Solution to Algebra I- MS- 15.pdf

(1a) Given that A, B are subgroups of G such that $A \subseteq N_G(B)$. We first show that $A \cap B \lhd A$. Let $g \in A \cap B$ and $a \in A$ then, clearly $aga^{-1} \in A$ and as $A \subseteq N_G(B)$, $aBa^{-1} = B$ for every $a \in A$ one has, $aga^{-1} \in B$ as well. Thus $A \cap B \lhd A$. Now, $AB = \{ab \mid a \in A, b \in B\}$ is a group as $e \in AB$, for $a_1b_1, a_2b_2 \in AB$, $a_1b_1a_2b_2 = a_1a_2(a_2^{-1}b_1a_2)b_2 = a_1a_2b_3b_2$ where $a_2^{-1}b_1a_2 = b_3 \in B$ and finally, $ab(a_0b_0)^{-1} = abb_0^{-1}a_0^{-1} = aa_0^{-1}(a_0bb_0^{-1}a_0^{-1}) = aa_0^{-1}b_1 \in AB$ where $a_0bb_0^{-1}a_0^{-1} = b_1 \in B$. Also, $B \lhd AB$ since $abB(ab)^{-1} = abBb^{-1}a^{-1} = aBa^{-1} = B$ as $A \subseteq N_G(B)$. We now define $\phi : A/A \cap B \longrightarrow AB/B$ as $\phi(aA \cap B) = aB$. This ,map is well defined for if $a_1^{-1}a_2 \in A \cap B$ then $a_1^{-1}a_2 \in B$. It also maps cosets to cosets, in fact, if $a_1, a_2 \in aA \cap B$ then $a_1^{-1}a_2 \in B$ so that $a_1, a_2 \in aB$. Observe that ϕ is a homomorphism, $\phi((aA \cap B)(bA \cap B)) = \phi(abA \cap B) = abB = aB\ bB = \phi(aA \cap B)\phi(bA \cap B)$. It remains to show that ϕ is a bijection. Suppose $\phi(aA \cap B) = \phi(bA \cap B) \Longrightarrow aB = bB \Longrightarrow a^{-1}b \in B$ but $a, b \in A$ implies $a^{-1}b \in A$. So, $a^{-1}b \in A \cap B \Longrightarrow aA \cap B = bA \cap B$. This proves injection. Suppose $gB \in AB/B$, this implies $g = ab$ for some $a \in A, b \in B$ so that $gB = abB = aB \Longrightarrow gB = \phi(aA \cap B)$. Thus, ϕ is a surjection and hence an isomorphism.

(1b) $N \lhd G$ with $|G/N| = p$ and $H \leqslant G$. Suppose $H \nsubseteq N$. As N is normal in G, and H is a subgroup of G, we conclude $H \subseteq N_G(N)$, $NH \leqslant G$ and by 1(a) $H \cap N$ is normal in H. Now, $p = [G : N] = [G : NH][NH : N]$. We claim that $[NH : N] = p$ so that $[G : NH] = 1$ giving $G = NH$. Suppose $[NH : N] = 1$.cOne has in the finite order case, by the isomorphism in (1a), $|NH| = |N||H|/|N \cap H| \Longrightarrow |H| = |H \cap N|$. This gives $H/H \cap N$ is trivial, *i.e.*, $H = H \cap N \subseteq N$. This is a contradiction to our assumption $H \nsubseteq N$. Thus, $G = NH$ and $[H : H \cap N] = [NH : N] = p$.

(2a) Statement of Cayley's theorem: Any group G is isomorphic to a subgroup of a permutation group.
Proof: Let G be a group. Let F be the set of all permutations (one-one functions) on elements of G. Then F is a group with the groups operation being function composition. Indeed, Function composition is associative and closed, the identity map being one-one belongs to F, for $f \in F$, if $f(x) = y$ then the inverse of f is f^{-1} which maps $f^{-1}(y) = x$. Clearly, $f^{-1} \in F$. Thus, F is a group. Now, for any element $g \in G$, consider the map $f_g(x) = gx$ for all $x \in G$. One has $f_g \in F$. Further, as $gh \in G$, we have $f_{gh} \in F$ and also $f_e \in F$ where e is the identity in G. Observe that $f_{gh}(x) = ghx = g(hx) = g(f_h(x)) = f_g f_h(x)$. Thus the set $\{f_g \mid g \in G\}$ is a subset of F which is closed and so is a subgroup of F. Clearly, G is isomorphic to this subgroup.

(2b) Let G be a finite group of order n, p be the smallest prime dividing n and let N be a subgroup of G of index p. To show that $N \lhd G$. Now, G acts on the left coset space G/N by left multiplication, $g \cdot aN = gaN$. As the index is p, we get a homomorphism ϕ of G into S_p, the symmetric group on p elements. The kernel K of ϕ is the set of all elements of G inducing trivial action on G/N and so $K \subset N$. One has G/K is isomorphic to a subgroup of S_p. This implies its order is a divisor of $p!$. But the order of G/K also divides G and as p is the smallest prime dividing $o(G)$, we have $o(G/K) = p$. One has $p = [G : K] = [G : N][N : K] = p[N : K] \implies [N : K] = 1$, so that $N = K$ is normal subgroup of G.

(3a) We exhibit a one-to-one correspondence between $Orb(x)$ and the left cosets of G_x in G. To the coset $gG_x \in G/G_x$, we associate the element $gx \in Orb(x)$. This association is well defined for, if $gG_x = hG_x$ then, $g^{-1}h \in G_x \implies g^{-1}hx = x \implies hx = gx$. Now, suppose $gx = hx$, then $g^{-1}hx = x \implies g^{-1}h \in G_x \implies gG_x = hG_x$. Thus, the association is one-to-one. If $h \in Orb(x)$ then, $h = gx$ for some $g \in G$ so that the coset gG_x gets associated to h. This proves surjection. We thus have a one-one correspondence between two finite sets which implies that they have the same cardinality.

(3b) Let n be the number of orbits of G-action on X. By orbit stabilizer theorem the size of an orbit $\mathcal{O}$ is given by $|\mathcal{O}| = |G|/|G_x|$ for some $x \in \mathcal{O}$ where $G_x = \{g \in G \mid g \cdot x = x\}$. This implies $|G_x| = |G|/|\mathcal{O}|$. Taking sum over $x \in \mathcal{O}$, $\sum_{x\in\mathcal{O}} |G_x| = |\mathcal{O}||G|/|\mathcal{O}| = |G|$. Thus the sum over all orbits is given by $\sum_{x\in X} |G_x| = |G|n \implies n = \sum_{x\in X} |G_x|/|G|$. Consider the set $G\times X := \{(g, x) \mid g \in G, x \in X\}$ and let $G_0 := \{(g, x) \mid g\cdot x = x\} \subset G\times X$. Then $|G_0| = \sum_{x\in X} |G_x| = \sum_{g\in G} |X^g|$ where $X^g = \{x \in X \mid g \cdot x = x\}$. Thus, $n = \sum_{g\in X} |X^g|/|G|$.

(4a) Statement: Let G be a finite group. The action of G on itself by conjugation partitions G into disjoint conjugacy classes. Let $g_1, ..., g_r$ be the representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then the *class equation* is given by $|G| = |Z(G)| + \sum\limits_{i=1}^{r} [G : C_G(g_i)]$ where $C_G(g_i)$ is the centralizer of g_i in G.
Proof: An element $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$. Let $Z(G) = \{e, z_1, ..., z_m\}$ and let $\mathcal{O}_1, ..., \mathcal{O}_r$ be the conjugacy classes of G not contained in $Z(G)$ having $g_1, ..., g_r$ as the respective representatives. Then $\{\{e\}, \{z_1\}, ..., \{z_m\}, H_1, ..., H_r\}$ gives a partition of G. We thus have $|G| = \sum\limits_{i=1}^{m} 1 + \sum\limits_{i=1}^{r} |H_i| = |Z(G)| + \sum\limits_{i=1}^{r} [G : C_G(g_i)]$.

(4b) (i) We prove this using induction on $|G| = n$. As $p \mid n$, when $|G| = n = p$, any element of G has order p. Now suppose $|G| = n_0 > p$ with $p \mid n_0$ and we asuume the induction hypothesis that for a group G with order $n < n_0$ such that $p \mid n$, G has an element of order p. Since $|G| = n_0$ is not a prime, G has a nontrivial proper subgroup H. We have $|G| = |H| \cdot [G : H]$ which implies that either $p \mid |H|$ or $p \mid [G : H]$. If $p \mid |H|$, by induction hypothesis we are done. We show that the other possibility does not occur. The center $Z(G)$ is a proper subgroup of G. For each $g \in G$, the centralizer $Z_G(g) = \{h \in G \mid hg = gh\}$ of g in G is a proper subgroup of G if $g \notin Z(G)$. If $p \mid |Z_G(g)|$ for some $g \notin Z(G)$, we are done by induction hypothesis. Also, if $p \mid |Z(G)|$, we are done. Now, if the conjugacy classes of size greater than 1 are represented by $g_1, ..., g_r$, by class equation we have $|G| = |Z(G)| + \sum_{i=1}^{r}[G : Z_G(g_i)] = |Z(G)| + \sum_{i=1}^{r} |G|/|Z_G(g_i)|$. The case when p does not divide any $|Z_G(g_i)|$ results in each index $[G : Z_G(g_i)]$ being divisible by p. Hence, the remaining term $|Z(G)|$ will also be divisible by p. That is either p divides $|Z(G)|$ or $p \mid |Z_G(g_i)|$ for some $g \notin Z(G)$. We are done here by induction hypothesis.

(ii) G acts on itself by self conjugation. Let $\mathcal{O}_1, ..., \mathcal{O}_r$ be the various distinct orbits of G. As G is a p-group, the order of each orbit is either 1 or power of p. By class equation $|G| = \sum_{i=1}^{r} |\mathcal{O}_i|$. The conjugacy classes having single elements are those of elements belonging to the center $Z(G)$. Now, LHS is divisible by p and so should be RHS. Thus, the number of single element conjugacy classes is a multiple of p, giving a nontrivial center.

(5a) *Sylow's first theorem*:Let G be a finite group. If p is a prime divisor of $|G|$ then there exists a p-Sylow subgroup of G.
Sylow's second theorem: Let G be a group of order $p^n q$ where p is a prime not dividing q. If P is a p-Sylow subgroup of G and H is any subgroup of G of order a power of p then $H \subseteq xPx^{-1}$ for some $x \in G$. In particular, any two p-Sylow subgroups of G are conjugates.
Sylow's third theorem: The number of p-Sylow subgroups of G divides $|G|$ and is of the form $1 + kp$ for some non-negative integer k.

(5b) Let G be a group of order $224 = 2^5 \cdot 7$. The number n_2 of 2-Sylow subgroups is such that $n_2 \mid 7$ and $n_2 \equiv 1(mod\ 2)$. Similarly, the number n_7 of 7-Sylow subgroups of G is such that $n_7 \mid 2^5$ and $n_7 \equiv 1(mod\ 7)$. Thus $n_2 = 1$ or 7 and $n_7 = 1$ or 8. Suppose G was simple, then $n_7 = 8$ and $n_2 = 7$. Then there are $(7 - 1) \cdot 8 = 48$ elements of order 7 and $(2^5 - 1) \cdot 7 = 31 \cdot 7 = 217$ elements of order 2 in G. This gives us a total of 266 elements in G including identity which is a contradiction to $|G| = 224$. Hence, G is not simple as we must have either $n_2 = 1$ or $n_7 = 1$.

(6a) Let $G = A_5$ then, $|G| = 60 = 2^2 \cdot 3 \cdot 5$. By Sylow's third theorem we have $n_3 \mid 2^2 \cdot 5$ and $n_3 \equiv 1(mod\ 3)$, so that $n_3 \in \{1, 4, 10\}$. But G contains 20 elements of order 3 ($5C_3$) which implies $n_3 = 10$. Let n_5 be the number of 5-Sylow subgroups of A_5 then, $n_5 \mid 2^2 \cdot 3$ and $n_5 \equiv 1(mod\ 5)$ so that $n_5 \in \{1, 6\}$. But A_5 has 24 elements of order 5, giving $n_5 = 6$. Finally, let n_2 be the number of 2-Sylow subgroups of A_5. Then, $n_2 \mid 3 \cdot 5$ and $n_2 \equiv 1(mod\ 2)$ so that $n_2 \in \{1, 3, 5, 15\}$. Now, A_5 has 15 elements of order 5 which implies $n_2 \in \{5, 15\}$. If $n_2 = 15$ and H is a 2-Sylow subgroup of A_5 then, as A_5 acts on the 2-Sylow subgroups by conjugation, the stabilizer $Stab(H)$ of H has index 15 in A_5. This implies $H = Stab(H) = N_{A_5}(H)$. This is not true as $(1, 2, 3) \in N_{A_5}(H) \setminus H$. Hence, $n_2 = 5$.

(6b) The 3-Sylow and 5-Sylow subgroups of S_5 are contained in A_5 so that $n_3 = 10$ and $n_5 = 6$. A 2-Sylow subgroup of S_5 has order 8. One has $n_2 \mid 15$ and $n_2 \equiv 1(mod2)$ so that $n_2 \in \{1, 3, 5, 15\}$ and as in the case of

A_5, $n_2 \in \{5, 15\}$. Permutation on the set $\{1,2,3,4\}$ gives a copy of D_8 inside S_5 which is a 2-Sylow subgroup of S_5. Thus all 2-Sylow subgroups are isomorphic to D_8. Now, 4 elements can be chosen in 5 distinct ways from $\{1,2,3,4,5\}$. Further, for each choice of 4 elements we have 3 distinct dihedral groups (cyclic permutations results in the same copy of D_8 and so does orderings of the form 1,2,3,4 and 1,4,3,2). We then have $n_2 = 5 \cdot 3 = 15$ distinct subgroups of order 8 isomorphic to D_8.

(7a) Given two groups H and K with a group homomorphism $\phi : H \longrightarrow Aut(K)$ then, the semi-direct product of K by H is denoted $K \rtimes_\phi H$ and is defined as the set $K \times H$ together with the operation $(k,h)\cdot(k_1,h_1) = (k\phi(h)k_1, hh_1)$ such that $(K \times H, \cdot)$ is a group. Evidently, the group operation is very much dependent on the homomorphism ϕ.

(7b) Let $K = \mathbb{Z}_n =< x >$ and $H = \mathbb{Z}_2 =< a >$. Consider the homomorphism $\phi : H \longrightarrow Aut(K)$ given by $\phi(a) = \phi_a$ where $\phi_a(x) = axa^{-1}$ for $x \in K$. It is easy to see that ϕ is a group homomorphism and the semidirect product $G = K \rtimes_\phi H$ is a group with the group operation as in (7a). We assert that $D_{2n} \cong G$. Let $\{(r,m) \mid r^n = m^2 = 1, rm = mr^{-1}\}$ be the presentation of D_{2n}. Since K is a subgroup of index 2 in G, we have $a \cdot x = axa^{-1} = x^{-1}$ for all $a \in H, x \in K$. Hence, $a^2xa^{-1} = ax^{-1}$. As $|H| = 2$, $a^2 = 1$ or $a = a^{-1}$, we have $a^2xa^{-1} = xa$ and $xa = ax^{-1}$. Consequently, the isomorphism of D_{2n} with $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ is given by the mapping $x \longmapsto r$ and $a \longmapsto m$.