STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

Report ZW 1962-015

ON COMMUTATIVITY OF TRANSFORMATIONS

by

Zdeněk Hedrlín

November 1962

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

Foreword

In this report the properties of commuting transformations are studied. Without loss of generality we may always assume that the transformations under consideration form a commutative semigroup that contains the identity map. For any set of pairwise commuting mappings of a set X into itself generates a commutative semigroup; and the identity may always be added to a commutative semigroup without damage to the commutativity.

The concept of a commutative transformation semigroup (F;X) of transformations of a set X into itself involves, in a certain sense, two different notions: the set X that is transformed under F, and the abstract commutative semigroup F (with composition as the operation of multiplication). The relation between these two notions will be studied here. There are then a few questions that arise naturally.

In the first place we may remark that every abstract commutative semigroup (A,.) defines in a natural way a semigroup of transformation of the set A into itself. If, for $a \in A$, the mapping m(a) of A into itself is defined by

$$m(a)(b) = a \cdot b,$$

and if furthermore

$$m(A) = \left\{ m(a) \ : \ a \in A \right\},$$

then the transformation semigroup (m(A),A) is almost the same as the abstract semigroup (A,.).

Of course a converse of this construction should be considered: how much can be said about a commutative transformation semigroup, using only results about abstract semigroups. The second chapter is devoted to a partial answer of this question. (In chapter 1 a number of definitions and the basic notations are introduced.) The crucial proposition in chapter 2 is proposition 2.2.1. It states that under a certain condition (F;X) can be considered as an abstract semigroup, F being identified with X in a natural way. This condition is the following: There must exist a point in X, whose orbit under F is all of X. If this condition is not met, we can in any case consider (F;X) as a subset of the product of a number of abstract semigroups; the number of semigroups needed in this product equals the number of orbits under F, necessary to cover X (cf. 2.5.4.). This result enables us to give estimates for the cardinal number of a commutative transformation semigroup.

In section 2.6 the results are applied to topological spaces, while in 2.7 we show that some well-known computing processes are based on the notion of commutativity.

In chapter 3 the approach is the following. It turns out that there are certain subsets of X, called cycles, with the property that the mapping of F, if restricted in a suitable way to such a cycle, form a group. These cycles are pairwise disjoint, and cover X. They are considered as the point of a new set Γ . These elements of Γ can be considered as groups, owing to the theory developed in chapter 2. In this way we arrive at some natural homomorphisms of the semigroup F into products of groups with zero (cf. 3.2.5.). Also a theorem on relations between the cycles is derived (cf. 3.3.1.). It seems interesting that corollary 3.3.4 has a formal resemblance to the Gelfand-Naimark theorem, dealing with the homomorphic representation of a complex Banach algebra B as a space of complex-valued continuous functions on the (compact) maximal ideal space of B. This resemblance is as follows. In 1.2.4. it is proved that the maximal invariant sets under a transformation semigroup play the role of maximal ideals. In 3.1.8.,on the other hand, it is shown that there is a one to one correspondence between the maximal invariant sets and the maximal cycles. Furthermore we may remark that the complex numbers are a group with zero under multiplication. Now corollary 3.3.4. states that there exists a homomorphism φ of F into the set of functions, defined on the space of all maximal cycles under F, and taking values in groups with zero (one to every maximal cycle). Theorem 3.3.5. also reminds one, by its structure, of the characterization of the kernel, of the homomorphism from the Gelfand Naimark theorem. Of course our results can not be applied to Banach algebras except after some suitable "linearisation".

The end of the third chapter is concerned with applications to the theory of abstract commutative semigroups.

We mentioned already that to every commutative transformation semigroup we can associate a system of groups Γ . This system Γ can be partially ordered in a natural way. In this way a partially ordered set, called the skeleton, is correlated to every commutative transformation semigroup. In chapter IV we study the relation between a semigroup and its skeleton. A few examples are given, and in theorem 4.3.3. it is shown which partially ordered sets can occur as skeletons of commutative transformation semigroups.

In chapter 5 there are some results concerning the existence of a common fixed point of a system of commutative mappings. This chapter was inspired by the so-called "Isbell problem". This problem is as follows: is it true or not that every two commuting continuous mappings of the closed unit segment into itself have a common fixed point? This problem seems still to be unsolved. In theorem 5.2.2. we prove a result that assures the existence of a common fixed point under certain very general conditions. Theorem 5.2.4. deals specifically with the existence of a common fixed point on the closed unit segment.

In chapter 6, finally, the above methods are applied in order to estimate the number of mappings in a commutative system of transformations of a finite set into itself. The best estimate is obtained in 6.1.13. This estimate is simplified (but also made less precise) in 6.1.14.

I wish to express my gratefulness to Prof. M. Katětov, who stimulated the research, the results of which are contained in this report, and to Prof. J. de Groot, who enabled me to finish this work in the pleasant atmosphere of the Mathematical Centre in Amsterdam. Furthermore I wish to thank my colleagues C. Sc. Zdeněk Frolík and Mrs. A.B. Paalman-de Miranda for many good advices they gave me during my work.

I want to thank especially P.C. Baayen, who was of great help to me. The whole of chapter 3 was written in collaboration with him. We also worked out together in close cooperation the sum- and product-constructions. The example of a non-realisable skeleton is also due to Mr. Baayen. Furthermore he gave me much assistance by reading through and checking the whole of this report, and by improving some of the proofs.

Amsterdam, November 29, 1962

Zdeněk Hedrlín

1. Definitions and notation

1.1. Systems of mappings, mappings restricted to subsets, invariant sets

1.1.1. If X is a set, then X^X will denote the set of all mappings of X into X. If $F \in X^X$, we shall write sometimes $(F;X)$ instead of F to stress the relation between F and X.
If $f,g \in X$, then $f \circ g$ denotes the mapping

$$f \circ g\,(x) = f(g(x)) \qquad \text{for every } x \in X.$$

This operation, called composition of mappings, is associative:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

for all $f, g, h \in X^X$.
The identity map of X onto itself is denoted by i. It has the property

$$f \circ i = i \circ f = f \qquad \text{for all } f \in X^X.$$

If $f \in X^X$, we define

$$\overset{o}{f} = i \;;$$

$$\overset{n+1}{f} = \overset{n}{f} \circ f \;, \quad \text{for } n=1,2,\ldots \;.$$

It follows from the associativity of composition of mappings that

$$\overset{m+n}{f} = \overset{m}{f} \circ \overset{n}{f}$$

An element $f \in X^X$ is called invertible if there exists an $\overset{-1}{f} \in X^X$ such that

$$f \circ \overset{-1}{f} = \overset{-1}{f} \circ f = i \;;$$

the mapping $\overset{-1}{f}$ then is uniquely determined and is called the inverse of f.
A mapping $f \in X^X$ is invertible if and only if it is both 1.1 and onto.

A subset F of X^X is called a commutative system of mappings of X into itself if for any $f,g \in F$,

$$f \circ g = g \circ f.$$

A system $F \subset X^X$ is called a maximal commutative system, if it is a commutative system and if $F \subset G \subset X^X$, where G is commutative, implies that $F=G$.

1.1.2. If $f \in X^X$ and $Y \subset X$, then the set $\{f(y) : y \in Y\}$ will be denoted by $f(Y)$. If $F \subset X^X$ and $x \in X$, the set $\{f(x) : f \in F\}$ will be denoted by $F(x)$; this set will be called the orbit of x under F. If $F \subset X^X$ and $Y \subset X$, then $F(Y)$ will denote the set $\{f(y) : f \in F \text{ and } y \in Y\}$.

Let D be an index set, and for every $a \in D$, let Y_a be a subset of X. Then, for every $F \subset X^X$,

(a) $$\bigcup_{a \in D} F(Y_a) = F(\bigcup_a Y_a) \ ;$$

(b) $$\bigcap_{a \in D} F(Y_a) \supset F(\bigcap_a Y_a) \ .$$

If $f \in X^X$ and $Y \subset X$, then $f|Y$ denotes the mapping of Y into X such that

$$(f|Y)(y) = f(y) \qquad \text{for every } y \in Y.$$

If $F \subset X^X$ and $Y \subset X$, then $F|Y$ denotes the set $\{f|Y : f \in F\}$, and $F\|Y$ denotes the set $\{f|Y : f \in F \text{ and } f(Y) \subset Y\}$. As $F\|Y \subset Y^Y$, two mappings in $F\|Y$ may be composed.

It follows from the definition, that $F(\emptyset)=\emptyset$ for every $F \subset X^X$. Here $\emptyset$ denotes the empty set.

1.1.3. A set $Z \subset X$ is called invariant under $F \subset X^X$ if $f(Z) \subset Z$ for every $f \in F$. Evidently $\emptyset$ and X are invariant under F, and if Z_1 and Z_2 are invariant under F, so are $Z_1 \cap Z_2$ and $Z_1 \cup Z_2$.

If Z is invariant under F, and $F_1 \subset F$, then Z is also invariant under F_1.

A subset Y of X is invariant under $F \subset X^X$ if and only if $F|Y = F\|Y$.

A maximal invariant subset of X under F is an invariant subset Y of X, $Y \neq X$, such that $Y \subset Z \subset X$, Z invariant under F, implies Z=Y or Z=X.

The empty set $\emptyset$ is a maximal invariant subset under F if and only if $\emptyset$ and X are the only invariant sets under F.

1.2. Semigroups, groups, homomorphisms, isomorphisms.

1.2.1. A semigroup $(A;.)$ is a pair consisting of a non-void set A, and a binary operation in A that is associative:

$$a.(b.c)=(a.b).c \qquad \text{for all } a,b,c \in A.$$

A semigroup $(A;.)$ is said to be commutative if

$$a.b = b.a \qquad \text{for all } a,b \in A.$$

If $(A;.)$ is a semigroup, and if $B \subset A$, $C \subset A$, then B.C will denote the set $\{ b.c : b \in B \text{ and } c \in C \}$.

Let $(A;.)$ be a commutative semigroup. A set $B \subset A$ is called an ideal of the semigroup if $A.B \subset B$. According to this definition, $\emptyset$ is always an ideal. An ideal B of a commutative semigroup $(A;.)$ is said to be maximal if $B \neq A$ and if A is the only ideal of $(A;.)$, strictly containing B.

There is at most one element a in a semigroup $(A;.)$ such that

$$e.a = a.e = a \qquad \text{for all } a \in A.$$

If such an element exists it is called the unit element or unity of $(A;.)$.

Let $(A;.)$ be a semigroup with a unit element e. An element a of A is called invertible if there exists a $b \in A$ such that

$$a.b = b.a = e.$$

Then this element b is uniquely determined; it is called the inverse of a and it is denoted by a^{-1}.

If every element of a semigroup $(A;.)$ has an inverse, the semigroup is called a group.

1.2.2. Let $(A;.)$ and $(A';.)$ be two semigroups, and let φ be a map of the set A into the set A'. The map φ is called a homomorphism of the semigroup $(A;.)$ into the semigroup $(A';.)$ if

$$\varphi(a.b) = \varphi(a).\varphi(b)$$

for all $a,b \in A$. The map φ is called an isomorphism of the semigroup $(A;.)$ if it is a 1.1 map of the set A onto the set A', and if φ and φ^{-1} are both homomorphisms.

1.2.3. Let $(A;.)$ be a semigroup. If $a \in A$, then $m(a)$ will denote the mapping $b \to a.b$ of A into A:

$$m(a)\ (b) = a.b \quad , \quad \text{for every } b \in A.$$

Accordingly, $m(A)$ is the subset of A^A consisting of all mappings $m(a)$, $a \in A$; instead of $m(A)$ we will also write mA. As composition is an associative binary operation in mA, the pair $(mA;o)$ is a semigroup.

The semigroup $(mA;o)$ contains the identity mapping if and only if $(A;.)$ has a unit element.

<u>Lemma</u> If $(A;.)$ is a commutative semigroup with a unit element, then the semigroups $(A;.)$ and $(mA;o)$ are isomorphic.

<u>Proof</u>

The mapping $m : a \to m(a)$ is a homomorphism of $(A;.)$ onto $(mA;o)$; as $(A;.)$ has a unit element e, the map m is also 1.1. . For if $m(a)=m(b)$, then

$$a=a.e=m(a)(e)=m(b)(e)=b.e=b.$$

It then follows that m^{-1} exists and is again a homomorphism.

<u>Remark</u> The assumption that $(A;.)$ has a unit element is essential, as is seen from the following example. Let A consist of two points a,b, and let . be the binary operation defined by the following multiplication table:

	a	b
a	b	b
b	b	b

Then the semigroup $(mA;0)$ has only one element.

1.2.4. Lemma. Let $(A;.)$ be a commutative semigroup. A set $B \subset A$ is an ideal of $(A;.)$ if and only if it is an invariant subset of A under mA.

The set B is a maximal ideal of A if and only if it is a maximal invariant subset of A under $(mA;A)$.

Proof

A subset B of A is an ideal of (A;.) if

$$B \supset A.B = \bigcup_{a \in A} a.B = \bigcup_{a \in A} m(a)(B);$$

hence B is an ideal if and only if $m(a)(B) \subset B$ for every $m(a) \in mA$, that is, if and only if B is invariant under mA.

It then follows at once that B is a maximal ideal of (mA;.) if and only if it is a maximal fixed set under (mA;A).

Remark It follows that the study of ideals of commutative semigroups is included in the study of invariant sets under systems of mappings.

1.3. Transformation semigroups

1.3.1. A system of mappings (F;X) is called a transformation semigroup if (F;o) is a semigroup. The transformation semigroup (F;X) is said to be commutative of the semigroup (F;o) is commutative. Similarly (F;X) is called a transformation group if (F;o) is a group. If X is a non-void set, then $(X^X;X)$ is a transformation semigroup.

If F contains the identity map, then this is the unit element of (F;o). However, if (F;o) has a unit element, it need not be the identity map of X onto itself, as is shown by the example in 1.2.3.

1.3.2. Let F' be a commutative system of mappings of X into itself. If F is the set of all finite compositions $f'_1 \circ f'_2 \circ f'_3 \circ \dots f'_n$, $f'_i \in F$ for i=1,2,...,n, then (F;o) is a semigroup, and it is the smallest subsemigroup of X^X containing F'. This semigroup is called the semigroup generated by F'.

1.3.3. If $F \subset X^X$ is a maximal commutative system, then F is a semigroup under composition, and F contains the identity map.

1.3.4. If $(F;X)$ is a commutative transformation semigroup, containing the identity map, and if $Y \subset X$ is invariant under F, then $(F|Y;Y)$ is a commutative transformation semigroup, containing the identity map. However, if (F,X) is maximal, the transformation semigroup $(F|Y;Y)$ need not be maximal.

Example. Let $X = \{a,b,c,d\}$, and let F consist of the mappings f_1, f_2, f_3, f_4 defined as follows:

	a	b	c	d
f_1	a	b	c	d
f_2	b	d	d	d
f_3	c	d	d	d.
f_4	d	d	d	d

Then $(F;X)$ is maximal, $Y = \{b,c,d\}$ is an invariant subset of X under F, but $(F|Y;Y)$ is not maximal, as the mapping g

	b	c	d
g	d	c	d

commutes with all mappings in $F|Y$.

1.3.5. If $(F;X)$ is a commutative transformation semigroup, and $Y \subset X$ is invariant under F, then the mapping $f \to f|Y$ is a homomorphism of $(F;o)$ onto $(F|Y;o)$.

1.3.6. A system of mappings $(F;X)$ is called a maximal commutative transformation group if $(F;o)$ is a commutative group and if there is no transformation group $(G;X)$ such that $F \subset G$, $F \neq G$.

1.4. The product of a system of transformation semigroups

1.4.1. In this section and in the next one we consider a family $\{(F_\alpha;X_\alpha) : \alpha \in A\}$ of transformation semigroups; A is a non-void set of indices, and $F_\alpha \subset X_\alpha^{X_\alpha}$ for each $\alpha \in A$. The identity map of X_α onto itself will be denoted by i_α ; it is assumed that $i_\alpha \in F_\alpha$ for each $\alpha \in A$. The union of all sets X_α will be denoted by X :

(a) $$X = \bigcup_{\alpha \in A} X_\alpha \ ,$$

and the identity map of X onto itself will be denoted by i.

The cartesian product of sets F_α, $\alpha \in A$, is denoted by $\prod_{\alpha \in A} F_\alpha$. If $f \in \prod_{\alpha \in A} F_\alpha$, then f_α denotes the component of f in F , and we will also write $(f_\alpha)_{\alpha \in A}$ instead of f.

1.4.2. <u>Proposition</u> Let S be the following subset of $\prod_{\alpha \in A} F_\alpha$:

(a) $$S = \left\{ (f_\alpha)_{\alpha \in A} \in \prod_{\alpha \in A} F_\alpha \ : \ (\forall \alpha, \beta \in A)(f_\alpha | X_\alpha \cap X_\beta = f_\beta \mid X_\alpha \cap X_\beta) \right\}.$$

Furthermore, let $F \subset X^X$ be defined in the following manner:

(b) $$F = \ f \in X^X \ : \ (\exists \ s \in S)(\forall \alpha \in A)(f | X_\alpha = s_\alpha) \quad .$$

Then F is a semigroup of transformations of X into itself, containing the identity map i. If F_α is commutative for every $\alpha \in A$, then F is also commutative.

<u>Proof</u>

First we show the following : if $s = (s_\alpha)_{\alpha \in A} \in S$ and $t = (t_\alpha)_{\alpha \in A} \in S$, then also $(s_\alpha \ o t_\alpha)_{\alpha \in A} \in S$.

As the F_α are semigroups, it is clear that $(s_\alpha \ o t_\alpha)_{\alpha \in A} \in \prod_{\alpha \in A} F_\alpha$. Now take $\alpha, \beta \in A$; we must show that

(c) $$s_\alpha \ o \ t_\alpha \mid X_\alpha \cap X_\beta = s_\beta \ o \ t_\beta \mid X_\alpha \cap X_\beta \ .$$

But we know that

(d) $$s_\alpha \mid X_\alpha \cap X_\beta = s_\beta \mid X_\alpha \cap X_\beta \ ,$$

(e) $$t_\alpha \mid X_\alpha \cap X_\beta = t_\beta \mid X_\alpha \cap X_\beta \ ,$$

as $s,t \in S$; this implies that $X_\alpha \cap X_\beta$ is invariant under s_α ,s_β ,t_α and

t_β . The assertion (c) now follows from (d) and (e).

We now can prove that F is a semigroup. It is evident that F is non-void, as $(i_\alpha)_{\alpha\in A} \in S$, and hence $i \in F$. Take $f,g \in F$. There exist $s,t \in S$ such that for every $\alpha \in A$

(f) $$f \mid X_\alpha = s_\alpha \quad , \quad g \mid X_\alpha = t_\alpha \quad .$$

It follows that $f(X_\alpha) \subset X_\alpha$ and $g(X_\alpha) \subset X_\alpha$; hence

(g) $$f \circ g \mid X_\alpha = s_\alpha \circ t_\alpha \quad .$$

As $(s_\alpha \circ t_\alpha)_{\alpha\in A} \in S$, this shows that $f \circ g \in F$.

Finally, we assume that every F_α is commutative. Take again $f,g \in F$ and let $s,t \in S$ such that (f) holds. Then it follows from (g) that

$$f \circ g \mid X_\alpha = s_\alpha \circ t_\alpha = t_\alpha \circ s_\alpha = g \circ f \mid X_\alpha$$

for every $\alpha \in A$; hence $f \circ g = g \circ f$. Thus F is commutative.

1.4.3. <u>Definition</u> The transformation semigroup $F \subset X^X$, defined in proposition 1.4.2. (by (a) and (b)), is called the <u>product</u> of the transformation semigroups $(F_\alpha;X_\alpha)$, $\alpha \in A$, and is denoted by

$$\mathbb{P}_{\alpha\in A} F_\alpha \qquad \text{or } \mathbb{P}\left\{F_\alpha : \alpha \in A\right\}.$$

1.4.4. Let J be a family of subsets of a set X. A system $F \subset X^X$ is said to be <u>J-invariant</u> if every member of J is an invariant set under F. The system F is called a <u>maximal commutative</u> J-<u>invariant system</u> if it is commutative and J-invariant, and if there is no commutative J-invariant system $G \subset X^X$ such that $F \subset G$, $F \neq G$.
The maximal commutative system, defined in 1.1.1. evidently is a maximal $\{\emptyset\}$-invariant system.

A maximal commutative J-invariant system is always a commutative semigroup containing the identity mapping $i : X \to X$.

1.4.5. It follows from the construction of $F = \mathbb{P}_{\alpha\in A} F_\alpha$ that every set X_α is an invariant subset of X under F. Hence:

Proposition. The transformation semigroup $\mathbb{P}_{\alpha \in A} F_\alpha$ is $\{X_\alpha : \alpha \in A\}$-invariant.

1,4,6. Proposition. If the sets X_α, $\alpha \in A$, are pairwise disjoint, then the abstract semigroup $(\mathbb{P}_{\alpha \in A} F_\alpha, o)$ is isomorphic with the (unrestricted) direct product of the abstract semigroups (F, o).

Proof

If S and F are as in 1.4.2., then, under the assumption that the X_α are pairwise disjoint, the set S is equal to the set $\prod_{\alpha \in A} F_\alpha$. If we define a multiplication. in S by

$$s.t = (s_\alpha \circ t_\alpha)_{\alpha \in A},$$

then (S,.) is even isomorphic with the direct product of the semigroups (F_α, o). The proposition now follows from the fact that

(a) $$f \rightarrow (f \mid X_\alpha)_{\alpha \in A}$$

is an isomorphism of (F,o) onto (S,.).

1.4.7. Proposition. If $X_\alpha = X$, for every $\alpha \in A$, then $\mathbb{P}_{\alpha \in A} F_\alpha = \bigcap_{\alpha \in A} F_\alpha$.

Proof.

If again S and F are as defined in 1.4.2., then $(f_\alpha)_{\alpha \in A} \in S$ implies

$$f_\alpha = f_\alpha \mid X = f_\alpha \mid X_\alpha \cap X_\beta = f_\beta \mid X_\alpha \cap X_\beta = f_\beta \mid X = f_\beta$$

for all $\alpha, \beta \in A$. Conversely, if $(f_\alpha)_{\alpha \in A} \in \prod_{\alpha \in A} F_\alpha$, and $f_\alpha = f_\beta$ for all $\alpha, \beta \in A$, then $(f_\alpha)_{\alpha \in A} \in S$. This proves the assertion, as $f_\alpha = f_\beta$ for all $\alpha, \beta \in A$, implies $f_\alpha \in \bigcap_{\beta \in A} F_\beta$.

1.5. The sum of a system of transformation semigroups

1.5.1. Definition. Let $\{(F_\alpha ; X_\alpha) : \alpha \in A\}$ be a system of transformation semigroups, and let $X = \bigcup_{\alpha \in A} X_\alpha$. The transformation semigroup $F \subset X^X$, generated by the set

(a) $T = \{ f \in X^X : (\exists \alpha \in A)(\exists f_\alpha \in F_\alpha)(f \mid X_\alpha = f_\alpha \text{ and } f \mid X \setminus X_\alpha = i \mid X \setminus X_\alpha) \}$

is called the <u>sum</u> of the transformation semigroups $(F_\alpha ; X_\alpha)$, and is denoted by

$$\mathop{\mathbb{S}}_{\alpha \in A} F_\alpha \quad \text{or} \quad \mathbb{S}\{F_\alpha : \alpha \in A\}.$$

It follows from the definition that for every $\alpha \in A$ there is an isomorphism of F_α into $\mathop{\mathbb{S}}_{\beta \in A} F_\beta$.

1.5.2. We are mainly interested in the case that $\mathop{\mathbb{S}}_{\alpha \in A} F$ is a commutative semigroup. By the above remark, every F_α then has to be commutative. But this is not sufficient; e.g. if $X_1 = X_2 = \{0,1\}$, and if F_1 consists only of i and the map f_1 such that $f_1(0) = f_1(1) = 0$, while F_2 consists of i and the map f_2 such that $f_2(0) = f_2(1) = 1$, then $(F_1;X_1)$ and $(F_2;X_2)$ are commutative, but $\mathbb{S}\{F_1, F_2\}$ is not commutative.

The following condition on the family $\{(F_\alpha ; X) : \alpha \in A\}$ will turn out to be sufficient, together with the commutativity of all F_α, in order to ensure that $\mathop{\mathbb{S}}_{\alpha \in A} F_\alpha$ is commutative:

(C) for all $\alpha, \beta \in A$, the sets $X_\alpha \cap X_\beta$ and $X_\alpha \setminus X_\beta$ are invariant subsets of X_α under F_α, and if $f_\alpha \in F_\alpha$ and $f_\beta \in F_\beta$, then $f_\alpha \mid X_\alpha \cap X_\beta$ and $f_\beta \mid X_\alpha \cap X_\beta$ commute.

1.5.3. <u>Proposition</u>. Let $\{(F_\alpha ; X_\alpha) : \alpha \in A\}$ be a family of commutative transformation semigroups, each containing the identity mapping $i_\alpha : X_\alpha \to X_\alpha$, and let condition (C) be satisfied. Then $\mathop{\mathbb{S}}_{\alpha \in A} F_\alpha$ is a commutative transformation semigroup containing the identity map.

<u>Proof</u>

Let T be as in 1.5.1., and let F be the subsemigroup of X^X generated by T. As it is evident that $i \in F$ we have only to show that F is commutative. Let $f, g \in F$. Then there are $\alpha, \beta \in A$ and $f_\alpha \in F_\alpha$, $f_\beta \in F_\beta$ such that

$$f \mid X_\alpha = f_\alpha \quad ; \quad g \mid X_\beta = f_\beta \quad ;$$
$$f \mid X \setminus X_\alpha = i \mid X \setminus X_\alpha \ ;$$
$$g \mid X \setminus X_\beta = i \mid X \setminus X_\beta \ .$$

As condition (C) is assumed to be satisfied, $f|X_\alpha \cap X_\beta$ and $g|X_\alpha \cap X_\beta$ commute. Furthermore, $f|X\setminus(X_\alpha \cup X_\beta) = g|X\setminus(X_\alpha \cup X_\beta) = i|X\setminus(X_\alpha \cup X_\beta)$. Hence we need only check what happens with points in $X_\alpha \setminus X_\beta$ or in $X_\beta \setminus X_\alpha$. Because of the symmetry of the situation, we may restrict our attention to points in $X_\alpha \setminus X_\beta$.

Let $x \in X_\alpha \setminus X_\beta$. Then

$$(f \circ g)(x) = f(g(x)) = f(x) = f_\alpha(x);$$

as $X_\alpha \setminus X_\beta$ is supposed to be invariant under F_α, $f_\alpha(x) \in X_\alpha \setminus X_\beta$; hence

$$f_\alpha(x) = g(f_\alpha(x)) = g(f(x)) = (g \circ f)(x).$$

This finishes the proof.

1.5.4. <u>Proposition</u>. If the sets $X_\alpha, \alpha \in A$, are pairwise disjoint, then the abstract semigroup $(\mathop{\mathfrak{S}}\limits_{\alpha \in A} F_\alpha, \circ)$ is isomorphic to the direct sum (restricted direct product) of the abstract semigroups $(F_\alpha, \circ), \alpha \in A$.

<u>Proof</u>

Let T be defined by 1.5.1. . Let φ be the mapping 1.4.6.(a). Then φ maps T 1.1 onto the subset of $\prod_{\alpha \in A} F_\alpha$, consisting of all $(f_\alpha)_{\alpha \in A}$ such that $f_\alpha \neq i_\alpha$ for at most one $\alpha \in A$; and φ maps F 1.1. onto the subset of $\prod_{\alpha \in A} F_\alpha$ such that $f_\alpha \neq i_\alpha$ for only finitely many $\alpha \in A$. It is immediately seen that $\varphi | F$ is a homomorphism of $(F, \circ)$ into the direct product of the $(F, \circ)$; hence $\varphi | F$ is an isomorphism, and $\varphi(F)$ is exactly the direct sum of the $(F_\alpha, \circ)$.

1.5.5. <u>Proposition</u>. Assume $X_\alpha = X$, for every $\alpha \in A$. Then condition (C) is satisfied if and only if $\bigcup_{\alpha \in A} F$ is commutative, and $\mathop{\mathfrak{S}}\limits_{\alpha \in A} F_\alpha$ is the subsemigroup of X^X generated by $\bigcup_{\alpha \in A} F_\alpha$.

Proof: evident.

1.6. The relations

1.6.1. Let R be a relation[1] defined in a set X. For $Y \subset X$, R(Y) will denote the set

$$R(Y) = \{ x \in X : (\exists\, y \in Y)\ (y\ R\ x) \} .$$

Instead of $R(\{y\})$ we will write R(y).

In particular, let E be an equivalence relation defined in X. Then for $x \in X$, E(x) is the equivalence class containing x. The set of all these equivalence classes will be denoted by X / E.

1.6.2. Let $F \subset X^X$. An relation R between elements of X is said to be compatible with F if

$$x\ R\ y \implies f(x)\ R\ f(y)$$

for all $x,y \in X$ and all $f \in F$. If R is an equivalence relation E, then it follows that for every $f \in F$ there is a uniquely determined map $\varphi : X/E \rightarrow X/E$ such that

$$\varphi(E(x)) = E(\varphi(x))$$

for all $x \in E$. This map φ will be denoted by f/E. Furthermore, F/E denotes the set

$$F/E = \{ f/E : f \in F \}$$

of mappings of X/E into itself.

1.6.3. A relation R, defined in a set X, is called a weak partial ordering (shortly: a w.p.o.) if it satisfies the following two conditions:

(a) xRx for every $x \in X$;

(b) $xRy,\ yRz \implies xRz$, for all $x,y,z \in X$;

----

1) in this section by "relation" always is meant a binary relation.

If R is a w.p.o. then the relation E_R, defined by

$$x \; E_R \; y \iff x \; R \; y \text{ and } y \; R \; x$$

is an equivalence relation in X. The corresponding set of equivalence classes X/E_R will be denoted by X_R.

In X_R a partial ordering $\leqslant_R$ can be defined such that:

$$E(x) \leqslant_R E(g) \iff x \; R \; y.$$

The partially ordered set $(X_R, \leqslant_R)$ is called the skeleton of the weakly partially ordered set (X,R).

1.6.4. If the w.p.o. R in X is compatible with $F \subset X^X$, we will write F_R instead of F/E_R (and f_R instead of F/E_R, for $f \in F$).

<u>Proposition</u>: If R is compatible with F, then E_R is compatible with F, and $\leqslant_R$ is compatible with F_R.

<u>Proof</u>

Suppose R is compatible with F. Then

$$x \; E_R \; y \Rightarrow x \; R \; y \;\&\; y \; R \; x \Rightarrow f(x) R \; f(y) \;\&\; f(y) R \; f(x) \Rightarrow f(x) \; E_R \; f(y).$$

Hence E_R is compatible with F. And

$$E(x) \leqslant_R E(y) \Rightarrow x \; R \; y \Rightarrow f(x) R \; f(y) \Rightarrow f_R(E(x)) = E(f(x)) \leqslant_R E(f(y)) = \\ = f_R(E(y)).$$

Hence $\leqslant_R$ is compatible with E_R.

1.6.5. Let $F \subset X^X$. Then $)_F$ will be the following relation on X:

$$x \;)_F \; y \iff \exists f \in F : \; f(x) = y.$$

<u>Proposition</u>. For every $F \subset X^X$, $)_F$ is compatible with F.

The equivalence relation $E_{)_F}$ will be denoted by C_F, the set X/C_F will be denoted by $\Gamma(F)$; and the partial ordering $\leqslant)_F$ in $\Gamma(F)$ will be denoted by $\leqslant_F$. If $f \in F$, then $\bar{f}$ denotes the mapping f/C_F of $\Gamma(F)$ into itself, and $\bar{F}$ denotes the set F/C_F. If there is no danger for confusion we will simply write $)$, C, Γ and $\leqslant$, instead of $)_F$, C_F, $\Gamma(F)$, $\leqslant_F$, respectively.

It may be remarked that $)_F(x)$ (as defined in 1.) coincides with $F(x)$.

1.6.6. A relation R between elements of a set X is called an N-relation if it is a w.p.o. and if it also satisfies the following property:

$$x\ R\ y_1\ ,\quad x\ R\ y_2 \Rightarrow \exists z \in X:\quad y_1\ R\ z\ ,\quad y_2\ R\ z\ ,$$

for all $x, y_1, y_2 \in X$.

Proposition. If R is an N-relation, then $\leqslant_R$ is an N-relation.

1.6.7. Proposition. Let (F;X) be a commutative transformation semigroup containing the identity map. Then $)_F$ is an N-relation.

Proof The relation $)_F$ is reflexive as the identity mapping belongs to F. $)_F$ transitive as F is a semigroup.
Let $x\ R\ y_1$ and $x\ R\ y_2$, that is $f_1(x)=y_1$, $f_2(x)=y_2$, f_1, $f_2 \in F$. But then $z=f_1 o f_2(x)$ fulfils the conditions $y_1 R\ z$ and $y_2 R\ z$.

1.6.8. Proposition. Let (F;X) be commutative transformation semigroup containing the identity map, and let E be an equivalence relation on X that is compatible with F. Then $(F_E;X_E)$ is a commutative transformation semigroup containing the identity map.

1.6.9. Proposition. Let (F;X) be a commutative transformation semigroup containing the identity map. Then

(a) $x\ )_F\ y \Rightarrow f(x)\ )_F\ f(y)$ for every $x,y \in X$, $f \in F$,

(b) $f(x)=x \Rightarrow \forall y,\ x\ )_F\ y,\ f(y)=y$,

(c) $f(x)\ )_F\ y \Rightarrow y \in f(X)$, for every $f \in F$.

Proof.

(a) $y=g(x) \Rightarrow f(y)=f \circ g(x)=g \circ (f(x))$,

(b) $y=g(x)=g \circ f(x) = f \circ g(x) = f(y)$,

(c) $y=g \circ f(x) \Rightarrow y=f \circ g(x)$.

1.6.10. <u>Proposition</u>. Let $(F;x)$ be a transformation semigroup containing the identity map. Then the relation M on x,

$$x \; M \; y \Longleftrightarrow \exists z \in X, \; x\,)_F z, \; y\,)_F z,$$

is an equivalence relation, that is compatible with F. Moreover, F/M consists only of the identity map.

<u>Proof</u>.

M is evidently reflexive and symmetric. We must prove that M is transitive. Let $x_1 \, M \, x_2$, $x_2 \, M \, x_3$. Then there exist $z_1, z_2 \in X$, $f_1, f_2, g_1, g_2 \in F$ such that

$$f_1(x_1)=z_1, \; f_2(x_2)=z_1, \; g_1(x_2)=z_2, \; g_2(x_3)=z_2.$$

Then

$$g_1 \circ f_2(x_2)=g_1 \circ f_1(x_1)=f_2 \circ g_1(x_2)=f_2 \circ g_3(x_3);$$

hence $x_1 \, M \, x_3$.

If $x \, M \, y$ then evidently $f(x) M f(y)$ for every $f \in F$, as $f(z)$ has the property required by definition of M.

As $f(x) M x$ for every $x \in X$ and $f \in F$, we have $f/M=i/M$ for every $f \in F$.

1.6.11. <u>Proposition</u>. M is the smallest equivalence relation R which is compatible with $(F;X)$ and $F/R=\{i/R\}$.

1.6.12. Example. Let Y be an invariant set under F. Then an equivalence relation, again denoted by Y, is defined as follows:

$$x \; Y \; y \Longleftrightarrow \text{either } x=y \text{ or both } x \in Y \text{ and } y \in Y.$$

This relation is compatible with F.

2. Orbits of commutative transformation semigroups

Throughout this chapter we shall assume that F is a commutative semigroup of transformations of a given set X into itself, containing the identity transformation.

2.1. The parameter of a semigroup

2.1.1. The orbit of a point $x \in X$ under F is the set $F(x)$. If F is a semigroup, then every orbit $F(x)$ is an invariant subset.
A system of orbits $\{F(x) : x \in Y\}$, when $Y \subset X$, is called an F-cover of X if $F(Y)=X$. If F contains the identity map, then X admits at least one F-cover.

An F-cover $\{F(x) : x \in Y\}$ is called disjoint if $F(x) \cap F(y) = \emptyset$ for all $x \neq y$, x and $y \in Y$.

2.1.2. If $f(x)=g(x)$, for some $x \in X$ and $f,g \in F$, then $f|F(x)=g|F(x)$.

Proof

Let $y \in F(x)$. Then $y=h(x)$, for some $h \in F$, and

$$f(y)=f \circ h(x)=h \circ f(x)=h \circ g(x)=g \circ h(x)=g(y).$$

2.1.3. If A is any set, then $|A|$ denotes the cardinal number of A.

The parameter of F is the least cardinal number α for which there exists an F-cover $\{F(x) : x \in Y\}$ of X with $|Y| = \alpha$. This cardinal number will be denoted by $p(F)$.

The following fact is evident from the definition: If $F \subset G$, then $p(F) \geqslant p(G)$.

2.1.4. If $\{F(x) : x \in Y\}$ is a disjoint F-cover, then $|Y| = p(F)$.

Proof

Let $\{F(z) : z \in Z\}$ be any F-cover such that $|Z|=p(F)$. We shall show that every orbit $F(z)$, $z \in Z$, is contained in an orbit $F(x)$, $x \in Y$. Suppose this were false. Then there would exist a $z \in Z$, and $x_1, x_2 \in Y$, $x_1 \neq x_2$, such that

$$F(z) \cap F(x_1) \neq \emptyset ,$$
$$F(z) \cap F(x_2) \neq \emptyset .$$

Let $f_1, f_2 \in F$ such that $f_1(z) \in F(x_1)$ and $f_2(z) \in F(x_2)$. Then $f_1(f_2(z)) \in F(x_1) \cap F(x_2)$, contradicting the assumption that $\{F(x) : x \in Y\}$ is disjoint.

2.1.5. If F is a group, then two orbits $F(x)$, $F(y)$ under F either coincide, or they are disjoint.

Proof

Suppose $F(x) \cap F(y) \neq \emptyset$; then let $z \in F(x) \cap F(y)$. There exist $f_1, f_2 \in F$ such that $z = f_1(x) = f_2(y)$. Then $x = f_1^{-1} \circ f_2(y)$, which implies $F(x) \subset F(y)$, and $y = f_2^{-1} \circ f_1(x)$, implying $F(y) \subset F(x)$. So if $F(x)$ and $F(y)$ are not disjoint, they coincide.

As an immediate consequence, we obtain the following:
If F is a group, then there exist disjoint F-covers.

For if Y is a set containing precisely one point from every orbit, then $\{F(x) : x \in Y\}$ is such a disjoint F-cover.

2.1.6. If $F(x) \cap F(y) \neq \emptyset$ and $F(y) \cap F(z) \neq \emptyset$ then $F(x) \cap F(z) \neq \emptyset$.

Proof

Let $f, g, h, j \in F$ such that $f(x) = g(y)$ and $h(y) = j(z)$. Then

$$j \circ f\ (x) = j \circ g(y) = g \circ j(y) = g \circ h(z),$$

which shows that $F(x) \cap F(z) \neq \emptyset$.

2.1.7. If $F(x) = X$ for every $x \in X$, then F is a group.

Proof

According to 2.1.2., two mappings $f, g \in F$ coincide as soon as they are equal in one point of X.

Now we will show that an arbitrary F has an inverse. Choose $x_o \in X$, and let $x=f(x_o)$. By our assumption, there exists an $f_1 \in F$ such that $x_o=f_1(x)$. It follows that $f_1 \circ f(x_o)=x_o=i(x_o)$. Hence, by our previous remark $f_1 \circ f=i$. As F is commutative, $f \circ f_1=i$ also; this proves that f_1 is the inverse of f.

2.2. Properties of semigroups with parameter 1.

2.2.1. If $p(F)=1$, then there exists a 1.1. mapping of F onto X.

Proof

As $p(F)=1$ there must exist a point $e \in X$ such that $F(e)=X$. We define $\varphi: F \to X$ as follows:

$$\varphi(f)=f(e) \quad , \text{ for all } f \in F.$$

Then φ maps F onto X, and φ is 1.1., for if $\varphi(f_1)=\varphi(f_2)$, then $f_1(e)=f_2(e)$, and it follows from 2.1.2. that

$$f_1=f_1|F(e) = f_2|F(e) = f_2 \quad .$$

An other formulation of this fact is the following.

2.2.2. $\quad p(F)=1$ implies $|F|=|X|$.

2.2.3. Let $p(F)=1$, We then can introduce a binary operation $*$ in X as follows:

$$x * y = \varphi[\varphi^{-1}(x) \circ \varphi^{-1}(y)] \quad ,$$

where φ is the map defined in 2.1.1.

Proposition. φ is an isomorphism of $(F;\circ)$ onto $(X;*)$ and for every $x \in X$ and $f \in F$ we have

$$\varphi(f) * x = f(x) \quad ,$$

$$f \circ \varphi^{-1}(x) = \varphi^{-1}(f(x)).$$

Proof

It is immediate from the definition of $*$ that φ is an isomorphism.

Now be $x \in X$ and $f \in F$. There exists a $g \in F$ such that $g(e)=x$. Then $x=\varphi(g)$, and hence

$$\varphi(f) * x=\varphi(f) * \varphi(g)=\varphi(f \circ g)=f \circ g(e)=f(x).$$

The second identity follows from the first by applying φ^{-1} .

2.2.4. If $p(F)=1$, then F is a maximal commutative system.

Proof

Let $g \in X^X$ commute with every $f \in F$, and let G be the commutative semigroup generated by F and g. Then $p(G) \leq p(F)$, hence $p(G)=1$.
Let $e \in X$ be such that $F(e)=X$; then for some $f \in F$, $f(e)=g(e)$. By 2.1.2. (as $G(e)=X$) it follows that $g = f$; hence $g \in F$.

2.3. The restriction of a transformation semigroup to one of its orbits.

As an orbit under F is an invariant subset, $(F|F(x);\ F(x))$ is a transformation semigroup, and evidently its parameter is 1. Hence we can at once apply the results of the previous paragraph.

2.3.1. $\quad \left| F|F(x) \right| = \left| F(x) \right|$, for every $x \in X$.

2.3.2. $\quad F|F(x)$ is a maximal commutative semigroup of mappings of $F(x)$ into itself.

2.3.3. In $F(x)$ a binary operation $*$ can be introduced in such a way that $(F(x);\ *)$ is isomorphic to $(F|F(x);\ \circ)$.

2.4. Commutative semigroups that are maximal with respect to their system of invariant sets.

In this section, $(F;X)$ is a commutative transformation semigroup, containing the identity transformation, and J will always denote a family of subsets of X that are invariant under F.

2,4,1. If J is such a family, then $\cup J$ will denote the set $\cup\{A : A \in J\}$, and $\mathbb{P}(J)$ will denote the semigroup

$$\mathbb{P}(J) = \mathbb{P}\{F|A : A \in J\} .$$

The following lemma is almost obvious:

Lemma $f \in \mathbb{P}(J) \Leftrightarrow f|A \in F|A$ for all $A \in J$.

From this lemma, the following propositions follow without difficulty:

Proposition. If $\cup J = X$, then $F \subset \mathbb{P}(J) \subset X^X$.

(If $\cup J \neq X$, then certainly not $F \subset \mathbb{P}(J)$, as $\mathbb{P}(J)$ consists of mappings of $\cup J$ into itself).

2.4.2. Proposition. Let both J_1 and J_2 consist of subsets of X that are invariant under F. If $\cup J_1 = \cup J_2$, then $J_1 \subset J_2$ implies $\mathbb{P}(J_1) \supset \mathbb{P}(J_2)$.

2.4.3. If J_1 and J_2 are both families of subsets of a set X, we will say that J_1 is a refinement of J_2, and write

$$J_1 \leqq J_2 ,$$

if for every $A_1 \in J_1$ there is an $A_2 \in J_2$ such that $A_1 \subset A_2$.

2.4.4. Proposition. Let both J_1 and J_2 consist of subsets of X that are invariant under F. If $\cup J_1 = \cup J_2$ and $J_1 \leqq J_2$, then $\mathbb{P}(J_1 \cup J_2) = \mathbb{P}(J_2)$.

Proof

By proposition 2,4.2., $\mathbb{P}(J_1 \cup J_2) \subset \mathbb{P}(J_2)$; on the other hand,

$$f \in \mathbb{P}(J_2) \Leftrightarrow (\forall A \in J_2)(f|A \in F|A) \Rightarrow (\forall A \in J_1 \cup J_2)(f|A \in F|A) \Leftrightarrow f \in \mathbb{P}(J_1 \cup J_2). .$$

Example If $X \in J$, then $\mathbb{P}(J) = F$.

Remark If A is not an invariant subset of X, then $F|A$ is not a semigroup. However, if we define $F\|A = \{f(A) : f \in A \text{ and } f(A) \subset A\}$, then $F\|A$ is a semigroup under composition. It is seen at once that

$$\mathbb{P}\left\{(F;X),\ (F \| A;A)\right\} = \left\{f \in F \ :\ fA \subset A\right\};$$

hence if A is not invariant, $F \not\subset \mathbb{P}(F, F \| A)$, although of course $X \cup A = X$.

2.4.5. Lemma Let J be the class of all subsets of X that are invariant under F, and let J' be the class of all orbits under F, $G \supset F$.

Then G is a commutative J-invariant system if and only if G is a commutative J'-invariant system.

Proof

As $J' \subset J$, every J-invariant system is J'-invariant. On the other hand, if $A \in J$, then

$$G(A) = \bigcup\left\{G(x) \ :\ x \in A\right\} = \bigcup\left\{B \in J' \ :\ B \subset A\right\}.$$

Hence every J'-invariant system is J-invariant.

2.4.6. Theorem Let $F \subset X^X$ be a commutative semigroup, containing the identity map. Let J be the class of all subsets of X that are invariant under F. Then there exists one and only one maximal commutative J-invariant semigroup $G \subset X^X$ containing F; and

$$G = \mathbb{P}\left\{F | F(x) \ :\ x \in X\right\}.$$

Proof

Let g be any mapping $X \longrightarrow X$ that commutes with every $f \in F$ and that maps every $A \in J$ into itself. We will show that $g \in G$.

Take any $x \in X$. Then $g|F(x)$ maps F(x) into itself, as $F(x) \in J$, and $g|F(x)$ commutes with every mapping in $F|F(x)$. But by 2.3.2, $F|F(x)$ is a maximal commutative semigroup; hence $g|F(x) \in F|F(x)$. It now follows from 2.4.1 that $g \in G$.

An immediate consequence is that $F \subset G$ (this also follows from proposition 2.4.1.). So it remains only to be proved that G is J-invariant. But by proposition 1.2.5, G is J'-invariant, where $J' = \left\{F(x) \ :\ x \in X\right\}$; now apply lemma 2.4.5.

2.4.7. Corollary: If $F \subset X^X$ is a maximal commutative transformation semigroup, then

$$F = \mathbb{P}\left\{ F|F(x) \ : \ x \in X \right\}.$$

Theorem. If $\left\{ F(x) \ : \ x \in Y \right\}$ is an F-cover of X, then $\mathbb{P}\left\{ F|F(x) \ : \ x \in Y \right\}$ is the maximal commutative J-invariant semigroup containing F (where J is the family of all subsets of X that are invariant under F).

2.5. Estimate of $|F|$

2.5.1. If $\left\{ F(x) \ : \ x \in Y \right\}$ is an F-cover of X, then

$$|F| \leq \prod_{x \in Y} |F(x)| \ .$$

For $F \subset \mathbb{P}_{x \in Y} F|F(x)$, hence $|F| \leq \left| \mathbb{P}_{x \in Y} F|F(x) \right| \leq \prod_{x \in Y} \left| F|F(x) \right|$, and the last expression equals $\prod_{x \in Y} |F(x)|$, by 2.3.1.

An immediate consequence is the following.

2.5.2. $$|F| \leq |X|^{p(F)}.$$

2.5.3. Let F be a maximal commutative system of mappings, and suppose X admits a disjoint F-cover $\left\{ F(x) \ : \ x \in Y \right\}$. Then

$$|F| = \prod_{x \in Y} |F(x)| \ .$$

Proof.

In this case, $F = \mathbb{P}_{x \in Y} F|F(x)$; as the orbits $F(x)$, $x \in Y$, are disjoint, $\mathbb{P}_{x \in Y} F|F(x)$ is isomorphic (and hence equipotent) to the full direct product $\prod_{x \in Y} F|F(x)$.

2.5.4. Let $\left\{ F(x) \ : \ x \in Y \right\}$ be an orbit cover, and for every $x \in Y$ let $*$ be the binary operation mentioned in 2.3.3 and 2.2.3. Then F can be isomorphically embedded into $\prod_{x \in Y} F(x)$.

Proof

F is contained in $\mathbb{P}_{x \in Y} F|F(x)$, and it follows from its definition that this semigroup can be isomorphically embedded in $\prod_{x \in Y} F|F(x)$. As $(F|F(x);\circ)$ is isomorphic with $(F(x);*)$, the assertion follows.

2.5.5. Let F be a group that is maximal, considered as a commutative semigroup. Then

$$|F| \geqslant |X| .$$

Proof

We may assume that X contains more than one point. Let $\{F(x) \ : \ x \in Y\}$ be a disjoint F-cover of X. Then by 2.5.3,

$$|F| = \prod_{x \in Y} |F(x)| .$$

As the F(x), $x \in Y$, are pairwise disjoint, we also have

$$|X| = \sum_{x \in Y} |F(x)| .$$

Hence it suffices to show that $|F(x)| \geqslant 2$, for every $x \in Y$. But indeed, if $|F(x)| = 1$ for some $x \in Y$, then x is a common fixed point of all $f \in F$; the mapping g such that $g(y) = x$, for all $y \in X$, then commutes with all $f \in F$, and the assumption that F is a maximal commutative semigroup implies $g \in F$. However, as we supposed that X contains at least two points, g is not invertible, contradicting the fact that F is a group.

2.6. Applications to topology

2.6.1. In this section, X will be a topological space. Then the product topology of X^X induces a topology in every $F \subset X^X$. This is the topology of pointwise convergence: $f_\alpha \to f$ if and only if $f_\alpha(x) \to f(x)$ for every $x \in X$, where $\{f_\alpha \ ; \alpha \in D\}$ is a net.

As before, we consider only subsets F of X^X that are commutative semigroups under composition, containing the identity map. All mappings in F are assumed to be continuous.

2.6.2. If $p(F) = 1$, then F (with the pointwise topology) is homeomorphic to X.

Proof

Let φ be the 1.1. map of F onto X considered in 2.2.1. Then φ is a homeomorphism.

Let $\{f_\alpha, \alpha \in D\}$ be a net, $f, f_\alpha \in F$ for $\alpha \in D$. If $f_\alpha(e) \to f(e)$, then $f_\alpha(x) \to f(x)$ for every $x \in X$. Clearly, for every $x \in X$ we can find $g \in F$ such that $g(e) = x$. We have

$$f_\alpha(x) = f_\alpha(g(e)) = g(f_\alpha(e))$$

and $f_\alpha(x) \to f(x)$, as g is assumed continuous. Therefore φ is open.

If $f_\alpha(x) \to f(x)$ for every $x \in X$, $f, f_\alpha \in F$, then $\varphi(f_\alpha) \to \varphi(f)$, and the assertion is proved.

2.6.3. If $\{F(x) : x \in Y\}$ is an F-cover of X, then F is homeomorphic to a subspace of $X^{|Y|}$.

<u>Proof</u>

Let $x \in Y$. Then $[F|F(x)]\ (x) = F(x)$. According to the preceding proposition there exists a homeomorphism φ_x from $F|F(x)$ onto $F(x)$. Let us define the mapping φ coordinatewise:

$$\varphi_x(f) = \varphi_x(f|F(x)) \quad \text{for every } x \in Y.$$

If $f_1, f_2 \in F$, $f_1 \neq f_2$, then there exists $x \in Y$ such that $f_1|F(x) \neq f_2|F(x)$, hence $\varphi_x(f_1) \neq \varphi_x(f_2)$, as φ_x is one-to-one. Therefore φ is one-to-one mapping from F onto $\varphi(F)$. It is sufficient to prove that φ is both continuous and open.

Let $f_\alpha \to f$, $f, f_\alpha \in F$. Then $\varphi_x(f_\alpha) \to \varphi_x(f)$ for every $x \in Y$.

Let $\varphi(f_\alpha) \to \varphi(f)$, $f, f_\alpha \in F$. To every $z \in X$ there exists $x \in Y$ such that $z \in F(x)$. We have $\varphi_x(f_\alpha) \to \varphi_x(f)$, and $f_\alpha(x) \to f(x)$. We can write $z = g(x)$, $g \in F$. Then $f_\alpha(x) = f_\alpha[g(x)] = g[f_\alpha(x)]$, and $f_\alpha(z) \to f(z)$, as g is continuous. The proof is concluded.

As an immediate consequence we find the following.

2.6.4. F can be homeomorphically embedded in $X^{p(F)}$.

2.6.5. Suppose there is a point $e \in X$ with a dense orbit: $\overline{F(e)} = X$, where $\overline{F(e)}$ denotes the closure of the set $F(e)$. Then, for every $x_1 \in X$, there is at most one continuous map $g : X \to X$ that commutes with every $f \in F$, and that sends e into x_1 : $g(e) = x_1$.

Proof

Assume two such maps, g_1 and g_2, exist. Then, if $f \in F$,

$$g_i \circ f(e) = f \circ g_i(e) = f(x_1) \qquad (i=1,2).$$

Hence g_1 and g_2 coincide on the dense set $F(e)$. This implies that $g_1 = g_2$.

2.6.6. If $\overline{F(e)} = X$ for some $e \in X$, then

$$|F| \leq |X|.$$

This follows at once from the previous theorem.

2.6.7. Suppose $\overline{F(x)} = X$, for every $x \in X$. Then if $x,y \in X$, there is at most one continuous mapping $g : X \to X$ that commutes with all $f \in F$, such that $g(x) = y$.

This follows at once from 2.6.4.

2.7. Examples

2.7.1. Let $X = (0,\infty)$, and let F consist of all mappings f,

$$f(x) = x^s ,$$

with $s \in (-\infty;+\infty)$.

Let $e \in X$, $e \neq 1$. Then $F(e) = X$; hence $p(F) = 1$. The mapping φ :

$$f \to f(e) = e^s$$

is a 1.1. mapping of F onto X. If $a \in X$, then $\varphi^{-1}(a)$ is the mapping

$$\varphi^{-1}(a) = x \to x^{\log_e a} ;$$

and

$$a * b = e^{\log_e a . \log_e b} .$$

From the equations

$$\varphi(f) * x = f(x),$$

$$f \circ \varphi^{-1}(x) = \varphi^{-1} \circ f(x),$$

we see that the value of f(x) can be determined if the mappings φ, φ^{-1} and one of the operations o and $*$ are known. In this case the operation o is easier of course, as it amounts to calculate f(x). In fact, this method is often used in actual calculations, as there are tables for φ, φ^{-1}.

2.7.2. A similar idea lies behind the theory of operators and of Laplace transformation. It would be too complicated to exhibit this completely here, however, we shall consider a discrete example.

Let X consist of all those sequences $\{a_n\}_0^\infty$ of real numbers, such that $a_n \neq 0$ for only finitely many n. Then X can be considered as a linear space.

Let the mapping $f : X \to X$ be defined as follows:

$$f\{a_n\} = \{b_n\}\ ,\ \text{where } b_o = 0,\ b_n = a_{n-1} \quad (n=1,2,\dots).$$

Finally, let F be the set of all mappings $X \to X$ of the form

$$\sum_{n=0}^{s} \alpha_n f^n ,$$

where s is any natural number, and the α_n are real numbers; here $f^o = i$.

If $e = \{1,0,0,\dots\}$, then evidently $F(e) = X$; hence $p(F) = 1$. If $a = \{a_o, a_1, \dots\}$ and $b = \{b_o, b_1, \dots\}$, then

$$a * b = \{a_o b_o\ ;\ a_1 b_o + a_o b_1;\ \dots;\ \sum_{k=0}^{n} a_k b_{n-k}; \dots\} .$$

This is just the ordinary convolution of number sequences.

Now in F the composition of functions amounts to the simple operation of multiplying two polynomials. This makes it easy to compute the convolution. As a special case, consider the following operation: given $\{a_n\} \in X$, to evaluate $a_o + a_1 + \dots + a_{n-1}$. (In the case of true Laplace transformation an analogous operation would be integration.) This operation can be described with the use of convolution: if $s_n = (\underbrace{1,1,1,\dots,1}_{n},0,0,\dots)$, then

$$a_o + a_1 + \dots + a_{n-1} = \{s_n * a\}_{n-1}$$

where $a = \left\{ a_n \right\}$. In order to calculate this sum, we can use the 1.1. map φ to go back to F:

$$\varphi^{-1}(s_n * a) = \varphi^{-1}(s_n) \circ \varphi^{-1}(a),$$

and the operation s_n is reduced to the multiplication of $\varphi^{-1}(a)$ by a polynomial (namely $\varphi^{-1}(s_n)$).

3. Cycles and structure of commutative transformation semigroups

In this section it is always assumed that X is a set, and that F is a commutative semigroup of mappings $X \to X$, containing the identity map i.

3.1. Cycles of F in X.

3.1.1. When F is a semigroup, we introduced a weak partial ordering in X as follows:

$$x \,)_F\, y \Leftrightarrow (\exists f \in F)(y = f(x)).$$

As usual, two points $x,y \in X$ are called equivalent according to this ordering, denoted xCy, if both $x \,)_F\, y$ and $y \,)_F\, x$. The equivalence classes are called the cycles of F in X; the set of all cycles is denoted by $\Gamma(F)$, or shortly by Γ if there is no danger of confusion. The cycle to which $x \in X$ belongs is denoted by C(x); explicitly, we have

$$C(x) = \{ y \in X: (\exists f_1, f_2 \in F)(f_1(x) = y \text{ and } f_2(y) = x).$$

The set $\Gamma(F)$ is partially ordered in a natural way, namely, if we define

$$C(x) \geqslant C(y) \Leftrightarrow x \,)_F\, y.$$

We will call the (strongly) partial ordered set $(\Gamma(F); \geqslant)$ the skeleton of the weakly ordered set $(X;)_F)$, or also the skeleton of X under F.

3.1.2. Proposition. $f|C(x) \in F\,\|\,C(x) \Leftrightarrow (\exists y \in C(x))(f(y) \in C(x))$.

Proof

By definition, $f|C(x) \in F\,\|\,C(x) \Leftrightarrow (\forall y \in C(x))(f(y) \in C(x))$. This evidently implies the right hand condition. Conversely, assume $f(y) \in C(x)$, for a certain $y \in C(x)$. Then there exists maps $f_1, f_2 \in F$ such that

$$y = f_1(x) \text{ and } x = f_2 \circ f(y).$$

Let $z \in C(x)$. We must show that $f(z) \in C(x)$.
As $z \in C(x)$, there are maps $f_3, f_4 \in F$ such that

$$z = f_3(x) \text{ and } x = f_2 \circ f(y) = f_2 \circ f \circ f_1(x) = f_2 \circ f \circ f_1 \circ f_4(z) =$$
$$= f_2 \circ f_1 \circ f_4(f(z)),$$

and this shows that $f(z) \in C(x)$.

3.1.3. Proposition. $y \in C(x) \Rightarrow (F \,|\, C(x))(y) = C(x)$.

Proof

If $z \in C(x)$, then $z = f_1(x)$ for some $f_1 \in F$. As $y \in C(x)$, $x = f_2(y)$ for some $f_2 \in F$. Then $f_1 \circ f_2(y) = z \in C(x)$; hence, by 3.1.2, $f_1 \circ f_2 | C(x) \in F \,\|\, C(x)$. Thus $z \in (F \,\|\, C(x))(y)$.

3.1.4. Theorem. For every cycle C in X, $F \,\|\, C$ is a group.

The proof is immediate from 2.1.7. and 3.1.3.

3.1.5. The proposition 3.1.2. shows that for every $C \in \Gamma(F)$ and for every $f \in F$ there are only two possibilities: either $f(C) \in C$ or $f(C) \cap C = \emptyset$. Actually, this follows already from the fact that the cycles are the equivalence classes of the weak partial ordering of X introduced in 1.6.5. From this there follows even more: for all $x \in X$ and all $f \in F$ we have

$$f(C(x)) \subset C(f(x)).$$

In general, it need not be true that $f(C(x)) = C(f(x))$.

Example. Let $X = \{1;2;3;4;5\}$, let F consist of the mappings f_1, f_2, f_3, f_4, f_5 defined as follows:

	1	2	3	4	5
f_1	1	2	3	4	5
f_2	2	1	3	4	5
f_3	3	3	3	4	5
f_4	4	4	4	5	3
f_5	5	5	5	3	4

It is immediately checked that F is a commutative semigroup of mappings $X \rightarrow X$. There are two cycles: $C_1 = \{1;2\}$, $C_2 = \{3;4;5\}$; and for instance $f_3(C(1)) \neq C(f_3(1))$.

Thus, in general the sets $f(C)$, $C \in \Gamma$, are not themselves cycles. Nevertheless, they share some properties with cycles, as is shown by the following theorem.

3.1.6. Theorem. For every $f \in F$ and for every $C \in \Gamma$, $F \| f(C)$ is a group, and there is a natural homomorphism of $F \| C$ onto $F \| f(C)$.

Proof

Take $C \in \Gamma$ and $f \in F$.

In the first place, we have

$$f_1 | C \in F \| C \Longrightarrow f_1 | f(C) \in F \| f(C),$$

as $f_1 \circ f(C) = f \circ f_1(C) \subset f(C)$.

Now let $y_1, y_2 \in f(C)$. We will show the existence of an $f_1 \in F$ such that $f_1 | f(C) \in F \| f(C)$ and $f_1(y_1) = y_2$. By 2.1.7, this will show that $F \| f(C)$ is a group.

Let $y_1 = f(x_1)$ and $y_2 = f(x_2)$, $x_1, x_2 \in C$. By 3.1.3 there is an $f_1 \in F$ such that $f_1 | C \in F \| C$ and $f_1(x_1) = x_2$. By the above remarks, $f_1 | f(C) \in F \| f(C)$; and

$$f_1(y_1) = f_1 \circ f(x_1) = f \circ f_1(x_1) = f(x_2) = y_2.$$

Next, we remark that $f_1 | C = f_2 | C \in F \| C$, for $f_1, f_2 \in F$ implies $f_1 | f(C) = f_2 | f(C)$. Hence we may define a map $\varphi : F \| C \to F \| f(C)$ by putting

$$\varphi(f_1 | C) = f_1 | f(C).$$

This map is obviously a homomorphism: if $f_1 | C \in F \| C$ and $f_2 | C \in F \| C$, then

$$\varphi((f_1 | C) \circ (f_2 | C)) = \varphi(f_1 \circ f_2 | C) = f_1 \circ f_2 | f(C) =$$

$$= (f_1 | f(C)) \circ (f_2 | f(C)) = \varphi(f_1 | C) \circ \varphi(f_2 | C).$$

It only remains to show that φ is onto.

Let $g \in F \| f(C)$. Take $y_1 \in f(C)$, and let $y_2 = g(y_1)$. By the above there is an $f_1 \in F$ such that $f_1 | C \in F \| C$ and $f_1 | C \in F \| C$ and $f_1(y_1) = y_2$. Then $\varphi(f_1) = f_1 | f(C) \in F \| f(C)$ and $(\varphi(f_1))(y_1) = y_2$, which shows that $\varphi(f_1) = g$.

3.1.7. If for some cycle C it happens that $f(C) \subset C$ for all $f \in F$, this means exactly that in skeleton $(\Gamma ; \geq)$ of X the cycle C is minimal. We will denote by Γ_m the subset of Γ consisting of all minimal cycles:

$$\Gamma_m = \left\{ C \in \Gamma : f(C) \subset C \text{ for all } f \in F \right\}.$$

Furthermore, we will write Γ_o for the set $\Gamma \setminus \Gamma_1$.

The maximal elements of $(\Gamma ; z)$ are the cycles C such that $C \supset f(C')$, $C' \in \Gamma$, $f \in F$, implies $C = C'$. From this it follows that if C is maximal, then $X \setminus C$ is an invariant subset in X under F.

The set of all maximal cycles will be denoted by Γ_M.

3.1.8. Theorem. A subset C of X is a maximal cycle if and only if $X \setminus C$ is a maximal invariant subset.

Proof

First assume C to be a maximal cycle. We saw already that $X \setminus C$ is invariant under F. If $x \in C$, then $F((X \setminus C) \cup \{x\}) = (X \setminus C) \cup F(x) = (X \setminus C) \cup C = X$; hence $X \setminus C$ is a maximal invariant subset.

Conversely, suppose that $X \setminus C$ is a maximal invariant subset. We first show that then C is a cycle. Indeed, if C were not a cycle then there would exist $x, y \in C$ such that $f(x) \neq y$, for all $f \in F$. But then $(F \setminus C) \cup F(x)$ would be an invariant subset distinct from X and strictly containing $X \setminus C$.

Finally, we prove that C is a maximal cycle. Suppose $C \supset f(C')$, for some $C' \in \Gamma$ and some $f \in F$. Then we cannot have $C' \subset X \setminus C$; but $C' \cap C \neq \emptyset \Rightarrow C' = C$.

3.1.8. Proposition. Every orbit contains at most one minimal cycle.

Proof

Let $F(x) \supset C_1$, $F(x) \supset C_2$, $C_1, C_2 \in \Gamma_m$. Then $f_1(x) \in C_1$, $f_2(x) \in C_2$, $f_1, f_2 \in F$. Then, $f_1 \circ f_2(x) \in C_2$, and $f_1 \circ f_2(x) = f_2 \circ f_1(x) \in C_1$. Hence, $C_1 = C_2$.

3.2. <u>The nuclei of F</u>.

3.2.1. Let G be an abstract semigroup, and let 0 be an element not contained in G. If we define in $G \cup \{0\}$ a multiplication as follows:

if $a,b \in G$ $a.b = ab$ where ab is the product in G;

$0.a = a.0 = 0.0 = 0$ for all $a \in G$;

then $G \cup \{0\}$ is a semigroup, containing G as a subsemigroup. We say that this semigroup is obtained from G by adjoining a zero element.

Every semigroup that can be obtained from a group in such a way will be called "par abus de language", a group with zero. For example, every ring is a group with zero under multiplication.

3.2.2. If $C \in \Gamma_o$, let Z(C) be the semigroup obtained from $F \| C$ by adjoining a zero element. If $C \in \Gamma_m$, let Z(C) be the group $F \| C$.

As it will not cause confusion, for every $C \in \Gamma_o$ we will denote the zero-element adjoined to obtain Z(C) by the same symbol 0.

<u>Theorem</u>. Let $G \in \Gamma$, and let φ be the mapping $F \to Z(C)$ defined as follows:

if $f(C) \subset C$, then $\varphi(f) = f|C$;

if $f(C) \cap C = \emptyset$, then $\varphi(f) = 0$.

Then φ is homomorphism of F onto Z(C).

<u>Proof</u>.

If $C \in \Gamma_m$ then always $f(C) \subset C$, and it is clear that $f \to f|C$ is a homomorphism of F onto $F \| C = Z(C)$.

If $C \in \Gamma_o$ and if $\varphi(f_1) \neq 0$ and $\varphi(f_2) \neq 0$, then it is again evident that $\varphi(f_1 \circ f_2) = (\varphi(f_1)) \circ (\varphi(f_2))$. Assume now that e.g. $\varphi(f_1) = 0$. Then we must prove that $\varphi(f_1 \circ f_2) = 0$ in order to show that again $\varphi(f_1 \circ f_2) = \varphi(f_1) \circ \varphi(f_2)$. Suppose $\varphi(f_1 \circ f_2) \neq 0$, or equivalently, $f_1 \circ f_2(C) \subset C$. Take $x \in G$; then $C = C(x)$, and as $f_1 \circ f_2(x) \in C$ there exists an $f \in F$ such that $x = f \circ f_1 \circ f_2(x) =$ $= f \circ f_2(f_1(x))$. But this shows that $f_1(x) \in C(x)$, contrary to our assumption that $\varphi(f_1) = 0$.

Finally, it is obvious that also for $C \in \Gamma_o$ the mapping $\varphi : F \to Z(C)$ is onto.

3.2.3. Let $S(F)$ be the (unrestricted) direct product

$$S(F) = \prod_{C \in \Gamma} Z(C).$$

Furthermore, let $S_m(F)$ be the (unrestricted) direct product

$$S_m(F) = \prod_{C \in \Gamma_m} Z(C),$$

except if $\Gamma_m = \emptyset$; if $\Gamma_m = \emptyset$, let $S_m(F)$ be an one-element group. Similarly, $S_M(F)$ will denote a one-element group if $\Gamma_M = \emptyset$, and will denote the direct product

$$S_M(F) = \prod_{C \in \Gamma_M} Z(C)$$

if $\Gamma_M \neq \emptyset$.

Then $S(F)$ and $S_M(F)$ are commutative semigroups and $S_m(F)$ is a commutative group. If there is no danger of confusion we will just write S, S_m and S_M.

We will interprete S, S_m and S_M as spaces of cuntions, defined on Γ, Γ_m or Γ_M, and taking their values in the semigroup $Z(C)$. For instance, if $s \in S$ we will write $s(C)$ for the component of s in $Z(C)$. Thus, $s \to s \mid \Gamma_m$ is the canonical homomorphism of S onto S_m, if $\Gamma_m \neq \emptyset$.

3.2.4. Definition. If $f \in F$, then let $\hat{f}$ be the element of $S(F)$ defined as follows:

$$\hat{f}(C) = f \mid C \qquad \text{if } f(C) \subset C;$$

$$\hat{f}(C) = 0 \qquad \text{if } f(C) \cap C = \emptyset.$$

Furthermore, let $\hat{f}' = \hat{f} \mid \Gamma_m$, if $\Gamma_m \neq \emptyset$; else, let $\hat{f}'$ be the unique element of S_m.

For every $C \in \Gamma$, the mapping $f \to \hat{f}(C)$ is a homomorphism of F onto $Z(C)$ by theorem 3.1.8. Hence the mapping $f \to \hat{f}$ is a homomorphism of F into $S(F)$, and the mapping $f \longrightarrow \hat{f}'$ is a homomorphism of F into $S_m(F)$.

3.2.5. <u>Definition</u>. The <u>nucleus</u> $N(F)$ of F is the subset

$$N(F) = \left\{ f \in F \;:\; \hat{f}(C) = 0 \text{ for all } C \in \Gamma_o \right\}$$

of F. The <u>extended nucleus</u> $N^*(F)$ of F is the set

$$N^*(F) = \left\{ f \in F \;:\; \hat{f}(C) = 0 \text{ for some } C \in \Gamma_o \right\}.$$

3.2.6. <u>Theorem</u>. Each of the sets N, N^* is either empty or an ideal of F, and $N \subset N^*$; and $N^* = \emptyset \Longleftrightarrow \Gamma_o = \emptyset$. Furthermore, $F \setminus N^*$ is a sub-semigroup of F, and the restriction of the map $f \longrightarrow \hat{f}$ to $F \setminus N^*$ is a 1.1. homomorphism of $F \setminus N^*$ into $S(F)$.

<u>Proof</u>

It is obvious that $N \subset N^*$ and that $N^* = \emptyset \Longleftrightarrow \Gamma_o = \emptyset$. The fact that N and N^*, if non-void, are ideals follows from the fact that $f(C) = 0$ implies $g \circ f(C) = g(C) \cdot f(C) = 0$ for all $g \in F$. If $f, g \in F \setminus N^*$, then $f(C) \subset C$ and $g(C) \subset C$ for all $C \in \Gamma$; hence $f \circ g(C) \subset C$ for all $C \in \Gamma$, or $f \circ g \quad F \setminus N^*$. This shows that $F \setminus N^*$ is a sub-semigroup of F.

Finally, we must show that the map $f \longrightarrow \hat{f}$ is 1.1. on $F \setminus N^*$. But if $f \neq g$, where $f, g \in F \setminus N^*$, then there is an $x \in X$ such that $f(x) \neq g(x)$. It follows that $\hat{f}(C(x)) = f|C(x) \neq g|C(x) = \hat{g}(C(x))$; hence $\hat{f} \neq \hat{g}$.

3.2.7. <u>Remark</u>. In general, the mapping $f \longrightarrow \hat{f}$ is not 1.1. on all of F. <u>Example</u>. Let X be the set of non-negative integers. Let $f : X \longrightarrow X$ be the mapping

$$f(0) = 0 \;; \qquad f(n) = n+1 \qquad \text{if } n \neq 0.$$

Let F be the commutative semigroup consisting of i and all iterates f^k $(k=1,2,\ldots)$. Then $\Gamma_o(F) = \left\{ \{n\} : n \neq 0 \right\}$, and $\Gamma_m(F) = \left\{ \{0\} \right\}$. All mappings f^k $(k=1,2,\ldots)$ are pairwise distinct; however, $\widehat{f^k} = \hat{f}$ for all k.

3.2.8. Also, the mapping $f \longrightarrow f'$, restricted to $F \setminus N^*$, in general is not a 1.1. map of $F \setminus N^*$ into $S_m(F)$, even if $\Gamma_m \neq 0$.

Example. . . . Let X be the set of all pairs (n,m) such that n is a non-negative integer and m=0,1 or 2. Let $f : X \to X$ be defined as follows:

$$f(0,m) = (0,m) \qquad \text{for } m=0,1,2;$$
$$f(n,m) = (n,m+1) \qquad \text{for } n\neq 0 \text{ and } m=0,1;$$
$$f(n,2) = (n,0) \qquad \text{for } n \neq 0.$$

Define $g : X \to X$ as follows:

$$g(0,m) = 0,m) \qquad \text{for } m=0,1,2;$$
$$g(n,m) = (n+1,m) \qquad \text{for } n\neq 0 \text{ and } m=0,1,2.$$

Then f,g and i generate a commutative semigroup $F \subset X^X$; $\Gamma_o(F)$ consists of all triples $\{(n,m) : m = 0,1,2\}$ with $n > 0$, and $\Gamma_m(F) = \{\{(0,0)\}, \{(0,1)\}, \{(0,2)\}$. Although f and f^2 are in $F \setminus N^*$ and $f \neq f^2$, we have $f|C = f^2|C = i|C$ for all $C \in \Gamma_m$; hence $\hat{f}' = \hat{f^2}'$.

3.2.9. In the proof of the next theorem we need some new notation. If $C \in \Gamma$, let M(C) be the following subset of X:

$$M(C) = \cup\{C' \in \Gamma : C' \geqslant C\}.$$

In other words, $M(C) = \{x \in X : (\exists f \in F)(f(x) \in C)\}$.
Furthermore, put

$$M_\infty = X \setminus \bigcup_{C \in \Gamma_m} M(C).$$

3.2.10. Lemma. For each $C \in \Gamma_m$, the subset M(C) of X is invariant under F. Similarly, M_∞ is invariant under F.

Proof

First assume $C \in \Gamma_m$; let $x \in M(C)$ and $f \in F$. We must show that $f(x) \in M(C)$. Let $f_1 \in F$ such that $f_1(x) \in C$. Then $f_1 \circ f(x) = f \circ f_1(x) \in C$ as C is minimal.

Next, let $x \in M_\infty$ and $f \in F$. Then $f(x) \in M_\infty$, for if $f(x) \in M(C)$ for some $C \in \Gamma_m$, then we would have $C \leqslant C(f(x)) \leqslant C(x)$, which implies $x \in M(C)$.

3.2.11. Theorem. Let $F \subset X^X$ be a commutative semigroup containing the identity map. Then there is a commutative semigroup G, $F \subset G \subset X^X$, with the following properties:

(a) $\Gamma_m(G) = \Gamma_m(F)$;

(b) $F \| C = G \| C$ for every $C \in \Gamma_m$; hence $S_m(G) = S_m(F)$;

(c) the homomorphism $g \to g'$ of G into $S_m(G)$ is onto.

Proof

We define a set G, $F \subset G \subset X^X$, as follows:

$$G = \{ g \in X^X : (\forall C \in \Gamma_m)(\exists f \in F)(f|M(C) = g|M(C)) \text{ and } (\exists f \in F)(f|M_\infty = g|M_\infty) \}.$$

It will be shown that G satisfies all requirements.

First we prove that G is a semigroup. Let $g_1, g_2 \in G$. Take a $C \in \Gamma_m$, and let $f_1, f_2 \in F$ such that $f_j|M(C) = g_j|M(C), (j=1,2,\ldots)$. Then $f_j(M(C)) \subset M(C)$ $(j=1,2,\ldots)$ by lemma 3.2.10, and it follows that $g_1 \circ g_2|M(C) = f_1 \circ f_2|M(C)$. In the same way, if $f_j \in F$ such that $f'_j|M_\infty = g_j|M_\infty$, we find that $g_1 \circ g_2|M_\infty = f'_1 \circ f'_2|M_\infty$. Hence $g_1 \circ g_2 \in G$.

In an exactly analogous way one shows that G is commutative. It is evident that G meets the requirements (a) and (b). We will show now that G also satisfies (c). As this is evident if $\Gamma_m = \emptyset$, we may assume $\Gamma_m \neq \emptyset$.

Let $s \in S_m(g)$. For every $C \in \Gamma_m$, let $f_C \in F$ such that $f_C|C = s(C)$. Then a mapping $f : X \to X$ is defined by putting

$$f|M(C) = f_C|M(C);$$
$$f|M_\infty = i|M_\infty.$$

Then $f \in G$, and obviously $\hat{f}' = s$.

3.2.12. Corollary. If $N^*(F) = \emptyset$, then F is contained in a commutative group of mappings $X \to X$.

Proof

$N^*(F) = \emptyset$ is equivalent to $\Gamma_o(F) = \emptyset$; we see from the above construction that this implies $\Gamma_o(G) = \emptyset$. Hence $S_m(G) = S(G)$. Then (using theorem 3.2.6. the mapping $g \to g'$ is a 1.1. homomorphism of G onto a group; this implies that G is a group.

3.2.13.Corollary. If F is a maximal commutative semigroup of mappings $X \to X$ then the homomorphism $f \to \hat{f}'$ of F into $S_m(F)$ is onto.

It does not follow from $N^*(F) = \emptyset$ that F is itself a group.

Example. Let X be the set of all pairs (n,m) such that n,m are natural numbers and $n \geq m$. Let $f : X \to X$ be defined as follows:

$$f(n,m) = (n,m+1) \qquad \text{if } m < n;$$
$$f(n,n) = (n,1).$$

Let F be the commutative semigroup consisting of i and all iterates f^k $(k \geq 1)$. Then $C(n,m) = \{(n,k) : 1 \leq k \leq n\}$; hence $\Gamma_o = \emptyset$, which is equivalent to $N^* = \emptyset$ (theorem 4). But F is not a group, for obviously f has no inverse in F.

3.2.14. The converse of corollary 3.2.12.is false: if F is contained in a commutative group $G \subset X^X$, it is not necessarily true that $N^*(F) = \emptyset$.

Example. Let X consist of all pairs (n,m) such that n is an integer and m = 0 or 1. Define $f : X \to X$ by

$$f(n,0) = (n,1) \qquad \text{for all } n;$$
$$f(n,1) = (n,0) \qquad \text{for all } n.$$

Define $g : X \to X$ as follows:

$$g(n,m) = (n+1,m) \qquad \text{for every } (n,m) \in X.$$

Then i,f and g generate a commutative semigroup F. As $C(n,m) = \{(n,0),(n,1)\}$ for every $(n,m) \in X$, we see that $g(C) \cap C = \emptyset$ for all $C \in \Gamma(F)$. Hence $g \in N^*(F)$, so $N^*(F) \neq \emptyset$.

Nevertheless, F is contained in a commutative group G. For if $h : X \to X$ is the mapping

$$h(n,m) = (n-1,m) \qquad \text{for every } (n,m) \in X,$$

then it is easily checked that i,f,g and h generate a commutative group containing F.

3.2.15. However, although the converse of corollary 3.2.12. is false; there is a weaker statement which is almost trivially true.

Theorem. If F is a group, then $N^*(F) = \emptyset$.

Proof

For no $C \in \Gamma$ and $f \in F$ it can occur that $\hat{f}(C) = 0$, as $\hat{f}(C).\widehat{f^{-1}}(C) = \hat{i}(C) \neq 0$.

3.2.16. Theorem. If $F \subset X^X$ is a maximal commutative group, and the mappings $f \in F$ have no common fixed point, then F is a maximal commutative semigroup.

Proof

By theorem 3.2.15. $N^*(F) = \emptyset$. It then follows from theorem 3.2.11. that the homomorphism $f \to \hat{f}$ is an isomorphism of F onto the group $S(F) = S_m(F)$.

Suppose F is properly contained in a commutative semigroup $G \subset X^X$; let $g \in G \setminus F$. Then there must exist an $x \in X$ such that $g(x) \notin C(x)$; let $C_1 = C(g(x))$. As there is no common fixed point, C_1 contains more than one point; let $y \in C_1$, $y \neq g(x)$.

As $f \to \hat{f}$ is onto, there exists an $f \in F$ such that $f \circ g(x) = y$ and $f|C(x) = i|C(x)$. Then $g \circ f(x) = g(x) \neq y = f \circ g(x)$, contradicting the assumption that G is commutative.

If F has a common fixed point, then the assertion is obviously false as soon as X contains more than one point. For if x_o is the common fixed point, the mapping f such that $f(x) = x_o$ for all $x \in X$ commutes with every map in F, and it cannot be contained in F as f is not 1.1. and all mappings in F are invertible.

3.3. Transformation semigroups F such that $N(F) = N^*(F)$

The transformation semigroups F for which the extended nucleus N coincides with the nucleus N^* have a number of nice properties. For in this case we often need only study the maximal and minimal cycles, as follows from the next theorem.

3.3.1. Theorem. If $N(F) = N^*(F)$, and if $C(f(x)) \in \Gamma_o$, then $C(f(x)) = fC(x)$, and the group $F \| C(f(x))$ is a homomorphic image of the group $F \| C(x)$.

Proof

Assume $N(F) = N^*(F)$, and let $C(f(x)) \in \Gamma_o$. Let $C = C(x)$; by 3.1.5.(a) $fC \subset C(f(x))$; we will show that f maps C onto $C(f(x))$.

Take $y \in C(f(x))$. Then there exists an $f_1 \in F$ such that $f_1(f(x)) = y$. As $\hat{f}_1(C(f(x)) \neq 0$, and as $C(f(x)) \in \Gamma_o$, we see that $\hat{f}_1 \notin N = N^*$; hence $\hat{f}_1(C) \neq 0$, which means that $f_1(C) \subset C$. In particular, $f_1(x) \in C$; as $y = f_1 \circ f(x) = f(f_1(x))$, we find that $y \in f(C)$.

The last assertion of the theorem is an immediate consequence of theorem 3.1.6.

3.3.2. As an immediate application, consider the case that $C(x)$ is finite. Then if $N(F) = N^*(F)$ and if $C(f(x))$ is not minimal, it follows from theorem 3.3.1. that the number of elements of $C(f(x))$ is a divisor of the number of elements of $C(x)$. (There is a 1.1. correspondence between the elements of C and the elements of $F \| C$, for every $C \in \Gamma$).

The following consequence of theorem 3.3.1. is of more importance. If $N = N^*$, we need only consider those cycles under F that are either maximal or minimal, assuming that there are enough maximal cycles; in a certain sense, the homomorphism of F into $\prod_{C \in \Gamma_M \cup \Gamma_m} Z(C)$ is just as good, in this case, as the representation $f \longrightarrow f$ of F into all of $S(F)$. This is expressed by the following theorem.

3.3.3. Theorem. Assume $N(F) = N^*(F)$, and suppose that for every $C \in \Gamma$ there exists a $C_M \in \Gamma_M$ such that $C \leqslant C_M$. Then the image of F in $S(F)$ under the map $f \longrightarrow \hat{f}$ is isomorphic to the image of F in $\prod_{C \in \Gamma_m \cup \Gamma_M} Z(C)$ under the map $f \longrightarrow \hat{f} \,|\, (\Gamma_m \cup \Gamma_M)$.

Proof

As $s \longrightarrow s \,|\, (\Gamma_m \cup \Gamma_M)$ is a homomorphism of $S(F)$ onto $\prod_{C \in \Gamma_M \cup \Gamma_m} Z(C)$, we need only to prove that this map, restricted to $\{\hat{f} : f \in F\}$, is 1.1.

Hence take $f, g \in F$ such that $\hat{f} \neq \hat{g}$. As $X = \bigcup_{C \in \Gamma} C$, there is a $C \in \Gamma$ such that $f|C \neq g|C$. If $C \in \Gamma_m$, it follows that

(a) $$\hat{f} \,|\, (\Gamma_m \cup \Gamma_M) \neq \hat{g} \,|\, (\Gamma_m \cup \Gamma_M);$$

if there is no $C \in \Gamma_m$ such that $f|C \neq g|C$, we must distinguish two cases. In the first place, it is possible that $f(C) \cap C \neq \emptyset$, for some $C \in \Gamma$. As

$N = N^*$, it follows that $\hat{f}(C) = 0$ for all $C \in \Gamma \setminus \Gamma_m$; furthermore $\hat{f}(C) = \hat{g}(C)$ for all $C \in \Gamma_m$. Hence $\hat{g}(C) \neq 0$ for all $C \in \Gamma$, as we assumed $\hat{f} \neq \hat{g}$. In particular, if $C \in \Gamma_M \setminus \Gamma_m$ (such C exist, as $\Gamma \setminus \Gamma_m \neq \emptyset$), then $\hat{f}(C) = 0 \neq \hat{g}(C)$, which again implies (a).

In the second place, it may happen that $\hat{f}(C) \neq 0$ and $\hat{g}(C) \neq 0$ for all $C \in \Gamma$. Let $C \in \Gamma$ such that $f|C \neq g|C$, and let $C_M \in \Gamma_M$ such that $C \leqslant C_M$. Then $f|C_M \neq g|C_M$, by theorem 3.3.1. and this again proves (a).

3.3.4. <u>Corollary</u>. Suppose F satisfies the following three conditions:

(a) $N(F) = N^*(F)$;

(b) for every $C \in \Gamma$ there exists a $C_M \in \Gamma_M$ such that $C \leqslant C_M$;

(c) every $C \in \Gamma_m$ consists of only one point.

Then the image of F in S(F) under the homomorphism $f \longrightarrow \hat{f}$ is isomorphic. to the image of F in $S_M(F)$ under the homomorphism $f \longrightarrow \hat{f} \mid \Gamma_M$.

Using theorem 3.1.8. this corollary could be stated in another form, in which maximal invariant subsets of X figure instead of maximal cycles.

3.3.5. If X is finite, it is easy to characterize N(F). In fact, a weaker assumption that the finiteness of X is sufficient. Let us call a partially ordered set $(S, \leqslant)$ <u>chain-finite</u> if every subset of S that is linearly ordered under $\leqslant$ is finite. Then the following holds:

<u>Theorem</u>. If the skeleton $(\Gamma, \leqslant)$ is chain-finite, then

$$N = \left\{ f \in F : (\forall x \in X)(f^n(x) \in \bigcup_{C \in \Gamma_m} C \text{ for some natural number } n) \right\} .$$

<u>Proof</u>

Assume $f \in N$, and let $x \in X$. If $f(C(x)) \subset C(x)$, then $C(x) \in \Gamma_m$ and $f(x) \in \bigcup_{C \in \Gamma_m} C$. If $f(C(x)) \not\subset C(x)$, then $C(f(x)) < C(x)$. If $C(f(x)) \in \Gamma_m$, then $f(x) \in C(f(x)) \in \bigcup_{C \in \Gamma_m} C$; else $C(f(x)) < C(f(x))$.

Now the chain $C(x) \geqslant C(f(x)) \geqslant C(f^2(x)) \geqslant \ldots$ must be finite, hence there is a natural number n such that $C(f^{n-1}(x)) = C(f^n(x))$. Then $C(f^n(x)) \in \Gamma_m$, and $f^n(x) \in \bigcup_{C \in \Gamma_m} C$.

Conversely, suppose that for every $x \in X$ there exist a natural number n such that $f^n(x) \in \bigcup_{C \in \Gamma_m} C$. Then it follows that $f \in N$, for if $C(x) \notin \Gamma_m$, $f(C(x)) \subset C(x)$ would imply $f^n(x) \in C(x)$ for all natural numbers n.

3.4. Abstract commutative semigroups

Let (A,.) be a commutative semigroup with identity e. If $a \in A$ we will denote by ma, see 1.2.3., the mapping

$$(ma)x = ax$$

of A into A.

We can interprete the theory of the previous sections in the case where F = (mA,o) and X=A. It then turns out that the cycles of F in A coincide with certain subsets of A studied in the theory of abstract semigroups.

3.4.1. In this latter theory the following two equivalence relations $\mathcal{L}$ and $\mathcal{R}$ are defined. One says that $a\mathcal{L}b$ if a and b generate the same principal right ideal in (A,.):

$$a\mathcal{L}b \Leftrightarrow \{a\} \cup Aa = \{b\} \cup Ab,$$

and analogously one says that $a\mathcal{R}b$ if a and b generate the same principal right ideal in (A,.):

$$a\mathcal{R}b \Leftrightarrow \{a\}\ aA = \{b\} \cup bA.$$

As (A,.) is commutative and has an identity element, $a \in aA = Aa$; hence the equivalence relations $\mathcal{L}$ and $\mathcal{R}$ coincide, and

$$a\mathcal{L}b \Leftrightarrow a\mathcal{R}b \Leftrightarrow aA = bA.$$

On the other hand,

$$\begin{aligned} a\mathcal{C}B &\Leftrightarrow (\exists\, mx \in F)(\exists\, my \in F)((mx)a = b \text{ and } (my)b = a) \\ &\Leftrightarrow (\exists\, x \in A)(\exists\, y \in A)(xa = b \text{ and } yb = a) \\ &\Leftrightarrow b \in aA \text{ and } a \in bA \\ &\Leftrightarrow aA = bA; \end{aligned}$$

hence the equivalence relation $\mathcal{C}$ coincides both with $\mathcal{L}$ and with $\mathcal{R}$, and the cycles are exactly the $\mathcal{L}$-sets or $\mathcal{R}$-sets.

3.4.2. <u>Theorem.</u> The skeleton $(\Gamma, \leq)$ of A under F is directed below.

<u>Proof</u>

Let $C_1, C_2 \in \Gamma$. Take $x \in C_1$ and $y \in C_2$; as $xy = (mx)y = (my)x$, we have $C(xy) \leq C_1$ and $C(xy) \leq C_2$.

<u>Corollary</u>. There is at most one minimal cycle.

<u>Corollary</u>. Either $M_\infty = A$ or $M_\infty = \emptyset$.

3.4.3. By theorem 3.2.15., if (A,.) is a group then $\Gamma_o = \emptyset$ and hence Γ consists only of the minimal cycle. On the other hand if (A,.) has only one cycle then it is a group, for in this case A = C(e), and C(e), the set of all invertible elements in A, is always a group.

3.4.4. In the theory of abstract semigroups the concept of quasi-invertible is defined. Reduced to the commutative case, an element a of a commutative semigroup (A,.) is said to be <u>quasi-invertible</u> if there exists an $a^* \in A$ such that

$$a^* ax = x$$

for all $x \in A$.

In our considerations, we need a weaker concept.

<u>Definition</u>. An element a of a commutative semigroup (A,.) is called <u>locally invertible</u> if there exists an $x \neq 0$ and an a^* in A such that $a^* ax = x$.

3.4.5. <u>Theorem</u>. Let (A,.) be a commutative semigroup with a zero and an identity element. Then N(mA) is the set of all ma $(a \in A)$ such that a is not locally invertible.

<u>Proof</u>

If a is a locally invertible element, then there are an $x \neq 0$ and an a^* in A such that $a^* ax = x$.

As $x \neq 0$, C(x) is not the minimal cycle $C(0) = \{0\}$; and $x = a^* ax$ implies $ax \in C(x)$, hence $(ma)(C(x)) \subset C(x)$; thus $ma \notin N(mA)$.

If a is not locally invertible, then for every $x \neq 0$, $(ma)C(x) \cap C(x) = \emptyset$; hence $ma \in N(mA)$.

3.4.6. Theorem. Let $(A,.)$ be a commutative semigroup with a zero and an identity element. Then $N(mA) = N^*(mA)$ if and only if every locally invertible element is invertible.

Proof

Suppose $N(mA) = N^*(mA)$, and let a be locally invertible. Then for some $x \neq 0$ and some $a^* \in A$, $a^*ax = x$. This means that $(ma)C(x) \subset C(x)$; as $C(x)$ is not minimal, it follows that $(ma)C(1) \subset C(1)$. Hence $a = a.1 \in C(1)$; i.e. a is invertible.

Conversely, suppose every locally invertible element is invertible. Assume $N \neq N^*$; then there exists an $a \in A$ such that $ma \in N^* \setminus N$. But then there must exist $x,y \in A$, $x \neq 0$, such that

$$(ma)C(x) \subset C(x), \quad (ma)C(y) \cap C(y) = \emptyset.$$

From $(ma)C(x) \subset C(x)$ it follows that there is an a^* such that $x = (ma^*)(ma)(x) = a^*ax$; hence a is locally invertible. But then a is invertible; let a^{-1} be its inverse. Then $y = a^{-1}.ay = (ma^{-1})(ma)y$, which shows that $(ma)y \in C(y)$: contradiction.

3.4.7. Example. If $(A,.)$ is a commutative cancellation semigroup with zero and identity, then $N(mA) = N^*(mA)$.

In the case of abstract semigroups, corollary 3.2.12 reduces to the following: $N^*(mA) = \emptyset$ if and only if every non-zero element is invertible.

As a corollary of theorem 3.4.2. we obtain

3.4.8. Theorem. In a finite commutative semigroup $(A,.)$ with 0 and 1, an element a is not locally invertible if and only if it is nilpotent:

$$a^n = 0 \qquad \text{for some natural number } n.$$

Similarly the other results of the previous sections can be applied to the case of abstract commutative semigroups with identity; the theory of these semigroups in a certain sense is contained in the theory of commutative transformation semigroups.

4. Realization of relations

4.1. Definitions

4.1.1. In 1.4.5. we showed that to every commutative semigroup of transformations $(F;X)$ we can adjoin a relation $)_F$ as follows:

$$x \,)_F\, y \Longleftrightarrow (\exists f \in F)(f(x) = y).$$

Now we can ask, which relations on the set X can be obtained by this process. Precisely:

Definition. Let R be a binary relation on the set X. The relation is said to be realisable by a commutative transformation semigroup, or shortly to be realisable, if there exists a commutative transformation semigroup $(F;X)$ containing the identity mapping such that

$$x\, R\, y \Longleftrightarrow x \,)_F\, y.$$

4.1.2. The following conditions are necessary for R in order to be realisable:

(a) $x\, R\, x$ for every $x \in Y$,

(b) $x\, R\, y,\ y\, R\, z \Rightarrow x\, R\, z$,

(c) $x\, R\, y_1,\ x\, R\, y_2 \Rightarrow (\exists z \in X)(y_1 Rz, y_2 Rz)$.

In other words: R must be an N-relation.
The proof follows immediately from 1.6.7.

4.1.3. Using the notation from 1.6. and 3.1.1., we have the following proposition:

If R is realisable by $(F;X)$ then $(X_R; \leq_R)$ is realisable by $(\overline{F}; \Gamma(F))$.

The following simple example shows that if $(X_R; \leq_R)$ is realisable by $(G;X_R)$, there need not exist a realisation of R by an $(F;X)$ such that $(G;X_R) = (\overline{F}; \Gamma(F))$, even if R itself is an N-relation.

Example. Let $X = \{1;2;3;4;5;6\}$ and let the relation R be defined as follows

	1	2	3	4	5	6
1	R	R	R	R	R	R
2	R	R	R	R	R	R
3			R	R	R	R
4			R	R	R	R
5			R	R	R	R
6						R

X_R contains three sets, namely $X_1 = \{1;2\}$, $X_2 = \{3;4;5\}$, $X_3 = \{6\}$.

The relation $P = \geqslant_R$ is the following relation:

	x_1	x_2	x_3
x_1	P	P	P
x_2		P	P
x_3			P

Let G consist of the mappings g_1, g_2, g_3, where

	x_1	x_2	x_3
g_1	x_1	x_2	x_3
g_2	x_2	x_3	x_3
g_3	x_3	x_3	x_3

Then $(G;X_R)$ is a realization of the relation $\geqslant_R$. Let us suppose that R is realisable by a system $(F;X)$ such that $(\bar{F}; \Gamma(F)) = (G;X_R)$. It is easily seen that $N(F) = N^*(F)$. According to 3.3.2., the cardinal $|X_1|$ must be divisible by $|X_2|$, and this is impossible as $|X_1| = 2$, $|X_2| = 3$.

4.1.4. Let R be an N-relation on a set X. According to 1.6.10 we shall define a relation M_R on x as follows:

$$x \, M_R y \iff \exists \, z \in X \, : \, x \, R \, z, \; y \, R \, z.$$

It is obvious that M_R is an equivalence relation. Evidently,

$$x \; R \; y \Longrightarrow x \; M_R \; y.$$

Theorem. Let R be an N-relation. R is realisable if and only if R, restricted to $M_R(x)$, is realisable for every $x \in X$.

Proof

If R is realisable by (F;X), then R on $M_R(x)$ is evidently realisable by $(F|M_R(x);\, M_R(x))$, as $M_R(x)$ is invariant under F.

Suppose R, restricted to $M_R(x)$, can be realized by $(F_x;M_R(x))$. Let Y, $Y \subset X$ be a subset of X such that $Y \cap M_R(x)$ contains precisely one point for every $x \in X$. Then

$$\mathfrak{S}\,(F_x;x \in Y)$$

realises F.

4.2. Dependence of cycles; non-realisable skeletons.

4.2.1. The example in 4.1.3. suggests the introduction of a notion of dependence of cycles.

Definition. Let (F;X) be a commutative transformation semigroup containing the identity mapping. Let C(x),C(y) be cycles under (F;X). The cycle C(x) is said to be dependent on C(y) if there exists a mapping $f \in F$ such that $\overset{-1}{f}(C(x)) = C(y)$.

Evidently each cycle is dependent on itself.

4.2.2. Proposition. If C(x) is dependent on C(y) then $F\|C(x)$ is a homomorphic image of $F\|C(y)$.

Proof

By 3.1.6., it is enough to prove that there exists an $f \in F$ such that $f(C(y)) = C(x)$. Let $f \in F$ be such mapping that $\overset{-1}{f}(C(x)) = C(y)$. Then also $C(x) = f(C(y))$ and the proposition is proved.

4.2.3. The cycle C(x) is called independent if C(x) is the only cycle on which C(x) depends.

F is said independent if every cycle defined by F is independent.

Theorem. Let R be an N-relation on a countable set X, such that $X_1, X_2 \in X_R$, $X_1 \cap X_2 = \emptyset$ implies that $|X_1|$ and $|X_2|$ are two different prime numbers. If R can be realised by (F;X), then F must be independent.

Proof

Let us suppose that (F;X) is not independent. Then there exist $X_1, X_2 \in X_R$ such that $X_1 \neq X_2$, X_1 depending on X_2. But this leads to a contradiction, as $F \| X_1$ must be a homomorphic image of $F \| X_2$, which is not possible as $F \| X_1$ and $F \| X_2$ are finite groups of the different prime orders.

4.2.4. In this section we prove the existence of an N-relation, which cannot be realized by any independent (F;X).

Lemma. Let $X = \{1;2;3;4;5;6\}$. Let R be the following relation

	1	2	3	4	5	6
1	R	R	R	R	R	R
2		R		R	R	R
3			R	R	R	R
4				R		R
5					R	R
6						R

Then R is an N-relation and R cannot be realized by any independent F.

Proof

Let us assume that R can be realized by any independent F. There must exist mappings $f_2, f_3 \in F$ such that $f_2(1) = 2$ and $f_3(1) = 3$. As F is supposed to be independent, the following must hold:

$$f_2(2) = 2, \quad f_3(3) = 3.$$

For if not, then 2 or 3 would depend on 1. According to 1.6.9. (b) we have $f_2(4) = 4$, $f_2(5) = 5$, $f_2(6) = 6$, $f_3(4) = 4$, $f_3(5) = 5$, $f_3(6) = 6$. Of course, also

$$f_2 \circ f_3(1) = f_3 \circ f_2(1)$$

which is the same as

$$f_3(2) = f_2(3).$$

As the points 4 and 5 play in the relation R the same role, we can assume that $f_2(3) = f_3(2) \neq 4$. (If not we can assume $f_2(3) = f_3(2) \neq 5$.)

There must exist a mapping $f_4 \in F$ such that $f_4(1) = 4$. As f_4 must commute with f_2 and f_3 we have

$$f_4(2) = f_4 \circ f_2(1) = f_2 \circ f_4(1) = f_2(4) = 4$$

$$f_4(3) = f_4 \circ f_3(1) = f_3 \circ f_4(1) = f_3(4) = 4$$

Now,

$$f_2 \circ f_4(3) = f_2(4) = 4.$$

But the value of $f_4 \circ f_2(3)$ cannot be 4 as $f_2(3)$ could be either 5 or 6, and if the image of one of these points is 4, then this point would have to be in relation R with 4, but this is not true. This is a contradiction.

4.2.5. Theorem. There exists an N-relation, which cannot be realized by any independent F. . Substituting cycles with different prime numbers of points for the points of this skeleton, we get a non-realisable N-relation. This fact follows from 4.2.3.

4.2.6. Now we shall exhibit an example of a non-realisable skeleton. This example was given by P.C. Baayen.

Let $X = \{1,2,3,4,5,6,7\}$ and let a relation R be given as follows

	1	2	3	4	5	6	7
1	R	R	R	R	R	R	R
2		R		R	R	R	R
3			R	R	R	R	R
4				R			R
5					R		R
6						R	R
7							R

Evidently R is an N-relation, $X_R = X$, $\geqslant_R = R$, as no R is below the diagonal. The proof is based on the propositions 1.6.9. (a),(b) and (c). We shall write only (a),(b),(c).

Let us suppose that R is realisable by $(F;X)$. There must exist a mapping $f_2 \in F$, such that $f_2(1) = 2$.

First we shall prove that $f_2(2) \neq 7$. Let $f_2(2) = 7$. Then $f_2(4) = f_2(5) = f_2(6) = 7$ by (a). By (c), $\{4;5;6\} \subset f_2(X)$, and this is impossible as only the point 3 can be carried by f_2 into the set $\{4;5;6\}$.

Let $f_2(2) \in \{4;5;6\}$. As the points 4,5,6 play a symmetrical role in R, we can assume that $f_2(2) = 4$. By (c), $\{5;6\} \subset f_2(X)$, but only the point 3 can be carried into $\{5;6\}$. Therefore we can assume that $f_2(6) = 6$, as the situation is again symmetrical with regard to 5 and 6. But 2 R 6, and therefore there must exist a mapping $g \in F$ such that $g(2) = 6$. Evidently $g \neq f_2$.
But

$$g \circ f_2(2) = g(4) = f_2 \circ g(2) = f_2(6) = 6.$$

Evidently $g(4) \neq 6$, as 4 is not in the relation R with 6.
Therefore $f_2(2) = 2$. By (a), $f_2(3) \in \{3;4;5;6\}$. Let $f_2(3) = 3$. There must exist a mapping $h \in F$ such that $h(1) = 3$.
Then

$$f_2 \circ h(1) = f_2(3) = 3 = h \circ f_2(1) = h(2).$$

But this is impossible as 2 is not in the relation R with 3.
The only remaining case is $f_2(3) = 4$, as the situation is symmetrical with respect to 4,5,6. As $f_2(2) = 2$, it follows that $f_2(5) = 5$ from (b). There must exist $g \in F$ such that $g(3) = 5$. Then

$$f_2 \circ g(3) = f_2 \circ (5) = 5 = g \circ f_2(3) = g(4).$$

This is not possible as 4 is not in the relation R with 5. The proof is completed.

4.3. Realisable relations

4.3.1. Let R be an N-relation on a set X. We know that the set X_R is partially ordered by the relation $\geqslant_R$.

Let Y be a subset of X_R. An element $E_R(x) \in X_R$ is called a lower bound of a subset Y if $E_R(x) \leqslant X_i$, for every $X_i \in Y$. A lower bound $E_R(y)$ is called a greatest bound or meet of Y, if $E_R(y) \geqslant E_R(x)$ for every lower bound $E_R(x)$ of Y.

The meet of a set $Y = \{E_R(x); E_R(y)\}$ we shall denote by $E_R(x) \wedge E_R(y)$. The partially ordered set X_R is called a lower semi lattice, if every two-element set $\{E_R(x)\}$ of X_R has a meet in X_R. It follows that every finite subset of X_R has a meet.

4.3.2. Let L be a lower semi lattice the elements of which are disjoint abstract commutative groups G . Let $X = \bigcup_{G_\alpha \in L} G_\alpha$. We can introduce on X a binary relation R putting

$$x \, R \, y \Leftrightarrow x \in G_\alpha \, , \; y \in G_\beta \, , \; G_\alpha \geqslant G_\beta \, .$$

Then the relation R is realisable by a commutative transformation semigroup.

<u>Proof</u>

Let us denote by $j[G_\alpha]$ the unit element of G_α and by $G_\alpha \wedge G_\beta$ the group that is the meet of G_α and G_β in the semi laatice L. If $x \in X$, say $x \in G_1$, and if $G_2 \in L$, we will define $G_2(x)$ by

$$G_2(x) = x \qquad \text{if} \quad G_1 \leqslant G_2$$
$$G_2(x) = j[G_2] \qquad \text{otherwise.}$$

Then for any $x \in X$ we define a mapping $f_x : X \longrightarrow X$ as follows:

$$f_x(y) = (G_1 \wedge G_2)(x) \; . \; (G_1 \wedge G_2)(y)$$

if $x \in G_1$, $y \in G_2$. The dot here denotes the group multiplication in $G_1 \wedge G_2$.

We assert that $f_x \circ f_y = f_y \circ f_x$, for all $x, y \in X$. Say $x \in G_1$, $y \in G_2$, and take any $z \in X$; say $z \in G_3$.

$$\begin{aligned} f_x \circ f_y(2) &= f_x(G_2 \wedge G_3)(y).(G_2 \wedge G_3)(z) = \\ &= (G_1 \wedge G_2 \wedge G_3)(x).(G_1 \wedge G_2 \wedge G_3)(y).(G_1 \wedge G_2 \wedge G_3)(z) = \\ &= f_y \circ f_x(z). \end{aligned}$$

Hence the f_x, $x \in X$, generate a commutative semigroup F. It is evident that (F;X) realises the relation R. For if

$$x \in G_1;\ y \in G_2, \text{ where } G_1 \geqslant G_2, \text{ then } f_y(x) = y,$$

while if $G_1 = G_2$ we have $f_z(x) = y$, where $z = x^{-1}.y$. On the other hand, if G_1 and G_2 are not comparable, we cannot obtain y as an image of x under any $f \in F$.

4.3.3. Let R be an N-relation on set X. Let $(X_R; \leqslant_R)$ be a lower semi lattice. Then R is realisable.

Proof

It can be easily proved that for every cardinal number t, there exists a commutative group G such that $|G| = t$.

Let $E_R(x) \in X_R$. According to the previous remark we can consider a binary operation, such that $(E_R(x); .)$ is an abstract group. This process can be applied for every $E_R(x) \in X_R$. Hence, we obtain X as a union of disjoint groups, such that the system of the groups forms, according to the assumption, a lower semi lattice.

Evidently,

$$x \mathrel{R} y \iff E_R(x) \geq E_R(y).$$

Applying 4.3.2 we get the assertion of the theorem.

5. Fixed points of commutative mappings

5.1. In this section we shall consider again a commutative transformation semigroup $(F;X)$ containing the identity mapping i, where X is an arbitrary set.

5.1.1. Let us denote by $I(f)$ the set of all fixed points of the mapping $f \in F$,

$$I(f) = \{ x; f(x) = x \} .$$

Proposition. For every $f \in F$ $I(f)$ is an invariant set under $(F;X)$.

Proof

Let $x = f(x)$. Then for each $g \in F$ we have

$$g(x) = g \circ f(x) = f[g(x)] ,$$

and therefore $g(x) \in I(f)$.

A point x_o is called a common fixed point of F if and only if $f(x_o) = x_o$ for every $f \in F$.

x_o is a common fixed point if and only if $x_o \in \bigcap_{f \in F} I(f)$.

x_o is a common fixed point if and only if $\{x_o\}$ is a minimal cycle.

5.1.2. From the previous proposition we immediately have the following:

Proposition. Let $(F;X)$ be a commutative transformation semigroup. Let some $f \in F$ have precisely one fixed point x_o. Then all mappings from $(F;X)$ have x_o as a common fixed point.

5.1.3. The proposition 5.1.2. can be applied in every situation where there is a theorem, which asserts that there exists only one fixed point for some mapping. For example:

Proposition. Let $(X;\rho)$ be a complete metric space, ρ be the metric. Let f be a Lipschitz mapping from X into X with constant $\alpha < 1$. That is

$$\rho[f(x_1);f(x_2)] \leq \alpha \ \rho(x_1;x_2) \qquad \text{for any } x_1,x_2 \in X.$$

Then every mapping g from X into X (continuity is not assumed) commuting with f possesses a fixed point.

5.1.4. Let $f \in (F;X)$, $|I(f)| = m$, where m is a natural number. Then for every mapping $g \in F$ there exists a natural number k, $1 \leq k \leq m$, and a point $x_o \in X$ such that

$$x_o = f(x_o) = \overset{k}{g}(x_o).$$

Proof

As I(f) is invariant, g carries all points of I(f) into I(f). As I(f) has only m points some power of g, less then or equal to m, must have a fixed point in I(f). But this is the assertion of the proposition.

5.1.5. We can discuss the existence of a common fixed point in the terminology of commutative mappings of the fact that (F;X) has a common fixed point x_o if and only if the constant mapping f_o, such that $f_o(x) = x_o$ for each $x \in X$, commutes with every mapping from F.

5.1.6. In every semigroup (F;X) we can introduce the notion of divisibility. Let $f,g \in F$. We shall say that f devides g (in F), if and only if there exists an $h \in F$ such that $g = h \circ f$.

Every mapping $f \in F$, which can be devided by all mapping from F, shall be called a common multiple.

We denote the set of common multiples in F by r(F); this set is called the retract of F.

5.1.7. r(F) is an ideal in (F;o).
r(F) = F if and only if F is a group.

5.1.8. The set r(F) can be void; an example is provided by the multiplicative semigroup of natural numbers.

5.1.9. Let (F;X) have a common fixed point. Then there exists a commutative transformation semigroup (G;X), $G \supset F$, such that $r(G) \neq \emptyset$.

Proof

Let x_o be the common fixed point of F. Let g be the mapping from X into X, such that $g(x) = x_o$ for each $x \in X$. Then g commutes with each mapping in F (see 5.1.5.) and therefore $G = \{F \cup g\}$ is a semigroup with the required property (as $g \in r(G)$).

5.1.10. If F is a finite semigroup, the $r(F) \neq \emptyset$, as the composition of all mappings in F belongs to F and in the same time to $r(F)$.

5.1.11. Proposition. Every mapping in $r(F)$ maps each point into a minimal cycle.

Proof

It is sufficient to prove that for each $x \in X$, $g \in F$, $f \in r(F)$ there exists an $h \in F$ such that

$$f(x) = h \circ g \circ f(x).$$

But f is devided by $g \circ f$, as f is assumed to be a common multiple, Therefore such an $h \in F$ exists.

5.1.12. Let $f_1, f_2 \in r(F)$, $x \in X$. Then $f_1(x)$ and $f_2(x)$ belong to the same minimal cycle.

The proof follows immediately from the fact that the orbit of each point can contain at most one minimal cycle (see 3.1.8).

5.1.13. $r(F)(x)$ is a minimal cycle for every $x \in X$.

Proof

$C(f(x))$, $f \in x(F)$, is a minimal cycle by 5.1.11. Let $y \in C(f(x))$; then for some $g,h \in F$, $y = g \circ f(x)$ and $f(x) = h(y)$. But $g \circ f \in r(F)$ as $r(F)$ is an ideal of $(F;\circ)$.

5.1.14. $r(F) \neq \emptyset$ implies $M_\infty = \emptyset$.

The inverse statement is not true. In general M_∞ may be void while $r(F)$ is empty , as can be seen from the example in 3.2.13.

5.2. In this section we shall formulate a few propositions about commutative transformation semigroups $(F;X)$, such that each mapping from F has at least one fixed point.

5.2.1. If $(F;X)$ is a commutative semigroup of transformations and if every mapping $f \in F$ has a fixed point, then $(F;X)$ need not have a common fixed point. This is easily seen from the following two examples.

a) Let $X = \{1;2;3;4;5;6\}$ and let $(F;X)$ be given by the following table

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	5	6
3	2	1	3	4	6	5
4	1	2	4	3	6	5

$(F;X)$ is evidently a commutative semigroup of transformations. Every mapping $f \in F$ has a fixed point. But there exists no common fixed point. In this case the mapping g

	1	2	3	4	5	6
g	2	1	4	3	6	5

commutes with F, and g has no fixed point.

b) Let X be the set of all non-negative integers. The binary operation

$$x * y = \max(x,y) \qquad x,y \in X$$

is commutative and associative. Therefore $(X;*)$ is a commutative semigroup. Using the notation introduced in 1.2.3., $(m(X);o)$ is a commutative semigroup of transformation. The orbit of 0 under $(m(X);o)$ is X. Hence by 2.2.4. $(m(X);o)$ is a maximal commutative semigroup. Every mapping of $(m(X);o)$ has a fixed point, but there exists no common fixed point.

In the first example we see, that if we embed the system in a maximal commutative system, then not all mappings will have a fixed point anymore.

In the second example the common fixed point is as it were pushed away to infinity.

5.2.2. <u>Theorem</u>. Let $(F;X)$ be a commutative transformation semigroup satisfying the following conditions:

(a) every $f \in \mathbb{P}\{F \mid F(x);\ x \in X\}$ has a fixed point

(b) $r(F) \neq \emptyset$.

Then all mappings in F have a common fixed point.

Proof

If there exists a minimal cycle containing only one point, then this point is a common fixed point by 5.1.1.

Let us assume that every minimal cycle has more than one point. In 1.6.10. we defined for every $(F;X)$ a relation M . The classes of equivalent points according to M are disjoint and cover X. Let Y be one of these classes.

Y contains at least one minimal cycle, as Y is invariant and $r(F)\neq\emptyset$. According to the definition of the relation M, Y cannot contain more than one minimal cycle, as no two points from disjoint minimal cycles can be in the relation M to each other. Therefore Y contains precisely one minimal cycle.

Let $f\in r(F)$. Then $f|Y$ has either no fixed point or it is the identity mapping on the minimal cycle which is contained in Y. This assertion we can prove as follows. $f|Y$ cannot have a fixed point outside of the minimal cycle, as, by 5.1.11., $f|Y$ maps every point of Y into a minimal cycle. Let us denote by C_Y the unique minimal cycle in Y. By 3.1.4., $F\|C_Y$ is a group, and as C_Y is minimal we have

$$F\|C_Y = F|C_Y.$$

Evidently $p(F|C_Y) = 1$.
Therefore every mapping $f\in F$ restricted on C_Y is either identity or has no fixed point in C_Y. As C_Y contains more than two points there must exist a mapping $g\in F$ such that $g|C_Y$ has no fixed point.

Let us define on Y a mapping h_Y as follows:

$$h_Y = f|Y \quad \text{if } f|C_Y \neq i|C_Y$$
$$h_Y = g \circ f|Y \quad \text{if } f|C_Y = i|C_Y.$$

Evidently h_Y has no fixed point in Y and commutes with every mapping in Y. Such a mapping h_Y is defined for every equivalence class according to M. As these classes cover X and are disjoint, we can define a mapping h on X as follows:

$$h|Y = h_Y .$$

Then h commutes with each mapping in F.
Moreover h belongs to $\mathbb{P}(F|F(x);x\in X)$, as h preserves orbits (see 2.4.6.). But h has no fixed point. This is a contradiction. Thus one of the minimal cycles has to have only one point, and the theorem is proved.

5.2.3. Theorem. Let $(F;X)$ be a maximal system of commutative transformations of a finite set X into itself. Let each mapping from $(F;X)$ have a fixed point. Then all mappings from $(F;X)$ have a common fixed point.

Proof

By 1.3.3 $(F;X)$ is a transformation semigroup. By 2.4.7. $\mathbb{P}(F|F(x);x\in X) = F$. By 5.1.10. $r(F) \neq \emptyset$. Therefore we can apply 5.2.2.

5.2.4. Proposition. Every orbit under F can contain at most one common fixed point. The proof follows immediately from 3.1.8.

5.2. In this section we shall show an application of the methods introduced before. Our aim is to prove the theorem 5.2.4.

5.2.1. Let $(F;X)$ be a commutative transformation semigroup containing the identity mapping. If $x_o \in X$, $F(x_o) = X$, $x' \in X$, then either

(a) $F|F(x')$ is a group or
(b) for some $y \in X$, $x' \notin F(y)$.

Proof

If (b) does not hold, then $x' \in F(x)$ for every $x \in X$. Clearly, $F(F(x)) \subset F(x)$ for every $x \in X$. Put $X'=F(x')$, $F' = F|X'$. Evidently, $X' = F'(x')$ and, for any $x \in X'$,

$$x' = F'(x') \subset F'(F'(x)) \subset F'(x),$$

hence $F'(x) = X'$.

Therefore the orbit of every $x \in X'$ under F' is X'. By 2.1.7. F' is a group.

5.2.2. Let $(G;X)$ be a commutative transformation group of continuous mappings of a given bounded connected subset Y of the real line into itself; let Y contain more than one point. Let $G(e) = Y$ for some $e \in Y$. Then Y is an open interval. If we put $Y = (a;b)$, then

$$\lim_{x \to a+} f(x) = a, \quad \lim_{x \to b-} f(x) = b \quad , \quad \text{for every } f \in G.$$

Proof

Every $f \in G$ is a one-to-one mapping from Y onto Y, and the values of two different mappings from G are distinct at every point. As the identity mapping belongs to G, every $f \in G$ in an increasing function. Let $\overline{Y} = [a,b]$. As every mapping $f \in G$ is onto, $\lim_{x \to a+} f(x) = a$ and $\lim_{x \to b-} f(x) = b$. From $a \in Y$, it would follow that $f(a) = a$, as f is continuous; and therefore that $G(a) = a$. As Y contains more than one point we would have $G(a) \neq Y$; hence $a \notin Y$. The same is valid for b.

5.2.3. Let X_o be a compact interval of the real line, c its centre. Let F be a commutative transformation semigroup of continuous mappings containing the identity mapping.

Suppose that, for some $x_o \in X_o$, $F(x_o)$ is connected, $\overline{F(x_o)} = X_o$ then either

(a) $F(c) = c$, or

(b) the endpoints of the interval $F(c)$ are common fixed points of F, or

(c) there exists $x_1 \in F(x_o)$ such that $F(x_1)$ is connected, and $d(F(x_1)) \leq \frac{1}{2}d(X_o)$,

where by d we denote the diameter of the set.

Proof

For any $x \in X_o$, the set $F(x)$ is connected since, for some $f \in F$, $F(x) = F(f(x_o)) = f(F(x_o))$. Consider the semigroup $F_o = F|F(x_o)$. By 5.2.1., either $F_o|F(c)$ is a group or there exists $x_1 \in F(x_o)$ such that $c \notin F(x_1)$. In the first case apply 5.2.2..(The case $F(c) = c$ is trivial.) In the second case

$$d(F(x_1)) \leq \tfrac{1}{2}d(F(x_o)) = \tfrac{1}{2}d(X_o) \text{ since } c \text{ non } \in F(x_1).$$

5.2.4. Theorem. Let $(F;X)$ be a commutative transformation semigroup of continuous mappings containing the identity mapping; let X be a compact interval. If $F(e)$ is connected for some $e \in X$, then all mappings in F have a common fixed point.

Proof

We put $X_o = F(e)$ and consider the semigroup $F|X_o$. Let c be the centre of F(e). By 5.2.3., either the endpoints of F(c) (or c itself) are fixed under F, or there exists $X_1 \in F(e)$ such that

$$d(F(x_1)) \leq \tfrac{1}{2}d(X_o),$$

and $X_1 = \overline{F(x_1)}$ satisfied the conditions required for X_o in 5.2.3.

Proceeding by induction, either we obtain, at some step, a fixed point for F, or a sequence of intervals $\{X_n\}$ is obtained with

(a) $X_n \supset X_{n+1}$,

(b) $d(X_{n+1}) \leq \tfrac{1}{2}d(X_n)$,

(c) $F(x_n) \subset X_n$.

In this last case, clearly, $\bigcap_{n=1}^{\infty} X_n$ is a one point set $\{z\}$, and z is a common fixed point of F.

6. The number of commutative transformations of a finite set into itself

Throughout this section X will be a finite set and F a commutative transformation semigroup containing the identity mapping. Evidently, F must be also finite. The aim of this chapter is to estimate the number of commuting mappings on X. If we assume that F is a group, then the number can be estimated very easily, using some previous results.

6.1.1. Theorem. Let F be a group. Then $|F| \leq \prod_{i=1}^{k} n_i$, where the n_i, $i=1,2,\ldots,k$, are natural numbers such that $\sum_{i=1}^{k} n_i = |X|$.

The proof follows immediately from the fact that the orbits are the cycles by 3.2.15. If we put $n_i = |C_i|$, then we know that $|F|C_i| = |F\|C_i| = |C_i|$, by 2.3.1. Forming $\mathbb{P} = \mathbb{P}(F|C_i; i=1,2,\ldots,k)$, we get $\prod_{i=1}^{k} n_i = |\mathbb{P}| \geq |F|$.

6.1.2. To make a similar estimate for a semigroup is not so simple, as, in general, the orbits are not the cycles. The estimate of $|F|$ is based, roughly, speaking, on the induction according to the number of maximal orbits. But first we must introduce a new notion and to prove a few lemmas.

We shall say that $F(y) = Y$ is a maximal orbit if $C(y) \in \Gamma_M$.

As X is assumed to be finite, the maximal orbits cover X. There exist no more than $|X|$ different maximal orbits.

6.1.3. Let Y_i, $i=1,2,\ldots,n$, and Z be orbits and let $Y = \bigcup_{i=1}^{n} Y_i$. Then

$$|Y \cap Z| \geq 2 \Longrightarrow |F|Y \cap Z| \geq 2.$$

Proof

The set $Y \cap Z$ is evidently invariant under F, and therefore F restricted to this set is a commutative transformation semigroup containing the identity mapping, by 1.3.4. Hence, $|F|Y \cap Z| \geq 1$. Let us suppose that $|F|Y \cap Z| = 1$. Then $F|Y \cap Z$ contains only the identity mapping, and all points in $Y \cap Z$ are the common fixed points under F, hence they are minimal cycles. The orbit Z cannot contain more than one minimal cycle, by 3.1.8. Hence, $|F|Y \cap Z| \geq 2$.

6.1.4. Let Y_i, Z_j, $i=1,2,\ldots,m$, $j=1,2,\ldots,n$, be orbits under F. Let $Y = \bigcup_{i=1}^{m} Y_i$, $Z = \bigcup_{j=1}^{n} Z_j$, $|F|Y \cap Z| = s$.

Then

$$|F|Y \cup Z| \leq |F|Y| \cdot |F|Z| \quad \text{for } s \leq 1,$$
$$|F|Y \cup Z| \leq (|F|Y|-1)(|F|Z|-1) + 1 \quad \text{for } s \geq 2.$$

Proof

Let $s \leq 1$. For every $f \in F|Y \cup Z$ there exist $f_1 \in F|Y$ and $f_2 \in F|Z$, such that $f|Y = f_1, f|Z = f_2$. Hence, every $f \in F|Y \cup Z$, is uniquely defined by a pair f_1, f_2. The number of such pairs is at most $|F|Y| \cdot |F|Z|$.

Let $s \geq 2$. We can devide all mappings from $F|Y$ in disjoint classes putting two mappings in the same class, if the restrictions to $Y \cap Z$ are equal. We get precisely s-classes. The same we can do for $F|Z$. If we denote the cardinals of classes of $F|Y$ by $m_1, m_2, \ldots, m_s$ and the cardinal of classes of $F|Z$ by $n_1, n_2, \ldots, n_s$, we get the following:

(a) $m_i \geq 1$, $i=1,1,\ldots,s$, $n_j \geq 1$, $j=1,2,\ldots,s$,

(b) $\sum_{i=1}^{s} m_i = |F|Y|$, $\sum_{i=1}^{s} n_i = |F|Z|$.

Every mapping from $F|Y \cup Z$ is uniquely determined by a pair of mappings, one from $F|Y$ and one from $F|Z$, such that both mappings must have the same restriction to $Y \cap Z$. Hence,

$$|F|Y \cup Z| \leq \sum_{i=1}^{s} m_i \cdot n_i .$$

It can be proved by elementary methods that the expression on the right hand side, has its maximum for $s=2$, $m_1 = |F|Y| - 1$, $m_2 = 1$, $n_1 = |F|Z| - 1$, $n_2 = 1$.

Hence, the proposition is proved.

6.1.5. Let Z, Y_i, $i=1,2,\ldots,n$, be orbits and let $Y = \bigcup_{i=1}^{n} Y_i$.

Then

$$|F|Y \cup Z| \leq |F|Y||F|Z| \quad \text{if } |Y \cap Z| \leq 1,$$
$$|F|Y \cup Z| \leq (|F|Y|-1)(|F|Z|-1) + 1 \text{ if } |Y \cap Z| \geq 2.$$

Proof

This is an immediately consequence of 6.1.3. and 6.1.4.

6.1.6. Let us denote by $a(t;r)$, t,r-natural numbers, $t \geqslant r$, the following function

$$a(t;r) = \max |F| ,$$

where the maximum is taken over all commutative semigroups of mappings $(F;X)$, containing the identity map, such that $|X| = t$ and such that there exists precisely r maximal orbits under F.

Evidently $a(t;r) \geqslant 1$, for every pair of natural numbers $t,r,t \geqslant r$. To see this, we can take r disjoint commutative algebraic groups $G_1, G_2, \ldots, G_r$, such that $\sum_{i-1}^{r} |G_i| = t$. Then $(F; \bigcup_{i=1}^{r} G_i) = \mathbb{P}(m(G_i);G_i)$ has the required properties.

Moreover, $a(t;1) = t$, as in this case $p(F) = 1$, for all F over which the maximum is taken, and $a(t;t) = 1$, as it can only be true for $F = \{i\}$ that the number of maximal orbits is equal to t.

6.1.7. Let $t \geqslant r \geqslant 2$. Then

$$\text{(a)} \quad a(t;r) \leqslant \max_{x;y;s} \left\{ \begin{array}{l} a(x+s;r-1)(y+s), \text{ where } x+s+y=t;\ 1 \geqslant s \geqslant 0; y \geqslant 1; x \geqslant r-1 \\ (a(x+s;r-1)-1)(y+s-1)+1, \text{ where } x+s+y=t; s \quad 2;\ y \geqslant 1; \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x \geqslant r-1 \end{array} \right\} .$$

All numbers, x,y,s are supposed to be integers.

Proof

Let $(F;X)$ have the following properties:

(a) $|X| = t$

(b) there exist precisely r different maximal orbits, $Y_1, Y_2, \ldots, Y_{r-1}, Z$.

Let us denote $\bigcup_{i=1}^{r-1} Y_i = Y$. If we denote $|Y \cap Z| = s$, $|Y| = x+s$, $|Z| = y+s$, we have

$$t = x + y + s.$$

Every Y_i is an orbit of a point, which does not belong to Y_j, $j \neq i$ or to Z. Therefore

$$x + s \geqslant r-1 + s, \text{ and hence } x \geqslant r-1.$$

According to definition we have

$$|F|Y| \leqslant a(x+s;r-1)$$
$$|F|Z| = a(y+s;1) = y+s.$$

The estimate of $a(t;r)$ follows immediately from 6.1.5.

6.1.8. For all natural numbers k,r, let us define the function $b(k+r;r)$ as follows:

$$b(k+1;1) = k+1$$
$$b(k+r;r) = \max_{y,s} \left\{ \begin{array}{ll} b(k+r-y;r-1)(1+y) , & \text{where } 1\leq y\leq k \\ b(k+r-y;r-1)-1)(y+s-1)+1) ; & \text{where } s \geq 2, \\ & 1\leq y \leq k-s+1 \end{array} \right\} ,$$

y,s being natural numbers.

6.1.9. $b(k+r;r)\geq a(k+r;r)$ for every pair of natural numbers k, r.

Proof

The assertion is true for $r=1$. Let us assume $r\geq 2$, and suppose that the assertion is true for $r-1$.

Let us consider the expression from 6.1.7.(a):

$$\max \left[a(x+s;r-1)(y+s)\right] , \text{ where } x+s+y=t,\ 1\geq s \geq 0,\ x \geq r-1.$$

Putting $t = r+k$, we can replace this expression by

$$\max \left[a(r+k-y;r-1)(y+s)\right] , \quad 1\geq s\geq 0,\ y\leq k-s+1 .$$

Using 6.1.6. we can easily verify that this expression is equal to

$$\max_{1\leq y \leq k} \left[a(r+k-y;r-1\right] (y+1)\right] .$$

According to the assumption we can write

$$\max_{1\leq y\leq k} \left[a(r+k-y;r-1)(y+1)\right] \leq \max_{1\leq y\leq k} \left[b(r+k-y;r-1)(y+1)\right] .$$

The rest of the proof is evident from the definitions.

6.1.10. Proposition.
$$b(r+1;r) = 2^r$$
$$b(r+2;r) = 2^{r-1}.3$$
$$b(r+k;r) = k^r+1,\ r\geq 3.$$

The equations can be obtained by elementary methods from definition 6.1.8.

6.1.11. Theorem. Let r,k be arbitrary natural numbers. Then there exists a commutative transformation semigroup $(F;X)$, $|X| = r+k$, which has precisely r different maximal orbits, such that

$$|F| = b(r+k;r).$$

<u>Proof</u>

(a) Let $k=1$, r arbitrary. Let $X = \{0;1;2;\ldots r\}$.

Let $(F_i;\{0;i\})$, $i=1,2,\ldots,r$, be the system of two mappings f_i^1, f_i^2, defined by the table

	0	i
f_i^1	0	i
f_i^2	0	0

Then $(\mathbb{P}(F_i;\ i=1,2,\ldots,r);X)$
has the required properties.

(b) Let $k=2$, $X = \{0;1;2;\ldots r-1;r;r+1\}$.

Let F_i; $i=1,2,\ldots,r-1$ have the same meaning as in (a).

Let $(H;\{0;r;r+1\})$ be defined as follows

	0	r	r+1
h_1	0	r	r+1
h_2	0	0	r
h_3	0	0	0

Then

$$(\mathbb{P}(F_i;H;i=1,2,\ldots,r-1);X)$$

has the required properties.

(c) Let $k \geq 3$ and $X = \{1,2,3,\ldots,k,a_1,a_2,\ldots,a_r\}$

Let $X_i = \{1;2;3;\ldots k;a_i\}$ $i=1,2,\ldots,r$, and let $F_i = \{f_i^1;f_i^2;\ldots f_i^n\}$ where

$$\left.\begin{aligned} f_i^j(l) &= 1, \quad l = 1,2,\ldots,k \\ f_i^j(a_i) &= j; \end{aligned}\right\} \quad \text{for } j=1,2,\ldots,k.$$

If $F = \mathbb{P}\{F_i, i=1,2,\ldots,r\} \cup \{i\}$, where by i we denote the identity map on X, then $|F| = k^r+1$.

6.1.12. Corollary. $a(k+r;r) = b(k+r;r)$ for every pair of natural numbers k,r.

6.1.13. Theorem. Let $(F;X)$ be a commutative system of mappings from a finite set X into itself. Then

$$|F| \leq 2^{|X|-1} \qquad \text{if } 1 \leq |X| \leq 6 \quad ,$$

$$|F| \leq \max_{r=1,2,\ldots,|X|} (|X|-r)^r + 1 \quad \text{if } |X| \geq 7.$$

For every finite X there exists an F such that the equality holds.

<u>Proof</u>

Evidently, $|F| \leq \max_{r=1,2,\ldots,|X|} b(|X|;r)$. Computing this expression we get the assertion of the theorem.

6.1.14. Theorem. Let $(F;X)$ be a commutative system of mappings from a finite set X into itself. Let $|X| \geq 4$. Then

$$|F| \leq (|X|-1)!$$

The proof follows immediately from 6.1.13. It is necessary to remark that this estimate is very rough.

Literature

A.H. Clifford and G.B. Preston, The algebraic theory of semigroups. Providence, Rhode Island 1961.

I.M. Gelfand, D.A. Rajkov, G.E. Shilov, Commutative normed rings. Moscow 1960.

E.S. Lyapin, Semigroups. Moscow 1960.

Contents

Foreword I

1. Definitions and notation 1

2. Orbits of commutative transformation semigroups 16

3. Cycles and structure of commutative transformation semigroups 26

4. Realization of relations 44

5. Fixed points of commutative mappings 52

6. The number of commutative transformations of a finite set into itself 60

7. Literature 66