No nontrivial Hamel basis is closed under multiplication

Richard D. Mabry

Summary: If H is a Hamel basis for a field $\mathbb{F}$ over a proper subfield of $\mathbb{F}$, then H cannot be closed under the taking of products.

Mathematics Subject Classification (2000): 12D99, 08A35, 39B32

In [2, p. 365] it is noted that there is no Hamel basis for the reals over the rationals that is closed under multiplication. Here we prove the following, more general

Theorem. *Let $\mathbb{F}$ be a field and let $\mathbb{P}$ be a proper subfield of $\mathbb{F}$. Then the condition*

$$h_1 h_2 \in H \text{ whenever } h_1, h_2 \in H \tag{1}$$

is impossible when H is a Hamel basis for $\mathbb{F}$ over $\mathbb{P}$.

What follows is given in two short sections, the first of which gives a few remarks and a bit of context for the result. The reader interested only in the proof can skip to section 2.

1 Remarks

The most commonly encountered Hamel basis for a field $\mathbb{F}$ over a subfield $\mathbb{P}$ occurs when $\mathbb{P}$ is the field $\mathbb{Q}$ of rationals and $\mathbb{F}$ is either the field $\mathbb{C}$ of complex numbers or the field $\mathbb{R}$ of reals. We note, however, that Hamel bases for $\mathbb{F}$ over $\mathbb{P}$ exist, for instance, if $\mathbb{F}$ is $\mathbb{C}$ or $\mathbb{R}$, and $\mathbb{P}$ is a subfield of $\mathbb{F}$ having cardinality less than the continuum ([3, p. 220]). We also note that the assumptions of our theorem exclude the situation of $\mathbb{F} = \mathbb{P}$, and in particular, that of $\mathbb{F} = \mathbb{Q}$; in these cases one can have the trivial basis $H = \{1\}$, which is indeed closed. But otherwise, we make no assumptions about the sizes of $\mathbb{F}$ and $\mathbb{P}$, so $\mathbb{F}$ could be, for example, a field properly containing $\mathbb{C}$. We require only the usual definition of representation by Hamel bases, namely, that of elements of a vector space ($\mathbb{F}$) whose nonzero elements are uniquely expressible as finite linear combinations (over $\mathbb{P}$) of basis elements (from H).

An endomorphism of the field $\mathbb{F}$ is any function $f : \mathbb{F} \to \mathbb{F}$ satisfying

$$f(x+y) = f(x) + f(y) \quad \text{and} \quad f(xy) = f(x)f(y) \quad \forall x, y \in \mathbb{F}. \tag{2}$$

An interesting role is played by the function $\tau_H : \mathbb{F} \to \mathbb{F}$ defined by

$$\tau_H\left(\sum_{i=1}^{n} p_i h_i\right) = \sum_{i=1}^{n} p_i, \tag{3}$$

which we note is not identically zero (since $\tau_H(h) = 1$ for $h \in H$), is $\mathbb{P}$-valued (and therefore not onto $\mathbb{F}$), and is, as can be easily checked, an endomorphism of $\mathbb{F}$ in the event that (1) holds.

The proof sketched in [2] for the case of our theorem in which $\mathbb{F} = \mathbb{R}$ and $\mathbb{P} = \mathbb{Q}$ is based on the fact that there are no nontrivial endomorphisms on $\mathbb{R}$ ([2, p. 356]). That is, there are no functions $f : \mathbb{R} \to \mathbb{R}$, other than $f(x) = x$ and $f(x) = 0$, for which (2) holds when $\mathbb{F} = \mathbb{R}$. But if (1) holds, then τ_H is a nontrivial endomorphism of $\mathbb{R}$, which is impossible. This proves that a Hamel basis H for $\mathbb{R}$ over $\mathbb{Q}$ cannot be closed with respect to multiplication. (The preceding argument works for any proper subfield $\mathbb{P}$ of $\mathbb{R}$ in place of $\mathbb{Q}$, though it wasn't stated that way in [2].) On a related note, J. Smítal proved that a weaker sort of closure is possible, namely that a Hamel basis H for $\mathbb{R}$ over $\mathbb{Q}$ does exist for which $h^n \in H$ whenever $h \in H$ and n is an integer [4].

On the other hand, there do exist nontrivial endomorphisms of the complex plane, these being functions $f : \mathbb{C} \to \mathbb{C}$, other than $f(z) = z$, $f(z) = \bar{z}$ and $f(z) = 0$, satisfying (2). See [1] or [2, p. 358]. This would seem to leave open the question of the existence of a Hamel basis H for $\mathbb{C}$ over $\mathbb{Q}$ satisfying (1). It turns out that the proof for the real case can be easily adapted to answer this question. This was pointed out by a referee, who noted that the only real-valued endomorphism of $\mathbb{C}$ is the zero function. (To see this, let $z \in \mathbb{C}$ and let u be a square root of z. Then if f is any real-valued endomorphism of $\mathbb{C}$, we have $f(z) = f(u^2) = (f(u))^2 \geq 0$, since $f(u)$ is real. Likewise, $-f(z) = f(-z) = f((iu)^2) = (f(iu))^2 \geq 0$, so $f(z)$ must be identically zero.) But assuming that $\mathbb{F} = \mathbb{C}$ and $\mathbb{Q} \subseteq \mathbb{P} \subseteq \mathbb{R}$, we see that τ_H is real-valued and nonzero on $\mathbb{C}$. If (1) holds, then τ_H is a real-valued nonzero endomorphism of $\mathbb{C}$. Hence (1) is impossible when $\mathbb{F} = \mathbb{C}$ and $\mathbb{Q} \subseteq \mathbb{P} \subseteq \mathbb{R}$.

The main result in this note is therefore of most interest when $\mathbb{P}$ is not a subset of $\mathbb{R}$ or when $\mathbb{F}$ differs from $\mathbb{R}$ and $\mathbb{C}$.

2 Proof of the result

In what follows, when a fixed nonzero element z of $\mathbb{F}$ is such that

$$z = \sum_{i=1}^{n} p_i h_i, \tag{4}$$

where the $h_i \in H$ are all distinct and each $p_i \in \mathbb{P} \setminus \{0\}$, we occasionally indicate the uniqueness of such a representation by writing $z \overset{H}{=} \sum_{i=1}^{n} p_i h_i$.

To prove our theorem, we first establish a few useful facts via a sequence of lemmas.

Lemma 1. *Suppose that* $\displaystyle\sum_{i=1}^{n} p_i h_i = \sum_{j=1}^{m} r_j k_j$, *where the* h_i *and* k_j *are in* H *and the* p_i *and* r_j *are in* $\mathbb{P}$. *Suppose further that the* p_i *are all nonzero and the* h_i *are all distinct. Then each of the* h_i *must occur among the* k_j, *i.e., for each* $i = 1, 2, \ldots, n$, *it must be that* $h_i = k_j$ *for some* $j = 1, 2, \ldots, m$.

Proof. This is clear using the independence (over $\mathbb{P}$) of the elements of H. $\square$

It is important to note that the reverse is not true in the above lemma, i.e., the k_j need not appear among the h_i, because when the k_j are not assumed distinct, the various terms $r_j k_j$ could cancel.

For the remainder of the paper we assume (until we obtain a contradiction) that H is a Hamel basis for $\mathbb{F}$ over $\mathbb{P}$ (with the conditions on $\mathbb{F}$ and $\mathbb{P}$ as already noted) such that (1) holds.

Lemma 2. *If $h \in H$ and $k \in H$, then h/k is in H.*

Proof. Let $\frac{h}{k} \overset{H}{=} \sum_{i=1}^{n} p_i h_i$. Then

$$h = \sum_{i=1}^{n} p_i h'_i, \tag{5}$$

where $h'_i = kh_i \in H$ for each i. But the h'_i are all themselves distinct, for if $h'_i = h'_j$ then we have $kh_i = kh_j$, implying $h_i = h_j$, which contradicts the uniqueness of the representation for h/k. But then it must be that $n = 1$, because the lefthand side of the representation (5) is certainly unique. This means that $p_1 = 1$ and $h'_1 = h$, hence $h/k = h_1 \in H$. $\square$

Letting h be any member of H and letting $k = h$ in Lemma 2 gives us the following useful fact.

Lemma 3. $1 \in H$.

Lemma 4. *If $h^n = 1$ for $h \in H$ and a positive integer n, then $h = 1$.*

Proof. Assume, to the contrary, that $h \in H$ and that $h \neq 1$. We may assume that n is the smallest positive integer for which $h^n = 1$. Clearly, $n > 1$, so we have

$$0 = h^n - 1 = (h-1) \sum_{i=0}^{n-1} h^i,$$

and therefore,

$$1 = \sum_{i=1}^{n-1} -h^i.$$

Since each h^i is in H, at least one of the h^i must equal 1, by Lemma 1 and Lemma 3. But this means that $h^i = 1$ for some i strictly between 0 and n, contradicting the minimality of n. $\square$

Lemma 5. *Suppose h and k are in H and that n is a nonzero integer such that $h^n = k^n$. Then $h = k$.*

Proof. The assumptions imply that $(h/k)^n = 1$, so Lemma 2 and Lemma 4 give us the proof. □

We're now ready to prove the main result.

Proof of Theorem. Let k_1 and k_2 be distinct members of H and observe that $k_1 + k_2 \neq 0$. Writing the Hamel representation for $1/(k_1 + k_2)$, i.e.,

$$\frac{1}{k_1 + k_2} \stackrel{H}{=} \sum_{i=1}^{n} p_i h_i, \tag{6}$$

we have

$$1 = \sum_{i=1}^{n} p_i h_i' + \sum_{i=1}^{n} p_i h_i'',$$

where the h_i' and h_i'' are elements of H with $h_i' = k_1 h_i$ and $h_i'' = k_2 h_i$. It is also clear that $h_i' \neq h_i''$ for each i, and the h_i' are all distinct, as are the h_i''. By Lemma 1 and Lemma 3, one of the h_i' or h_i'' must equal 1, so without loss of generality (by re-indexing , if necessary) we may let $h_1' = 1$.

We note that if $n = 1$, then $1 = p_1 h_1' + p_1 h_1''$. Because h_1' and h_1'' are distinct with $h_1' = 1$, it would then follow that the coefficient of h_1' is 1 while the coefficient of h_1'' is zero. This is clearly nonsensical, so we must have $n > 1$.

Writing

$$(1 - p_1) h_1' + \sum_{i=2}^{n} -p_i h_i' = \sum_{j=1}^{n} p_j h_j'', \tag{7}$$

the observations about the distinct elements, along with Lemma 1, show that each h_i' on the left is equal to exactly one h_j'' on the right. (Our attention is, however, first drawn to the fact that the coefficient of h_1' might be zero, but this cannot be the case. For if so, then the pigeonhole principle puts two distinct h_j'' equal to some h_i', and therefore equal to each other, which is impossible.)

We will repeatedly use the fact that when $h_i' = h_j''$ we have

$$\frac{k_1}{k_2} = \frac{h_j}{h_i}.$$

Now it cannot be that $h_1' = h_1''$, so we must have $h_1' = h_j''$ for some $j > 1$. We may let (by reindexing the h_j'', if necessary) $h_1' = h_2''$. Considering the possibility that $h_2' = h_1''$, we would then have

$$\frac{k_1}{k_2} = \frac{h_2}{h_1} = \frac{h_1}{h_2}.$$

But this implies that

$$\left(\frac{k_1}{k_2}\right)^2 = \frac{h_2}{h_1}\frac{h_1}{h_2} = 1,$$

so $k_1^2 = k_2^2$. But then $k_1 = k_2$ by Lemma 5. This is impossible, as is the remaining possibility that $h'_2 = h''_2$. We therefore must have $n > 2$.

This process continues and shows that no finite sum such as (7) is possible. The proof is by induction. If (7) is impossible for $n = 1, 2, \ldots, N$ (which we have shown explicitly for $N = 1, 2$), it must be that $n > N$, so we relabel when appropriate and necessary to obtain the pairings

$$h'_1 = h''_2, \quad h'_2 = h''_3, \quad \ldots, \quad h'_N = h''_{N+1}.$$

If we now consider the possibility that $h'_{N+1} = h''_1$, we obtain

$$\frac{k_1}{k_2} = \frac{h_2}{h_1} = \frac{h_3}{h_2} = \cdots = \frac{h_{N+1}}{h_N} = \frac{h_1}{h_{N+1}}.$$

It follows that

$$\left(\frac{k_1}{k_2}\right)^{N+1} = \left(\frac{h_2}{h_1}\right)\left(\frac{h_3}{h_2}\right)\cdots\left(\frac{h_{N+1}}{h_N}\right)\cdot\left(\frac{h_1}{h_{N+1}}\right) = 1.$$

But then $k_1^{N+1} = k_2^{N+1}$, so again by Lemma 5, we have the contradiction $k_1 = k_2$.

This shows that it is impossible that $h'_{N+1} = h''_1$ and so it must be that $h'_{N+1} = h''_i$ for some $i > N + 1$ (otherwise $h'_{N+1} = h''_{N+1}$). But this means $n > N + 1$ and shows that (7) is impossible for $n = N + 1$, and inductively, for all n.

We have now proved that no representation of the form (6) is possible, and hence H cannot span $\mathbb{F}$ over $\mathbb{P}$. Thus H cannot be a Hamel basis for $\mathbb{F}$ over $\mathbb{P}$. $\square$

References

[1] Kestelman, H., Automorphisms of the field of complex numbers, *Proc. London Math. Soc., II. Ser.*, **53** (1951), 1-12.

[2] M. Kuczma, *An introduction to the theory of functional equations and inequalities*, Panstwowe Wydawnictwo Naukowe, Warszawa, 1985.

[3] J. C. Morgan II, *Point Set Theory*, Marcel Dekker, New York, 1989.

[4] Smítal, J., On a problem of Aczél and Erdős concerning Hamel bases, *Aequationes Math.*, **28** (1985), no. 1-2, 135-137.

Department of Mathematics
Louisiana State University in Shreveport
Shreveport, LA 71115-2399
USA
e-mail: rmabry@pilot.lsus.edu