Homework 5 Solutions

Section 10:

2. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.

   Solution.

$$\begin{aligned} 4\mathbb{Z} &= \{4n \mid n \in \mathbb{Z}\} \\ 2 + 4\mathbb{Z} &= \{2 + 4n \mid n \in \mathbb{Z}\} \end{aligned}$$

4. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

   Solution.

$$\begin{aligned} \langle 4 \rangle &= \{0, 4, 8\} \\ 1 + \langle 4 \rangle &= \{1, 5, 9\} \\ 2 + \langle 4 \rangle &= \{2, 6, 10\} \\ 3 + \langle 4 \rangle &= \{3, 7, 11\} \end{aligned}$$

6. Find all left cosets of the subgroup $\{\rho_0, \mu_2\}$ of the group D_4 given by Table 8.12.

   Solution.

$$\begin{aligned} &\{\rho_0, \mu_2\} \\ \rho_1\{\rho_0, \mu_2\} =& \{\rho_1, \delta_2\} \\ \rho_2\{\rho_0, \mu_2\} =& \{\rho_2, \mu_1\} \\ \rho_3\{\rho_0, \mu_2\} =& \{\rho_3, \delta_1\} \end{aligned}$$

12. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.

    Solution. $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$, so we have $|\mathbb{Z}_{24}| = 24$ and $|\langle 3 \rangle| = 8$. Hence

$$(\mathbb{Z}_{24} : \langle 3 \rangle) = \frac{24}{8} = 3.$$

16. Let $\mu = (1, 2, 4, 5)(3, 6) \in S_6$. Find the index of $\langle \mu \rangle$ in S_6.

    Solution. $|(1, 2, 4, 5)| = 4$ and $|(3, 6)| = 2$, so $|\langle \mu \rangle| = |\mu| = \text{lcm}(4, 2) = 4$ and $|S_6| = 6!$. Hence

$$(S_6, \langle \mu \rangle) = \frac{6!}{4} = 180.$$

28. Let H be a subgroup of a group G such that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. Show that every left coset gH is the same as the right coset Hg.

    Proof. Let $g \in G$ and suppose $a \in gH$. Then $a = gh$ for some $h \in H$. Since $ghg^{-1} = (g^{-1})^{-1}hg^{-1} \in H$, it follows that there is some $h' \in H$ such that $ghg^{-1} = h'$, i.e. $a = gh = h'g \in Hg$. Therefore $gH \subseteq Hg$.

    Now suppose $b \in Hg$. Then $b = kg$ for some $k \in H$. Since $g^{-1}kg \in H$, it follows that there is some k' in H such that $g^{-1}kg = k'$, i.e. $b = kg = gk' \in gH$. Therefore $Hg \subseteq gH$ and so it follows that $gH = Hg$. $\square$

34. Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

Proof. Let $H < G$. Then, by Lagrange's Theorem, $|H|\Big||G|$, i.e. $|H|\Big|pq$. Since H is a *proper* subgroup of G, it follows that $|H| \neq pq$ and so $|H|$ is 1, p, or q. If $|H| = 1$, then $H = \{e\} = \langle e \rangle$ is cyclic. Every group of prime order is cyclic (as proven in class and the book), so if $|H| = p$ or $|H| = q$, then H is cyclic. In any case, we have shown that H is cyclic, so, every proper subgroup of G is cyclic. $\square$

39. Show that if H is a subgroup of index 2 in a finite group G, then every left coset of H is also a right coset of H.

Proof. Let G be a finite group and let $H \leq G$ such that $(G : H) = 2$. Since $(G : H) = 2$, H has 2 left cosets. Left cosets of H partitition G, so it follows that the two left cosets of H are H and $G \setminus H$. Fix $g \in G$. We will show that $gH = Hg$. This is clear if $g \in H$, so we focus on the case when $g \notin H$.

If $g \notin H$, then $gH \neq H$, so it must be that $gH = G \setminus H$. We will show that $Hg = G \setminus H$ as well. Indeed, if $h \in H$, then $hg \notin H$ (otherwise, we would have $g = h^{-1}(hg) \in H$), so $Hg \subseteq G \setminus H$. Now, since $g \notin H$, we must also have $g^{-1} \notin H$ (else we would have $g = (g^{-1})^{-1} \in H$). So $g^{-1}H = G \setminus H$. Let $a \in G \setminus H$. Then $a^{-1} \in G \setminus H$ (for the same reasoning as with g) and so $a^{-1} \in g^{-1}H$. Hence $a^{-1} = g^{-1}h$ for some $h \in H$ and so $a = (a^{-1})^{-1} = (g^{-1}h)^{-1} = h^{-1}(g^{-1})^{-1} = h^{-1}g$. Since $h^{-1} \in H$, this shows that $a \in Hg$, i.e. $G \setminus H \subseteq Hg$. It follows that $Hg = G \setminus H = gH$. $\square$

[Note: This would have been easier to prove if we used Exercise 35 from Section 10, which says that there are the same number of left cosets as right cosets of any subgroup. This is not too hard to prove. Simply show that $gH \mapsto Hg^{-1}$ gives a well-defined bijection from the set of left cosets to the set of right cosets. "Well-defined" is important to check since you could have $aH = bH$ for some $a \neq b$.]

40. Show that if a group G with identity e has finite order n, then $a^n = e$ for all $a \in G$.

Proof. Let G be a group with identity e and finite order n and suppose $a \in G$. We showed in class that $\langle a \rangle \leq G$, so by Lagrange's Theorem, $|a| = |\langle a \rangle|\Big||G| = n$. Let $|a| = k$. Then $k|n$, so $n = k\ell$ for some $\ell \in \mathbb{Z}$. Now, we showed in class that if $|a| < \infty$, then $a^{|a|} = e$, so $a^k = e$ and we conclude $a^n = a^{k\ell} = (a^k)^\ell = e^\ell = e$. $\square$

<u>Section 11</u>:

5. Find the order of $(8, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

Solution. $|8| = 3$ in $\mathbb{Z}_{12}$ and $|10| = 9$ in $\mathbb{Z}_{18}$, so $|(8, 10)| = \operatorname{lcm}(3, 9) = 9$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

8. What is the largest order among the orders of all the cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_8$? of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$?

Solution. Let H be a cyclic subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_8$. Then $H = \langle (a, b) \rangle$ for some $(a, b) \in \mathbb{Z}_6 \times \mathbb{Z}_8$. But then $|H| = |(a, b)| = \operatorname{lcm}(|a|, |b|)$, so we must find the largest that $\operatorname{lcm}(|a|, |b|)$ could be for $a \in \mathbb{Z}_6$ and $b \in \mathbb{Z}_8$. But Lagrange's Theorem tells us that $|a|\Big|6$ and $|b|\Big|8$, so $\operatorname{lcm}(|a|, |b|)$ must divide $\operatorname{lcm}(6, 8) = 24$. In fact $|(1, 1)| = 24$, so 24 is the largest order among the orders of all cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_8$.

Similarly, $|(1, 1)| = \operatorname{lcm}(12, 15) = 60$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$, so the largest order among the orders of cyclic subgroups of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is 60.

10. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution.

$$\{(0,0,0),(1,0,0)\}$$
$$\{(0,0,0),(0,1,0)\}$$
$$\{(0,0,0),(0,0,1)\}$$
$$\{(0,0,0),(1,1,0)\}$$
$$\{(0,0,0),(1,0,1)\}$$
$$\{(0,0,0),(0,1,1)\}$$
$$\{(0,0,0),(1,1,1)\}$$
$$\{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$$
$$\{(0,0,0),(1,0,0),(0,0,1),(1,0,1)\}$$
$$\{(0,0,0),(0,1,0),(0,0,1),(0,1,1)\}$$
$$\{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\}$$
$$\{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}$$
$$\{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}$$
$$\{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$$

11. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ of order 4.

Solution.

$$\{(0,0),(0,1),(0,2),(0,3)\}$$
$$\{(0,0),(1,1),(0,2),(1,3)\}$$
$$\{(0,0),(0,2),(1,0),(1,2)\}$$

12. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ that are isomorphic to the Klein 4-group.

Solution.

$$\{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$$
$$\{(0,0,0),(1,0,0),(0,0,2),(1,0,2)\}$$
$$\{(0,0,0),(0,1,0),(0,0,2),(0,1,2)\}$$
$$\{(0,0,0),(1,0,0),(0,1,2),(1,1,2)\}$$
$$\{(0,0,0),(0,1,0),(1,0,2),(1,1,2)\}$$
$$\{(0,0,0),(0,0,2),(1,1,0),(1,1,2)\}$$
$$\{(0,0,0),(1,1,0),(1,0,2),(0,1,2)\}$$

<u>**Additional Exercises**</u>:

2. Verify that $\langle(1,2),(2,3)\rangle = S_3$ by expressing every non-identity element of S_3 as a product whose factors are each either $(1,2)$ or $(2,3)$.

   Solution.

$$\begin{aligned}(1,2) &= (1,2)\\ (2,3) &= (2,3)\\ (1,3) &= (1,2)(2,3)(1,2) = (2,3)(1,2)(2,3)\\ (1,2,3) &= (1,2)(2,3)\\ (1,3,2) &= (2,3)(1,2)\end{aligned}$$

   [Note: $(1,2)$ and $(2,3)$ are often called "simple transpositions". In general, simple transpositions are those of the form $(k,k+1)$ and they form a *minimal* generating set for S_n. You might have noticed that we had to multiply 3 simple transpositions to get $(1,3)$, while the others could be expressed using fewer. For this reason, $(1,3)$ can be thought of as the "longest" element of S_3. In this sense, S_n has a *unique* longest element with respect to how many simple transpositions it takes to express it.]

3. Consider $H = \langle(2,4),(1,2,3,4)\rangle \leq S_4$.

   (a) Find 7 distinct non-identity elements of H and express them as products of disjoint cycles.

   Solution.

$$\begin{aligned}(1,2,3,4) &= (1,2,3,4)\\ (1,2,3,4)(1,2,3,4) &= (1,3)(2,4)\\ (1,2,3,4)(1,2,3,4)(1,2,3,4) &= (1,4,3,2)\\ (2,4) &= (2,4)\\ (1,2,3,4)(2,4) &= (1,2)(3,4)\\ (1,2,3,4)(1,2,3,4)(2,4) &= (1,3)\\ (1,2,3,4)(1,2,3,4)(1,2,3,4)(2,4) &= (1,4)(2,3)\end{aligned}$$

   (b)* Prove that H has exactly 8 elements. To what group that we've previously seen is H isomorphic?

   Proof. The 7 elements we wrote in (a) together with ι make up 8 elements of H, so H has at least 8 elements. We will show that these 8 elements form a subgroup of S_4, say K. According to Additional Exercise 1, it follows that $H \leq K$ and so $H = K$ and so H has 8 elements.
   Set $r = (1,2,3,4)$, $s = (2,4)$, and $K = \{r^k s^\ell \mid k \in \mathbb{Z}_4, \ell \in \mathbb{Z}_2\}$ (i.e. K consists of ι and our elements from (a)). We note that $|r| = 4$ and $|s| = 2$, so $r^{k_1}r^{k_2} = r^{k_1 +_4 k_2}$ and $s^{\ell_1}s^{\ell_2} = s^{\ell_1 +_2 \ell_2}$ for $k_1, k_2 \in \mathbb{Z}_4$ and $\ell_1, \ell_2 \in \mathbb{Z}_2$. Also,

$$sr = (2,4)(1,2,3,4) = (1,4)(2,3) = (1,2,3,4)(1,2,3,4)(1,2,3,4)(2,4) = r^3 s.$$

   We may then observe that

$$\begin{aligned}sr^2 &= srr = r^3 sr = r^3 r^3 s = r^2 s \text{ and}\\ sr^3 &= sr^2 r = r^2 sr = r^2 r^3 s = rs,\end{aligned}$$

so altogether, $sr^k = r^{4-k}s$ for $k \in \mathbb{Z}_4$ (of course, if $k = 0$, this says that $r^4 = \iota$). Now, we may explicitly see that, for $k_1, k_2 \in \mathbb{Z}_4$ and $\ell_1, \ell_2 \in \mathbb{Z}_2$,

$$(r^{k_1}s^{\ell_1})(r^{k_2}s^{\ell_2}) = \begin{cases} r^{k_1+_4k_2}s^{\ell_2} & \text{if } \ell_1 = 0 \\ r^{k_1+_4(4-k_2)}s^{1+_2\ell_2} & \text{if } \ell_1 = 1 \end{cases}.$$

In both cases, $(r^{k_1}s^{\ell_1})(r^{k_2}s^{\ell_2}) \in K$, so K is closed under permutation multiplication. We've already noted that $\iota \in K$ and from the above computation one easily sees that, for $k \in \mathbb{Z}_4$ and $\ell \in \mathbb{Z}_2$,

$$(r^k s^\ell)^{-1} = \begin{cases} r^{4-k} & \text{if } \ell = 0 \\ r^k s & \text{if } \ell = 1 \end{cases}.$$

In both cases, $(r^k s)^{-1} \in K$. It follows that $K \leq S_4$. As explained at the beginning of this proof, this implies that $|H| = 8$. $\square$

The subgroup $H \leq S_4$ is isomorphic to D_4 (or, if you take the books definition of D_4, they are equal). If we think of $(2,4)$ and $(1,2,3,4)$ as permuting numbered vertices of a square, $(2,4)$ corresponds to reflecting the square over the diagonal between the first and third vertices, while $(1,2,3,4)$ corresponds to rotating the square $90°$ (the direction depends on your numbering convention).

In fact, every dihedral group D_n can be generated by 1) one reflection and one rotation or 2) two reflections. However, not just any choice will do (in either case!). I'd encourage you to find two reflections that generate D_4.