8. Permutations

In: Otakar Borůvka (author): Foundations of the Theory of Groupoids and Groups. (English). Berlin: VEB Deutscher Verlag der Wissenschaften, 1974. pp. 60--69.

Persistent URL: http://dml.cz/dmlcz/401547

2. Assuming the situation described in exercise 1., let $\overline{G}$ be the decomposition on G corresponding to the mapping $\boldsymbol{g}$. Show that the equality $\boldsymbol{g}(A \cap B) = \boldsymbol{g}A \cap \boldsymbol{g}B$ applies if and only if there holds $(A \cap B) \sqsubset \overline{G} = (A \sqsubset \overline{G}) \cap (B \sqsubset \overline{G})$.

3. Let $\boldsymbol{g}$ be a mapping of the set G onto G^* and $\{\bar{a}, \bar{b}, \ldots\}$ stand for a decomposition on G. Then $\{\boldsymbol{g}\bar{a}, \boldsymbol{g}\bar{b}, \ldots\}$ is a decomposition on G^* if and only if $\{\bar{a}, b, \ldots\}$ is a covering of the decomposition corresponding to $\boldsymbol{g}$.

4. Suppose $\boldsymbol{g}$ is a simple mapping of the set G onto G^*. Let, moreover, $A \subset G$ be a nonempty subset and $\bar{A}$, $\bar{B}$ stand for decompositions in (on) G. In this situation there holds:
   a) the extended mapping $\bar{\boldsymbol{g}}$ of the system of all the nonempty parts' of G onto the system of all the nonempty parts of G^* is simple;
   b) the sets A, $\boldsymbol{g}A$ are equivalent, i.e., $A \simeq \boldsymbol{g}A$;
   c) $\boldsymbol{g}\bar{A}$ is a decomposition in (on) the set G^*;
   d) the decompositions $\bar{A}$, $\boldsymbol{g}\bar{A}$ are equivalent, i.e., $\bar{A} \simeq \boldsymbol{g}\bar{A}$;
   e) if the decompositions $\bar{A}$, $\bar{B}$ are equivalent or loosely coupled or coupled, then the decompositions $\boldsymbol{g}\bar{A}$, $\boldsymbol{g}\bar{B}$ have, in each case, the same property.

8. Permutations

In this chapter we shall deal with simple mappings of finite sets onto themselves; they play an important role in algebra, particularly, in the theory of groups.

8.1. Definition

By a *permutation of the set* G we mean a simple mapping of the set G onto itself (6.6).

In this section we shall restrict our considerations to permutations of *finite* sets.

Let G denote an arbitrary set consisting of a finite number $n(\geqq 1)$ of elements. From the assumption that G is finite it follows that every simple mapping $\boldsymbol{p}$ of the set G into itself is a permutation of G (6.10.2).

Let the elements of G be denoted by the letters $a, b, \ldots, m$. Then we can uniquely associate, with every permutation $\boldsymbol{p}$ of the set G, a symbol of the form:

$$\begin{pmatrix} a & b & \ldots & m \\ a^* & b^* & \ldots & m^* \end{pmatrix}.$$

where $a^*, b^*, \ldots, m^*$ are the letters denoting the elements $\boldsymbol{p}a, \boldsymbol{p}b, \ldots, \boldsymbol{p}m$. Since $\boldsymbol{p}G = G$, the letters $a^*, b^*, \ldots, m^*$ are again $a, b, \ldots, m$ written in a certain order.

Conversely, every symbol of the above form, where the letters $a^*, b^*, \ldots, m^*$ are again the letters $a, b, \ldots, m$ written in a certain order, determines a certain permutation of the set G, namely, the permutation under which every element denoted by a letter x in the first row is mapped onto the element denoted by the letter lying under x in the second row. Note that the same permutation $\boldsymbol{p}$ may similarly be expressed by other symbols if the letters $a, b, \ldots, m$ in the first row are written in a different order but under each of them there remains the same letter as before. The identical mapping of G is, naturally, a particular permutation of G, the so-called *identical permutation*; it is denoted by the symbol $\begin{pmatrix} a\,b\,\ldots\,m \\ a\,b\,\ldots\,m \end{pmatrix}$ or any of the other symbols, e.g., $\begin{pmatrix} b\,a\,\ldots\,m \\ b\,a\,\ldots\,m \end{pmatrix}$.

8.2. Examples of permutations

Let us first introduce a few simple examples of permutations of sets containing $n = 1, 2, 3, 4$ elements.

1. $n = 1$. Let G be a set consisting of a single point a in a plane. In that case there exists, of course, exactly one permutation of G, namely, the identical permutation $\begin{pmatrix} a \\ a \end{pmatrix}$.

2. $n = 2$. Let G be a set consisting of two arbitrary points a, b in a plane. If a, b are rotated, in the plane, in one or the other direction, about the center of the line segment with the end-points a, b through an angle α, then the point a shifts to a certain point a' and the point b to b' and we have a simple mapping of the set G onto the set $\{a', b'\}$. If α equals 0°, 180°, then the set $\{a', b'\}$ is identical with G and we have the following permutations of the set G: $\begin{pmatrix} a\,b \\ a\,b \end{pmatrix}$, $\begin{pmatrix} a\,b \\ b\,a \end{pmatrix}$, respectively.

3. $n = 3$. Suppose G is a set of three points on a plane: a, b, c, forming the vertices of an equilateral triangle. If the points a, b, c are rotated, in the plane, in one or the other direction, about the center of the triangle through an angle α, then the point a shifts to a certain point a', the point b to b', the point c to c' and we have a simple mapping of the set G onto the set $\{a', b', c'\}$. If α equals 0°, 120°, 240°, then the set $\{a', b', c'\}$ is identical with G and we have the following permutations of G:

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix},$$

respectively. Further permutations of G are obtained by associating, with the

points a, b, c, the points symmetric with regard to some axis of symmetry of the triangle in question. The latter has altogether three axes of symmetry; each of them passes through one vertex and bisects the opposite side. Associating, with each of the points a, b, c, the point symmetric with regard to the axis of symmetry passing through a, we obtain the permutation

$$\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix};$$

in a similar way we obtain further permutations:

$$\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \qquad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

So we have found, in this case, altogether 6 permutations, namely:

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

4. $n = 4$. Now let G be a set of four points in a plane: a, b, c, d, forming the vertices of a square. Rotating the points a, b, c, d, in the plane, in one or the other direction about the center of the square through an angle α, we again obtain a simple mapping of the set G onto the set of certain points a', b', c', d' in the plane; if $\alpha = 0°, 90° 180°, 270°$, then we get the following permutations of the set G, respectively:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}.$$

Further permutations of the set G are found, again, by associating, with the points a, b, c, d, the points symmetric with regard to some axis of symmetry of the mentioned square. The latter has althogether four axes of symmetry; two of them pass through two diagonal vertices and the other two bisect the two opposite sides. Associating, with each of the points a, b, c, d, the point symmetric with regard to the axis of symmetry passing through the vertices a, c, we obtain the permutation

$$\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix};$$

in a similar way we obtain further permutations:

$$\begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

Thus we have found, in this case, altogether 8 permutations, namely:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix},$$

$$\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

8.3. The number of permutations

Let us now resume our study of the permutations on a set G of $n(\geqq 1)$ elements $a, b, \ldots, m$.

How many permutations of G are there altogether? To answer this question, let us first note the fact that, under an arbitrary permutation $\boldsymbol{p}$ of G, the element a is mapped onto a certain element $\boldsymbol{pa}$ of G; if $n > 1$ then, moreover, the element b is mapped onto an element $\boldsymbol{pb}$ different from $\boldsymbol{pa}$, the element c onto an element $\boldsymbol{pc}$ different from $\boldsymbol{pa}$, $\boldsymbol{pb}$, etc., up to the element m mapped onto an element $\boldsymbol{pm}$ different from the elements $\boldsymbol{pa}, \boldsymbol{pb}, \boldsymbol{pc}, \ldots$. Conversely, associating with the element a any element $a^* \in G$ and, if $n > 1$, with the element b any element $b^* \in G$ different from a^* and with the element c any element $c^* \in G$ different from a^*, b^* and so on up to the element $m^* \in G$ different from the elements $a^*, b^*, c^*, \ldots$, we obtain a certain permutation

$$\begin{pmatrix} a & b & c & \ldots & m \\ a^* & b^* & c^* & \ldots & m^* \end{pmatrix}$$

of the set G. The number of the permutations is exactly the same as the number of the possibilities of the above associations. But with the element a we may associate an element $a^* \in G$ in n ways: first, the element a itself, then the element b and so on, until, the n^{th} time, the element m; if $n > 1$ we may, moreover, associate with the element b an element $b^* \in G$ different from a^* in altogether $n - 1$ ways and, similarly, with the element c some element $c^* \in G$ different from a^*, b^* in altogether $n - 2$ ways, and so on up to the element m with which we may associate some element $m^* \in G$ different from $a^*, b^*, c^*, \ldots$, exactly in one way. So we have altogether $n(n-1)(n-2)\ldots 1$ possibilities and the answer to the above question is that there *exist exactly* $1.2.3 \ldots n$ *permutations of the set* G. This number is generally denoted by the symbol $n!$. For example, for every set consisting of $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ elements there exist exactly $n! = 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800$ permutations. The permutations we have found in the above examples of $1, 2, 3$ points in a plane are evidently all that there exist but, in case of 4 points in a plane, there exist, beside the 8 permutations we have found, $2.8 = 16$ further permutations.

8.4. Properties of permutations

1. *Inverse permutations.* Let us now proceed to a more detailed study of the properties of permutations. Suppose $\boldsymbol{p}$ is a permutation of the set G. Since $\boldsymbol{p}$ is a simple mapping, there exists an inverse permutation $\boldsymbol{p}^{-1}$ of $\boldsymbol{p}$ of G. It is easy to see that the symbol of $\boldsymbol{p}^{-1}$ is obtained by interchanging the two rows in the symbol $\boldsymbol{p}$. For instance, the permutations inverse of the above 8 permutations of four points in

a plane are:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix},$$
$$\begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

2. *Invariant elements.* An arbitrary point $x \in G$ is mapped, under the permutation $\boldsymbol{p}$, onto an element $\boldsymbol{p}x$ which is or is not identical with x. In the first case, $\boldsymbol{p}x = x$, we say that *the permutation* $\boldsymbol{p}$ *leaves the element* x *invariant* (*unchanged*) or that the element x is invariant under the permutation $\boldsymbol{p}$. It is obvious that, under the permutation $\boldsymbol{p}$ and the inverse permutation $\boldsymbol{p}^{-1}$, the same elements of the set G are invariant. For instance, the above permutations of four points in a plane leave the following elements invariant: a, b, c, d; none; none; none; a, c; b, d; none; none.

3. *Cyclic* (or *circular*) *permutations.* An element x and the permutation $\boldsymbol{p}$ uniquely determine the sequence of elements of G: x, $\boldsymbol{p}x$, $\boldsymbol{p}(\boldsymbol{p}x)$, $\boldsymbol{p}\big(\boldsymbol{p}(\boldsymbol{p}x)\big)$, ..., in which every element except the first is the $\boldsymbol{p}$-image of the preceding one. Instead of x, $\boldsymbol{p}x$ we sometimes write $\boldsymbol{p}^0x$, $\boldsymbol{p}^1x$ and, for brevity, instead of $(\boldsymbol{pp}x)$, $\boldsymbol{p}\big(\boldsymbol{p}(\boldsymbol{p}x)\big)$ we generally put $\boldsymbol{p}^2x$, $\boldsymbol{p}^3x$, ...

The permutation $\boldsymbol{p}$ is called *cyclic* or *circular* if there exists an element $x \in G$ and a positive integer k such that, in the sequence x, $\boldsymbol{p}x$, $\boldsymbol{p}^2x$, $\boldsymbol{p}^3x$, ..., $\boldsymbol{p}^{k-1}x$, no two elements are identical but the image $\boldsymbol{p}^kx$ of $\boldsymbol{p}^{k-1}x$ is again the element x and if, moreover, all the other elements of G—if there are any—remain invariant under $\boldsymbol{p}$. The permutation $\boldsymbol{p}$ can be more precisely described as a cyclic (circular) permutation with regard to the elements x, $\boldsymbol{p}x$, $\boldsymbol{p}^2x$, ..., $\boldsymbol{p}^{k-1}x$.

The ordered set of elements x, $\boldsymbol{p}x$, $\boldsymbol{p}^2x$, ..., $\boldsymbol{p}^{k-1}x$ is called a *cycle of the permutation* $\boldsymbol{p}$ or, more precisely, a *k-membered cycle* or a *k-cycle of* $\boldsymbol{p}$. If, in particular, $k = n$, i.e., if every element of G lies in this cycle we say that $\boldsymbol{p}$ is a *pure cyclic* (*circular*) *permutation.*

Let the permutation $\boldsymbol{p}$ be cyclic with regard to the elements $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$. Then the permutation $\boldsymbol{p}$ is usually expressed by a simple symbol: the elements x, $\boldsymbol{p}x$, $\boldsymbol{p}^2x$, ..., $\boldsymbol{p}^{k-1}x$ are written in this order, next to each other, in parentheses. The inverse of the permutation $\boldsymbol{p}$, i.e. $\boldsymbol{p}^{-1}$, maps every element of the sequence x, $\boldsymbol{p}x$, $\boldsymbol{p}^2x$, ..., $\boldsymbol{p}^{k-1}x$ except the first onto the preceding one, the element x onto $\boldsymbol{p}^{k-1}x$ and the other elements of G—if there are any—remain invariant; consequently, $\boldsymbol{p}^{-1}$ is cyclic with regard to $\boldsymbol{p}^{k-1}x$, ..., $\boldsymbol{p}^2x, \boldsymbol{p}x, x$. If we change the symbols of the elements of G by denoting the elements $x, \boldsymbol{p}x, \boldsymbol{p}^2x, \ldots, \boldsymbol{p}^{k-1}x$ by the letters $a, b, c, \ldots, j$, respectively, and the other elements of G—if there are any—by other arbitrarily chosen letters, then the simplified symbol of $\boldsymbol{p}$ is: $(a, b, c, \ldots, j)$. The permutation may, of course, be expressed by any other symbol: $(b, c, \ldots, j, a)$, $(c, \ldots, j, a, b)$, etc., altogether in k ways. Then the symbol of the inverse permutation is, for example, $(j, \ldots, c, b, a)$.

The simplest cyclic permutations are those with regard to one single element; by the above definition, every permutation of this kind is the identical permutation of G and, consequently, may be expressed by any symbol (a), (b), ..., (m).

Every cyclic permutation of G with regard to two elements is called a *transposition.*

For instance, in the above permutations of the set of $n = 1, 2, 3, 4$ points in a plane we have the following cyclic permutations:

for $n = 1$: (a);

for $n = 2$: (a), (a, b);

for $n = 3$: (a), (a, b), (a, c), (b, c), (a, b, c), (a, c, b);

for $n = 4$: (a), (a, c), (b, d), (a, b, c, d), (a, d, c, b).

4. *Invariant subsets and decompositions.* Now, let again $\boldsymbol{p}$ stand for an arbitrary permutation of the set G. Any nonempty subset $A \subset G$ is mapped, under the extended mapping $\boldsymbol{p}$, onto a subset $\boldsymbol{p}A \subset G$ which is or is not a part of A. In the first case, if $\boldsymbol{p}A \subset A$, then $\boldsymbol{p}A = A$. In fact, by the definition of the partial mapping $\boldsymbol{p}_A$, there holds $\boldsymbol{p}A = \boldsymbol{p}_A A$; moreover, as $\boldsymbol{p}$ is a simple mapping of the finite set A into itself, it is a permutation of the set A; so we have $\boldsymbol{p}_A A = A$.

If $\boldsymbol{p}A = A$, we say that *the permutation $\boldsymbol{p}$ leaves the subset A invariant* or that *the subset A is invariant under the permutation $\boldsymbol{p}$.*

The subset A is invariant under the permutation $\boldsymbol{p}$ if each of its elements is invariant under $\boldsymbol{p}$. If $\boldsymbol{p}$ leaves the subset A invariant, then the same evidently holds for the inverse permutation $\boldsymbol{p}^{-1}$. For example, the above permutations of four points in the plane leave the following proper subsets of the set $\{a, b, c, d\}$ invariant: all; none; $\{a, c\}$, $\{b, d\}$; none; $\{a\}$, $\{c\}$, $\{b, d\}$; $\{b\}$, $\{d\}$, $\{a, c\}$; $\{a, b\}$, $\{c, d\}$; $\{a, d\}$, $\{b, c\}$. Note that, if $\boldsymbol{p}$ is the cyclic permutation $(a, b, c, \ldots, j)$, then every subset $A \subset G$ containing the elements $a, b, c, \ldots, j$ is invariant under $\boldsymbol{p}$, the partial permutation $\boldsymbol{p}_A$ is cyclic as well and is expressed by the same symbol $(a, b, c, \ldots, j)$.

Suppose $\overline{G} = \{\bar{a}, \bar{b}, \ldots, \overline{m}\}$ is a decomposition of the set G. If $\overline{G}$ has the property that, under the extended mapping $\boldsymbol{p}$, the image of every element of $\overline{G}$ is again an element of $\overline{G}$, we say that *the permutation $\boldsymbol{p}$ leaves the decomposition $\overline{G}$ invariant* or that *the permutation $\overline{G}$ is invariant under the permutation $\boldsymbol{p}$.* It is clear that, if the permutation $\boldsymbol{p}$ leaves the decomposition $\overline{G}$ invariant, the same holds for the inverse permutation $\boldsymbol{p}^{-1}$.

Let us, in particular, consider the case when every element of $\overline{G}$ is invariant under $\boldsymbol{p}$ so that $\boldsymbol{p}\bar{a} = \bar{a}$, $\boldsymbol{p}\bar{b} = \bar{b}$, ..., $\boldsymbol{p}\overline{m} = \overline{m}$. Then, $\bar{x}$ being an element of $\overline{G}$, the partial mapping $\boldsymbol{p}_{\bar{x}}$ is a permutation of $\bar{x}$. The partial permutations $\boldsymbol{p}_{\bar{a}}, \boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ uniquely determine the permutation $\boldsymbol{p}$ in the sense that the $\boldsymbol{p}$-image of every element $x \in G$ is the same under the partial permutation $\boldsymbol{p}_{\bar{x}}$ of the element $\bar{x} \in \overline{G}$ containing x. Under the inverse permutation $\boldsymbol{p}^{-1}$ every element of $\overline{G}$ is invariant

as well and $\boldsymbol{p}^{-1}$ is determined by the inverse permutations $\boldsymbol{p}_{\bar{a}}^{-1}$; $\boldsymbol{p}_{\bar{b}}^{-1}$, ..., $\boldsymbol{p}_{\bar{m}}^{-1}$. Conversely, let $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ be an arbitrary decomposition on G and choose, on each of its elements $\bar{x}$, an arbitrary permutation $\boldsymbol{p}_{\bar{x}}$; define, on G, the permutation $\boldsymbol{p}$ by associating with every element $x \in G$ its $\boldsymbol{p}_{\bar{x}}$-image where $x \in \bar{x}$; then every element of $\bar{G}$ is invariant under $\boldsymbol{p}$ and $\boldsymbol{p}_{\bar{a}}$, $\boldsymbol{p}_{\bar{b}}$, ..., $\boldsymbol{p}_{\bar{m}}$ are the determining partial permutations of $\boldsymbol{p}$.

8.5. The determination of permutations by pure cyclic permutations

Now we shall show that *an arbitrary permutation* $\boldsymbol{p}$ *of any set* G *consisting of* $n(\geqq 1)$ *elements is determined by a finite number of pure cyclic permutations*, in other words, that there exists a decomposition $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ of G such that each element of G is invariant under $\boldsymbol{p}$ and the partial permutations are pure cyclic permutations of the elements $\bar{a}, \bar{b}, \ldots, \bar{m}$.

The proof will be based on the method of complete induction.[1]) For $n = 1$ our statement is correct because, in that case, $\boldsymbol{p}$ is the identical permutation of G and the greatest decomposition of G has the above property. It remains to be shown that, if our statement holds for every set consisting of at most $n - 1$ elements, n standing for an integer > 1, then it also holds for any set consisting of n elements. Let G stand for a set of n elements and $\boldsymbol{p}$ for a permutation of G. Let, moreover, a denote an element of G. Consider the sequence of the elements $a, \boldsymbol{p}a, \boldsymbol{p}^2a, \ldots, \boldsymbol{p}^na$ of G, each of which is the $\boldsymbol{p}$-image of the preceding element. The number of these elements is $n + 1$ so that at least one element occurs in G at least twice. Proceeding, in the mentioned sequence, from the first element a successively to the subsequent elements, we arrive, *for the first time*, at:

a) a certain element $\boldsymbol{p}^ja$, j denoting a number $0, \ldots, n - 1$ that occurs among the elements $\boldsymbol{p}^{j+1}a, \ldots, \boldsymbol{p}^na$ at least once more;

b) the element $\boldsymbol{p}^{j+k}a$, k being a number $1, \ldots, n - j$ which is identical with the element $\boldsymbol{p}^ja$, so that $\boldsymbol{p}^ja = \boldsymbol{p}^{j+k}a$.

If $\boldsymbol{p}^ja$ is not the first element a, i.e., if $j > 0$, then both elements $\boldsymbol{p}^{j-1}a$ and $\boldsymbol{p}^{j+k-1}a$ are mapped, under $\boldsymbol{p}$, onto the same element $\boldsymbol{p}^ja$ and, since $\boldsymbol{p}$ is a simple mapping, there holds $\boldsymbol{p}^{j-1}a = \boldsymbol{p}^{j+k-1}a$; but that is not possible because, in the sequence $a, \boldsymbol{p}a$,

---

[1]) The method of complete induction is based on the following theorem: *If one associates, with every positive integer* n, *a certain statement* $\boldsymbol{g}n$ *such that:* (1) *the statement* $\boldsymbol{g}1$ *is correct,* (2) *for every* $n > 1$ *for which the statements* $\boldsymbol{g}1, \ldots, \boldsymbol{g}(n-1)$ *are correct, even* $\boldsymbol{g}n$ *is correct, then all the statements are correct.* In fact, in the opposite case the incorrect statements are associated with certain positive integers one of which, let us denote it by m, is the least. By the assumption (1), there holds $m > 1$; by the definition of m, the statements $\boldsymbol{g}1, \ldots, \boldsymbol{g}(m-1)$ are correct, whereas the statement $\boldsymbol{g}m$ is incorrect, but that contradicts the assumption (2).

An analogous theorem applies to the statements associated with integers greater than or equal to an integer k.

$\boldsymbol{p}^2a, \ldots, \boldsymbol{p}^na$, the element $\boldsymbol{p}^ja$ is not preceded by any element occurring once more whereas, according to the above equality, $\boldsymbol{p}^{j-1}a$ is such an element. Thus we have ascertained that $j = 0$. By the definition of the number k, we have $\boldsymbol{p}^ka = a$ but none of the elements $\boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ is a. If any two of the elements $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ are equal, i.e., if for some integers r, s satisfying the inequalities $0 \leqq r < s \leqq k-1$, there holds $\boldsymbol{p}^ra = \boldsymbol{p}^sa$, then we have $\boldsymbol{p}^{k-s}(\boldsymbol{p}^ra) = \boldsymbol{p}^{k-s}(\boldsymbol{p}^sa)$, i.e., $\boldsymbol{p}^{k-s+r}a = \boldsymbol{p}^ka = a$; but this contradicts the fact that none of the elements $\boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ is a because $1 \leqq k - s + r \leqq k - 1$ and therefore $\boldsymbol{p}^{k-s+r}a$ is one of these elements. Thus we have verified that no two elements $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$ are equal.

Let $\bar{a}$ stand for the set of the elements $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$. We observe that the subset $\bar{a} \subset G$ is invariant under the permutation $\boldsymbol{p}$ and that the partial permutation $\boldsymbol{p}_{\bar{a}}$ is a pure cyclic permutation of $\bar{a}$. If $k = n$, i.e., if $\bar{a} = G$, then $\boldsymbol{p}_{\bar{a}} = \boldsymbol{p}$ and the greatest decomposition of G has the above property. Let us now consider the case $k < n$. In that case the set G contains, besides $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$, further elements the number of which is, at most, $n - 1$; the set of these elements will be denoted by H. Under the partial mapping $\boldsymbol{p}_H$, the image of every element $x \in H$ is again an element of H because, in the opposite case, there holds $\boldsymbol{p}x = \boldsymbol{p}^la$, l standing for one of the numbers $0, \ldots, k-1$ and, consequently, $x = \boldsymbol{p}^{l-1}a$ and $x = \boldsymbol{p}^{k-1}a$ if $l > 0$ and $l = 0$, respectively; but in both cases this contradicts the assumption $x \in H$. The permutation $\boldsymbol{p}_H$ is therefore a mapping of the set H into itself and, since it is simple and H has only a finite number of elements, $\boldsymbol{p}_H$ is a permutation of H. If our statement holds for every set of, at most, $n - 1$ elements, then there exists a decomposition $\overline{H} = \{\bar{b}, \ldots, \overline{m}\}$ of the set H such that every element of H is invariant under the permutation $\boldsymbol{p}_H$ and the partial permutations of the elements $\bar{b}, \ldots, \overline{m}$, determined by $\boldsymbol{p}_H$ are pure cyclic permutations. Since $\boldsymbol{p}_H$ maps every element of H onto the same element as $\boldsymbol{p}$, the partial mappings $\boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ of $\bar{b}, \ldots, \overline{m}$, determined by $\boldsymbol{p}$, are exactly these pure cyclic permutations. The system of the sets $\overline{G} = \{\bar{a}, \bar{b}, \ldots, \overline{m}\}$ is obviously a decomposition of G and we see that each element $\bar{a}, \bar{b}, \ldots, \overline{m}$ is invariant under $\boldsymbol{p}$ and that $\boldsymbol{p}_{\bar{a}}, \boldsymbol{p}_{\bar{b}}, \ldots, \boldsymbol{p}_{\overline{m}}$ are pure cyclic permutations of $\bar{a}, \bar{b}, \ldots, \overline{m}$, which completes the proof.

8.6. The method of determining the pure cyclic permutations forming a given permutation

Given a permutation $\boldsymbol{p}$ of the set G consisting of $n \geqq 1$ elements, the pure cyclic permutations by which it is determined are obtained as follows: Starting from an arbitrary element $a \in G$ we first determine the cycle $a, \boldsymbol{p}a, \ldots, \boldsymbol{p}^{k-1}a$; then, if $k < n$, we choose an element $b \in G$ which is not in this cycle and determine the next cycle $b, \boldsymbol{p}b, \ldots, \boldsymbol{p}^{l-1}b$; furthermore, if $k + l < n$, we choose an element $c \in G$ which is not in any of the preceding cycles and determine the cycle beginning with the element c; in this way we proceed. To express the permutation $\boldsymbol{p}$ we then write, in a certain order, side by side, the symbols of the individual pure cyclic permutations. From this we obtain the symbol of the inverse permutation

$\boldsymbol{p}^{-1}$ by way of reversing, in each cycle, the order of the letters. For example, the above permutations of the set of $n = 1, 2, 3, 4$ points in a plane is determined by pure cyclic permutations as follows:

if $n = 1$: (a);

if $n = 2$: $(a)(b)$, (a, b);

if $n = 3$: $(a)(b)(c)$, (a, b, c), (a, c, b), (a) (b, c), $(a, c)(b)$, $(a, b)(c)$;

if $n = 4$: $(a)(b)(c)(d)$, (a, b, c, d), $(a, c)(b, d)$, (a, d, c, b), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$.

The inverse permutations of the latter are:

if $n = 1$: (a);

if $n = 2$: $(a)(b)$, (a, b);

if $n = 3$: $(a)(b)(c)$, (c, b, a), (b, c, a), $(a)(b, c)$, $(a, c)(b)$, $(a, b)(c)$;

if $n = 4$: $(a)(b)(c)(d)$, (d, c, b, a), $(a, c)(b, d)$, (b, c, d, a), $(a)(c)(b, d)$, $(a, c)(b)(d)$, $(a, b)(c, d)$, $(a, d)(b, c)$.

8.7. Composition of permutations

1. *The concept of the composition of permutations.* The permutations of the set G may, of course, be composed according to the rule of composing mappings. Let $\boldsymbol{p}$, $\boldsymbol{q}$ denote arbitrary permutations of G. The mapping $\boldsymbol{qp}$ composed of the permutations $\boldsymbol{p}$, $\boldsymbol{q}$ is again a permutation of G. The symbol of the latter is obtained by writing, under each letter x denoting some element of G, the letter of the element $\boldsymbol{q}(\boldsymbol{p}x)$. If the permutations $\boldsymbol{p}$, $\boldsymbol{q}$ are expressed in usual two-lined symbols, then the letter denoting the element $\boldsymbol{q}(\boldsymbol{p}x)$ is found as follows: First we find the letter denoting the element $\boldsymbol{p}x$ which lies, in the symbol of $\boldsymbol{p}$, under x, and then the letter denoting the element $\boldsymbol{q}(\boldsymbol{p}x)$ which lies, in the symbol of $\boldsymbol{q}$, under the letter denoting $\boldsymbol{p}x$. If, for instance, $n = 3$ and $\boldsymbol{p}$, $\boldsymbol{q}$ are given by the symbols

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \qquad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix},$$

then the symbol of $\boldsymbol{qp}$ is

$$\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

Analogously we proceed if $\boldsymbol{p}$, $\boldsymbol{q}$ are expressed by the pure cyclic permutations by which they are determined. For example, if $n = 3$ and $\boldsymbol{p}$, $\boldsymbol{q}$ are given by the symbols (a, b, c), $(a)(b, c)$, then $\boldsymbol{qp}$ is expressed by $(a, c)(b)$.

2. *Interchangeable permutations.* Note that the result of composing two permutations of G may depend on the order in which they are composed, i.e., the permutation $\boldsymbol{qp}$ composed of $\boldsymbol{p}$, $\boldsymbol{q}$ may be different from the permutation $\boldsymbol{pq}$ composed of $\boldsymbol{q}$, $\boldsymbol{p}$. In the above example there holds $\boldsymbol{qp} \neq \boldsymbol{pq}$, for $\boldsymbol{qp}$ is the permutation (a, c), whereas $\boldsymbol{pq}$ is (a, b). If the permutations $\boldsymbol{p}$, $\boldsymbol{q}$ are such that the results of their composition does not depend on their order, i.e., if $\boldsymbol{qp} = \boldsymbol{pq}$, then they are called *interchangeable*. E.g., the identical permutation of the set G and any other permutation of G are interchangeable.

3. *Associative law for the composition of permutations.* To any permutations $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ of the set G there, of course, applies the associative law

$$\boldsymbol{r}(\boldsymbol{qp}) = (\boldsymbol{rq})\boldsymbol{p};$$

the permutation of G lying on either side of this equality is briefly denoted by $\boldsymbol{rqp}$.

4. *The inverse of a composed permutation.* By means of the associative law we can easily show that *the inverse of the composed permutation* $\boldsymbol{qp}$ *is* $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$, i.e., that there holds

$$(\boldsymbol{qp})^{-1} = \boldsymbol{p}^{-1}\,\boldsymbol{q}^{-1}.$$

In fact, let x denote an arbitrary element of G. Taking account of the definition of $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$ and the associative law, we have $(\boldsymbol{p}^{-1}\boldsymbol{q}^{-1})(\boldsymbol{qp}x) = \boldsymbol{p}^{-1}\big(\boldsymbol{q}^{-1}(\boldsymbol{qp}x)\big) = \boldsymbol{p}^{-1}\big((\boldsymbol{q}^{-1}\boldsymbol{q})\boldsymbol{p}x\big)$ and, furthermore, $\boldsymbol{p}^{-1}\big((\boldsymbol{q}^{-1}\boldsymbol{q})\boldsymbol{p}x\big) = \boldsymbol{p}^{-1}\big(\boldsymbol{e}(\boldsymbol{p}x)\big) = \boldsymbol{p}^{-1}\big((\boldsymbol{ep})x\big) = \boldsymbol{p}^{-1}(\boldsymbol{p}x)$ $= (\boldsymbol{p}^{-1}\boldsymbol{p})x = \boldsymbol{e}x = x$, where $\boldsymbol{e}$ denotes the identical permutation of G. Consequently. the permutation $\boldsymbol{p}^{-1}\boldsymbol{q}^{-1}$ maps the element $\boldsymbol{qp}x$ onto x and our statement is correct.

8.8. Exercises

1. Give an example of a simple mapping of an infinite set (let us say, the set of all natural numbers) into itself which is not a permutation.
2. Write down the symbols of all the permutations of a set consisting of four elements and express the single permutations by means of pure cyclic permutations.
3. Say by which rule you would proceed if you were to write down the symbols of all the permutations of a set consisting of $n(\geqq 1)$ elements so as not to forget any of them.
4. A regular n-gon ($n \geqq 3$) in a plane has altogether n axes of symmetry. Rotating the vertices about the center of the n-gon through the angles of $0°$, $\left(\frac{360}{n}\right)°$, $\left(2.\frac{360}{n}\right)°$, ..., $\left((n-1).\frac{360}{n}\right)°$ and, furthermore, associating with them the vertices symmetric with regard to the single axes of symmetry we obtain, altogether, $2n$ permutations of the set of vertices; let us denote the set of these permutations M_n. Prove that M_n has the following properties: 1. If $\boldsymbol{p} \in M_n$, $\boldsymbol{q} \in M_n$, then even $\boldsymbol{qp} \in M_n$; 2. $\boldsymbol{e} \in M_n$; 3. if $\boldsymbol{p} \in M_n$, then $\boldsymbol{p}^{-1} \in M_n$.
5. Any two cyclic permutations of a set of $n(\geqq 1)$ elements whose cycles have no common elements are interchangeable.