Embedding theorems for infinite groups

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, 60, No. 5 and Indag. Math., 19, No. 5, 1957

MATHEMATICS

EMBEDDING THEOREMS FOR INFINITE GROUPS

BY

N. G. DE BRUIJN

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of May 25, 1957)

Notations. Bold face letters $\mathbf{m}, \mathbf{n}, \ldots$ denote cardinal numbers.

If M is a set, with cardinal number $\mathbf{m}$, and if G is a group, then G^M is the group of all functions defined on M, with values in G, with the obvious multiplication rule. The structure of G^M is determined by G and $\mathbf{m}$. In many statements it will be irrelevant which set M of the given power $\mathbf{m}$ is taken, and in such cases we write $G^{\mathbf{m}}$ instead of G^M.

$G^{\mathbf{m}}$ is called the unrestricted direct product of $\mathbf{m}$ groups G. The (restricted) direct product of $\mathbf{m}$ groups G is the subgroup of G^M, consisting of all functions f of M to G which are such that $f(\mu)$ equals the unit element of G for all but a finite number of elements of M.

The notion of free product of a set of groups G_α (α runs through some index set N) is also taken in this restricted sense: it consists of all finite words built out of elements of the groups G_α, so that in every word only a finite number of the G_α's play a rôle (it is understood that no word contains two consecutive symbols representing elements of one and the same G_α; for the product of two words we have the cancellation rule that adjacent symbols should be multiplied if they belong to the same G_α).

$\sum_M$ denotes the set of all permutations of M, i.e. the set of all one-to-one mappings of M onto itself.

If $\sigma \in \sum_M$, then the image of the element $\mu \in M$ under the mapping σ is written as $\sigma(\mu)$.

If M is infinite, and if $\mathbf{n}$ is an infinite cardinal number $\leqslant \mathbf{m}$, then $\sum_{M,\mathbf{n}}$ is the group of all $\mathbf{n}$-restricted permutations of M. A permutation $\sigma \in \sum_M$ is called $\mathbf{n}$-restricted if $\sigma(\mu) = \mu$ for almost all $\mu \in M$, where "almost all" means that the number of exceptions is less than $\mathbf{n}$. In cases where it does not matter which M we take (of given power $\mathbf{m}$) we shall write $\sum_{\mathbf{m},\mathbf{n}}$ and $\sum_{\mathbf{m}}$ instead of $\sum_{M,\mathbf{n}}$ and $\sum_M$.

1. *Introduction.* The following question was raised independently by Prof. J. DE GROOT and by Mr. T. J. DEKKER: Does the infinite symmetric group $\sum_{\mathbf{m}}$ (which has $2^{\mathbf{m}}$ elements) contain a free subgroup of order $2^{\mathbf{m}}$? The answer is affirmative; in fact it can be proved that $\sum_{\mathbf{m}}$ contains the free product of $2^{\mathbf{m}}$ given groups, provided that each one of them can be embedded into $\sum_{\mathbf{m}}$. For, the free product of $2^{\mathbf{m}}$ copies of $\sum_{\mathbf{m}}$ itself can be embedded into $\sum_{\mathbf{m}}$ (Theorem 4.2).

The corresponding statement holds for the direct product of $2^{\mathbf{m}}$ copies of $\Sigma_{\mathbf{m}}$. Both results are applications of the following general theorem:

Theorem 1.1. Let $\mathbf{m}$ be an infinite cardinal, and let H and S be arbitrary groups. If for every finite number k the free product of k copies of H can be embedded into S, then the free product of $2^{\mathbf{m}}$ groups H can be embedded into the unrestricted direct product $S^{\mathbf{m}}$.

If, for every finite k, the direct product H^k can be embedded into S, then the direct product of $2^{\mathbf{m}}$ groups H can be embedded into $S^{\mathbf{m}}$.

In order to be able to prove theorem 1.1 simultaneously for the case of free products and for the case of direct products, the notion of symmetrically generated groups is introduced (sec. 2). Both cases of theorem 1.1 will appear as special cases of theorem 3.1.

Prof. R. Baer raised the further question whether the factor groups $\Sigma_{\mathbf{m}}/\Sigma_{\mathbf{m},\mathbf{n}}$ contain free groups of order $2^{\mathbf{m}}$. The answer is affirmative, since $\Sigma_{\mathbf{m}}$ itself can be embedded into such factor groups (theorem 4.4).

B. Jónsson announced [3] a proof for the existence of universal relational systems. For the special case of groups his result states (under the assumption of the Generalized Continuum Hypothesis) the existence of a group G of power $\mathbf{m}$ ($\mathbf{m}$ infinite) such that every group of power $\mathbf{m}$ can be embedded into G.

Knowing that so many groups of order $2^{\mathbf{m}}$ can be embedded into $\Sigma_{\mathbf{m}}$, it is natural to ask whether $\Sigma_{\mathbf{m}}$ is universal in this respect. The answer is negative; in sec. 5 we shall show, if $\mathbf{k}>\mathbf{m}$, $\mathbf{a}=\aleph_0$, that the group $\Sigma_{\mathbf{k},\mathbf{a}}$ cannot be embedded into $\Sigma_{\mathbf{m}}$ (although the order $\mathbf{k}$ of $\Sigma_{\mathbf{k},\mathbf{a}}$ may be less than the order of $\Sigma_{\mathbf{m}}$ if the generalized continuum hypothesis is false).

The author does not know whether the factor group $\Sigma_{\mathbf{m}}/\Sigma_{\mathbf{m},\mathbf{n}}$ ($\mathbf{n}\leqslant\mathbf{m}$) can be embedded into $\Sigma_{\mathbf{m}}$.

For abelian groups there is a positive result: every abelian group of order $\leqslant 2^{\mathbf{m}}$ can be embedded into $\Sigma_{\mathbf{m}}$ (Theorem 4.3; the special case that the group of all real numbers can be embedded into the group of all permutations of a countable set is contained in a paper by A. Karrass and D. Solitar [4]).

For the proof of this theorem and for many other useful remarks made in discussions during the preparation of this paper, the author is indebted to Prof. J. de Groot.

The principal tool of this paper is the following theorem (see [2]):

Theorem 1.2. Let M be an infinite set of cardinality $\mathbf{m}$. Let for each $\mu\in M$ a non-empty set A_μ be given, and assume that, for each finite number n, there are still $\mathbf{m}$ elements $\mu\in M$ such that A_μ has more than n elements. Then there exists a collection F of $2^{\mathbf{m}}$ choice functions f with the following properties:

(i) Each $f\in F$ is defined as a function on M, with $f(\mu)\in A_\mu$ for each $\mu\in M$.

(ii) For each finite subset $\{f_1, \ldots, f_k\}$ of F ($f_1, \ldots, f_k$ distinct) there exists a $\mu_0 \in M$ such that $f_1(\mu_0), \ldots, f_k(\mu_0)$ are mutually different.

2. *Symmetrically generated groups.* Let Ω and H be groups, and let $\mathbf{n}$ be a finite or infinite cardinal number. Assume that Ω contains $\mathbf{n}$ copies of H. That is, there is a set N of power $\mathbf{n}$, and for each $\alpha \in N$ there is an isomorphic mapping χ_α of H onto a subgroup $H_\alpha = \chi_\alpha(H)$ of Ω. Possibly H_α is one and the same group for all $\alpha \in N$, but in that case our results will be trivial.

We shall impose a certain condition of symmetry. We consider arbitrary finite subsets Γ of N, and if Γ has been chosen, we consider arbitrary mappings φ of Γ into N:

$$\varphi\colon\ \Gamma \to \varphi(\Gamma) \subset N.$$

If Γ consists of the elements $\gamma_1, \ldots, \gamma_n$, then the group $G(H_{\gamma_1}, \ldots, H_{\gamma_n})$, i.e. the subgroup of Ω, generated by $H_{\gamma_1}, \ldots, H_{\gamma_n}$, will be denoted by G_Γ. Similarly, $G_{\varphi(\Gamma)}$ is the group generated by $H_{\varphi(\gamma_1)}, \ldots, H_{\varphi(\gamma_n)}$. (Notice that $\varphi(\gamma_1), \ldots, \varphi(\gamma_n)$ need not be distinct.)

S y m m e t r y c o n d i t i o n. For every finite $\Gamma \subset N$ and for every mapping φ of Γ into N there is a homomorphism

$$\psi_{\Gamma,\varphi}\colon\ G_\Gamma \to \psi_{\Gamma,\varphi} G_\Gamma \subset \Omega, \tag{2.1}$$

with the property that, for each $\gamma \in \Gamma$, its restriction to H_γ is the trivial mapping of H_γ onto $H_{\varphi(\gamma)}$:

$$\psi_{\Gamma,\varphi}\, \chi_\gamma(h) = \chi_{\varphi(\gamma)}(h) \quad (h \in H). \tag{2.2}$$

A consequence of (2.1) and (2.2) is that

$$\psi_{\Gamma,\varphi}\, G_\Gamma = G_{\varphi(\Gamma)}, \tag{2.3}$$

since both sides are generated by the elements specified in (2.2) ($h \in H$, $\gamma \in \Gamma$).

A further consequence is that if two H_α's coincide, then all H_α's coincide, and if two χ_α's are equal, then all χ_α's are equal. We do not discuss this in detail, as it will not be used and only leads to trivialities.

A third consequence is as follows: Let Γ and Δ be finite subsets of N, with $\Gamma \subset \Delta$. Therefore $G_\Gamma \subset G_\Delta$. Let φ map Δ into N; for simplicity the restriction of φ to Γ is also denoted by φ. Then $\psi_{\Gamma,\varphi}$ is the restriction of $\psi_{\Delta,\varphi}$ to G_Γ:

$$\psi_{\Gamma,\varphi}(g) = \psi_{\Delta,\varphi}(g) \quad (g \in G_\Gamma). \tag{2.4}$$

A fourth consequence is that $\psi_{\Gamma,\varphi}$ is an isomorphism if $\varphi(\Gamma)$ has as many elements as Γ (in other words, if φ is one-to-one). For in that case the rôles of Γ and $\varphi(\Gamma)$ can be interchanged. The homomorphism $\psi_{\varphi(\Gamma),\varphi^{-1}}\, \psi_{\Gamma,\varphi}$ of G_Γ into itself is an isomorphism, because of the invariance of the H_γ's.

It will be convenient to assume that the natural numbers are contained in the set N (if $\mathbf{n}$ is finite, we require instead that N consists of all natural numbers $\leqslant \mathbf{n}$). If we now put $G(H_1, \ldots, H_k) = G_k$ ($k = 1, 2, 3, \ldots$), and if Γ has k elements, we obviously have

$$G_\Gamma \cong G_k. \tag{2.5}$$

Definition. If the symmetry condition holds and if the group Ω is generated by the H_α's ($\alpha \in N$), then we say that Ω is symmetrically generated by $\mathbf{n}$ groups H.

The simplest non-trivial examples are (i) Ω is the free group generated by $\mathbf{n}$ copies of H, and (ii) Ω is the restricted direct product of $\mathbf{n}$ copies of H. In both cases, the symmetry condition is easily verified. From these examples it follows that the fact that Ω is symmetrically generated by $\mathbf{n}$ groups H, by no means determines the structure of Ω uniquely.

In the symmetry condition, the fact that the values $\varphi(\gamma_1), \ldots, \varphi(\gamma_n)$ are not forced to be distinct, is not as innocent as it might appear at first sight. We consider an example.

Let H be the cyclic group of order 2, and let $\sum_t$ ($t \geqslant 5$) be the symmetric group of order $t!$, consisting of all permutations of the set $\{0, 1, \ldots, t-1\}$. H_j ($j = 1, \ldots, t-1$) consists of the unit permutation and of the permutation $(0j)$ (i.e. the one that interchanges the objects 0 and j). Then $\sum_t$ is generated by $H_1, \ldots, H_{t-1}$. Now take $n = 4$, $\gamma_1 = 1$, $\gamma_2 = 2$, $\gamma_3 = 3$, $\gamma_4 = 4$. If the $\varphi(\gamma)$'s are mutually different, there is obviously a homomorphic mapping of the type indicated in the symmetry condition. If we take, however, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 3$, then there is no such homomorphism. For, we have $((01)\cdot(02)\cdot(03)\cdot(04))^5 = (04321)^5 = e$, whereas $((01)\cdot(01)\cdot(02)\cdot(03))^5 = (032)^5 \neq e$. It follows that $\sum_t$ is not symmetrically generated by $H_1, \ldots, H_{t-1}$.

3. *Embedding theorem for symmetrically generated groups*

Theorem 3.1. If $\mathbf{m}$ is an infinite cardinal, and $\mathbf{n} = 2^{\mathbf{m}}$, if Ω is symmetrically generated by $\mathbf{n}$ groups H, and if, for each positive integer k the group G_k (see (2.5)) can be embedded into a fixed group S, then Ω can be embedded into $S^{\mathbf{m}}$.

Proof. We first split the set M into a countable number of disjoint subsets $M = M_1 \cup M_2 \cup M_3 \cup \ldots$, each M_j still having power $\mathbf{m}$. For each $\mu \in M$ the number $p(\mu)$ will represent the uniquely defined index such that $\mu \in M_{p(\mu)}$.

For each $\mu \in M$ the finite set $\{1, 2, \ldots, p(\mu)\}$ will be denoted by A_μ.

According to theorem 1.2 we can find a collection F_0 of $2^{\mathbf{m}}$ choice functions with the properties stated in that theorem. Using some one-to-one mapping of F_0 onto N (notice that $2^{\mathbf{m}} = \mathbf{n}$), we can denote the elements of F_0 by f_α ($\alpha \in N$), and their values by $f_\alpha(\mu)$. This $f_\alpha(\mu)$ is a function of the variables α and μ. We shall write $\alpha(\mu)$ instead of $f_\alpha(\mu)$ if it is considered as a function of μ (α fixed), and we use the notation $\mu(\alpha)$ if μ is fixed and α variable. By theorem 1.2 we have the following properties:

(i) If $\alpha \in N$, $\mu \in M$ then $\alpha(\mu) \in A_\mu$, and so $1 \leqslant \alpha(\mu) \leqslant p(\mu)$.

(ii) If $\alpha_1, \ldots, \alpha_k$ represent any finite number of distinct elements of N, then there is a $\mu_0 \in M$ such that $\alpha_1(\mu_0), \ldots, \alpha_k(\mu_0)$ are distinct.

The given embedding of $G_k = G(H_1, \ldots, H_k)$ into S will be denoted by η_k:

$$\eta_k: \quad G_k \to \eta_k G_k \subset S \qquad (k = 1, 2, 3, \ldots).$$

Let Γ be any finite subset of N. We shall construct an embedding τ_Γ of G_Γ into S^{m}:

$$\tau_\Gamma: \quad G_\Gamma \to \tau_\Gamma G_\Gamma \subset S^{\mathrm{m}}.$$

Each $\gamma \in \Gamma$ corresponds to a function f_γ on M, and

$$1 \leqslant f_\gamma(\mu) = \gamma(\mu) = \mu(\gamma) \leqslant p(\mu).$$

We shall now consider $\mu(\gamma)$ (with μ fixed) as a function defined on Γ. It maps Γ into A_μ. Assuming that N contains all natural numbers (although N need not be countable), we have $A_\mu \subset N$. So μ can play the rôle of φ in (2.1). $\psi_{\Gamma,\mu}$ maps G_Γ onto $\psi_{\Gamma,\mu} G_\Gamma$, and by (2.3) this group is $G_{\mu(\Gamma)}$ ($\mu(\Gamma)$ denotes the image of Γ under the mapping μ). It follows that $\psi_{\Gamma,\mu} G_\Gamma \subset G_{p(\mu)}$.

This image can be mapped into S by $\eta_{p(\mu)}$. We define $\tau_{\Gamma,\mu}$ by

$$g \to \tau_{\Gamma,\mu} g = \eta_{p(\mu)} \psi_{\Gamma,\mu} g \in S \quad (g \in G_\Gamma), \tag{3.1}$$

and $\tau_{\Gamma,\mu}$ is a homomorphic mapping of G_Γ into S.

If Γ is given, we can find $\mu_0 \in M$ such that τ_{Γ,μ_0} is an isomorphism of G_Γ onto a subgroup of S. For, by (ii) μ_0 can be found such that $\mu_0(\Gamma)$ has the same number of elements as Γ itself. It follows that ψ_{Γ,μ_0} is one-to-one. Since $\eta_{p(\mu_0)}$ is also one-to-one, we infer that τ_{Γ,μ_0} is one-to-one.

Our following step maps G_Γ into S^{m}. Every element of S^{m} is a function, defined on M, with values in S. Let g be an element of G_Γ. We define $\tau_\Gamma g$ as the function on M, whose value at $\mu \in M$ equals $\tau_{\Gamma,\mu} g$. In formulas:

$$\tau_\Gamma: \quad g \to \tau_\Gamma g \in S^{\mathrm{m}} \quad (g \in G_\Gamma);$$

$$(\tau_\Gamma g)\,(\mu) = \tau_{\Gamma,\mu} g \in S \quad (g \in G_\Gamma, \mu \in M).$$

Obviously, the mappping τ_Γ of G_Γ into S^{m} is a homomorphism. It is even an embedding, since τ_{Γ,μ_0} is one-to-one.

Next consider two finite subsets Γ and Δ of N, where $\Gamma \subset \Delta$. We have $G_\Gamma \subset G_\Delta$, and we can show that τ_Γ is the restriction of τ_Δ to G_Γ. This follows from the fact that, for all $\mu \in M$

$$\tau_{\Gamma,\mu} g = \tau_{\Delta,\mu} g \quad (g \in G_\Gamma),$$

which is a direct consequence of (2.4) and (3.1).

As Ω is generated by the H_α's ($\alpha \in N$), Ω is the union of all G_Γ's, where Γ runs through all finite subsets of N. So if $g \in \Omega$ is given, we can find

Γ's with $g \in G_\Gamma$. For all such Γ's we get the same value of $\tau_\Gamma g$, for if Δ is the union of Γ_1 and Γ_2, we have $\tau_{\Gamma_1} g = \tau_\Delta g = \tau_{\Gamma_2} g$. This common value of these $\tau_\Gamma g$'s can be denoted by τg. As each τ_Γ is an isomorphism, τ is also an isomorphism, and our proof is complete.

4. *Application to symmetric groups*

Theorem 4.1. If $\mathbf{m}$ is an infinite cardinal, then the direct product Ω of $2^{\mathbf{m}}$ groups $\Sigma_{\mathbf{m}}$ can be embedded into $\Sigma_{\mathbf{m}}$ itself.

Proof. Ω is symmetrically generated by $2^{\mathbf{m}}$ groups $\Sigma_{\mathbf{m}}$. The subgroups G_k (see sec. 2) are direct products of k groups $\Sigma_{\mathbf{m}}$, whence they can be embedded into $\Sigma_{\mathbf{m}}$. Now theorem 3.1 shows that Ω can be embedded into $(\Sigma_{\mathbf{m}})^{\mathbf{m}}$. The latter group can be considered as an intransitive permutation group on $\mathbf{m}$ objects, having $\mathbf{m}$ transitivity sets of $\mathbf{m}$ elements each. So $(\Sigma_{\mathbf{m}})^{\mathbf{m}} \subset \Sigma_{\mathbf{m}^2} = \Sigma_{\mathbf{m}}$.

Theorem 4.2. If $\mathbf{m}$ is an infinite cardinal, then the free product of $2^{\mathbf{m}}$ groups $\Sigma_{\mathbf{m}}$ can be embedded into $\Sigma_{\mathbf{m}}$.

Proof. It is sufficient to show (cf. the proof of the preceding theorem) that the free product of k groups $\Sigma_{\mathbf{m}}$ can be embedded into $\Sigma_{\mathbf{m}}$. Moreover, it is sufficient to show this for $k = 2$, for then the case of general finite k can be dealt with by induction.

Let M be a set of power $\mathbf{m}$. We consider the cartesian product $M \times M$, consisting of all pairs (i, j) $(i \in M, j \in M)$. Let T be the $\aleph_0$-restricted permutation group of $M \times M$, i.e. the group of all those permutations of $M \times M$ which leave all but at most a finite number of elements of $M \times M$ invariant. Therefore, the number of elements of T equals $\mathbf{m}$. Furthermore we consider the (unrestricted) permutation groups Σ_M, $\Sigma_{M\times M}$ and $\Sigma_{M\times M\times T}$.

We first embed Σ_M into $\Sigma_{M\times M}$ by a mapping ϱ. If $s \in \Sigma_M$, then $\varrho(s) = s'$ is defined as the permutation of $M \times M$ that turns the pair (i, j) into the pair $(s(i), j)$ $(i, j \in M)$. The advantage of this operation is that we now have a permutation group $\varrho(\Sigma_M)$ $(\varrho(\Sigma_M) \subset \Sigma_{M\times M})$, every element of which (apart from the unit element) alters infinitely many objects of $M \times M$.

We next construct two embeddings φ and ψ of $\Sigma_{M\times M}$ into $\Sigma_{M\times M\times T}$. If $s \in \Sigma_{M\times M}$, $a \in M \times M$, $t \in T$ then the effect of $\varphi(s)$ and $\psi(s)$ on the pair (a, t) is defined by

$$\varphi(s)(a, t) = (s(a), t),$$
$$\psi(s)(a, t) = (t^{-1}st(a), t).$$

It is obvious that $\varphi\varrho$ and $\psi\varrho$ give embeddings of Σ_M into $\Sigma_{M\times M\times T}$. We shall show that $\varphi\varrho(\Sigma_M)$ and $\psi\varrho(\Sigma_M)$ are free generators of a subgroup of $\Sigma_{M\times M\times T}$. To this end we have to show the following: If $s_1, \ldots, s_{2n}$ are elements of $\varrho(\Sigma_M)$, all different from the unit element, then we cannot have

$$\psi(s_{2n})\varphi(s_{2n-1}) \ldots \varphi(s_3)\psi(s_2)\varphi(s_1) = e.$$

This would imply, according to the definitions of φ and ψ, that the product relation

$$t^{-1}s_{2n}ts_{2n-1}\ldots s_3t^{-1}s_2ts_1=e \tag{4.1}$$

(notice that all factors belong to $\sum_{M\times M}$) would hold for all $t\in T$. But it is easy to find a counterexample. Choose $a_1\in M\times M$ such that $s_1(a_1)\neq a_1$. Choose $a_2\in M\times M$ such that a_1, $s_1(a_1)$, a_2, $s_2(a_2)$ are mutually different. This process can be continued (each s altering infinitely many objects of $M\times M$). So we finally get $a_1,\ldots,a_{2n}$ such that $a_1,s_1(a_1),a_2,s_2(a_2),\ldots,a_{2n},s_{2n}(a_{2n})$ are mutually different. We can easily find $t\in T$ such that $t(s_1(a_1))=a_2$, $t^{-1}(s_2(a_2))=a_3$, $t(s_3(a_3))=a_4$, $\ldots$, $t(s_{2n-1}(a_{2n-1}))=a_{2n}$, $t^{-1}(s_{2n}(a_{2n}))\neq a_1$.

So the left hand side of (4.1) does not transform the object a_1 into itself, whence it cannot be the unit permutation.

We infer that $\sum_{M\times M\times T}$ contains a subgroup which is the free product of $\varphi\varrho(\sum_M)$ and $\psi\varrho(\sum_M)$. Finally, $M\times M\times T$ has power $\mathbf{m}^3=\mathbf{m}$, whence $\sum_{M\times M\times T}$ and $\sum_M$ are isomorphic. This proves the theorem.

Corollary. If we have $2^{\mathbf{m}}$ groups ($\mathbf{m}$ infinite), each one of which can be embedded into $\sum_{\mathbf{m}}$, then their direct product and their free product can be embedded into $\sum_{\mathbf{m}}$.

In view of applications of this corollary we remark that every group of order $\mathbf{m}$ can be embedded into $\sum_{\mathbf{m}}$, simply by its Cayley representation. This remark can be used for the proof of

Theorem 4.3. If $\mathbf{m}$ is an infinite cardinal number, then every abelian group of order $2^{\mathbf{m}}$ can be embedded into $\sum_{\mathbf{m}}$.

Proof. It seems that the axiom of choice is needed for the proof. The possibility of embedding arbitrary abelian groups follows from the following arguments, for which I am indebted to Prof. J. de Groot:

(i) Every abelian group can be embedded into a complete group.

(ii) Every complete group is a direct product of quasicyclic and rational groups, i.e. of countable groups.

The proofs can be found in Kurosh [5]; the proof of (ii) is based upon the axiom of choice.

So every abelian group of order $2^{\mathbf{m}}$ can be embedded into the direct product of $2^{\mathbf{m}}$ countable groups. Every countable group can be embedded into $\sum_{\mathbf{m}}$, whence application of theorem 4.1 proves theorem 4.3.

The normal subgroups of $\sum_{\mathbf{m}}$ ($\mathbf{m}$ is any infinite cardinal) are precisely known (see [1]). They are all of the form $\sum_{\mathbf{m},\mathbf{n}}$, where $\mathbf{n}$ is any infinite cardinal $\leqslant\mathbf{m}$. It is easily seen that the factor group $\sum_{\mathbf{m}}/\sum_{\mathbf{m},\mathbf{n}}$ still has the order $2^{\mathbf{m}}$.

Everything that can be embedded into $\sum_{\mathbf{m}}$ can also be embedded into $\sum_{\mathbf{m}}/\sum_{\mathbf{m},\mathbf{n}}$, by virtue of the following theorem:

Theorem 4.4. If $\mathbf{m}$ and $\mathbf{n}$ are infinite cardinals, $\mathbf{n}\leqslant\mathbf{m}$, then $\sum_{\mathbf{m}}$ can be embedded into $\sum_{\mathbf{m}}/\sum_{\mathbf{m},\mathbf{n}}$.

Proof. Let $\sum_M$ and $\sum_{M\times M}$ denote the groups of all permutations of M and of $M \times M$, respectively. Both groups are isomorphic to $\sum_{\mathbf{m}}$.

Let $T = \sum_{M\times M,\mathbf{n}}$ denote the **n**-restricted subgroup of $\sum_{M\times M}$, consisting of all permutations which leave almost all elements of $M \times M$ invariant (we use the phrase "almost all" for "with less than **n** exceptions"). As in the proof of theorem 4.2, we first construct an embedding ϱ of $\sum_M$ into $\sum_{M\times M}$, by

$$s \to \varrho(s) = s^*, \quad s^*(i, j) = (s(i), j) \quad (i, j \in M, \ s \in \textstyle\sum_M).$$

We put $\varrho(\sum_M) = \sum^*$, so that $\sum_M \cong \sum^* \subset \sum_{M\times M}$. We next consider the product $\sum^* T$, which is a subgroup of $\sum_{M\times M}$ (since T is a normal subgroup of $\sum_{M\times M}$). It is easily seen that $\sum^* \cap T = e$. So every element of $\sum^* T$ can be uniquely represented as a product $\varrho(s)t$ ($s \in \sum$, $t \in T$). We now map $\sum^* T$ onto $\sum_M$, by the mapping

$$\psi: \quad \varrho(s)t \to \psi(\varrho(s)t) = s \qquad (s \in \textstyle\sum_M, \ t \in T).$$

It can be shown that ψ is a homomorphism. To this end it suffices to show that

$$\varrho(s_1)t_1\varrho(s_2)t_2 = \varrho(s_3)t_3, \ s_i \in S, \ t_i \in T, \tag{4.2}$$

imply that $s_1 s_2 = s_3$. As $t_1, t_2, t_3 \in T$, we have, for almost all $j \in M$, that $t_1(i, j) = t_2(i, j) = t_3(i, j) = (i, j)$ for all $i \in M$. The $\varrho(s)$'s transform the i's only, and therefore (4.2) implies that for almost all j we have

$$\varrho(s_1)\, \varrho(s_2)\, (i, j) = \varrho(s_3)\, (i, j)$$

identically in i. We infer that $s_1 s_2(i) = s_3(i)$ for all i, whence $s_1 s_2 = s_3$, and $\varrho(s_1)\, \varrho(s_2) = \varrho(s_3)$. This shows that ψ is a homomorphism. Its kernel is T, so we have $\sum_M \cong (\sum^* T)/T$.

Finally, we have $(\sum^* T)/T \subset \sum_{M\times M}/T = \sum_{M\times M}/\sum_{M\times M,\mathbf{n}} \cong \sum_{\mathbf{m}}/\sum_{\mathbf{m},\mathbf{n}}$, and the proof is complete.

5. *Groups that cannot be embedded into* $\sum_{\mathbf{m}}$

Theorem 5.1. Let **k** and **m** be infinite cardinals, $\mathbf{k} > \mathbf{m}$, and let **a** be the cardinal number of a countable set. Then $\sum_{\mathbf{k},\mathbf{a}}$ cannot be embedded nto $\sum_{\mathbf{m}}$ (which is trivial if $\mathbf{k} > 2^{\mathbf{m}}$, the order of $\sum_{\mathbf{k},\mathbf{a}}$ being **k**).

Proof. Let M be a set of power **m**, and K a set of power **k**. Let ω be a fixed element of K, and put $K^* = K \setminus \omega$.

The group $\sum_{K,\mathbf{a}}$ contains the elements g_α ($\alpha \in K^*$), where $g_\alpha = (\omega\alpha)$ (i.e. the permutation of K that interchanges ω and α, but that leaves all other elements of K untouched). If $\alpha, \beta, \gamma, \delta$ are distinct elements of K^*, then $g_\alpha g_\beta = (\omega\alpha\beta)$, $g_\alpha g_\beta g_\gamma g_\delta = (\omega\delta\gamma\beta\alpha)$. So we infer that g_α has the exact order 2, $g_\alpha g_\beta$ has the exact order 3, and $g_\alpha g_\beta g_\gamma g_\delta$ has the exact order 5.

We shall prove the theorem by showing that $\sum_M$ does not contain **k** elements h_α ($\alpha \in K^*$) such that all h_α's have order 2, all products

$h_\alpha h_\beta$ $(\alpha \neq \beta)$ have order 3, and all products $h_\alpha h_\beta h_\gamma h_\delta$ $(\alpha, \beta, \gamma, \delta$ distinct) have order 5. Henceforth assuming the existence of such elements, a contradiction will be obtained.

From now on we drop the asterisk, writing K instead of K^*.

Lemma. Let $\alpha, \beta, \gamma, \delta$ be distinct elements of K. Assume that R is a subset of M, which is mapped onto itself by each of the permutations h_α, h_β, h_γ and h_δ. Let $h_{\alpha R}$ denote the restriction of h_α to R, and let $h_{\beta R}$, $h_{\gamma R}$, $h_{\delta R}$ be similarly defined. Now assuming that $h_{\alpha R} = h_{\beta R} = h_{\gamma R}$, we also have $h_{\alpha R} = h_{\delta R}$.

Proof. The order of a restriction of a permutation to an invariant subset divides the order of the permutation itself. So $h_{\alpha R} h_{\delta R}$ has order 1 or 3, $h_{\alpha R} h_{\beta R} h_{\gamma R} h_{\delta R}$ has order 1 or 5. As $h_{\beta R}$ has order 1 or 2, and as $h_{\beta R} = h_{\gamma R}$, we have $h_{\beta R} h_{\gamma R} = e$. So the order of $h_{\alpha R} h_{\delta R}$ divides both 3 and 5, whence this order equals 1. So $h_{\alpha R} = h_{\delta R}^{-1} = h_{\delta R}^{-1} h_{\delta R}^2 = h_{\delta R}$. This proves the lemma.

Returning to the proof of the theorem, we argue as follows. The number of α's in K exceeds the number of objects permuted by the h_α's, and therefore at least one of the following four possibilities occurs:

(i) For each $a \in M$, the element $h_\alpha(a)$ is independent of α.

(ii) There is an $a \in M$ such that $h_\alpha(a) = a$ for $\mathbf{k}$ elements $\alpha \in K$, and such that there is a $\delta \in K$ with $h_\delta(a) \neq a$.

(iii) There are elements $a, b \in M$, $a \neq b$, such that $h_\alpha(a) = b$ for $\mathbf{k}$ α's, and $h_\delta(a) = a$ for at least one $\delta \in K$.

(iv) There are distinct elements $a, b, c \in M$, such that $h_\alpha(a) = b$ for $\mathbf{k}$ α's, and $h_\delta(a) = c$ for at least one $\delta \in K$.

We shall deduce a contradiction in each case. Once for all we remark that all h's have order 2, whence $h_\alpha(p) = q$ always implies $h_\alpha(q) = p$.

Case (i) is ruled out immediately, for then all h's would be equal. And then every product $h_\alpha h_\beta$ $(\alpha \neq \beta)$ would be $= h_\alpha^2 = e$, whence it would not have order 3.

Case (ii). We have $h_\alpha(a) = a$ for $\mathbf{k}$ α's, and $h_\delta(a) = b$, $h_\delta(b) = a$, with $b \neq a$. Among the $\mathbf{k}$ α's with $h_\alpha(a) = a$ there are at least $\mathbf{k}$ whose effect on b is equal (since $\mathbf{k} > \mathbf{m}$). So we have simultaneously $h_\alpha(a) = a$, $h_\alpha(b) = c$, $h_\alpha(c) = b$ for $\mathbf{k}$ α's. We have $c \neq a$, since $h_\alpha(a) \neq h_\alpha(c)$. We show that $c \neq b$. Assuming $c = b$, we take for R the set $\{a, b\}$. For $\mathbf{k}$ α's R is permuted as (a) (b), and for one δ as (ab). Since $\mathbf{k} > 3$, our lemma gives a contradiction.

So a, b, c are distinct. Again by the lemma, applied to $R = \{a, b, c\}$, we have $h_\delta(c) \neq c$ (otherwise R would be permuted as (a) (bc) by 3 α's, and as (ab) (c) by δ).

We get our final contradiction by showing that there cannot be an α and a δ with $h_\alpha(a) = a$, $h_\alpha(b) = c$, $h_\delta(a) = b$, $h_\delta(c) \neq c$. We would have $(h_\delta h_\alpha)^3(c) = (h_\delta h_\alpha)^2(a) = h_\delta h_\alpha(b) = h_\delta(c) \neq c$, in contradiction with the fact that $h_\delta h_\alpha$ has order 3.

Case (iii). Applying the lemma to $R = \{a, b\}$, we infer that $h_\delta(b) \neq b$ (otherwise R would be permuted as (ab) three times, and once as $(a)(b)$). So $h_\delta(b) = c$, where a, b, c are distinct. The remainder of the proof is parallel to case (ii) with α and δ interchanged. We show that $h_\alpha(a) = b$, $h_\alpha(c) = c$ cannot hold for three α's (otherwise $\{a, b, c\}$ would be permuted as $(ab)(c)$ three times, and once as $(a)(bc)$). So there are an α and a δ with $h_\delta(a) = a$, $h_\delta(b) = c$, $h_\alpha(a) = b$, $h_\alpha(c) \neq c$, and we get a contradiction from the fact that $h_\alpha h_\delta$ has order 3.

Case (iv). We have $h_\alpha(a) = b$, $h_\alpha(b) = a$ for $\mathbf{k}$ α's, and $h_\delta(a) = c$. We may assume that $h_\delta(b) \neq b$, for otherwise we have again case (iii) (interchanging a and b). Obviously, $h_\delta(b)$ cannot be a or c, as a and c are transformed into each other by h_δ. So $h_\delta(b) = d$, where a, b, c, d are distinct.

The set $\{a, b, c, d\}$ is permuted by h_δ as $(ac)(bd)$, so by the lemma there cannot be three α's with $h_\alpha(a) = b$, $h_\alpha(c) = d$, nor can there be three α's with $h_\alpha(c) = c$, $h_\alpha(d) = d$. As c and d play the same rôle, we may assume that there are $\mathbf{k}$ α's with $h_\alpha(a) = b$, $h_\alpha(c) \neq c$, $h_\alpha(c) \neq d$.

The number of possible values of $h_\alpha(c)$ is at most $\mathbf{m}$. As $\mathbf{m} < \mathbf{k}$, there is an element $p \in M$ $(p \neq c, p \neq d)$ such that $h_\alpha(a) = b$, $h_\alpha(c) = p$ for $\mathbf{k}$ values of α. So there is a set of $\mathbf{k}$ α's which permute a, b, c, p as $(ab)(cp)$. For any such α we have $d = (h_\alpha h_\delta)^3(d) = (h_\alpha h_\delta)^2(a) = h_\alpha h_\delta(p)$, whence $h_\alpha(d) = h_\delta(p)$. This element $h_\delta(p)$ cannot be a, c, b or d (h_δ already permutes $(ac)(bd)$), and it cannot be p, since $p = h_\alpha(c) \neq h_\alpha(d) = h_\delta(p)$. So $h_\alpha(d) = h_\delta(p) = q$, and a, b, c, d, p, q are distinct. These six elements are permuted by $\mathbf{k}$ α's as $(ab)(cp)(dq)$, and by δ as $(ac)(bd)(pq)$. Again applying the lemma, we get our final contradiction, and the proof of the theorem is complete.

University of Amsterdam.

REFERENCES

1. Baer, R., Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich. Studia Math. **5**, 15–17 (1934).
2. Bruijn, N. G. de, A theorem on choice functions. These Proc. vol. LX (series A), 409 (1957).
3. Jónsson, B., Universal relational systems (abstract). Bull. Amer. Math. Soc. **62**, 403 (1956).
4. Karrass, A. and D. Solitar, Some remarks on infinite symmetric groups. Math. Zeitschr. **66**, 64–69 (1956).
5. Kurosh, A. G. The theory of groups I, 165–166. New York (1956).