V. Rechnoi

EXISTENCE THEOREMS FOR COMMUTATIVE DIAGRAMS

(submitted by B. Shapukov)

ABSTRACT. Given a relation $f \subset A \times B$, there exist two symmetric relations (see [1], Chapter 2) $f^{-1}f \subset A^2, ff^{-1} \subset B^2$. These relations make it possible to formalize definitions and proofs of existence theorems. For example, the equation $h = gf$, where h and g (or h and f) are given maps, admits a solution f (g, respectively.) if and only if $hh^{-1} \subset gg^{-1}(h^{-1}h \supset f^{-1}f)$. Well-known ,,homomorphism theorems" get more general interpretation. Namely, any map can be represented up to bijection as a composition of surjection and injection, and any morphism of diagrams can be represented up to isomorphism as a composition of epimorphism and monomorphism.

In this paper we further develop the scheme from [2] and consider it as an application in category of vector spaces and linear maps.

1. INTRODUCTION AND PRELIMINARIES

We use the symbol ,,$\Rightarrow$" instead of the conditional sentence ,,if ..., then ..." or instead of ,,from ... it follows ...", and we use the symbol ,,$\Leftrightarrow$" instead of ,, ... if and only if ...".

Suppose A and B be two sets. We say that any subset of the direct product $A \times B$ (also an empty set and the set $A \times B$ itself) is called a

---

relation between sets A and B and is denoted by

$$f \subset A \times B.$$

If $(a, b) \in f$, then we say that elements $a \in A$ and $b \in B$ are connected by relation f or simply f-*connected.*

The *inverse relation* $f^{-1} \subset B \times A$ is defined by

$$(a, b) \in f \quad \Leftrightarrow \quad (b, a) \in f^{-1}.$$

It is clear that $(f^{-1})^{-1} = f$.

Given a relation $f \subset A \times B$, let us define for element $a \in A$ the *image* $f(a)$ in B and for element $b \in B$ the *original* $f^{-1}(b)$ in A by

$$(a, b) \in f \quad \Leftrightarrow \quad b \in f(a) \quad \Leftrightarrow \quad a \in f^{-1}(b),$$

and also define for subset $U \subset A$ the *image* $f(U) = \bigcup_{a \in U} f(a)$ and for subset $V \subset B$ the *original* $f^{-1}(V) = \bigcup_{b \in V} f^{-1}(b)$.

A relation f can be defined in the product $A \times A = A^2$. Then it is possible that $f = f^{-1}$. In this case the relation f is called *symmetric.* For example, the *diagonal* of the set A^2, denoted

$$1_A = \left\{ (a_1, a_2) \in A^2 | a_1 = a_2 \right\},$$

is a symmetric relation.

For any two relations $f \subset A \times B$ and $g \subset B \times C$ there exists the *composition* $h \subset A \times C$ (denoted by $h = gf$ and read: h is composition of relations f and g) such that

$$(a, c) \in h \quad \Leftrightarrow \quad f(a) \cap g^{-1}(c) \neq \emptyset.$$

It follows that elements $a \in A$ and $c \in C$ are h-connected if and only if the element a is f-connected to some element $b \in B$ and the elements b and c are g-connected.

The composition of relations has the following properties.

1) For any three relations $f_1 \subset A_1 \times A_2$, $f_2 \subset A_2 \times A_3$ and $f_3 \subset A_3 \times A_4$ (*associativity of compositions*)

$$(f_3 f_2) f_1 = f_3 (f_2 f_1)$$

is valid in the set $A_1 \times A_4$. From this follows, that the composition $f_3 f_2 f_1$ is understood uniquely.

2) The *rule of inversion of composition*:

$$h = gf \quad \Leftrightarrow \quad h^{-1} = (gf)^{-1} = f^{-1} g^{-1}.$$

3) Given a relation $f \subset A \times B$, there exist two symmetric relations

$$f^{-1}f \subset A^2, \quad ff^{-1} \subset B^2$$

such that

$$(a_1, a_2) \in f^{-1}f \quad \Leftrightarrow \quad f(a_1) \cap f(a_2) \neq \emptyset,$$
$$(b_1, b_2) \in ff^{-1} \quad \Leftrightarrow \quad f^{-1}(b_1) \cap f^{-1}(b_2) \neq \emptyset.$$

Proposition 1.1. *Suppose a relation $f \subset A \times B$ satisfies one of inclusions*

$$\begin{array}{llll} (1) & ff^{-1} \subset 1_B, & (2) & f^{-1}f \supset 1_A, \\ (3) & f^{-1}f \subset 1_A, & (4) & ff^{-1} \supset 1_B. \end{array}$$

If inclusion (1) holds (inclusion (2), respectively), then for any element $a \in A$ the image $f(a)$ contains at most (at least) one element from set B. If inclusion (3) holds (inclusion (4), respectively), then for any element $b \in B$ the original $f^{-1}(b)$ contains at most (at least) one element from A.

Proof. First, we have

$$(1) \quad \Rightarrow \quad \forall b_1, b_2 \in f(a), \quad (b_1, b_2) \in ff^{-1} \subset 1_B \quad \Rightarrow \quad b_1 = b_2;$$

from (1) it follows that for any element $a \in A$ the image $f(a)$ is empty or contains only one element from B. Second,

$$(2) \quad \Rightarrow \quad \forall a \in A, \quad (a, a) \in 1_A \subset f^{-1}f \quad \Rightarrow \quad f(a) \neq \emptyset;$$

from (2) it follows that for any element $a \in A$ the image $f(a)$ is non-empty, i.e., contains at least one element from B. The inclusions (3) and (4) for relation f coincide with inclusions (1) and (2) for inverse relation f^{-1}, respectively. $\square$

These inclusions are the basis for the following definitions.

Definition 1.1. The relation $f \subset A \times B$ is said to be
– a *function* from set A to set B, if inclusion (1) holds;
– a *map* from set A to set B, if inclusions (1) and (2) hold;
– an *injection* from set A to set B, if inclusions (1), (2) and (3) hold;
– a *surjection* from set A onto set B, if inclusions (1), (2) and (4) hold;
– a *bijection* between sets A and B, if inclusions (1), (2), (3) and (4) hold;
– a *multi-valued map* from set A to set B, if inclusion (2) holds.

There are also other names: for example, a bijection is also called an one-to-one correspondence between sets A and B, an injection is called an one-to-one map from A to B and a surjection is also called a map from A onto B.

We say that the relation $f \subset A \times B$ is *left-invertible*, if $f^{-1}f = 1_A$, see inclusions (2) and (3), or *right-invertible*, if $ff^{-1} = 1_B$, see inclusions (1) and (4). Thus, an injection is a left-invertible map and a surjection is a right-invertible map. A bijection is both left-invertible and right-invertible.

It follows that *an equality of relations is reducible by injection from left and by surjection from right*, i.e.,
if g is injection, then $gf_1 = gf_2 \Rightarrow g^{-1}gf_1 = g^{-1}gf_2 \Rightarrow f_1 = f_2$;
if f is surjection, then $g_1f = g_2f \Rightarrow g_1ff^{-1} = g_2ff^{-1} \Rightarrow g_1 = g_2$.

A map from one set to another is the most important relation since *any function can be expanded to a map* and *any multi-valued map can be restricted to a map*, i.e.,
if g is a function, then there always exists the map f such that $f \supset g$;
if g is a multi-valued map, then there always exists the map f such that $f \subset g$.

Inclusions (1)–(4) allow to prove some statements without using elements. Let us prove, that for any map f the following equalities hold (we use them below in the proof of Theorem 2.1):

$$ff^{-1}f = f, \qquad f^{-1}ff^{-1} = f^{-1}.$$

By definition, the map f satisfies the inclusions (1) and (2). Then we have

$$(1) \quad \Rightarrow \quad ff^{-1}f = (ff^{-1})f \subset f,$$
$$(2) \quad \Rightarrow \quad ff^{-1}f = f(f^{-1}f) \supset f.$$

Hence, it follows that $ff^{-1}f = f$. From $(ff^{-1}f)^{-1} = f^{-1}ff^{-1} = f^{-1}$ we obtain the second equality.

For a map f the relation $f^{-1}f \subset A^2$ is an equivalence relation on a set A since $f^{-1}f$ satisfies
(*i*) reflexivity: $f^{-1}f \supset 1_A$,
(*ii*) symmetry: $(f^{-1}f)^{-1} = f^{-1}f$,
(*iii*) transitivity: $(f^{-1}f)^2 = f^{-1}ff^{-1}f = f^{-1}f$.
Thus we have a partition of A into equivalence classes.

2. Existence Theorems

Throughout this paper we use the following notation: $f : A \to B$ or $A \xrightarrow{f} B$ denotes a map f from a set A to a set B, while the arrows $\rightarrowtail$ and $\twoheadrightarrow$ are used for an injection and a surjection, respectively.

Suppose the map h is a composition of the maps f and g, i.e. $h = gf$, then a triangular diagram

is called *commutative*.

If one of the maps f and g is missing how we can find the absent map such that the diagram is commutative? Namely, how to solve the equation $h = gf$ with respect to f, if the maps g and h are given, or with respect to g, if f and h are given. The inclusions

$$(5) \qquad hh^{-1} \subset gg^{-1} \qquad\qquad (6) \qquad h^{-1}h \supset f^{-1}f$$

give us an answer to this question.

Theorem 2.1. a) *Suppose the maps g and h are given. Let the inclusion (5) hold. Then there exists a map f such that $h = gf$. Moreover, the map f is obtained by restriction of the multi-valued map $g^{-1}h$.*

b) *Suppose the maps f and h are given. Let the inclusion (6) hold. Then there exists a map g such that $h = gf$. Moreover, the map g is obtained by extension of the function hf^{-1}.*

Proof. a) First, consider the relation $g^{-1}h$. From (5) it follows that

$$(g^{-1}h)^{-1}g^{-1}h = h^{-1}gg^{-1}h \supset h^{-1}hh^{-1}h = h^{-1}h \supset 1_A.$$

It means that $g^{-1}h$ satisfies inclusion (2). Hence, the relation $g^{-1}h$ is a multi-valued map which we may restrict to a map f. Then we have

$$f \subset g^{-1}h \quad \Rightarrow \quad gf \subset gg^{-1}h \subset h$$

(since the map g satisfies inclusion (1)) and, on the other hand,

$$f^{-1} \subset h^{-1}g \quad \Rightarrow \quad h \subset hf^{-1}f \subset hh^{-1}gf \subset gg^{-1}gf \subset gf$$

(since the condition (5) holds and the map f satisfies inclusion (2)). Finally, from the inclusions $h \supset gf$ and $h \subset gf$ we obtain the equality $h = gf$.

b) Consider the relation hf^{-1}. From (6) it follows that

$$hf^{-1}(hf^{-1})^{-1} = hf^{-1}fh^{-1} \subset hh^{-1}hh^{-1} = hh^{-1} \subset 1_C.$$

It means that hf^{-1} satisfies inclusion (1). Therefore, the relation hf^{-1} is a function which is possible to extend to a map g. Then we have

$$g \supset hf^{-1} \quad \Rightarrow \quad gf \supset hf^{-1}f \supset h$$

(since the map f satisfies inclusion (2)) and, on the other hand,

$$g^{-1} \supset fh^{-1} \quad \Rightarrow \quad h \supset gg^{-1}h \supset gfh^{-1}h \supset gff^{-1}f \supset gf$$

(since the condition (6) holds and the map g satisfies inclusion (1)). Similarly, from the inclusions $h \supset gf$ and $h \subset gf$ we obtain the equality $h = gf$. $\qquad\square$

Remark. Notice, that we don't use elements in proof of Theorem 2.1. But if we use elements, then in the case a) the inclusion (5) is equivalent to the inclusion $h(A) \subset g(B)$. We construct the map $f : A \to B$ so that for element $a \in A$ the image $f(a) \in B$ has to satisfy the condition $g(f(a)) \in h(A)$. Because of $h(A) \subset g(B)$ it is possible that the condition $g(f(a)) \in h(A)$ holds for each element $a \in A$. In the case b) the set A has two equivalence relations $f^{-1}f$ and $h^{-1}h$. Thus we have two partitions of A into equivalence classes. From (6) it follows that the first partition is a refinement of the second one. For $b \in f(A)$ we have $g(b) = hf^{-1}(b)$ since hf^{-1} is a function. For $b \in B$ outside $f(A)$ we choose $g(b)$ arbitrary.

However, it is preferable to use the inclusions (1)–(6) instead of using elements of the sets. As they say, these inclusions formalize proofs.

Consecuence 1. Suppose the inclusion (5) holds and the map g is an injection. Then the relation $g^{-1}h$ is a map: $g^{-1}h(g^{-1}h)^{-1} = g^{-1}hh^{-1}g \subset g^{-1}g = 1_B$ (besides (2) inclusion (1) also holds for this relation), and the map f is defined uniquely by $f = g^{-1}h$.

Consecuence 2. Suppose the inclusion (6) holds and the map f is a surjection. Then the relation hf^{-1} is a map: $(hf^{-1})^{-1}hf^{-1} = fh^{-1}hf^{-1} \supset ff^{-1} = 1_B$ (besides (1) inclusion (2) also holds for this relation), and the map g is defined uniquely by $g = hf^{-1}$.

Consecuence 3. If g is a surjection, $gg^{-1} = 1_C$, then inclusion (5) is valid automatically and there always exists the map f such that $h = gf$.

Consecuence 4. If f is an injection, $f^{-1}f = 1_A$, then inclusion (6) is valid automatically and there always exists the map g such that $h = gf$.

Consecuence 5. For a composition $h = gf$ with h injective it follows that f is also injective:

$$h^{-1}h \subset 1_A \quad \Rightarrow \quad f^{-1}f \subset f^{-1}g^{-1}gf = h^{-1}h \subset 1_A.$$

Similarly, if h is a surjection, then g is a surjection too:

$$hh^{-1} \supset 1_C \quad \Rightarrow \quad gg^{-1} \supset gff^{-1}g^{-1} = hh^{-1} \supset 1_C.$$

In particular, if $gf = 1_A$, then the map f is always injection and the map g is always surjection. In this case f is called a *section* of the surjection g, while g is called a *retraction* of the injection f.

Definition 2.1. If in the composition $h = gf$ the map f is a surjection and g is an injection, the commutative diagram
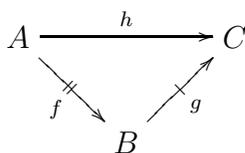
is said to represent a *canonical representation* of the map h.

Theorem 2.2. *For any map $h : A \to C$ the canonical representation is defined up to natural bijection. It means if h has two canonical representations $h = g_1 f_1$ and $h = g_2 f_2$, see diagram below, then there exists the unique bijection $\beta : B_1 \to B_2$ such that the entire diagram*
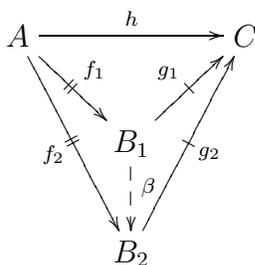
is commutative, i.e., $f_2 = \beta f_1$ and $g_1 = g_2 \beta$.

Proof. Since $h = g_1 f_1 = g_2 f_2$ we have

$$hh^{-1} = g_1 f_1 f_1^{-1} g_1^{-1} = g_2 f_2 f_2^{-1} g_2^{-1} \quad \Leftrightarrow \quad g_1 g_1^{-1} = g_2 g_2^{-1}$$

(since f_1 and f_2 are surjections) and

$$h^{-1}h = f_1^{-1} g_1^{-1} g_1 f_1 = f_2^{-1} g_2^{-1} g_2 f_2 \quad \Leftrightarrow \quad f_1^{-1} f_1 = f_2^{-1} f_2$$

(since g_1 and g_2 are injections). The first relation means that for triangle $B_1 B_2 C$ the inclusion (5) holds, i.e., $g_1 g_1^{-1} \subset g_2 g_2^{-1}$. Analogously, the second relation means that for triangle $AB_1 B_2$ the inclusion (6) holds, i.e., $f_2^{-1} f_2 \supset f_1^{-1} f_1$. Hence, from Theorem 2.1 it follows that the maps

$\beta_1 : B_1 \to B_2$ and $\beta_2 : B_1 \to B_2$ are defined in triangles $B_1 B_2 C$ and $A B_1 B_2$, respectively. Thus we have

$$g_1 = g_2 \beta_1, \quad f_2 = \beta_2 f_1, \quad h = g_2 \beta_1 f_1 = g_2 \beta_2 f_1.$$

If we now reduce the last equality by surjection f_1 from right and by injection g_2 from left, then we obtain $\beta_1 = \beta_2 = \beta$. From Consequences 1 and 5 it follows that β is uniquely defined bijection. $\square$

The next two theorems are generalizations of Theorem 2.

Theorem 2.3. *Suppose we have a prism diagram with faces I, II and III:*
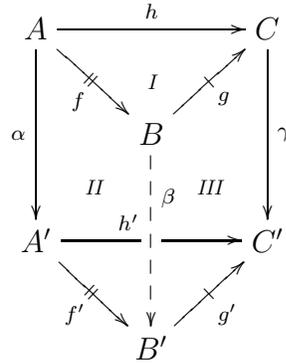
where the face I is a commutative square, i.e., $\gamma h = h' \alpha$. The maps h and h' have canonical representations $h = gf$ and $h' = g'f'$, respectively. Then there exists the unique map β such that the faces II and III are commutative.

Proof. First, let us consider the commutative triangle $AA'C'$ on the face I, where arrow AC' is a composition γh. The inclusion (5) is valid for this triangle, i.e.,

$$\gamma h (\gamma h)^{-1} \subset h' h'^{-1}$$
$$\Leftrightarrow \quad \gamma h h^{-1} \gamma^{-1} \subset h' h'^{-1}$$
$$\Leftrightarrow \quad \gamma g f f^{-1} g^{-1} \gamma^{-1} \subset g' f' f'^{-1} g'^{-1}$$
$$\Leftrightarrow \quad \gamma g g^{-1} \gamma^{-1} \subset g' g'^{-1}$$
$$\Leftrightarrow \quad \gamma g (\gamma g)^{-1} \subset g' g'^{-1}$$

(since f and f' are surjections, $ff^{-1} = 1_B$, $f'f'^{-1} = 1_{B'}$). Moreover, this inclusion is also inclusion (5) for triangle $BB'C'$, where arrow BC' is a composition γg. Hence, there exists the unique map β_1 such that

$$\gamma g = g' \beta_1$$

(see Theorem 2.1 and Consequence 1).

Second, let us consider the commutative triangle ACC' on the face I, where arrow AC' is a composition $h'\alpha$. The inclusion (6) is valid for this triangle, i.e.,

$$(h'\alpha)^{-1}h'\alpha \supset h^{-1}h$$
$$\Leftrightarrow \quad \alpha^{-1}h'^{-1}h'\alpha \supset h^{-1}h$$
$$\Leftrightarrow \quad \alpha^{-1}f'^{-1}g'^{-1}g'f'\alpha \supset f^{-1}g^{-1}gf$$
$$\Leftrightarrow \quad \alpha^{-1}f'^{-1}f'\alpha \supset f^{-1}f$$
$$\Leftrightarrow \quad (f'\alpha)^{-1}f'\alpha \supset f^{-1}f$$

(since g and g' are injections, $g^{-1}g = 1_B, g'^{-1}g' = 1_{B'}$). Moreover, this inclusion is also inclusion (6) for triangle ABB', where arrow AB' is a composition $f'\alpha$. Hence, there exists the unique map β_2 such that

$$f'\alpha = \beta_2 f$$

(see Theorem 2.1 and Consequence 2).

Now we write f on the right of the both sides of equality $\gamma g = g'\beta_1$ and g' on the left of the both sides of equality $f'\alpha = \beta_2 f$. From $\gamma gf = g'f'\alpha$ (or $\gamma h = h'\alpha$) it follows that

$$g'\beta_1 f = g'\beta_2 f.$$

By using reduction we obtain $\beta_1 = \beta_2 = \beta$ (since f is a surjection and g' – an injection). $\qquad\square$

Definition 2.2. If in the prism diagram from Theorem 3 the faces I, II and III are commutative, a triple (α, β, γ) is said to define the *morphism of two diagrams ABC* and $A'B'C'$. A morphism is a *mono*morphism (*epi*morphism) of diagrams, if α, β and γ are injections (surjections, respectively). A morphism, which is both epi- and monomorphism, is called an *iso*morphism of diagrams. A *canonical representation of morphism of diagrams ABC* and $A'B'C'$ is it presentation in composition of epimorphism and monomorphism.

Theorem 2.4. *The canonical representation of morphism of diagrams ABC and $A'B'C'$ exists up to isomorphism. It means that there exists a*

commutative diagram UVW such that the entire diagram
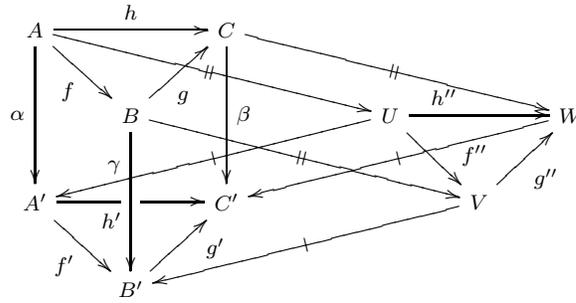
is commutative and the diagram UVW is defined up to isomorphism.

Proof. The sets U, V and W are obtained up to isomorphism by canonical representation of the maps α, β and γ, respectively, see Theorem 2.2. Applying Theorem 2.3 for each prism diagram $AUA'BVB'$, $BVB'CWC'$ and $AUA'CWC'$ separately we obtain maps f'', g'' and h''. It is easily proved that $h'' = g''f''$ and the triangle UVW is defined up to isomorphism. $\square$

Theorem 2.5. *For any commutative square $ACC'A'$ there exists a decomposition on blocks:*
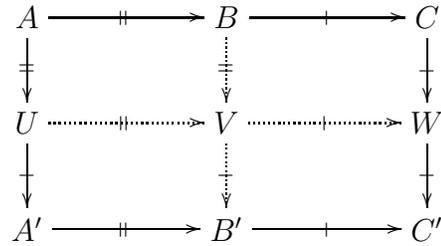
where the northwest block $ABVU$ consists of surjections, while the southeast block $VWC'B'$ consists of injections. This decomposition is defined up to isomorphism.

Proof. This diagram is a particular case of diagram from Theorem 2.4, if triangles ABC, $A'B'C'$ and UVW define the canonical distributions of the maps h, h' and h'', respectively. $\square$

Let us apply the map $h : A \to A$ repeatedly to the set A. Let $h = g_1 f_1$ be a canonical representation of h. Then we may construct a map $h_1 = f_1 g_1$, which has a canonical representation $h_1 = g_2 f_2$. Thus, the canonical representation of the second iteration is

$$h^2 = g_1 f_1 g_1 f_1 = g_1 h_1 f_1 = g_1 g_2 f_2 f_1.$$

Continuing in the same way, we see that the result of iterations m times is

$$h^m = g_1 g_2 ... g_m f_m ... f_2 f_1,$$

where $f_m ... f_2 f_1$ and $g_1 g_2 ... g_m$ are compositions of surjections and injections, respectively.

Theorem 2.6. *Let h be a map from set A to itself:*

$$h : A \to A.$$

Let us form the sequence of maps

$$h, h_1, h_2, ..., h_{k-1}, h_k, ...,$$

where $h_1 = f_1 g_1 : B_1 \to B_1$ is defined after canonical representation $h = g_1 f_1$, and $h_k = f_k g_k : B_k \to B_k$ after canonical representation $h_{k-1} = g_k f_k, k = 2, 3, ...$ If A is a finite set, then there exist the minimal integers m and n, such that

$$h^{m+n} = h^m \quad \Leftrightarrow \quad (h_m)^n = 1_{B_m}$$
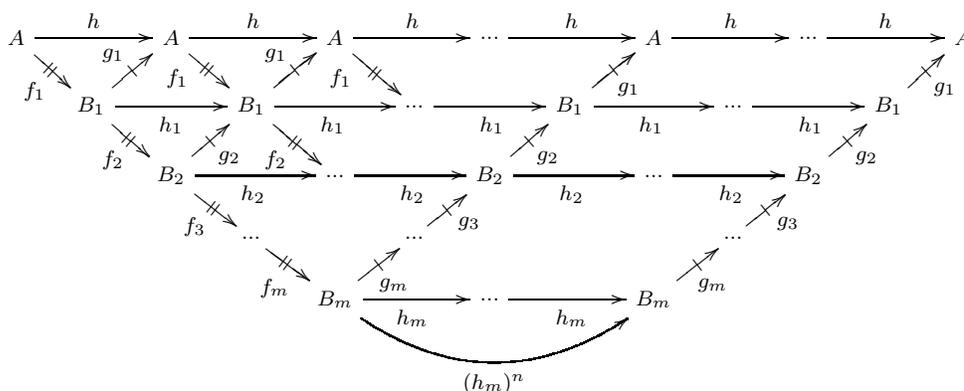
It means, that after n steps the iteration h^m repeats if and only if $h_m : B_m \to B_m$ is a bijection and $(h_m)^n$ is identical map.

Proof. Let us show using mathematical induction, that the iteration h^m admits the canonical representation

$$h^m = g_1 g_2 ... g_m f_m ... f_2 f_1.$$

Suppose it is true for h^{m-1}. Then from $g_k f_k = f_{k-1} g_{k-1}, k = 2, 3, ..., m$, it follows that

$$h^m = h^{m-1} h = g_1 g_2 ... g_{m-1} f_{m-1} ... f_2 f_1 (g_1 f_1) =$$
$$= g_1 g_2 ... g_{m-1} f_{m-1} ... f_2 (f_1 g_1) f_1 = g_1 g_2 ... g_{m-1} f_{m-1} ... f_2 (g_2 f_2) f_1 =$$
$$= g_1 g_2 ... g_{m-1} f_{m-1} ... (f_2 g_2) f_2 f_1 = g_1 g_2 ... g_{m-1} f_{m-1} ... (g_3 f_3) f_2 f_1 = ... =$$
$$= g_1 g_2 ... g_m f_m ... f_2 f_1.$$

The iteration h^{m+n} admits the canonical representation

$$h^{m+n} = g_1 g_2 ... g_m (h_m)^n f_m ... f_2 f_1.$$

The equality $h^{m+n} = h^m$ means that

$$g_1 g_2 ... g_m (h_m)^n f_m ... f_2 f_1 = g_1 g_2 ... g_m f_m ... f_2 f_1.$$

If we reduce both sides of the last equality by surjections $f_1, f_2, ..., f_m$ from right and by injections $g_1, g_2, ..., g_m$ from left, we obtain $(h_m)^n = 1_{B_m}$.

Such integers m and n exist, since the number of elements in the sets $A, B_1, B_2, ...$ not increase. $\qquad \square$

3. CANONICAL REPRESENTATION OF MATRIX

Let us show, that a linear map between two finite-dimensional vector spaces has a canonical representation to composition of epimorphism and monomorphism, and this representation is defined up to isomorphism. It means, that the diagram from Theorem 2.2 remains the same for vector spaces and linear maps.

Let A and C be vector spaces of dimensions n and m, respectively. Then the linear map $h : A \to C$ is defined by $m \times n$-matrix H. If h is an epimorphism (monomorphism), then the rows (columns, respectively) of H are linearly independent. If h is an isomorphism, then the matrix H is nonsingular.

Theorem 3.1. *Suppose p is the rank of matrix H. Then the matrix H can be represented as a product $H = GF$, where F is a surjective $p \times n$-matrix and G is an injective $m \times p$-matrix. Therefore, for any other product of surjective $p \times n$-matrix F' and injective $m \times p$-matrix G' such that $H = G'F'$, there exists a non-degenerated $p \times p$-matrix Q such that $G' = GQ^{-1}$, $F' = QF$ and $H = (GQ^{-1})(QF)$.*

Proof. Without loss of generality it can be assumed that the matrix H is a block matrix

$$H = \left(\begin{array}{c|c} U & Y \\ \hline X & V \end{array} \right),$$

where block U is a rank minor. The blocks U, X, Y and V are matrices of orders $p \times p$, $(m-p) \times p$, $p \times (n-p)$ and $(m-p) \times (n-p)$, respectively, with respect to the order of $m \times n$-matrix H. The southeast block V may be expressed by the blocks X, U and Y:

$$V = XU^{-1}Y.$$

Indeed, the columns $\begin{pmatrix} Y \\ -\,-\,- \\ V \end{pmatrix}$ may be written as linear combinations

of the columns $\begin{pmatrix} U \\ -\,-\,- \\ X \end{pmatrix}$. In other words, there exist $p \times (n-p)$-matrix

Z, such that

$$\begin{pmatrix} Y \\ -\,-\,- \\ V \end{pmatrix} = \begin{pmatrix} U \\ -\,-\,- \\ X \end{pmatrix}(Z)$$

or $Y = UZ$ and $V = XZ$. Since U is nonsingular, we have $Z = U^{-1}Y$
and $V = XU^{-1}Y$. By the way, the rows $\begin{pmatrix} X & | & V \end{pmatrix}$ may be written as
linear combinations of the rows $\begin{pmatrix} U & | & Y \end{pmatrix}$:

$$\begin{pmatrix} X & | & V \end{pmatrix} = \begin{pmatrix} XU^{-1} \end{pmatrix}\begin{pmatrix} U & | & Y \end{pmatrix}.$$

Thus, we have

$$H = \begin{pmatrix} U \\ -\,-\,- \\ X \end{pmatrix} \cdot \begin{pmatrix} E_p & | & U^{-1}Y \end{pmatrix} = \begin{pmatrix} E_p \\ -\,-\,- \\ XU^{-1} \end{pmatrix} \cdot \begin{pmatrix} U & | & Y \end{pmatrix},$$

where E_p is a unit matrix of order p. In both expressions of H the right
matrices are surjective and the left matrices are injective.

Let us consider the diagram from Theorem 2.2. Now the arrows h, f, g,
f', g' and β are expressed by the matrices $H, F, G, F' = QF, G' = GQ^{-1}$
and Q, respectively:

$$\begin{array}{ccc}
A & \xrightarrow{\quad H \quad} & C \\
\end{array}$$

(diagram: A top-left, C top-right, arrow H from A to C; F from A down to B_1, G from B_1 up to C; F' from A down to B_2, G' from B_2 up to C; Q from B_1 down to B_2.)
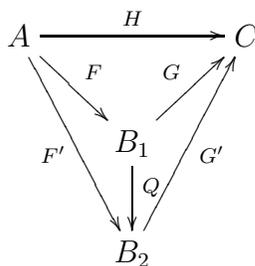
where Q is non-degenerated matrix. Thus, from $H = GF$ we obtain
any other decomposition $H = (GQ^{-1})(QF)$ with respect to arbitrary
non-degenerated matrix Q. $\qquad\square$

The following table shows the especial role of matrices XU^{-1} and
$U^{-1}Y$:

Rows	Columns
$\mathrm{Im}h^* \subset A^*$	$\mathrm{Ker}h \subset A$
$\left(E_p \,\middle|\, U^{-1}Y\right)$	$\begin{pmatrix} -U^{-1}Y \\ --- \\ E_{m-p} \end{pmatrix}$
$\mathrm{Ker}h^* \subset C^*$	$\mathrm{Im}h \subset C$
$\left(-XU^{-1} \,\middle|\, E_{n-p}\right)$	$\begin{pmatrix} E_p \\ --- \\ XU^{-1} \end{pmatrix}$

The basis of kernel $\mathrm{Ker}h$ and image $\mathrm{Im}h$ of a linear map $h : A \to C$ are represented by the columns of right hand side matrices. It is clear that the matrices from the second column annihilate the matrices from the first column. It means that the image $\mathrm{Im}h^*$ and kernel $\mathrm{Ker}h^*$ of the dual map $h^* : C^* \to A^*$ are represented by the rows of the left hand side matrices, respectively.

4. Exponential of matrix

For any square matrix H of order n (as an element of Lie algebra $gl(n, \mathbb{R})$ of a Lie group $GL(n, \mathbb{R})$) there exists the exponential

$$e^{tH} = \sum_{k=0}^{\infty} \frac{(tH)^k}{k!},$$

which is a one-parameter subgroup of $GL(n, \mathbb{R})$. Moreover, in space $\mathbb{R}^n$ there exists a linear vector field X (dynamic system) generated by the matrix H. The *flow* of the vector field X is defined by the *exponential law* (see [3])

$$U' = HU \quad \Rightarrow \quad U_t = e^{tH}U$$

and is denoted by $a_t : U \mapsto U_t$. It means, that an arbitrary point $U \in \mathbb{R}^n$ moves along its own trajectory U_t with initial velocity U'.

The canonical representation of the matrix H (see Theorem 3.1) allows to find the exponential e^{tH} and the flow a_t (see the next example).

Example. Let

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 1 & 3 & 2 \end{pmatrix}$$

be a map from set $A = \{1, 2, 3, 4, 5\}$ to itself. Let us represent the map h as a square matrix $H = (h_{ij})$ by

$$h_{ij} = \begin{cases} 1, & \text{if } j = h(i), \\ 0, & \text{if } j \neq h(i), \end{cases} \quad i, j = 1, ..., 5.$$

Corresponding to the scheme from Theorem 2.6 the equality of iterations $h^4 = h^2$ can be written

$$h^4 = g_1 g_2 h_2^2 f_2 f_1,$$
$$H^4 = G_1 G_2 H_2^2 F_2 F_1,$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Each matrix from the last equality corresponds to a linear map: endomorphism $H : \mathbb{R}^5 \to \mathbb{R}^5$, two epimorphisms $F_1 : \mathbb{R}^5 \to \mathbb{R}^3$, $F_2 : \mathbb{R}^3 \to \mathbb{R}^2$, automorphism $H_2 : \mathbb{R}^2 \to \mathbb{R}^2$ and two monomorphisms $G_2 : \mathbb{R}^2 \to \mathbb{R}^3$, $G_1 : \mathbb{R}^3 \to \mathbb{R}^5$ (in this paper, matrices and corresponding linear maps are denoted by the same symbol). After two iterations we have

$$\operatorname{Ker} H \subset \operatorname{Ker} H^2 = \operatorname{Ker} H^3, \quad \operatorname{Im} H \supset \operatorname{Im} H^2 = \operatorname{Im} H^3.$$

Let $\{x^i\}$ be the coordinates of space $\mathbb{R}^5$ according to the usual basis $\{e_i\}, i = 1, ..., 5$. Then the kernel $\operatorname{Ker} H$ is a two-dimensional coordinate plane $x^1 = x^2 = x^3 = 0$, the kernel $\operatorname{Ker} H^2$ is a three-dimensional coordinate space $x^1 = x^2 = 0$, the image $\operatorname{Im} H$ is a three-dimensional hyperplane spanned by vectors $\{e_2 + e_3, e_1 + e_5, e_4\}$ and $\operatorname{Im} H^2$ is a two-dimensional plane spanned by vectors $\{e_2 + e_3, e_1 + e_4 + e_5\}$. The second iteration of the automorphism H_2 is the identical map of the plane $\operatorname{Im} H^2$. Thus, from Theorem 2.6 it follows that

$$H^4 = H^2 \quad \Leftrightarrow \quad H_2^2 = E_2,$$

where E_2 is a unit matrix of order 2.

This result is useful in the next situation. Let us consider the matrix H as an element of Lie algebra $gl(5, \mathbb{R})$. Then the exponential e^{tH} is a one-parameter subgroup of Lie group $GL(5, \mathbb{R})$. Since $H^4 = H^2$ we have

$$e^{tH} = E_5 - H^2 + (H - H^3)t + H^2 \cosh t + H^3 \sinh t.$$

The linear vector field corresponding to the matrix H is

$$X = x^1\left(\frac{\partial}{\partial x^2} + \frac{\partial}{\partial x^3}\right) + x^2\left(\frac{\partial}{\partial x^1} + \frac{\partial}{\partial x^5}\right) + x^3\frac{\partial}{\partial x^4}.$$

Note that all vectors in X are parallel to $\mathrm{Im}H$. The field X has a *canonical parameter*

$$s = \frac{x^1 - x^4}{x^2 - x^3}$$

and four *invariants*

$$I_1 = x^1 - x^5, \quad I_2 = x^2 - x^3, \quad I_3 = \frac{1}{2}\ln\left|(x^1)^2 - (x^2)^2\right|, \quad I_4 = s - \frac{1}{2}\ln\left|\frac{x^1 + x^2}{x^1 - x^2}\right|.$$

The exponential law $U' = HU \Rightarrow U_t = e^{tH}U$ defines a flow $a_t : U \mapsto U_t$ (see e^{tH}),

$$U_t = U - U'' + (U' - U''')t + U''\cosh t + U'''\sinh t,$$

generated by vector field X. In particular, the points, represented by basis vectors, move along trajectories

$$(e_1)_t = -e_4 - e_5 + (e_1 + e_4 + e_5)\cosh t + (e_2 + e_3)\sinh t,$$
$$(e_2)_t = -e_3 - e_4 t + (e_2 + e_3)\cosh t + (e_1 + e_4 + e_5)\sinh t,$$
$$(e_3)_t = e_3 + e_4 t,$$
$$(e_4)_t = e_4,$$
$$(e_5)_t = e_5.$$

It means that under the action of a_t the points $U \in \mathrm{Ker}H$ are fixed (see $(e_4)_t$ and $(e_5)_t$), the points $U \in \mathrm{Ker}H^2\backslash\mathrm{Ker}H$ move along the straight lines (see $(e_3)_t$) and the points $U \in \mathbb{R}^2\backslash\mathrm{Ker}H^2$ participate in a hyperbolic rotation in the plane $\mathrm{Im}H^2$ (see $(e_1)_t$ and $(e_2)_t$). Note that the hyperbolic rotation in the plane $\mathrm{Im}H^2$ can be described using the basis vectors:

$$(e_1 + e_4 + e_5)_t = (e_1 + e_4 + e_5)\cosh t + (e_2 + e_3)\sinh t,$$
$$(e_2 + e_3)_t = (e_2 + e_3)\cosh t + (e_1 + e_4 + e_5)\sinh t.$$

The coordinate transformation $(x^1, x^2, x^3, x^4, x^5) \mapsto (s, I_1, I_2, I_3, I_4)$ transforms the basis $\{e_i\}$ into another *invariant* basis: a coframe $(ds, dI_1, dI_2, dI_3, dI_4)$

and a frame

$$\frac{\partial}{\partial s} = X,$$

$$\frac{\partial}{\partial I_1} = -\frac{\partial}{\partial x^5},$$

$$\frac{\partial}{\partial I_2} = -\frac{\partial}{\partial x^3} - s\frac{\partial}{\partial x^4},$$

$$\frac{\partial}{\partial I_3} = x^1\left(\frac{\partial}{\partial x^1} + \frac{\partial}{\partial x^5}\right) + x^2\left(\frac{\partial}{\partial x^2} + \frac{\partial}{\partial x^3} + \frac{\partial}{\partial x^4}\right),$$

$$\frac{\partial}{\partial I_4} = -x^1\left(\frac{\partial}{\partial x^2} + \frac{\partial}{\partial x^3}\right) - x^2\left(\frac{\partial}{\partial x^1} + \frac{\partial}{\partial x^4} + \frac{\partial}{\partial x^5}\right).$$

This transformation follows from Jacobi matrix and its inverse:

$$\begin{pmatrix} \frac{1}{I_2} & -\frac{s}{I_2} & \frac{s}{I_2} & -\frac{1}{I_2} & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 & 0 \\ \frac{x^1}{(x^1)^2-(x^2)^2} & -\frac{x^2}{(x^1)^2-(x^2)^2} & 0 & 0 & 0 \\ \frac{1}{I_2}+\frac{x^2}{(x^1)^2-(x^2)^2} & -\frac{s}{I_2}-\frac{x^1}{(x^1)^2-(x^2)^2} & \frac{s}{I_2} & -\frac{1}{I_2} & 0 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} x^2 & 0 & 0 & x^1 & -x^2 \\ x^1 & 0 & 0 & x^2 & -x^1 \\ x^1 & 0 & -1 & x^2 & -x^1 \\ x^3 & 0 & -s & x^2 & -x^2 \\ x^2 & -1 & 0 & x^1 & -x^2 \end{pmatrix}.$$

The operators $\left(\frac{\partial}{\partial s}, \frac{\partial}{\partial I_1}, \frac{\partial}{\partial I_2}, \frac{\partial}{\partial I_3}, \frac{\partial}{\partial I_4}\right)$ commute with vector field X.

Hence, these operators are *infinitesimal symmetries* of X. From $\frac{\partial}{\partial s} = X$ it follows that the flow generated by X becomes a *group of translations* $s \mapsto s+t$. In the coordinates (s, I_1, I_2, I_3, I_4) the trajectories are the lines s and the classification of these trajectories makes no sense.

We have done the following seven steps:
a) took a map h from set A (consists of 5 elements) to itself;
b) represented the map h as 5×5-matrix H with the rank 3;
c) considered the matrix H as an element of Lie algebra $gl(5, \mathbb{R})$;
d) found the one-parameter subgroup e^{tH} of Lie group $GL(5, \mathbb{R})$;
e) in space $\mathbb{R}^5$ the exponential e^{tH} defines a flow a_t generated by corresponding vector field X;
f) the classification of the trajectories depends on kernels $\mathrm{Ker}H$ and $\mathrm{Ker}H^2$;

g) in curvilinear coordinates such as the invariant coordinates (s, I_1, I_2, I_3, I_4) the flow simplifies, but the classification makes no sense.

The steps b)–g) can be applied to any square matrix with an arbitrary rank.

Acknowledgment

References

[1] N. Bourbaki, *Éléments de mathématique*, Fasc. XVII, 1$^{\text{ère}}$ partie, livre I, Théorie des ensembles, Paris, Hermann, 1960.

[2] M. Rahula, ,,About Theory of Maps", *Webs and Quasigroups*, University of Kalinin, (1981), pp 136-153. (in Russian).

[3] M. Rahula, *Vector Fields and Symmetries*, Tartu University press, Tartu, 2004 (in Russian).

Institute of Pure Mathematics, Faculty of Mathematics and Computer Science, University of Tartu, J. Liivi Str., 2-218, 50409 Tartu, Estonia

E-mail address: vitali@math.ut.ee