Marianne Morillon

Linear forms and axioms of choice

Commentationes Mathematicae Universitatis Carolinae, Vol. 50 (2009), No. 3, 421--431

Persistent URL: `http://dml.cz/dmlcz/134914`

Linear forms and axioms of choice

Marianne Morillon

Abstract. We work in set-theory without choice **ZF**. Given a commutative field $\mathbb{K}$, we consider the statement $\mathbf{D}(\mathbb{K})$: "On every non null $\mathbb{K}$-vector space there exists a non-null linear form." We investigate various statements which are equivalent to $\mathbf{D}(\mathbb{K})$ in **ZF**. Denoting by $\mathbb{Z}_2$ the two-element field, we deduce that $\mathbf{D}(\mathbb{Z}_2)$ implies the axiom of choice for pairs. We also deduce that $\mathbf{D}(\mathbb{Q})$ implies the axiom of choice for linearly ordered sets isomorphic with $\mathbb{Z}$.

Keywords: Axiom of Choice, axiom of finite choice, bases in a vector space, linear forms

Classification: Primary 03E25; Secondary 15A03

1. Introduction

1.1 Existence of bases in vector spaces. We work in set-theory without the Axiom of Choice **ZF**. According to a theorem due to Höft and Howard (see [5]), the Axiom of Choice (**AC**) is equivalent (in **ZF**) to the statement **ST**: *"Every connected graph contains a spanning tree"* (for other statements equivalent to **AC** formulated in terms of "spanning graphs", see [2]). In a recent paper (see [6]), Howard showed that given a commutative field $\mathbb{K}$, the following statement $\mathbf{BE}(\mathbb{K})$ — which Howard denotes by $AL19(\mathbb{K})$ — implies **ST** (and thus **AC**):

> $\mathbf{BE}(\mathbb{K})$ (Basis Extraction): *"Given a vector space E over $\mathbb{K}$, every generating subset of E contains a basis of E."*

This enhances a result due to Halpern (see [3]) who showed that the statement "$\forall \mathbb{K}\, \mathbf{BE}(\mathbb{K})$" (i.e. the existence of a basis in a generating subset of any vector space over *any* commutative field) implies **AC**. This also extends a result due to Keremedis (see [10]) who showed that $\mathbf{BE}(\mathbb{Z}_2)$ implies **AC**: here, where for each integer $n \geq 2$, we denote by $\mathbb{Z}_n$ the ring $\mathbb{Z}/n\mathbb{Z}$. Now, consider the following consequence of $\mathbf{BE}(\mathbb{K})$:

> $\mathbf{B}(\mathbb{K})$: *"Every vector space over $\mathbb{K}$ has a basis."*

Blass ([1], 1984) showed in **ZF** that the statement "$\forall \mathbb{K}\, \mathbf{B}(\mathbb{K})$" (i.e. the existence of a basis in every vector space over *any* commutative field) implies **AC**, or rather the following equivalent of **AC** (see [8]):

> **MC** ("Multiple Choice"): *"For every family $(A_i)_{i\in I}$ of non-empty sets, there exists a family $(F_i)_{i\in I}$ of non-empty finite sets such that for every $i \in I$, $F_i \subseteq A_i$".*

The following question is open (see [6]):

1 Question. Does there exist a (commutative) field $\mathbb{K}$ such that $\mathbf{B}(\mathbb{K})$ implies $\mathbf{AC}$? For example, does $\mathbf{B}(\mathbb{Q})$ imply $\mathbf{AC}$? Does $\mathbf{B}(\mathbb{Z}_2)$ imply $\mathbf{AC}$? Does the statement "For every prime number p, $\mathbf{B}(\mathbb{Z}_p)$" imply $\mathbf{AC}$?

1.2 Existence of non-null linear forms. Given a commutative field $\mathbb{K}$, and a $\mathbb{K}$-vector space E, a *linear form* on E is a linear mapping $f : E \to \mathbb{K}$. The set E^* of linear forms on E is a vector subspace of $\mathbb{K}^E$, which is called the *algebraic dual* of E. Consider the following consequences of $\mathbf{B}(\mathbb{K})$.

(i) $\mathbf{LE}(\mathbb{K})$ (Linear extender): *For every $\mathbb{K}$-vector space E, and every vector subspace F of E, there exists a linear mapping $T : F^* \to E^*$ such that for each $f \in F^*$, $T(f)$ extends f.*

(ii) $\mathbf{DE}(\mathbb{K})$ (dual extension): *"For any non null $\mathbb{K}$-vector space E, every vector subspace F of E, and every linear form $f : F \to \mathbb{K}$, there exists a linear form $\tilde{f} : E \to \mathbb{K}$ which extends f."*

(iii) $\mathbf{DS}(\mathbb{K})$ (dual separating): *"For any non null $\mathbb{K}$-vector space E and every $a \in E\backslash\{0\}$, there exists a linear form $f : E \to \mathbb{K}$ such that $f(a) = 1$."*

(iv) $\mathbf{D}(\mathbb{K})$ (dual): *"For any non null $\mathbb{K}$-vector space E, there exists a linear form $f : E \to \mathbb{K}$ which is not null."*

In Sections 2 and 3, we shall show that the above three statements (ii), (iii) and (iv) are equivalent (in $\mathbf{ZF}$). Moreover, we shall also show that $\mathbf{B}(\mathbb{K}) \Rightarrow \mathbf{LE}(\mathbb{K}) \Rightarrow \mathbf{D}(\mathbb{K})$.

2 Question. Given a commutative field $\mathbb{K}$, does $\mathbf{D}(\mathbb{K})$ imply $\mathbf{B}(\mathbb{K})$? Does $\mathbf{D}(\mathbb{K})$ imply $\mathbf{LE}(\mathbb{K})$? Does $\mathbf{LE}(\mathbb{K})$ imply $\mathbf{B}(\mathbb{K})$?

1.3 Various axioms of choice. In [6], Howard proved that $\mathbf{B}(\mathbb{Z}_2)$ implies that "Every *well ordered* family of pairs has a non-empty product". In this paper, we shall enhance this result and we shall prove that $\mathbf{D}(\mathbb{Z}_2)$ implies that "Every family of pairs has a non-empty product".

1 *Notation.* For every finite set F, we denote by $|F|$ its cardinal.

We now review various axioms of "Finite Choice":

$\mathbf{AC}^{\text{fin}}$: *"Every family of non-empty finite sets has a non-empty product."*

The statement $\mathbf{AC}^{\text{fin}}$ does not imply $\mathbf{AC}$ and $\mathbf{ZF}$ does not imply $\mathbf{AC}^{\text{fin}}$ (see [8] or [7]). Given an integer $n \geq 2$, and some prime natural number p, consider the following consequences of $\mathbf{AC}^{\text{fin}}$.

(i) $\mathbf{AC}^n$: *"Every family $(A_i)_{i\in I}$ of finite non-empty sets having at most n elements has a non-empty product."*

(ii) $\mathbf{AC}^n_{wo}$: *"For every ordinal α, every family $(A_i)_{i\in\alpha}$ of non-empty finite sets with at most n elements has a non-empty product."*

(iii) $\mathbf{C}(p)$: *"For every family $(A_i)_{i\in I}$ of finite non-empty sets, there exists a family $(F_i)_{i\in I}$ of finite sets such that for all $i \in I$, $F_i \subseteq A_i$, and p does not divide the cardinal $|F_i|$ of F_i."*

For every integer $n \geq 2$, denote by $\mathbf{AC}^{=n}$ the statement *"Every family of n-element sets has a non-empty product."* Then $\mathbf{C}(2) \Rightarrow \mathbf{AC}^2$ and $\mathbf{C}(3) \Rightarrow \mathbf{AC}^{=3}$.

3 Question. Does $\mathbf{C}(5)$ imply $\mathbf{AC}^{=5}$?

In this paper, we shall prove that:

(i) if p is a prime natural number, then $\mathbf{D}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$ (see Section 4);
(ii) $\mathbf{D}(\mathbb{Q})$ implies that every family of linearly ordered sets isomorphic with $\mathbb{Z}$ has a non-empty product (see Section 5).

Notice that the statement "For every prime number p, $\mathbf{C}(p)$" implies the statement "For every integer $n \geq 2$, $\mathbf{AC}^n$" (see Remark 4 in Section 4). However, the statement "For every integer $n \geq 2$ $\mathbf{AC}^n$" does not imply $\mathbf{AC}^{\text{fin}}$ (see [8] or [7]).

1 *Remark.* Keremedis ([11]) proved in **ZFA** (set-theory with atoms described in [8]), that for every integer $n \geq 2$, $\mathbf{B}(\mathbb{Q})$ implies the following statement: "For every sequence $(F_k)_{k \in \mathbb{N}}$ of non-empty finite sets each having at most n elements, there exists an infinite subset A of $\mathbb{N}$ such that $\prod_{n \in A} F_n$ is non-empty".

4 Question. Does $\mathbf{B}(\mathbb{Q})$ imply $\forall n \geq 2\ \mathbf{AC}^n$?

1 Proposition. *Let $\mathbb{K}$ be a commutative field with null characteristic (for every integer $n \geq 1$, $n \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$). In* **ZFA**, **MC** *implies* $\mathbf{DS}(\mathbb{K})$ *(and thus* **MC** *implies* $\mathbf{DS}(\mathbb{Q})$*).*

Proof: Let E be a $\mathbb{K}$-vector space. Using **MC**, there is a mapping Φ such that for every vector subspaces V, W of E satisfying $V \subseteq W$ and W/V is finite-dimensional, for every linear mapping $f : V \to \mathbb{K}$, $\Phi(V, W, f) : W \to \mathbb{K}$ is a linear mapping extending f. Indeed, let Z be the set of such (V, W, f). For each $(V, W, f) \in Z$, the vector-space W/V is finite-dimensional, thus the set $A_{V,W,f}$ of linear mappings $u : W \to \mathbb{K}$ extending f is non-empty (in **ZFA**). Using **MC**, consider some family $(B_i)_{i \in Z}$ of non-empty finite sets such that for every $i \in Z$, $B_i \subseteq A_i$. Then, for every $i \in Z$, define $\Phi(i) := \frac{1}{|B_i|} \sum_{u \in B_i} u$ (here we use the fact that the characteristic of $\mathbb{K}$ is null). Now, assume that $a \in E \backslash \{0\}$. Using **MC**, there exists an ordinal α and some partition $(F_i)_{i \in \alpha}$ in finite sets of E. This implies that there is a family $(V_i)_{i \in \alpha}$ of vector subspaces of E such that for every $i < j < \alpha$, $V_i \subseteq V_j$ and V_j/V_i is finite-dimensional. Without loss of generality, we may assume that $a \in V_0$. Using the choice function Φ, we define by transfinite recursion a family $(f_i)_{i \in \alpha}$ such that for each $i \in \alpha$, $f_i : V_i \to \mathbb{K}$ is linear, $f_0(a) = 1$, and for every $i < j \in \alpha$, f_j extends f_i. Define $f := \bigcup_{i \in \alpha} f_i$. Then $f : E \to \mathbb{K}$ is linear and $f(a) = 1$. □

Consider the following statement (form [18A] in [7, p. 28]): "Every denumerable set of two-element sets has an infinite subset with a choice function".

1 Corollary. *In* **ZFA**, $\mathbf{DS}(\mathbb{Q})$ *does not imply "form* [18A]*". Thus in* **ZFA**, $\mathbf{DS}(\mathbb{Q})$ *does not imply* $\mathbf{B}(\mathbb{Q})$*.*

Proof: In the second Fraenkel model of **ZFA** (the model $\mathcal{N}2$ described in [7, p. 178]), **MC** holds thus **DS**($\mathbb{Q}$) also holds (use Proposition 1), however, "form [18A]" does not hold (see [7, p. 178]). Using Keremedis's result quoted in Remark 1, it follows that **B**($\mathbb{Q}$) does not hold in this model. □

2. D($\mathbb{K}$) ⇒ DS($\mathbb{K}$)

2.1 Preliminaries about reduced products of $\mathbb{L}$-structures. We now review techniques described and used by W.A.J. Luxemburg in [12].

2.1.1 Reduced products of sets. Given a filter $\mathcal{F}$ on a (non-empty) set I, and a family $(E_i)_{i\in I}$ of sets, let $E := \prod_{i\in I} E_i$, and let $\sim_\mathcal{F}$ be the binary relation on E defined as follows: if $x = (x_i)_{i\in I}$, $y = (y_i)_{i\in I} \in E$, then $x \sim_\mathcal{F} y$ if and only if the set $\{i \in I : x_i = y_i\}$ belongs to $\mathcal{F}$. Then, the binary relation $\sim_\mathcal{F}$ is an equivalence relation on E.

2.1.2 Reduced products of $\mathbb{L}$-structures. Let $\mathbb{L}$ be a (egalitary) first order language. Let $\mathcal{F}$ be a filter on a (non-empty) set I. Let $(\mathfrak{M}_i)_{i\in I}$ be a family of (egalitary) $\mathbb{L}$-structures with (non-empty) underlying sets M_i. Assume that the set $M := \prod_{i\in I} M_i$ is non-empty (this is the case in **ZF** if, for example, the language $\mathbb{L}$ contains a constant symbol). Endow M with the *direct product* (egalitary) $\mathbb{L}$-structure $\mathfrak{M}$ (see [4, p. 413]).

We define an egalitary $\mathbb{L}$-structure $\mathfrak{M}_\mathcal{F}$ on the quotient set $M/{\sim_\mathcal{F}}$ as follows (see [4, pp. 442–443]). For each constant symbol $\sigma \in \mathbb{L}$, we consider the equivalence class $\sigma^{\mathfrak{M}_\mathcal{F}}$ of the interpretation $\sigma^{\mathfrak{M}}$ of σ in $\mathfrak{M}$; for each n-ary function symbol $\sigma \in \mathbb{L}$, its interpretation $\sigma^{\mathfrak{M}} : M^n \to M$ in $\mathfrak{M}$ has a unique quotient $\sigma^{\mathfrak{M}_\mathcal{F}} : M_\mathcal{F}^n \to M_\mathcal{F}$; for each n-ary relation symbol $\sigma \in \mathbb{L}$, we consider the n-ary relation $\sigma^{\mathfrak{M}_\mathcal{F}}$ on $M_\mathcal{F}$ satisfying for every $x_1 = (x_i^1)_{i\in I}, \ldots, x_n = (x_i^n)_{i\in I} \in M$: $\sigma^{\mathfrak{M}_\mathcal{F}}(can((x_i^1)_{i\in I}), \ldots, can((x_i^n)_{i\in I}))$ iff $\{i \in I : \sigma^{\mathfrak{M}_i}(x_i^1, \ldots, x_i^n)\} \in \mathcal{F}$.

2.1.3 Preservation of basic Horn formulae. An $\mathbb{L}$-formula ϕ is a *basic Horn formula* if ϕ is of the form $((\wedge_{p\in F} p) \to q)$ where F is a finite set of atomic $\mathbb{L}$-formulae and q is an atomic $\mathbb{L}$-formula.

2 Proposition. *Let $\mathcal{F}$ be a filter on a set I, and let $(\mathfrak{M}_i)_{i\in I}$ be a family of $\mathbb{L}$-structures with (non-empty) underlying sets M_i. Assume that the product set $M = \prod_{i\in I} M_i$ is non-empty. Endow the quotient set $M/{\sim_\mathcal{F}}$ with the $\mathbb{L}$-structure $\mathfrak{M}_\mathcal{F}$. If ϕ is a Horn $\mathbb{L}$-formula which is satisfied by every $\mathbb{L}$-structure $\mathfrak{M}_i$, then $\mathfrak{M}_\mathcal{F} \models \phi$.*

Proof: The proof is straightforward. See for example Hodges [4]. □

2.1.4 Reduced powers of an $\mathbb{L}$-structure. If M is a set and $\mathcal{F}$ is a filter on a set I, then we denote by $M_\mathcal{F}$ the set $M^I/{\sim_\mathcal{F}}$. We also denote by $\Delta_I : M \hookrightarrow M^I$ the "diagonal mapping" associating to each $x \in M$ the constant mapping $I \to M$ with value x; we denote by $can_\mathcal{F}^M : M \hookrightarrow M_\mathcal{F}$ the one-to-one mapping associating to each $x \in M$ the equivalence class of $\Delta_I(x)$ *modulo* $\sim_\mathcal{F}$.

If $\mathfrak{M}$ is an $\mathbb{L}$-structure with underlying set M and $\mathcal{F}$ is a filter on a set I, then we denote by $\mathfrak{M}_{\mathcal{F}}$ the set $M_{\mathcal{F}}$ endowed with the reduced product $\mathbb{L}$-structure described previously. Then $can^M_{\mathcal{F}} : M \hookrightarrow M_{\mathcal{F}}$ is an $\mathbb{L}$-embedding.

1 Example (Reduced powers of a commutative unitary ring)**.** Given a commutative unitary ring A and a filter $\mathcal{F}$ on a set I, the reduced power $A_{\mathcal{F}}$ is a commutative unitary ring. Moreover, if $\mathbb{K}$ is a commutative field and if A is a $\mathbb{K}$-algebra, then $A_{\mathcal{F}}$ is also a $\mathbb{K}$-algebra.

2 *Notation.* Let A, B be sets. Let $u \in (B^A)_{\mathcal{F}}$: then u is the equivalence class of some family $(u_i)_{i\in I}$ of B^A. We denote by $\hat{u} : A_{\mathcal{F}} \to B_{\mathcal{F}}$ the mapping such that for each $(x_i)_{i\in I}$, denoting by $\dot{x}$ the equivalence class of $(x_i)_{i\in I}$ in $A_{\mathcal{F}}$, $\hat{u}(\dot{x})$ is the equivalence class of $(u_i(x_i))_{i\in I}$ in $B_{\mathcal{F}}$.

2.1.5 Concurrent relations. Let E, F be two sets and let $R \subseteq E \times F$ be a binary relation. The relation R is said to be *concurrent* if for every non-empty finite subset G of E, the set $\cap_{x\in G} R(x)$ is nonempty. The relation R is concurrent if and only if the subsets $R(x)$ of F satisfy the finite intersection property: in this case, we denote by $\mathcal{F}_R$ the filter on F generated by the sets $R(x)$, $x \in E$.

3 Proposition (Luxemburg, [12])**.** *Let E, I be two sets and let $R \subseteq E \times I$ be a concurrent binary relation. Let $\mathcal{F}$ be the filter on I generated by the sets $R(x)$, $x \in E$. Then, there exists an equivalence class $\iota = \dot{(\iota_i)}_{i\in I}$ in $I_{\mathcal{F}}$ such that for every $x \in E$, $\{i \in I : R(x, \iota_i)\} \in \mathcal{F}$.*

Proof: Let $\mathrm{Id}_I : I \to I$ be the "identity mapping" and let ι be the equivalence class of Id_I in $I_{\mathcal{F}}$. Then, for every $x \in E$, $\{i \in I : R(x, i)\} = R(x) \in \mathcal{F}$. □

2.2 $\mathbf{D}(\mathbb{K}) \Rightarrow \mathbf{DS}(\mathbb{K})$.

1 Lemma. *Let $\mathbb{K}$ be a commutative field, let E be a non-null $\mathbb{K}$-vector space and $a \in E\backslash\{0\}$. Let $I := \mathbb{K}^E$. There exists a filter $\mathcal{F}$ on I and a linear mapping $u : E \to \mathbb{K}_{\mathcal{F}}$ such that $u(a) = 1_{\mathbb{K}_{\mathcal{F}}}$.*

Proof: Let $R \subseteq (\mathcal{P}_{\text{fin}}(E) \times I)$ be the following binary relation: given a finite subset F of E and some mapping $u : E \to \mathbb{K}$, then $R(F, u)$ iff $u(a) = 1$ and $u_{\restriction F}$ is linear. Here, " $u_{\restriction F}$ is linear" means that for every $x, y \in F$ and $\lambda \in \mathbb{K}$, $x + y \in F \Rightarrow u(x + y) = u(x) + u(y)$ and $\lambda x \in F \Rightarrow u(\lambda x) = \lambda u(x)$. Using Proposition 3, let $\mathcal{F}$ be a filter on I and $\iota = \dot{(\iota_i)}_{i\in I} \in I_{\mathcal{F}}$ such that for every finite subset F of E, the set $\{i \in I : R(F, \iota_i)\}$ belongs to $\mathcal{F}$. Using Notation 2, $\hat{\iota} \in {\mathbb{K}_{\mathcal{F}}}^{E_{\mathcal{F}}}$, thus $\hat{\iota}$ induces a mapping $\iota_E : E \to \mathbb{K}_{\mathcal{F}}$. Moreover, $\iota_E(a) = 1_{\mathbb{K}_{\mathcal{F}}}$. For every $x, y \in E$ and $\lambda \in \mathbb{K}$, $\iota_E(x + \lambda y) = \iota_E(x) + \lambda\iota(y)$: indeed, let $F := \{x, y, \lambda y, x + \lambda y\}$; by definition of ι, the set $J := \{i \in I : R(F, \iota_i)\}$ belongs to $\mathcal{F}$, and J is a subset of the set $\{i \in I : \iota_i(x + \lambda y) = \iota_i(x) + \lambda\iota_i(y)\}$. □

1 Theorem. $\mathbf{D}(\mathbb{K}) \Rightarrow \mathbf{DS}(\mathbb{K})$.

Proof: Let E be a $\mathbb{K}$-vector space and $a \in E\backslash\{0\}$. Using the previous lemma, let $\mathcal{F}$ be a filter on a set I and a linear mapping $u : E \to \mathbb{K}_{\mathcal{F}}$ such that $u(a) = 1$. Using $\mathbf{D}(\mathbb{K})$, let $f : \mathbb{K}_{\mathcal{F}} \to \mathbb{K}$ be a non-null linear mapping. Let $z \in \mathbb{K}_{\mathcal{F}}$ such that $f(z) = 1$. Denoting by $m_z : \mathbb{K}_{\mathcal{F}} \to \mathbb{K}_{\mathcal{F}}$ the linear mapping associating to each $x \in \mathbb{K}_{\mathcal{F}}$ the element zx, it follows that $v := f \circ m_z \circ u : E \to \mathbb{K}$ is linear and that $v(a) = f \circ m_z(1) = f(z) = 1$. □

3. Other equivalents of $\mathbf{D}(\mathbb{K})$

3.1 Equivalents of $\mathbf{DS}(\mathbb{K})$.

2 Theorem. *Given a commutative field $\mathbb{K}$, the following statements are equivalent.*

(i) $\mathbf{DE}(\mathbb{K})$ (dual extension): *"For any non null $\mathbb{K}$-vector space E, every vector subspace F of E, and every linear form $f : F \to \mathbb{K}$, there exists a linear form $\tilde{f} : E \to \mathbb{K}$ which extends f."*

(ii) (multiple $\mathbf{DE}(\mathbb{K})$) *"Given a family $(E_i)_{i\in I}$ of $\mathbb{K}$-vector spaces, a family $(F_i)_{i\in I}$ such that each F_i is a vector subspace of E_i, and a family $(f_i)_{i\in I}$ such that each $f_i : F_i \to \mathbb{K}$ is linear, there exists a family $(\tilde{f}_i)_{i\in I}$ such that each $\tilde{f}_i : E_i \to \mathbb{K}$ is a linear form extending f_i."*

(iii) (multiple $\mathbf{DS}(\mathbb{K})$) *"Given a family $(E_i)_{i\in I}$ of $\mathbb{K}$-vector spaces, a family $(F_i)_{i\in I}$ such that each a_i is a non null element of E_i, there exists a family $(f_i)_{i\in I}$ such that each $f_i : E_i \to \mathbb{K}$ is a linear form and $f_i(a_i) = 1$."*

(iv) $\mathbf{DS}(\mathbb{K})$.

Proof: (i) ⇒ (ii). Let $(E_i, F_i, f_i)_{i\in I}$ be a family such that each E_i is a $\mathbb{K}$-vector space, F_i a vector subspace of E_i and $f_i : F_i \to \mathbb{R}$ is a linear form. Then $F = \oplus_{i\in I} F_i$ is a vector subspace of $E = \oplus_{i\in I} E_i$, and the mapping $f = \oplus_{i\in I} f_i : F \to \mathbb{K}$ is linear. Using $\mathbf{DE}(\mathbb{K})$, extend f by a linear mapping $\tilde{f} : E \to \mathbb{K}$. For each $i \in I$, let $\tilde{f}_i := \tilde{f} \circ can_i$ where $can_i : E_i \hookrightarrow E$ is the canonical mapping. Then each mapping $\tilde{f}_i : E_i \to \mathbb{K}$ is linear and extends f_i.

(ii) ⇒ (iii) ⇒ (iv) is easy.

(iv) ⇒ (i). Let E be a $\mathbb{K}$-vector space, let F be a vector subspace of E, let $f : F \to \mathbb{K}$ be a linear mapping. Let $N := \mathrm{Ker}(f)$ and let $a \in F$ such that $f(a) = 1$. Let $can : E \to E/N$ be the canonical mapping and let $b := can(a) = a + N$. Using $\mathbf{DS}(\mathbb{K})$, let $g : E/N \to \mathbb{K}$ be a linear mapping such that $g(b) = 1$. Let $\tilde{f} := g \circ can : E \to \mathbb{K}$. Then $\tilde{f}$ is linear, $\tilde{f}$ is null on N and $\tilde{f}(a) = 1$, thus $\tilde{f}$ extends f. □

2 *Remark.* Given a real normed space E, denote by $\mathbf{DS}_E$ (resp. $\mathbf{DE}_E$) the statement $\mathbf{DS}(\mathbb{R})$ (resp. $\mathbf{DE}(\mathbb{R})$) restricted to the case of the vector space E. Then, for $E := L^2[0,1]$, $\mathbf{DS}_E$ holds in $\mathbf{ZF}$, however, there are models of $\mathbf{ZF}$ where $\mathbf{DE}_E$ does not hold.

Proof: Recall that $E := L^2[0,1]$ is the Cauchy-completion of the normed space $C([0,1])$ endowed with the N_2 norm. Thus E is a (separable) Hilbert space so $\mathbf{DS}_E$

is satisfied (for example, given $a \in E\backslash\{0\}$, consider the "scalar product" form $x \mapsto \langle x, a\rangle$). Now, consider the "evaluating form" $\delta_0 : C([0,1]) \to \mathbb{R}$ associating to each $f \in C([0,1])$ the real number $f(0)$: δ_0 is linear. However, there are models of **ZF** in which δ_0 has no linear extension to the whole space E (thus $\mathbf{DE}_E$ is not satisfied). Indeed, consider a model $\mathfrak{M}$ of **ZF** in which every linear form on a separable Banach space is continuous (for example, consider models of **ZF** in which every subset of a polish space is a Baire set — see [17], [16], [15]). In such a model $\mathfrak{M}$, if $\phi : E \to \mathbb{R}$ is a linear mapping extending δ_0, then ϕ is non null and $\mathrm{Ker}(\phi)$ is dense in E (because $\mathrm{Ker}(\delta_0)$ is already dense in $L^2[0,1]$), thus the linear form $\phi : E \to \mathbb{R}$ is not continuous: this is contradictory in $\mathfrak{M}$! □

3.2 Linear extenders. Given a commutative field $\mathbb{K}$, and a vector space E, we denote by E^* the *algebraic dual* of E i.e. the vector space of $\mathbb{K}$-linear forms on E. Consider the following statement:

> $\mathbf{LE}(\mathbb{K})$ (Linear extender): *For every $\mathbb{K}$-vector space E, and every vector subspace F of E, there exists a linear mapping $T : F^* \to E^*$ such that for each $f \in F^*$, $T(f)$ extends f.*

Denoting by *can* $: E^* \to F^*$ the linear mapping associating to each $f \in E^*$ its restriction $f_{\restriction F}$ to F, the axiom $\mathbf{LE}(\mathbb{K})$ says that *can* $: E^* \to F^*$ is onto and has a linear section $T : F^* \hookrightarrow E^*$.

4 Proposition. $\mathbf{B}(\mathbb{K}) \Rightarrow \mathbf{LE}(\mathbb{K}) \Rightarrow \mathbf{DS}(\mathbb{K})$.

Proof: We prove $\mathbf{B}(\mathbb{K}) \Rightarrow \mathbf{LE}(\mathbb{K})$. Given a vector space E and a vector subspace F of E, the axiom $\mathbf{B}(\mathbb{K})$ implies the existence of a basis B of the dual space F^*. Using the multiple form of $\mathbf{DS}(\mathbb{K})$, consider for each $e \in B$, a linear form $\tilde{e} : E \to \mathbb{K}$ extending e. Let $T : F^* \to E^*$ be the linear mapping such that for each $e \in B$, $T(e) = \tilde{e}$. Then T is a linear section of *can* $: E^* \to F^*$. □

3.3 $\mathbf{D}(\mathbb{Z}_2)$ restricted to boolean algebras.

3.3.1 Boolean algebras. A *boolean algebra* is a (commutative) ring with a unit $(\mathbb{B}, \oplus, ., 0, 1)$, such that for every $x \in \mathbb{B}$, $x \oplus x = 0$. The proof of the following result is classical in **ZFC**, set-theory with the Axiom of Choice. However, this result is also provable in **ZF** (see [9] or [14]).

Theorem (Coproduct of boolean algebras in **ZF**). *Given a family $(\mathcal{B}_i)_{i\in I}$ of boolean algebras, there exists a boolean algebra $\mathcal{B}$ and a family $(j_i : \mathcal{B}_i \to \mathcal{B})_{i\in I}$ of morphisms of boolean algebras (thus for every $i \in I$, $j_i(1_{\mathcal{B}_i}) = 1_{\mathcal{B}}$) such that for every boolean algebra $\mathcal{C}$, and every family $(g_i : \mathcal{B}_i \to \mathcal{C})_{i\in I}$ of morphisms, there exists a unique morphism $g : \mathcal{B} \to \mathcal{C}$ satisfying $g \circ j_i = g_i$.*

Proof: We sketch the proof which is in [14]. The case where every boolean algebra $\mathcal{B}_i$ is equal to $\mathcal{P}(\mathbb{N})$ is easy. The general case follows from the fact that every boolean algebra is a sub-algebra of a reduced power of $\mathcal{P}(\mathbb{N})$ (using methods described by Luxemburg [12]). □

3.3.2 A boolean consequence of $\mathbf{D}(\mathbb{Z}_2)$. Every boolean algebra $\mathbb{B}$ is a vector space over $\mathbb{Z}_2$. Notice that a $\mathbb{Z}_2$-linear form on $\mathbb{B}$ is just a mapping $f : \mathbb{B} \to \mathbb{Z}_2$ which is *additive*: for every $x, y \in \mathbb{B}$, $f(x \oplus y) = f(x) + f(y)$. The following statement is a consequence of $\mathbf{D}(\mathbb{Z}_2)$:

> $\mathbf{D}_{bool}(\mathbb{Z}_2)$: *"Given a non-trivial boolean algebra $\mathcal{B}$, there exists a non null linear mapping $f : \mathcal{B} \to \mathbb{Z}_2$."*

3 Theorem. *The following statements are equivalent to $\mathbf{D}_{bool}(\mathbb{Z}_2)$.*

(i) *"For every boolean algebra $\mathcal{B}$ and every $a \in \mathcal{B}$ such that $a \neq 0$, there exists a linear mapping $f : \mathcal{B} \to \mathbb{Z}_2$ such that $f(a) = 1$."*

(ii) *The "multiple form": "If $(\mathcal{B}_i)_{i\in I}$ is a family of non-null boolean algebras, there exists a family $(f_i)_{i\in I}$ such that for every $i \in I$, $f_i : \mathcal{B}_i \to \mathbb{Z}_2$ is linear and $f_i(1_{\mathcal{B}_i}) = 1$".*

(iii) *"If $(\mathcal{B}_i, a_i)_{i\in I}$ is a family of boolean algebras, and if each $a_i \in \mathcal{B}_i \backslash \{0\}$, then there exists a family $(f_i)_{i\in I}$ such that for every $i \in I$, $f_i : \mathcal{B}_i \to \mathbb{Z}_2$ is linear and $f_i(a_i) = 1$."*

(iv) $\mathbf{D}(\mathbb{Z}_2)$.

PROOF: $\mathbf{D}_{bool}(\mathbb{Z}_2) \Rightarrow$ (i). For every element $u \in \mathcal{B}$, let $\mathcal{B}_u := \{x \in \mathcal{B} : x \leq u\}$: $\mathcal{B}_u$ is a boolean algebra. Using $\mathbf{D}_{bool}(\mathbb{Z}_2)$, let $g : \mathcal{B}_a \to \mathbb{Z}_2$ be a non-null linear mapping. Let $b \in \mathcal{B}_a$ such that $g(b) = 1$. Let $r : \mathcal{B} \to \mathcal{B}_b$ be the mapping $x \mapsto (x \wedge b)$: then r is linear and $r(a) = b$. Let $f := g \circ r$. Then $f : \mathcal{B} \to \mathbb{Z}_2$ is linear and $f(a) = 1$.

(i) $\Rightarrow$ (ii). Let $(\mathcal{B}_i)_{i\in I}$ be a family of boolean algebras. Let $(\mathcal{B}, (j_i)_{i\in I})$ be the *boolean coproduct* of the family $(\mathcal{B}_i)_{i\in I}$. Using (i), let $f : \mathcal{B} \to \mathbb{Z}_2$ be a linear mapping such that $f(1_{\mathcal{B}}) = 1$. For each $i \in I$, let $f_i := f \circ j_i$. Then each $f_i : \mathcal{B}_i \to \mathbb{Z}_2$ is linear and $f_i(1) = 1$.

(ii)$\Rightarrow$ (iii). For each $i \in I$, consider the boolean algebra $\mathcal{B}'_i := \{x \in \mathcal{B}_i : x \leq a_i\}$. Apply (ii) to the family of boolean algebras $(\mathcal{B}'_i)_{i\in I}$.

(iii) $\Rightarrow \mathbf{D}_{bool}(\mathbb{Z}_2)$: easy.

(i) $\Rightarrow \mathbf{D}(\mathbb{Z}_2)$. Let E be a $\mathbb{Z}_2$-vector space. Using results of Section 2.1, there exist a set I, a filter $\mathcal{F}$ on I and a one-to-one mapping $j : E \to (\mathbb{Z}_2)_{\mathcal{F}}$ which is $\mathbb{Z}_2$-linear. Now $(\mathbb{Z}_2)_{\mathcal{F}}$ is a boolean algebra (because, on the language $\mathbb{L}_{ring} := \{+, \times, \mathbf{0}, \mathbf{1}\}$ of rings, the axioms defining boolean algebras are atomic formulae). Using (i), let $f : (\mathbb{Z}_2)_{\mathcal{F}} \to \mathbb{Z}_2$ be a linear mapping which is not null on $j[E]$. Then $f \circ j : E \to \mathbb{K}$ is linear and non null.

$\mathbf{D}(\mathbb{Z}_2) \Rightarrow \mathbf{D}_{bool}(\mathbb{Z}_2)$: easy. □

2 Corollary. $\mathbf{D}_{bool}(\mathbb{Z}_2) \Rightarrow \mathbf{C}(2)$.

PROOF: Let $(A_i)_{i\in I}$ be a family of non-empty finite sets. The multiple form of $\mathbf{D}_{bool}(\mathbb{Z}_2)$ gives a family $(f_i)_{i\in I}$ such that for each $i \in I$, $f_i : \mathcal{P}(A_i) \to \mathbb{Z}_2$ is $\mathbb{Z}_2$-linear and $f_i(A_i) = 1$. Now, for each $i \in I$, let $B_i := \{t \in A_i : f_i(\{t\}) = 1\}$. Then the cardinal $|B_i|$ of B_i is odd because $f_i(A_i) = |B_i| \; mod \; 2$. □

4. $\mathbf{D}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$

3 Corollary. *For every prime number p, $\mathbf{D}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$.*

Proof: Given a prime number p, denote by $\mathbb{K}$ the field $\mathbb{Z}_p$. Let $(A_i)_{i\in I}$ be a family of non-empty finite sets. For every $i \in I$, let E_i be the $\mathbb{K}$-vector space $\mathbb{K}^{A_i}$ and let $1_{A_i} : A_i \to \mathbb{K}$ be the constant mapping with value 1. Using the multiple form of $\mathbf{DS}(\mathbb{Z}_p)$ (which is equivalent to $\mathbf{D}(\mathbb{Z}_p)$), consider some family $(f_i)_{i\in I}$ such that for every $i \in I$, $f_i : E_i \to \mathbb{K}$ is linear and $f_i(1_{A_i}) = 1$. Then $f_i(1_{A_i}) = \sum_{t\in\{0..p-1\}} t|F_i(t)|$, where for every $i \in I$, and every $t \in \{0..p-1\}$, $F_i(t) := \{x \in A_i : f_i(x) = t\}$. If $i \in I$, then p does not divide $1 = f_i(1_{A_i})$; thus there exists $t \in \{0..p-1\}$ such that $|F_i(t)|$ is not multiple of p; let t_i be the first such element of $\{0..p-1\}$; then $F_i := F_i(t_i)$ is a subset of A_i and p does not divide $|F_i|$. □

3 *Remark.* Let N be an integer ≥ 2. Let P_N be the set of prime numbers p such that $2 \leq p \leq N$. Then the statement $\wedge_{p\in P_N}\mathbf{C}(p)$ implies that for every set $\mathcal{A}$ of non-empty finite sets, there exists a mapping Φ with domain $\mathcal{A}$ such that for every $F \in \mathcal{A}$, $\varnothing \neq \Phi(F) \subseteq F$ and, for every $p \in F_N$, p does not divide the cardinal of F.

Proof: Let X be an infinite set. Let $\mathcal{A}$ be the set of non-empty finite subsets of X. Using the statement $\wedge_{p\in P_N}\mathbf{C}(p)$, consider for each $p \in P_N$, a mapping $\Phi_p : \mathcal{A} \to \mathcal{A}$ associating to each $F \in \mathcal{A}$ a non-empty finite subset G of F such that p does not divide the cardinal of G. Now, given $F \in \mathcal{A}$ with cardinal n, we define a descending sequence $(F_i)_{0\leq i<n}$ of non-empty subsets of F such that $F_0 = F$ and, for every $i \in 0..|F|$, if some $p \in P_N$ divides $|F_i|$, then $F_{i+1} \subsetneq F_i$, else $F_{i+1} = F_i$: then F_{n-1} is a non-empty finite subset of F such that no element of P_N divides the cardinal of F_n. We define Φ as the mapping associating to each $F \in \mathcal{A}$ with n elements the non-empty finite subset F_{n-1} of F. □

4 *Remark.* Let N be an integer ≥ 2. Then the statement $\wedge_{2\leq p\leq N;\ p \text{ prime}}\mathbf{C}(p)$ implies the statement $\mathbf{AC}^N$.

Proof: Use the previous remark. □

5. $\mathbf{D}(\mathbb{Q})$ implies $\mathbf{AC}^{\mathbb{Z}}$

Given an infinite set X, we denote by $\mathcal{P}_\infty(X)$ the set of infinite subsets of X; we also denote by fin_X the set of finite subsets of X. In [13], chameleons and cyclic chameleons were defined: given some integer $n \geq 2$, a *n-cyclic chameleon* is a mapping $\chi : \mathcal{P}_\infty(X) \to \mathbb{Z}_n$ such that for every infinite subset A of X and every $m \in X\backslash A$, $\chi(A \cup \{m\}) = \chi(A) + 1$ *mod* n. We define a *$\mathbb{Z}$-chameleon* on X as a mapping $\chi : \mathcal{P}_\infty(X) \to \mathbb{Z}$ such that for every infinite subset A of X and every $m \in X\backslash A$, $\chi(A \cup \{m\}) = \chi(A) + 1$. Consider the following statements:

> $\mathbf{C}\mathbb{Z}$: *"On every infinite set there exists a $\mathbb{Z}$-chameleon."*

and, for every integer $n \geq 2$:

$\mathbf{C}\mathbb{Z}_n$: *"On every infinite set there exists a cyclic n-chameleon."*

Notice that for every integer $n \geq 2$, $\mathbf{C}\mathbb{Z}$ implies $\mathbf{C}\mathbb{Z}_n$.

4 Theorem. $\mathbf{D}(\mathbb{Q}) \Rightarrow \mathbf{C}\mathbb{Z}$.

Proof: Let E be the $\mathbb{Q}$-vector space $\mathbb{Q}^X$. We identify the set $\mathcal{P}(X)$ of subsets of X with the set $\{0,1\}^X$. Then we may think of $\mathcal{P}(X)$ as a subset of E. Using $\mathbf{D}(\mathbb{Q})$ (or rather the equivalent statement $\mathbf{DE}(\mathbb{Q})$ in Theorem 2 of Section 3.1), let $f : E \to \mathbb{Q}$ be a $\mathbb{Q}$-linear form such that for every $x \in X$, $f(\{x\}) = 1$. For every $C \in \mathcal{P}(X)/\mathrm{fin}_X$ such that $C \neq 0$, the subset $f[C]$ of $\mathbb{Q}$ is order isomorphic with $\mathbb{Z}$, and one can choose some $\mu_C \in f[C]$ (for example let μ_C be the first element of $f[C] \cap \mathbb{Q}_+^*$ where $\mathbb{Q}_+^* := \{q \in \mathbb{Q} : 0 < q\}$); let $d_C : f[C] \to \mathbb{Z}$ be the order isomorphism such that $d_C(\mu_C) = 0$, and let $f_C := d_C \circ f_{\restriction C} : C \to \mathbb{Z}$. Let $\chi := \bigcup_{C \in \mathcal{P}(X)/\,\mathrm{fin}, C \neq 0} f_C$. Then χ is a $\mathbb{Z}$-chameleon on X. □

5 *Remark.* For every prime number p, $\mathbf{D}(\mathbb{Z}_p) \Rightarrow \mathbf{C}\mathbb{Z}_p$.

Proof: The proof is similar but slightly simpler. □

5 Proposition. *The axiom $\mathbf{C}\mathbb{Z}$ is equivalent to the following statement $\mathbf{AC}^{\mathbb{Z}}$: "For every family $(X_i, \leq_i)_{i \in I}$ of ordered sets isomorphic with $\mathbb{Z}$, the product set $\prod_{i \in I} X_i$ is non-empty."*

Proof: $\Rightarrow$ Let $(X_i, \leq_i)_{i \in I}$ be a non-empty family of ordered sets isomorphic with $\mathbb{Z}$. We may assume that the sets X_i are pairwise disjoint. Let $X := \bigcup_{i \in I} X_i$. Using $\mathbf{C}\mathbb{Z}$, let $\chi : \mathcal{P}_\infty(X) \to \mathbb{Z}$ be a $\mathbb{Z}$-chameleon. For each $i \in I$, there exists a unique $x_i \in X_i$ such that $\chi(\leftarrow, x_i]) = 0$ — here, we denote by $\leftarrow, x_i]$ the interval $\{t \in X_i : t \leq x_i\}$ of the ordered set X_i. Now $x = (x_i)_{i \in I} \in \prod_{i \in I} X_i$.

$\Leftarrow$ Let X be an infinite set. In order to define a $\mathbb{Z}$-chameleon on X, it is sufficient (and also necessary) to define a $\mathbb{Z}$-chameleon on every non null class $C \in \mathcal{P}_\infty(X)/\mathrm{fin}_X$. Given such a class C, the *poset* P_C of $\mathbb{Z}$-chameleons on C ordered by the product order of $\mathbb{Z}^C$ is isomorphic with $\mathbb{Z}$. Using $\mathbf{AC}^{\mathbb{Z}}$, consider some element $(\chi_C)_{0 \neq C \in P_\infty(X)/\mathrm{fin}_X} \in \prod_{C \in \mathcal{P}_\infty(X)/\mathrm{fin}_X, C \neq 0} P_C$; then $\chi := \bigcup \chi_C : \mathcal{P}_\infty(X) \to \mathbb{Z}$ is a $\mathbb{Z}$-chameleon on X. □

6 Proposition. $\mathbf{AC}^{\mathbb{Z}}$ *does not imply* $\mathbf{AC}$.

Proof: There is a model of $\mathbf{ZF}+\neg\mathbf{AC}$ where every family of non-empty well-orderable sets has a non-empty product (see [8], [7]). Such a model satisfies $\mathbf{AC}^{\mathbb{Z}}$. □

References

[1] Blass A., *Existence of bases implies the axiom of choice*, in Axiomatic Set Theory (Boulder, Colo., 1983), Contemp. Math., 31, pp. 31–33, American Mathematical Society, Providence, RI, 1984.

[2] Delhommé C., Morillon M., *Spanning graphs and the axiom of choice*, Rep. Math. Logic **40** (2006), 165–180.

[3] Halpern J.D., *Bases in vector spaces and the axiom of choice*, Proc. Amer. Math. Soc. **17** (1966), 670–673.
[4] Hodges W., *Model Theory*, Encyclopedia of Mathematics and its Applications, 42, Cambridge University Press, Cambridge, 1993.
[5] Höft H., Howard P., *A graph theoretic equivalent to the axiom of choice*, Z. Math. Logik Grundlagen Math. **19** (1973), 191.
[6] Howard P., *Bases, spanning sets, and the axiom of choice*, MLQ Math. Log. Q. **53** (2007), no. 3, 247–254.
[7] Howard P., Rubin J.E., *Consequences of the Axiom of Choice*, Mathematical Surveys and Monographs, 59, American Mathematical Society, Providence, RI, 1998.
[8] Jech T.J., *The Axiom of Choice*, North-Holland Publishing Co., Amsterdam, 1973.
[9] Jurie P.-F., *Coproduits Booléiens* (*Théorie générale et application à la théorie des anneaux booléiens monadiques*), PhD Thesis, University of Clermont-Ferrand, 1965.
[10] Keremedis K., *Bases for vector spaces over the two-element field and the axiom of choice*, Proc. Amer. Math. Soc. **124** (1996), no. 8, 2527–2531.
[11] Keremedis K., *The vector space Kinna-Wagner principle is equivalent to the axiom of choice*, MLQ Math. Log. Q. **47** (2001), no. 2, 205–210.
[12] Luxemburg W., *Reduced powers of the real number system and equivalents of the Hahn-Banach extension theorem*, Applications of Model Theory to Algebra, Analysis and Probability (Internat. Sympos., Pasadena, Calif., 1967), Holt, Rinehart and Winston, New York, 1969, pp. 123–137.
[13] Mathias A., *A note on chameleons*, preprint.
[14] Morillon M., *Algèbres de Boole mesurées et axiome du choix*, in Séminaire d'Analyse, 5, (Clermont-Ferrand, 1989–1990), Exp. No. 15, Univ. Clermont-Ferrand II, Clermont, 1993.
[15] Shelah S., *Can you take Solovay's inaccessible away?*, Israel J. Math. **48** (1984), no. 1, 1–47.
[16] Solovay R.M., *A model of set-theory in which every set of reals is Lebesgue measurable*, Ann. of Math. (2) **92** (1970), 1–56.
[17] Wright J.D.M., *All operators on a Hilbert space are bounded*, Bull. Amer. Math. Soc. **79** (1973), 1247–1250.

ERMIT, Département de Mathématiques et Informatique, Université de La Réunion, Parc Technologique Universitaire, Bâtiment 2, 2 rue Joseph Wetzell, 97490 Sainte-Clotilde, France

Email: mar@univ-reunion.fr

URL: `http://personnel.univ-reunion.fr/mar`

(*Received* November 20, 2008, *revised* April 2, 2009)