Queen Mary
University of London

MTHM024/MTH714U Group Theory

Solutions 3 November 2011

---

1 (a) Let $G = C_n$, with generator a, and let H be a subgroup of G. Let k be the smallest positive integer for which $a^k \in H$. (There certainly are some positive integers with this property, e.g. $k = n$.) Now we claim that, if $a^m \in H$, then k divides m. For if not, then let $m = kq + r$, with $0 < r < k$; then $a^r = a^m \cdot (a^k)^{-q} \in H$, contradicting the definition of k. So a^k generates H, which is thus cyclic.

(b) Let G be the dihedral group of order $2n$, the group of symmetries of a regular n-gon. Then G contains a cyclic group C of order n consisting of rotations; all the elements outside C are reflections. Let H be any subgroup of G. If $H \leq C$, then H is cyclic, by (a); so suppose not. Then $H \cap C$ is a cyclic group of order m, say, and $|H| = 2m$. An element of H outside C is a reflection (so has order 2) and conjugates a generator of $H \cap C$ to its inverse (since it conjugates every element of C to its inverse). Thus H is a dihedral group.

(c) Further to (b), we see that G contains a unique cyclic subgroup of order m consisting of rotations, for every m dividing n. Also, if K is such a subgroup, and t any reflection, then $\langle K, t\rangle$ is a dihedral group. If $|K| = m$, then the dihedral group $\langle K, t\rangle$ contains m reflections. Since there are n involutions, there must be n/m dihedral subgroups of order $2m$.

If n is odd, then all these dihedral groups are conjugate, so they are not normal (unless $m = n$, in which case we have the whole group). If n is even, the reflections fall into two conjugacy classes. Now if n/m is even, then the dihedral group of order $2m$ contains reflections from only one class, so there are two conjugacy classes of dihedral groups, while if n/m is odd, then all the dihedral groups contain reflections from both classes and so all is conjugate.

So the normal subgroups are: all the cyclic rotation groups C_m; and the dihedral groups D_{2m} for $m = 1$ and (if n is even) $m = 2$.

(d) In D_{12}, we see that there are three normal subgroups of index 2, namely C_6 and two D_6s. Moreover, C_6 has two composition series $C_6 \rhd C_2 \rhd \{1\}$ and $C_6 \rhd C_3 \rhd \{1\}$, while D_6 has only one, namely $D_6 \rhd C_3 \rhd \{1\}$. So there are four composition series for D_{12}.

2 The normal subgroups of S_4 are A_4, V_4 (the Klein group) and $\{1\}$. So any composition series must begin $S_4 \rhd A_4$. Now the normal subgroups of A_4 are V_4 and $\{1\}$, so the series must continue $A_4 \rhd V_4$. Finally, V_4 has three cyclic subgroups of order 2, all normal, so there are three ways to continue the series as $V_4 \rhd C_2 \rhd \{1\}$.

3 Let $|G| = 120$ and let G have composition factors C_2 and A_5. Then G has at most one normal subgroup of order 60, and at most one normal subgroup of order 2. [Why? Use the fact that A_5 is simple. For example, if H and K were two normal subgroups of order 60, then $H \cong A_5$, and $H \cap K$ is a subgroup of index 2 in H.]

(a) If normal subgroups of both orders exist, then their intersection is $\{1\}$ and their product is G, so G is their direct product, and is isomorphic to $C_2 \times A_5$.

(b) The group $G = S_5$ has its only non-trivial normal subgroup A_5, which is simple, so $S_5 \rhd A_5 \rhd \{1\}$ is the only composition series.

(c) The group $\mathrm{SL}(2,5)$ has a normal subgroup $\{\pm I\}$ of order 2, and as we have seen, the quotient is $\mathrm{PSL}(2,5) \cong A_5$. This group has only one element of order 2, so cannot have any other subgroup of order 2, and cannot have a subgroup isomorphic to A_5. So $\mathrm{SL}(2,5) \rhd \{\pm I\} \rhd \{I\}$ is the only composition series.

4 (a) Let G be an elementary abelian p-group. If its order were divisible by a prime $q \neq p$, then by Cauchy's Theorem it would contain an element of order q, which it does not. So $|G|$ is a power of p.

(b) There are two ways to argue. First, use the structure theorem for finite abelian groups to express G as a direct product of cyclic groups. Since all non-identity elements have order p, these cyclic groups must all be C_p.

The second method avoids using this theorem. Write the abelian group G additively, and define $ng = g + g + \cdots + g$ (n times) for $0 \leq n \leq p-1$. Since $pg = 0$, it is easy to show that this scalar multiplication makes G into a vector space over the field $\mathrm{GF}(p)$ of integers mod p. Choose a basis for this vector space. Translating back to group theory language, the elements of this basis are generators of cyclic groups whose direct product is G.