Algebra 2025/2026: Exercise sheet 3

Exercise 1.

Let p be a prime number. Show that the group $Aut_{\mathcal{G}rp}(\mathbb{Z}/p\mathbb{Z})$ of automorphisms of the group $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of (non zero elements in) the field $\mathbb{Z}/p\mathbb{Z}$.

(We will prove later in the lecture that this group is always cyclic.)

Exercise 2.

Let G be a group of order p^2 with p a prime number.

1) If G contains an element of order p^2 show that G isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

We assume from now on, that G has no element of order p^2.

2) Show that all elements of $G \setminus \{e_G\}$ have order p. Let g be one of them. Conclude from Exercise 3 below that $\mathbb{Z}/p\mathbb{Z} \cong < g > \subset G$ is normal.

3) Show that the quotient $G/ < g >$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and conclude that G is isomorphic to the semi-direct product $\mathbb{Z}/p\mathbb{Z} \rtimes_\rho \mathbb{Z}/p\mathbb{Z}$ with respect to some group homomorphism $\rho : \mathbb{Z}/p\mathbb{Z} \to Aut_{\mathcal{G}rp}(\mathbb{Z}/p\mathbb{Z})$.

4) Conclude from Exercise 1) of this sheet that G is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. In particular every group of order p^2 is abelian!

Exercise 3.

Let H be a subgroup of the finite group G and assume the index $[G : H] = |G/H|$ is a prime number p. We have seen in the exercise 4 of the exercise sheet 1 that in general H is not normal ($D_4 \subset S_4$ has order 3 and is not normal). Now we assume that p is the smallest prime number that divides $|G|$. We will prove that in that case H is normal.

1) Let G act on the quotient G/H, by the formula $G \times (G/H) \ni (g, \alpha) \mapsto g.\alpha$. For each g this formula defines a permutation of G/H; we get in this way a group homomorphism $G \to S_{G/H} \cong S_p$. The kernel K of that group homomorphism consists of the $g \in G$ such that for any left coset $\alpha \in G/H$, $g.\alpha = \alpha$. Show that $K \subset H$.

2) Show that the index $[G : K]$ divides $p!$. [Hint: the quotient G/K group is a subgroup of S_p.]

3) Conclude that $[G : K] = p$. [Hint: use the fact that $[G : K]$ also divides $|G|$. And use that p is the smallest prime number that divides $|G|$.]

4) Show that $[G : K] = [G : H][H : K]$ and conclude that $[H : K] = 1$ that is to say $H = K$. As K is normal, H is also normal.

Exercise 4. *Classification of groups of order* 8.

Let G be a group with 8 elements.

1) Assume G is abelian. Show it is isomorphic to $\mathbb{Z}/8\mathbb{Z}$ if it has an element of order 8. Assume now G has an element of order 4 but none of order 8. Show that G is isomorphic to $\mathbb{Z}/4 \times \mathbb{Z}/2$. If G has no element of order 4 or 8, show that it is naturally a $\mathbb{Z}/2\mathbb{Z}$-vector space, thus isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. Show that none of the groups $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4 \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ is isomorphic to an other.

2) If G is non abelian, show that it has at least one element of order 4. (you may use the exercise 2 of sheet 1 or the exercise 3 of the tutorial sheet 1)

From now on, we assume that G is non abelian, and we choose a cyclic subgroup $H \subset G$ of order 4, whose existence is given by question 2).

3) Show that H is normal. (You can use the first question of exercise 4 in the first exercise sheet.) Deduce that if there is an element of order 2 in $G \setminus H$, then G is isomorphic the dihedral group D_4, semi direct product of $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ over the unique non trivial action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/4\mathbb{Z}$.

4) Now we assume that no element of $G \setminus H$ has order 2. Conclude that G has only one element of order 2 (also contained in H) which is denoted by -1, and that $-1 \in Z(G)$.

We also denote by $1 = e_G$ the neutral element of G and for $g \in G$ by $-g$ the product $(-1).g$.

5) Let $g \in G \setminus H$. Show that $< g > \cap H = \{1, -1\}$, and that $< g >= \{1, -1, g, -g\}$.

6) Choose a generator i of H. Choose an element $j \in G \setminus H$. Show that $< i > \cup < j >$ has exactly 6 elements. Denote by k the product ij. Show that $k \in G\setminus < i > \cup < j >$. And show that $G = \{1, -1, i, -i, j, -j, k, -k\}$ and that the product in G is given by the formulas:

$$i^2 = j^2 = k^2 = -1 = ijk$$

(this group is called the *quaternion* group)