MATH411 Assignment 2

Elliott Hughes

May 2, 2022

2.1

If M is a finite Abelian group with $|M| = 600$ then by the fundamental theorem of finite Abelian groups M is isomorphic to a direct product of groups of the form $\mathbb{Z}/n_i\mathbb{Z}$, where $\prod_i n_i = 600$ and each n_i is a prime power. Since $|M| = 600 = 2^3 \cdot 3 \cdot 5^2$ it follows that M can be factored into a direct product of an Abelian group of order 2^3, an Abelian group of order 3 and an Abelian group of order 5^2. The group of order 2^3 (denoted G_2) must be isomorphic to some direct product of Abelian groups of order 2^r, $r \in \{1, 2, 3\}$. There are clearly only three possible options

$$G_2 = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \quad \text{or} \quad G_2 = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \quad \text{or} \quad G_2 = \frac{\mathbb{Z}}{8\mathbb{Z}}$$

These are the only possible groups of order eight which are Abelian by the fundamental theorem of finite Abelian groups. Clearly the only possible group of order three is just

$$G_3 = \frac{\mathbb{Z}}{3\mathbb{Z}}$$

Finally there are two possible groups of order 5^2.

$$G_5 = \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \quad \text{or} \quad G_5 = \frac{\mathbb{Z}}{25\mathbb{Z}}$$

Consequently there are $3(2) = 6$ unique Abelian groups of order 600.

2.2

Consider $\phi, \psi \in \text{Aut}(G)$. Then for $g, h \in G$ we have $\phi \circ \psi(gh) = \phi(\psi(g)\psi(h))$. Since $\psi(g), \psi(h) \in G$ it is clear that $\phi\psi(gh) = \phi\psi(g)\phi\psi(h) \in G$. Therefore the set $\text{Aut}(G)$ is closed under the operation $\phi \times \psi \to \phi \circ \psi$. Let ψ_e be the function taking $g \to g$ for all $g \in G$. This is an automorphism as clearly for $g, h \in G$ we have $\psi_e(gh) = \psi_e(g)\psi_e(h)$ and ϕ_e is trivially bijective. Then for $\phi \in \text{Aut}(G)$ and $g \in G$ we have $\phi \circ \psi_e(g) = \phi(\psi_e(g)) = \phi(g)$ so $\phi \circ \psi_e = \phi$. Thus ψ_e is a valid identity element for the candidate group $\text{Aut}(G)$. Since ϕ is an isomorphism from G to G, the inverse function ϕ^{-1} is also an isomorphism from G to G. Furthermore for $g \in G$, $\phi \circ \phi^{-1}(g) = \phi(\phi^{-1}(g)) = g$ so $\phi \circ \phi^{-1} = \psi_e$. Finally by the properties of functions for $\phi_1, \phi_2, \phi_3 \in \text{Aut}(G)$, $(\phi_1 \circ \phi_2) \circ \phi_3 = \phi_1 \circ (\phi_2 \circ \phi_3)$ and so $\text{Aut}(G)$ is a valid group.

Then for some $g \in G$ let $\phi_g : G \to G$, such that for $h \in G$, $\phi_g(h) = ghg^{-1}$. If we take $h_1, h_2 \in G$ we have $\phi(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \phi_g(h_1)\phi_g(h_2)$ so ϕ_g is a homomorphism from G to G. Clearly ϕ_g is injective as for $h_1, h_2 \in G$ then if $gh_1g^{-1} = gh_2g^{-1}$ it follows that $h_1 = h_2$. It is also surjective as if $h \in G$ then there exists $g^{-1}hg \in G$ such that $\phi(g^{-1}hg) = h$. So ϕ_g is an automorphism.

We may now define the function $\Phi : G \to \text{Aut}(G)$, $\Phi(g) = \phi_g$. It remains to show that this is a homomorphism. Consider $g_1, g_2 \in G$. Then $\Phi(g_1 g_2) = \phi_{g_1 g_2}$ and for $h \in G$ $\phi_{g_1 g_2}(h) = g_1 g_2 h (g_1 g_2)^{-1} = \phi_{g_1} \circ \phi_{g_2}(h)$. Since this holds for all $h \in G$, it follows that $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$ and thus Φ is a homomorphism. Clearly the kernel of Φ includes the group of all elements which commute with any element in G (as if $g \in Z(G)$ then for any $h \in G$ we have $ghg^{-1} = gg^{-1}h = h$) so $\ker(\Psi) = Z(G)$. Furthermore if for $ghg^{-1} = h$ for all $h \in G$ then clearly $gh = hg$ and so $g \in Z(G)$ so $\ker(\Phi) = Z(G)$.

This is not necessarily a surjective function, however. Let G be an Abelian group with elements which have order higher than two. Consider $\phi : G \to G$, $\phi(g) = g^{-1}$ for some $g \in G$. This is clearly injective by the uniqueness of inverses and onto as for $g \in G$ there exists $(g^{-1})^{-1} = g$. Finally for $g, h \in G$ so that $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \phi(g)\phi(h)$ so this an automorphism. Then if we consider Φ from this group G to $\text{Aut}(G)$ it is clear that Ψ maps only to the identity (as $Z(G) = G$) and since G has elements which have a higher order than two it follows that ϕ is not in the image of Φ. Thus Φ is not surjective.

2.3

Note A_4 is a subgroup and is of index two, so it is normal (see 2.4). Furthermore A_4 is clearly of maximal size as there are no divisors for 24 which are larger than 12. So A_4 is a valid first term in a composition series. Then, consider V_4 the subgroup of A_4 comprised of the identity and three pairs of 2-cycles. This subgroup contains all the elements of order 2 in $v \in V_4$, so for $g \in V_4$ we have gvg^{-1} is also an element of order 2, so V_4 is normal. Any larger subgroup containing V_4 would have to be of order six or 12. It is trivial to see that if one introduces multiplies a 3 cycle by the elements of V_4 more than two new elements are created, so this series $S_4 \triangleright A_4 \triangleright V_4$ is part of a valid composition series for S_4. Clearly since any cyclic subgroup of V_4 generated by a non-identity element a is both normal and maximal (any larger subgroup is the group itself) it follows that the final composition series of A_4 is

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \langle a \rangle \triangleright 1$$

Is a valid composition series for S_4. The consequent Jördan-Holder factors are

$$S_4/A_4 \cong \mathbb{Z}_2 \qquad A_4/V_4 \cong \mathbb{Z}_3 \qquad V_4/\langle a \rangle \cong \mathbb{Z}_2 \qquad \langle a \rangle/1 \cong \mathbb{Z}_2$$

2.4

Let G be a group. If G is a p-group then the desired result holds by Corollary 11.6. Otherwise $|G| = p^r m$ where p is the smallest prime dividing the order of G, m is co-prime to p and $r \geq 1$. Then let $H < G$ such that $|H| = p^{r-1}m$. Denote the set of cosets of H (of which there are p) as

$$S = \{H, g_1 H, \ldots g_{p-1} H\}$$

Then we can define the permutation group of this set as $\text{Sym}(S)$. If one multiplies each element of S by some element of G then each coset is either fixed or sent to a new coset and so this defines a permutation T_g. Consider the function $\phi : g \to T_g$. Then for $g, g' \in G$ we have $\phi(gg') = T_{gg'}$ and so for some $s \in S$, $T_{gg'} = gg'(s) = g(g'(s)) = T_g(T_{g'}(s))$ and so $\phi(gg') = \phi(g)\phi(g')$. Therefore ϕ defines a homomorphism between these two groups.

Since $\text{Im}(\phi)$ is a subgroup of $\text{Sym}(S)$ the order of $\text{Im}(\phi)$ must divide $p!$. By the first isomorphism theorem this implies that $G/\ker(\phi)$ must also divide $p!$. Clearly the order of $G/\ker(\phi)$ cannot have prime factors larger than p. Consequently we have that $[G : \ker(\phi)]$ must be some power of p as p is the smallest prime that divides the order of G. If $[G : \ker(\phi)] = p^k$, then $k = 0, 1$ as p only appears once in $p!$.

If $[G : \ker(\phi)] = 0$ then the kernel of ϕ is the whole group. This would imply that for all $g \in G$, T_g is simply the identity permutation. However if one chooses $g \notin H$ then clearly gH is not the same as H so the kernel of ϕ is not the whole group. Thus we have that $[G : \ker(\phi)] = p$. It should be clear from the argument above that if $g \notin H$ then $g \notin \ker(\phi)$ and consequently that $\ker(\phi) \subseteq H$. However since both subgroups have the same index in the group we have that $\ker(\phi) = H$ and thus H is normal in G.

2.5

Let G be a finite group with $|G| = 10 = 2 \cdot 5$. Consider $G \circlearrowright G$ by conjugation. The orbit-stabilizer theorem requires that the orbit of an element under conjugation (its conjugacy class) divides the order of the group. Therefore we can eliminate the third tuple as a possible candidate. Furthermore, since the set of all elements that commute with all elements $Z(G)$ (that is, those where $\text{Stab}(x) = G$) is a subgroup its order must divide the order of the group. Thus we can eliminate the first tuple which has three elements in $Z(G)$.

Consider the fourth tuple. This contains a non-identity element which commutes with all other elements. However, if $a, b \in G$ and $|a| = 2$ and $|b| = 5$ then if these commute the product ab must have order 10 (as $(ab)^5 = a^5b^5 = a$ and $(ab)^2 = a^2b^2 = b^2$). However then ab must commute with all other elements as all other elements can be expressed as powers of ab. This leads to a contradiction and so we can eliminate the fourth tuple.

This leaves us with the second tuple. Consider the group D_5. If s is a reflection from this group and r is a rotation then the identity $srs = srs^{-1} = r^{-1}$ demonstrates that r and r^{-1} are conjugate. Furthermore since the stabilizer of r is the group of rotations all rotations have only two elements in their orbit and thus belong to a conjugacy class of order two. Furthermore, since $rsr^{-1} = rrs = r^2s$ it is clear that rotations do not fix reflections under conjugations and since for s' a different reflection $s'ss' \neq s$ the stabilizer of s must be of size two. Consequently the orbit must be of size five and so all reflections must be in the same conjugacy class (as the orbits of elements in G must partition G). Therefore the orders of the conjugacy classes of D_5 match the second tuple and so this is a valid choice.

2.6

Let σ be an r-cycle in S_n and let $\tau \in S_n$. Then clearly $\tau\sigma\tau^{-1} \in S_n$. Suppose $\sigma = (i_1 i_2 i_3 \dots i_r)$. Then for $\tau(i_k)$, $k \in \{1, 2, \dots, r-1\}$ we have

$$\tau\sigma\tau^{-1}(\tau(i_k)) = \tau\sigma(i_k) = \tau(i_{k+1})$$

And for $\tau(i_r)$, $\tau\sigma\tau^{-1}(\tau(i_r)) = \tau(i_1)$ by direct computation. Suppose then that $j \notin \{\tau(i_1), \tau(i_2), \dots, \tau(i_r)\}$. Then

$$\tau\sigma\tau^{-1}(j) = \tau\tau^{-1}(j) = j$$

Thus $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_r))$ as required.

2.7

Suppose P and Q are normal Sylow-P-Subgroups for different primes. Since all elements of P have orders which do not divide the order of Q and visa-versa they must have only trivial intersection. Thus we can apply lemma 7.2 and so their elements must commute.

2.8

Clearly $351 = 3^2 \cdot 13$ so any group of order 351 will contain a Sylow-13-Group. In fact there will be s_{13} of these, where $s_{13} \cong 1 \bmod 13$ and $s_{13} | 9$. Clearly then $s_{13} = 1$ so this subgroup is normal. Therefore this group is not simple.

2.9

Note $72 = 3^2 \cdot 2^3$. There exists s_3 groups of order 9, where $s_3 \cong 1 \bmod 3$ and $s_3|8$. Therefore s_3 is either 1 or 4.

Suppose $s_3 = 4$. Then for some Sylow-3-Group H we can apply the Orbit-Stabilizer theorem to note this implies that there exists some group $\text{Stab}(H) = K < G$ such that $[G : K] = 4$. Consider the set of permutations of the cosets in K (as in 2.4). This group clearly has $4! = 24$ elements. Then one can define a homomorphism ϕ between G and K (again as in 2.4). Since G has 72 elements and $\text{Sym}(K)$ has 24 elements it follows that $[G : \ker(\phi)] \leq 3$ (since $|G/\ker(\phi)|$ has to be smaller than $|\text{Sym}(K)|$ by the first isomorphism theorem). Therefore there must exist some non-trivial kernel of this homomorphism and consequently if $s_3 = 4$ then G is not normal.

If $s_3 = 1$ then clearly there only exists one Sylow-3-Group and this group must be normal. Thus there are no simple groups of order 72.

2.10

Since the prime-factorization of 20449 is $11^2 \cdot 13^2$, then for G such that $|G| = 20449$ G must contain s_{11} Sylow-11-Groups and it must also contain s_{13} Sylow-13-Groups. Furthermore s_{11} must be that $s_{11} \cong 1 \bmod 11$ and $s_{11}|169$. Since the only divisors of 169 are 1, 13 and 169, it follows that $s_{11} = 1$. Also s_{13} must be such that $s_{13} \cong 1 \bmod 13$ and $s_{13}|121$. By an identical argument as above, it follows that $s_{13} = 1$.

Let H_{11} denote the subgroup of G with order 121 and H_{13} denote the subgroup of G with order 169. Since both are the only elements of their conjugacy classes, it follows that H_{11} and H_{13} are normal in G. Furthermore, since they have trivial intersection and $|G| = |H_{11}||H_{13}|$ it follows that $G \cong H_{11} \times H_{13}$.

Since this holds for any group G with order 20449, it remains to show to classify the groups of order 121 and 169. Since both these groups are of order p^2 for some prime p, by corollary 11.5 these groups are Abelian. Therefore by the fundamental theorem of Abelian groups, it must be true that H_{11} and H_{13} are isomorphic to a direct product of groups of integers mod p where p is the relevant prime. Therefore H_{11} must be one of two possible groups

$$H_{11} \cong \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{11\mathbb{Z}} \quad \text{or} \quad H_{11} \cong \frac{\mathbb{Z}}{121\mathbb{Z}}$$

and H_{13} must be one of

$$H_{13} \cong \frac{\mathbb{Z}}{13\mathbb{Z}} \times \frac{\mathbb{Z}}{13\mathbb{Z}} \quad \text{or} \quad H_{13} \cong \frac{\mathbb{Z}}{169\mathbb{Z}}$$

Thus there are only four possible groups of order 20449:

$$G \cong \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{13\mathbb{Z}} \times \frac{\mathbb{Z}}{13\mathbb{Z}}$$
$$G \cong \frac{\mathbb{Z}}{121\mathbb{Z}} \times \frac{\mathbb{Z}}{13\mathbb{Z}} \times \frac{\mathbb{Z}}{13\mathbb{Z}}$$
$$G \cong \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{169\mathbb{Z}}$$
$$G \cong \frac{\mathbb{Z}}{121\mathbb{Z}} \times \frac{\mathbb{Z}}{169\mathbb{Z}}$$