Some new algebraic equivalents of the Axiom of Choice

By A. HAJNAL (Budapest) and A. KERTÉSZ (Debrecen)

The aim of this note is to prove the Theorem below. We shall work within ZF, i.e. ZERMELO—FRAENKEL *set theory without the Axiom of Choice*; we shall use the usual notations and terminology of set theory. In particular, ordinals are identified with their predecessors.

Theorem. *In ZF, the following statements are equivalent:*

(i) *Axiom of Choice.*

(ii) *On every nonempty set there exists a cancellative groupoid.*[1])

PROOF. First let us consider the implication (i)⇒(ii). In the case of a finite set (with n elements) choose the group of n-th roots of unity; in the case of a countably infinite set take, for instance, the additive group of the rational integers. In general, an algebraic structure $\langle X, +, 0\rangle$ is a group if and only if it is a model of a formula φ in a language L of first order predicate calculus containing the symbols $+$ and 0. (φ means the conjunction of the usual group axioms.) If a formula φ in a language with countably many symbols has an infinite model then, according to the upward LÖWEHEIM—SKOLEM theorem, it has a model of an arbitrary infinite power.[2])

As to the implication (ii)⇒(i): Evidently, it is sufficient to prove from (ii) that every non-empty set can be mapped on a suitable well-ordered set in a one-to-one way. We shall use the following

Lemma. (HARTOGS [1].) *In ZF, the following statement is true: Let A be an arbitrary set. Then there exists an ordinal α such that A does not possess any subset which can be mapped on α in a one-to-one way.*

PROOF OF THE LEMMA. Put

$$\alpha = \bigcup \{\text{type}\,(\langle X, R\rangle)+1 : X \subseteqq A, \quad R \subseteqq A\times A, \quad \text{and } R \text{ wellorders } X\},$$

where type $(\langle X, R\rangle)$ denotes the order type of $\langle X, R\rangle$. The right-hand side of this formula does indeed define a set. This follows from the conjunction of several axioms among them the Power Set Axiom and instances of the Replacement Scheme. Moreover, it is clear that α is an ordinal satisfying the requirements of the lemma.[3])

---

[1]) We remark that the property "cancellative" in both parts is essential and neither of them can be spared: Evidently, every set S becomes a right (but not left) cancellative semigroup be defining $x+y=x$ $(x, y\in S)$.

[2]) For other more algebraic proofs see e. g. [2].

[3]) This short proof was pointed out to us by A. MÁTÉ.

Let A be an arbitrary set and α an ordinal with the property described in the lemma. Let $\langle B, \prec \rangle$ denote a well-ordered set of type α. We may suppose $A \cap B = \emptyset$. Put $C = A \cup B$. According to (ii) there exists a binary operation $+$ on C such that $\langle C, + \rangle$ is a cancellative groupoid.

Now we shall prove the following proposition:

($*$) *For each $x \in A$ there is a $y \in B$ for which $x+y \in B$ holds.*
Suppose, ($*$) does not hold. Then there exists an $x \in A$ such that $x+y \in A$ for each $y \in B$. Because of the cancellation law, the function $f(y) = x+y$ ($y \in B$) maps the well-ordered set B of type α into A in a one-to-one way, which contradicts the choice of α. This proves ($*$).

Now, let be $D = B \times B$ and $\prec'$ the lexicographic ordering, which is a well-ordering of D obtained from $\prec$. We define a map $g: A \to D$ as follows:

For $x \in A$ put $g(x) = \min_{\prec'} \{\langle y, z \rangle | y, z \in B \text{ and } x+y = z\}$. The ordering $\prec'$ being a wellordering, by ($*$), the mapping g is defined for each $x \in A$ and is single-valued. Furthermore, g is one-to-one, because, in view of the cancellation law, from $x \neq x'$ it follows that $g(x) \neq g(x')$. Hence g is a one-to-one mapping of A onto a subset of the well-ordered set D. Consequently, the set A can be well-ordered.[4])

Corollary. *The Axiom of Choice is equivalent to any of the assertions listed under* ($**$).

($**$) *On every nonempty set there exists,*

(a) *a cancellative semigroup,*

(b) *a cancellative abelian semigroup,*

(c) *a quasigroup,*

(d) *a loop,*

(e) *a group,*

(f) *an abelian group,*

(g) *a ring,*

(h) *a commutative ring,*

(i) *an integral domain with unit.*

References

[1] F. Hartogs, Über das Problem der Wahlordnung, *Math. Ann.* **76** (1915) 438—443.
[2] A. Kertész, Das Kuratowski-Zornsche Lemma und seine Anwendungen in der Algebra, Lecture Notes, University of Jyväskylä, *Jyväskylä* 1973.
[3] A. Tajtelbaum—A. Tarski, Sur quelques théorèmes qui équivalent à l'axiome du choix. *Fund. Math.* **5** (1924), 197—201.

(Received April 5, 1971)

[4]) The proof of the implications $(ii) \Rightarrow (i)$ is an unessential modification of a proof of the following theorem due to A. Tarski: If $m^2 = m$ holds for every infinite power m, then the Axiom of Choice also holds [3].