Solution 1

Groups, Cyclic groups

1. Prove the following properties of inverses.

   (a) If an element a has both a left inverse l and a right inverse r, then $r = l$, a is invertible and r is its inverse.
   Solution Since l is a left inverse for a, then $la = 1$. In the same way, since r is a right inverse for a the equality $ar = 1$ holds. Let us now consider the expression lar. By associativity of the composition law in a group we have

   $$r = 1r = (la)r = lar = l(ar) = l1 = l.$$

   This implies that $l = r$. Since $l = r$, it holds also that that $ar = 1 = la = ra$ hence a is invertible and r is its inverse.

   (b) If a is invertible, its inverse is unique.
   Solution Let i_1 and i_2 be inverses of a. In particular i_1 is a left inverse of a and i_2 is a right inverse of a. By point (a) $i_1 = i_2$.

   (c) Inverses multiply in the opposite order: if a and b are invertible, then the product ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.
   Solution In order to show that ab is invertible, it is enough to exhibit an element that is a right and a left inverse of ab. The element $b^{-1}a^{-1}$ is a right inverse of ab since

   $$abb^{-1}a^{-1} = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1.$$

   It is a left inverse since

   $$b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-1}1b = b^{-1}b = 1$$

   This proves that ab is invertible and that $b^{-1}a^{-1}$ is its inverse.

2. Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots\}$ of natural numbers, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses. Deduce that in a set with a law of composition, an element may have a left inverse, even if it is not invertible.
   Solution Let us assume by contradiction that there exist a right inverse r of the shift map s. Since the identity for the composition law of functions $\mathbb{N} \to \mathbb{N}$ is the identity map, the fact that r is a right inverse for s means that $s \circ r$ is the identity

map, and this means that for any natural number n the equation $sr(n) = n$ holds. Let now m be the natural number $r(1)$. Since $sr(1) = 1$ we get

$$s(r(1)) = s(m) = m + 1 = 1$$

This implies that $m = 0$ which is a contradiction since 0 doesn't belong to $\mathbb{N}$.

To construct infinitely many left inverses of s let us consider, for any natural number k, the map l_k defined by

$$l_k(x) = \begin{cases} x - 1 & \text{if } x \neq 1; \\ k & \text{if } x = 1. \end{cases}$$

For any natural number k, the map l_k is a left inverse of s, in fact $l_k(s(x)) = l_k(x+1) = x$, where in the last equality we have used the fact that $x+1$ is always different from 1 if x is a natural number. Moreover clearly the maps l_k are pairwise distinct since their value in 1 is different.

3. Make a multiplication table for the symmetric group S_3.
Solution We will consider the group S_n of permutations of a set of n elements as the subgroup of $GL_n(\mathbb{R})$ consisting of permutation matrices, the matrices representing the endomorphisms of $\mathbb{R}^n$ that permute the elements of the standard basis.

Let us denote by x the cyclic permutation of the indices, that is represented by the matrix

$$x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and for y the permutation which interchanges 1 and 2 fixing 3, that means that

$$y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is easy to verify that $xy = yx^2$, indeed

$$xy = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$yx^2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Similarly $x^3 = 1$ and $y^2 = 1$.

The six permutations of $\{1, 2, 3\}$ are

$$\left\{1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, x^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, yx = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, yx^2 \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\right\}$$

and the multiplication table is

$\cdot$	e	x	x^2	y	yx	yx^2
e	e	x	x^2	y	yx	yx^2
x	x	x^2	e	yx^2	y	yx
x^2	x^2	e	x	yx	yx^2	y
y	y	yx	yx^2	e	x	x^2
yx	yx	yx^2	y	x^2	e	yx
yx^2	yx^2	y	yx	x	x^2	e

4. In which of the following cases is H a subgroup of G?

   (a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.
   SolutionThe invertible real matrices form a subgroup of the invertible complex matrices:

   - *Closure*: if a and b are real matrices the same is true for the product matrix ab.
   - *Identity*: since 1 belongs to $\mathbb{R}$, the identity matrix, that is the identity of the group $GL_n(\mathbb{C})$ belongs to $GL_n(\mathbb{R})$.
   - *Inverses*: the inverse of an invertible real matrix M is real, since it can be written as $\frac{1}{\det M}\widetilde{M}$ where $\widetilde{M}$ is the complementary matrix of M.

   (b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.
   Solution The set $\{1, -1\}$ is a subgroup of $\mathbb{R}^\times$:

   - *Closure:* In fact $1 \cdot 1 = 1$, $1 \cdot (-1) = -1$ and $(-1) \cdot (-1) = 1$.
   - *Identity:* 1 is the identity of $\mathbb{R}^\times$ and it belongs to H.
   - *Inverses:* $1 = 1^{-1}$ and $-1 = (-1)^{-1}$.

   (c) $G = \mathbb{Z}^+$ and H is the set of positive integers.
   Solution The set of positive integers is not a subgroup of $\mathbb{Z}^+$ since it doesn't contain the inverse of its elements: the inverse of 1 in $\mathbb{Z}^+$ is -1 that doesn't belong to $\mathbb{N}$.

   (d) $G = \mathbb{R}^\times$ and H is the set of positive reals.
   SolutionThe set of positive reals is a subgroup of $\mathbb{R}^\times$:

   - *Closure:* If a and b are positive real numbers, then ab is positive.
   - *Identity:* The identity of $\mathbb{R}^\times$ is 1 that is positive.
   - *Inverses:* For any positive real number x, $1/x$ is still positive.

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, with $a \neq 0$.

Solution The set of matrices of the form $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ is a subgroup of $GL_2(\mathbb{R})$:

- *Closure:* The product of two matrices in H belongs to H:

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}.$$

- *Identity:* The identity of G is the identity matrix that belongs to H.
- *Inverses:* The matrix $\begin{bmatrix} 1/a & 0 \\ 0 & 1 \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ and it belongs to H.

5. In the definition of a subgroup H of a group G the identity element of H is required to be the identity of G. Prove that it would be enough to require that H has an identity element x: in that case x must be the identity of G.
Solution Let us denote by 1_H the identity of a subset H of the group G that is a group with the composition law given by the restriction of the multiplication in G. By definition of inverse, for any element h in H, it holds $1_H h = h 1_H = h$. In particular this holds for the element 1_H itself:

$$1_H 1_H = 1_H. \tag{1}$$

Since 1_H is an element of G, 1_H is invertible, this means that there exist an element g in G such that $1_H g = 1$. Multiplying both sides of (1) on the right by g we get

$$1_H = 1_H(1_H g) = (1_H 1_H)g = 1_H g = 1.$$

6. Describe all groups G that contain no proper subgroup.
Solution We claim that a group with no proper subgroup is cyclic of prime order.

Proof. Let G be a group that contains no proper subgroup and let z be an element in G different from the identity. The subgroup generated by z is a cyclic group that is a subgroup of G. Since G contains no proper subgroup, $G = \langle z \rangle$, in particular G is cyclic.

Let us now consider the subgroup generated by z^2. Since G contains no proper subgroup, $z \in \langle z^2 \rangle$ and this implies that there exist an integer m such that $z = (z^2)^m = z^{2m}$. This implies that $z^{2m-1} = 1$, in particular the order of z must be finite.

Assume now that the order n of z is not prime and let us write $n = pq$ for some natural numbers p, q different from one. We claim that $\langle z^p \rangle$ is a proper subgroup of G. Indeed $\langle z^p \rangle = \{1, z^p, \ldots, z^{p(q-1)}\}$. This gives again a contradiction, hence the order of z is prime.

In order to prove the claim it is now enough to show that a cyclic group of prime order p has no proper subgroups. Indeed every element of a cyclic group of prime order generates the whole cyclic group, hence G cannot have proper subgroups.

7. Recall from Gerd Fisher, Lineare Algebra, Section 2.7 that an elementary matrix of the first kind in $GL_n(\mathbb{R})$ is a diagonal matrix $S_i(\lambda)$ having all diagonal elements equal to one apart from the i-th that is equal to λ for some real number λ different from 0; and recall that an elementary matrix of the second kind is a matrix $Q_i^j(\lambda)$ such that every diagonal entry of $Q_i^j(\lambda)$ is 1 and such that all other entries are zero apart from the entry in the i-th row and j-th column that is equal to λ, for some real number λ and some pair (i, j) with i different from j and between 1 and n. Prove that:

   (a) The elementary matrices of the first and second kind generate $GL_n(\mathbb{R})$.
   Solution Let A be a matrix, the matrix $A_1 = AS_i(\lambda)$ is the matrix obtained by A multiplying the i-th column by λ and the matrix $A_2 = AQ_i^j(\lambda)$ is the matrix obtained by A adding to the j-th column the i-th column multiplied by λ. Since the determinant of $Q_i^j(\lambda)$ is 1, column operations of the second kind do not change the determinant of a matrix A.

   Gauss algorithm for solving linear sistems implies that any invertible matrix can be transformed in a triangular matrix performing a finite number of column operation of the second kind. Moreover since the determinant of the triangular matrix is non zero, all its diagonal elements are different from zero This implies that, performing other column operations, it is possible to transform the invertible matrix A in a diagonal matrix.

   In formulas this proves that, given an invertible matrix M, there exist k, a diagonal matrix D, real numbers $\lambda_1, \dots \lambda_k$, and pairs $(i_1, j_1), \dots, (i_k, j_k)$ such that

   $$D = MQ_{i_1}^{j_1}(\lambda_1) \dots Q_{i_k}^{j_k}(\lambda_k).$$

   Since a diagonal matrix D is the product $D = S_1(D_{11}) \dots S_n(D_{nn})$, and since the inverse of an elementary matrix of the second kind is still an elementary matrix of the second kind $(Q_i^j(\lambda)^{-1} = Q_i^j(-\lambda))$, we get that

   $$M = DQ_{i_k}^{j_k}(-\lambda_k) \dots Q_{i_1}^{j_1}(-\lambda_1) = S_1(D_{11}) \dots S_n(D_{nn})Q_{i_k}^{j_k}(-\lambda_k) \dots Q_{i_1}^{j_1}(-\lambda_1).$$

   (b) The elementary matrices of the second kind generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

   SolutionClearly the elementary matrices of the second kind are contained in $SL_n(\mathbb{R})$ hence they generate a subgroup of $SL_n(\mathbb{R})$. We have to show that any matrix in $SL_n(\mathbb{R})$ can be written as a product of elementary matrices of the second kind. We will first show this for a diagonal matrix in $SL_n(\mathbb{R})$.

For any nonzero real number a, the diagonal matrix $\left[\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right]$ of $SL_2(\mathbb{R})$ can be written as the product $Q_1^2(a)Q_2^1(1-a^{-1})Q_1^2(-1)Q_2^1(1-a)$ of elementary matrices of the second kind:

$$\begin{aligned} & \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-a^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-a & 1 \end{bmatrix} = \\ = & \begin{bmatrix} a & a \\ 1-a^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-a & 1 \end{bmatrix} = \\ = & \begin{bmatrix} a & 0 \\ 1-a^{-1} & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1-a & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}. \end{aligned}$$

For generic n, a diagonal matrix D is in $SL_n(\mathbb{R})$ if all its diagonal elements are non zero. Let d_k be the product of the first k diagonal elements of D and let us define, for any i smaller than n the diagonal matrix D_i such that its diagonal entries are all 1 apart from the i-th that is equal to d_k and the $i+1$-th that is equal to $(d_k)^{-1}$. The matrix D is the product of the matrices D_i, moreover the computation in the $SL_2(\mathbb{R})$ case shows that $D_i = Q_i^{i+1}(d_i)Q_{i+1}^i(1-d_i^{-1})Q_i^{i+1}(-1)Q_{i+1}^i(1-d_i)$. This concludes the proof of the fact that any diagonal matrix in $SL_n(\mathbb{R})$ can be written as product of elementary matrices of the second kind.

In order to conclude the proof it is enough to notice that the same argument as in point (a) shows that any matrix M in $SL_n(\mathbb{R})$ is the product of a diagonal matrix D and some elementary matrices $Q_{i_k}^{j_k}(-\lambda_k)\dots Q_{i_1}^{j_1}(-\lambda_1)$. Moreover since $SL_n(\mathbb{R})$ is a group, M and the elementary matrices $Q_{i_l}^{j_l}(-\lambda_l)$ belong to $SL_n(\mathbb{R})$ and D can be written as $D = MQ_{i_1}^{j_1}(\lambda_1)\dots Q_{i_k}^{j_k}(\lambda_k)$, then D belongs to $SL_n(\mathbb{R})$ since $SL_n(\mathbb{R})$ is *closed*. In particular D can be written as a product of elementary matrices of the second kind. This concludes the proof:

$$M = S_1(D_{11})\dots S_n(D_{nn})Q_{i_k}^{j_k}(-\lambda_k)\dots Q_{i_1}^{j_1}(-\lambda_1).$$

More challenging problems

The homophonic group

1. By definition, English words have the same pronunciation if their phonetic spellings in the dictionary are the same. The *homophonic* group $\mathcal{H}$ is generated by the letters of the alphabet, subject to the following relations: English words with the same pronunciation represent equal elements of the group. Thus $be = bee$, and since $\mathcal{H}$ is a group, we can conclude that $e = 1$ (why?). Try to determine the group $\mathcal{H}$.