ALGEBRA I HOMEWORK II

HOJIN LEE 2021–11045

Problem 1. *Solve the following*

1. *Find an example of a group G with at least two distinct (but equivalent) composition series.*
2. *Find an example of groups $K \leq H \leq G$ with $H \trianglelefteq G$ and $K \trianglelefteq H$ but $K \not\trianglelefteq G$.*
3. *Find an example of a nonabelian group G such that every subgroup is normal.*

Proof. 1. Let $G = \mathbb{Z}/6\mathbb{Z}$. Then $\langle 6\rangle \leq \langle 2\rangle \leq \langle 1\rangle$ and $\langle 6\rangle \leq \langle 3\rangle \leq \langle 1\rangle$ are two different composition series. They are indeed composition series since their quotients are simple. □

Proof. 2. Consider the subgroup $H = \{e, (12)(34), (13)(24), (14)(23)\}$ of A_4. If $\sigma \in S_4$, then $\sigma(ab)(cd)\sigma^{-1}$ sends $\sigma(a)$ to $\sigma(b)$, $\sigma(c)$ to $\sigma(d)$ and vice versa. Either way, this becomes an element of H, obviously. Thus $H \trianglelefteq S_4$ so $H \trianglelefteq A_4$. Also, H is a group of order 4 such that every nontrivial element has order 2, so $H \cong V_4$. The subgroup $\{e, (12)(34)\}$ of H is normal since H is abelian. However, $(123)(12)(34)(123)^{-1} = (14)(23)$, so H is not normal in A_4. □

Proof. 3. Consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Since $ij = -ji$, this group is nonabelian. The nontrivial subgroups are ± 1, $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$, but index 2 subgroups are automatically normal, and ± 1 obviously is invariant under conjugation. Hence all subgroups are normal. □

Problem 2. *Let G a group, $N \trianglelefteq G$.*

1. *If $H \leq G$ is a subgroup where $N \cap H = \{e\}$ and $NH = G$, then G is a semidirect product of H and N, and write $G = N \rtimes H$. In this case, show $H \cong G/N$. If $G = N \rtimes H$, also show $N \times H \to G$ given by $(n, h) \mapsto nh$ is bijective, and it is a group homomorphism if and only if the group homomorphism $\varphi : H \to \mathrm{Aut}(N)$ given by $\varphi(h)(n) = hnh^{-1}$ is trivial.*
2. *Let $1 \to N \to G \xrightarrow{\pi} H \to 1$ be a SES of groups. A splitting of the SES is a group homomorphism $s : H \to G$ such that $\pi \circ s = \mathrm{id}_H$. Show if $s : H \to G$ is a splitting, then $G = N \rtimes s(H)$.*

Proof. 1. Define $f : H \to G/N$ as $h \mapsto hN$. This is obviously a group homomorphism. We claim that f is bijective. We want to show for any $g \in G$, there exists some $h' \in H$ such that $h'N = gN$. Since $G = NH$, we may write $g = n'h'$. Then $gN = n'h'N = h'N$, so f is surjective. Now suppose $hN = N$, i.e. $h \in N$. Then $h = e$ since $N \cap H = \{e\}$. Therefore $H \cong G/N$.

Date: March 20, 2024.

The set map $(n,h) \mapsto nh$ is surjective, since $G = NH$. Suppose $nh = n'h'$. It follows that $n = n'h'h^{-1}$, so $h'h^{-1} \in N$, i.e. $h'h^{-1} = e$. Then $h' = h$. From right cancellation, it also follows that $n = n'$. Thus the set map is bijective.

Suppose $\varphi : H \to \mathrm{Aut}(N)$ is trivial, i.e. $hnh^{-1} = n$ for all $n \in N$ and $h \in H$. For the map to be a group homomorphism, we must have $nn'hh' = nhn'h'$ for all $n, n' \in N$ and $h, h' \in H$. This holds.

Conversely, if $nn'hh' = nhn'h'$ for all n, n', h, h', and take $n = h' = e$, then we get $n'h = hn'$ for all n' and all h. Thus $hnh^{-1} = n$ for all n, h, so φ is trivial. □

Proof. 2. Suppose $s : H \to G$ such that $\pi \circ s = \mathrm{id}_H$. We first show that $N \cap s(H) = \{e\}$ and $Ns(H) = G$. Suppose $g \in s(H) \cap N$. Then, $\pi(g) = e$ by exactness. But, $\pi \circ s = \mathrm{id}_H$, so if $h \in H$ such that $s(h) = g$, then $\pi(s(h)) = e = h$. Therefore $h = e$, so $g = s(e) = e$.

To show $G = Ns(H)$, it suffices to show that every coset gN of N in G can be represented by an element of $s(H)$. Consider the images through π, given by $g \mapsto \pi(g)$ and $s(\pi(g)) \mapsto \pi(s(\pi(g))) = \pi(g)$. It follows that $\pi(g^{-1}s(\pi(g))) = e$, so $g^{-1}s(\pi(g)) \in N$, i.e. $gN = s(\pi(g))N = Ns(\pi(g))$. Therefore, every element of G can be written as an element of $Ns(H)$. It follows that $G = N \rtimes s(H)$. □

Problem 3. *Let H and N be groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism.*

1. *Show that we can endow the set $N \times H$ with the structure of a group via*
$$(n,h)(n',h') = (n(\varphi(h)(n')), hh').$$
Write $N \rtimes_\varphi H$ for the resulting group. Observe $N \rtimes_\varphi H = N \times H$ preciesly when φ is trivial.
2. *Identifying N and H with the subgroups $N \times \{1\}$ and $\{1\} \times H$ of $G = N \rtimes_\varphi H$, show that*
   (a) *$nh = (n,h)$ for all $n \in N$ and $h \in H$,*
   (b) *$N \trianglelefteq G$ and*
   (c) *$\varphi(h)(n) = hnh^{-1}$ for all $h \in H$ and $n \in N$.*

   Conclude that $G = N \rtimes H$ and $(n,h)(n',h') = (nhn'h^{-1}, hh')$ for all $(n,h), (n',h') \in G$.

Proof. 1. We show that the operation has identity, is associative, and has inverse.

Consider $(e_N, e_H) \cdot (n,h)$. This is $(e_N(\varphi_{e_H}(n)), h) = (n,h)$. Also, $(n,h) \cdot (e_N, e_H) = (n(\varphi_h(e_N)), h) = (n,h)$, so (e_N, e_H) is the identity.

Now we show $(n_1,h_1)\cdot(n_2,h_2)\cdot(n_3,h_3)$ is well-defined. First, $(n_1,h_1)\cdot(n_2,h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2)$, and multiplying again with (n_3,h_3) results in

$$(n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3).$$

Now in the other direction, $(n_2,h_2) \cdot (n_3,h_3) = (n_2\varphi_{h_2}(n_3), h_2h_3)$, and again multiplying with (n_1,h_1) on the left makes $(n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3)$. The two agree, so the operation is associative.

Now we claim that $(n,h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Multiply by (n,h) on the right to get $(\varphi_{h^{-1}}(n^{-1})\varphi_{h^{-1}}(n), h^{-1}h) = (e_N, e_H)$. The same holds on the left. Note that $n\varphi_h(n') = nn'$ for all n, n', h if and only if $\varphi_h = \mathrm{id}_N$ for all h, i.e. φ is trivial. □

Proof. 2. (a) $nh = (n,1)\cdot(1,h) = (n\varphi_1(1), h) = (n,h)$.

(b) We show that $(n,h)\cdot N\cdot(n,h)^{-1}\subset N$. Suppose we have $(n',1)$. Then, $(n,h)\cdot(n',1)\cdot(n,h)^{-1}=(n\varphi_h(n'),h)\cdot(n,h)^{-1}=(n\varphi_h(n'),h)\cdot(\varphi_{h^{-1}}(n^{-1}),h^{-1})=(n\varphi_h(n')n^{-1},1)\in N$.

(c) $hnh^{-1}=(1,h)\cdot(n,1)\cdot(1,h)^{-1}=(1,h)\cdot(n,1)\cdot(\varphi_{h^{-1}}(1),h^{-1})=(1,h)\cdot(n,1)\cdot(1,h^{-1})=(\varphi_h(n),h)\cdot(1,h^{-1})=(\varphi_h(n),1)\sim\varphi_h(n)$.

Therefore, $N\cap H=\{1\}\times\{1\}$, and $NH=G$ by (a), so we have $G=N\rtimes H$. Also, since $\varphi_h(n)=hnh^{-1}$, we have $(n,h)\cdot(n',h')=(nhn'h^{-1},hh')$. □

Problem 4. *Let p,q be prime. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.*

Proof. Using the class formula $|G|=|Z(G)|+\sum_x[G:G_x]$ where x runs through non central elements of G, and G acts on itself by conjugation, we conclude that since $|G|=p^2$, and each $[G:G_x]$ is divisible by p, that $|Z(G)|$ must be divisible by p. Thus $|Z(G)|$ is either of order p or order p^2. In the latter case, $G=Z(G)$ so G is abelian. In the former case, $G/Z(G)$ is a group of order p, hence cyclic. In homework I, we have proved that if $G/Z(G)$ is cyclic, then it must be trivial. Therefore the former case cannot even happen, so G is abelian. Since G is abelian in all cases, we may use the structure theory of finitely generated abelian groups to conclude there exist only two up to isomorphism, namely $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. □

Problem 5. *Let p,q be distinct primes. Prove that a group of order p^2q is solvable, and one of its Sylow subgroups is normal.*

Proof. First assume $q<p$. Then q is the smallest prime dividing $|G|$. Also, by the Sylow theorems there exist a Sylow-p subgroup H. Then $[G:H]=q$, so by Lemma 6.7 we have $1\trianglelefteq H\trianglelefteq G$. By Problem 4, we know that H is abelian. Also, $|G/H|=q$, so $G/H\cong\mathbb{Z}/q\mathbb{Z}$. Hence G is solvable.

Now suppose $p<q$. Again by the Sylow theorems, there exists a subgroup H of order q, and $n_q\equiv 1 \bmod q$. Note that $n_q=|\operatorname{orb}(H)|=[G:N_G(H)]$, where since $[G:H]=p^2$, n_q must divide p^2. Therefore, $n_q=1,p,p^2$. However $n_q\neq p$ since otherwise $p=1+nq$ for $n>0$, but by assumption $p<q$. Thus we have two possibilities; $n_q=1$ or $n_q=p^2$.

Suppose $n_q=1$. Since all Sylow q-subgroups are conjugate, H is self-conjugate, i.e. is normal. Therefore $1\triangleleft H\triangleleft G$, where $H\cong\mathbb{Z}/q\mathbb{Z}$ and G/H is abelian, again by Problem 4. In this case G is solvable.

Now suppose $n_q=p^2$. Then each of the p^2 Sylow q-subgroups has $q-1$ elements of order q, and in this case distinct Sylow q-subgroups intersect trivially, we conclude G has $p^2(q-1)$ elements of order q. Thus G has p^2 elements of order not q. We also know that there exists a Sylow p-subgroup of order p^2, and all elements of such subgroup must have order dividing p^2. If the order divides p^2, then it certainly is not q, so the p^2 elements having order not q are contained in a Sylow p-subgroup, and in fact they form this unique p-subgroup, since elements either have order q or not. Denote this Sylow p-subgroup as P. By uniqueness $1\trianglelefteq P\trianglelefteq G$, and $G/P\cong\mathbb{Z}/q\mathbb{Z}$, also P is of order p^2, hence abelian. □

Problem 6. *Let p,q be odd primes. Prove that a group of order $2pq$ is solvable.*

Proof. In the case $p=q$, the group G has a Sylow p-subgroup of index 2, which is normal. If we call this H, then H has order p^2, and $G/H\cong\mathbb{Z}/2\mathbb{Z}$ so G is solvable.

WLOG let $p < q$. By the Sylow theorems, there exists a subgroup of order q, and $n_q \equiv 1 \bmod q$, and n_q must divide $2p$. Thus n_q may be one of $1, 2, p, 2p$. Since 2 and p are impossible, $n_q = 1, 2p$.

Suppose $n_q = 1$. Then there exists a unique Sylow q-subgroup, which is normal. Call this H. Then we have $1 \trianglelefteq H \trianglelefteq G$, where G/H is of order $2p$. Order $2p$ groups are solvable, since by the Sylow theorems we have a subgroup of order p, and its index is 2, so it is normal. The quotients are $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ respectively, thus G/H is solvable. Since G/H and H are solvable, G is solvable.

Now suppose $n_q = 2p$. There are $2p$ Sylow q-subgroups, each having $q - 1$ elements of order q, so G has $2p(q-1)$ elements of order q. Therefore, G has $2p$ elements having order not q. Also, by the Sylow theorems, there exists a Sylow p subgroup, and $n_p = 1, q, 2q$. Since all Sylow p-subgroups intersect trivially (if they share a nontrivial element, they are the same, since they are cyclic) if we have $n_p = q$ or $2q$, then we would have $q(p-1)$ or $2q(p-1)$ elements having order p. We claim that $q(p-1) > 2p$, which implies that $n_p = q$ or $2q$ cannot happen.

Since we assumed $p < q$, we know $q \geq 5$. Hence $q - 2 \geq 3 \Rightarrow \frac{2}{3} \geq \frac{2}{q-2} \Rightarrow 1 + \frac{2}{q-2} \leq \frac{5}{3}$, and also p is an odd prime so $p > 2$. Thererfore $1 + \frac{2}{q-2} \leq \frac{5}{3} < p \Rightarrow q < pq - 2p \Rightarrow 2p < q(p-1)$.

Therefore $n_p = 1$, so there is a unique Sylow p-subgroup of G, say H. Then H is normal, so $1 \triangleleft H \triangleleft G$, where G/H is of order $2q$. As we argued above, order $2q$ groups are solvable. Therefore G is solvable. □

Problem 7. *Show every group of order < 60 is solvable, and find a non-solvable group of order 60.*

Proof. We consider the cases of order p^k, $p^k m$ where $1 < m < p$, and where $m! < p^k m$. We already know that all order p^k groups are solvable.

Now suppose $|G| = p^k m$ where $1 < m < p$. Then by Sylow theorems, there exists a Sylow p-subgroup where $n_p \equiv 1 \bmod p$, and n_p divides m. For this to happen, n_p must be 1, since otherwise n_p exceeds m. Therefore this Sylow p-subgroup is unique, hence normal, and the quotient group is of order m.

This time suppose $|G| = p^k m$ where $m! < |G|$. Let P denote the set of Sylow p-subgroups of G. Define a homomorphism $G \to S_P$ by conjugation action, where $|P|$ is at most m, so $|S_P| \leq m! < p^k m = |G|$. The kernel of this homomorphism must be nontrivial. If the kernel is all of G, then $|P| = 1$, so (by abuse of notation) $P \trianglelefteq G$, and G/P is of order m, and P is solvable.

In both cases, solvability of the group depends on the solvability of the group of order m. We want that m is again of the form $q^k m'$ for some prime q, and some m' satisfying either of the two conditions. Therefore, it is enough to check numbers below 60 that do not satisfy the above conditions.

First, numbers of the form pq for distinct primes, take the larger one to be p. For numbers $p^2 q$, we need not treat them since we already proved such groups are solvable in Problem 5. Now we look at numbers of the form $p^3 q$. If $q < p$, we are done. If $p < q$, we need $(q-1)! < p^3$. Such (p, q) that are possible are $(2,3), (2,5), (2,7)$, but $(2,5)$ and $(2,7)$ do not satisfy $(q-1)! < p^3$ since $8 < 24$ and $8 < 6!$. Therefore we need special proofs for order 40, 56. Now look at numbers of the form $p^4 q$. Again, if $q < p$ we are done. If $p < q$, the only possible combination is $(2,3)$, and since $2! < 2^4$ this satisfies the conditions.

Now we look at numbers of the form pqr, for $p < q < r$ primes. In this case, the only two possible combinations are $(2, 3, 5)$ and $(2, 3, 7)$ which are of the form $2pq$, which we know to be solvable. The smallest number not of the forms listed above is $60 = 2^2 \times 3 \times 5$, so all we need to prove is for order 40 and 56.

Since $40 = 5 \times 8$, we must have $n_5 \equiv 1 \bmod 5$, and must divide 8, so $n_5 = 1$. Call this normal subgroup H, then G/H is of order 8, hence solvable, and H itself is cyclic so is solvable.

Now consider a group of order $56 = 2^3 \times 7$. We have $n_7 \equiv 1 \bmod 7$, and must divide 8 so is either 1 or 7. If $n_7 = 1$, there is nothing else to prove. Suppose $n_7 = 8$. Then each Sylow 7-subgroup has 6 elements of order 7, so G has $6 \times 8 = 48$ elements of order 7. Therefore G has 8 elements of order not 7. Since this group has a Sylow 2-subgroup of order 8, such group must be unique, otherwise there are more than 8 elements of order not 7. Hence the Sylow 2-subgroup is unique, thus normal, and the quotient has order 7 thus cyclic. Therefore all groups of order < 60 are solvable!

We claim that A_5, of order 60, is not solvable. Since A_5 is nonabelian, it suffices to show that A_5 is simple. In class, we showed that A_5 is generated by 3-cycles, so it suffices to show that all 3-cycles of A_5 are conjugate, and show that every nontrivial normal subgroup contains a 3-cycle.

Suppose we have $(x_1x_2x_3)$ and $(y_1y_2y_3)$ as 3-cycles in A_5. Denote by x_4, x_5 and y_4, y_5 the remaining symbols, respectively. Note that there exists a permutation σ sending x_i to y_i for $1 \leq i \leq 5$, and if this σ has negative sign, then compose σ with (x_4x_5) to get an element of A_5. This still sends $(x_1x_2x_3)$ to $(y_1y_2y_3)$ since it doesn't interfere with $1 \leq i \leq 3$. Notice that $\sigma(x_1x_2x_3)\sigma^{-1} = (y_1y_2y_3)$ via checking where each y_i maps to.

Now suppose $1 \neq N \trianglelefteq A_5$. If N does not contain a 3-cycle, then it either contains the product of two disjoint transpositions, or a 5-cycle. This is because elements of A_5 are either the identity, a 3-cycle, a 5-cycle, or a proudct of two disjoint transpositions. If N contains a 5-cycle, then N contains all 5-cycles, since by the Sylow theorems we know that elements of order 5 are contained in Sylow 5-subgroups, and these subgroups are all conjugate to one another. Together with the fact that N is normal, this implies N contains all 5-cycles. Then just take $(12345)(12543) = (132) \in N$. If N contains the product of two disjoint transpositions, say $(ab)(cd)$, then for $\sigma \in A_5$, $\sigma(ab)(cd)\sigma^{-1}$ sends $\sigma(a)$ to $\sigma(b)$ and $\sigma(c)$ to $\sigma(d)$. Setting $\sigma(e) = e$ and by changing the alphabets, this can be the product of any two disjoint transpositions in A_5. Thus N contains all such elements. Then, take $(12)(34)(12)(35) = (354)$. □

Problem 8. *Let G be a finite group.*

1. *Let H be a proper subgroup of G. Show G is not the union of all the conjugates of H.*
2. *Suppose G acts transitively on a set S with $|S| \geq 2$. Prove that there is an element $x \in G$ such that $xs \neq s$ for all $s \in S$.*

Proof. 1. Let $[G : H] = n$. We have $|G| = n|H|$ for $n > 1$. Also, conjugates gHg^{-1} of H are subgroups of G, since they contain the identity and are multiplicatively closed. Since conjugation is bijective on G, we conclude that there are at most n distinct gHg^{-1}'s. Since each gHg^{-1} contains the identity, there are at most

$n(|H|-1)+1$ distinct elements in $\bigcup_{g\in G} gHg^{-1}$. We assumed $1-n<0$ so this is strictly less than $n|H| = |G|$. □

Proof. 2. Suppose each $g \in G$ has a fixed point. Therefore we have $\sum_{x\in S} |G_x| > |G|$, since each $g \in G$ belongs to one of the G_x, and each G_x all contains e (and $|S| > 1$). By Problem 9, we know that $\sum_{x\in S} |G_x| = |G\backslash S||G|$, so $|G\backslash S| > 1$. Therefore the G-action cannot be transitive. □

Problem 9. *Let G be a finite group acting on a finite set S. For each $x \in G$ let $F(x) = |\{s \in S \mid xs = s\}|$. Show $|G\backslash S| = \frac{1}{|G|}\sum_{x\in G} F(x)$.*

Proof. We first construct a bijection between $\operatorname{orb}(x)$ and the set of left cosets G/G_x of the stabilizer subgroup G_x of x in G. Given gx in the orbit, send this to gG_x. If $gx = g'x$, then $g^{-1}g'x = x$, so $g^{-1}g' \in G_x$ which implies $gG_x = g'G_x$. Therefore, this function is well-defined. This is obviously surjective, and suppose $gG_x = g'G_x$. Then $g^{-1}g' \in G_x$, so $g^{-1}g'x = x$, so $g'x = gx$. Hence this correspondence is bijective.

Now, notice that

$$|G\backslash S| = \sum_{\text{orbit}\in G\backslash S} 1 = \sum_{\text{orbit}\in G\backslash S} \sum_{x\in\text{orbit}} \frac{1}{|\operatorname{orb}(x)|} = \sum_{x\in X} \frac{1}{|\operatorname{orb}(x)|}.$$

Also, by the bijective correspondence above, we have $|\operatorname{orb}(x)| = |G|/|G_x|$ so

$$\begin{aligned} |G\backslash S| &= \sum_{x\in X} |G_x|/|G| \\ &= \frac{1}{|G|}\sum_{x\in X} |G_x| \\ &= \frac{1}{|G|}\#(\{(g,x) \in G\times X \mid gx = x\}) \\ &= \frac{1}{|G|}\sum_{g\in G} F(g). \end{aligned}$$

□