Problem 1 Cayley tables

The composition law of finite groups $\mathcal{G} = \{g_1, \ldots, g_N\}$ can be described by Cayley tables of the form:

	g_1	$\cdots$	g_i	$\cdots$	g_N
g_1					
$\vdots$			$\vdots$		
g_j		$\cdots$	$g_j \cdot g_i$	$\cdots$	
$\vdots$			$\vdots$		
g_N					

1. Show that each element of $\mathcal{G}$ appears exactly once in each row and each column in the Cayley table.
2. Prove Cayley's theorem: Each group of N elements is isomorphic to a subgroup of the symmetric group S_N (i.e., the set of all permutations of N elements).

Solution to Problem 1:

1. For each g_i, the map $\sigma^l_{g_i}(g) = g_i \cdot g$ is an automorphism of $\mathcal{G}$ (but not a group homomorphism). To show injectivity, assume that $\sigma^l_{g_i}(g) = \sigma^l_{g_i}(g')$, i.e., $g_i \cdot g = g_i \cdot g'$. It follows that $g = g'$. Since both sets have the same cardinality, the map must be bijective. We can also explicitly verify surjectivity by considering that for each g', we can take $g = g_i^{-1} \cdot g' \in \mathcal{G}$ and obtain $\sigma^l_{g_i}(g) = g'$. This shows that each row contains a permutation of the group elements, and the same follows for the columns using the automorphisms $\sigma^r_{g_i}(g) = g \cdot g_i$.
2. Consider the map $g \mapsto \sigma^l_g$. We have seen that σ^l_g permutes the elements of $\mathcal{G}$ and can therefore be interpreted as a permutation $\sigma \in S_N$ of $\mathcal{G}$, which is a set of $|\mathcal{G}| = N$ elements. This map $\sigma^l : \mathcal{G} \to S_N$ is not surjective (for $N > 2$) since $|S_N| = N!$, but it is injective: $\sigma^l_g = \sigma^l_{g'}$ means that for all $g'' \in \mathcal{G} : g \cdot g'' = g' \cdot g''$, implying $g = g'$. Moreover, σ is a group homomorphism: $\forall g \in \mathcal{G}$ holds: $(\sigma^l_{g_1} \cdot \sigma^l_{g_2})(g) = g_1 \cdot g_2 \cdot g = (\sigma^l_{g_1 \cdot g_2})(g)$. Hence, σ^l is a group isomorphism between $\mathcal{G}$ and $\mathrm{Im}(\sigma^l)$, which is a subgroup of S_N according to Corollary 2.5 in the script.

Problem 2 The group D_3

The group D_3 describes all symmetries (rotations and mirror operations) of an equilateral triangle.

1. Construct the Cayley table of D_3. Is the group Abelian?
2. Find all subgroups of D_3. Whenever possible, construct the corresponding quotient group and its Cayley table. Find the left- and right cosets of some non-normal subgroup.

Solution to Problem 2:

1. The elements of D_3 are given by identity e, rotation r around 120°, r^2 and the three reflections $\{f_1, f_2, f_3\}$ leaving one of the corners unchanged. We use the rules derived in the previous exercise to construct the Cayley table as far as possible. In

the upper diagonal block, we recognize the cyclic subgroup of rotations $\{e, r, r^2\}$. We only need to explicitly determine two combinations to fully determine the off-diagonal 3×3 blocks, e.g., $r \cdot f_1 = f_3$ and $f_1 \cdot r = f_2$. The remaining block on the diagonal is determined from, e.g., $f_2 \cdot f_1 = r^2$. We find

	e	r	r^2	f_1	f_2	f_3
e	e	r	r^2	f_1	f_2	f_3
r	r	r^2	e	f_3	f_1	f_2
r^2	r^2	e	r	f_2	f_3	f_1
f_1	f_1	f_2	f_3	e	r	r^2
f_2	f_2	f_3	f_1	r^2	e	r
f_3	f_3	f_1	f_2	r	r^2	e

.

The group is not Abelian as is reflected by the Cayley table being not symmetric with respect to the diagonal. Note that, generally, the identity must be found on the diagonal or symmetrically around the diagonal since if h is the inverse of g we have $e = g \cdot h = h \cdot g$.

2. From the Cayley table we identify three subgroups, $C_3 = \{e, r, r^2\}$ and the groups $\mathcal{H}_i = \{e, f_i\}$. Since $r f_i r^{-1} = f_j$ (as can be seen for some example from the table) the $\mathcal{H}_i$ are not normal. Left- and right-cosets can be explicitly constructed, e.g., $\mathcal{H}_1 = \{e, f_1\}$, $r\mathcal{H}_1 = \{r, f_3\}$, $r^2\mathcal{H}_1 = \{r^2, f_2\}$ whereas $\mathcal{H}_1 r = \{r, f_2\}$ and $\mathcal{H}_1 r^2 = \{r^2, r_3\}$. These can be interpreted as the $\mathcal{H}_1$-orbits of the left/right-regular group action onto itself, which yields a partition of D_3 (but not a quotient group, i.e., the orbits do not behave like elements of a group, since $\mathcal{H}_1$ is not normal). Since $f_i r^k f_i^{-1} = f_i r^k f_i = f_j f_i = r^{k'} \in C_3$, the subgroup C_3 is normal. The quotient group D_3/C_3 has two elements (see also Lagrange's theorem below) with $C_3 = [e] \in D_3/C_3$. It is apparent from the Cayley table that multiplication of C_3 with any f_i yields the set $[f] = \{f_1, f_2, f_3\}$. The group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and its Cayley table can be derived from the one of D_3 by identifying the 3×3 blocks with the elements of the quotient group. *Interesting to note*: Up to isomorphism, the only groups of order 6 are D_3 and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$.

Problem 3 Lagrange's theorem

Show that for a finite group $\mathcal{G}$ with subgroup $\mathcal{H} \leq \mathcal{G}$, the order $|\mathcal{H}|$ divides $|\mathcal{G}|$.

Solution to Problem 3:

Recall that the (left-)cosets of $\mathcal{H}$ define a partition of $\mathcal{G}$, leading to $|\mathcal{G}| = \sum_k |g_k\mathcal{H}|$. Moreover, each coset is a translated copy of $\mathcal{H}$, and therefore $|g_k\mathcal{H}| = |\mathcal{H}|$. Let k be the number of cosets, then we obtain the result $|\mathcal{G}| = k|\mathcal{H}|$ and hence $|\mathcal{H}|$ divides $|\mathcal{G}|$.

Problem 4 Modular arithmetics

1. Construct the quotient groups of $(\mathbb{Z}, +)$.
2. Show that for any $g \in \mathcal{G}$, where $\mathcal{G}$ is a finite group, $P_g = \{k \in \mathbb{Z} | g^k = e\}$ can be written as $|g|\mathbb{Z}$. The number $|g|$ is called the order of g.
3. Show that $|g|$ divides $|\mathcal{G}|$.
4. Show that every group $\mathcal{G}$ whose order $|\mathcal{G}| = p$ is prime is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Solution to Problem 4:

1. All subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ (Theorem 2.1 in the script). They are normal because of the commutativity of the addition. We construct the corresponding quotient groups $\mathbb{Z}/n\mathbb{Z}$ by finding the cosets. The subgroup itself acts as the identity element $n\mathbb{Z} = [0] \in \mathbb{Z}/n\mathbb{Z}$ with $n\mathbb{Z} = \{k \in \mathbb{Z} | k \mod n = 0\}$. To identify the cosets of $n\mathbb{Z}$, we consider without restriction $n > 0$. Any $m \in \mathbb{Z}$ with $0 < m < n$ is not an element of $n\mathbb{Z}$ and we obtain the coset $[m] = n\mathbb{Z} + m = \{k \in \mathbb{Z} | k \mod n = m\}$. We obtain the quotient group $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$. This describes modular arithmetics, i.e., addition modulo n.

2. The group homomorphism $f : \mathbb{Z} \to \mathcal{G}$ defined as $f(k) = g^k$ leads to $P_g = \mathrm{Ker}(f)$. From $\mathrm{Im}(f) \simeq \mathbb{Z}/\mathrm{Ker}(f)$, we conclude that the kernel cannot be trivial since otherwise $\mathrm{Im}(f) \simeq \mathbb{Z}/\{0\} = \mathbb{Z}$, which is an infinite set, whereas the codomain of f is the finite set $\mathcal{G}$. Since $\mathrm{Ker}(f)$ is a subgroup of $\mathbb{Z}$, we conclude that there exists a $|g|$ such that $P_g = |g|\mathbb{Z}$. For every $g \in \mathcal{G}$ in a finite group there exists a $k \in \mathbb{Z}$, such that $g^k = e$: Since there are only a finite set of elements in $\mathcal{G}$, there exist distinct $k_1, k_2 \in \mathbb{Z}$ such that $g^{k_1} = g^{k_2}$, i.e., $g^{k_1 - k_2} = e$.

3. The subgroup $\langle g \rangle = \{g^k | k \in \mathbb{Z}\} \leq \mathcal{G}$ contains exactly $|g|$ elements. Lagrange's theorem ensures that $|g|$ divides $|\mathcal{G}|$.

4. From Lagrange's theorem we know that any subgroup of $\mathcal{G}$ has either 1 or p elements. For $g_0 \neq e$, the subgroup $\langle g_0 \rangle$ contains at least the two elements e and g_0 and thus must have p elements. This means that $\langle g_0 \rangle = \mathcal{G}$. Consequently, for any $g \in \mathcal{G}$, there exists a $k \in \mathbb{Z}$ such that $g = g_0^k$. We use this to define $f : \mathcal{G} \to \mathbb{Z}/p\mathbb{Z}$ as $f(g) = [k]$. This definition is indeed independent of the specific k since if $g^k = g^{k'}$ then $g^{k-k'} = e$ and $k - k' \in P_g = |g|\mathbb{Z}$. Hence, there exists $m \in \mathbb{Z}$ such that $k - k' = |g|m$ with $|g| = p$, i.e., $[k] = [k']$.

   It remains to be shown that f is a group isomorphism. For any $g, g' \in \mathcal{G}$, we can find $k, k' \in \mathbb{Z}$ such that $g = g_0^k$ and $g' = g_0^{k'}$ and $g \cdot g' = g_0^{k+k'}$. Hence $f(g \cdot g') = [k + k'] = [k] + [k'] = f(g) + f(g')$. We know that $f(\mathcal{G})$ must be a subgroup of $\mathbb{Z}/p\mathbb{Z}$ and therefore have order 1 or p. If the order was 1 that would imply $\mathcal{G} = \{e\}$ in contradiction to the assumption that $|\mathcal{G}| = p$ is a prime. We thus have $f(\mathcal{G}) = \mathbb{Z}/p\mathbb{Z}$, i.e., f is surjective. Since the sets $\mathcal{G}$ and $\mathbb{Z}/p\mathbb{Z}$ have the same cardinality, the map f is a bijection.