

The conclusion from the foregoing is that Steinhaus conjectured the ham sandwich theorem and Banach gave the first proof, using the Ulam-Borsuk theorem. This shows that Stone and Tukey were not correct in attributing the ham sandwich theorem to Ulam. However, Ulam did make a fundamental contribution in proposing the antipodal map theorem.

**Remarks.** We first mention a recent application by Blair Swartz of ham sandwich theorems for fractions other than  $1/2$  to interface reconstruction in hydrodynamic calculations. See paragraph 20 of the web site:

<http://www-troja.fjfi.cvut.cz/~liska/bbw/abs-list.html>

There is a cautionary note stating that for some shapes or configurations of cells there exist  $n$ -tuples of mass fractions that cannot be simultaneously sliced from cells.

Finally, we note a paper by Steinhaus [3] that represents work Steinhaus did in Poland on the ham sandwich problem in World War II while hiding out with a Polish farm family.

**ACKNOWLEDGEMENT.** We thank Sharon Smith for help in finding material in Polish libraries.

#### REFERENCES

---

1. R. D. Mauldin, ed., *The Scottish Book*, Birkhäuser, Boston, 1981.
2. A. H. Stone and J. W. Tukey, Generalized “sandwich” theorems, *Duke Math. J.* **9** (1942) 356–359.
3. H. Steinhaus, Sur la division des ensembles de l’espace par les plans et des ensembles par les cercles, *Fund. Math.* **33** (1945) 245–263.

*Los Alamos National Laboratory, Mail Stop K710, Los Alamos, NM, 87545*  
*beyer@lanl.gov*  
*azs@lanl.gov*

---

## Roots Appear in Quanta

---

Alexander R. Perlis

---

We start with a special case. Consider an irreducible quintic polynomial

$$f(X) = X^5 + a_1X^4 + a_2X^3 + a_3X^2 + a_4X + a_5$$

with rational coefficients and with three real roots and one pair of complex conjugate roots. For example,  $f(X)$  could be  $X^5 - 10X + 5$ .

**Question.** If  $\alpha$  is a root of  $f$ , then how many roots of  $f$  lie in the field  $\mathbf{Q}(\alpha)$ ?

The field  $\mathbf{Q}(\alpha)$  is obtained by adjoining the root  $\alpha$  to  $\mathbf{Q}$ . Thus  $\mathbf{Q}(\alpha)$  contains at least one root of  $f$ , and of course it can contain at most five roots of  $f$ .

**Answer.** The number  $r(f)$  of roots of  $f$  in  $\mathbf{Q}(\alpha)$  is 1. We prove that, for an arbitrary irreducible polynomial  $f$  and root  $\alpha$ ,  $r(f)$  divides the degree of  $f$ . For the quintic

under discussion, adjoining one of the real roots cannot possibly produce the nonreal roots, so  $r(f)$ , being a divisor of 5, must be 1.

An informal survey of books and colleagues indicates that the divisibility result “ $r(f)$  divides the degree” is not well known. In what follows,  $K$  is a field and, unless stated otherwise, all roots and field extensions are taken in a fixed algebraic closure  $\bar{K}$  of  $K$ . When  $K = \mathbf{Q}$ , we always take  $\bar{K}$  inside the complex numbers so that we can speak of real roots and nonreal roots.

**Theorem 1.** *Let  $f(X)$  in  $K[X]$  be an irreducible polynomial, and let  $\alpha$  be a root of  $f$ . Set*

$$r_K(f) := \text{number of roots of } f \text{ that lie in } K(\alpha),$$

$$s_K(f) := \text{number of fields of the form } K(\alpha'), \text{ where } \alpha' \text{ is a root of } f.$$

*Then  $r_K(f)$  is independent of the choice of  $\alpha$ , and*

$$r_K(f) \cdot s_K(f) = \text{cardinality of the set of roots of } f.$$

*In particular,  $r_K(f)$  divides the degree of  $f$ .*

Concerning the last statement of the theorem: the cardinality of the set of roots of  $f$  is known as the *separable degree* of  $f$ , and it is well known that the separable degree divides the usual degree.

*Proof.* For this proof, we let “root” mean “root of  $f$ ” and let “stem field” signify a field of the form  $K(\alpha')$ , where  $\alpha'$  is a root. Since  $f$  is irreducible, each stem field is  $K$ -isomorphic to the abstract field  $K[X]/(f(X))$ , whence any two stem fields are  $K$ -isomorphic. Isomorphisms take roots to roots, so  $r_K(f)$  is the same for each stem field. Each root  $\alpha'$  lies in precisely one stem field: it lies in  $K(\alpha')$ , and if it also lies in  $K(\alpha'')$ , then  $K(\alpha') \subseteq K(\alpha'')$ , but because the two stem fields have the same degree over  $K$  (they are  $K$ -isomorphic), we must have  $K(\alpha') = K(\alpha'')$ . In summary, the set of roots is partitioned by the stem fields into  $s_K(f)$  collections with  $r_K(f)$  roots in each collection, making  $r_K(f) \cdot s_K(f)$  the cardinality of the set of roots. ■

The symbol  $r_K(f)$  is determined both by the polynomial  $f$  and by the base field  $K$ . When  $K$  is understood, as it was earlier when  $K = \mathbf{Q}$ , the simpler notation  $r(f)$  can be used. There doesn't seem to be an established name for the quantity  $r_K(f)$ , and I propose: *root quantum number of  $f$  over  $K$* . While this name initially sounds rather fancy for a simple concept, the following theorem shows that the roots of  $f$  really do come bundled in collections of size  $r_K(f)$ .

**Theorem 2.** *Let  $f(X)$  in  $K[X]$  be irreducible. If  $L/K$  is a field extension (not necessarily algebraic), then the number of roots of  $f$  in  $L$  is a multiple of  $r_K(f)$ .*

*Proof.* The proof of Theorem 1 exhibits a partition of the set of roots of  $f$  into collections of equal size  $r_K(f)$ , where each collection has the property: in any field extension of  $K$ , the presence of one of the roots implies the presence of the remaining ones. ■

**Remark.** We can also see that the cardinality of the set of roots of  $f$  lying *outside* a given extension  $L/K$  (counted in an algebraically closed field containing  $L$ ) is a

multiple of  $r_K(f)$ . Theorem 1 shows that  $r_K(f)$  divides the total number of roots, and Theorem 2 shows that  $r_K(f)$  divides the number of roots in  $L$ , so  $r_K(f)$  also divides the difference of these two numbers.

**Corollary.** *If  $f(X)$  in  $\mathbf{Q}[X]$  is irreducible, then the number of real roots of  $f$  is a multiple of  $r_{\mathbf{Q}}(f)$ . The same can be said about the number of nonreal roots.*

*Proof.* Keeping the remark in mind, take  $L = \mathbf{R}$  in Theorem 2. ■

Theorem 2 may be summarized as follows: *roots appear in quanta*. This places combinatorial restrictions on the way  $f$  can factor. For example, if  $f(X)$  in  $K[X]$  is irreducible and separable of degree 15, with  $\alpha$  a root, then the factorization of  $f$  over  $K(\alpha)$  cannot have the following form:

$$(\text{linear})(\text{linear})(\text{linear})(\text{quadratic})(\text{quadratic})(\text{octic}).$$

To see this, assume for the sake of contradiction that the factorization of  $f$  over  $K(\alpha)$  has the form indicated. Since  $f$  is separable, the three linear factors correspond to distinct roots of  $f$  in  $K(\alpha)$ , so  $r_K(f) = 3$ . The field  $L$  obtained from  $K(\alpha)$  by adjoining the roots of the two quadratic factors has degree at most 4 over  $K(\alpha)$ . Thus  $L$  contains none of the roots of the octic factor, so  $L$  contains precisely seven of the roots of  $f$ . This contradicts the fact that the number of roots of  $f$  in  $L$  must be a multiple of three.

The interested reader can check that the root quantum number has the following three descriptions in terms of Galois theory. Let  $f$  be irreducible and separable over  $K$ , with Galois group  $G$ , viewed as a permutation group on the set of roots of  $f$ . Let  $H \subset G$  be the subgroup fixing a root  $\alpha$ . Then:

- i.  $r_K(f)$  is the number of roots fixed by  $H$ ;
- ii.  $r_K(f)$  is the cardinality of  $\text{Aut}(K(\alpha)/K)$ ; and
- iii.  $r_K(f)$  is the index  $[\text{N}_G(H) : H]$  of  $H$  in its normalizer.

Finally, it is instructive to think about the triples  $(K, n, r)$  that indicate the existence of an irreducible polynomial  $f(X)$  in  $K[X]$  of degree  $n$  with root quantum number  $r$ . The necessary condition discussed in this note is that  $r$  must divide  $n$ . Here are some exercises involving these triples:

1. Show that  $(\mathbf{Q}, 2, 1)$  does *not* appear.
2. Find a field  $K$  for which  $(K, 2, 1)$  *does* appear.
3. Let  $r$  divide  $n$ . Show that there exists  $K$  for which  $(K, n, r)$  appears.
4. (Advanced) Let  $r$  divide  $n$ . Except for  $(\mathbf{Q}, 2, 1)$ , show that  $(\mathbf{Q}, n, r)$  appears.

Solutions can be obtained from the author.

**ACKNOWLEDGMENTS.** David Marshall and Robert Perlis helped improve earlier versions of this note. Comments from two anonymous referees led to additional improvements. To all of you: my sincere thanks.

*Department of Mathematics, The University of Arizona, Tucson, Arizona, 85721-0089*  
*aprl@math.arizona.edu*