Algebra homework 10
Permutations, cosets

Exercise 1. Compute the left and the right cosets of the following subgroups $H_i$ of the following groups $G_i$.

1. $H_1 = \langle 4 \rangle$ (subgroup generated by 4) in $G_1 = \mathbb{Z}/12\mathbb{Z}$.
   
   Solution.
   
   By definition, $H_1 = \langle 4 \rangle = \{0, 4, 8\}$.
   
   Therefore, $0 + H_1 = H_1 + 0 = \{(0 + 0), (4 + 0), (8 + 0)\} = \{0, 4, 8\} = H_1$.
   
   Similarly:
   
   - $1 + H_1 = H_1 + 1 = 5 + H_1 = H_1 + 5 = 9 + H_1 = H_1 + 9 = \{1, 5, 9\}$
   - $2 + H_1 = H_1 + 2 = 6 + H_1 = H_1 + 6 = 10 + H_1 = H_1 + 10 = \{2, 6, 10\}$
   - $3 + H_1 = H_1 + 3 = 7 + H_1 = H_1 + 7 = 11 + H_1 = H_1 + 11 = \{3, 7, 11\}$
   - $4 + H_1 = H_1 + 4 = 8 + H_1 = H_1 + 8 = \{0, 4, 8\} = H_1$

2. $H_2 = 5\mathbb{Z}$ in $G_2 = \mathbb{Z}$.
   
   Solution.
   
   By definition, $H_2 = \{5k \mid k \in \mathbb{Z}\}$.
   
   Therefore, for $n \equiv 0 \pmod{5}$, $n + H_1 = H_1 + n = H_1$.
   
   Similarly:
   
   - For $n \equiv 1 \pmod{5}$, $n + H_1 = H_1 + n = 1 + H_1 = H_1 + 1 = \{5k + 1 \mid k \in \mathbb{Z}\}$
   - For $n \equiv 2 \pmod{5}$, $n + H_1 = H_1 + n = 2 + H_1 = H_1 + 2 = \{5k + 2 \mid k \in \mathbb{Z}\}$
   - For $n \equiv 3 \pmod{5}$, $n + H_1 = H_1 + n = 3 + H_1 = H_1 + 3 = \{5k + 3 \mid k \in \mathbb{Z}\}$
   - For $n \equiv 4 \pmod{5}$, $n + H_1 = H_1 + n = 4 + H_1 = H_1 + 4 = \{5k + 4 \mid k \in \mathbb{Z}\}$

3. $H_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$ in $G_3 = \mathfrak{S}_3$.
   
   Solution.
   
   Note that $(1, 2, 3)^2 = (1, 3, 2)$.
   
   Therefore, $H_3$ is a cyclic group of order 3 ($H_3 = \{\text{id}, a, a^2\}$, with $a = (1, 2, 3)$).
   
   It implies that $\text{id}H_3 = H_3\text{id} = (1, 2, 3)H_3 = H_3(1, 2, 3) = (1, 3, 2)H_3 = H_3(1, 3, 2) = H_3$.
   
   Then, we have: $(1, 2)H_3 = H_3(1, 2) = (1, 3)H_3 = H_3(1, 3) = (2, 3)H_3 = H_3(2, 3) = \{(1, 2), (1, 3), (2, 3)\}$.

4. $H_4 = \{\text{id}, (1, 3)\}$ in $G_4 = \mathfrak{S}_3$.
   
   Solution.
   
   We have $\text{id}H_4 = H_4\text{id} = H_4$.
   
   Also: $(1, 2)H_4 = \{(1, 2), (1, 2)(1, 3)\} = \{(1, 2), (1, 3, 2)\}$, and $H_4(1, 2) = \{(1, 2), (1, 2, 3)\}$.
   
   Finally, $(1, 3, 2)H_4 = \{(1, 3, 2)\text{id}, (1, 3, 2)(1, 3)\} = \{(1, 3, 2), (1, 2)\}$ and $H_4(1, 3, 2) = \{(1, 3, 2), (2, 3)\}$.
   
   These are 3 distinct left (and right) cosets of $H_4$ in $G_4$. Note that this is consistent with the counting formula, which says that there should be $[\mathfrak{S}_3 : H_4] = \frac{|\mathfrak{S}_3|}{|H_4|} = \frac{3!}{2} = 3$ distinct left cosets (and the same number of right cosets) of $H_4$ in $G_4$. 
5. $H_5 = \mathfrak{A}_n$ in $G_5 = \mathfrak{S}_n$ (Hint: show that it cannot have more than two different cosets).

Solution.

Remember that $\text{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ is a group homomorphism.

Therefore, for $\rho \in \mathfrak{S}_n$, $\rho \mathfrak{A}_n = \mathfrak{A}_n \rho = \mathfrak{A}_n$ if $\text{sgn}(\rho) = 1$ and $\rho \mathfrak{A}_n = \mathfrak{A}_n \rho = \mathfrak{S}_n \setminus \mathfrak{A}_n$ if $\text{sgn}(\rho) = -1$.

Remark: you can also use our study of subgroups of index 2 from the lectures. By the counting formula, $\mathfrak{A}_n$, being of order $n!/2$, is of index 2, which gives that there are two cosets $\mathfrak{A}_n$ and $\mathfrak{S}_n \setminus \mathfrak{A}_n$.

Exercise 2. Let $G$ be a group and $H$ a subgroup of $G$. We assume that $H$ is such that for all $h \in H$ and all $g \in G$, the product $ghg^{-1}$ is an element of $H$ (we say that $H$ is a normal subgroup of $G$).

1. Show that all subgroups of an abelian group are normal.

Solution.

If $G$ is abelian, then for all $g \in G$, and $h \in H$, $gh = hg$, so $ghg^{-1} = h \in H$.

2. Show that for all $g \in G$, $gH = Hg$, that is, the right and the left cosets of $H$ are the same.

Solution.

Let $g \in G$. For any $x \in gH$, there exists $h \in H$ such that $x = gh$.

By assumption, there exists $h' \in H$ such that $ghg^{-1} = h'$.

Therefore, $gh = h'g \in Hg$.

The other inclusion is checked by symmetry. Therefore $gH = Hg$, and this holds for any $g \in G$.

3. Find an example of a group $G$ and of a subgroup $H$ of $G$ which is not normal.

Solution.

We have seen such an example in the previous exercise, question 4:

$(1, 3, 2)H_4 = \{(1, 3, 2)\text{id}, (1, 3, 2)(1, 3)\} = \{(1, 3, 2), (1, 2)\}$ and $H_4(1, 3, 2) = \{(1, 3, 2), (2, 3)\}$.

Thus, the left coset $(1, 3, 2)H_4$ is different from the right coset $H_4(1, 3, 2) = \{(1, 3, 2), (2, 3)\}$, which by the previous question implies that $H_4$ is not a normal subgroup of $G_4$.

Exercise 3. Let $H$ and $K$ be subgroups of a group $G$.

1. Show that $H \cap K$ is a subgroup of $G$.

Solution.

- First, $H \cap K \subset G$.
- Then, since $1_G \in H$ and $1_G \in K$, we have, $1_G \in H \cap K$.
- Let $h \in H \cap K$, $k \in H \cap K$. We have $hk \in H$ by closure of $H$ under the law of $G$, and $hk \in K$ by closure of $K$. Therefore $hk \in H \cap K$.
- Lastly, let $h \in H \cap K$. We have $h^{-1} \in H$ by closure of $H$ under inversion and $h^{-1} \in K$ for the same reason. Therefore, $h^{-1} \in H \cap K$.

With these points, $H \cap K$ is a subgroup of $G$.

2. Show that for every $g \in G$, $gH \cap gK$ is a coset of $H \cap K$ in $G$.

Solution. Let $g \in G$.

Let $x \in gH \cap gK$. There exist $h \in H$ and $k \in K$ such that $x = gh = gk$.

From this equality, we get $h = k$, which is an element of $H$ and also an element of $K$. Therefore, $h \in H \cap K$. This implies that $x \in g(H \cap K)$.

As a consequence, $gH \cap gK = g(H \cap K)$. 

**Exercise 4.** Let $n \geq 2$ and let $\phi : \mathfrak{S}_n \to \{1, -1\}$ be a non-trivial group homomorphism. The aim of this exercise is to prove that $\phi$ is equal to the $\text{sgn}$ homomorphism.

1. Show that there exists at least one transposition $\tau \in \mathfrak{S}_n$ such that $\phi(\tau) = -1$.

   **Solution.**

   If it was not the case, using the homomorphism property and the fact that any permutation can be decomposed into a product of transpositions, $\phi$ would be trivial ($\phi(\sigma) = 1$ for all $\sigma \in \mathfrak{S}_n$).

   Therefore, there exists $\tau \in \mathfrak{S}_n$ such that $\phi(\tau) = -1$.

2. Show that for all permutations $\alpha, \sigma \in \mathfrak{S}_n$, we have $\phi(\sigma \alpha \sigma^{-1}) = \phi(\alpha)$.

   **Solution.**

   $\mathcal{A} \times \{1, -1\}$ is an abelian group.

   Using the homomorphism property, we have:

   $$\phi(\sigma \alpha \sigma^{-1}) = \phi(\sigma) \phi(\alpha) \phi(\sigma)^{-1} = \phi(\sigma) \phi(\sigma)^{-1} \phi(\alpha) = \phi(\alpha)$$

3. Show that for any transposition $\tau' \in \mathfrak{S}_n$, we have $\phi(\tau') = -1$.

   **Solution.**

   There exists a permutation $\sigma \in \mathfrak{S}_n$ such that $\tau' = \sigma \tau \sigma^{-1}$. Indeed, write $\tau = (a, b)$. There are two cases to consider: first of all, assume $\tau$ and $\tau'$ are disjoint, that is, $\tau' = (c, d)$ with $\{c, d\} \cap \{a, b\} = \emptyset$. Then $\sigma = (ac)(bd)$ works. If they are not disjoint, then we may assume $\tau' = (a, c)$ for some $c \neq b$. Then $\sigma = (b, c)$ works.

   With the previous question: $\phi(\tau') = \sigma \tau \sigma^{-1} = \phi(\tau) = -1$.

4. Deduce that $\phi = \text{sgn}$.

   **Solution.**

   Once again, using the homomorphism property and the fact that any permutation can be decomposed into a product of transpositions, $\phi$ and $\text{sgn}$ coincide on all permutations of $\mathfrak{S}_n$.

   That is, $\phi = \text{sgn}$.

   $\text{sgn}$ is the only non trivial homomorphism from $\mathfrak{S}_n$ to $\{1, -1\}$.

**Exercise 5.** Let $n \geq 3$ be an integer. The aim of this exercise is to show that $\mathfrak{A}_n$ is generated by cycles of length 3 of the form $(1, 2, i)$, $i \in \{3, \ldots, n\}$.

1. Check that this is true for $n = 3$.

   **Solution.** For $\mathfrak{A}_3$, we have:

   - $\text{id} = (1, 2, 3)^3$
   - $(1, 3, 2) = (1, 2, 3)^2$
   - $(1, 2, 3) = (1, 2, 3)$

2. Show that for all distinct $a, b, c \in \{2, \ldots, n\}$, we have the equality $(a, b, c) = (1, a, b)(1, b, c)$.

   **Solution.**

   Image by image, we have:

   - $((1, a, b)(1, b, c)) (a) = b$
   - $((1, a, b)(1, b, c)) (b) = c$
   - $((1, a, b)(1, b, c)) (c) = a$
• \(((1, a, b)(1, b, c)) (k) = k, \text{ if } k \not\in \{a, b, c\}\)

Therefore, \((1, a, b)(1, b, c) = (a, b, c)\).

3. Deduce that \(\mathfrak{A}_n\) is generated by cycles of length 3 of the form \((1, i, j), i, j \in \{2, \ldots, n\}\).

**Solution.** Remember that \(\mathfrak{S}_n\) is generated by cycles of length 3. By the previous question, every cycle of length 3 can itself be written as a product of cycles of the form \((1, i, j)\), whence the result.

Other method: remember that \(\mathfrak{S}_n\) is generated by \((1, i)\) transpositions. \(\mathfrak{A}_n\) is the set of permutations that can be written as product of an even number of transpositions, so you just have to generate products of two transpositions.

Observe that \((1, j)(1, i) = (1, i, j), \text{ for } i \neq j, i, j \geq 2\).

This implies that \(\mathfrak{A}_n\) is generated by \((1, i, j)\) cycles, \(i \neq j, i, j \geq 2\).

4. Let \(\sigma \in \mathfrak{A}_n\) be a cycle of length 3 containing 1 and 2. Show that either \(\sigma\) or \(\sigma^{-1}\) is of the form \((1, 2, i)\).

**Solution.**

Let’s assume \(\sigma \neq (1, 2, i)\), i.e. \(\sigma = (1, i, 2)\).

In that case, \(\sigma^{-1} = (2, i, 1) = (1, 2, i)\) (checking image by image).

5. Let \(\sigma \in \mathfrak{A}_n\) be a cycle of the form \((1, i, j)\). Show that we have

\[(1, i, j) = (1, 2, j)^{-1}(1, 2, i)(1, 2, j)\]

**Solution.**

We have \((1, 2, j)^{-1} = (j, 2, 1)\). And you can check that:

- \(((j, 2, 1)(1, 2, i)(1, 2, j)) (1) = i\)
- \(((j, 2, 1)(1, 2, i)(1, 2, j)) (i) = j\)
- \(((j, 2, 1)(1, 2, i)(1, 2, j)) (j) = 1\)
- \(((j, 2, 1)(1, 2, i)(1, 2, j)) (k) = k, \text{ if } k \not\in \{1, i, j\}\)

Conclusion:

\[(1, i, j) = (1, 2, j)^{-1}(1, 2, i)(1, 2, j)\]

Note: you can also rewrite this relation as

\[(1, i, j) = (j, 2, 1)(1, 2, i)(j, 2, 1)^{-1}\]

and use the formula for \(\sigma(a_1, \ldots, a_k)\sigma^{-1}\) we have seen in lectures.

6. Conclude that \(\mathfrak{A}_n\) is generated by cycles of length 3 of the form \((1, 2, i)\).

**Solution.**

With the previous result, since \(\mathfrak{A}_n\) is generated by cycles of the form \((1, i, j)\) and since those can be written as products of cycles of the form \((1, 2, i)\), \(\mathfrak{A}_n\) is generated by \((1, 2, i)\) cycles.