Solutions of exercise sheet 4

The content of the marked exercises **(*)** should be known for the exam.

1. Prove the following two properties of groups:

1. Every subgroup of a cyclic group is cyclic [Recall, we say that a group G is cyclic if $G = \langle g \rangle$ for some $g \in G$. A cyclic group can be either finite or infinite.]
2. Given a group G, if $\mathrm{Aut}(G)$ is cyclic then G is abelian [*Hint:* Consider the conjugation map $G \to \mathrm{Aut}(G)$.]

Solution:

1. Suppose G is a cyclic group and $H \leq G$. Let $G = \langle g \rangle$. If $H = \{1_G\}$, then it is cyclic (generated by 1_G) and we are done. Else there exists $m \in \mathbb{Z} \setminus \{0\}$ such that $x = g^m \in H$. Up to inverting x, we may assume that $m > 0$. Then we can assume without loss of generality that m is the minimal positive integer such that $g^m \in H$. We claim that $H = \langle g^m \rangle$, which makes H cyclic. The inclusion "$\supseteq$" follows from the facts that $g^m \in H$ and $H \leq G$. For the inclusion "$\subseteq$", pick an element $g^s \in H$. Then, diving s by m in $\mathbb{Z}$, i.e., finding $k \in \mathbb{Z}$, $0 \leq r < m$ such that $s = km + r$, we obtain $g^s = (g^m)^k g^r$, that is $g^r = g^s \cdot (g^m)^{-k} \in H$. By minimality of m, we obtain $r = 0$, so that $g^s = (g^m)^k \in \langle g^m \rangle$ and $H \subseteq \langle g^m \rangle$.
2. Now suppose G is a group with $\mathrm{Aut}(G)$ cyclic. Then, considering the conjugation morphism $\gamma : G \to \mathrm{Aut}(G)$ sending g to the inner automorphism $x \mapsto gxg^{-1}$, we have that $\ker(\gamma) = Z(G)$ (see previous Exercise sheet's solution, Exercise 6), so that $G/Z(G) \cong \mathrm{Im}(\gamma) \leq \mathrm{Aut}(G)$, and by previous point $G_1 := G/Z(G)$ is cyclic. Take a generator $tZ(G)$ for G_1, by fixing a suitable $t \in G$. Then every element $x \in G$ can be written as $x = t^n c$, with $c \in Z(G)$ and $n \in \mathbb{Z}$. We now prove that $t \in Z(G)$, so that $Z(G) = G$ and G is abelian. Let $x \in G$ and take the commutator $[x, t] = xtx^{-1}t^{-1}$. Writing down $x = t^n c$, we get
$$[x, t] = t^n ctc^{-1}t^{-n}t^{-1} = t^{n+1}cc^{-1}t^{-n-1} = 1_G$$
because $c \in Z(G)$. Hence $t \in Z(G) = G$ and we are done.

2. Let H, K be subgroups of G, and assume that $hK = Kh$ for every $h \in H$.

1. Show that:
   - $H \cap K \trianglelefteq H$;

Please turn over!

- $HK \leq G$;
- $K \trianglelefteq HK$.

2. Prove that there is an isomorphism $H/(H \cap K) \xrightarrow{\sim} HK/K$ [*Hint:* Define first a group homomorphism $H \longrightarrow HK/K$]

Solution:

1. Assume $x \in H \cap K$ and $h \in H$. By hypothesis, $hx = yh$ for some $y \in K$, and being $y = hxh^{-1} \in H$, we obtain $hxh^{-1} \in H \cap K$, proving $H \cap K \trianglelefteq H$.

   Now we prove that $HK \leq G$ using subgroups' criterium:

   - $1_G = 1_G \cdot 1_G \in HK$;
   - Given elements $h_i \in H$ and $k_i \in K$, $i = 1, 2$ one has $h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$. Then $k_1 k_2^{-1} h_2^{-1} \in K h_2^{-1} = h_2^{-1} K$, so that we can write $k_1 k_2^{-1} h_2^{-1} = h_2^{-1} k_0$, with $k_0 \in K$, implying $h_1 k_1 (h_2 k_2)^{-1} = h_1 h_2^{-1} k_0 \in HK$.

   K is clearly contained in HK (as the set of elements of the form $1_G \cdot k$, with $k \in K$), hence $K \leq HK$. Moreover, $\forall k \in K$ and $x \in HK$, $x = h_0 k_0$, we have $xkx^{-1} = h_0 k_0 k k_0^{-1} h_0^{-1} \in hKh^{-1} = K$ by hypothesis, and we conclude that $K \trianglelefteq HK$.

2. We define the group map $f : H \longrightarrow HK/K$ sending $h \mapsto hK$. It is easily seen to be surjective: every element in HK/K has the form hkK with $h \in H$ and $k \in K$. But $hkK = hK = f(h)$. Then applying the First Isomorphism Theorem we get an induced isomorphism $\bar{f} : H/\ker(f) \to HK/K$ defined by $\bar{f}(h \ker(f)) = hK$, where $\ker(f) = \{h \in H : hK = K\} = H \cap K$, so that $\bar{f}$ is the required isomorphism.

3. Let G be a group with a normal subgroup $H \trianglelefteq G$ and consider the canonical projection $\pi : G \to G/H$ sending $g \mapsto gH$. Prove the following statements:

1. If $K \leq G/H$, then $\pi^{-1}(K)$ is a subgroup of G containing H.
2. Conversely, if we have an intermediate subgroup $H \leq K' \leq G$, then $\pi(K') \leq G/H$.
3. The map

$$f : \left\{ \begin{array}{c} \text{subgroups } K', \\ H \leq K' \leq G \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ K \leq G/H \end{array} \right\}$$
$$K' \longmapsto \pi(K')$$

   is a bijection.
4. For every $H \leq K' \leq G$, one has that $K' \trianglelefteq G$ if and only if $f(K') \trianglelefteq G/H$.

Solution:

1. Since π is a group homomorphism, we have that $\pi^{-1}(K) \leq G$ by Exercise 1.4 from Exercise Sheet 2 (where the answer was "yes"). Moreover, for $h \in H$ we have that $\pi(h) = 1_{G/H} \in K$, so that $h \in \pi^{-1}(K)$, and $H \leq \pi^{-1}(K)$.

See next page!

2. We have that $\pi(K') = \mathrm{Im}(\pi \circ i_K)$, where $i_K : K \to G$ is the canonical inclusion of K in G (a group homomorphism). Hence $\pi(K') \leq G/H$.
3. Let us prove that the map g in the other direction defined via $g(K) = \pi^{-1}(K)$ is an inverse of f:
   - $f \circ g = \mathrm{id}$: Let $K \leq G/H$. Then $(f \circ g)(K) = \pi(\pi^{-1}(K)) = \{\pi(x) | x \in G, \pi(x) \in K\} = K \cap \mathrm{Im}(\pi) = K$, being π surjective. Hence $f \circ g = \mathrm{id}$.
   - $g \circ f = \mathrm{id}$: Let $H \leq K' \leq G$. Then $(g \circ f)(K') = \pi^{-1}(\pi(K')) = \{x \in G : \pi(x) = \pi(y), y \in K'\} = \{x \in G : xH = yH, y \in K'\} = \{x \in yH, y \in K'\} = K'H = K'$, being $H \leq K$. Hence $f \circ g = \mathrm{id}$.
4. Suppose that $K' \trianglelefteq G$. Then we have a unique group homomorphism $p_{K',H} : G/H \to G/K'$ such that $p_{K',H} \circ \pi = \pi_{K'}$, where $\pi_{K'}$ is the canonical projection $\pi_{K'} : G \to G/K'$. This homomorphism $p_{K',H}$ is the one sending $gH \mapsto gK'$, which is well-defined because $H \leq K' = \ker(\pi_{K'} : G \to G/K')$, so that the ambiguity of taking $gH \in G/H$, which lies in H does not change the image of the element. Then $f(K') = \pi(K') = \{k'H : k' \in K'\} = \ker(pi_{K',H}) \trianglelefteq G/H$.

   Conversely, suppose that $f(K') = \pi(K') \trianglelefteq G/H$. Then by previous point we have $K' = \pi^{-1}(\pi(K')) = \pi^{-1}(f(K')) \trianglelefteq G$ because the counterimage of a normal subgroup via a group homomorphism is always normal subgroup, and we are done [The proof that given a group homomorphism $\alpha : G_1 \to G_2$ and $K_2 \trianglelefteq G_2$ we get $\alpha^{-1}(K_2) \trianglelefteq G_1$ can be done as follows: consider the canonical projection $\pi_2 : G_2 \to G_2/K_2$. Then

$$\begin{aligned} f^{-1}(H_2) &= \{x \in G_1 | f(x) \in H_2\} = \{x \in G_1 | f(x) \in \ker(\pi_2)\} = \\ &= \{x \in G_1 | (\pi_2 \circ f)(x) = 1_{G_2/K_2}\} = \ker(\pi_2 \circ f) \trianglelefteq G_1.] \end{aligned}$$

4. Let G be a group and $H \leq G$ with $[G : H] = 2$. Prove: $H \trianglelefteq G$.

Solution:

Being $[G : H] = 2$, we have $H \neq G$, and we can take $g \in G \setminus H$. Then H and gH are two disjoint right cosets of H, while H and Hg are two disjoint left cosets of H. Since $[G : H] = 2$, we have $H \cup gH = G = H \cup Hg$, and disjointness gives $gH = G \setminus H = Hg$. So now let $x \in G$. If $x \in H$, i.e. $xH = H$, i.e. $H = Hx$, then $xH = Hx$. Else, $xH = gH = Hg = Hx$. Hence $xH = Hx$ in any case, and $H \trianglelefteq G$.

5. **(*)** Let A be a simple finite abelian group.

1. Show that A is generated by an element $x \in A$ different from 1_A.
2. Show that $A \cong \mathbb{Z}/k\mathbb{Z}$ where k is a prime. Conversely, show that $\mathbb{Z}/p\mathbb{Z}$ is a simple group for every prime number p.

Solution:

1. Suppose $M \leq A$. Then being A abelian, for each $a \in A$ one has $aHa^{-1} = \{aha^{-1} | h \in H\} = H$, so that $H \trianglelefteq A$. This means that, being A simple, $M = A$ or $M = \{1_A\}$. Also, by definition of simple group we have $A \neq \{1_A\}$, and we can take $x \in A$, $x \neq 1_A$. Look at $M = \langle x \rangle$. Being $1_A \neq x \in M$, we get $M \neq \{1_A\}$, so that $M = A$. Hence A is generated by (any element) $x \neq 1_A$.
2. Let $x \in A$, $x \neq 1_A$. Then we have just proved that the map $\vartheta : (\mathbb{Z}, +) \to A$ sending $n \mapsto a^n$ is surjective. It is easily seen to be a group homomorphism so that $A \cong \mathbb{Z}/\ker(\vartheta)$. By Exercise 1.1, we have that $\ker(\vartheta)$ is a cyclic subgroup of $(\mathbb{Z}, +)$, implying $\ker(\vartheta) = k\mathbb{Z}$, where we can k can be taken positive. We can exclude the cases $k = 0$ (which gives $|A| = [\mathbb{Z} : 0\mathbb{Z}] = \infty$, contradiction with A finite) and $k = 1$ (which gives $A = \{1_A\}$). As, seen in the last point, every non-trivial element generates A, so that all the non-trivial elements have the same order k. This implies that k is prime. Else, there would be some proper divisor $1 \neq d \neq k$ of k, and for $x \in A$ of order k we would have that the order of $x^d \in A \setminus \{1_A\}$ is k/d. Hence $A \cong \mathbb{Z}/k\mathbb{Z}$, with k a prime number.

   Conversely, every group $\mathbb{Z}/p\mathbb{Z}$, with p prime number is simple, since it has $p > 1$ elements, and by Lagrange Theorem every subgroup needs to have order dividing p, that is, order 1 or p.

6. (*) Given two group homomorphisms $\alpha : H \to G$ and $\beta : G \to K$ we say that

$$H \overset{\alpha}{\to} G \overset{\beta}{\to} K$$

is an exact sequence if $\mathrm{Im}(\alpha) = \ker(\beta)$. Moreover, given group morphisms

$$(**) \qquad \cdots \longrightarrow G_{n-2} \overset{\alpha_{n-2}}{\longrightarrow} G_{n-1} \overset{\alpha_{n-1}}{\longrightarrow} G_n \overset{\alpha_n}{\longrightarrow} G_{n+1} \overset{\alpha_{n+1}}{\longrightarrow} G_{n+2} \longrightarrow \cdots$$

we say that $(**)$ is an exact sequence if $G_{i-1} \overset{\alpha_{i-1}}{\longrightarrow} G_i \overset{\alpha_i}{\longrightarrow} G_{i+1}$ is an exact sequence for every i.

We denote by 1 the trivial group $\{1\}$. Notice that for every group G there exists a unique homomorphism $1 \to G$ and a unique homomorphism $G \to 1$.

1. Prove that for any group homomorphism $f : G \to H$ one has:
   - $1 \to G \overset{f}{\to} H$ is an exact sequence if and only if f is injective;
   - $G \overset{f}{\to} H \to 1$ is an exact sequence if and only if f is surjective.
2. We call a short exact sequence any exact sequence of groups of the form

$$1 \to H \to G \to K \to 1.$$

   Show that given the exact sequence above, there exists a subgroup $H' \trianglelefteq G$ such that $H \cong H'$ and $K \cong G/H'$.

Solution:

See next page!

1. We have that $1 \to G \xrightarrow{f} H$ is an exact sequence if and only if $\ker(f) = \mathrm{Im}(1 \to G) = 0$, if and only if f is injective. Moreover, $G \xrightarrow{f} H \to 1$ is an exact sequence if and only if $\mathrm{Im}(f) = \ker(H \to 1) = H$, if and only if f is surjective.
2. Let $\alpha : H \to G$ and $\beta : G \to K$ be the given maps. Call $H' := \alpha(H)$ via the first map. Being α injective by previous point, we have that the map $H \to H'$ sending $h \mapsto \alpha(h)$ is an isomorphism $H \cong H'$. Using exactness at G, we have $H' = \ker(\beta)$. Then applying First Isomorphism Theorem to the map β, which is surjective by previous point, we obtain $K \cong G/\ker(\beta) \cong G/H'$ and we are done.