1. *Let H be a set of at least two elements. Show that the set $P(H)$ of all the subsets of H does not form a group with the operation $\cap$ or $\cup$ but it is a group with the symmetric difference $A \triangle B := (A \cup B) \setminus (A \cap B)$.*

Solution: Though the operations $\cap$ and $\cup$ are associative, and there is a neutral element for both (H for $\cap$ and $\emptyset$ for $\cup$), the subsets $A \neq H$ have no inverses for $\cap$ and the subsets $A \neq \emptyset$ have no inverses for $\cup$.
The symmetric difference is a binary operation defined on $P(H)$, which can also be written as $A \triangle B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$. To prove the associativity we rewrite first a complement of $A \triangle B$:
$\overline{A \triangle B} = \overline{A \cap \overline{B}} \cap \overline{\overline{A} \cap B} = (\overline{A} \cup B) \cap (A \cup \overline{B}) = (\overline{A} \cap A) \cup (\overline{A} \cap \overline{B}) \cup (B \cap A) \cup (B \cap \overline{B}) = \emptyset \cup (\overline{A} \cap \overline{B}) \cup (A \cap B) \cup \emptyset = (\overline{A} \cap \overline{B}) \cup (A \cap B)$
The operation$\triangle$ is associative: $(A \triangle B) \triangle C = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)$, so $(A \triangle B) \triangle C$ consists of those elements that are contained either exactly in one of A, B, C or in all three of them. Clearly, we get the same when we expand $A \triangle (B \triangle C) = (B \triangle C) \triangle A$ (here we also use the fact that $\triangle$ is obviously a symmetric relation).
There is a neutral element, the empty set: $A \triangle \emptyset = \emptyset \triangle A = A$ for every A,
and every element $A \in P(H)$ is the inverse of itself: $A \triangle A = \emptyset$.
So $(P(H), \triangle)$ is a group, moreover, it is an abelian group.

2. *Do the following sets form a group with the addition or multiplication of matrices as the operation?*
a) $n \times n$ *real matrices with determinant* 1*;*
b) $n \times n$ *real matrices with positive determinant;*
c) $n \times n$ *matrices over* $\mathbb{Z}$*;*
d) $n \times n$ *matrices over* $\mathbb{Z}$ *with nonzero determinant;*
e) $n \times n$ *matrices over* $\mathbb{Z}$ *with determinant* 1*;*
f) $n \times n$ *real upper triangular matrices.*

Solution: Note that all six sets are subsets of the matrix ring $\mathbb{R}^{n\times n}$, where both the addition and the multiplication operation are associative. Furthermore, each set contains the identity matrix I, which is the neutral element for the multiplication, and c) and f) contain the zero matrix, which is the neutral element of $\mathbb{R}^{n\times n}$ for addition, while the other four sets are not even closed under addition (the determinant of the matrices I_n and $\operatorname{diag}(-1, -1, 1, \ldots, 1)$ is 1 but their sum has determinant 0). So the only thing to check in the $6 + 2$ remaining cases is that they are closed under multiplication/addition, and see whether they are all invertible in $\mathbb{R}^{n\times n}$, and whether the inverses are also in the given subset. Let's start with the additive structure.

c),f) They are obviously closed under addition and the additive inverse of any element, that is, $-A$ for A also has integer elements/upper triangular form if A has. So c) and f) are additive groups.

Now for the multiplication:

a),b) The product rule $|AB| = |A| \cdot |B|$ shows that a) and b) are closed under multiplication. Furthermore, since the elements have nonzero determinants by assumption, every element A has an inverse A^{-1} in $\mathbb{R}^{n\times n}$. Since $|A^{-1}| = |A|^{-1}$ is 1 if $|A| = 1$, and positive if $|A| > 0$, the inverse is also in the subset. Thus a) and b) are multiplicative groups.

c),f) Though these are closed under multiplication, they contain non-invertible matrices, e.g. the zero matrix, so they cannot be groups with multiplication as the operation.

d) The product of matrices over $\mathbb{Z}$ also has integer elements, and the product rule of determinants implies that the product of the elements also has a nonzero determinant, so this set is closed under multiplication, and its elements are invertible in $\mathbb{R}^{n\times n}$. However, their inverses (note that the inverse is unique, so it must be the same in the subset) may not have integer elements, e.g. $(2I)^{-1} \notin \mathbb{Z}^{n\times n}$.

e) This is closed under multiplication, and its elements have nonzero determinants, so they are invertible in $\mathbb{R}^{n\times n}$. Furthermore, the inverses of its elements are also in this subset: we can use the formula $A^{-1} = \frac{1}{|A|} \operatorname{adj} A$, where the elements $(\operatorname{adj} A)_{ij} = A_{ji}$ of $\operatorname{adj} A$ are subdeterminants of A, so they are also integers. So e) is a multiplicative group.

3. *Let G be a group and suppose that $x^2 = 1$ for every $x \in G$. Prove that G is commutative.*

Solution: Let $a, b \in G$ then by the assumption $1 = (ab)^2 = abab$. Multiply this equation by a from the left and b from the right. Also using the associativity, we get $ab = a^2bab^2 = 1ba1 = ba$. Since this is true for any a, b the group G is commutative.

4. *What are the possible orders of the elements in the following groups?*

a) $(\mathbb{R} \setminus \{0\}, \cdot)$;
b) $(\mathbb{R}, +)$;
c) $(\mathbb{C} \setminus \{0\}, \cdot)$;
d) $GL_3(\mathbb{R})$.

Solution: Note that each group has elements of infinite order, say, 2 in a), b), c) and $2I$ in d) are such elements (the powers in the multiplicative cases are 2^n or 2^nI, and in the additive case $2n$, wich cannot be 1, I or 0, respectively, if n is a positive integer. So the question is what the possible finite orders are.

a) If $a \in \mathbb{R} \setminus \{0\}$, and $n > 0$ integer then $a^n = 1$ would imply that $|a| = 1$, that is, $a = \pm 1$. If $a = 1$ then $o(a) = 1$, if $a = -1$ then $a^1 = -1 \neq 1$, $a^2 = 1$, so $o(-1) = 2$. So the possible orders are $1, 2, \infty$.

b) If $a \neq 0$ and n is a positive integer then $na \neq 0$, so in this group 0 is the only element of finite order, and its order is 1. Thus in this group the orders of the elements are $1, \infty$.

c) Here any finite order is possible: the order of a primitve n'th root of unity, say that of $\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ is n. Thus in this group every order $(1, 2, 3, \ldots, \infty)$ is possible.

d) We have seen in problem 1/4.c) that $GL_2(\mathbb{R})$ contains elements of every order. On the other hand, for a 2×2 matrix A, the block diagonal matrix $B = \operatorname{diag}(A, 1)$ has powers $B^k = \operatorname{diag}(A^k, 1)$, so the order of B is the same as the order of A. It implies that $GL_3(\mathbb{R})$ also has elements of every order.

5. *Find all the elements of finite order in the group of upper triangular 2×2 invertible matrices over $\mathbb{R}$. Do they form a subgroup?*

Solution: Since in the product of two upper triangular matrices the diagonal elements are the products of the corresponding diagonal elements of the two matrices, the power of such a real matrix cannot be I unless all the diagonal elements are 1 or -1. For $A = \begin{bmatrix} 1 & c \\ 0 & -1 \end{bmatrix}$, $A^2 = I$, so $o(A) = 2$, and the order of $-A = \begin{bmatrix} -1 & -c \\ 0 & 1 \end{bmatrix}$ is also 2. On the other hand, for $A = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}$, we have $A^n = \begin{bmatrix} 1 & nc \\ 0 & 1 \end{bmatrix}$, so $o(A) = \infty$ unless $c = 0$, and similarly, for $-A$. So of the second type only I and $-I$ are of finite order (the orders are 1 and 2, respectively). The elements of finite order do not form a subgroup, e.g. for

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}, \qquad AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$o(A) = o(B) = 2$ but $o(AB) = \infty$.

6. *List all possible cycle structures for the elements of S_4. What are the orders of these elements, and how many elements are there for each cycle structure (equivalently, for each partition of 4)?*

Solution: The cycle structures (which tell us how many cycles for each cycle length appear in the dcd) can be described by partitions of n in S_n, that is, the possible sums of positive integers which give n. To make it unique, we only take partitions where the summands are in decreasing order. For $n = 4$ this gives 4, $3+1$, $2+2$, $2+1+1$ and $1+1+1+1$, giving the cycle structures (....), (...)(.) = (...), (..)(..), (..)(.)(.) = (..) and (.)(.)(.)(.) = 1 (the dots represent the numbers in the cycle, and 1-cycles, that is, fixed points can be omitted in the dcd).

partition	*cycle str.*	*#elements*	*order*
4	(....)	6	4
3 + 1	(...)	8	3
2 + 2	(..)(..)	3	2
2 + 1 + 1	(..)	6	2
1+1+1+1	1	1	1

For (....) the cycle contains all elements of the base set, and we may assume that it starts with 1. Then all the orderings of $2, 3, 4$ give different permutations, so there are $3! = 6$ such elements. For (...), we can choose $\binom{4}{3} = 4$ different ways which elements are in the cycle, and if we start the cycle with its smallest elements, there are 2 ways to continue, so altogether this gives $4 \cdot 2 = 8$ elements of cycle structure (...). For (..)(..), we can choose the first cycle in $\binom{4}{2} = 6$ ways (the order of the elements in a 2-cycle doesn't make a difference), the second is then determined, but we get every permutation twice because we can switch the two cycles, so this gives $6 \cdot 1 \cdot \frac{1}{2} = 3$ elements of form (..)(..). There are $\binom{4}{2} = 6$ of form (..), and 1 identity element.
The order in each case is the least common multiple of the cycle lengthes.

7. *Let $g = (1345)(236)(41)$ and $h = (145)(231)$ be two elements of S_6*
a) Give the disjoint cycle decomposition of g, h, and gh.
b) Calculate g^2, g^3 and h^{-1}. What is the order of g, h, gh and hg?

Solution: a) $g = (1623)(45)$, $h = (14523)$, $gh = (1623)(45)(14523) = (16342)$.

b) $g^2 = (12)(63)$, $g^3 = (3261)(45)$, $h^{-1} = (32541)$, $o(g) = \mathrm{lcm}(4, 2) = 4$, $o(h) = 5$, $o(gh) = 5$. Finally, $hg = (15362)$ gives $o(hg) = 5$. (Actually, $o(hg) = o(gh)$ is always true: $(gh)^n = 1 \Leftrightarrow h(gh)^n = h \Leftrightarrow (hg)^n h = h \Leftrightarrow (hg)^n = 1$.)

8. *a) What is the number of elements of order* 10 *and of order* 4 *in*S_{10}*?*
b) What is the maximum of the orders of the elements in S_8*?*

Solution: a) The order only depends on the cycle structure of the disjoint cycle decomposition, so we first want to find partitions of 10 with least common multiple 10 or 4.

We first count the elements of order 10. We need $10 = c_1 + \ldots + c_k$ $(c_1 \geq \cdots \geq c_k \geq 1)$ such that $\mathrm{lcm}(c_1, \ldots, c_k) = 10$. Each c_i must be a divisor of 10, on the other hand, there should exist i and j (possibly $i = j$) such that $5 \mid c_i$ and $2 \mid c_j$. If $c_i = 10$ then $i = k = 1$, that is, there is only a 10-cycle in the decomposition, and the order is, indeed, 10. If there is no 10-cycle then there must be a c_i with $5 \mid c_i \mid 10$ and a c_j with $2 \mid c_j \mid 10$ such that $c_i, c_j < 10$, so $c_i = 5$ and $c_j = 2$. The remaining 3 can only be partitioned as $2 + 1$ or $1 + 1 + 1$ so that the summands would divide 10, hence the possible partitions for order 10 are 10, 5+2+2+1 and 5+2+1+1+1. How many such permutations exist? The 10-cycle must contain all 10 elements, and we may assume that it starts with 1. So there are 9! options to finish it, and the permutations we get this way are all different. For the third partition, $5 + 2 + 1 + 1 + 1$ we first choose the 5 elements moved by the 5-cycle ($\binom{10}{5}$ ways), then these can form 4! different cycles. For each case, we can choose the elements in the 2-cycle in $\binom{5}{2}$ ways but there the order does not matter. So we have $\binom{10}{5} \cdot 4! \cdot \binom{5}{2}$ such elements. Finally, for the second partition $5 + 2 + 2 + 1$ there are $\binom{10}{5} \cdot 4! \cdot \binom{5}{2}\binom{3}{2}\frac{1}{2}$ choices (we had to divide by 2 in the end because we can swap the two 2-cycles and still get the same permutation. So there are

$$9! + \binom{10}{5} \cdot 4! \cdot \binom{5}{2} + \binom{10}{5} \cdot 4! \cdot \binom{5}{2}\binom{3}{2}\frac{1}{2} = 514080$$

elements of order 10 in S_{10}.

The cycle structure for order 4 can only have 4-, 2- and 1-cycles (the latter we usually omit), and at least one 4-cycle should be there. So the possible cycle structure should be (....)(....)(..), (....)(....), (....)(..)(..)(..), (....)(..)(..), (....)(..) and (....). The number of such permutations is

$$\binom{10}{4}3!\binom{6}{4}3! \cdot \frac{1}{2} + \binom{10}{4}3!\binom{6}{4}3! \cdot \frac{1}{2} + \binom{10}{4}3!\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{3!} +$$

$$\binom{10}{4}3!\binom{6}{2}\binom{4}{2}\frac{1}{2!} + \binom{10}{4}3!\binom{6}{2} + \binom{10}{4}3! = 209160.$$

Note that we always had to divide by the factorial of the number of k-cycles for any k because any permutation of those cycles gives the same element of the symmetric group.

Remark: We can also count the number of elements having a given cycle structure in a different way: if cycle lengthes in a cycle structure in S_n are $n_1 > \cdots > n_k$ (including the 1-cycles, so $n = x_1 n_1 + \ldots + x_k n_k$) and the number of n_i-cycles in the given structure is x_i for each i, then the number of such elements in S_n is $n!/(n_1^{x_1} \cdots n_k^{x_k} \cdot x_1! \cdots x_k!)$. We get this by observing that we can fill the cycles with elements in $n!$ different ways, but we have to divide $n!$ by the number of how many of these actually give the same permutation. Since an n_i-cycle can be rotated in n_i different ways, and for a given i, the n_i-cycles can be permuted among themselves in $x_i!$ ways, and still giving the same permutation written in the same cycle pattern, the number of equal permutations among the $n!$ is exactly $n_1^{x_1} \cdots n_k^{x_k} \cdot x_1! \cdots x_k!$. One can check that this formula gives the same result as the one we calculated earlier.

b) We want to find the maximum of $m = \operatorname{lcm}(c_1, \ldots, c_k)$ where $c_i \geq 2$ are integers and $c_1 + \ldots + c_k \leq 8$ (the other elements in the partition are 1's). We may assume that all c_i's are prime powers because if $c_i = ab$, where $\gcd(a, b) = 1$, then we can replace c_i with $c_i' = a$ and $c_i'' = b$ in the partition (note that $a + b \leq ab$), and still get the same least common multiple. We can also assume that these c_i's are powers of different primes, otherwise we may just keep the highest power and still have the same least common multiple.
If $7 \mid m$ then the partition can only be $7 + 1$, so $m = 7$.
Suppose 5 is the greatest prime divisor of m. Then the partition can be $5 + 3$ or $5 + 2$ or 5, giving $m = 15, 10, 5$. If 3 is the greatest prime divisor then the partition can be $3 + 4$, $3 + 2$ or 3, giving $m = 12, 6, 3$. Finally if the greatest prime divisor of m is 2, then the partition is 8, 4 or 2, giving $m = 8, 4, 2$. This shows that the maximal order is 15.

HW1. *Let I be the open interval $I = (-1, 1) = \{\, x \in \mathbb{R} \mid -1 < x < 1 \,\}$. and define $a * b = \dfrac{a+b}{1+ab}$. Show that $(I, *)$ is a group. (Do not forget to check that for $a, b \in I$, the number $a * b$ is also in I.*

HW2. *What is the number of elements of order 6 in S_7?*