PROBLEM SET 4 (Solutions)

1. 58 #6

   $G_1, G_2$ simple. Show $H \triangleleft G = G_1 \times G_2$, $H = G_1$ or $H = G_2$.

   \[ H \triangleleft G \iff H \triangleleft G_1 \text{ or } H \triangleleft G_2 \]

   **Proof:**

   \[ G = \{ (g_1, g_2) | g_1 \in G_1, g_2 \in G_2 \} \quad (i = 1, 2 \text{ for which problem}) \]

   Let $\pi_i$ be projection into $G_i$.

   Let $H_i = \pi_i(H)$ so

   \[ H = \{ (h_1, h_2) | h_1 \in H_1, h_2 \in H_2 \} \]

   $H \triangleleft G \iff g^i H g^{-i} = H \quad \forall g \in G$

   but $g \in G$ is $g = (g_1, g_2) \in G_1 \times G_2$ so

   \[ H \triangleleft G \Rightarrow g^1 H g^{-1} = H \quad \forall g \in G \]

   \[ g_1^1 H g_1^{-1} = H_1 \text{ and } g_2^1 H_2 g_2^{-1} = H_2 \quad \forall g_1 \in G_1 \]

   \[ \Rightarrow H_1 = G_1, \quad H_2 = G_2 \]

   Since $G_1, G_2$ normal $H_1 = \{ 1 \}$ or $G_1$ and $H_2 = \{ 1 \}$ or $G_2$.

   If both just identity then $H = 1$.

   If both all of $G_i$, then $H = G_i$.

   Thus either $1 \times G_2$ or $G_1 \times \{ 1 \}$.

   Clearly $\pi_1$ is an isomorphism for case 1 and

   $\pi_2$ isomorphism for case 2. Thus

   $H \triangleleft G_1$ or $H \triangleleft G_2$. 

If \( HK = G \), \( H, K \leq G \) then \( |H : H \cap K| = |G : H \cap K| \).

**Proof:** Let \( \alpha : H \times K \to G \)
\[
(h, k) \mapsto hk
\]
and note \( HK = G \) is \( \alpha \) onto.

Consider \( \Gamma = \alpha^{-1}(hk) = \{ (h', k') \mid h' \in H, k' \in K, h'k' = hk \} \).

Notice \( h'k' = hk \iff h' = hk (k')^{-1} = h (k''k')^{-1} \)
\[
\quad \iff k' = (k')^{-1} \quad \iff h'k = (h''h)k.
\]

Note \( h'k' = hk \iff k'^{-1} = h' \quad \iff h'k = (h''h)k \)

Let \( f = k'^{-1} = h'^{-1}h \in H \cap K \)
\[
\quad \iff h''h = h' \quad \iff k' = fk.
\]

Thus, for \( h \in H, k \in K \)
\[
\alpha^{-1}(hk) = \{ (h', k') \mid h' \in H, k' \in K, \exists f \in H \cap K : h''h = h', k' = fk \}.
\]

Notice each \( f \in F \) will produce exactly one (unique)
element of \( H \) and \( K \), i.e.
\[
f \in F, k' = fk \quad \text{and} \quad k'' = f'k \implies k' = k''.
\]

and \( fK = f_2K \implies f = f_2 \) (similar for \( h \)).

So \( |\alpha^{-1}(hk)| = |H \cap K| \), \( h \in H \cap K = G \)

So \( \alpha : H \times K \to G \) is a \( H \cap K \to 1 \) map

Recall \( H \times K = H \cdot K \). Now, there are \( |H \cap K| \) elements of \( H \times K \)
for each element of \( G \). So \( |H \cap K| \cdot |G| = |H \cdot K| = |H| \cdot |K| \).
3. Note that $I$ clearly contains the identity and is closed under inverses: if $a \in I$, then $a = a(a^{-1}a^{-1}) = a(a^{-1}) = a$.

Consider the case where $|I| > \frac{1}{2} |G|$. Fix a nonidentity $a \in I$. Then by the pigeonhole principle, $H = I \cap aI > \frac{1}{2} |G|$. Fix some element $ab \in H$. Then $a(ab) = a(a(a^{-1}b^{-1})) = b^{-1}a^{-1}$. Implies $a(ba) = ba$. So $a$ commutes with all elements $b \in I$ where $ab \in H$, and the centralizer subgroup of $a$ contains $\frac{1}{2} |G|$ elements, so the centralizer of $a$ must be $G$ (by Lagrange’s theorem) for all $a \in I$. This means every element of $G$ commutes with every element of $I$, which means the centralizer of $G$ contains $I$, and Lagrange’s theorem tells us the centralizer of $G$ is $G$, so $G$ is abelian.

When $|I| = \frac{1}{2} |G|$, a similar argument applies. By the pigeonhole principle, because the action of $a$ on $I$ is injective, we have $H = I \cap aI \geq \frac{1}{2} |G|$, and that $a$ commutes with every element in $a^{-1}H$. As before, we see that $a^{-1}H$ is contained in the centralizer $C(a)$ of $a$. By Lagrange’s theorem, either $|C(a)| = \frac{1}{2} |G|$ or $|C(a)| = |G|$. Suppose $|C(a)| = |G|$ for all $a \in I$. Then $G$ is abelian as before, and $I$ is closed under multiplication: for $a, b \in I$, $a(ab) = a^{-1}b^{-1} = b^{-1}a^{-1} = (ab)^{-1}$. This would mean that $I$ is a subgroup, which is a contradiction by Lagrange’s theorem (it has order $\frac{1}{2} |G|$).

So there is some $a$ with $C(a) = a^{-1}H$ and $|C(a)| = \frac{1}{2} |G|$. It suffices to show this group is abelian. Fix $b$ and $c$ in $C(a)$. Then $bc$ is also in $a^{-1}H$ and in particular in $I$, so $a(bc) = c^{-1}b^{-1} = a(b)c = b^{-1}c^{-1}$ and $b$ and $c$ commute, so $C(a)$ is an abelian subgroup of index 2 as desired.

4. Every element of $(S)$ is a word on $S$ of the form $s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}$ where $s_i \in S$. Consider $\sigma = s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}g^{-1}$ for any $g \in G$. This is equal to $g\sigma g^{-1} = s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}g^{-1}$ for some $s_i \in S$ because $g\sigma g^{-1} \in S$.

Continuing this, we can move the $g^{-1}$ past all elements in the word until we reach $g^{-1}s_1^{a_1}\cdots s_n^{a_n} = s_1^{a_1}\cdots s_n^{a_n} \in (S)$, so $(S)$ is normal.

Now suppose $T \subseteq G$ and $S = \cup g \in G g^{-1} T g$. Each element of $S$ is of the form $g^{-1}t g$ for some $g \in G$ and $t \in T$. Any normal subgroup containing $T$ necessarily contains these elements, and any group containing these elements necessarily contains the group generated by them. However, it is easy to see that $(S)$ is normal if $g^{-1}t g \cdots g^{-1}t a g \in (S)$, noting that taking powers of elements collapse them, conjugation by $h$ yields $(g h)^{-1}t h \cdots (g h)^{-1}t a h g h \in (S)$, so it is the smallest normal subgroup containing $T$, as desired (because if $T \subseteq N$ is a normal subgroup, then $(S) \subseteq N$ by the above reasoning).

6. Let $H = \{ \pm 1 \}$. By the fundamental theorem of group homomorphisms, we know that $G/H$ is a 4-element group consisting of the cosets $H, \alpha H, \beta H, \text{ and } \gamma H$. There are only 2 groups of order 4, and each of the elements here has order 2, so this group is not cyclic and hence isomorphic to $V_4 = \{ e, a, b, ab \}$. So the map $\phi$ sending $\pm 1$ to $\alpha, \pm \alpha b$ to $\beta$, and $\pm b$ to $ab$ is easily seen to be a homomorphism, as it is the composition of the natural homomorphism to the quotient group and and an isomorphism from the quotient group to $V_4$.

(To see the last map is an isomorphism, note that sends elements of order 2 to elements of order 2, that the map preserves the fact that multiplying any two distinct non-identity elements produces the other non-identity element, and that these facts are enough to characterize the multiplication tables of both groups.)
(5) Let $\mathfrak{F}_n := \text{free gp. on } (n-1) \text{ generators } x_2, \ldots, x_n$

\[ \mathfrak{F}_n = \mathfrak{F}_n / \langle \langle f_{ij}, f(x_{ij})^3, \{ x_i x_j x_i x_j \} \rangle \rangle \]

II \implies x_i x_j x_i \equiv (1) \ x_j x_i x_j \quad \text{in } \mathfrak{F}_n.

III \implies x_j x_i x_k \equiv (2) \ x_i x_k x_i x_j x_i \quad \text{in } \mathfrak{F}_n.

Consider the copy $\overline{\mathfrak{F}}_{n-1} \cong \langle x_2, \ldots, x_{n-1} \rangle \leq \overline{\mathfrak{F}}_n \triangleright \mathfrak{F}_n$ and the commutative diagram of homomorphisms:

\[ \begin{array}{ccc}
\overline{\mathfrak{F}}_{n-1} & \xrightarrow{\phi} & \mathfrak{F}_n \\
\downarrow & & \downarrow \\
\conjugacyClass & \xrightarrow{\phi} & \conjugacyClass
\end{array} \]

Inductively assuming (3) is an isomorphism, we must show that (4) is an isomorphism of sets (hence groups), for which checking

\[ \overline{\mathfrak{F}}_n = \overline{\mathfrak{F}}_{n-1} \sqcup x_n \overline{\mathfrak{F}}_{n-1} \sqcup x_2 x_n \overline{\mathfrak{F}}_{n-1} \sqcup \ldots \sqcup x_n x_n \overline{\mathfrak{F}}_{n-1} \]

will suffice. An arbitrary coset may be written

\[ \overline{\mathfrak{F}}_{n-1} \]

where $\overline{x}$ is a word of length $k$ not ending in $x_n$, with no "$x_i x_i$" ($2 \leq i \leq n$).

Inductively assume that if $\text{len}(\overline{x}) < k$, then $\overline{x} \neq x_n \overline{\mathfrak{F}}_{n-1}$ is one of the cosets in (5).

Now, (6) is either of the form

\[ \overline{x} \overline{x} \overline{\mathfrak{F}}_{n-1} = \overline{x} \overline{x} \overline{\mathfrak{F}}_{n-1} \]

or

\[ \overline{x} \overline{x} \overline{\mathfrak{F}}_{n-1} = \overline{x} \overline{x} \overline{\mathfrak{F}}_{n-1} \]

In each case, $\overline{x} \neq x_n \overline{\mathfrak{F}}_{n-1}$ has length $k-1$ and we are done by 2nd induction.

We know the cosets on $\text{RUS}(5)$ are disjoint b/c they map to each in $\mathfrak{F}_n$.\)
(7) Show (i) that (for arbitrary group $G$) $[G, G] \leq G$, and (ii) that the resulting quotient group $G/[G, G]$ is abelian. Finally, (ii) show that $\mathbb{A}_S \cong \mathfrak{A}_S/[\mathfrak{A}_S, \mathfrak{A}_S]$. (Here $\mathbb{A}_S$ is the free abelian group on $S$ and $\mathfrak{A}_S$ the [nonabelian] free group.)

(i) For some $a^{-1}b^{-1}ab \in [G, G]$ and an arbitrary element $g \in G$, notice that
\[
g^{-1}a^{-1}b^{-1}abh : b^{-1}a^{-1}
= (g^{-1}a^{-1}b^{-1})(ab)(bag)(g^{-1}b^{-1}a^{-1})
= (bag)^{-1}(g^{-1}b^{-1}a^{-1})^{-1}(bag)(g^{-1}b^{-1}a^{-1})
\]
is contained in $[G, G]$ and since $bab^{-1}a^{-1}$ is also contained in $[G, G]$, so is $g^{-1}a^{-1}b^{-1}abh$, which shows $[G, G] \leq G$.

(ii) For any two elements $g, h \in G$, since $h^{-1}g^{-1}hg \in [G, G]$, then $hgh[G, G] = gh[G, G]$, which is to say $G/[G, G]$ is abelian.

(iii) $\mathbb{A}_S$ is the group of formal sums on $S$, i.e., each element of $\mathbb{A}_S$ has the form of a formal sum $\sum_{s \in S} a_s s$, where $a_s \in \mathbb{Z}$ and $s \in S$. Now we define a surjective homomorphism $\varphi : \mathfrak{A}_S/[\mathfrak{A}_S, \mathfrak{A}_S] \rightarrow \mathbb{A}_S$ such that for every word $w \in \mathfrak{A}_S$, $\varphi(w[\mathfrak{A}_S, \mathfrak{A}_S]) = \sum_{s \in S} a_s s$, where $a_s$ is the “net number” of $s$ in $w$, i.e., $a_s = \#$ of $s$ in $w - \#$ of $s^{-1}$ in $w$.

We first need to check $\varphi$ is well-defined. Let $w, w'$ be two distinct words in $\mathfrak{A}_S$ such that $w[\mathfrak{A}_S, \mathfrak{A}_S] = w'[\mathfrak{A}_S, \mathfrak{A}_S]$. Since we can change the order of symbols of a word without changing the coset, and let $e_i$ denote the net number of symbol $s_i$ in the word $w$ and $e'_i$ be the net number of $s_i$ in $w'$, the $w[\mathfrak{A}_S, \mathfrak{A}_S] = (\prod_{s \in S} e_i^n)[\mathfrak{A}_S, \mathfrak{A}_S] = w'[\mathfrak{A}_S, \mathfrak{A}_S] = (\prod_{s \in S} e'_i^n)[\mathfrak{A}_S, \mathfrak{A}_S]$, i.e., $\prod_{s \in S} e_i^n \in [\mathfrak{A}_S, \mathfrak{A}_S]$, then we must have $e_i = e'_i$, and hence $\varphi(w[\mathfrak{A}_S, \mathfrak{A}_S]) = \varphi(w'[\mathfrak{A}_S, \mathfrak{A}_S])$, which shows the definition of $\varphi$ is independent of the choice of the word. Then it is easy to check $\varphi$ is a homomorphism and it is obviously surjective. To show that $\varphi$ is also injective, assume $\varphi(z[\mathfrak{A}_S, \mathfrak{A}_S]) = 0$ for some word $z \in \mathfrak{A}_S$, then by definition the net number of each symbol $s_i \in S$ is 0 and hence $z[\mathfrak{A}_S, \mathfrak{A}_S] = 1$, which completes our proof.
(8) Check the claim on page 92 of the notes: given an automorphism \( \alpha \in \text{Aut}(\mathfrak{S}_n) \) sending transpositions to transpositions and \((12) \rightarrow (ab), (13) \rightarrow (ac) \ (c \neq a, b) \) in particular, show that \( \alpha((1y)) = (ad) \) for some \( d \neq a \) (depending on \( y \neq 1 \)).

Firstly in the case that \( n = 2 \), \( \text{Aut}(\mathfrak{S}_n) \) is trivial and so is the claim. Then for \( n \neq 6 \), every automorphism on \( \mathfrak{S}_n \) is inner, which is to say it corresponds to a permutation \( \tau \) sending transposition \((xy)\) to \((\tau(x)\tau(y))\). And for our automorphism \( \alpha((xy)) = \tau(xy)\tau^{-1} \), it is obvious that \( \tau(1) = a \). Finally, for \( n = 6 \), \( \text{Aut}(\mathfrak{S}_6) = \mathfrak{S}_6 \times \mathbb{Z}_2 \). Due to the same reason in other symmetric groups, all inner automorphisms send \((1y) = (ad)\) for some \( d \neq a \) when \( y \neq 1 \). We claim that if an automorphism sends transposition to transposition, then it must be inner. Let us assume an automorphism \( \alpha \) on \( \mathfrak{S}_6 \) sends \((12) \) to \((ab) \), then the restriction of \( \alpha \) on \(((13), (14), (15), (16)) = \mathfrak{S}_5 \) could be inner (if not, use a automorphism sending the generators of \( \alpha(\mathfrak{S}_5) \) to generators of \( \mathfrak{S}_5 \) and compose it with \( \alpha \)). We assume that \( \alpha((13)) = (a'c), \alpha((14)) = (a'd), \alpha((15)) = (a'e) \) and \( \alpha((16)) = (a'f) \) where \( a, a', b, c, d, e, f \in \{1, 2, 3, 4, 5, 6\} \) such that \( a \neq b \) and \( a', c, d, e, f \neq a \). Now if \( a = a' \), then we are done. Otherwise without loss of generality, we can assume \( a = c \). Now firstly if \( b \) is not equal to any of \( d, e, f \), since \( \alpha(23) = \alpha((13)(12)(13)) = (a'c)(ob)(a'c) = (a'b) \), then \( \alpha((23)(14)) = (a'b)(a'd) \), which is a contradiction since the left-hand side is an element of order 2 while the right-hand side is an element of order 3; therefore \( b \) must be one of \( d, e, f \), and again without loss of generality we can assume \( b = d \), but \( \alpha((34)) = \alpha((13)(14)(13)) = (a'c)(a'd)(a'c) = (a'd) = \alpha(12) \) by our assumption, which is impossible. And to conclude from our argument above, the automorphism \( \alpha \) sending transposition to transposition must be inner, and then the statement is obvious.