Uncountable Fields Have Proper Uncountable Subfields

Ralph S. Butcher
United States Naval Academy
Annapolis, MD 21402

Wallace L. Hamilton
John G. Milcetich
University of the District of Columbia
Washington, DC 20008

In a first encounter of the study of fields in an abstract algebra course, a student learns about various subfields of $\mathbb{R}$ and $\mathbb{C}$ which are usually obtained by adjoining a finite number of elements to the field $\mathbb{Q}$. The student may also learn about the subfield of $\mathbb{R}$ consisting of those real numbers which are algebraic over $\mathbb{Q}$. Each of these subfields of $\mathbb{R}$ has the property that it contains a countable number of elements. Since the field $\mathbb{R}$ is uncountable, the question naturally arises as to whether there exists an uncountable proper subfield of $\mathbb{R}$. An affirmative answer to this may be given by appealing to the existence of a transcendental basis of $\mathbb{R}$ over $\mathbb{Q}$ [**1**]. The idea of a transcendental basis is not commonly encountered in an undergraduate abstract algebra course, but many students do encounter Zorn's lemma with which one can construct an elementary, yet interesting, proof of the following proposition.

Proposition. *If all proper subfields of a field F contain a countable number of elements, then F contains a countable number of elements.*

To see this, we first note that the prime field of F, which is the smallest subfield of F (the field generated by the multiplicative identity), is isomorphic either to $\mathbb{Q}$ or to a finite field of p elements. So without loss of generality we may assume that F properly contains its prime field. Let c be an element of F which is not in the prime field. Define S to be the collection of all subfields of F which do not contain c. S is nonempty because the prime field is in S. Moreover, the collection S is partially ordered by set inclusion. If $\{K_\alpha\}$ is any chain from S, then $\bigcup_\alpha K_\alpha$ is in S and is an upper bound. By Zorn's lemma, there exists a maximal subfield M of F which does not contain c. By assumption M is countable. Let y be an arbitrary element of $F \setminus M$. Then $M(y)$ is a field which properly contains M and, hence, by the maximality of M, we have that c is in $M(y)$. This means that $c = p(y)/q(y)$, where $p(y)$ and $q(y)$ are polynomials in y with coefficients from M. We then obtain $p(y) - cq(y) = 0$, which shows that y is algebraic over the field $M(c)$. But $M(c)$ is countable and there are only countably many algebraic elements over $M(c)$. (The number of polynomials over a countable field is countable and each polynomial has only a finite number of roots in the algebraic closure of the field.) Consequently both M and $F \setminus M$ are countable, which gives us the fact that F is countable.

An immediate corollary to the proposition is that the uncountable field $\mathbb{R}$ contains an uncountable proper subfield.

A few remarks are worth noting. First, keeping the notation of the proof, we see that every element of the field F is algebraic over $M(c)$. Second, the proof is valid for any infinite cardinal number. That is, if $\aleph$ is any infinite cardinal number and if all proper subfields of F have cardinality at most $\aleph$, then F has cardinality at most $\aleph$. However, it is not true that the field must be finite if all proper subfields of the field are finite. A standard construction shows that there exists a countable field all of whose proper subfields are finite. To see this, let F_1 be the finite field of p elements for some prime p. There is always an irreducible polynomial of degree 2 over any finite field of q elements because the number of polynomials of the form $x^2 + ax + b$ is q^2 and the number of those of the form $(x - a)(x - b)$ is $q + q(q - 1)/2$. Suppose we have defined

fields $F_1, \ldots, F_{n-1}$ for some $n \geqslant 2$, such that each field is a subfield of the algebraic closure of F_1 and $F_1 \subset F_2 \subset \cdots \subset F_{n-1}$. Then let a_n be an element of the algebraic closure of F_1 which is a root of an irreducible polynomial in $F_{n-1}[x]$ and define $F_n = F_{n-1}[a_n]$. Then $F_1 \subset F_2 \subset F_3 \subset \cdots$ and $F = \bigcup_n F_n$ is a countable field. Assume that K is a countable subfield of F. For each α in K, there is a smallest $n(\alpha)$ such that α is in $F_{n(\alpha)}$. Since α is not in $F_{n(\alpha)-1}$, α is a generator of the cyclic group of nonzero elements in $F_{n(\alpha)}$. Hence we have $F_{n(\alpha)} \subset K$. Since there are countably many elements in K, $\sup\{n(\alpha): \alpha \in K\} = \infty$. The nesting of the F_n's now shows that $F = \bigcup_\alpha F_{n(\alpha)} = K$.

References

[1] S. Lang, Algebra, Addison-Wesley, Reading, Mass., 1965, pp. 253–255.

Imitation of an Iteration

DANIEL A. RAWSTHORNE
Wheaton, MD 20902

A most fascinating and frustrating problem is the **Collatz $3x+1$ problem**. *Does repeated iteration of the function*

$$T(n) = \begin{cases} \dfrac{n}{2}, & n \text{ even}, \\ \dfrac{3n+1}{2}, & n \text{ odd}, \end{cases}$$

always reach 1, *for any positive starting point*? This convergence to 1 has been verified for n up to the billions, but a proof of convergence for all n does not yet exist. In fact, the problem seems intractable as stated, and has a place of honor in R. Guy's article, "Don't Try to Solve These Problems!" [7]. What *is* known of this problem is probabilistic in nature, such as: "For almost all positive starting points, there is some iterate smaller than the starting point."

In this note we consider a generalization of the $3x+1$ problem and prove a fairly strong probabilistic result. This result is not completely new, but the purpose here is to demonstrate that a probabilistic model can give information concerning a number-theoretic problem. Finally, we make a strong conjecture concerning the generalized iteration problem, and present some empirical data concerning this conjecture.

We deal with the following generalization of the $3x+1$ problem. Define a **Collatz-type iteration** function $C(n)$ by its action on different residue classes of the positive integers mod d as

$$C(n) = \left\{ h_i(n) = \frac{a_i n + b_i}{d}, \quad \text{for } n \equiv i \bmod d\text{: } 0 \leqslant i \leqslant d-1 \right\}, \tag{1}$$

where $a_i n + b_i \equiv 0 \bmod d$. For example, the function $T(n)$ is given by definition (1) with $d=2$, and $a_0 = 1$, $b_0 = 0$, $a_1 = 3$, $b_1 = 1$. Let the trajectory of n be the sequence of iterations $(n, C(n), C^{(2)}(n), C^{(3)}(n), \ldots)$. We say that the **trajectory** of n **converges to a cycle** if the sequence ends in a repeating loop. For example, the trajectory of 13 for $T(n)$ in the $3x+1$ problem is $(13, 20, 10, 5, 8, 4, 2, 1, 2, \ldots)$, which converges to the cycle $(1, 2, 1)$. Clearly, the trajectory of n converges to $(1, 2, 1)$ in the $3x+1$ problem if and only if some iterate of $T(n)$ reaches 1, so we have another way of looking at the problem—by looking at convergence of trajectories.

With the notation in (1), we can now ask the general Collatz-type question: *For which functions $C(n)$ do the trajectories of all positive n converge to a finite set of known cycles*?