On the axiom of choice for families of finite sets

by

K. Wiśniewski (Warszawa)

The investigation of the axiom of choice for families of finite sets was initiated by Mostowski [4]. Further mathematical investigations of this topic are due to Szmielew [6] and Sierpiński [5], and metamathematical ones—to Zuckerman [8] and Gaunt [1]. In the present paper we prove that some forms of the axiom of choice for families of finite sets are independent of others forms. This paper is a continuation of [7]. The writer thanks Professor Mostowski for his kind help in the preparation of this paper and Professor Rydl-Naruszewski for his valuable suggestions and criticism.

In this paper we consider the set theory $ZF'$, which differs from $ZF$ by containing the constant $\emptyset$ for the empty set, and the axiom stating the existence of an infinite set of individuals. The axiom of extensionality in $ZF'$ is restricted only to sets (1).

We consider the following propositions:

[a]: For every family of $n$-element sets there exists a choice function;

[b]: For every linearly ordered family of $n$-element sets there exists a choice function;

[c]: For every denumerable family of $n$-element sets there exists a choice function.

Let $G$ be a group and $\mathcal{H}$ a family of proper subgroups of $G$. Consider the set $S_i = \{H \in \mathcal{H} : H \cap G \leq H \cap G \}$. The group $\Gamma_i$ of permutations $\pi_0$ of the set $S_i$ which are defined by the formula

$$\pi_0 = \left( (eH, i) \mapsto \left( (yH, i) \right) \right)_{H \in \mathcal{H}}$$

(1) The restriction to $ZF'$ set theory is inessential. We may use the Fraenkel-Mostowski method for the other set theories, e.g. the set theory of the Gödel-Bernays type with classes and individuals or set theories in which unfounded sets are allowed (cf. [2]). The results of the present paper are valid for the "ordinary" set theory i.e. the set theory with no individuals and with the axiom of regularity. This can be shown by the Cohen method modified by Marek [3].

*Footnote* Fundamenta Mathematicae, T. LXXIII.
is a representation of $G$. The sets $T^G_\xi = \{ (\xi H, i) : x \in G \}$ are the orbits of the group $G$. The length of $T^G_\xi$ is $\vert G : H \vert$ for $H \leq G$. $T^G_\xi$ is a faithful representation of $G$; there exists a subgroup $H \leq G$ containing no non-trivial normal subgroup of $G$.

Let $S = S^G = \bigcup_{\xi \in \Gamma} S_\xi$. Let $\Gamma^\ast$ be a weak product of groups $\Gamma_\xi$. We assign to every element $\pi$ of the group $\Gamma^\ast$ a permutation of the set $S$ defined by the formula $\pi(a) = \beta^G(a)$ for $a \in S_\xi$. In the sequel we consider the group $\Gamma^\ast$ as the group of permutations of the set $S$ which are defined above.

Now we shall define for ordinal numbers $\xi > 0$ the sets $S^G_\xi$ and extend the permutation $\pi \in \Gamma^\ast$ to those sets. Suppose that for $\eta < \xi$ we have defined the set $S^G_\eta$ and that $\pi(\eta)$ is defined for $x \in S^G_\eta$ For $x \in P(\bigcup_{\xi \leq \eta} (S^G_\xi - S^G_\eta)$ we put $\phi(x) = (\phi(y) : y \in x)$. We define the set $S^G_\xi$ as the subset of the set $P(\bigcup_{\xi \leq \eta} (S^G_\xi - S^G_\eta)$ consisting of all elements $x$ for which there exists a $y \in \alpha$ such that for arbitrary $x \in \Gamma^\ast$ the equalities $\pi^y(x) = \ldots = \pi^y = 1$ imply $\pi(x) = x$. Let $M = M(G, \Xi)$ be the class consisting of all elements $x$ for which there exists an ordinal number $\xi$ such that $x \in S^G_\xi$. The class $M$ is a model of $ZF$.

**Theorem 1.** Let $P$ be an additive semigroup of positive integers generated by a set $Z$ of prime numbers. Then there exists a model $M$ of $ZF$ in which every proposition $\forall n \in P$ and every proposition $\forall n \in P$ is false.

**Proof.** Let $G = \prod_{\xi \in \Xi} G_\xi$, $G_\xi$ being the cyclic group of order $\xi$; let $\Xi$ be the set of all proper subgroups of the group $G$ and $M = M(G, \Xi)$. If $n \in P$ then $n = \sum_{\xi \in Z} k_\xi$, where $k_\xi \in Z$ and $k_\xi$ are positive integers. Let $H_\xi, \ldots, H_n$ be subgroups of $G$ such that $[G : H_\xi] = k_\xi$. Then in the model $M$ there exists no choice function for the set

\[ \bigcup_{\xi \in Z} (T^G_\xi \times \xi) : \xi \in \Xi, \]

where $\xi$ denotes the $\xi$-th member of von Neumann. Thus $\forall n \in P$ is false in $M$.

Suppose that $n \in P$. Let $\pi \in \Gamma^\ast$ be a family of disjoint $n$-element sets. Then there exists an integer $q$ such that $\pi(x) = x$ provided $\pi \in \Gamma^\ast$ and $x^q = \ldots = x^q = 1$. If $\pi \in \Gamma^\ast$ then $\pi(x) = x$. Every equivalence class of the relation $\sim$ consists exactly one element $e_x$.

Let $\theta_\xi = \{ \pi \in A : \pi(e_x) = e_x \}$. If for every $x \in e_x$ there existed a permutation $\pi \in A$ such that $\pi(x) \neq x$, then the group $\theta_\xi$ would have a representation which is a group of permutations of the set $e_x$ with no fixed point, and thus of degree $n$, which is impossible. Thus there exists an element $f \notin e_x$ such that $\pi(f) = f$ for every permutation $\pi \in A$. The set

\[ \{ \pi(f) : \pi \in A \} = \{ \pi(x) : \pi \in A \} \]

is a selector for the set $x$ and belongs to $M(\Xi)$.

**Theorem 2.** Let $G$ be a finite group, $Q(G)$—the additive semigroup of positive integers generated by indices of proper subgroups of the group $G$, and $E(G)$—the additive semigroup of positive integers generated by orders of non-trivial (i.e., $\not= 1$) elements of the group $G$. Then there exists a model $M$ of $ZF$ in which propositions $\forall n \in Q(G)$ are true and propositions $\forall n \in E(G)$ are false.

**Lemma 1.** Let $G_1, \ldots, G_n$ be finite groups and $K_1, \ldots, K_n$—sets of positive integers such that index of each proper subgroup of the group $G_i$ is divisible by at least one of the numbers of the set $K_i$. Then the index of each proper subgroup of the group $\prod_{i=1}^n G_i$ is divisible by at least one of the numbers of the set $\bigcup_{i=1}^n K_i$.

The proof of lemma is inductive (with respect to $r$) and the following simple fact is used:

If $G_1$ and $G_2$ are finite groups and $H_1, H_2$—a subgroup of $G_1 \times G_2$, then

\[ [G_1 \times G_2 : H_1] = [G_1 : G_2] [G_2 : H_1] \]

where

\[ G_1 = (x \in G_1 : (E(x), y) \in H_1) \]

\[ G_2 = (y \in G_2 : (E(x), y) \in H_1) \]

\[ H_1 = (x \in G_1 : (x, 1) \in H_1) \]

\[ H_2 = (y \in G_2 : (1, y) \in H_1) \]

**Proof of theorem 2.** Let $M = M(G, \Xi)$, where $\Xi$ is the set of all proper subgroups of the group $G$.

Let $n \in Q(G)$ and $x \in S^G$ be a family of $n$-element sets which is linearly ordered by $\prec$. Then there exists a positive integer $q$ such that $\pi(x) = x$ provided $\pi \in \Gamma^\ast$, and $x^q = \ldots = x^q = 1$. If $\pi \in \Gamma^\ast$ then $\pi(x) = x$. Suppose that there exists a $\pi \in A$ such that $\pi(x) = x$. Then $\pi$ is the cyclic group generated by $x$. The finiteness of $G$ implies that $\theta$ is finite. Thus the set $\{ \pi(x) : \pi \in A \}$ is finite and has at least 2 elements. This implies that $\pi(x) = x$ is an ordering relation.

---

(1) The proof given above is a slight modification of the proof in Mostowski's paper [4].

(2) This lemma and its proof have been given by Prof. Mostowski.
Let \( u \) be an arbitrary element of the family \( \mathcal{X} \). For every \( x \in u \), there is the least positive integer such that \( a \neq I^a \) and \( a \neq \cdots = a^{b+1} = 1 \) imply \( a(x) = a \). Put \( g(u) = \max (g(x) : x \in u) \). If \( g(u) < q \) then for every \( x \in u \) and \( a \neq \mathcal{X} \) we have \( a(x) = a \). If \( g(u) > q \) then for every \( x \in u \) and \( a \neq \mathcal{X} \) we have \( g(x) = g(u) \), where \( a^{b+1} = a^{b+1} = 1 \) for \( i < g(u) \) and \( a^{b+1} = 1 \). Let \( \mathcal{X}' = \{ x \in \mathcal{H} : (i+1)^{a^{b+1}} = 1 \} \). If for every \( x \in u \) there existed a permutation \( a \neq \mathcal{X} \) such that \( a(x) = a \), then the group \( \mathcal{X} \) would have a representation of degree \( a \). Since \( \mathcal{X} \) is isomorphic with the product of \( q \) copies of \( G \) and \( q \neq Q(G) \), we obtain a contradiction. Thus, for every \( u \in \mathcal{X} \) there exist an \( e_u \in \mathcal{X} \) such that \( a(e_u) = a \) for \( a \neq \mathcal{X} \). The set \( \{ (u, e_u) : u \in \mathcal{X} \} \) is a choice function for the family belonging to \( M \); therefore \( |\mathcal{X}| \) is true in \( M \).

Now let \( \mathcal{X} \in \mathcal{R}(\mathcal{G}) \), i.e., \( |\mathcal{X}| = \sum_{\mathcal{X} \in \mathcal{X}} r_\mathcal{X} \), where \( r_\mathcal{X} \) are the orders of non-trivial elements of the group and \( k \) is positive integers. Without loss of generality we may assume that \( r_\mathcal{X} \) are prime numbers. Let \( \mathcal{H} \in \mathcal{X} \) contain no non-trivial normal subgroup of the group \( G \). Consider the set
\[
a = \bigcup_{\mathcal{X} \in \mathcal{X}} \left\{ (a \times b) : a \in P^{\mathcal{X}}(\mathcal{X}^b \times (a \mathcal{X})) \right\},
\]
where \( P^{\mathcal{X}}(\mathcal{X}) \) denotes the family of all \( q \)-element subsets of the set \( \mathcal{X} \). It is clear that \( a \) belongs to the model. We must show that in \( M \) there exists no choice function. Suppose that such a function exists. Let \( e \) be a choice function for \( a \). Then there exists a positive integer \( q(e) \) such that if \( \mathcal{X} \neq I^a \) and \( a \neq \cdots = a^{b+1} = 1 \) then \( a(x) = a \). Let \( g(x) > q(e) \) be a number divisible by \( x \). Further, let \( \mathcal{X} \) be a permutation of order \( \mathcal{X} \) of the group \( \mathcal{X}^a \), \( (1 \leq i \leq e) \). We have \( a^i = a^i \mathcal{X}^a \neq 1 \). Let \( h_1, \ldots, h_e \) be the sets of elements of fixed cycles of permutations \( a_1, \ldots, a_e \). Evidently, \( b = \bigcup_{i=1}^e (h_i \times b) \). We define the element \( \mathcal{X} \) of the group putting \( \mathcal{X}^a = 1 \) for \( i < q(e) \) and \( \mathcal{X}^a = 1 \) for \( i \geq q(e) \). Let \( h \) be a choice function for \( \mathcal{X} \) in \( M \).

\[
\varphi((h, x)) \in \varphi(x) \quad \forall x \in \mathcal{X}.
\]

Hence we get \( \mathcal{X} = \mathcal{X} \) (which is impossible, because \( a \neq \mathcal{X} \)). Therefore the proposition \( [a] \) is false in the model \( M \). At last, if \( n \neq Q(G) \) then \( n = \sum_{i=1}^t \mathcal{X}_i \), where \( \mathcal{X}_i \) is the index of the proper subgroup of the group \( G \) and \( \mathcal{X}_i \) is a positive integer. Let \( H_1, \ldots, H_t \in \mathcal{X} \) satisfy the equalities \( G = H = \mathcal{X}_i \) for \( 1 \leq i \leq t \). Then in the model there is no choice function for
\[
\{ (\bigcup_{i=1}^t (H_i \times b) : 1 \leq i \leq t) \}.
\]

Thus the proposition \( [a] \) is false in \( M \), q.e.d.

**Lemma 2.** If \( p \) and \( q \) are prime numbers such that \( p = (p^2-1)/(p-1) \) is a prime number, then there exists a group \( G \) such that the indices of its proper subgroups are divisible by \( p \) or \( q \).

**Proof.** Let \( p \) be a prime number such that \( p \) is a prime number. Let \( \mathcal{A} \) be an elementary Abelian group of order \( p^2 \). Then the order of its automorphism group is divisible by \( p \). In virtue of the Cauchy theorem there exists an automorphism \( a \) of the group \( \mathcal{A} \) of the order \( p \). Consider the set of pairs \( (a, x) \), where \( x \in \mathcal{A} \). This set becomes a group if we define multiplication by the formula
\[
(a, x)(a', y) = (a+1, (a')^{-1} + xy).
\]

Denote this group by \( G(p, q) \). The order of \( G(p, q) \) is \( p^2 \cdot p \). The set of elements of the form \((1, y)\) is a subgroup of the group \( G(p, q) \) and its index is equal to \( p \); the set of elements of the form \((a, 1)\) is a subgroup of index \( p^2 \). Let \( H \) be a subgroup of the group \( G(p, q) \) such that its index is divisible neither by \( p \) nor \( q \). Thus the order of \( H \) is of the form \( p^2 \cdot p \), where \( 0 < q < p \). By the Cauchy theorem there exist elements \( u, v \in \mathcal{H} \) of the orders \( p_1 \) and \( p_2 \), respectively. It is easy to see that \( u = (a, x) \) and \( v = (1, y) \), where \( x, y \) are elements of the group \( \mathcal{A} \) and \( p_1 \neq p_2 \).

Let \( \tau \) be a transformation of the group \( \mathcal{A} \). Consider the automorphism \( \tau \) of the group \( \mathcal{A} \) as a permutation of the set \( A = (1, 1) \). It is easy to see that \( \tau \) is a permutation with no fixed points, i.e., it is the product of \( p-1 \) cycles of the length \( p^2 \). If \( \tau \in A = (1, 1) \), \( \tau \neq (1, 1) \), then the elements \( w, w' \) belong to different cycles of permutation \( \tau \). If this were not the case (without loss of generality we may assume that \( l = 1 \)), then the elements \( w, w', w'' \) would form a cycle of the length \( < p-1 \), which is impossible because the order \( \tau \) is equal to \( p_1 \).

Therefore, for arbitrary \( \tau \in A = (1, 1) \) the elements \( w, w', w'' \) belong to different cycles of permutation \( \tau \). The elements of the form \( u^m v^n \) are all elements of the group \( G(p, q) \) of the form \((1, y)\). Thus there exist elements \( k_0 \) and \( k_0 \) such that \( (1, y^{-1}) = u^m v^n \). Hence we get \( (a, 1) = u^m v^n \). Thus all elements of the group \( G(p, q) \) are of the form \( u^m v^n \), which is impossible because the order \( \tau \) is equal to \( p_1 \). Therefore, \( \mathcal{X} \) is a permutation with no fixed points, i.e., it is the product of \( p-1 \) cycles of the length \( p^2 \). If \( \tau \in A = (1, 1) \), \( \tau \neq (1, 1) \), then the elements \( w, w' \) belong to different cycles of permutation \( \tau \). If this were not the case (without loss of generality we may assume that \( l = 1 \)), then the elements \( w, w', w'' \) would form a cycle of the length \( < p-1 \), which is impossible because the order \( \tau \) is equal to \( p_1 \).

**Theorem 3.** Let \( p \) and \( q \) be prime numbers such that \( p = (p^2-1)/(p-1) \) is a prime number. Then there exists a model \( M \) for \( \mathcal{X} \) in which the propositions \( [a] \), where \( a \) is of the form \( kp^2 + lq \), are true, the propositions \( [n] \), where \( n \) is of the form \( kp + lq \), are false, and the propositions \( [a] \) for \( a \neq \mathcal{X} \) are false.

**Proof.** It is sufficient to put \( G = G(p, q) \) in Theorem 2.

**Theorem 4.** If for every prime number \( p \) there exist infinitely many prime numbers of the form \((p^2-1)/(p-1)\), then there exists a model of \( \mathcal{X} \).
in which every sentence \([n^p]\) is true and every sentence \([n]\) for \(n > 1\) is false \((\ast)\).

Proof. Let \(A\) and \(B\) be arbitrary finite sets of positive integers and \(\min B > 1\). We shall show that there exists a model \(M\) for \(\mathbb{Z}^p \cup \{\neg [n]: n \in A\} \cup \{\neg \neg [n]: n \in B\}\). Let \(p_1, \ldots, p_k\) be prime numbers such that every element of the set \(B\) is divisible by at least one of these numbers. From the assumption it follows that there exist prime numbers \(q_1, \ldots, q_k\) such that \((p_i^q - 1)(p_i - 1)\) are prime numbers greater than the numbers of the set \(A\). By lemma 2 there exist groups \(G_1, \ldots, G_k\) such that the index of every proper subgroup of the group \(G_i\) is divisible by at least one of the numbers of the set \(C_i \equiv (p_i^q - 1)(p_i - 1)\). Let \(G = \bigcap_{i=1}^k G_i\). Using lemma 1, we infer that the index of every proper finite subgroup of the group \(G\) is divisible by at least one of the numbers of the set \(\bigcup C_i\). In virtue of theorem 2 there exists a model in which the propositions \([n^p]\) for \(n \in A\) are true and the propositions \([n]\) for \(n \in B\) are false. Using the compactness theorem we obtain the assertion of theorem 4.

\(^{(*)}\) The famous conjecture on the existence of infinitely many Mersenne primes (i.e., the numbers \(2^p - 1\)) is a particular case of the conjecture stated in the assumption of the theorem.

References


Reçu par la Rédaction le 27. I. 1970

Some properties of convex metric spaces

by

B. Krakus (Stockholm)

1. Introduction. A point \(x\) of a metric space \((X, \rho)\) is said to be a frontier point (see [6]) if there exists a point \(y \in X\) such that for every point \(z \in X \setminus \{x\}\) we have

\[\rho(y, z) - \rho(x, z) > \rho(y, x).\]

The aim of this paper is to give a topological characterization of a frontier point of a compact strongly convex \((\ast)\) finite-dimensional metric space \((X, \rho)\) without ramifications \((\ast)\) (denoted by \((X, \rho) \in \text{SCWB}\). Holzszynski and Kuperberg have proved (see [4]) that every frontier point of a space \((X, \rho) \in \text{SCWB}\) is a labile point in \(X\) \((\ast)\). It follows from [3] that the set of the frontier points of a space \((X, \rho) \in \text{SCWB}\) is a boundary set (see [6]). In the present note it is shown that this set is compact.

I give some remarks concerning the set of the stable points \((\ast)\) of the SCWB-spaces.

2. Property of a ball. Let \((X, \rho) \in \text{SCWB}\). Then there exists exactly one function \(\lambda: X \times X \times I \to X\) where \(I = (0, 1)\) such that

\[\rho(x, \lambda(x, y, t)) = t\rho(x, y) \quad \text{and} \quad \rho(x, \lambda(x, y, 0)) = (1 - t)\rho(x, y).\]

It is not difficult to see that the function \(\lambda\) defined above is continuous. Let us write \([x, y] = \lambda([x, y] \times I)\). This means that \(x \in [x, y]\) if and only if

\[\rho(x, z) - \rho(x, y) = \rho(x, y) .\]

\(^{(*)}\) A metric space \((X, \rho)\) is said to be strongly convex (see [1]) if for every two points \(x, y \in X\) there exists exactly one point \(z \in X\) such that \(\rho(x, z) = \rho(x, y) = \rho(y, z)\).

\(^{(**)}\) A metric space \((X, \rho)\) is said to be without ramifications if for all points \(x, y, z \in X\) the conditions \(\rho(x, z) = \rho(y, z) = \rho(y, x) = \rho(x, y)\) imply \(x = z\) (see (6)).

\(^{(***)}\) A point \(p\) of topological space \(X\) is said to be a labile point in \(X\) if for any neighbourhood \(U\) of \(p\) there exists a homotopy \(h: X \times I \to X\) such that the following conditions hold: (i) \(h(x, 0) = x\) for every \(x \in X\), (ii) \(h(x, t) = x\) for every \(x \in X \setminus \{p\}, t \in I\), (iii) \(h(x, t) = p\) for every \(x \in X \setminus \{p\}, t \in I\), (iv) \(h(x, 1) = p\) for every \(x \in X \setminus \{p\}\). A point of topological space \(X\) is said to be a stable point in \(X\) if it is not a labile point.