Problem 1 All finite groups of up to 5 elements

Find all finite groups up to order 5 by using results of the last TD or by constructing all valid Cayley tables of up to 5 elements (each element has to appear exactly once in each row and once in each column). Show that the groups are Abelian and identify the different groups by isomorphisms to (products of) the cyclic groups $\mathbb{Z}/n\mathbb{Z}$.

Solution to Problem 1:

We know that all groups of prime order $|G| = p$ are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. These are cyclic and therefore generated by a single element g. This answers the question for $n = 1, 2, 3, 5$. E.g. the (only) finite group of 5 elements is $G_5 = \{e, g, g^2, g^3, g^4\}$ with $g^5 = e$.

For $n = 4$ there are four possible valid Cayley tables (do explicitly case-by-case). Then, notice that three of them are isomorphic to each other (up to relabeling), while another is apparently different. First look at $\mathbb{Z}/4\mathbb{Z}$ and show that each of the three identical ones can be mapped to it by an isomorphism. Finally consider $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with elements $\{(0,0), (1,0), (0,1), (1,1)\}$ and composition rule $(a_1, b_1)+(a_2, b_2) = (a_1+a_2 \mod 2, b_1+b_2 \mod 2)$ and show that it is isomorphic to the fourth possible group of order 4. It is easy to see that no isomorphism between $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ can be constructed: Group homomorphisms must conserve the property that an element is self-inverse. Since $\mathbb{Z}/4\mathbb{Z}$ has only a single self-inverse element that is not identity (namely 2) but in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ all elements are self-inverse, the groups are not isomorphic.

Finally note that these groups are Abelian they since they are cyclic or since their Cayley tables are symmetric under reflection on the main diagonal.

Problem 2 Union of groups

Let G_1 and G_2 be two subgroups of G. In the lecture you saw that the intersection of two subgroups always defines a group. When does the union $G_1 \cup G_2$ give rise to a group?

Solution to Problem 2:

We show that $G_1 \cup G_2$ is a group if and only if either $G_1 \leq G_2$ or $G_2 \leq G_1$ ($H \leq G$ is usually used to denote that H is a subgroup of G, while $\subseteq$ mearly means subset) . If $G_1 \leq G_2$ then $G_1 \cup G_2 = G_2$ and $(G_2, \cdot)$ is a group. Similarly for $G_2 \leq G_1$.

To show the converse, we assume that $G_1 \cup G_2$ is a group and pick as the first option $g_1 \in G_1$ completely free and $g_2 \in G_2$ such that $g_2 \notin G_1$. If this is not possible we pick instead as the second option $g_2 \in G_2$ unconstrained and $g_1 \in G_1$ such that $g_1 \notin G_2$ (if this is also not possible then $G_1 = G_2$). The group axiom ensures that $g_1 g_2 \in G_1 \cup G_2$. Hence,

$$g_1 g_2 = g, \tag{1}$$

where $g \in G_1$ or $g \in G_2$. Having $g \in G_1$ implies $g_2 = g_1^{-1} g \in G_1$ which contradicts the first option. Therefore we have $g \in G_2$ which implies $g_1 = g g^{-1} \in G_2$. Since g_1 was unconstrained we showed that $G_1 \leq G_2$. If we had to pick g_1 and g_2 according to the second option, then it follows analogously that $G_2 \leq G_1$.

Problem 3 Quotient groups

1. Remember that the set of left costs G/H only forms a group, called quotient group, if $H \triangleleft G$, i.e. if H is a normal subgroup of G. Given a subgroup of this quotient

group $A \leq G/H$, show that we can reduce G to a subgroup $G' \leq G$ with $H \triangleleft G'$ such that A can be also written as a quotient group $A = G'/H$.

2. Let $\varphi : G \to G'$ be a group homomorphism. Show that

$$\mathrm{Im}(\varphi) \simeq G/\mathrm{Ker}(\varphi). \tag{2}$$

3. Show that

$$G/Z(G) \simeq \mathrm{Inn(G)}, \tag{3}$$

where Inn(G) is the group of inner automorphisms of G. An inner automorphism is defined as

$$\varphi_g : G \to G \tag{4}$$
$$h \mapsto \varphi_g(h) = g \cdot h \cdot g^{-1}. \tag{5}$$

Solution to Problem 3:

1. We denote cosets of H in their usual way as $[g] = gH = \{gh \mid h \in H\}$. $G' = \{g \in G \mid [g] \in A\}$ is a subgroup of G since A is a group. Moreover, $H = [e] \in A$ and therefore $H \leq G'$. Since $H \triangleleft G$ it is also a normal subgroup of G' and we have $H \triangleleft G' \leq G$. Let us now construct the quotient group $G'/H = \{[g'] \mid g' \in G'\}$. By definition of G', we find $G'/H = A$.

2. First of all this quotient group exists since $\mathrm{Ker}(\varphi) \triangleleft G$. This can be checked quickly: The properties of group homomorphisms ensure that $e \in \mathrm{Ker}(\varphi)$ and for $g_1, g_2 \in \mathrm{Ker}(\varphi)$, $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = e$, so $g_1 \cdot g_2 \in \mathrm{Ker}(\varphi)$ and $\mathrm{Ker}(\varphi) \leq G$. Moreover, for $h \in \mathrm{Ker}(\varphi)$ and $g \in G$: $\varphi(g \cdot h \cdot g^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = e$ and $g \cdot h \cdot g^{-1} \in \mathrm{Ker}(\varphi)$, since $\varphi(h) = e$, ensuring that $\mathrm{Ker}(\varphi) \triangleleft G$.

   We now define the map

$$f : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi) \tag{6}$$
$$[g] \mapsto \varphi(g). \tag{7}$$

   Whenever we define a map on a quotient set we first have to make sure that it is well defined, i.e., its definition must not depend on the choice of the representative. Assume that $[g_1] = [g_2]$, then $\exists h \in \mathrm{Ker}(\varphi) : \; g_1 = g_2 \cdot h$. This implies $\varphi(g_1) = \varphi(g_2 \cdot h) = \varphi(g_2) \cdot \varphi(h) = \varphi(g_2)$ and the map is well defined. To show that f is a group homomorphism, consider $f([g_1] \cdot [g_2]) = f([g_1 \cdot g_2]) = \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = f([g_1]) \cdot f([g_2])$. f is clearly surjective and to show injectivity we assume $f([g_1]) = f([g_2])$, i.e., $\varphi(g_1) = \varphi(g_2)$. We obtain $e = \varphi(g_1)^{-1} \cdot \varphi(g_2) = \varphi(g_1^{-1} \cdot g_2)$ and therefore $g_1^{-1} \cdot g_2 \in \mathrm{Ker}(\varphi)$ which is the definition of $[g_1] = [g_2]$. In conclusion, f is a group isomorphism.

3. We define the map

$$\varphi : G \to \mathrm{Inn}(G) \tag{8}$$
$$g \mapsto \varphi_g. \tag{9}$$

We have $\mathrm{Im}(\varphi) = \mathrm{Inn}(G)$. Notice that there are less elements in $\mathrm{Inn}(G)$ than there are in G since some elements in G may give rise to the same map. Indeed these elements are from the center of the group. Let us analyze the kernel of φ:

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{g \in G \mid \varphi_g = \mathrm{id}\} && (10)\\ &= \{g \in G \mid \varphi_g(h) = h\} && (11)\\ &= \{g \in G \mid ghg^{-1} = h\} && (12)\\ &= \{g \in G \mid gh = hg\} && (13)\\ &= Z(G). && (14)\end{aligned}$$

The result now follows from

$$G/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi). \quad (15)$$

Bonus question: When is $\mathrm{Inn}(G)$ *trivial? Answer: If and only if* G *is abelian.*

Problem 4 Harder questions about normal subgroups

1. Is the relation $\triangleleft$ (i.e. the property of being a normal subgroup) transitive? In other words, is it true that if H, F and G are groups such that $H \triangleleft F \triangleleft G$, then $H \triangleleft G$?

2. Let G be a finite group, and H be a subgroup of G of prime index p. Show that if no prime smaller than p divides $|G|$, then H is a normal subgroup.

Solution to Problem 4:

1. Since the order of a subgroup divides the order of the group, we have $|H|$ divides $|F|$ divides $|G|$. Furthermore we need $|H| \geq 2$ (otherwise it is just the identity which is always a normal subgroup), so the minimal order of $|G|$ that could serve as a counterexample is 8.

   There is indeed such a group: The dihedral group D_4, corresponding to the symmetries of the 4-sided regular polygon (i.e. a square in this case). The group is generated by rotations r of $\pi/2$ and reflections s by an arbitrarily chosen symmetry axis of the square (take $s = f_k$ for some arbitrary k to agree with the notation of the lecture notes), together with the relations $r^4 = e$, $s^2 = e$ and $rsr = s$ (you can verify these by applying them explicitly to a square). Thus the groups consists of the 8 elements

   $$G = D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}. \quad (16)$$

   It has the normal subgroup $F = \{e, r^2, s, r^2s\}$ (check it!) which itself has a normal subgroup $H = \{e, s\}$. But H is not a normal subgroup of G because for example for $g = r \in G$ (then $g^{-1} = r^3$) and $s \in H$, we have $rsr^3 = r^2s$ (by using the relation $rsr = s$ multiple times) and $r^2s \notin H$.

2. Let $X = \{gH | g \in G\}$. By definition of the index, the cardinality of X is the index of the subgroup H in G, so $|X| = p$. Consider the map

   $$\begin{array}{rccc}\phi: & G & \to & \mathrm{Bij}(X) \\ & g & \mapsto & \left(\begin{array}{c} X \to X \\ g'H \mapsto gg'H \end{array}\right).\end{array}$$

This map is a group morphism, as for all $g_1, g_2, g_3 \in G$ one has

$$(\phi(g_1 g_2))(g_3 H) = g_1 g_2 g_3 H = (\phi(g_1) \circ \phi(g_2))(g_3 H)\,.$$

Let K be the kernel of ϕ. Being the kernel of a group morphism, K is a normal subgroup of G. We now prove the three following properties:

- $K \subset H$.
  Indeed, if $k \in K$ then $\phi(k) = \mathrm{id}_X$, so for all $g \in G$, $kgH = gH$. In particular for $g = e_G$ this gives $kH = H$, and therefore $k \in H$.
- The group G/K has index p.
  Indeed, the order of the group G/K is $|G|/|K|$, which is a divisor of $|G|$. Therefore, because of the assumption, the prime number decomposition of $|G/K|$ contains only primes which are $\geq p$. On the other hand, by the isomorphism theorem, G/K is isomorphic to the image of ϕ, which is a subgroup of $\mathrm{Bij}(X) \cong S_p$. So its order divides the order of S_p which is $p!$. Therefore the prime number decomposition of $|G/K|$ contains only primes which are $\leq p$, and p can appear with multiplicity at most one. This proves the claim.

From this we conclude that $K = H$, and therefore H is normal.