J. Group Theory **17** (2014), 667–669
DOI 10.1515/jgt-2013-0054 

# On a theorem of Carlitz

Michael E. Zieve

Communicated by Nigel Boston

**Abstract.** Carlitz proved that, for any prime power $q > 2$, the group of all permutations of $\mathbb{F}_q$ is generated by the permutations induced by degree-one polynomials and $x^{q-2}$. His proof relies on a remarkable polynomial which appears to have been found by magic. We show here that no magic is required: there is a straightforward way to produce a simple polynomial which has the same remarkable properties as the complicated polynomial in Carlitz's proof. We also identify the crucial subtlety which allows such simple polynomials to exist, and discuss some consequences.

The theorem in the title is as follows:

**Theorem 1.** *If $q > 2$ is a prime power, then every permutation of $\mathbb{F}_q$ is the composition of permutations induced by $x^{q-2}$ and by degree-one polynomials over $\mathbb{F}_q$.*

Betti proved this for $q = 5$ (as the final assertion in [2]), and Dickson proved it for $q = 7$, see [8, p. 119]. In response to a question posed by Straus, Carlitz proved it in general [3], via the following argument. It suffices to prove the result in the case where the permutation is a 2-cycle of the form $(0\ a)$ with $a \in \mathbb{F}_q^*$, since every permutation is a product of such 2-cycles. And Carlitz observed that $(0\ a)$ is the permutation of $\mathbb{F}_q$ induced by

$$f_a(x) := -a^2\left(\left((x-a)^{q-2} + \frac{1}{a}\right)^{q-2} - a\right)^{q-2}.$$

Although it is straightforward to verify that $f_a$ induces the permutation $(0\ a)$, it is not at all clear how one could have discovered the polynomial $f_a$ in the first place. Indeed, several authors have presented $f_a$ as a mysterious and complicated object: for instance, [14, p. 169] and [12, p. 358] assert that this representation of $(0\ a)$ demonstrates that "simplicity as polynomials and simplicity as permutations are not equivalent."

My purpose here is to remove the mystery from Carlitz's proof, by presenting a straightforward procedure for producing a simple polynomial which has the same crucial property as $f_a$, namely that of inducing the permutation $(0\ a)$. Note that the

The author was partially supported by NSF grant DMS-1162181.

rational function $\mu(x) := 1 - 1/x$ induces an order-3 permutation of $\mathbb{F}_q \cup \{\infty\}$, and one cycle of $\mu$ is $(\infty\ 1\ 0)$. Then $h(x) := 1 - x^{q-2}$ agrees with $\mu$ on $\mathbb{F}_q^*$, and $h$ interchanges 0 and 1, so $g(x) := h(h(h(x)))$ induces the permutation $(0\ 1)$ on $\mathbb{F}_q$. Thus $ag(x/a)$ induces the permutation $(0\ a)$.

The surprising feature of this proof – and of Carlitz's result, once we identify $x^{q-2}$ with $1/x$ – is that we have expressed each element of the symmetric group $S_q$ as a composition of degree-one rational functions, which should not be possible since the set $G$ of degree-one rational functions is closed under composition and $\#G = q^3 - q$ is typically much smaller than $q!$. However, the two notions of composition are incompatible in a subtle way, since we are not viewing an action of $G$: although we begin with the action of $G$ on $\mathbb{F}_q \cup \{\infty\}$, we must identify $\infty$ with 0 in order to view $1/x$ as a permutation of $\mathbb{F}_q$, but we cannot make a compatible identification for other degree-one rational functions such as $x + 1$.

Note that $x^{q-2}$ permutes $\mathbb{F}_{q^k}$ for infinitely many $k$: specifically, for all $k$ such that $q^k - 1$ is coprime to $q - 2$, which amounts to requiring that $k$ is not divisible by any of the numbers $r_\ell$, where $\ell$ is a prime factor of $q - 2$ and $r_\ell$ is the order of $q$ in $\mathbb{F}_\ell^*$. Thus, as noted by Carlitz [5, Theorem 1], any composition of degree-one polynomials and copies of $x^{q-2}$ will also permute these infinitely many extensions of $\mathbb{F}_q$, so any such composition is an *exceptional polynomial* (cf. [11] and the references therein). Hence Carlitz's result implies that every permutation of $\mathbb{F}_q$ is induced by an exceptional polynomial.

The condition $q > 2$ in the above theorem is needed only because $x^{q-2}$ does not permute $\mathbb{F}_q$ when $q = 2$. When $q = 2$, every permutation of $\mathbb{F}_q$ is represented by a degree-one polynomial.

Further results related to the above theorem are given in [1, 4, 6, 7, 9, 10, 13, 14].

**Acknowledgments.** The author thanks Bill Kantor for his encouragement to publish this note.

## Bibliography

[1] E. Aksoy, A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, On the Carlitz rank of permutation polynomials, *Finite Fields Appl.* **15** (2009), 428–440.

[2] E. Betti, Sopra la risolubilitá per radicali delle equazioni algebriche irriduttibili di grado primo, *Ann. Sci. Mat. Fis.* **2** (1851), 5–19 (*Opere Matematiche di Enrico Betti*, vol. 1, Accademia de Lincei, Milano (1903), 17–27).

[3] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.* **4** (1953), 538.

[4] L. Carlitz, A note on permutations in an arbitrary field, *Proc. Amer. Math. Soc.* **14** (1963), 101.

[5] L. Carlitz, Permutations in finite fields, *Acta Sci. Math. (Szeged)* **24** (1963), 196–203.

[6] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, Enumeration of a class of sequences generated by inversions, in: *Coding and Cryptology*, World Scientific, Hackensack (2008), 44–57.

[7] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* **14** (2008), 593–614.

[8] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* **11** (1896), 65–120.

[9] K. D. Fryer, A class of permutation groups of prime degree, *Canad. J. Math.* **7** (1955), 24–34.

[10] K. D. Fryer, Note on permutations in a finite field, *Proc. Amer. Math. Soc.* **6** (1955), 1–2.

[11] R. M. Guralnick, J. E. Rosenberg and M. E. Zieve, A new family of exceptional polynomials in characteristic 2, *Ann. of Math. (2)* **172** (2010), 1367–1396.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Addison–Wesley, Reading, 1983.

[13] R. M. Stafford, Groups of permutation polynomials over finite fields, *Finite Fields Appl.* **4** (1998), 450–452.

[14] C. Wells, Generators for groups of permutation polynomials over finite fields, *Acta Sci. Math. (Szeged)* **29** (1968), 167–176.

Received October 31, 2013.

**Author information**

Michael E. Zieve, Department of Mathematics, University of Michigan,
Ann Arbor, MI 48109–1043, USA;
and Mathematical Sciences Center, Tsinghua University,
Beijing 100084, P. R. China.
E-mail: zieve@umich.edu