Abstract Algebra I Homework 3

Carson Connard

Section 3.3

Let G be a group.

4 Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

Proof. For the first part, consider the subgroup $(C \times D) \leq (A \times B)$, and pick some element $(a, b) \in (A \times B)$. Then we have that $(a, b)(C \times D) = aC \times bD$, and since $C \trianglelefteq A$ and $D \trianglelefteq B$, we have that $aC \times bD = Ca \times Db = (C \times D)(a, b)$, and therefore $(C, D) \trianglelefteq (A, B)$.
For the next part, let us define $\phi : (A \times B) \to (A/C) \times (B/D)$ as $(a, b) \mapsto (aC, bD)$. Certainly ϕ is surjective. We aim to show that $\ker \phi = C \times D$ in order to invoke the first isomorphism theorem. So, if $(a, b) \in \ker \phi$, we have that $(aC, bD) = (C, D)$, therefore $a \in C$ and $b \in D$, and thus $(a, b) \in C \times D$ and $\ker \phi \subset C \times D$. If $(a, b) \in C \times D$, then $(aC, bD) = (C, D)$, therefore $\ker \phi \supset C \times D$, and therefore we have equality of $\ker \phi = C \times D$. Then by the first isomorphism theorem, we have that $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$. □

7 Let $M, N \trianglelefteq G$ such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$ (draw the lattice).

Proof. We have the following subgroup lattice for G:

$$\begin{tikzcd}
 & G \arrow[dl] \arrow[dr] & \\
M \arrow[dr] & & N \arrow[dl] \\
 & M \cap N \arrow[d] & \\
 & \{1\} &
\end{tikzcd}$$

Define the homomorphism $\phi : G \to G/M \times G/N$ as $g \mapsto (gM, gN)$. Indeed, the kernel of ϕ is equivalent to $M \cap N$, as any element in said intersection yields the identity in the target of ϕ. This will be used to invoke the first isomorphism theorem. We now aim to show that ϕ is surjective. So, take $(g_1M, g_2N) \in G/M \times G/N$. Appealing to the fact that $G = MN$ and $M, N \trianglelefteq G$, we take $g_1 = m_1n_1$ and $g_2 = m_2n_2$ for $m_i \in M$ and $n_i \in N$, and we have

$$\begin{aligned} g_1M = Mg_1 &= Mm_1n_1 = Mn_1 = n_1M \\ bN &= m_2n_2N = m_2N. \end{aligned}$$

Moreover, we have

$$\phi(m_2n_1) = (Mm_2n_1, m_2n_2N) = (n_1M, m_2N) = (g_1M, g_2N).$$

So, ϕ is surjective. Finally, invoking the first isomorphism theorem, we have that $G/(M \cap N) \cong (G/M) \times (G/N)$. □

Section 3.5

4 Show that $S_n = \langle (1\ 2)(1\ 2\ 3\ ...\ n) \rangle$ for all $n \geq 2$.

Proof. First note that S_n is generated by transpositions, as detailed in the commentary following the definition of a transposition in Dummit & Foote.
Lemma. We claim that in fact S_n is generated by transpositions of the form $(i\ i+1)$ for $1 \leq i \leq n-1$. Indeed, it suffices to show that any transposition $(i\ j)$ is generated by $(i\ i+1)$. Take without loss of generality $i < j$, and we

will induct over $j - i \geq 1$. The base case, $i+1 = j$, is trivial. Now note that $(i\ j) = (i\ i+1)(i+1\ j)(i\ i+1)$. As such, if $(i+1\ j) \in \langle (i\ i+1) \rangle$, then it follows that $(i\ j) \in \langle (i\ i+1) \rangle$ as well. QED.
We consider now $\tau = (1\ 2)$ and $\sigma = (1\ 2\ \cdots\ n)$. From our lemma, we have that indeed $(i\ i+1) = \sigma^{i-1}\tau\sigma^{-(i-1)}$ for $1 \leq i \leq n-1$. So, since $(i\ i+1)$ generates S_n, we must have that $(1\ 2)(1\ 2\ 3\ ...\ n)$ does as well. □

Section 4.1

9 Assume G acts transitively on the finite set A and let $H \trianglelefteq G$. Let $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1, ..., \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, ..., r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{ga : a \in \mathcal{O}\}$. Prove that G is transitive on $\{\mathcal{O}_1, ..., \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.

Proof. By definition of orbit, for each i we have that some $a_i \in A$ is such that $\mathcal{O}_i = Ha_i$. Since $H \trianglelefteq G$, taking $g \in G$ we see that $g\mathcal{O}_i = gHa_i = Hga_i$. So now $ga_i \in Ha_j = \mathcal{O}_j$ for some j since the $\mathcal{O}_j$'s $(j = 1, ..., r)$ partition the set A. Therefore $Hga_i = Ha_j$ for some j. By definition of our group action of G on A, we have for each i and j that there is some $g \in G$ such that $ga_i = a_j$, and therefore $g\mathcal{O}_i = \mathcal{O}_j$.

Now consider two elements $h, h' \in H$. Certainly $gha_i = gh'a_i$ if and only if $ha_i = h'a_i$, and therefore we must have that all orbits $\mathcal{O}_i$ have the same cardinality. □

(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$.

Proof. Consider $h_1, h_2 \in H$ such that $h_1 a = h_2 a$, which implies that $h_2^{-1}h_1$ is an element of the stabilizer of H with respect to a. Equivalently, we have $h_1 H_a = h_2 H_a$. Notice that the set of points $a_i \in \mathcal{O}_1$ are of the same cardinality as $|H : H_a|$ via Proposition 4.1.2. Certainly $H_a = H \cap G_a$, so we have that $|\mathcal{O}_1| = |H : H \cap G_a|$.

For the second part, since G acts on A, we have that $|A| = |G : G_a|$. Again, A is partitioned into the r orbits of H on A. We know that these all have the same size as previously shown. So, we have that $|A| = r|\mathcal{O}_1| = r|H : H_a|$. Since H is a normal subgroup, we have that $N_G(H) = G \geq G_a$. Now by the Second Isomorphism Theorem, we have that $G_aH/H \cong G_a/(G_a \cap H)$. Since $H_a = H \cap G_a$, we see that this gives $|G_aH : H| = |G_a : H_a|$. Since H is normal, we have that $HG = GH$. So, we have the following:

$$\begin{aligned}
|G : G_aH||G_ah : H_a| &= |G : H_a| \\
&= |G : G_a||G_a : H_a| \\
&= |A||G_a : H_a| \\
&= r|H : H_a||G_aH : H| \\
&= r|G_aH : H_a|
\end{aligned}$$

Therefore, we have $r = |G : G_aH| = |G : HG_a|$ □

Section 4.2

8 Prove that if H has finite index n then there is a normal subgroup $K \trianglelefteq G$ with $K \leq H$ and $|G : K| \leq n!$.

Proof. Notice that G acts on G/H by left multiplication, which 'affords' (per definition) the permutation representation $\phi : G \to S_{G/H}$. Also, let us take $K = \ker\phi$. Certainly, $K \trianglelefteq G$ and $K \leq H$. Then by the first isomorphism theorem we have that there exists a homomorphism $\psi : G/K \to S_{G/H}$. By definition of S_n, we have that $|S_{G/H}| = n!$, and since $K \leq H$, we see that $|G : K| \leq n!$ as desired. □

Section 4.3

2 Find all conjugacy classes and their sizes in the following groups:

(a) D_8

Solution. First notice that $Z(G) = \{1, r^2\}$. Therefore we have that $\mathcal{K}_1 = \{1\}$ and $\mathcal{K}_{r^2} = \{r^2\}$.

Now for rotations. Notice $\langle r \rangle \leq C_G(r) \leq G$. Also, $|\langle r \rangle| = 4$. Since $C_G(r) \neq G$, by Lagrange's Theorem we have that $C_G(r) = \langle r \rangle$. So, r has $|G : C_G(z)| = 2$ conjugates in G. Notice that $srs^{-1} = r^3$, and so we have that the conjugacy class which contains r is $\mathcal{K}_r = \{r, r^3\}$.

Now for reflections. Notice $\langle s\rangle \le C_G(s) \le G$ and $|\langle s\rangle| = 2$. By Lagrange's Theorem, we have that $C_G(s) = \langle s\rangle$ or $|C_G(s)| = 4$. But since $r^2s = sr^2$, we have that $|C_G(s)| = 4$. So, the conjugacy class which contains s has $|G : C_G(s)| = 2$ elements. Since $rsr^{-1} = sr^2$, we have that the conjugacy class containing s is $\mathcal{K}_s = \{s, sr^2\}$.

We have sr, sr^3 remaining. Since they are not in the center, they must share a conjugacy class. So, $\mathcal{K}_{sr} = \{sr, sr^3\}$.

So, we have the following conjugacy classes with their size being given by their cardinality:

$$\{1\},\ \{r, r^3\},\ \{r^2\},\ \{s, sr^2\},\ \{sr, sr^3\}.$$

(b) Q_8

Solution. First notice that $Z(G) = \{1, -1\}$. Therefore we have that $\mathcal{K}_1 = \{1\}$ and $\mathcal{K}_{-1} = \{-1\}$.

Let us consider i. We see that conjugation of i by any $g \in G$ yields $gig^{-1} = i$ or $gig^{-1} = -i$. So, we have the conjugacy class $\mathcal{K}_i = \{\pm i\}$. The same exact thing happens for j and k, that is $\mathcal{K}_j = \{\pm j\}$ and $\mathcal{K}_k = \{\pm k\}$.

So, we have the following conjugacy classes with their size being given by their cardinality:

$$\{1\},\ \{-1\},\ \{\pm i\},\ \{\pm j\},\ \{\pm k\}.$$

(c) A_4

Solution. First notice that $Z(G) = \{1\}$. Therefore we have that $\mathcal{K}_1 = \{1\}$.

Let us consider the three elements of the form $(ab)(cd)$. Since the size of a conjugacy class equals $|A_4 : G_a|$ for some a, we must have that the cardinality of each conjugacy class must divide the order of A_4, which is 12 (i.e. classes must be of cardinality 2, 3, 4, or 6 [not 12 since $\mathcal{K}_1$ exists]). So, since there are only three elements of the form specified, the conjugacy class of (say) $(1\ 2)(3\ 4)$ must be of order 1 or 3. Indeed, we see that $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3)$, and therefore we cannot have size 1, we must have size 3. Therefore we have a class $\mathcal{K}_{(12)(34)} = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Now there are 8 elements of the form $(a\ b\ c)$, but since 8 is not a factor of 12, we must have that there are at least two conjugacy classes of elements of the listed form. Moreover, we can only have that the sizes of the conjugacy classes divide 8 and 12, that is they are going to be of size 1 or 4, but certainly we cannot have 1 else we would have a class of size 7. So we must have two classes of size 4. Let us consider the element $(1\ 2\ 3)$. We must have that for $g \in A_4$ that $g(1\ 2\ 3)g^{-1}$ is in the conjugacy class of $(1\ 2\ 3)$. Notice that conjugation by transposition only swaps two digits in the (verbosely written) cycle $(1\ 2\ 3)(4)$; certainly, conjugation by an even number of transpositions yields an even number of swaps. So, we can obtain the following conjugacy class by performing just two swaps: $\mathcal{K}_{(123)} = \{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\}$.

Recall that the final class must be of size 4, and we have 4 elements left. Therefore we have $\mathcal{K}_{(132)} = \{(1\ 3\ 2), (1\ 2\ 4), (2\ 3\ 4), (1\ 4\ 3)\}$.

So, we have the following conjugacy classes with their size being given by their cardinality:

$$\{1\},\ \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},\ \{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\},\ \{(1\ 3\ 2), (1\ 2\ 4), (2\ 3\ 4), (1\ 4\ 3)\}.$$

10 Let σ be the 5-cycle $(1\ 2\ 3\ 4\ 5)$ in S_5. In each of (a) to (c) find an explicit element $\tau \in S_5$ which accomplishes the specified conjugation.

Solution. Let us first note that for $\sigma = (1\ 2\ 3\ 4\ 5)$, we have $\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5))$.

(a) $\tau\sigma\tau^{-1} = \sigma^2$. Notice that our τ must satisfy $\tau(1) = 1,\ \tau(2) = 3,\ \tau(3) = 5,\ \tau(4) = 2,\ \tau(5) = 4$. Certainly, τ is the cycle $(2\ 3\ 5\ 4)$.

(b) $\tau\sigma\tau^{-1} = \sigma^{-1}$. Notice that our τ must satisfy $\tau(1) = 5,\ \tau(2) = 4,\ \tau(3) = 3,\ \tau(4) = 2,\ \tau(5) = 1$. Certainly, τ is the cycle $(1\ 5)(2\ 4)$.

(c) $\tau\sigma\tau^{-1} = \sigma^{-2}$. Notice that our τ must satisfy $\tau(1) = 4,\ \tau(2) = 5,\ \tau(3) = 1,\ \tau(4) = 2,\ \tau(5) = 3$. Certainly, τ is the cycle $(1\ 4\ 2\ 5\ 3)$.

Section 4.4

13 Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

Proof. Notice that $|G| = 203 = 7 \cdot 29$. Consider $H \trianglelefteq G$ such that $|H| = 7$. There exists a homomorphism $\phi : G \to \mathrm{Aut}(H)$ which is the group action of conjugation, more specifically we define ϕ by $g \mapsto c_g \in \mathrm{Aut}(H)$ where $c_g(h) = ghg^{-1}$. By Proposition 4.4.16, we see that $|\mathrm{Aut}(H)| = 6$. Therefore, $\mathrm{im}(\phi)$ is a subgroup of order 6 which is isomorphic to $G/\ker(\phi)$ such that its order divides 6 and 203. But, $(6, 203) = 1$, and so we must have ϕ being trivial, or rather that c_g is the identity map on H for all elements $g \in G$. So, $ghg^{-1} = c_g(h) = h$ for all $h \in H$ and $g \in G$, and therefore $H \leq Z(G)$ as desired.

Consider now $Z(G)$. Via Lagrange's Theorem, we see that $Z(G)$ is either equal to G or H. So, assume $Z(G) = G$, then we are done. If $Z(G) = H$, then $G/Z(G)$ has order 29, which is prime and therefore cyclic and abelian. But, this would imply that $Z(G) = G$, so we must have that G is abelian. $\square$

Section 4.5

13 Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Proof. Notice that $|G| = 56 = 2^3 \cdot 7$. Sylow's Theorem states that the number of Sylow p-subgroups of G is of the form $1 + kp$, rather $1 \equiv n_p \bmod p$. So, we know that $n_7 \equiv 1 \bmod 7$ and $n_7 \mid 56$. So, we must have that either $n_7 = 1$ or $n_7 = 8$. If $n_7 = 1$ then we have that the Sylow 7-subgroup is normal via Corollary 20. So, let us assume that $n_7 = 8$. Note that since prime-ordered groups are cyclic, we must have that each Sylow 7-subgroup is cyclic, and excluding the identity, we have that 6 of the elements of each 7-subgroup have order 7. Moreover, since these eight 7-subgroups (which we call M_i) are distinct, we have that $M_i \cap M_j = \{1\}$ for all $i \neq j$. So, there are $8 \cdot 6 = 48$ elements of G.

Now consider N to be a Sylow 2-subgroup. Then $|N| = 8$. Certainly no elements in N have order 7, and therefore there are $48 + 8 = 56$ distinct elements, which coincices with the order of G. So, there is a single, unique p-subgroup, which implies that $N \trianglelefteq G$. $\square$

22 Prove that if $|G| = 132$ then G is not simple.

Proof. Notice that $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Let us assume for the sake of contradiction that G is simple. By Sylow's Theorem, there exist p-subgroups for $p = 2, 3, 11$ with the following possible multiplicities:

$$n_2 \in \{1, 3, 11, 33\}, \quad n_3 \in \{1, 4, 22\}, \quad n_{11} \in \{1, 12\}.$$

By our assumption that G is simple, we must have that $n_{11} = 12$, that is G has $12 \cdot 10 = 120$ elements of order 11. Then if $n_3 = 22$, we have that G has too many elements. So, we must have $n_3 = 4$, which leaves $132 - 120 - (2 \cdot 4) = 4$. But, there is not a possibility for 4 Sylow 2-subgroups in G. This is a contradiction, and therefore G cannot be simple. $\square$