NORMAL ELEMENTS IN FINITE FIELDS

TREVOR HYDE

If L/K is a finite Galois field extension with Galois group G, then $\alpha \in L$ is called a *normal element* if the G-orbit of α forms a basis of L as a vector space over K. The normal basis theorem [4, Thm. 13.1] asserts that every finite Galois extension has a normal element.

If $\mathbb{F}_{q^n}/\mathbb{F}_q$ is an extension of finite fields, then there are finitely many normal elements in $\mathbb{F}_{q^n}$. We give a simple proof of a formula for $N_n(q)$ the number of normal elements in $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Theorem 1. *Let $p = \mathrm{char}(\mathbb{F}_q)$ and write $n = dp^m$ where p does not divide d. For e coprime to q let $o_e(q)$ denote the multiplicative order of q modulo e, and let φ be the Euler totient function. Then*

$$N_n(q) = q^n \prod_{e|d} \left(1 - \frac{1}{q^{o_e(q)}}\right)^{\varphi(e)/o_e(q)}.$$

Proofs of Theorem 1 appear in [1], [2, Cor. 2.4.7], [5, Sec. 1], and [7, Chp. 1, Thm. 12]. Ore [7, Pg. 251] attributes the problem of determining $N_n(q)$ to Eisenstein and the first complete solution to Hensel [3]. At the end of this note we discuss the relation between our proof and those mentioned above.

Our proof is based on Theorem 2 which describes a general relation between normal elements and units in the Galois group ring. This result was communicated to us by O'Desky and Rosen [6]. While Theorem 2 and its application to Theorem 1 may be known to experts, we did not find this in the literature. The aim of this note is to derive Theorem 1 with a simple, direct argument and to bring Theorem 2 to a wider audience.

Theorem 2 ([6])**.** *If L/K is a finite Galois extension with Galois group G, then the units $K[G]^\times$ in the group algebra for G over K act freely and transitively on the set of normal elements in L/K. In other words, the normal elements in L/K form a torsor for $K[G]^\times$.*

Proof. First suppose that $u \in K[G]^\times$ and α is a normal element. We claim that $\beta := u\alpha$ is a normal element. If for some $b_g \in K$

$$0 = \sum_{g\in G} b_g g\beta = \sum_{g\in G} b_g gu\alpha,$$

then α normal implies that $\sum_{g\in G} b_g gu = 0$ in $K[G]$. Dividing by u on the right gives $\sum_{g\in G} b_g g = 0$, hence $b_g = 0$ for all g. Thus the G-orbit of β is linearly independent, hence β is normal. Furthermore, by the normality of α, we see that $u\alpha = \alpha$ implies $u = 1$. This shows that $K[G]^\times$ acts freely on the normal elements in L/K.

Next we show $K[G]^\times$ acts transitively on normal elements. Suppose that α and β are both normal elements in L/K. Then for some $a_g, b_g \in K$ we have

$$\alpha = \sum_{g\in G} a_g g\beta \qquad\qquad \beta = \sum_{g\in G} b_g g\alpha.$$

If $u := \sum_{g\in G} a_g g$ and $v := \sum_{g\in G} b_g g$, then $\alpha = u\beta$ and $\beta = v\alpha$. Thus $uv\alpha = \alpha$ and $vu\beta = \beta$. Since α and β are normal elements this implies that $uv = 1 = vu$, hence v is a unit in $K[G]^\times$. Therefore every normal element β is a $K[G]^\times$ multiple of α. □

A weaker version of Theorem 2 appears implicitly in Suwa [11, Cor. 1.7] where it is traced back to an argument of Serre [10, Chp. IV, Prop. 7]. Their statement is an equivalence between the existence of a normal basis of a Galois algebra and of a certain pull-back diagram involving units in a group scheme associated to the Galois group ring.

Lemma 3 below is the function field analog of the classic formula for Euler's totient function

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

where the product on the right is taken over all prime divisors of n without multiplicity. Note that $\varphi(n)$ may be defined as the number of multiplicative units modulo n. Lemma 3 is well-known, see [9, Prop. 1.7] for example. We give a proof for completeness.

Lemma 3. *If $f(x) \in \mathbb{F}_q[x]$ is non-constant, then*

$$|(\mathbb{F}_q[x]/(f))^\times| = q^{\deg(f)}\prod_{p(x)|f(x)}\left(1-\frac{1}{q^{\deg(p)}}\right),$$

where the product is taken over all monic irreducible factors of $f(x)$ without multiplicity.

Proof. Let $\varphi(f) := |(\mathbb{F}_q[x]/(f))^\times|$. Then the probability of a uniformly random element of $\mathbb{F}_q[x]/(f)$ being a unit is, on one hand, simply $\varphi(f)/q^{\deg(f)}$. On the other hand, $u(x) \in (\mathbb{F}_q[x]/(f))^\times$ is equivalent to $u(x)$ not being divisible by any irreducible $p(x)$ dividing $f(x)$, and these events are independent for distinct monic irreducibles by the Chinese Remainder Theorem. Hence

$$\frac{\varphi(f)}{q^{\deg(f)}} = \prod_{p(x)|f(x)}\left(1-\frac{1}{q^{\deg(p)}}\right).$$ □

Proof of Theorem 1. The Galois group of $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of order n generated by the Frobenius automorphism $\sigma : a \mapsto a^q$. Therefore the group algebra $\mathbb{F}_q[\langle\sigma\rangle]$ is naturally isomorphic to $\mathbb{F}_q[x]/(x^n-1)$ by $\sigma \mapsto x$. Theorem 2 implies that the number of normal elements $N_n(q)$ is equal to the number of units in $\mathbb{F}_q[\langle\sigma\rangle]$, hence by Lemma 3

$$N_n(q) = |(\mathbb{F}_q[x]/(x^n-1))^\times| = q^n\prod_{p(x)|x^n-1}\left(1-\frac{1}{q^{\deg(p)}}\right). \tag{1}$$

If $n = dp^m$ where p does not divide d, then $x^n - 1 = (x^d-1)^{p^m}$ in $\mathbb{F}_q[x]$, hence the product (1) may be taken over irreducibles $p(x) \mid x^d-1$. By Galois theory these irreducible factors correspond to orbits of Frobenius on the dth roots of unity. The orbit of a primitive eth root of unity has length $o_e(q)$, the multiplicative order of q modulo e, and there are $\varphi(e)/o_e(q)$ such orbits. Hence

$$N_n(q) = q^n\prod_{e|d}\left(1-\frac{1}{q^{o_e(q)}}\right)^{\varphi(e)/o_e(q)}.$$ □

The proofs of Theorem 1 in [1, 3, 5, 7] use $\mathbb{F}_q$-linear polynomials to count normal elements in $\mathbb{F}_{q^n}/\mathbb{F}_q$. Recall that a polynomial $f(x) \in \mathbb{F}_q[x]$ is $\mathbb{F}_q$-*linear* (or simply *linear* when the field is understood,) if $f(ax+by) = af(x)+bf(y)$ for all $a, b \in \mathbb{F}_q$, or equivalently if $f(x) =$

$\sum_{i=0}^{d} a_i x^{q^i}$. Non-trivial linear polynomials are an essentially positive characteristic phenomenon and thus this approach gives the impression that the enumeration in Theorem 1 hinges on some special feature of positive characteristic fields. However, the ring of linear polynomials (with multiplication defined by composition) is isomorphic to the Galois group ring $\mathbb{F}_q[\langle\sigma\rangle]$, and the latter generalizes to Galois extensions in any characteristic. The important underlying structure is the free transitive action of the units in the Galois group ring on normal elements (Theorem 2) and the structure of finite fields only comes in to count $(\mathbb{F}_q[x]/(x^n-1))^\times$.

For example, if L/K is any degree n cyclic Galois extension, then each choice of normal element in L/K and generator of the Galois group provides an explicit bijection between all normal elements and units in the algebra $K[x]/(x^n-1)$.

Ore [7, Chp. 1] proves Theorem 1 by studying the minimal linear polynomial associated to each element of $\mathbb{F}_{q^n}$ and observing that normal elements are precisely those whose minimal linear polynomial is $x^{q^n}-x$. He then uses an inclusion-exclusion argument to arrive at the product formula (1). Akbik [1] independently came to essentially the same proof nearly 60 years later. Lenstra and Schoof [5, Sec. 1] give an exposition of Ore's proof in their work on primitive normal bases; the ideas behind our proof appear there between the lines. They describe Ore's results as pertaining to the Galois module structure of $\mathbb{F}_{q^n}/\mathbb{F}_q$, but neither explicitly state that the ring of linear polynomials is the group ring of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ nor refer to Theorem 2 directly. They do allude to the general connection between normal elements and units in the Galois group ring in their assertion [5, (1.15) Pg. 221].

Perlis [8, Lem. 1] gives a criterion for an element in $\mathbb{F}_{q^n}$ to generate an normal basis which is equivalent to Ore's characterization in terms of minimal linear polynomials. Gao [2, Pg. 18] notes that Perlis's result can be used to count the number of normal elements. Perlis [8, Thm. 1] also shows that normal elements may be detected by the non-vanishing of their trace, and Gao [2, Cor. 2.4.7] uses this to give another enumeration of normal elements.

Acknowledgments. We thank Andrew O'Desky for sharing Theorem 2 and clarifying its relation to the work of Suwa and Serre. We thank Julian Rosen and Mike Zieve for bringing references to our attention, in particular [2, 5, 7, 8]. We thank Darij Grinberg, Jeff Lagarias, Bob Lutz, Andrew O'Desky for helpful comments and feedback.

REFERENCES

[1] S. Akbik, Normal generators of finite fields, *J. Number Theory*, **41**, (1992), 146-149.
[2] S. Gao, Normal bases over finite field, Dissertation, *University of Waterloo*, (1993).
[3] K. Hensel, Über die Darstellun der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, *Journal für Mathematik*, **103**, (1888), 230-237.
[4] S. Lang, *Algebra*, **211**, Springer Science & Business Media, (2002).
[5] H. W. Lenstra, R. Schoof, Primitive normal bases for finite fields, *Math. Comp.*, **48**, No. 177, (1987), 217-231.
[6] A. O'Desky, J. Rosen, Group rings, normal bases, and étale algebras, in preparation.
[7] O. Ore, Contributions to the theory of finite fields, *Trans. Amer. Math. Soc.*, **36**, No. 2, (1934), 243-274.
[8] S. Perlis, Normal bases of cyclic fields of prime-power degree, *Duke Math. J.* **9**, No. 3, (1942), 507-517.
[9] M. Rosen, *Number Theory in Function Fields*, **210**, Springer Science & Business Media, (2002).
[10] J.-P. Serre, *Algebraic groups and class fields*, **117**, Springer Science & Business Media, (2012).
[11] N. Suwa, Around Kummer theories, RIMS Kôkyûroku Bessatu B12, (2009), 115-148.

E-mail address: tghyde@uchicago.edu