MATH 3322 Problem Set 4

February 25, 2019

Solutions

Notation: Let D_n be the dihedral group of symmetries of the regular n-gon, generated by two elements r and s such that $r^n = 1,\ s^2 = 1,\ rs = sr^{-1}$.

Note that many authors call this D_{2n}, to reflect the order of the group. Ames (our text) or Beachy and Blair use the name D_n as we have defined it; Dummit and Foote, another important reference, uses D_{2n}.

[3] **Question 1.** Let $p \in \mathbb{Z}$ be prime.

Prove that $\mathbb{Z}/p^n\mathbb{Z}$ has a unique composition series.

Proof: [The key point lies in recognizing that the subgroup lattice of $\mathbb{Z}/p^n\mathbb{Z}$ is a chain: and this is what proves uniqueness.

Every subgroup and every image of a cyclic group is cyclic, and the sugroups of $\mathbb{Z}_n$ are precisely $d\mathbb{Z}_n \cong \mathbb{Z}_{(n/d)}$ where $d|n$; and so every subgroup and every image of a p-group is a p-group. Therefore in particular the subgroup lattice of $\mathbb{Z}/p^n\mathbb{Z}$ is determined by the chain of divisors of p^n: it is a chain with subgroups (isomorphic to)

$$0 \subset \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \cdots \hookrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \hookrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

and each factor of this subnormal series is $\mathbb{Z}/p\mathbb{Z}$, which is simple. Any shorter chain of subgroups must have a factor $\mathbb{Z}/p^k\mathbb{Z}$, $k > 1$. ∎

[4] **Question 2.** The sublattice diagrams for the quaternion group $\mathbf{Q}_8$ and the dihedral group $\mathbf{D}_4$ are attached.

Using only these diagrams and the fact that both groups have 8 elements, explain why $\mathbf{Q}_8$ has exactly 3 distinct composition series and $\mathbf{D}_8$ has exactly 7 distinct composition series.

Solution: Since each group has 8 elements, subgroups can only have cardinality 1, 2, 4, or 8, and in these two cases, the cardinality of a subgroup can be identified by its height in the subgroup lattice. From the lengths of the chains, there are subgroups of every possible size. The only possible composition factor is $\mathbb{Z}/2\mathbb{Z}$. From the diagrams, we see in fact that any "covering pair" of subgroups has $\mathbb{Z}/2\mathbb{Z}$ as its quotient (and any subgroup of index 2 is normal). Therefore the paths through the subgroup lattice are, in each case, composition series. But $\mathbf{Q}_8$ has 3 paths and $\mathbf{D}_8$ has 7 paths.

Remark: The insightful way to solve this problem is to prove that in any group of order 2^n, a chain of subgroups of length $n+1$ is necessarily a composition series (the orders of the groups in such a chain are necessarily 1, 2, 4, ..., 2^n) and so since each has index 2 in the following one, each subgroup is normal in its successor and the factor groups are all $\mathbb{Z}_2$, which is simple.

In fact, if you read the text section on nilpotent groups, you will find a proof of the the fact that every finite p-group is nilpotent, for roughly the same reasons as given here.

[3] **Question 3.** Prove that if G has a composition series and $1 \neq H \trianglelefteq G$, then G has a composition series containing H.

Proof: WLOG $H \neq G$ as well. By the Schreier Refinement Theorem the subnormal series $1 \lhd H \lhd G$ and any composition series for G have a equivalent refinements, one of which necessarily contains H. After deleting duplications, since it is equivalent to a composition series, all its factors are simple, that is, it is itself a composition series. ∎

[4] **Question 4.** Prove that D_{2^n} is solvable for each n.

Hint: Of course you only need to be able to find one subnormal series with abelian factors; the work you did on the previous question and the diagram for D_4 should give you a hint towards a fairly easy answer.

Proof: We saw in the previous solution that we get a sequence of groups each of index 2 in the next.

Consider $D_{2^{n+1}} = \left\langle\!\left\langle r, s : r^{2^{n+1}} = 1,\ s^2 = 1,\ rs = sr^{-1} \right\rangle\!\right\rangle$. Let $t = r^2$. Then $t^{2^n} = \left(r^2\right)^{2^n} = r^{2 \cdot 2^n} = 1$ and $ts = r^2 s = rsr^{-1} = sr^{-2} = st_1$, so the subgroup generated by t and s is isomorphic to D_{2^n}. Therefore we get the descending chain of subgroups

$$D_{2^{n+1}} > D_{2^n} > \cdots > D_2 > 1\,,$$

each of index 2 in the one above, and hence normal with simple abelian factor $\mathbb{Z}/2\mathbb{Z}$. ∎

Proof: And several of you came up with a much shorter proof. It is not actually necessary to find a composition series, as above.

Consider D_{2^n}, a group of order 2^{n+1}. Note that $\langle\!\langle r \rangle\!\rangle \cong \mathbb{Z}/2^n/ZZ$, an abelian group of order 2^n, hence of index 2 in D_{2^n}. Therefore $D_{2^n}/\langle\!\langle r \rangle\!\rangle \cong \mathbb{Z}/2\mathbb{Z}$ and so the subnormal series $D_{2^n} \trianglerighteq \langle\!\langle r \rangle\!\rangle \trianglerighteq 1$ shows that D_{2^n} is solvable.

Note that this same argument applies to ∎

Question 5. Prove that:

[3] (a) Every subgroup of a solvable group is solvable.

[3] (b) Every homomorphic image of a solvable group is solvable.

Proof: Suppose

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

with G_i/G_{i+1} abelian.

(a) Let H be a subgroup of G. Then $H \cap G_{i+1}$ is normal in $H \cap G_i$ since G_{i+1} is normal in G_i. Furthermore $(H \cap G_i)/(H \cap G_{i+1}) \cong G_{i+1}(H \cap G_i)/G_{i+1}$ by the Second Isomorphism Theorem, but the latter is a subgroup of the abelian group G_i/G_{i+1}. Therefore

$$H = H \cap G_0 \geq H \cap G_1 \geq H \cap G_2 \geq \cdots \geq H \cap G_n = 1$$

shows that H is solvable.

(b) Let $H \trianglelefteq G$. Then $(HG_{i+1})/H \trianglelefteq (HG_i)/H)$ for each i, and $(HG_i)/H \trianglelefteq (HG_{i+1})/H) \cong HG_i/HG_{i+1}$ by the First Isomorphism Theorem. But the map $G_i/G_{i+1} \to HG_i/HG_{i+1}$ defined by $g_i/G_{i+1} \mapsto g_i/HG_{i+1}$ is a well-defined homomorphism since $G_{i+1} \subseteq HG_{i+1}$ and is a surjection since $H \subseteq HG_{i+1}$. Therefore HG_i/HG_{i+1} is the image of an abelian group and is therefore also abelian. Therefore

$$G/H = HG_0/H \geq HG_1/H \geq HG_2/H \geq \cdots \geq HG_n/H = 1$$

shows that G/H is solvable.

You can work exactly the same proof by considering an epimorphism $\varphi : G \twoheadrightarrow K$ and setting $K_i = \varphi[G_i]$. (For if you set $H = \ker(\varphi)$, then $K_i \cong HG_{i+1})/H$.)

∎

Supplementary notes on the dihedral group D_{2^n} .

Proposition D_N is solvable for all N .

D_N is nilpotent iff $N = 2^n$ for some n . D_{2^n} is nilpotent of class n .

Proof: Clearly $\langle\langle r\rangle\rangle \cong \mathbb{Z}/N\mathbb{Z}$, an abelian subgroup of order N , and hence of index 2 in D_N . Therefore it is normal, and the quotient is $\mathbb{Z}/2\mathbb{Z}$, so the subnormal series $D_N \trianglerighteq \langle\langle r\rangle\rangle \trianglerighteq 1$ shows that D_N is solvable.

For the second assertion, first we show that for any $m > 2$, the centre of D_m is non-trivial iff $m = 2k$, in which case the centre is isomorphic to $\langle\langle r^k\rangle\rangle \cong \mathbb{Z}_2$. (Note that D_2 is abelian and so is its own centre.)

Fix m . When can r^k be in the centre $(k < m)$? Certainly it must commute with s , so we have $sr^k = r^k s = sr^{-k}$, and so $r^k = r^{-k}$ or $r^{2k} = 1$. Since m is the least positive value for which $r^m = 1$, $2k = m$, that is, m is even. Since r^k trvially commutes with r , certainly in this case r^k is in the centre of D_{2k} . What about an element of the form $r^t s$ for some t ? If it is in the centre, it must commute with r , and so $r(r^t s) = (r^t s)r = r^t r^{-1} s$, and therefore $r^{t+1} = r^{t-1}$, and so $r^2 = 1$. But we assume that $m > 2$, so this is impossible. So for $m > 2$, D_m has a centre iff $m = 2k$ for some k , in which case r^k generates the centre.

Remark: So we have immediately D_m is not nilpotent if m is odd, but is solvable whenever m is even. It follows from the rest of the argument that e.g., D_6 is an example of a solvable group which is not nilpotent.

Now we show that for $k > 1$, $G = D_{2k}/\langle\langle r^k\rangle\rangle \cong D_k$. But this is easy: G is generated by the cosets $\bar{r}$ and $\bar{s}$ of r and of s respectively, and only r is collapsed: $\bar{s}^2 = 1$, $\bar{r}\bar{s} = \bar{s}\bar{r}^{-1}$, and $\bar{r}^k = 1$, exactly the presentation of D_k .

In general, any natural number $N \geq 2$ can be written uniquely in the form $N = 2^n(2k+1)$ with $n, k \geq 0$. We claim that the upper central series of $\mathbf{D}_N$ has the form

$$\{1\} = Z_0 \triangleleft Z_1 \triangleleft \cdots \triangleleft Z_n \trianglelefteq \mathbf{D}_N ,$$

with equality at the last step if $k = 0$ (i.e. N is a power of 2) and D_N/Z_n being centreless otherwise. If $n = 0$ and $k > 0$, we have seen that $\mathbf{D}_N$ is centreless. For $n = m+1$, the centre Z_1 has two elements and $D_{2^{m+1}(2k+1)}/Z_1 \cong D_{2^m(2k+1)}$. So if the claim holds for $N = 2^m(2k+1)$, we have by inductive hypothesis an upper central series

$$\{1\} = Z_1/Z_1 \triangleleft Z_2/Z_1 \triangleleft \cdots \triangleleft Z_{m+1}/Z_1 \trianglelefteq \mathbf{D}_{2^{m+1}(2k+1)}/Z_1 \cong \mathbf{D}_{2^m(2k+1)} ,$$

with equality if $k = 0$ and $(D_{2^{m+1}(2k+1)}/Z_1)/(Z_{m+1}/Z_1)$ being centreless otherwise. That is, for each i, $1 \leq i < m+1$, Z_{i+1}/Z_1 is chosen so that $(Z_{i+1}/Z_1)/(Z_i/Z_1)$ is the centre of $(D_{2^{m+1}(2k+1)}/Z_1)/(Z_i/Z_1)$. Now just apply the second isomorphism theorem to simplify these terms: Z_{i+1} is chosen so that Z_{i+1}/Z_i is the centre of $D_{2^{m+1}(2k+1)}/Z_i$, that is,

$$\{1\} = Z_0 \triangleleft Z_1 \triangleleft \cdots \triangleleft Z_{m+1} \trianglelefteq D_{2^{m+1}(2k+1)}$$

is the upper central series of $D_{2^{m+1}(2k+1)}$, with equality if $k = 0$ and $D_{2^{m+1}(2k+1)}/Z_{m+1}$ being centreless otherwise.

So we have the claim, and therefore if $N = 2^n$ then D_N is nilpotent of class n , and if $N = 2^n(2k+1)$ with $k > 0$ then D_N is not nilpotent.

As a final point, it follows from the construction that Z_k is generated by $r^{2^{n-k}}$ and so is isomorphic to the cyclic group of order 2^k . ∎