the *center* of G. Show that $Z(G)$ is a normal subgroup of G.

Solution. Let $y \in G$ and $g \in Z(G)$. Then, $ygy^{-1} = gyy^{-1}$, since $yg = gy$. This is just $g \in Z(G)$. □

(c) Let $G = GL(n, \mathbb{R})$, the invertible $n \times n$ matrices. Describe $Z(G)$ explicitly.

Solution. This is a fact usually proved in linear algebra courses. The center is just the subgroup of scalar matrices, aI, a a non-zero real number and I the identity matrix. □

(3) For a set S, we as usual denote the group $A(S)$, set of all one-to-one onto maps from S to itself, with composition as the group operation. Let G be a group and $f : G \to A(S)$ a group homomorphism. We shorten $f(g)(s)$ as just gs, when f is understood. (This is usually called an *action* of G on S.) We give below a few maps which you should decide whether are group homomorphisms and if so, find its kernel.

(a) Consider the map $f : G \to A(G)$, given as $f(g) = \phi_g$ where $\phi_g(h) = gh$.

Solution. We attempt to check the homomorphism property. $f(gh) = \phi_{gh}$ where $\phi_{gh}(x) = ghx$ for any $x \in G$. While, $\phi_g \phi_h(x) = \phi_g(hx) = ghx$. Thus, $f(gh) = f(g)f(h)$. So, it is a group homomorphism. If $g \in \ker f$, then $f(g)$ is the identity in $A(G)$, so $f(g)(x) = x$, which says $gx = x$ and then by cancellation, $g = e$. So $\ker f$ is just the trivial group $\{e\}$. □

(b) Consider $f : G \to A(G)$ given as $f(g) = \psi_g$ where $\psi_g(h) = ghg^{-1}$.

Solution. Again, we c try to see whether $f(gh) = f(g)f(h)$ for $g, h \in G$. That is, $\psi_{gh} = \psi_g \psi_g$. For any $x \in G$, we have $\psi_{gh}(x) = (gh)x(gh)^{-1} = ghxh^1 g^{-1}$. On the other hand, $\psi_g \psi_h(x) = \psi_g(hxh^{-1}) = ghxh^{-1}g^{-1}$. This says, f is indeed a homomorphism.

If $g \in \ker f$, we must have $gxg^{-1} = x$ for all $x \in G$. This just says $gx = xg$ for all x and this was just our definition of the center. So, $\ker f = Z(G)$. □

(c) Let H be a subgroup of G and let L be the left cosets of H in G. Let $f : G \to A(L)$ be defined as $f(g) = \theta_g$ where $\theta_g(aH) = gaH$.

Solution. We check $f(gh) = f(g)f(h)$, that $\theta_{gh} = \theta_g\theta_h$. $\theta_{gh}(xH) = ghxH$ for any $x \in G$, while, $\theta_g\theta_h(xH) = \theta_g(hxH) = ghxH$, so f is indeed a group homomorphism. Let $g \in \ker f$. This says, $gaH = aH$ for all $a \in G$. So, $a^{-1}gaH = H$ for all a. This just says $a^{-1}ga \in H$ for all a which is same as saying $g \in aHa^{-1}$ for all a. Thus $\ker f = \cap_{a\in G} aHa^{-1}$. □

(4) Let G, H, K be groups.

Solution. The arguments for the following problem is completely straight forward. If you have difficulties, we will discuss it. □

(a) Let $f : G \to H, g : G \to K$ be group homomorphisms. Show that the map $\phi : G \to H \times K$, $\phi(a) = (f(a), g(a))$ is a group homomorphism.

(b) Let $f : H \to G, g : K \to G$ be group homomorphisms. Show by an example that the map $\phi : H \times K \to G$ given by $\phi(a, b) = f(a)g(b)$ may not be a group homomorphism, but it is if G is abelian.

(c) Show that the map $f : G \to G$, $f(a) = a^{-1}$ may not be a group homomorphism, but it is if G is abelian.

(5) Let G be a group and $S \subset G$, a subset. We write $\hat{S} = \cap_{S\subset H} H$, intersection of all subgroups of G containing S.

(a) Let $S' = \{s^{-1} | s \in S\}$. Show that any element of the form $s_1 s_2 \cdots s_n$ for some n with $s_i \in S \cup S'$ is in $\hat{S}$ and conversely every element in $\hat{S}$ is of this form.

Solution. Because of the above property, $\hat{S}$ is called the group *generated* by S.

We show $s_i s_2 \cdots s_n \in \hat{S}$ by induction on n. If $n = 1$, then either $s_1 \in S$ and since the intersection is taken over groups with $S \subset H$, we get $s_1 \in \hat{S}$, or $s_1^{-1} \in S$ and then again $s_1^{-1} \in \hat{S}$, but the latter is a subgroup and thus $s_1 \in \hat{S}$.
Assume proved for $n-1$ and let us prove for n. So, given $s_1 s_2 \cdots s_n$, we know $a = s_1 s_2 \cdots s_{n-1} \in \hat{S}$. As before, $s_n \in \hat{S}$ and thus $as_n \in \hat{S}$, being a group.
Let $T = \{s_1 s_2 \cdots s_n | s_i \in S \cup S'\}$. We want to show $T = \hat{S}$. Since $T \subset \hat{S}$ and $S \subset T$, we only need to show that T is a subgroup. As usual we check the two required properties. If $a = s_i s_2 \cdots s_n, b = t_1 t_2 \cdots t_m \in T$, with $s_i, t_j \in S \cup S'$, clearly $ab = s_1 s_2 \cdots s_n t_1 t_2 \cdots t_m \in T$. Similarly, if a is as above, then $a^{-1} = s_n^{-1} \cdots s_1^{-1}$ and since $s_i^{-1} \in SUS'$, $a^{-1} \in T$. □

(b) Let $S = \{xyx^{-1}y^{-1} | x, y \in G\}$ (these elements are called *commutators*). Show that $\hat{S}$ (which is usually written as $[G, G]$ and called the *commutator subgroup*) is a normal subgroup of G.

Solution. First notice that if $s \in S$, then $s^{-1} \in S$, so any element $a \in [G, G]$ can be written as $a = s_1 s_2 \cdots s_n$ for $s_i \in S$, from the previous part of the problem. We need to show that for any $g \in G$, $gag^{-1} \in [G, G]$. But, $gag^{-1} = g(s_1 s_2 \cdots s_n)g^{-1} = (gs_1 g^{-1})(gs_2 g^{-1}) \cdots (gs_n g^{-1})$ and so suffices to show that for any $s \in S$, $gsg^{-1} \in [G, G]$. So, let $s = xyx^{-1}y^{-1}$.

$$gsg^{-1} = ((gx)y(gx)^{-1}y^{-1})(ygxx^{-1}y^{-1}g^{-1}).$$

The first term in paranthesis is in S and the second term is $ygy^{-1}g^{-1} \in S$ too. So, their product is in $[G, G]$. □

(c) Show that $G/\hat{S}$ is abelian.

Solution. We have an onto group homomorphism $\pi : G \to G/[G, G]$ and if $a, b \in G/[G, G]$, we can find $x, y \in G$ such that $\pi(x) = a, \pi(y) = b$. Since $xyx^{-1}y^{-1} \in [G, G]$, the image of this element in $G/[G, G]$ is the identity e' in this group. So,

$$e' = \pi(xyx^{-1}y^{-1}) = \pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = aba^{-1}b^{-1}$$

and this says, $ab = ba$. a, b are arbitrary and so $G/[G, G]$ is abelian. □

(d) If H is any normal subgroup of G such that G/H is abelian, show that $\hat{S} \subset H$.

Solution. Consider the onto group homomorphism $p : G \to G/H$. If $s = xyx^{-1}y^{-1}$, $p(s) = e'$,, the identity of G/H, since it is abelian. Thus the kernel of p contains all such s and then it contains $[G, G]$ □

(6) (a) Let G be a group and Z its center. If G/Z is cyclic, show that $Z = G$.

Solution. As usual, we consider the onto group homomorphism, $\pi : G \to G/Z$ and let $b \in G/Z$ be a generator (G/Z is cyclic). Lift it to $a \in G$. Then, any element $x \in G$ is of the form $x = a^k z$ where $k \in \mathbb{Z}$ and $z \in Z$ and can be seen as follows. We know that $\pi(x) = b^k$ for some k and then, $\pi(a^{-k}x) = b^{-k}b^k$, identity of G/Z and so this element belongs to the kernel which is Z. So, $a^{-k}x = z \in Z$ and then, $x = a^k z$. Now, take two elements $x = a^k z_1, y = a^l z_2$, where k, l are integers and $z_1, z_2 \in Z$. Then,

$$xy = a^k z_1 a^l z_2 = a^k a^l z_1 z_2.$$

Now use again $z_1 z_2 = z_2 z_1, a^k a^l = a^l a^k$ etc. to get $xy = yx$. □

(b) Show that any group of order 9 is abelian.

Solution. This is the hardest of the problems and the statement is true for any group of order p^2, p any prime. Since the proof is similar, I shall give a proof of the general result. If you fail to finish this problem, do not despair.
So, let G be a group with $o(G) = p^2$. By Lagrange, every element in G must have order 1, p or p^2, since this order must divide $o(G)$. The only element with order 1 is e. If it had an element of order p^2, then it must be the cyclic

group and so we are done. Thus we may assume every element other than e has order p.

Let $S = \{H_1, \ldots, H_n\}$, distinct subgroups (necessarily cyclic) of order p. In a group of order p we have seen that any non-identity element generates it and so $H_i \cap H_j = \{e\}$. Since every non-identity element has order p, they must be in one of the H_i. Thus, we see that $G - \{e\} = \cup(H_i - \{e\})$, a disjoint union. Since each $H_i - \{e\}$ has exactly $p - 1$ elements, we get $p^2 - 1 = n(p - 1)$ and so $n = p + 1$.

Next, we look at the map $\phi : G \to A(S)$ (the group of one-to-one onto maps from S to itself, with composition as the binary operation) given as $\phi(g)(H_i) = gH_ig^{-1}$. Easy to see that this is a group homomorphism. Let $N = \ker\phi$. Then $G/N = \phi(G)$ and $o(G/N) = o(G)/o(N) = o(\phi(G)) = d$. So, d divides p^2 and $o(A(S)) = (p + 1)!$. Since $\gcd(p^2, (p + 1)!) = p$, we see that $d = 1$ or $d = p$. This says $N \neq \{e\}$. Every element g of N has thus the property, $gH_ig^{-1} = H_i$ for all i. If necessary, we restrict to a subgroup of N (if $N = G$) and assume $o(N) = 3$. This says, we have a map $f_i : N \to \mathrm{Aut}(H_i)$ (why?) given as $f_i(g)(x) = gxg^{-1}$ for $g \in N, x \in H_i$. But, $o(H_i) = p$ and thus $o(\mathrm{Aut}(H_i)) = p-$, so f_i is not one-to-one. But, $o(N) = 3$, so its subgroups are just the trivial groups and thus kernel of f_i is all of N. This says, $N \subset Z(G)$ and then the previous problem finishes the proof.

We will give a slightly better proof after we do class equation. □