1) Compute the Cayley tables for the additive group $\mathbb{Z}_7$ and for the multiplicative group $\mathbb{Z}_7^*$ of non-zero elements in $\mathbb{Z}_7$.

2) Let G be a group written additively. Recall that the order of an element a is the minimal natural number n such that $na = 0$. If such n does not exits then one says that the order of a is infinity.

i) Find the order of the following elements $2, 3, 5, 6 \in \mathbb{Z}_{12}$.

ii) If G is a group written multiplicatively, the order of an element a is the minimal natural number n such that $a^n = 1$. Find the order of the elements $2, \frac{1}{2}, -1, i \in \mathbf{C}^*$, where $\mathbf{C}^*$ is the multiplicative group of non-zero complex numbers.

iii) Find the order of the following elements $2, 3, 5, 6 \in \mathbb{Z}_7^*$, where Z_7^* is the multiplicative group of non-zero elements in $\mathbb{Z}_7$.

3) i) Let G be a group written additively. An element a of a group G is called a generator if any element $x \in G$ has the form $x = na$ for some integer n. For example -1 and 1 are generators of $\mathbb{Z}$, while $\mathbf{Q}$ has no generators at all. Find all generators of the group $\mathbb{Z}_{12}$.

ii) In multiplicative notation, an element a of a group G is called a generator if any element of G can be written as a power of a. Carl Friedrich Gauss proved that for any prime p the group $\mathbb{Z}_p^*$ has a generator. Verify this statement for all primes ≤ 17 giving explicitly a generator of the group $\mathbb{Z}_p^*$ in each case.

Remark. Can you see any regularity among these generators for different primes? Probably not. A conjecture of Artin (which is still open) claims that if a is an integer which is not a perfect square there are infinitely many primes p for which a is a generator in $\mathbb{Z}_p^*$.

4) i) Let G be a group written multiplicatively. For any element $a \in G$, consider the map $f_a : G \to G$ given by $f_a(x) = ax$. Prove that f_a is always a bijection.

ii) Let $G = \mathbb{Z}_p^*$ be the multiplicative group of the non-zero elements in the field $\mathbb{Z}_p$. For any integer a, which is not divisible by p, the bijection $f_{\bar{a}} : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ can be considered as a permutation and hence as an element of S_p. The sign of this permutation is denoted by $\left(\frac{a}{p}\right)$ and is called Legendre symbol. Here $\bar{a}$ denotes the class of a modulo p. For example if $p = 5$ and $a = 23$, then $\bar{a} = 3$ and the corresponding permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1423)$$

This is because $f_3(x) = 3x$, so $f_3(1) = 3, f_3(2) = 6 = 1$ in $\mathbb{Z}_5$ etc. Hence $\left(\frac{23}{5}\right) = -1$. One of the most famous results of Carl Friedrich Gauss claims that for any odd primes p and q one has

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Verify the theorem for $p = 7$ and $q = 11$.