Aequationes Math. 60 (2000) 137–141
0001-9054/00/010137-5 \$ 1.50+0.20/0

Aequationes Mathematicae

On some questions concerning a functional equation involving Möbius transformations

Karanbir Singh Sarkaria

Summary. Given a field $\mathbb{F}$, is it true that any bijection which preserves the single operation $(x, y) \longmapsto (x+y)/(x-y)$ is necessarily a field automorphism? We show that the answer is "yes" for $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{F}_p$ with $p \neq 5$, or if $\mathbb{F}$ is a Galois extension of $\mathbb{Q}$ of degree 2^k, and "no" for $\mathbb{F} = \mathbb{F}_5$.

Mathematics Subject Classification (2000). Primary 39B99; Secondary 12E99.

The following problem, from an Olympiad training camp, was brought to my attention by V. K. Grover.

Problem. *Let f be any function from reals to reals such that*

$$f\left(\frac{x+y}{x-y}\right) = \frac{f(x)+f(y)}{f(x)-f(y)} \tag{1}$$

for all $x \neq y$. Show that $f(x) = x$ for all x.

Since any automorphism f of the field $\mathbb{R}$ of real numbers would of course satisfy (1), the above problem includes the well-known fact — see e.g. Lang [1], Ex. 25, p. 316 — that *the only field automorphism of $\mathbb{R}$ is the identity map.* Now, besides $\mathbb{R}$, there are lots of fields $\mathbb{F}$ having this property. So it is natural to enquire if the above problem generalizes to all such fields? In this context, my solution of the above problem gives the following.

Theorem 1. *Let $\mathbb{F} = \mathbb{R}$, or $\mathbb{Q}$, the field of rational numbers, or $\mathbb{F}_p$, a prime field of characteristic $p \neq 5$, and let f be a bijection of $\mathbb{F}$ for which* (1) *holds for all $x \neq y$. Then $f(x) = x$ for all x. On the other hand, the prime field $\mathbb{F}_5$ of characteristic* 5 *admits a non-identity bijection f which also satisfies* (1) *for all $x \neq y$.*

Proof. Postponing the exceptional cases $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_5$ till the very end, we shall first assume $\mathbb{F} = \mathbb{R}$, $\mathbb{Q}$, or $\mathbb{F}_p$, with $p \geq 7$.

For any $c \in \mathbb{F}$, one can find $x, y \in \mathbb{F}$ with $x \neq y$ such that $c = (x+y)/(x-y)$: if $c = 1$ take $x = 1$, $y = 0$, and if $c \neq 1$, take any y and $x = y(c+1)/(c-1)$. Then, interchanging these x and y in (1), we see that

$$f(-c) = -f(c) \text{ for all } c \in \mathbb{F}. \tag{2}$$

This implies, because $\mathrm{char}(\mathbb{F}) \neq 2$, that we must have

$$f(0) = 0. \tag{3}$$

Then, by using $x = 1$ and $y = 0$ in (1), we also get

$$f(1) = 1. \tag{4}$$

Also note that, on replacing y by $-y$ in (1), and using $f(-y) = -f(y)$ one gets

$$f\left(\frac{x-y}{x+y}\right) = \frac{f(x) - f(y)}{f(x) + f(y)}. \tag{5}$$

Any $c \neq -1$ can be written as $(x+y)/(x-y)$ by taking any x and $y = x(c-1)/(c+1)$. Substituting these in (1) we get

$$f(c) = \frac{f(x) + f\left(x\frac{c-1}{c+1}\right)}{f(x) - f\left(x\frac{c-1}{c+1}\right)},$$

which gives

$$f\left(\frac{c-1}{c+1}x\right) = \frac{f(c)-1}{f(c)+1}f(x) = f\left(\frac{c-1}{c+1}\right)f(x)$$

by (4) and (5).

Since any $r \neq 1$ can be written $(c-1)/(c+1)$, $c \neq -1$ — take $c = (-1-r)/(r-1)$ — this, and (4), show that f *is multiplicative*:

$$f(rx) = f(r)f(x), \text{ for all } r, x \in \mathbb{F}. \tag{6}$$

We are now ready to tackle $f(2) = z$, say. Since $\mathrm{char}(\mathbb{F}) \neq 2$, $2 \neq 0$, and so $z \neq 0$. Further, by using multiplicativity, (6), we see that $f(4) = z^2$. On the other hand, using (1) thrice as follows we get another formula for $f(4)$.

$$\begin{aligned}
f(3) &= f\left(\frac{2+1}{2-1}\right) = \frac{z+1}{z-1}, \\
f(5) &= f\left(\frac{3+2}{3-2}\right) = \frac{\frac{z+1}{z-1} + z}{\frac{z+1}{z-1} - z} = \frac{1+z^2}{1+2z-z^2}, \\
f(4) &= f\left(\frac{5+3}{5-3}\right) = \frac{\frac{1+z^2}{1+2z-z^2} + \frac{z+1}{z-1}}{\frac{1+z^2}{1+2z-z^2} - \frac{z+1}{z-1}} = \frac{4z}{-2-2z-2z^2+2z^3}.
\end{aligned}$$

Equating with z^2 gives $z^4 - z^3 - z^2 - z - 2 = 0$, i.e. $(z-2)(z+1)(z^2+1) = 0$. We cannot have $z = -1$, i.e. $f(2) = f(-1)$, for this implies $2 = -1$, i.e. that $\mathrm{char}(\mathbb{F}) = 3$. Likewise, we cannot have $z^2 = -1$, i.e. $f(4) = f(-1)$, for then $4 = -1$, i.e. $\mathrm{char}(\mathbb{F}) = 5$. Hence $z = 2$, i.e. we have shown that

$$f(2) = 2. \tag{7}$$

For the case $\mathbb{F} = \mathbb{Q}$ it suffices now, by multiplicativity, (6), to show that f also maps each odd prime $2k+1 \in \mathbb{Z} \subset \mathbb{Q}$ to itself. This follows by using $x = k+1$ and $y = k$ in (1), because by factorizing $k+1$ and k into smaller primes, we can assume inductively that $f(k+1) = k+1$ and $f(k) = k$ have already been verified. The same calculations, done $\bmod p$, also complete the proof for any $\mathbb{F} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with $p \geq 7$.

For the case $\mathbb{F} = \mathbb{R}$ these same calculations show, a priori, only that f is the identity map on the rationals $\mathbb{Q} \subset \mathbb{R}$. However, a real number is positive iff it is the square of a nonzero real: so by multiplicativity, (6), f maps positive reals to positive reals, and it follows by using $x > y > 0$ in (1), that f is *order preserving*. Since any real number is nested between two arbitrarily close rationals, this implies that f must be the identity map of $\mathbb{R}$.

The case $\mathbb{F} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ follows because there is only one non-identity bijection, viz. $0 \longmapsto 1$, $1 \longmapsto 0$, and this does not satisfy (1) for $x = 1$, $y = 0$. The case $\mathbb{F} = \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$ follows, because (3) and (4) are still valid, and so f, being a bijection, must also take the remaining element, 2, to itself.

For the case $\mathbb{F} = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0,1,2,3,4\}$, we still have (2)–(4), so the only possible non-identity bijection f is $0 \longmapsto 0$, $1 \longmapsto 1$, $4 \longmapsto 4$, $2 \longmapsto 3$, $3 \longmapsto 2$. Obviously (1) holds for f if $x = -y$, so to establish (1) for all $x \neq y$, it remains only to verify it for $(x,y) = (1,2)$, $(1,3)$, $(2,4)$ and $(3,4)$, which is easily done. $\square$

The above is, by no means, a complete list of fields $\mathbb{F}$ for which the only field automorphism is the identity map. For example, one has also the fields $\mathbb{Q}_p$ of p-adic numbers — see e.g. Lang [1], Ex. 3, p. 312 — and, as was pointed out to me by R. N. Gupta, say the field $\mathbb{Q}(2^{\frac{1}{3}})$ obtained by attaching to $\mathbb{Q}$ the real cube root of 2. I expect that the above problem generalizes to many such fields, e.g. to the p-adics, but also that it fails for many others.

Turning to a quite general field $\mathbb{F}$, one can ask if a bijection f which satisfies (1) is necessarily a field automorphism? In this context, my solution of the above problem also gave the following.

Theorem 2. *Let $\mathbb{F}$ be a Galois extension of $\mathbb{Q}$ of degree 2^k, and let f be a bijection of $\mathbb{F}$ which satisfies* (1) *for all $x \neq y$. Then f must be a field automorphism of $\mathbb{F}$.*

Proof. First, note that the proof of Theorem 1 shows that f is multiplicative, and that its restriction $f \mid \mathbb{Q}$ is the identity automorphism of the rational subfield $\mathbb{Q} \subset \mathbb{F}$.

Also, since $\mathbb{F}$ is Galois of degree 2^k over $\mathbb{Q}$ it can be obtained from $\mathbb{Q}$ by succesively attaching k square roots; or, in case $i \in \mathbb{F}$, from $\mathbb{Q}(i)$ by succesively attaching $k-1$ square roots. So, without loss of generality, we can assume that $\mathbb{F}$ is a quadratic extension $\mathbb{G}(\alpha^{\frac{1}{2}})$, $\alpha \in \mathbb{G}$, of a subfield $\mathbb{G}$, such that $f \mid \mathbb{G}$ is a field automorphism of $\mathbb{G}$, and that, if $i \in \mathbb{F}$ then, either $\alpha^{\frac{1}{2}} = i$ and $\mathbb{G} = \mathbb{Q}$, or else $i \in \mathbb{G}$.

By multiplicativity, f must map the square root $\alpha^{\frac{1}{2}}$ of α, either to itself, or to the other squre root $-\alpha^{\frac{1}{2}}$ of α. Let ϕ denote the field automorphism of $\mathbb{F}$ which coincides with f on $\mathbb{G}$ and on the element $\alpha^{\frac{1}{2}}$. So, since any element of $\mathbb{F}$ is of the type $a + b\alpha^{\frac{1}{2}}$, with $a, b \in \mathbb{G}$, it follows by (1) that the value of f, on any square

$$(a + b\alpha^{\frac{1}{2}})^2 = (a^2 - b^2\alpha)\frac{a + b\alpha^{\frac{1}{2}}}{a - b\alpha^{\frac{1}{2}}},$$

is precisely the same as the value of ϕ on it.

Hence, for any $z \in \mathbb{F}$, we have $(f(z))^2 = (\phi(z))^2$, and thus $f(z) = \pm\phi(z)$. If $f(z) = -\phi(z)$, by using (1), we see that

$$\pm\frac{\phi(z)+1}{\phi(z)-1} = \pm\phi\left(\frac{z+1}{z-1}\right) = f\left(\frac{z+1}{z-1}\right) = \frac{f(z)+1}{f(z)-1} = \frac{-\phi(z)+1}{-\phi(z)-1} = \frac{\phi(z)-1}{\phi(z)+1},$$

which gives $\left(\frac{\phi(z)+1}{\phi(z)-1}\right)^2 = \pm 1$, i.e. $\frac{\phi(z)+1}{\phi(z)-1} = \pm 1$ or $\pm i$; so $\phi(z) = 0$ or $\pm i$, i.e. $z = 0$ or $\pm i$. However, on these elements, $f(z) = \phi(z)$; so we must have $f(z) = \phi(z)$ for all $z \in \mathbb{F}$. $\square$

To conclude, I remark that the bijections f of $\mathbb{F}$ which satisfy (1) form a *group* containing the group Gal($\mathbb{F}$) of all field automorphisms of $\mathbb{F}$. More generally, for any integer matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{Z})$, one can consider the group $G_A(\mathbb{F})$ of all bijections f of $\mathbb{F}$ satisfying

$$f\left(\frac{ax+by}{cx+dy}\right) = \frac{af(x)+bf(y)}{cf(x)+df(y)}. \tag{8}$$

Clearly $\cap_A G_A(\mathbb{F})$ =Gal($\mathbb{F}$), however it might well be that one can find a single A for which $G_A(F)$ =Gal($\mathbb{F}$)?

Acknowledgement. I am grateful to the referee for pointing out a mistake in my original argument for Theorem 2.

Note added in proof. The problem with which this paper starts was proposed, with the extra condition that f is continuous, by R. S. Luthar in the *Americal Mathematical Monthly* of 1969: E2176, 554. One of its solvers, S. Reich, pointed out that the continuity hypothesis was not needed: see *Americal Mathematical Monthly 78* (1971), 675.

Reference

[1] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

K. S. Sarkaria
Department of Mathematics
Panjab University
Chandigarh 160014
India

Manuscript received: April 12, 1999 and, in final form, August 23, 1999.