Algebra homework 9
Permutations, Cosets, Lagrange’s theorem
Due November 20th, 2019

Please hand in your homework stapled, with your name written on it. All answers have to be justified.

Exercise 1. Describe the left and the right cosets of the following subgroups \( H_i \) of the following groups \( G_i \), and compute \([G_i : H_i]\) for every \( i \).

1. \( H_1 = \langle 4 \rangle \) (subgroup generated by 4) in \( G_1 = \mathbb{Z}/12\mathbb{Z} \).

   Solution. \( \mathbb{Z}/12\mathbb{Z} \) is commutative, so left and right cosets are equal. By definition, \( H_1 = \langle 4 \rangle = \{0, 4, 8\} \).

   Therefore, \( 0 + H_1 = H_1 + 0 = \{0, 4, 8\} = H_1 \).

   Similarly:
   
   - \( 1 + H_1 = H_1 + 1 = 5 + H_1 = H_1 + 5 = 9 + H_1 = H_1 + 9 = \{1, 5, 9\} \)
   - \( 2 + H_1 = H_1 + 2 = 6 + H_1 = H_1 + 6 = 10 + H_1 = H_1 + 10 = \{2, 6, 10\} \)
   - \( 3 + H_1 = H_1 + 3 = 7 + H_1 = H_1 + 7 = 11 + H_1 = H_1 + 11 = \{3, 7, 11\} \)
   - \( 4 + H_1 = H_1 + 4 = 8 + H_1 = H_1 + 8 = \{0, 4, 8\} = H_1 \)

   We deduce that \([G_1 : H_1] = 4\).

2. \( H_2 = 3\mathbb{Z} \) in \( G_2 = \mathbb{Z} \).

   Solution.

   By definition, \( H_2 = \{3k \mid k \in \mathbb{Z}\} \).

   Therefore, for \( n \equiv 0 \pmod{3} \), \( n + H_1 = H_1 + n = H_1 \).

   Similarly:
   
   - For \( n \equiv 1 \pmod{3} \), \( n + H_1 = H_1 + n = 1 + H_1 = H_1 + 1 = \{3k + 1 \mid k \in \mathbb{Z}\} \)
   - For \( n \equiv 2 \pmod{3} \), \( n + H_1 = H_1 + n = 2 + H_1 = H_1 + 2 = \{3k + 2 \mid k \in \mathbb{Z}\} \)

   We have \([G_2 : H_2] = 3\).

3. \( H_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\} \) in \( G_3 = S_3 \).

   Solution.

   We have \( \text{id}H_3 = H_3\text{id} = (1, 2, 3)H_3 = H_3(1, 2, 3) \).

   Then, we have: \( (1, 2)H_3 = H_3(1, 2) = (1, 3)H_3 = H_3(1, 3) = (2, 3)H_3 = H_3(2, 3) = \{(1, 2), (1, 3), (2, 3)\} \).

   We have \([G_3 : H_3] = 2\).

4. \( H_4 = \{\text{id}, (1, 3)\} \) in \( G_4 = S_3 \).

   Solution.

   We have \( \text{id}H_4 = H_4\text{id} = H_4 = (13)H_4 = H_4(13) \).

   For the other left cosets:
   
   \( (1, 2)H_4 = \{(1, 2), (1, 2)(1, 3)\} = \{(1, 2), (1, 3, 2)\} = (1, 3, 2)H_4 \),
Exercise 3. Let $H_4 = \{(1, 2, 3)\text{id}, (1, 2, 3)(1, 3)\} = \{(1, 2, 3), (2, 3)\} = (2, 3)H_4$.

For the other right cosets: $H_4(1, 2) = \{(1, 2), (1, 2, 3)\} = H_4(1, 2, 3)$ and $H_4(1, 3, 2) = \{(1, 3, 2), (2, 3)\} = H_4(2, 3)$.

We have $[G_4 : H_4] = 3$.

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 $\sgn : \mathfrak{S}_n \rightarrow \{-1, 1\}$ is a group homomorphism.

Therefore, for $\rho \in \mathfrak{S}_n$, $\rho\mathfrak{A}_n = \mathfrak{A}_n\rho = \mathfrak{A}_n$ if $\sgn(\rho) = 1$ and $\rho\mathfrak{A}_n = \mathfrak{A}_n\rho = \mathfrak{S}_n \setminus \mathfrak{A}_n$ (the set of odd permutations) if $\sgn(\rho) = -1$. We have $[G_5 : H_5] = 2$.

**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 in the same way. 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 $n \geq 2$ and let $\phi : \mathfrak{S}_n \rightarrow \{1, -1\}$ be a non-trivial group homomorphism. The aim of this exercise is to prove that $\phi$ is equal to the 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 $\alpha, \sigma \in S_n$, we have $\phi(\sigma \alpha \sigma^{-1}) = \phi(\alpha)$.

Solution.

$(\{-1, 1\}, \times)$ is an abelian group.

Using the homomorphism property, we have:

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

3. Let $\alpha, \alpha'$ be two transpositions.

(a) Put $\alpha = (a, b)$. Show that if $\alpha' \neq \alpha$, we may assume that either $\alpha' = (c, d)$ with $c, d$ distinct from $a, b$, or $\alpha' = (a, c)$ with $c$ distinct from $a, b$.

Solution. Write $\alpha' = (c, d)$. If $\alpha' \neq \alpha$, it must be that the intersection $\{c, d\} \cap \{a, b\}$ has at most one element. There are two cases: if it has exactly one element, then, up to exchanging $c, d$ and $a, b$, we may assume $d = a$, so that $\alpha = (a, c)$. If it is empty, then $c, d$ are distinct from $a, b$.

(b) Show that there exists a permutation $\sigma$ such that $\sigma \alpha \sigma^{-1} = \alpha'$.

Solution. Note that for any $\sigma$, $\sigma \alpha \sigma^{-1} = (\sigma(a), \sigma(b))$. If $\alpha = \alpha'$, then $\sigma = \text{id}$ works. Now assume $\alpha$ and $\alpha'$ are disjoint, that is, $\alpha' = (c, d)$ with $\{c, d\} \cap \{a, b\} = \emptyset$. Then $\sigma = (ac)(bd)$ works. If they are not disjoint and not equal, by the previous question we may assume $\alpha' = (a, c)$ for some $c \neq b$. Then $\sigma = (b, c)$ works.

4. Show that for any transposition $\tau' \in S_n$, we have $\phi(\tau') = -1$.

Solution.

There exists a permutation $\sigma \in S_n$ such that $\tau' = \sigma \tau \sigma^{-1}$.

With question 2: $\phi(\tau') = \sigma \tau \sigma^{-1} = \phi(\tau) = -1$.

5. Deduce that $\phi = \text{sgn}$, that is, that $\phi(\sigma) = \text{sgn}(\sigma)$ for all $\sigma \in S_n$.

Solution. Let $\sigma \in S_n$. Decomposing $\sigma = \tau_1 \ldots \tau_r$ into a product of transpositions, we have $\phi(\sigma) = \phi(\tau_1) \ldots \phi(\tau_r) = (-1)^r = \text{sgn}(\sigma)$.

Thus, $\phi = \text{sgn}$ and $\text{sgn}$ is the only non trivial homomorphism from $S_n$ to $\{-1, 1\}$.

Exercise 4. Let $G$ be a group of order 25.

1. Prove that $G$ has at least one element of order 5.

Solution.

Since $G$ has order 25, there exists an element $g$ in $G$ of order strictly greater than 1 (otherwise, $G = \{1\}$, which is of order 1).

The order of such an element divides 25. Since 25 = $5 \times 5$. Therefore, the order of $g$ is either 5 or 25.

If $g$ has order 5, the cyclic group generated by $g$ is a subgroup of order 5 of $G$.

If $g$ has order 25, the cyclic group generated by $g^5$ is a subgroup of order 5 of $G$. Indeed, denoting $h = g^5$, we have that the elements $h^2 = g^{10}$, $h^3 = g^{15}$, $h^4 = g^{20}$ are different from the identity element, whereas $h^5 = g^{25} = 1$.

2. Deduce that $G$ has at least one subgroup of order 5.

Solution. It suffices to take $\langle g \rangle$ where $g$ is an element of order 5.
3. If $G$ is cyclic, show that it contains exactly one subgroup of order 5.

   \textit{Solution.} If $G$ is cyclic, it is isomorphic to $\mathbb{Z}/25\mathbb{Z}$ and we saw in lectures that the latter has exactly one subgroup of order 5, namely $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$.

4. Show that if $G$ is not cyclic, it must have more than one subgroup of order 5.

   \textit{Solution.}

   Let’s assume that $G$ contains a single subgroup of order 5. We must show that $G$ is cyclic.

   Let $g \in G$ different from the identity. If $g$ has order 25, then we are done: $\langle g \rangle = G$, so $G$ is cyclic.

   If not, by Lagrange’s theorem it must have order 5. So by the above assumption, $\langle g \rangle$ is the only subgroup of order 5 of $G$.

   Let $h \in G \setminus \langle g \rangle$. The order of $h$ is necessarily 25 since it can’t be 1 ($h \neq e$, since $e \in \langle g \rangle$) and it can’t be 5 ($\langle h \rangle$ would be another group of order 5 in $G$).

   Therefore, the order of $h$ is 25 and $G = \langle h \rangle$, i.e. $G$ is cyclic.