Solutions to Homework Assignment 4

Daniel Mathews

November 1, 2004

Section 3.4, Problem 8.

The implications (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are easy to prove. If (iii) holds, then G has a sequence of subgroups $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$ where each H_{i+1}/H_i has prime order. But every group of prime order is cyclic, so (ii) then holds. And every cyclic group is abelian, so (i) then holds.

Now we show (i) $\Rightarrow$ (iii). Suppose G is solvable, so it has a sequence of subgroups with abelian quotients. The idea is to add sufficiently many extra groups into our sequence between H_i and H_{i+1} until the quotients become cyclic. By the correspondence theorem, this is equivalent to finding such subgroups between 1 and H_{i+1}/H_i. We can prove this by induction on $|H_{i+1}/H_i|$. For $|H_{i+1}/H_i| = 1$ (or in fact $|H_{i+1}/H_i|$ any prime), there is nothing to prove. Now suppose $|H_{i+1}/H_i| = n$, and take a prime $p|n$. By Cauchy's theorem H_{i+1}/H_i contains an element of order p, hence a subgroup P_1 of order p. As H_{i+1}/H_i is abelian all subgroups are normal, so $1 \trianglelefteq P_1 \trianglelefteq H_{i+1}/H_i$. Now $P_1/1$ has prime order (hence is simple). It remains to add subgroups between P and H_{i+1}/H_i with quotients of prime order. But by the correspondence theorem this is equivalent to finding subgroups between 1 and $(H_{i+1}/H_i)/P_1$. Since this has order less than n, by induction we may find the desired groups, and we obtain $1 \trianglelefteq P_1 \trianglelefteq \cdots \trianglelefteq P_k \trianglelefteq H_{i+1}/H_i$ where each quotient has prime order. Inserting these into our original sequence via the correspondence theorem gives a composition series for G where all factors have prime order, so (iii) holds.

We have now shown equivalence of (i), (ii) and (iii). We now turn to (iv). Clearly (iv) $\Rightarrow$ (i), as a chain of normal subgroups with abelian quotients gives a solvable group. To finish we prove that (iii) $\Rightarrow$ (iv). So assume G has composition factors all of prime order (so is solvable). We will show how to obtain a chain of normal subgroups with abelian quotients. The proof is by induction on $|G|$. If $|G| = 1$ there is nothing to prove. Let $|G| = n$. We find the first nontrivial group in our series; the rest will follow by induction. So let M be a minimal nontrivial normal subgroup of G. As a subgroup of a solvable group M is solvable, hence M satisfies property (iii), hence we may take a series $1 = M_0 \trianglelefteq \cdots \trianglelefteq M_r = M$ where all quotients have prime order. Let $N = M_{r-1}$, $N \trianglelefteq M$ and M/N has prime order, hence is cyclic and abelian. Taking $x, y \in M$ we see $xN, yN \in M/N$ commute, so $xyx^{-1}y^{-1}N = 1N$ and $xyx^{-1}y^{-1} \in N$. Similarly, for any $g \in G$ we have $gxg^{-1}, gyg^{-1} \in M$ as M is normal. Then $(gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = gxyx^{-1}y^{-1}g^{-1} \in N$, so

$xyx^{-1}y^{-1} \in g^{-1}Ng$. So $xyx^{-1}y^{-1}$ lies in all G-conjugates $g^{-1}Ng$ of N. But N is a subgroup of G, hence $g^{-1}Ng$ is a subgroup of G, and the intersection $\cap_{g\in G} g^{-1}Ng$ is a subgroup which is normal in G, since conjugation by an element in G just moves between the different G-conjugates of N. But then $\cap_{g\in G} g^{-1}Ng$ is a normal subgroup of G, strictly smaller than M. By minimality of G then $\cap_{g\in G} g^{-1}Ng = \{1\}$, so $xyx^{-1}y^{-1} = 1$. So M is abelian. We can choose M to be the first normal subgroup of our series for G. By induction we can now find a series for the smaller group G/M, and by the correspondence theorem lift this to a series between M and G.

Section 3.4, Problem 9.

This is tricky. Suppose we have two composition series $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_r = G$ and $1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G$, so all quotients are simple. Note that if $N_{r-1} = M_1$ then the result is immediate, as $M_1/M_0 = M_1$ is simple, hence N_{r-1} is simple, hence $r = 2$ and N_{r-1} has no nontrivial normal subgroups. So assume $M_1 \neq N_{r-1}$ and consider $M_1 \cap N_{r-1}$, which is a subgroup of M_1; we will prove that $r = 2$ and $G/M_2 \cong N_1/1$, $M_1/1 \cong G/N_1$. In fact as $M_1 \trianglelefteq M_1$ (trivially) and $N_{r-1} \trianglelefteq M_1$ (as $N_{r-1} \trianglelefteq G$) we have $M_1 \cap N_{r-1} \trianglelefteq M_1$. By the second isomorphism theorem

$$\frac{M_1}{M_1 \cap N_{r-1}} = \frac{M_1 N_{r-1}}{N_{r-1}} = \frac{G}{N_{r-1}}.$$

All this is clear except the last equality. We see that $M_1 N_{r-1} \trianglelefteq G$ (as both the factors are) but the subgroups are not equal. Further, we cannot have $M_1 < N_{r-1}$, as then G/N_{r-1} is a nontrivial quotient of G/M_1 which is assumed to be simple. Similarly we cannot have $N_{r-1} < M_1$. So $M_1 N_{r-1}$ is a normal subgroup of G strictly larger than M_1, and as G/M_1 is simple it must be all of G.

Now the quotient $M_1/(M_1 \cap N_{r-1})$ is isomorphic to G/N_{r-1}, which by assumption is nontrivial and simple. As M_1 is simple, the only nontrivial quotient is M_1 itself. Thus $M_1 \cap N_{r-1} = 1$ and $M_1 \cong G/N_{r-1}$. Now applying the seond isomorphism theorem again we have

$$N_{r-1} = \frac{N_{r-1}}{M_1 \cap N_{r-1}} = \frac{N_{r-1} M_1}{M_1} = \frac{G}{M_1}.$$

But G/M_1 is simple, so we have $r = 2$ and $N_1 \cong \frac{G}{M_1}$. We have proved the result.

Section 3.5, Problem 2.

There are many ways to prove this result. If we understand the sign homomorphism $\epsilon : S_n \longrightarrow \{\pm 1\}$ then for any $\sigma \in S_n$ we have $\epsilon(\sigma) = \pm 1$ so $\epsilon(\sigma^2) = (\pm 1)^2 = 1$, so $\sigma^2 = 1$.

Alternatively, consider the cycle structure of σ. Every odd-length cycle in σ remains a cycle of the same length (but different order) in σ^2. Every cycle of length 2 in σ disappears in σ^2. And every cycle of length $2k$ in σ, for $k \geq 2$, splits into two cycles of length k in σ. So the only even cycles that can arise in σ^2 come from this splitting effect, which creates even cycles in pairs. So σ^2 always has an even number of even cycles, hence is an even permutation.

Thirdly, let σ be represented as a product of k transpositions. Then σ^2 is a product of $2k$ transpositions, hence is even.

Section 3.5, Problem 7.

Every rigid motion of a tetrahedron permutes the 4 vertices, so the group of rigid motions is a subgroup of S_4. But not every permutation is possible: for instance one cannot transpose two vertices while holding others fixed.

However 3-cycles are certainly possible: for instance (123) can be achieved by rotating $120°$ around the vertex labelled 4. And $(2,2)$-cycles are also possible: one can see that, say, $(12)(34)$ can be achieved by a rotation of $180°$ about the line joining the midpoints of the edges connecting $1,2$ and $3,4$. So the group of rigid motions contains A_4, which has index 2 in S_4, but is strictly smaller than S_4. Hence it is precisely A_4.

Section 4.1, Problem 1.

Note if $x \in G_a$, so $x.a = a$, then $gxg^{-1}.b = gx.a = g.a = b$, so $gxg^{-1} \in G_b$. Thus $gG_ag^{-1} \subseteq G_b$. By an identical argument $g^{-1}G_bg \subseteq G_a$, so $G_b \subseteq gG_ag^{-1}$. Thus $G_b = gG_ag^{-1}$.

If G acts transitively on A, then the kernel of the action is the set of $x \in G$ fixing every point of A, i.e. $x \in \cap_{a\in A}G_a$. Since G is transitive, for every $b \in A$ there is a $g \in G$ such that $g.a = b$. Then we have $G_b = gG_ag^{-1}$. So the kernel of the action is precisely

$$\bigcap_{a\in A} G_a = \bigcap_{g\in G} gG_ag^{-1}.$$

Section 4.1, Problem 2.

We have G acting on A, regarding $G \le S_A$. From the argument in the previous problem we have $G_{\sigma(a)} = \sigma G_a\sigma^{-1}$. If G acts transitively on A, then

$$\bigcap_{\sigma\in G} \sigma G_a\sigma^{-1} = \bigcap_{\sigma\in G} G_{\sigma(a)} = \bigcap_{a\in A} G_a$$

consists precisely of those permutations which fix every element of A. But the only such permutation is the identity itself. So $\cap_{\sigma\in G}\sigma G_a\sigma^{-1} = 1$.

Section 4.1, Problem 7.

(i) If $g, h\ inG_B$ then both g and h fix the block B, hence so does gh. Similarly if $g \in G_B$ then g fixes B, hence so does g^{-1}. So $G_B \le G$.

Now if $g \in G_a$ then g fixes $a \in B$. So $a \in g(B)$ and $g(B)$ intersects B. Hence by definition of a block $g(B) = B$, so $g \in G_B$. Thus $G_a \le G_B$.

(ii) If G acts on A transitively, then $a \in A$ is taken to every other element of A by some element of G. Thus the block B containing a is mapped onto every element of G. So every element of A lies in some $\sigma_i(B)$.

Now suppose $\sigma_i(B) \cap \sigma_j(B) \neq \emptyset$. Then $\sigma_j^{-1}\sigma_i(B) \cap B \neq \emptyset$. So by the definition of a block $\sigma_j^{-1}\sigma_i(B) = B$ and $\sigma_i(B) = \sigma_j(B)$ so $i = j$. So the $\sigma_i(B)$ form a partition of A.

(iii) The action of D_8 as a permutation group on the four vertices of a square is not primitive as a set of two opposite vertices forms a block. Under any symmetry of the square, two opposite vertices are taken to two opposite vertices.

(iv) We show G acts non-primitively if and only if there exists $a \in A$ with a subgroup H lying strictly between G_a and G, i.e. $G_a < H < G$. (This is clearly equivalent to the stated problem.)

Suppose the action is not primitive. Then there exists a non-trivial block B. Consider the subgroup G_B of G. This is strictly smaller than G, as G is transitive (so some element of G will map an element of B outside B). We have shown above that $G_a \leq G_B$. But since B is nontrivial, it contains at least two elements $\{a, b\}$, and as G acts transitively, there is a $g \in G$ with $g(a) = b$. For this g we have $g(B) \cap B \neq \emptyset$ so $g(B) = B$ and $g \in G_B$ but $g \notin G_a$. So $G_a < H < G$.

Now suppose we have H with $G_a < H < G$. Consider the set $B = H(a)$, i.e. the orbit of a under H. We claim B is a block. Clearly, for any $h \in H$, $h(B) = B$. Suppose for some $g \in G$ we have $g(B) \cap B \neq \emptyset$, say $g(b_1) = b_2$ where $b_1, b_2 \in B$. By definition of B there exist $h_1, h_2 \in H$ such that $h_1(a) = b_1$ and $h_2(a) = b_2$. Then $h_2^{-1} g h_1(a) = a$ so $h_2^{-1} g h_1 \in G_a$. But clearly $G_a < H$ so we have $g \in H$ and then $g(B) = B$. So B is a block. It remains to show B is nontrivial. As $G_a < H$ there is some element of H not fixing a, so B contains at least two elements. Suppose $B = A$, then H acts on A transitively, and we claim $H = G$. For take $g \in G$, and let $g(a) = c$. Then there exists h with $h(a) = c$ also, so $h^{-1}g(a) = a$ and $h^{-1}g \in G_a < H$. So $g \in H$ and we have $H = G$. But as $H < G$, we have $B \neq A$ and B is a nontrivial block, so G acts non-primitively.