



---

An Overlooked Example of Nonunique Factorization

Author(s): Hale F. Trotter

Source: *The American Mathematical Monthly*, Vol. 95, No. 4 (Apr., 1988), pp. 339-342

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2323570>

Accessed: 26/01/2009 12:22

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

REMARKS 1. If we take  $F(X, Y, Z) = XZ - 2ZY$ , the polynomial identity  $(x + 2y)xy = xy(x + 2y)$ , or if we take  $F(X, Y, Z) = XYZ$ , then the polynomial identity  $(xy)^2 = xy^2x$  for all  $x$  and  $y$  in  $R$  implies commutativity. Other examples can be constructed ad libitum ad infinitum.

2. More subtle commutativity theorems, which do not work for all rings with unity, also often assume polynomial identities of the form  $F(x, y, xy - yx) = 0$ , but with  $F(1, 1, Z) = 0$ .

#### REFERENCES

1. Ram Awtar, A Remark on Commutativity of Certain Rings, *Proc. Amer. Math. Soc.*, 41 (1973) 370–372.
2. \_\_\_\_\_, On the Commutativity of Non-Associative Rings, *Publ. Math. (Debrecen)*, 22 (1975) 177–188.
3. R. N. Gupta, Nilpotent Matrices with Invertible Transpose, *Proc. Amer. Math. Soc.*, 24 (1970) 572–575.
4. A. Hermanci, Two Elementary Commutativity Theorems for Rings, *Acta Math. Acad. Sci. Hungar. Tomus*, 29 (1977) 23–29.
5. E. C. Johnsen, D. L. Outcalt, and Adil Yaqub, An Elementary Commutativity Theorem for Rings, *Amer. Math. Monthly*, 75 (1968) 288–289.
6. Murtaza A. Quadri, A Note on Commutativity of Semiprime Rings, *Math. Japonica*, 22 (1978) 509–511.

## An Overlooked Example of Nonunique Factorization

HALE F. TROTTER

*Department of Mathematics, Princeton University, NJ 08544*

On the face of it, the familiar identity

$$\sin^2 t = 1 - \cos^2 t = (1 + \cos t)(1 - \cos t) \quad (1)$$

asserts that two different-looking pairs of factors have the same product. It seems to have gone unnoticed, however, that (1) is actually a valid example of nonunique factorization in an integral domain when looked at in the proper context. Its familiarity makes it a particularly attractive example to present to students encountering nonunique factorization for the first time. Just as the usual textbook examples involving integers in quadratic number fields, such as  $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , show that unique factorization can fail in rings very much like the integers, the example treated here shows that it can fail in a ring very much like the ring of polynomials over a field.

Of course we have to do more than simply remark that the two sides of (1) look different. We must specify the ring we are working in, and then show that the factors  $\sin t$ ,  $1 + \cos t$ , and  $1 - \cos t$  are irreducible, and that  $\sin t$  is not the product of one of the other factors and a unit (invertible element) of the ring.

We shall work with the real trigonometric polynomials, that is, the functions representable as finite sums of the form

$$a_0 + \sum_{n=1}^k (a_n \cos nt + b_n \sin nt) \quad (2)$$

in which the  $a$ 's and  $b$ 's are real numbers. Students who have seen anything of Fourier series find it natural enough to consider these functions, although they may not have seen them called trigonometric polynomials, or considered the question of whether they form a ring. The familiar Fourier coefficient formulas  $a_0 = (2\pi)^{-1} \int_{-\pi}^{\pi} f(x) dx$ ,  $a_n = \pi^{-1} \int_{-\pi}^{\pi} f(x) \cos nx dx$ , and  $b_n = \pi^{-1} \int_{-\pi}^{\pi} f(x) \sin nx dx$  for  $n > 0$ , show that the coefficients in (2) are uniquely determined by the function.

The *degree* of a nonzero trigonometric polynomial is defined as the largest value of  $n$  for which  $a_n$  and  $b_n$  are not both zero. The following well-known lemma shows that the trigonometric polynomials form a ring, and that degrees behave as they do for ordinary polynomials.

**LEMMA.** *The product of a trigonometric polynomial of degree  $m$  and one of degree  $n$  is a trigonometric polynomial of degree  $m + n$ .*

*Proof.* The assertion of the lemma is obvious if  $m$  or  $n$  is 0, because a trigonometric polynomial of degree zero is simply a constant function. From now on we assume  $m, n > 0$ . Recall the standard identities for expressing products of sines and cosines in terms of sums and differences of other sines and cosines:

$$(\sin a)(\sin b) = [\cos(a - b) - \cos(a + b)]/2$$

$$(\cos a)(\cos b) = [\cos(a - b) + \cos(a + b)]/2$$

$$(\sin a)(\cos b) = [\sin(a + b) + \sin(a - b)]/2.$$

Applying these to the product of  $p \cos mt + q \sin mt$  and  $r \cos nt + s \sin nt$  and collecting terms, gives the result

$$A \cos(m - n)t + B \sin(m - n)t + C \cos(m + n)t + D \sin(m + n)t, \quad (3)$$

where  $A = (pr + qs)/2$ ,  $B = (ps - qr)/2$ ,  $C = (pr - qs)/2$ , and  $D = (ps + qr)/2$ . When  $m > n$ , (3) is already in the form (2). If  $n > m$ , replacing  $\cos(m - n)$  by  $\cos(n - m)$  and  $\sin(m - n)$  by  $-\sin(n - m)$  puts it in the proper form, while if  $m = n$  it is necessary to replace  $\sin 0$  by 0 and  $\cos 0$  by 1. Direct calculation gives

$$C^2 + D^2 = (p^2 + q^2)(r^2 + s^2)/4,$$

which shows that if neither factor is zero (so  $p^2 + q^2 \neq 0$  and  $r^2 + s^2 \neq 0$ ) then  $C^2 + D^2 \neq 0$ , so the product has degree  $m + n$ .

Now consider the product of any two trigonometric polynomials of respective degrees  $m$  and  $n$ . It is a sum of products of terms of the type just considered, so it is a trigonometric polynomial. The product of the two high-order terms gives a non-zero term of degree  $m + n$  which cannot be cancelled by any other term in the product, so the result has degree  $m + n$  as claimed.

**PROPOSITION.** *The trigonometric polynomials form an integral domain. Furthermore,*

- (a) *The units (invertible elements) in this domain are the elements of degree 0, that is, the constant functions.*
- (b) *All elements of degree 1, including  $\sin t$ ,  $1 + \cos t$ , and  $1 - \cos t$ , are irreducible.*

The proposition follows at once from the lemma, just as with ordinary polynomials, and we leave the details to the reader.

It follows from (a) and (b) that the factors in (1) are irreducible and that  $\sin t$  is not the product of one of the other factors with a unit. Hence we have a genuine case of nonunique factorization.

One can very well stop here in an elementary discussion, but the example does raise another point that may be of interest.

The proof of the lemma uses the fact that the sum of the squares of two real numbers is zero only when both are zero, and breaks down if complex coefficients are allowed. Using the complex exponential forms of the sine and cosine shows that the ring of trigonometric polynomials with complex coefficients is the same as the ring of polynomials in positive and negative powers of  $z = e^{it}$  with complex coefficients. To see that this is a unique factorization ring, define the degree of a polynomial in  $z$  and  $z^{-1}$  as the difference between the largest and smallest exponents appearing in non-zero terms. With this definition, the elements of degree zero are the monomials, which are exactly the invertible elements in this ring. The usual proof that ordinary polynomials over a field form a Euclidean ring then goes through with no essential change.

What is it about the change of coefficients that alters the nature of factorization in the ring? For one thing, introducing complex coefficients produces many more units—all the non-zero constant multiples of powers of  $z = \cos t + i \sin t$  and  $z^{-1} = \cos t - i \sin t$ . Our particular example breaks down because the factors involved cease to be irreducible. We have

$$\sin t = (z - z^{-1})/(2i) = z^{-1}(z - 1)(z + 1)/(2i),$$

$$1 - \cos t = (-z + 2 - z^{-1})/2 = -z^{-1}(z - 1)^2/2,$$

and

$$1 + \cos t = z^{-1}(z + 1)^2/2,$$

so both sides of (1) become

$$-z^{-2}(z - 1)^2(z + 1)^2/4$$

when expressed as a product of irreducible factors.

A ring of algebraic integers can sometimes be enlarged to another in a way that restores unique factorization, although the problem of how and when it can be done is not at all elementary, and as far as I know is not solved in general. For example, the ring  $\mathbf{Z}[\sqrt{-3}]$  consisting of numbers of the form  $a + b\sqrt{-3}$  with  $a$  and  $b$  integers does not have unique factorization, as the equation  $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$  shows. Unique factorization can be restored in this case by enlarging to the ring of *all* algebraic integers in the field  $\mathbf{Q}(\sqrt{-3})$ , which is  $\mathbf{Z}[\omega]$ , where  $\omega = (1 + \sqrt{-3})/2$  is a complex cube root of one. This does not work for the ring  $\mathbf{Z}[\sqrt{-5}]$  used in the example at the beginning of the paper, because that is already the ring of all algebraic integers in the field  $\mathbf{Q}(\sqrt{-5})$ . The ring of all algebraic integers in the enlarged field  $\mathbf{Q}(\sqrt{-5}, i)$ , however, which can be shown to be the ring  $\mathbf{Z}[\eta]$  where  $\eta = (i + \sqrt{-5})/2$  is a root of  $x^4 + 3x^2 + 1$ , is an enlargement of  $\mathbf{Z}[\sqrt{-5}]$  that does have unique factorization. I do not know an elementary proof of

the last assertion, but it is easily established by standard arguments based on Minkowski's estimate, as illustrated in [1, chapter 12], [2, chapter 13], or [3, chapter 5].

#### REFERENCES

1. E. Artin, *Theory of Algebraic Numbers*, Math. Inst. Göttingen, 1959.
2. H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, New York, 1978.
3. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.

## Two Counterexamples in General Topology

P. V. KRISHNAIAH

*Department of Mathematics, The University of Toledo, Ohio*

In [3] Albert Wilansky inserted two axioms between the separation axioms  $T_1$  and  $T_2$ , namely the *US*-axiom (every convergent sequence has a unique limit) and the *KC*-axiom (every compact subset is closed). He showed that  $T_2 \Rightarrow KC \Rightarrow US \Rightarrow T_1$  and discussed at length the problem of constructing counterexamples of compact spaces showing the failure of each of the reverse implications, proving several interesting results in the process. As a consequence of theorems 4 and 5 of [3], it was brought out that, if a  $T_2$ -space  $X$  is not a  $k$ -space (a  $k$ -space is one in which a set is closed iff its intersection with each closed compact set is closed) then its one point compactification  $X^+$  is *US* but not *KC*. An example of a  $T_2$ -space, which is not a  $k$ -space is given in [3], example 7. Since this example involves the Čech compactification, it seems worthwhile to have the following two elementary examples.

*Example 1.* The Appert space  $A$  (see [1], p. 117) whose ground set is the set of all positive integers and  $E \subseteq A$  is open iff either  $1 \notin E$  or  $1 \in E$  and

$$\lim_{n \rightarrow \infty} \frac{1}{n} \left\{ \sum_{r=1}^n \chi_E(r) \right\} = 1.$$

*Example 2.* The Fortissimo space  $F$  (see [1], p. 53) whose ground set is any uncountable set with a particular point  $p$  and  $E \subseteq F$  is open iff either  $p \notin E$  or  $p \in E$  and  $F \setminus E$  is countable.

One easily verifies that both  $A$  and  $F$  above are noncompact  $T_2$ -spaces, that both are pseudofinite (i.e., all compact subsets are finite) and that neither is discrete. Hence, neither of them is a  $k$ -space so that both  $A^+$  and  $F^+$  are *US* but not *KC*. This can in fact be shown directly. While  $A^+ \setminus \{1\}$  and  $F^+ \setminus \{p\}$  are compact nonclosed subsets of  $A^+$  and  $F^+$ , respectively, one easily imitates the proof of theorem 4 in [3] to show that they are *US* spaces.

Other examples may be found in [2, example 2.3] and [4, p. 345].