1. *Determine the number of isometries (in other word, symmetries) for a*
a) square;
b) regular tetrahedron;
c) cube.
How many of these are reflections or rotations?

Solution: a) Clearly, the four reflections across the diagonals and the bisectors of the edges are isometries, and so are the four rotations around the center by $90°, 180°, 270°, 0°$ (we can count the identity map as a rotation by $0°$), so there are at least 8 isometries. To prove that there are no more, we notice that any isometry maps vertices to vertices, and actually the permutation of the vertices determines the isometry (the image of three non-collinear points determines the image of any point of the plane), so we only have to count how many permutions of the vertices can be realized by isometries. Note also that composition of isometries is also an isometry. Let us denote the vertices by $1, 2, 3, 4$, going around the square. The image $f(1)$ of 1 can be any of the vertices, using the approriate rotation. In all of these four cases the image $f(2)$ of 2 will be a neighbour of $f(1)$, which gives only 2 possibilities, then the image $f(4)$ of 4 (the other neighbour of $f(1)$), and the remaining vertex $f(3)$ are determined, so there are at most $4 \cdot 2 = 8$ options. So there are exactly 8 isometries, 4 of which are rotations and 4 are reflections.

b) Let's start now by calculating the exact number of isometries, which similarly to the case of the square, means counting how many permutations of the four vertices can be realized by isometries. Let the vertices be again $1, 2, 3, 4$. Vertex 1 can be mapped to any of the vertices, using a rotation about one of the lines connecting a vertex with the center of the opposite face. If the image $f(1)$ of 1 is given, then $f(2)$ can still be any of the other vertices: if at first we do not get the right one, then we can still apply a rotation about the line of symmetry through $f(1)$, thus the composition of the two rotations still maps 1 to $f(1)$ and 2 to the intended vertex. Let this (possibly a composite) map be g. Then the image $g(3)$ of 3 can be any of the remaining two vertices: if it is not what we want then we can compose g with a reflection across a plane through the edge $g(1)g(2)$ and the midpoint of the opposite edge. Finally, the image of 4 is just the remaining vertex. So there are exactly $4 \cdot 3 \cdot 2 \cdot 1 = 24$ possibilities. In fact, we got that all permutations of the vertices can be realized by isometries.

The rotations are the 8 rotations by $120°$ and $240°$ about the lines going through a vertex and the midpoint of the opposite face, the three rotations by $180°$ about the lines connecting the midpoints of two opposite edges (this is the transversal of the two lines), and the identity, altogether 12 rotations. The reflections are the ones across the planes containing one edge and the midpoint of the opposite edge. This means 6 reflections. What remains to show is that there are no more rotations or reflections. Since rotations are orientation preserving, and reflections (across planes or points) are orientation reversing, problem 2.a) implies that there cannot be more than 12 rotations, so we only have to show that there are no more reflections. Every isometry of the tetrahedron leaves the center fixed, and the reflection across the center does not map the tetrahedron into itself, so we are looking for planes of symmetries containing the center. It cannot contain all vertices, so there are at least two vertices which are images of each other, so the plain must be a perpendicular bisector of the connecting edge. These are exactly the six reflections we have found. Thus the remaing six isometries are neither rotations nor reflections.

c) Here we need to determine the possible permutations of the vertices $1, 2, 3, 4, 5, 6, 7, 8$ (the first four are the vertices of the base square, and $k + 4$ is above k) that can be realized by isometries. Actually, it is enough to give the image of 1 and its two neighbours $2, 4$, then the rest is determined. 1 can go to any of the vertices by one or two rotations about lines connecting the centers of opposite faces. Then 2 can go to any of the three edge-neighbours of $f(1)$: if we do not get the correct one at first then we apply a rotation about the main diagonal through $f(1)$. Finally, if $f(1)$ and $f(2)$ are fixed then the image of 3 can be any of the remaining neighbours of $f(1)$: if we want other than what we got then we apply a reflection across a plane connecting the edge $f(1)f(2)$ with the center of the cube (and the opposite parallel edge). So the number of possible permutations is $8 \cdot 3 \cdot 2 = 48$.

There are $3 \cdot 3 = 9$ rotations about lines connecting the centers of parallel faces (by $90°, 180°, 270°$), $4 \cdot 2 = 8$ rotations about the four main diagonals (by $120°, 240°$), 6 rotations about lines connecting opposite parallel edges (by $180°$), and the identity. Altogether 24 rotations. There is 1 reflection across the center of the cube, 3 reflections across bisecting planes parallel to some of the faces, and 6 reflections across planes containing two opposite parallel edges. Altogether 10 reflections.

Similarly to part b), we can see that all orientation preserving isometries are rotations (we have identified all 24 of them). The question is if there are any more plains of symmetries than the ones we listed. Again, such a plain must contain the center, and must be a bisector of a segment connecting two vertices. If these two are endpoints of an edge then the reflection is one of the 3 reflections across a plain parallel to some faces of the cube. If these are endpoints of a diagonal of a face then the reflection is one of the other 6 we have found. Finally, if the two points are endpoints of a main diagonal then the plain goes through the midpoints of the six edges not adjacent to any of the endpoints of this diagonal. But this reflection does not map the cube into itself (actually, we get the cube which is the original cube rotated around the main diagonal by $60°$ and reflected across the center). So the remaining 14 isometries are neither rotations nor reflections.

2. *a) Show that exactly as many of the isometries in problem 1 are orientation preserving as orientation reversing.*

b) Let $1, 2, 3, 4$ *denote the corners of the tetrahedron in problem 1.b), and* $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$ *be the permutation of the corners determining an isometry* f. *Show that* f *is neither a rotation nor a reflection. Try to obtain it as the composition (product) of two of those.*

Solution: a) Compositions of two orientation preserving or two orientation reversing maps are orientation preserving, a composition of an orientation preserving and an orientation reversing map in any order is orientation reversing. So if P is the set of orientation preserving isometries and R is the set of orientation reversing maps, and $R \neq \emptyset$ then composing the elements of P with a fixed element $r \in R$ is an injective map from P to R, so $|P| \leq |R|$, and conversely, composing the elements of R by r

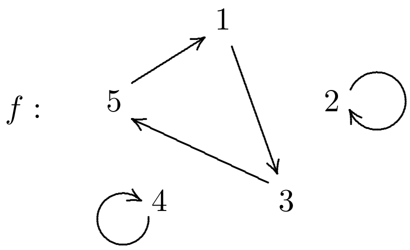
gives an injective map from R to P, so $|R| \leq |P|$. Thus $|P| = |R|$.
Note that rotations are always orientation preserving and reflections of the plane across lines, or reflections of the 3 dimensional space across planes or points are orientation reversing. (Reflection of the space across a straight line is actually a rotation by $180°$.) Also, that in the three cases of problem 1, the number of orientation preserving isometries must be half the number of all isometries: 4, 12 and 24, which is exactly the number of rotations. Actually, with a little linear algebra one can prove that any orientation preserving isometry of the plane or of the three dimensional space which has a fixed point must be a rotation about a point in the planar case, and about a line in the three dimensional space.

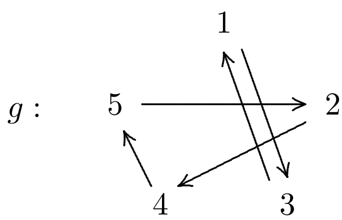
b) It follows from part a) that the tetrahedron has only 12 orientation preserving isometries, so there cannot be more rotations than those listed. However the rotations about the lines through a vertex leave that vertex fixed, so it cannot be f, and the order of the rotations by $180°$ is 2, that is, if we apply them twice, we get the identity, but $f \circ f$ takes 1 to 3. So f cannot be a rotation. The order of the reflections is also 2, so f cannot be a reflection, either.
We can find a rotation with the action $1 \mapsto 2 \mapsto 3 \mapsto 1$ and $4 \mapsto 4$. To get f, we have to compose it with a map that leaves 2 and 3 fixed, and switches 1 with 4. This is the reflection across the plain that contains the edge 23, and bisects the edge 14. So f is the composition of a rotation and a reflection.
Remark: The same is true for any permutation of $\{1, 2, 3, 4\}$ *that acts as a* 4*-cylce, and there are exactly* 6 *of those. This gives an alternative proof to the fact that of the* 12 *orientation reversing isometries only the six listed in the solution of problem* 1*.b) can be reflections of the tetrahedron.*

3. *Consider the following permutations (bijections) of the set* $\{1, 2, 3, 4, 5\}$ *(where each* i *is mapped to the element below).*

$$f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \qquad g : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Show the action of each permutation on an oriented graph with vertices $1, 2, 3, 4, 5$. *How many times do we need to apply the permutation to get the identity map* ($i \mapsto i\ \forall i$)*?*
Solution:





Since every vertex has one outgoing and one incoming edge, the graph falls apart into disjoint oriented cycles. The kth power of the permutation (that is, when we apply the permutation k times) sends every vertex to the kth element along its cycle. So the kth power is the identity if and only if k is divisible by the lengths of all of the cycles. The smallest of these numbers is the least common multiple of the cycle lengths, that is, the order of f is $\text{lcm}(3, 1, 1) = 3$, and the order of g is $\text{lcm}(3, 2) = 6$.

4. *Let $GL_n(K)$ (general linear group) denote the set of invertible $n \times n$ matrices over the field K. The order of a matrix A in this group is the smallest positive integer k such that $A^k = I$, where I denotes the identity matrix (the order is ∞ if such a k does not exist).*
a) What is the order of the following matrices?

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \in GL_5(\mathbb{R}), \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$$

$$C = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \in GL_2(\mathbb{Z}_3) \qquad D = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in GL_3(\mathbb{Z}_2)$$

b) What is the number of elements in the group $G = GL_2(\mathbb{Z}_3)$ and in $G = GL_3(\mathbb{Z}_2)$?
c) What are the possible orders of the elements of $GL_2(\mathbb{R})$?

Solution: a) A is a block diagonal matrix with diagonal blocks $A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$, $A^k = \operatorname{diag}(A_1^k, A_2^k) = I \Leftrightarrow A_1^k = I$ and $A_2^k = I$. By calculating the first few powers we see that $A_1^k = I \Leftrightarrow 2 \mid k$ and $A_2^k = I \Leftrightarrow 3 \mid k$, so the smallest positive k to make $A^k = I$ is 6.

Actually, A is a permutation matrix, that is, it acts as a permutation on the standard basis elements of $\mathbb{R}^5$, say, if we let it act on the column vectors from the left then the action is $\mathbf{e}_1 \mapsto \mathbf{e}_2 \mapsto \mathbf{e}_1$ and $\mathbf{e}_3 \mapsto \mathbf{e}_5 \mapsto \mathbf{e}_4 \mapsto \mathbf{e}_3$. The order of A must be the same as the order of that permutation, so we could calculate its order the same way as in problem 3.

We can show that $B^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ either by calculating a few powers, and then use induction, or by recognizing B as a Jordan block and using the power formula. This is never equal to I, so the order of B is ∞.

$C^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, $C^3 = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$, $C^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, so the order of C is 4. (The elements of C are supposed to be taken from $\mathbb{Z}_3$, so we have to do all calculations modulo 3.)

If we calculate the powers of D (over $\mathbb{Z}_2$!) then we see that $D^k \neq I$ for $k = 1, 2, \ldots, 6$ but $D^7 = I$, so the order of D is 7.

b) A square matrix is invertible if and only if its row vectors are independent. So let us count how many ways we can fill a matrix row by row if we are careful to make the rows independent. The 2-dimensional vector space $\mathbb{Z}_3^2 = \{(a, b) \mid a, b \in \mathbb{Z}_3\}$ has $3 \cdot 3 = 9$ elements. The first row in itself is independent if it is nonzero, so we have $9 - 1 = 8$ choices for the first row. Next we have to make sure that the second row does not depend on the first, that is, it is not a scalar multiple of the firs row (the possible scalars being $0, 1, 2$). This leaves us $9 - 3 = 6$ options for the second row in each case. This gives altogether $8 \cdot 6 = 48$ invertible matrices, so $|GL_2(\mathbb{Z}_3)| = 48$. As for $GL_3(\mathbb{Z}_2)$, we have to choose three rows which are independent in $\mathbb{Z}_2^3$. For this there are $(8-1)(8-2)(8-4) = 7 \cdot 6 \cdot 4 = 168$ options (when we choose the third row we have to avoid all possible linear combinations of the first two, and by their independency their $2 \cdot 2 = 4$ linear combinations all give different vectors). So $|GL_3(\mathbb{Z}_2)| = 168$.

Note that the order of $C \in GL_2(\mathbb{Z}_3)$ is a divisor of $|GL_2(\mathbb{Z}_3)| = 48$, and the order of $D \in GL_3(\mathbb{Z}_2)$ is a divisor of $|GL_3(\mathbb{Z}_2)| = 168$.

c) The 2×2 real matrices can be considered as linear transformations of the real plane. Among these the rotations by $\frac{2\pi}{n}$ have order n, so every order is possible in this group, too.

5*. *What are the possible orders of the elements of $GL_3(\mathbb{Z}_2)$? (Hint: The order of a matrix is k if and only if k is the smallest positive integer such that the minimal polinomial of the matrix divides $x^k - 1$.)*

Solution: The minimal polynomial of a 3×3 matrix has degree at most 3, and it should have a nonzero constant term if the matrix is invertible. Thus only options are the following: $x+1 = x-1$ (this belongs to the identity matrix), $x^2+1 = (x-1)^2$ (this can be the minimal polynomial of a Jordan matrix consisting of a 2×2 and a 1×1 Jordan block for eigenvalue 1). Then $x^2 + x + 1$ cannot be the minimal polynomial, since then the characteristic polynomial would be the product of this and a first degree polynomial (which could only be $x + 1$), so 1 would be an eigenvalue of the matrix, which is not a root of the minimal polynomial, and this we know to be impossible. Finally, all appropriate cubic polynomials ($x^3 + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$ and $x^3 + x^2 + x + 1$) are the minimal polynomials of their companion matrices. (In fact, D of problem 4 is the companion matrix of $x^3 + x + 1$, and we have seen that its order is 7.) $x + 1 = x - 1$, $x^2 + 1 = x^2 - 1$ and $x^3 + 1 = x^3 - 1$ shows that the matrices with minimal polynomials $x + 1$, $x^2 + 1$ and $x^3 + 1$ have orders 1, 2, and 3, respectively. The cubic polynomial $x^3 + x^2 + x + 1$ can easily be multiplied into $x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1)$, so the order of the corresponding matrices is 4. If we multiply $x^3 + x + 1$ by the listed linear, quadratic and cubic polynomials, including themselves, to find all appropriate multiples of degree ≤ 6, we do not get a polynomial $x^k - 1$ (and similarly for $x^3 + x^2 + 1$), so 7 is a the smallest possible order for these. And it is easy to see from the product $(x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$ that these polynomials, indeed, divide $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$, thus the order of the matrices with these minimal polynomials is 7. We got that all the possible orders in $GL_3(\mathbb{Z}_2)$ are $1, 2, 3, 4, 7$.

Remark: This problem becomes simpler once we know about field extensions and finite fields.

HW1. *Let C be a square based rectangular cuboid with vertices $(\pm1, \pm1, \pm2)$. Determine the number of isometries of C. How many of these are reflections across planes or points and how many are rotations about a straight line?*

HW2. *Draw the action of the permutation* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 6 & 5 & 4 & 8 & 7 & 2 \end{pmatrix}$ *as an oriented graph as in problem 3. Determine the order of the permutation, that is, the smallest positive integer k such that if we apply the permutation k times we get the identity map.*