BULL. AUSTRAL. MATH. SOC.
VOL. 8 (1973), 221-232.

02E99, 12L99, 12D99

Axioms for constructive fields

John Staples

In constructive mathematics the Dedekind cut definition of real number is not equivalent to the definition of real number by Cauchy sequences, and the Dedekind real numbers do not satisfy Heyting's axioms for constructive fields. A more general notion of constructive field is proposed which includes the Dedekind real numbers; some linear algebra is given which applies to such fields.

1. Introduction

It was observed in [4] that Heyting's axioms for constructive fields as given in [2] cannot be satisfied by the Dedekind real numbers. Heyting defines a field K to be a commutative ring with unity on which an *apartness* relation, $\#$, is defined between field elements, which satisfies the following axioms: for all $a, b, c \in K$,

(i) $a \# b$, $a = b$ are mutually exclusive,

(ii) $a \# b$ implies for all c that $a \# c$ or $b \# c$,

(iii) not $(a \# b)$ implies $a = b$,

(iv) $b \# c$ implies $a + b \# a + c$,

(v) $1 \# 0$,

(vi) $a \# 0$ implies there is b such that $ab = 1$,

(vii) $b \# c$, $a \# 0$ implies $ab \# ac$.

The following are consequences of the above;

(viii) $ab \# 0$ implies $a \# 0$ and $b \# 0$,

Received 10 November 1972.

(ix) $a \# b$ if and only if $b \# a$.

Heyting's motivation, [2, p. 5], for the introduction of this new primitive relation is that $a \# 0$ provides a sufficient condition for the existence of an inverse for a . Since however the condition is also necessary (from (ii) and (viii)) the reason for its introduction must be sought elsewhere.

Inspection of the theory which Heyting develops shows that it relies heavily on axiom (ii) and on the (equivalent) property: $a + b \# 0$ implies $a \# 0$ or $b \# 0$. It is fair to say that the introduction of such an apartness relation has three purposes:

(a) it ensures *stability* of equality, that is

$$\text{not}(\text{not } x = y) \text{ implies } x = y \ ;$$

(b) it ensures that zero is the only non-invertible element;

(c) it provides a means for writing axiom (ii) neatly.

To see that these are its only functions, suppose that K is a commutative ring with unity and stable equality which satisfies the axiom

(x) $x \neq 0$ implies not(for all y, $xy \neq 1$) .

Define $x \# y$ to mean

$$\text{there is } z \text{ such that } (x-y)z = 1 \ ;$$

then all except (ii) of axioms (i) to (ix) are satisfied.

Hence we adopt the following definition; a field is a commutative ring with unity which satisfies axiom (x). If it also has a stable equality then we call it a stable field. Apartness is equivalent to the negation of equality for fields with decidable equality; the same is true for the following field (classically equivalent to the real numbers) even though its equality relation is not decidable.

Define a set K to have as elements all subsets s of the set of Dedekind real numbers which satisfy the conditions

(a) $s \neq \emptyset$, and not(not $x \in s$) implies $x \in s$,

(b) $a, b \in s$ implies $a = b$.

Addition of elements of K is defined by

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$$s_1 + s_2 = \{t : t_1 \in s_1 \text{ and } t_2 \in s_2 \text{ implies } t = t_1 + t_2\} .$$

Similarly the additive inverse of s and the product of s_1 and s_2 are defined by

$$-s = \{t : u \in s \text{ implies } t = -u\}$$

and

$$s_1 \cdot s_2 = \{t : t_1 \in s_1 \text{ and } t_2 \in s_2 \text{ implies } t = t_1 \cdot t_2\} .$$

The unity 1_K and zero 0_K of K are defined to be $\{1\}$ and $\{0\}$ respectively, and equality on K is the usual equality of sets. One can check, using the stability of equality for Dedekind reals, that with these definitions K forms a field.

For $s \in K$ we define a set s^* by

$$s^* = \{t : u \in s \text{ implies } tu = 1\} .$$

If $s \neq 0$ then $s^* \in K$ and $ss^* = 1$; thus K is a stable field in which apartness is equivalent to inequality.

2. Matrices and determinants

It is simple to check the usual ring-theoretic properties of matrices over a field; that is, that matrices of a given size form an additive group, and multiplication of compatible matrices is associative and distributive.

Likewise the elementary properties of determinants can be verified by direct computation, as for example in the first chapter of Mirsky [3] (his method of proving the alternating property does not apply to fields in general but the result follows by direct computation from the definition of determinant). We shall not list or prove these results but will use them as necessary: a basic result is that any square matrix A with $\det(A) \# 0$ has an inverse, computed by the usual formula.

3. Linear algebra

In Heyting's development, [2], vectors are n-tuples of scalar coordinates for some natural number n , and apartness of vectors is a central notion which is defined in terms of the coordinates. We shall

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

treat vectors axiomatically and do not need to define apartness for vectors.

As in Bishop, [1, p. 244], a vector space is an abelian group with a scalar multiplication by field elements which satisfies the usual axioms. An arbitrary field K of scalars is fixed throughout.

A subspace S of a vector space V is a subset of V which is closed under addition and scalar multiplication. The span of a finite sequence $x_1, \ldots, x_k$ of vectors in a space V is the set of vectors of V of the form

$$\sum_{i=1}^{k} \alpha_i x_i ,$$

where $\alpha_i \in K$, $i = 1, \ldots, k$. An element of this span is said to be (linearly) dependent on $x_1, \ldots, x_k$.

A finite sequence $x_1, \ldots, x_k$ of vectors in V is called *mutually free* (in V) if there is a k-linear alternating function d from V^k to K such that

$$d(x_1, \ldots, x_k) = 1 .$$

A limitation of this definition should be noted. If vectors which are mutually free in a subspace S of an arbitrary vector space V are necessarily free in V, then Markov's principle holds. To see this we take Markov's principle in the following equivalent form:

for all Cauchy real numbers x, $x \neq 0$ implies $x \# 0$.

For an arbitrary Cauchy real $x \neq 0$, x is mutually free in the span of x, since for any $y = \alpha x$, α a Cauchy real, α is uniquely determined by y and so we can define a linear map d by $d(y) = \alpha$. If x is free in the Cauchy reals then $d'(1)$ is defined for some linear function d' on the Cauchy reals such that $d'(x) = 1$.

Hence $1 = d'(x) = d'(x.1) = x.d'(1)$; so x is invertible, that is, $x \# 0$ as required.

A *basis* of a subspace S of a vector space V is defined to be a finite sequence $x_1, \ldots, x_k$ of elements of S, mutually free in V,

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

whose span is S. Such a basis is also called a basis *in* V of S. If $S \subseteq W \subseteq V$ are vector spaces then a basis in V of S is a basis in W of S. A basis in V of V is called simply a basis of V.

PROPOSITION 1. *Any two bases for a vector space V have the same number of elements.*

Proof. If V has bases $x_1, \ldots, x_k$ and $y_1, \ldots, y_m$, $k, m \geq 1$, we get a contradiction as follows from the assumption $k < m$.

Write d_y for an alternating m-linear function such that $d_y(y_1, \ldots, y_m) = 1$, and suppose $y_i = \sum_{j=1}^{k} \eta_{i,j} x_j$, $i = 1, \ldots, m$. We substitute for y_i, $i = 1, \ldots, m$ and expand by the m-linearity of d_y to obtain from $d_y(y_1, \ldots, y_m)$ a sum of scalar multiples of scalars of the form $d_y\left(x_{p_1}, \ldots, x_{p_m}\right)$. Since $k < m$ at least two p_i, $i = 1, \ldots, m$ are identical so $d_y\left(x_{p_1}, \ldots, x_{p_m}\right) = 0$, so $0 = d_y(y_1, \ldots, y_m) = 1$, a contradiction as required.

It follows from Proposition 1 that any two bases for a subspace of V have the same number of elements. Hence if a subspace S of V has a basis of k elements we say that S has dimension k.

PROPOSITION 2. *Any k vectors of a k-dimensional subspace S of V which are mutually free in V form a basis in V of S.*

Proof. If $x_1, \ldots, x_k \in S$ are mutually free in V, we have only to prove that S is the span of $x_1, \ldots, x_k$ so we may assume $V = S$.

Suppose then that $y_1, \ldots, y_k$ is a basis of S and that d_x is an k-linear alternating function such that

$$d_x(x_1, \ldots, x_k) = 1 .$$

We can write $x_i = \sum_{j=1}^{k} \chi_{ij} y_j$, $i = 1, \ldots, k$ and substitute in d_x to obtain

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$$1 = \Delta . d_x(y_1, \ldots, y_k) ,$$

where Δ is the determinant of the coordinates of $x_1, \ldots, x_k$ with respect to $y_1, \ldots, y_k$. Hence Δ is invertible, so the matrix of coefficients of $x_1, \ldots, x_k$ is invertible and $y_1, \ldots, y_k$ can therefore be expressed as linear combinations of $x_1, \ldots, x_k$, giving the result required.

An $m \times n$ matrix A of field elements has columns which can be regarded as elements of K^m; we say A has (column) *rank* r if r of these columns are mutually free in K^m and all other columns are dependent on them.

PROPOSITION 3. *If the $m \times n$ matrix A has rank r then the solutions of the homogeneous equation $Ax = 0$ form a finite-dimensional subspace of K^n of dimension $n - r$, with a basis $x_{r+1}, \ldots, x_n$ which can be extended to a basis $x_1, \ldots, x_n$ for K^n such that $Ax_1, \ldots, Ax_r$ is a basis in K^m for the space*

$$\{y : \text{there is } x \in K^n \text{ such that } y = Ax\} .$$

Proof. The case $r = n$ is trivial from the definition of rank, since if $A = (a_1, \ldots, a_n)$ and $\sum_{i=1}^{n} a_i \chi_i = 0$ and d is an n-linear alternating function on K^m such that $d(a_1, \ldots, a_n) = 1$, then

$$\chi_i = d\Big(a_1, \ldots, a_{i-1}, \sum_{i=1}^{n} a_j \chi_j, a_{i+1}, \ldots, a_n\Big) =$$

$$= d(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = 0 .$$

Hence in this case we can take the canonical basis of K^n as $x_1, \ldots, x_n$.

Now consider the case $r < n$. We can assume without loss of generality that $a_1, \ldots, a_r$ are mutually free in K^m and that

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$a_i = \sum_{j=1}^{r} \alpha_{ij} a_j$, $i = r+1, \ldots, n$. Write $\chi_1, \ldots, \chi_n$ for the coordinates of x . Note that $Ax = 0$ if and only if

$$\sum_{j=1}^{r} \chi_j a_j = - \sum_{i=r+1}^{n} \chi_i a_i = - \sum_{i=r+1}^{n} \chi_i \sum_{j=1}^{n} \alpha_{ij} a_j ,$$

so $Ax = 0$ if and only if

$$\chi_j = - \sum_{i=r+1}^{n} \alpha_{ij} \chi_i , \quad j = 1, \ldots, r .$$

The $n - r$ solutions $x^{(j)}$ given by

$$\chi_i^{(j)} = \delta_{i,j} , \quad n-r+1 \leq i, j \leq n$$

are mutually free in K^n since they can be extended to n vectors with determinant of coefficients equal to 1 by

$$\chi_i^{(j)} = \delta_{i,j} , \quad 1 \leq j \leq n-r , \quad 1 \leq i \leq n .$$

It is clear from the above that $x^{(j)}$, $n-r+1 \leq j \leq n$, span the space of solutions, and that $a_i = Ax^{(i)}$, $i = 1, \ldots, r$, are mutually free in K^m and span the range of A as required.

To conclude our discussion of linear equations we observe that, as classically, the general solution of the nonhomogeneous equation $Ax = b$ is obtained by adding to a fixed solution an arbitrary solution of $Ax = 0$. Hence we give conditions that $Ax = b$ have a solution. Writing $A = (a_1, \ldots, a_n)$ again, clearly the existence of a solution is equivalent to the dependence of b on $a_1, \ldots, a_n$, so

PROPOSITION 4. *If the ranks of* $(a_1, \ldots, a_n)$, $(a_1, \ldots, a_n, b)$ *are defined and equal then* $(a_1, \ldots, a_n)x = b$ *has a solution. Conversely if the rank,* r *say, of* $(a_1, \ldots, a_n)$ *is defined and* $(a_1, \ldots, a_n)x = b$ *has a solution then the rank of* $(a_1, \ldots, a_n, b)$ *is defined and equals* r .

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

Proof. If both ranks are defined and equal r, we may suppose that $a_1, \ldots, a_r$ are free in K^m; hence they are free in the r-dimensional space spanned by $a_1, \ldots, a_n, b$, so $a_1, \ldots, a_r$ form a basis of this space, hence b is dependent on them as required.

If conversely $(a_1, \ldots, a_n)$ has rank r, and supposing again that $a_1, \ldots, a_r$ are free in K^m, since $(a_1, \ldots, a_n)x = b$ has a solution b is dependent on $a_1, \ldots, a_n$, hence on $a_1, \ldots, a_r$ and $(a_1, \ldots, a_n, b)$ has rank r as required.

We now consider briefly linear maps on vector spaces; a linear map $f : V \to W$ is by definition an isomorphism if it has an inverse, and an injection if $f(x) = f(y)$ implies $x = y$.

PROPOSITION 5. *The image under an isomorphism $f : V \to W$ of a basis of V is a basis of W.*

Proof. Since f is onto, $f(x_1), \ldots, f(x_n)$ spans W if $x_1, \ldots, x_n$ spans V. If $x_1, \ldots, x_n$ are a basis for V they are also mutually free, so every $y \in W$ has a unique expression in the form $y = \sum_{i=1}^{n} \eta_i f(x_i)$, for if also $y = \sum_{i=1}^{n} \xi_i f(x_i)$, then

$$0 = \sum_{i=1}^{n} (\eta_i - \xi_i) f(x_i) = f\left(\sum_{i=1}^{n} (\eta_i - \xi_i) x_i \right),$$

so $0 = \sum_{i=1}^{n} (\eta_i - \xi_i) x_i$, since f is an injection. Since $x_1, \ldots, x_n$ are mutually free, $\eta_i = \xi_i$, $i = 1, \ldots, n$ as required.

Hence an n-linear alternating function d_W from W^n to K is defined by $d_W(f(x_1), \ldots, f(x_n)) = 1$, so $f(x_1), \ldots, f(x_n)$ form a basis of W as required.

The *rank* of a linear map $f : V \to W$ is defined to be the number (if one exists) n such that V has a basis $v_1, \ldots, v_n$ such that

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$f(v_1)$, ..., $f(v_r)$ are free in W and form a basis for the range of f. Any such number r is unique since it is the dimension of the range of f, so rank is well-defined.

PROPOSITION 6. *If W is a finite-dimensional vector space then the linear map $f : V \to W$ has rank r if and only if there are bases of V and W such that the matrix of f with respect to these bases has rank r.*

The proof is immediate from the definitions. From Proposition 3 we therefore have

COROLLARY. *If W is finite-dimensional then the linear map $f : V \to W$ has rank r if and only if the nullspace of f has dimension $n - r$ (where n is the dimension of V) and has a basis which can be extended to a basis of V.*

The statements of Propositions 3 and 6 hint at a difficulty which we have managed to avoid above; it is not clear in general how mutually free vectors in a finite-dimensional vector space can be extended to a basis of that space. In one simple case however, this can always be done:

PROPOSITION 7. *If x_1, ..., x_{k-1} are mutually free vectors in a k-dimensional space V, then there is a vector x_k in V such that x_1, ..., x_k form a basis for V.*

Proof. Write d for a $(k-1)$-linear alternating function from V^k to K such that $d(x_1, \ldots, x_{k-1}) = 1$; write y_1, ..., y_k for a basis of V, and $x_i = \sum_{j=1}^{k} \chi_{i,j} y_j$, and observe that

$$1 = \sum_{1 \le j_1, \ldots, j_{k-1} \le k} x_{1,j_1} \cdot x_{2,j_2} \cdot \ldots \cdot x_{k-1,j_{k-1}} \cdot d\left(y_{j_1}, \ldots, y_{j_{k-1}}\right).$$

If $1 \le p \le n$ and j_1, ..., j_{k-1}, q_1, ..., q_{k-1} are both permutations of $1, \ldots, \hat{p}, \ldots, n$, then

$$\varepsilon_{j_1,\ldots,j_{k-1},p} d\left(y_{j_1}, \ldots, y_{j_{k-1}}\right) = \varepsilon_{q_1,\ldots,q_{k-1},p} d\left(y_{q_1}, \ldots, y_{q_{k-1}}\right),$$

since d is alternating, so we can define $x_k = (\chi_{k,p})$, $1 \le p \le n$, by

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$$\chi_{k,p} = \varepsilon_{j_1,\ldots,j_{k-1},p}\, d\left(y_{j_1}, \ldots, y_{j_{k-1}}\right) ,$$

where $j_1, \ldots, j_{k-1}$ is some permutation of $1, \ldots, \hat{p}, \ldots, n$. The determinant of the coordinates of $x_1, \ldots, x_k$ with respect to $y_1, \ldots, y_k$ is therefore

$$\sum_{1\le j_1,\ldots,j_k\le k} \varepsilon_{j_1,\ldots,j_k} x_{1,j_1} \cdot \ldots \cdot x_{k,j_k}$$

$$= \sum_{1\le j_1,\ldots,j_{k-1}\le k} x_{1,j_1} \cdot \ldots \cdot x_{k-1,j_{k-1}} \left(\sum_{j_k=1}^{k} \varepsilon_{j_1,\ldots,j_k} \cdot \varepsilon_{j_1,\ldots,j_k} \cdot d\left(y_{j_1}, \ldots, y_{j_{k-1}}\right)\right)$$

$$= d(x_1, \ldots, x_{k-1}) = 1 ,$$

hence the determinant of coefficients of an n-tuple of vectors of V with respect to the basis $y_1, \ldots, y_k$ is an n-linear alternating function, as required to show $x_1, \ldots, x_k$ are mutually free.

The extension of mutually free vectors in a finite dimensional space to a basis of the space is straightforward if the underlying field of scalars is the Dedekind real or complex numbers, in view of the following result.

PROPOSITION 8. *If K is the Dedekind real or complex numbers and A is a matrix with entries from K, then there is a square, invertible matrix B such that BA is upper triangular.*

Proof. If $A = (\alpha_{i,j})$ is an $n \times k$ matrix, we may assume $n \ge 2$. We show first that it is sufficient to be able, given arbitrary $a, b \in K$, to find $c, s \in K$ such that $ac - bs = 0$ and $|c^2+s^2| = 1$.

In that case we can first put $b = \alpha_{n-1,1}$, $a = \alpha_{n,1}$ and premultiply A by $(\beta_{i,j})$, $1 \le i, j \le n$ where $\beta_{i,j} = \delta_{i,j}$ except for $i = n-1, n$ and $j = n-1, n$ and where

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

$$\begin{pmatrix} \beta_{n-1,n-1} & \beta_{n-1,n} \\ \beta_{n,n-1} & \beta_{n,n} \end{pmatrix} = \begin{pmatrix} c & s \\ -s & c \end{pmatrix} .$$

We get by this means an $n \times k$ matrix $A' = (\alpha'_{i,j})$ with $\alpha'_{n,1} = 0$. By successive similar rotations we obtain a matrix A' with $\alpha'_{j,1} = 0$, $j = 2, \ldots, n$; further rotations give also $\alpha'_{j,2} = 0$, $3 \leq j \leq n$, and so on until finally $\alpha'_{i,j} = 0$ for $i > j$, $1 \leq i \leq n$, $1 \leq j \leq k$. The product of these rotations in the order indicated is the required matrix B.

Hence we find a map $K \times K \to K \times K$, say $(a, b) \mapsto (c, s)$, such that $ac = bs$ and $|c^2+s^2| = 1$. For $b \# 0$ we define

$$c = b/\sqrt{|a^2+b^2|} , \quad s = a/\sqrt{|a^2+b^2|} .$$

This map extends to domain $K \times K$ to give the map required. We sketch the argument for the real case.

For arbitrary b we can define by the lower bound theorem a function $\mathrm{sgn}(b)$ on K, such that $b = \mathrm{sgn}(b).|b|$. The map $(a, b) \mapsto (c, s)$ defined by

$$c' = |b|/\sqrt{a^2+b^2} , \quad s' = |a|/\sqrt{a^2+b^2} \quad \text{for } b \# 0$$

extends to $K \times K$ by continuity, so we define the required map by $c = \mathrm{sgn}(b).c'$, $s = \mathrm{sgn}(a).s'$.

For the complex case the argument is similar, since we can define on K a function arg such that for $z \in K$, $z = |z|.\arg z$.

4. Discussion

The results given show that some basic linear algebra is available in the absence of an apartness relation which satisfies Heyting's axioms; but they do not support particularly the definition of field we have given. Indeed inspection shows that, except for Proposition 8, the work on linear algebra holds for modules over an arbitrary commutative ring with unity.

The main case for our particular definition of field is its generality. It could be held that it is too general since the sole axiom

https://doi.org/10.1017/S0004972700042477 Published online by Cambridge University Press

which distinguishes fields from general commutative rings with unity is the negative assertion (x): but the obvious strengthening of this axiom, to

$$(\forall y)(xy \neq 1) \text{ implies } x = 0$$

is so strong as to imply the stability of equality. Indeed it clearly gives

$$\neg (x \# 0) \text{ implies } x = 0 ;$$

On the other hand $\neg\neg (x = 0)$ implies $\neg (x \# 0)$, so we have stability of equality as stated.

References

[1] Errett Bishop, *Foundations of constructive analysis* (McGraw-Hill, New York; Toronto, Ontario; London; 1967).

[2] A. Heyting, "Untersuchungen über intuitionistische Algebra", *Verh. Nederl. Akad. Wetensch., Afd. Natuurk.* Sect. 1 18, no. 2 (1941), 1-36.

[3] L. Mirsky, *An introduction to linear algebra* (Clarendon Press, Oxford, 1955).

[4] John Staples, "On constructive fields", *Proc. London Math. Soc.* (3) 23 (1971), 753-768.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.