Publ. Math. Debrecen
50 / 3-4 (1997), 257–263

On a conditional Cauchy functional equation involving powers of finite and number fields

By J. L. GARCÍA ROIG (Barcelona) and J. SALILLAS (Barcelona)

Abstract. In this paper we solve the conditional Cauchy equation $f(x^m + y) = f(x^m) + f(y)$, where f is a map from either a finite or a number field K into itself. We have naturally been led to the algebraic query of existence of an mth power generating a field extension, which is also established.

1. Introduction

The aim of this paper is to deal with the conditional Cauchy functional equation

$$f(x^m + y) = f(x^m) + f(y), \tag{1}$$

for $f : K \to K$, when K is either a finite or a number field, and m being a positive integer greater than 1. Of course in the elaboration of our results we have paid special attention to the case $m = 2$ before jumping to the general case.

In the case that K is a field of characteristic zero (in particular a number field), there are simple formulae coming from the calculus of finite differences (or other sources) which immediately yield the solutions of (1), but they leave us with an elementary algebraic problem, namely that of finding out whether a number field (finite over $\mathbb{Q}$) can be generated over $\mathbb{Q}$ by an mth power. We have proved that this is actually the case, which in turn yields an alternative way of solving (1).

However, in case of positive characteristic, the simple formulas mentioned above turn out to be useless and thus we have been led first to the

Mathematics Subject Classification: 39B52.
Key words and phrases: conditional Cauchy functional equation, field extension, finite fields, number fields, root of unity.

question of deciding when a finite field is generated by an mth power over its prime field before attacking functional equation (1).

2. The case of number fields

In this section we first solve functional equation (1) for the case f is a map from an arbitrary number field K (of finite degree over $\mathbb{Q}$) into itself and then ask for a purely algebraic question in connection with (1).

We start with a simple but useful lemma which works for any map $f : A \to B$ between two $\mathbb{Q}$-algebras A and B.

Lemma 1. *If f satisfies (1) then it also satisfies $f(0) = 0$ and for any positive integer s and any rational numbers $q_1, \dots, q_s$,*

$$f\left(\sum_{i=1}^{s} q_i x_i^m + y\right) = \sum_{i=1}^{s} q_i f(x_i^m) + f(y). \tag{1a}$$

Conversely, (1a) *obviously entails* (1).

Proof. Setting $x = y = 0$ in (1), we get $f(0) = 0$ (as usual with Cauchy functional equations).

Next we easily see recursively that, for any positive integer n,

$$f(nx^m + y) = nf(x^m) + f(y). \tag{2}$$

Now, if t is a positive integer,

$$f(x^m) = f\left(t^m \cdot \left(\frac{x}{t}\right)^m\right) = f\Big[\underbrace{\left(\frac{x}{t}\right)^m + \cdots + \left(\frac{x}{t}\right)^m}_{t^m \text{ terms}}\Big] = t^m f\left(\left(\frac{x}{t}\right)^m\right),$$

so that

$$f\left(\frac{x^m}{t^m}\right) = \frac{1}{t^m} f(x^m). \tag{3}$$

From (1), (2) and (3), if n and t are positive integers,

$$\begin{aligned} f\left(\frac{n}{t} \cdot x^m + y\right) &= f\left(nt^{m-1} \cdot \left(\frac{x}{t}\right)^m + y\right) = nt^{m-1} f\left(\left(\frac{x}{t}\right)^m\right) + f(y) \\ &= nt^{m-1} \cdot \frac{1}{t^m} f(x^m) + f(y) = \frac{n}{t} f(x^m) + f(y). \end{aligned}$$

This may be written as $f(qx^m + y) = qf(x^m) + f(y)$, for any positive rational q. For any such q, from

$$f(y) = f\left(qx^2 - qx^2 + y\right) = qf(x^2) + f(-qx^2 + y)$$

we see that $f(-qx^2+y) = -qf(x^2)+f(y)$ and, recursively, for any rationals $q_1, \ldots, q_s$

$$f\left(\sum_{i=1}^{s} q_i x_i^m + y\right) = \sum_{i=1}^{s} q_i f(x_i^m) + f(y). \qquad \square$$

Although we are primarily interested in number fields, the next theorem can be stated with more generality for $\mathbb{Q}$-algebras.

Theorem 1. *If A and B are $\mathbb{Q}$-algebras (not necessarily commutative) and $f : A \to B$ satisfies either* (1) *or* (1a) *then f is a solution of Cauchy functional equation, i.e. a $\mathbb{Q}$-linear map from A into B considered as $\mathbb{Q}$-vector spaces. (In particular this holds if $A = B$ is a number field.)*

Proof. This comes from the fact that, for any $\mathbb{Q}$-algebra (in particular for any number field K), any element is a linear combination with rational coefficients of mth powers, as a consequence of Theorem 402 on p. 325 of [H-W] (a result arising from the calculus of finite differences). $\square$

Remark. We could have used Fisher's result [F] setting, for instance, $x_2 = \ldots = x_n = 1$ instead of Theorem 402 in the preceding proof. In the special case $m = 2$, the polarization identity could also be used.

We next observe that an alternative way to deal with functional equation (1) is this: if we had known from scratch that K (or more generally any $\mathbb{Q}$-algebra) has a $\mathbb{Q}$-basis (as vector space) consisting entirely of mth powers, then the fact that (1) implies Cauchy would have been automatic. Obviously Theorem 402 of [H-W] entails this is indeed the case. In fact all mth powers are a generator system from which a basis can be selected. But this leads in the case of number fields (of finite degree over $\mathbb{Q}$) to a slightly stronger version of the question: Is K generated as a field extension of $\mathbb{Q}$ by an element which is an mth power? More generally, if $F|K$ is a finite extension field and $\operatorname{char} K = 0$ then does there exist an α in F such that $F = K(\alpha^m)$? We will next show that this is actually the case, and as a consequence (considering the successive powers of it) we will immediately have a K-basis of F consisting of mth powers.

Theorem 2 (cf. [L], Ch. V, Ex. 2, p. 253)**.** *Let $F|K$ be a finite extension field with* $\operatorname{char} K = 0$*, and let m be a positive integer. Then there exists α in F such that $F = K(\alpha^m)$.*

Proof. By the theorem of the primitive element (see [L], Ch. V, Therem 4.6, p. 243) we have $F = K(\beta)$ for some β in F. Let β have degree d over K, denote by $\beta_1 = \beta, \beta_2, \ldots, \beta_d$ the conjugates of β over

K, and consider $L := K(\beta_1, \ldots, \beta_d)$. As there are only finitely many mth roots of unity, there are infinitely many λ in K such that

$$\lambda \neq \frac{\zeta\beta_j - \beta_i}{1-\zeta}$$

for each distinct i, j between 1 and d, and for each mth root of unity $\zeta \neq 1$. It follows that for these λ and for all positive integers m, $(\beta_i + \lambda)^m$ are pairwise distinct for $i = 1, \ldots, d$, whence $F = K((\beta + \lambda)^m)$. □

Corollary. *A number field admits a $\mathbb{Q}$-basis consisting of mth powers.*

Remark. In special cases, Theorem 2 can still be refined. For instance, if $m = 2$, then it holds for any finite simple extension of an infinite field having characteristic $\neq 2$. Moreover, still in case $m = 2$, Theorem 2 also holds for finite fields: every finite field $\mathbb{F}_q$ is generated by a square over its prime field (see Remark 2c in the next section below).

3. The case of finite fields

Assume first that m is such that $\mathbb{F}_q$ ($q = p^n$, p prime) is generated as a field over its prime field $\mathbb{F}_p$ by an mth power, i.e. that there exists ξ in $\mathbb{F}_q$ such that $\mathbb{F}_q = \mathbb{F}_p(\xi^m)$. Then we have

Proposition 1. *If $f : \mathbb{F}_q \to \mathbb{F}_q$ satisfies functional equation* (1) *and $\mathbb{F}_q$ can be generated by an mth power over $\mathbb{F}_p$, then f satisfies Cauchy functional equation, i.e. f is an $\mathbb{F}_p$-linear map of $\mathbb{F}_q$ (considered as $\mathbb{F}_p$-space) into itself and, consequently, the number of solutions is q^n.*

Proof. Trivial, since (1) is obviously equivalent to

$$f\left(\sum_{i=1}^{s} n_i x_i^m + y\right) = \sum_{i=1}^{s} n_i f(x_i^m) + f(y), \tag{1b}$$

where the n_i's are in $\mathbb{F}_p$, (and may be thought of as positive integers less than p), and $\mathbb{F}_p(\xi^m) = \mathbb{F}_p[\xi^m]$. □

However, contrary to the case of characteristic 0, given m, not always may we assure that $\mathbb{F}_q$ is generated over $\mathbb{F}_q$ by an mth power. The simplest example of this is probably the case $m = q-1$ where $x^m = 1$, for all $x \in \mathbb{F}_q^*$ ($= \mathbb{F}_q \backslash \{0\}$). Thus we are led to pay attention to all such m. In what follows we can restrict our attention to exponents between 1 and $q-1$ (since $x^q = x$, for all x), and we begin with the simple

Lemma 2. *Let $q = p^n$, p prime. Then the field $\mathbb{F}_q$ is generated by an mth power over $\mathbb{F}_p$ if and only if there exists a divisor d of n, $d < n$, such that the integer $\frac{p^n-1}{p^d-1}$ divides m.*

Proof (cf. [L-N], Ch. 2 and 3). $\mathbb{F}_q$ is well-known to be generated over $\mathbb{F}_p$ by a primitive $(q-1)$th root of unity ζ, i.e. $\mathbb{F}_q = \mathbb{F}_p(\zeta)$, and that the group $\mathbb{F}_q^*$ is cyclic generated by ζ.

Suppose m is such that for all $\xi \in \mathbb{F}_q$ we have $\mathbb{F}_p(\xi^m) \neq \mathbb{F}_q$. In particular, $\mathbb{F}_p(\zeta^m) \neq \mathbb{F}_q$. Then $\mathbb{F}_p(\zeta^m)$ is a proper subfield of $\mathbb{F}_q$, necessarily of type $\mathbb{F}_{p^d}$, for $d|n$ and $d < n$. But, obviously, $\zeta^{\frac{p^n-1}{p^d-1}}$ is a primitive (p^d-1)th root of unity generating a (cyclic) group of order $p^d - 1$, and consequently $\mathbb{F}_{p^d} = \mathbb{F}_p\left(\zeta^{\frac{p^n-1}{p^d-1}}\right)$. Now, from the fact ζ^m belongs to the cyclic group generated by $\zeta^{\frac{p^n-1}{p^d-1}}$, as we may assume $m < p^n$, we infer the result. The converse is obvious. □

Remarks. 1) It is easy to see that there are exactly $\sum_{d|n} \mu(d)p^{n/d}$ (where μ is the Möbius function) primitive elements over $\mathbb{F}_p$ in $\mathbb{F}_{p^n}$ (see [L-N] Theorem 3.25, p. 84, or [L], Ch. V, Exercise 22, p. 255). For instance, if $p = 5$, $n = 6$, $\mathbb{F}_{5^6}$ has $5^6 = 15,625$ elements from which $5^6 - 5^3 - 5^2 + 5 = 15,480$ can serve as generators over $\mathbb{F}_5$.

2a) If $m = 2$, as any element of $\mathbb{F}_q$ is a sum of 2 squares (see [S], p. 34), it is clear that (1) is equivalent to the Cauchy functional equation.

2b) Furthermore, directly from the lemma we also observe that $\mathbb{F}_q$ can be generated as a field over $\mathbb{F}_p$ by a square: in fact if $p = 2$, all elements of $\mathbb{F}_q$ are squares and if $p > 2$ then $\frac{p^n-1}{p^d-1}$ is a divisor of 2 makes nonsense for $d|n$, $d < n$.

2c) However, an alternative proof of the assertion of 2b) can also be given: as for $p = 2$ all elements are squares, we can assume $p > 2$ and $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, for some $\alpha \in \mathbb{F}_q$. For $\lambda = 0, 1, \ldots, p-1$, consider the intermediate fields $\mathbb{F}_p\left((\alpha+\lambda)^2\right)$ which have index 1 or 2 with respect to $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha+\lambda)$. If one of these is of index 1, we are done. Otherwise all of them coincide and in particular $\mathbb{F}_p(\alpha^2 + 2\lambda\alpha) = \mathbb{F}_p(\alpha^2 + 2\mu\alpha)$ for $\lambda \neq \mu$. Subtracting $\alpha^2 + 2\lambda\alpha$ to $\alpha^2 + 2\mu\alpha$, we get $\alpha \in \mathbb{F}_p(\alpha^2 + 2\lambda\alpha)$, so that $\mathbb{F}_p(\alpha^2 + 2\lambda\alpha) = \mathbb{F}_p(\alpha)$. Notice however that no square in $\mathbb{F}_q^*$ generates the cyclic group $\mathbb{F}_q^*$, for q odd.

Theorem 3. *With the preceding notations, let m be such that $\mathbb{F}_p(\zeta^m) = \mathbb{F}_{p^d}$, for some proper divisor d of n. Then all solutions of the*

functional equation (1) *(or* (1b)*), for* $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$*, are obtained by setting*

$$f(z) = \begin{cases} f_0(z), & \text{if } z \in \mathbb{F}_{p^d}, \\ \varphi(y_i) + f_0(x), & \text{if } z \in \mathbb{F}_{p^n} \backslash \mathbb{F}_{p^d}, \end{cases}$$

where f_0 *stands for an arbitrary* $\mathbb{F}_p$*-linear map from* $\mathbb{F}_{p^d}$ *into* $\mathbb{F}_q$*,* φ *is an arbitrary map from a complete set of representatives* $\{y_2, \ldots, y_{\frac{n}{d}}\}$ *for the nontrivial cosets of* $\mathbb{F}_q$ *modulo* $\mathbb{F}_{p^d}$ *(i.e., where the trivial coset* $\mathbb{F}_{p^d}$ *has been excluded) into* $\mathbb{F}_q$*, and where we have written* $z = y_i + x$*, for a unique representative* y_i $\left(2 \le i \le \frac{n}{d}\right)$ *and a unique* $x \in \mathbb{F}_{p^d}$*.*

Thus there are $q^{\frac{n}{d}-1} \cdot p^{dn} = q^{\frac{n}{d}-1+d}$ *solutions of functional equation* (1)*.*

Proof. Any nonzero element of $\mathbb{F}_q$ is a power of ζ and consequently any mth power of an element of $\mathbb{F}_q$ lies in $\mathbb{F}_q(\zeta^m) = \mathbb{F}_{p^d}$. As any element of $\mathbb{F}_p(\zeta^m)$ can be written as a polynomial in ζ^m with coefficients in $\mathbb{F}_p$ (which are obviously sums of mth powers of 1) we see that functional equation (1) or (1b) is equivalent to the Cauchy functional equation

$$f(x + y) = f(x) + f(y) \tag{6}$$

restricted to the pairs (x, y) of $\mathbb{F}_{p^d} \times \mathbb{F}_{p^n}$.

Now it is easy to see (see [A-D], Section 16.2) that all solutions of (6) are obtained by combining any $\mathbb{F}_p$-linear map $f_0 : \mathbb{F}_{p^d} \to \mathbb{F}_{p^n}$ (there are of course $p^{dn} = q^d$ such maps) together with the arbitrary assignment of images to a complete set of representatives for the cosets of $\mathbb{F}_q$ modulo $\mathbb{F}_{p^d}$, once the null coset $\mathbb{F}_{p^d}$ has been excluded (there are $\frac{n}{d}$ cosets, i.e. $\frac{n}{d} - 1$ without the null-coset and thus, $q^{\frac{n}{d}-1}$ possibilities for these latter maps). The theorem now follows easily. □

Remark. For $d = n$ in Theorem 3 we obviously recover Proposition 1.

Acknowledgement. The authors thank the referees for their helpful suggestions and in particular for simplifying the proof of Theorem 2.

References

[A-D] J. Aczél and J. Dhombres, Functional Equations in Several Variables, *Cambridge Univ. Press*, 1989.

[F] I. Fisher, Sums of Like Powers of Multivariate Linear Forms, *Math. Magazine* **67** no. 1 (1994), 59-61.

[H-W] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., *Clarendon Press*, *Oxford*, 1989.

[L] S. Lang, Algebra, 3rd ed., *Addison-Wesley*, 1993.

[L-N] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, *Cambridge Univ. Press*, 1986.

[S] J-P. SERRE, A Course in Arithmetic, GTM 7. 2nd. ed., *Springer*, 1978.

J. L. GARCÍA ROIG
SECCIÓ MATEMÁTIQUES I INF. ETSAB
UNIVERSITAT POLITÉCNICA CATALUNYA
DIAGONAL 649
08028 BARCELONA
SPAIN

J. SALILLAS
SECCIÓ MATEMÁTIQUES I INF. ETSAV
UNIVERSITAT POLITÉCNICA CATALUNYA
PERE SERRA, 1–15
08190 SANT CUGAT DEL VALLÉS. BARCELONA
SPAIN

(Received January 19, 1996; revised June 10, 1996)