Algebra homework 11
Index, Lagrange’s theorem

Exercise 1. Compute the indexes of the following subgroups $H_i$ of the following groups $G_i$.

1. $H_1 = \langle 3 \rangle$ (subgroup generated by 3) in $G_1 = \mathbb{Z}/81\mathbb{Z}$.
   
   Solution. The group $H_1$ has three cosets: $H_1$, $1 + H_1$ and $2 + H_1$, so its index is 3. You can also compute it using Lagrange’s theorem, by first computing the order of $H_1$. We have
   
   $H_1 = \{0, 1 \cdot 3, 2 \cdot 3, \ldots, 26 \cdot 3\}$
   
   so $|H_1| = 27$, and therefore
   
   $[G_1 : H_1] = \frac{|G_1|}{|H_1|} = \frac{81}{27} = 3$.

2. $H_2 = 23\mathbb{Z}$ in $G_2 = \mathbb{Z}$.
   
   Solution.
   
   Let us use the equivalence relation the equivalence classes of which are the cosets of $H_2$ in $G_2$ (cf. 4.1.6 in the lecture notes). The equivalence class of a given $n \in \mathbb{Z}$ is:
   
   $\tilde{n} = \{m \in \mathbb{Z} : m - n \in 23\mathbb{Z}\} = \{n + 23k : k \in \mathbb{Z}\}$
   
   The cosets correspond to the 23 possible remainders of the Euclidean division by 23. Hence, $[G_2 : H_2] = 23$.

3. $H_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$ in $G_3 = \mathfrak{S}_3$.
   
   Solution.
   
   The index of $H_3$ in $G_3$ is given by Lagrange’s theorem:
   
   $[G_3 : H_3] = \frac{|G_3|}{|H_3|} = \frac{6}{3} = 2$

4. $H_4 = \{\text{id}, (1, 3)\}$ in $G_4 = \mathfrak{S}_3$.
   
   Solution.
   
   The index of $H_4$ in $G_4$ is given by Lagrange’s theorem:
   
   $[G_4 : H_4] = \frac{|G_4|}{|H_4|} = \frac{6}{2} = 3$

Exercise 2. Let $f : \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ given by $f(x) = 3x$.

1. Prove that $f$ is a group homomorphism.
   
   Solution.
   
   $f$ is clearly well-defined. Let $x, y \in \mathbb{Z}/9\mathbb{Z}$. We have:
   
   $f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$
   
   This is true for any $x, y$. As a consequence $f$ is a homomorphism.
2. Compute $\ker f$ and $\text{Im } f$.

\textit{Solution.}

By definition, $\ker f = \{ x \in \mathbb{Z}/9\mathbb{Z} : 3x = 0 \} = \{ 0, 3, 6 \}$.

And: $\text{Im } f = \{ 3x : x \in \mathbb{Z}/9\mathbb{Z} \} = \{ 0, 3, 6 \}$.

3. Check that $[\mathbb{Z}/9\mathbb{Z} : \ker f] = |\text{Im } f|$.

\textit{Solution.}

With the previous calculation, using Lagrange’s theorem:

$$[\mathbb{Z}/9\mathbb{Z} : \ker f] = |\mathbb{Z}/9\mathbb{Z}| - |\ker f| = \frac{|\mathbb{Z}/9\mathbb{Z}|}{|\{ 0, 3, 6 \}|} = \frac{9}{3} = 3 = |\text{Im } f|$$

\textbf{Exercise 3.} 1. Give a list of all the subgroups of $\mathbb{Z}/14\mathbb{Z}$ together with their orders.

\textit{Solution.}

The order of a subgroup of $\mathbb{Z}/14\mathbb{Z}$ must divide 14. Therefore, non trivial subgroups can be of order 2 or 7.

We have: $\{ 0, 2, 4, 6, 8, 10, 12 \}$ of order 7 and $\{ 0, 7 \}$ of order 2.

2. Check that

$$14 = \sum_{d|14} \phi(d)$$

where $\phi$ is Euler’s function.

\textit{Solution.}

By definition of Euler’s function, we have $\phi(14) = 6$, since 1, 3, 5, 9, 11, 13 are relatively prime with 14, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(7) = 6$.

Therefore the formula is satisfied on this example: $14 = \phi(1) + \phi(2) + \phi(7) + \phi(14)$.

\textbf{Exercise 4.} Let $G$ be a group of order 25.

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

\textit{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. Prove that if $G$ contains only one subgroup of order 5, then it is cyclic.

\textit{Solution.}

Let’s assume that $G$ contains a single subgroup of order 5.

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, 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 (the identity is 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.

**Exercise 5.** Let \( \phi : G \to G' \) be a group homomorphism. Assume that \( G \) is of order 18, \( G' \) is of order 15 and that \( \phi \) is not the trivial homomorphism. What is the order of \( \text{Ker} \phi \)?

**Solution.**
As seen in lectures, (proposition 4.5.2 of the notes), \(|\text{Ker} \phi| \times |\text{Im} \phi| = |G| = 18\). Let’s analyze the order of the image. It’s a subgroup of \( G' \) and therefore, by Lagrange’s theorem, \(|\text{Im} \phi|\) divides 15. So it’s either 3, 5 or 15 (1 is excluded since \( \phi \) is not trivial.).

It can’t be 5 nor 15 since \(|\text{Ker} \phi| \times |\text{Im} \phi| = 18\) implies that \(|\text{Im} \phi|\) is also a divisor of 18. Therefore, \(|\text{Im} \phi| = 3\), and it follows that \(|\text{Ker} \phi| = \frac{18}{3} = 6\).

**Exercise 6.** Does a group of order 16 necessarily contain an element of order 4? Justify your answer by either proving the existence of such an element or providing an example where it doesn’t exist.

**Solution.**
No, a counterexample is \((\mathbb{Z}/2\mathbb{Z})^4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\). Its elements are of the form \(x = (x_1, x_2, x_3, x_4)\) where \(x_i \in \mathbb{Z}/2\mathbb{Z}\) for all \(i \in \{1, \ldots, 4\}\). For such an element \(x\), we have 

\[2x = (2x_1, 2x_2, 2x_3, 2x_4) = (0, 0, 0, 0),\]

so all elements of this group other than the identity element are of order 2. At the same time, the order of this group is \(|\mathbb{Z}/2\mathbb{Z}|^4 = 16\).

**Exercise 7.** Let \( n \geq 1 \) be an integer and let \( G \) be a group of order \( 2^n \).

1. Prove that the number of elements of order 2 in \( G \) is odd. (Hint: recall that elements of order 2 are their own inverses.)

**Solution.**
Removing from \( G \) all pairs \(\{x, x^{-1}\}\) such that \(x \neq x^{-1}\), we still have an even number of elements.

Removing the identity (order 1), we get an odd number of elements, which are exactly the elements of order 2 in \( G \).

2. Show that \( G \) must contain a subgroup of order 2.

**Solution.**
As a consequence of the previous question, there exists at least one element \(x\) of order 2 in \( G \). The subgroup \( \langle x \rangle = \{1, x\} \) it generates is a subgroup of order 2 of \( G \).

**Exercise 8.**
1. Find an integer \( x \) such that \( x^2 \equiv -1 \pmod{5} \).

**Solution.**
Observe that \(3^2 \equiv -1 \pmod{5}\).

2. Find an integer \( x \) such that \( x^2 \equiv -1 \pmod{13} \).

**Solution.**
Observe that \(5^2 \equiv -1 \pmod{13}\).

3. Let \( p \) be a prime congruent to 3 modulo 4. Show that there is no solution to the equation \( x^2 \equiv -1 \pmod{p} \).

**Solution.**
Assume there exists \( x \) such that \( x^2 \equiv -1 \pmod{p} \). The integer \( p - 1 \) is even, so we may raise both sides to the power \( \frac{p-1}{2} \). On the left-hand side we get \((x^2)^{\frac{p-1}{2}} = x^{p-1}\), which by Fermat’s
little theorem should be congruent to 1 modulo $p$. On the right-hand side we get $(-1)^{\frac{p-1}{2}}$: since $p$ is of the form $3 + 4k$ for some integer $k$, we get that $\frac{p-1}{2} = 1 + 2k$ is odd, so that $(-1)^{\frac{p-1}{2}} = -1$. We therefore get $1 \equiv -1 \pmod{p}$, which implies that $p$ divides 2, which is impossible.