IMO 2012 A5

Problem

Let R be a commutative ring and S be a field. Find all functions $f : R \to S$ such that, for any $x, y \in R$,

$$f(xy + 1) - f(x + y) = f(x)f(y). \tag{*}$$

Warning. This problem is an extremely buffed version of the original problem with $R = S = \mathbb{R}$ and without the condition $f(-1) \neq 0$. The original problem seems to be of difficulty level A5. If $f(-1) = 0$ is allowed, then the difficulty level would only rise to A6 in the modern era. Note that Cauchy's functional equation $(f(x + y) = f(x) + f(y))$ becomes well-known nowadays.

However, I believe that the difficulty level of this problem is way beyond the IMO. The official solution and the simplest solution for the case $f(-1) = 0$ does not work in general since it relies on the properties of $\mathbb{R}$.

Answer

The solutions can be described via the following nine classes of functions. For the 8th class, $\phi, \psi \in S$ satisfies $\phi + \psi = 1$ and $\phi\psi = -1$. The map into the intermediate ring is necessarily a ring homomorphism in this context.

Class	Intermediate ring	Map to S
1	0	$0 \mapsto 0$
2	S	$x \mapsto x - 1$
3	S	$x \mapsto x^2 - 1$
4	$\mathbb{F}_2$	$[0, 1] \mapsto [-1, 0]$
5	$\mathbb{F}_3$	$[0, 1, 2] \mapsto [-1, 0, 1]$
6	$\mathbb{F}_3$	$[0, 1, 2] \mapsto [-1, 0, 0]$
7	$\mathbb{Z}/4\mathbb{Z}$	$[0, 1, 2, 3] \mapsto [-1, 0, 1, 0]$
8	$\mathbb{F}_2[X]/\langle X^2 \rangle$	$[0, 1, X, X + 1] \mapsto [-1, 0, 1, 0]$
9	$\mathbb{F}_4$	$[0, 1, X, X + 1] \mapsto [-1, 0, \phi, \psi]$

Solution

I will present a very long and technical solution. The solution seems to be generalizable to the case where R is not necessarily commutative. Most parts of the solution only requires S to be a domain, not even commutative. Also, most parts can be done without assuming that R is commutative. However, one part seems to require that S is a field.

Regardless, `mathlib`'s API for ideal quotient of a ring (`ideal.quotient`) only supports commutative rings. Another possibility is using `ring_con` to construct the quotients, but I found it hard to use. Thus, to avoid complications, we will assume that R is commutative. We also assume that S is an integral domain for the same reason and for the benefit of access to the `ring` tactic.

Step 1: Small observations

One can check manually that all functions described above works. We now focus on showing that they are all the solutions.

Plugging $x = y = 1$ into (*) yields $f(1) = 0$. Now plugging $y = 0$ into (*) yields $-f(x) = f(x)f(0)$ for all $x \in R$. This means that we have

$$f \equiv 0 \text{ or } f(0) = -1. \tag{1.1}$$

From now on, we assume that $f(0) = -1$.

Plugging $y = -1$ into (*) yields

$$f(1 - x) - f(x - 1) = f(x)f(-1) \quad \forall x \in R. \tag{1.2}$$

This also implies

$$f(-x) - f(x) = f(x + 1)f(-1) \quad \forall x \in R. \tag{1.3}$$

In particular, the case $f(-1) = 0$ yields that f is even.

Step 2: Ring quotients

We construct an ideal I of R such that f is constant on the cosets of I. We define the two ideals

$$J = \{c \in R : \forall x \in R, f(cx + 1) = 0\}, \tag{2.1}$$

$$I = \{c \in R : \forall x \in R, f(c + x) = f(x)\}. \tag{2.2}$$

Lemma 1. *For any $c \in R$, we have $c \in J$ if and only if $f(c + x) = -f(c)f(x)$ for all $x \in R$. The set J is an ideal of R.*

Proof. The first part is clear since $f(cx + 1) - f(c + x) = f(c)f(x)$. For the second part, closure under addition is easy to prove from the equation $f(c + x) = -f(c)f(x)$. Meanwhile, closure under multiplication in R follows from the equation $f(cx + 1) = 0$. Finally, $f(1) = 0$ yields $0 \in J$. $\square$

For any $c \in J$, we have $f(c + 1) = -f(c)f(1) = 0$. Thus, (1.3) yields $f(-c) = f(c)$. The above lemma yields $-1 = f(0) = -f(-c)f(c) = -f(c)^2$, so

$$f(c) = \pm 1 \quad \forall c \in J. \tag{2.3}$$

Lemma 2. *For any $c \in R$, we have $c \in I$ if and only if $c \in J$ and $f(c) = -1$. The set I is an ideal of R.*

Proof. If $c \in I$, then $f(c) = f(0) = -1$, and $c \in J$ holds by the previous lemma. The converse is also easy to check. Now we prove that I is an ideal of R. It is easily a subgroup of R, so we just need to prove closure under multiplication over R.

Let $c \in I$ and $d \in R$. It suffices to show that if $d \notin J$, then $dc \in I$. In the more general case, $d \in J$ would imply $d - 1, 1 \notin J$, and then $(d - 1)c, c \in I$ and thus $dc \in I$. Thus, we now assume that $d \notin J$.

Since $f(c + y) = f(y)$ for all $y \in R$, (*) yields $f(d(c + x) + 1) = f(dx + 1)$ for all $x \in R$. Since J is an ideal containing I, we have $cx \in J$. That means we have $-f(dc)f(dx + 1) = f(dx + 1)$ for all $x \in R$. Fixing x, this implies either $f(dc) = -1$ or $f(dx + 1) = 0$ for all $y \in R$. Since we assumed $d \notin J$, the latter does not hold. The former together with $c \in J$ and the previously proved statement yields $dc \in I$. $\qquad\square$

For any $a, b \in R$ such that $a - b \in I$, it is clear that $f(a) = f(b)$. Thus, we get an induced map $g : R/I \to S$ such that $f = g \circ \phi$, where $\phi : R \to R/I$ is the quotient map. Since ϕ is surjective, one can check that g satisfies (*) as well. Thus, from now on, we can WLOG assume that $I = \{0\}$ whenever necessary.

Lemma 3. *Suppose that $I \subsetneq J$, and fix some $c \in J \setminus I$. Then $R/I = \{[0], [1], [c], [c + 1]\}$, where the bracket denotes quotient mod I.*

Proof. First note that $|J/I| = 2$. Indeed, consider any $c, d \in J \setminus I$. By Lemma 1, it is easy to check that $f(c - d) = f(0) = -1$. Thus, by Lemma 2, $c - d \in I$, so $[c] = [d]$.

Now fix the unique element $c \in J \setminus I$. We claim that if $d \notin J$, then $dc \notin I$. This suffices to prove the lemma as follows. If $d \notin J$, we have $dc, c \in J \setminus I$. The previous paragraph yields $(d - 1)c = dc - c \in I$. Now the claim implies $d - 1 \in J$. As a result, we have either $d \in J$ or $d - 1 \in J$. Since $J/I = \{[0], [c]\}$, this yields $[d] \in \{[0], [1], [c], [c + 1]\}$. This would prove the lemma.

We now prove the claim. Fix $d \notin J$; our goal is to show that $dc \notin I$. Since $d \notin J$, we can choose $x \in R$ such that $f(dx + 1) \neq 0$. By definition of I, it suffices to show that $f(dc + dx + 1) \neq f(dx + 1)$.

Since $c \in J \setminus I$, we have $f(c) = 1 \neq -1$ and thus

$$f(d(c + x) + 1) = f(d + c + x) + f(d)f(c + x) = -(f(d + x) + f(d)f(x)) = -f(dx + 1).$$

But $1 \neq -1$ in S and $f(dx + 1) \neq 0$ yields $-f(dx + 1) \neq f(dx + 1)$. THis proves that $f(dc + dx + 1) \neq f(dx + 1)$. $\qquad\square$

Step 3: Case 1: $f(-1) \neq 0$

The results displayed here are relevant up to Step 5.

Here, (1.3) yields

$$f(-x + 1) = -f(x + 1) \quad \forall x \in R. \tag{3.1}$$

In particular, since $f(0) = -1$, we have

$$f(2) = 1. \tag{3.2}$$

Plugging (3.1) back into (1.2) yields

$$f(x + 1) + f(x - 1) = -f(x)f(-1) \quad \forall x \in R. \tag{3.3}$$

For any $y \in R$, plugging $x = 2$ into (*) yields $f(2y + 1) = f(y) + f(y + 2)$. Applying (3.1) and (1.3) then yields

$$f(2y + 1) = -f(y + 1)f(-1) \quad \forall y \in R. \tag{3.4}$$

This is sufficient to compute $f(-1)$.

Claim. *We have $f(-1) \in \{-2, 1\}$.*

Proof. For convenience, let $C = f(-1)$. By (3.1), we get $f(3) = -C$. Now, by (3.4), we have $f(5) = C^2$. On the other hand, by (3.3) and $f(2) = 1$ (from (3.2)), we get

$$C^2 = f(5) = -f(4)C - f(3) = -f(4)C + C = (1 - f(4))C.$$

3

Since the case's hypothesis implies $C \neq 0$, this implies $C = 1 - f(4)$. Computing $f(4)$ using (3.3) again gives

$$f(4) = -f(3)C - f(2) = C^2 - 1 \implies C = 1 - (C^2 - 1) \iff C^2 - 1 = 1 - C.$$

Since $C^2 - 1 = (C+1)(C-1)$, this yields either $C + 1 = -1$ or $C - 1 = 0$. Respectively, they give $C = -2$ and $C = 1$. □

Before continuing with the subcases, we have some more useful observations. Compare the (*) with the same equality but with (x, y) replaced by $(-x, -y)$. Subtracting yields

$$f(x+y) - f(-x-y) = f(-x)f(-y) - f(x)f(y) \quad \forall x, y \in R. \tag{3.5}$$

Applying (1.3) yields

$$-f(x+y+1)f(-1) = f(-x)f(-y) - f(x)f(y) \quad \forall x, y \in R. \tag{3.6}$$

Plugging $x = y$ and applying (3.4) again into the above equation yields

$$f(x+1)f(-1)^2 = f(-x)^2 - f(x)^2 = (f(-x) - f(x))(f(-x) + f(x)).$$

By (1.3), we get

$$f(x+1)f(-1)^2 = f(x+1)f(-1)(f(-x) + f(x)).$$

Since $f(-1) \neq 0$, we get that for any $x \in R$,

$$f(x+1) \neq 0 \text{ implies } f(-x) + f(x) = f(-1) \quad \text{for any } x \in R. \tag{3.7}$$

Finally, before we move on to the two subcases, we prove that

$$f(x+1) = 0 \text{ implies } f(-x) = f(x) = -1 \quad \text{for any } x \in R. \tag{3.8}$$

Suppose that $f(x+1) = 0$. Plugging $y = x + 1$ into (3.5) gives us

$$f(2x+1) - f(-2x-1) = f(-x)f(-x-1).$$

By (3.4), we get

$$f(2x+1) - f(-2x-1) = -f(x+1)f(-1) + f(-x)f(-1) = f(-x)f(-1).$$

On the other hand, plugging $y = -x - 1$ into (3.5) (or (3.6)) gives us

$$f(-1) = -f(x)f(-x-1).$$

Since $f(x+1) = 0$, (1.3) yields $f(-x) = f(x)$, so

$$f(-1) = -f(-x)f(-x-1) = -f(-x)f(-1).$$

Finally, since $f(-1) \neq 0$, this yields $f(-x) = 1$. Since we already have $f(-x) = f(x)$, we have proved (3.8).

We now split into two subcases.

4

Step 4: Subcase 1.1: $f(-1) = -2 \neq 0$

Here, we consider the subcase where $f(-1) = -2 \neq 0$. Note that this also means that $\text{char}(S) \neq 2$. We claim that $f + 1$ is a ring homomorphism from R to S. That is, $f + 1$ is both additive and multiplicative. This corresponds to the class 2 solutions.

Combining (3.7) and (3.8) yields

$$f(-x) + f(x) = -2 \quad \forall x \in R. \tag{4.1}$$

On the other hand, (1.3) gives us $f(-x) - f(x) = -2f(x+1)$ for all $x \in R$. Subtracting the second equation from the first equation yields $2f(x) = 2f(x+1) - 2$. Since $2 \neq 0$ in S, this gives us

$$f(x+1) = f(x) + 1. \tag{4.2}$$

We first show that $f + 1$ is additive. That is, $f(x+y) = f(x) + f(y) + 1$ for all $x, y \in R$. Indeed, recall (3.6):

$$2f(x+y+1) = -f(x+y+1)f(-1) = f(-x)f(-y) - f(x)f(y).$$

Applying (4.2) on the left hand side and (4.1) on the right hand side gives

$$2(f(x+y)+1) = (-f(x)-2)(f(y)-2) - f(x)f(y) = 2(f(x)+f(y)+2).$$

Again, $2 \neq 0$ in S, so we get $f(x+y) + 1 = f(x) + f(y) + 2$ for any $x, y \in R$.

Finally, we give a quick proof that $f + 1$ is multiplicative. We just go back to (*). For any $x, y \in R$,

$$\begin{aligned}
f(xy) + 1 &= f(xy+1) \\
&= f(x)f(y) + f(x+y) \\
&= f(x)f(y) + f(x) + f(y) + 1 \\
&= (f(x)+1)(f(y)+1).
\end{aligned}$$

Step 5: Subcase 1.2: $f(-1) = 1 \neq -2$

Here, we consider the subcase where $f(-1) = 1 \neq -2$. This also means that $\text{char}(S) \neq 3$. The solution in this subcase corresponds to class 5 solutions. That is, we claim that f factors through a ring homomorphism $R \to \mathbb{F}_3$.

Recall the definition of the ideal I as in (2.2):

$$I = \{c \in R : \forall x \in R, f(c+x) = f(x)\}.$$

By our work in Step 2 (mainly Lemma 2), we can assume WLOG that $I = 0$. With this assumption, it suffices to show that $R \cong \mathbb{F}_3$. Note that the values $f(-1) = 1$, $f(0) = -1$, and $f(1) = 0$ are already known in this subcase.

First we prove that for any $c \in R$,

$$f(c+1) = 0 \text{ implies } c \in I \text{ implies } c = 0. \tag{5.1}$$

Indeed, (3.8) yields $f(-c) = f(c) = -1$, and thus plugging $x = c$ into (3.6) yields

$$-f(c+y+1) = -f(c+y+1)f(-1) = -(f(-y) - f(y)) \quad \forall y \in R.$$

But (1.3) yields $f(-y) - f(y) = f(y+1)f(-1) = f(y+1)$. Replacing y with $x - 1$ yields $f(c+x) = f(x)$ for all $x \in R$, i.e., $c \in I$.

Now we go back to the main goal. In this step, (3.3) reads as

$$f(x+1) + f(x-1) = -f(x) \iff f(x-1) + f(x) + f(x+1) = 0. \tag{5.2}$$

In particular, it is easy to see that $f(x+2) = f(x-1)$ for any $x \in R$. Thus $3 \in I$, and so char$(R) = 3$; note that R cannot be trivial since $f(0) = -1 \neq 0 = f(1)$.

Finally, we show that $x \in \{-1, 0, 1\}$ for any $x \in R$. Note that by (5.1), (3.7) now reads as

$$x \neq 0 \text{ implies } f(-x) + f(x) = 1. \tag{5.3}$$

Suppose for the sake of contradiction that $x \notin \{-1, 0, 1\}$. Then $x, x+1, x-1 \neq 0$, so we get

$$f(-x) + f(x) = f(-(x+1)) + f(x+1) = f(-(x-1)) + f(x-1) = 1.$$

Summing all three equations and using (5.2) yields $3 = 0$. A contradiction, since char$(S) \neq 3$.

Step 6: Case 2: $f(-1) = 0$

This covers the rest of the solution, which consists of four subcases. The Subcase 2.3 needs to steal some results from Subcase 2.1. The details will come later.

As before, we collect important equations here and do an important computation. We computed $f(-1)$ in the previous case; now we will compute $f(2)$ instead.

Note that (1.3) only yields that f is even, i.e.,

$$f(-x) = f(x) \quad \forall x \in R. \tag{6.1}$$

Replacing y with $-y$ in (*) now gives

$$f(xy - 1) - f(x - y) = f(x)f(y) \quad \forall x, y \in R. \tag{6.2}$$

Plugging $y = x$ into the above equation yields

$$f(x^2 - 1) = f(x)^2 - 1 \quad \forall x \in R. \tag{6.3}$$

Since $f(-1) = 0$, plugging $y = x + 1$ into (6.2) gives

$$f(x(x+1) - 1) = f(x)f(x+1) \quad \forall y \in R. \tag{6.4}$$

Next, consider (*) with $y = 2$. We apply it twice on the equation $f(2x+1) = f(-2x-1)$. Together with the fact that f is even, we get

$$f(x+2) + f(2)f(x) = f(x-1) + f(2)f(x+1).$$

This can be rewritten as

$$f(x+2) = f(2)(f(x+1) - f(x)) + f(x-1) \quad \forall x \in R. \tag{6.5}$$

Claim. *We have*

$$f(2) \in \{-1, 0, 1, 3\}.$$

Proof. For convenience, let $C = f(2)$. We start with $f(3) = C^2 - 1$ from (6.3). Next we have $f(4) = f(2)(f(3) - f(2)) = C(C^2 - 1 - C)$ from (6.5). Finally, we compute $f(5)$ in two ways, one using (6.4) and one using (6.5):

$$f(5) = f(2)f(3) = C(C^2 - 1),$$

6

$$f(5) = f(2)(f(4) - f(3)) + f(2) = C(C(C^2 - 1 - C) - (C^2 - 1)) + C.$$

That is, we have
$$C^2 + C(C^2 - 1 - C) = C(C(C^2 - 1 - C) - (C^2 - 1)) + C,$$

which rearranges to
$$C(C-1)(C-3)(C+1) = 0.$$

This proves the claim. □

Before bashing the four subcases, we prove an equality based on the polynomial identity
$$x(x+1) - 1 = (x-1)(x+2) + 1 = x^2 + x - 1.$$

Plugging $(x, y) \mapsto (x - 1, x + 2)$ yields
$$f(x)f(x+1) = f(x^2 + x - 1) = f(x-1)f(x+2) + f(2x+1) \quad \forall x \in R.$$

Since $f(1) = 0$, applying (*) with $y = 2$ and applying (6.4) yields
$$f(x)f(x+1) - f(x-1)f(x+2) = f(2)f(x) + f(x+2) \quad \forall x \in R. \tag{6.6}$$

Step 7: Subcase 2.1: $f(2) = 0 \neq 3$

Here, we consider the subcase where $f(2) = 0 \neq 3$. This also means that $\text{char}(S) \neq 3$. The solution in this subcase corresponds to class 6 solutions. That is, we claim that f factors through a ring homomorphism $R \to \mathbb{F}_3$. Note we already know that $f(0) = -1$ and $f(-1) = f(1) = 0$.

Recall the definition of the set I as in (2.2):
$$I = \{c \in R : \forall x \in R, f(c+x) = f(x)\}.$$

As in Step 5, we can assume WLOG that $I = 0$. From (6.5), we get $3 \in I \iff 3 = 0$ in R. Plugging the value of $f(2)$ into (6.6) gives
$$f(x)f(x+1) - f(x-1)^2 = f(x-1) \quad \forall x \in R. \tag{7.1}$$

Replacing x with $x + 1$ and using the fact that $3 = 0$ in R, we get
$$f(x+1)f(x-1) - f(x)^2 = f(x).$$

Subtracting the two equalities and factoring gives
$$f(x) = f(x-1) \text{ or } f(x-1) + f(x) + f(x+1) = -1 \quad \forall x \in R. \tag{7.2}$$

We show that
$$f(c+1) = f(c-1) = 0 \text{ implies } c = 0 \quad \forall c \in R. \tag{7.3}$$

It suffices to show that $f(c + x) = f(x)$ for all $y \in R$. Indeed, assume that $f(c+1) = f(c-1) = 0$. By (*), we get the equations
$$f((c+1)x + (c-1)) = f((c^2 - 1)x + 1) = f((c-1)x + (c+1)),$$

which can be rewritten as
$$f((c+1)(x+1) + 1) = f((c-1)(x+1) - 1)$$

7

since $2 = -1$ in R. Now apply (6.2) on the left hand side and (*) again on the right hand side. We get $f(x + c + 2) = f(x - c + 2)$ for any $x \in R$. Now replace x with $x - 2 - c$ and use the fact that $2 = -1 \in R$ again to finish. This proves (7.3).

Now we can show that the second equality in (7.2) must always hold. That is, we have

$$f(x - 1) + f(x) + f(x + 1) = -1 \quad \forall x \in R. \tag{7.4}$$

Suppose for the sake of contradiction that this does not hold. Then (7.2) tells us that $f(x) = f(x + 1) = f(x - 1)$. Plugging into (7.1) gives us $f(x) = f(x + 1) = f(x - 1) = 0$. Then (7.3) yields $x = 0$; but $f(0) = -1 \neq 0$, a contradiction. This proves (7.4).

Next, we show that

$$f(x) \in \{0, -1\} \quad \forall x \in R. \tag{7.5}$$

By (*), (7.1), and the fact that $2 = -1$ in R, we get

$$f(x^2) = f(x + 1)f(x - 1) + f(2x) = f(x)^2 + f(x) + f(-x) = f(x)^2 + 2f(x)$$

and

$$f(x^2 + 1) = f(x)^2 + f(2x) = f(x)^2 + f(x).$$

Now we add the two equalities and also add with (6.3) to get

$$f(x^2) + f(x^2 + 1) + f(x^2 - 1) = 3f(x)^2 + 3f(x) - 1.$$

Using (7.4) gives us $3f(x)^2 + 3f(x) = 0$. Together with char$(S) \neq 3$, this proves (7.5).

Finally, we show that $R \cong \mathbb{F}_3$, i.e., $x \in \{-1, 0, 1\}$ for any $x \in R$. By (7.5), each of $f(x)$, $f(x + 1)$, and $f(x - 1)$ takes the value 0 or -1. By (7.4), at least one of the three expressions must be equal to -1. Thus it now suffices to show that

$$f(x) = -1 \text{ implies } x = 0 \quad \forall x \in R. \tag{7.6}$$

Proof. Fix $x \in R$ and suppose that $f(x) = -1$. By (7.3), it suffices to show that $f(x + 1) = f(x - 1) = 0$. Since $f(x) = -1$, (7.4) yields $f(x + 1) + f(x - 1) = 0$. On the other hand, (7.1) with x replaced by $x + 1$ yields $f(x + 1)f(x - 1) = 0$. The two equations yields $f(x + 1) = f(x - 1) = 0$, as desired. $\square$

Step 8: Subcase 2.2: $f(2) = 1 \neq -1$

Here, we consider the subcase where $f(2) = 1 \neq -1$. This also means that char$(S) \neq 2$. The solution in this subcase corresponds to class 7 solutions. That is, we claim that f factors through a ring homomorphism $R \to \mathbb{Z}/4\mathbb{Z}$. Note we already know that $f(0) = -1$, $f(-1) = f(1) = 0$, and $f(2) = 1$.

Recall from (2.1) that

$$J = \{c \in R : \forall x \in R, f(cx + 1) = 0\}.$$

Clearly, $2 \neq 0$ in R since $f(2) = 1 \neq -1 = f(0)$. By Lemma 3, it suffices to show that $2 \in J$. That is, $f(2x + 1) = 0$ for any $x \in R$.

Since $f(2) = 1$, (6.5) yields

$$f(x + 2) + f(x) = f(x + 1) + f(x - 1) \quad \forall x \in R. \tag{8.1}$$

It is easy to see from the above equation that $4 \in I$. Now fix any $x \in R$. By (*), (8.1) implies $f(2x + 1) = f(2x - 1)$. Now (6.2) with (x, y) replaced by $(2, 2x + 1)$ implies

$$f(4x + 1) = f(2x + 1) + f(2x - 1) = 2f(2x + 1).$$

Note that $f(4x + 1) = 0$ since $4 \in I$. Thus, we also get $f(2x + 1) = 0$ since char$(S) \neq 2$. This shows that $2 \in J$.

8

Step 9: Subcase 2.3: $f(2) = 3 \neq 1$

Here, we consider the subcase where $f(2) = 3 \neq 1$. This also means that $\mathrm{char}(S) \neq 2$. The solution in this subcase corresponds to class 3 solutions. That is, we claim that there exists a ring homomorphism $\phi : R \to S$ such that $f = \phi^2 - 1$.

The solution in this subsection requires at least that 2 is invertible in S. For convenience, we just assume that S is a field. We will still begin with only assuming that S is an integral domain. Note that we will borrow (7.4) to cover the case $\mathrm{char}(S) = 3$ in the first important statement.

In this subcase, (6.5) reads as

$$f(x + 2) = 3(f(x + 1) - f(x)) + f(x - 1) \quad \forall x \in R. \tag{9.1}$$

Applying the above equality to (6.6) yields

$$f(x)(3f(x - 1) + f(x + 1)) - (f(x - 1) + 3f(x + 1))(1 + f(x - 1)) = 0 \quad \forall x \in R. \tag{9.2}$$

Replacing x with $-x$ and using (6.1) yields

$$f(x)(3f(x + 1) + f(x - 1)) - (f(x + 1) + 3f(x - 1))(1 + f(x + 1)) = 0 \quad \forall x \in R.$$

Subtracting (9.2) from this equation yields

$$f(x + 1) + f(x - 1) = 2f(x) + 2 \text{ or } f(x + 1) = f(x - 1) \quad \forall x \in R. \tag{9.3}$$

Next, we prove that

$$f(x + 1) + f(x - 1) = 2f(x) + 2 \text{ or } f(x + 1) = f(x - 1) = 0 \quad \forall x \in R. \tag{9.4}$$

Suppose that the former does not hold for some $x \in R$. By (9.3), we have $f(x + 1) = f(x - 1)$. Plugging into (9.2) yields

$$f(x + 1) = f(x - 1) = 0 \text{ or } f(x + 1) = f(x - 1) = f(x) - 1.$$

By (9.1), the latter yields $f(x+2) = f(x)-4$. By manual computation and $\mathrm{char}(S) \neq 2$, this contradicts (9.3). So, we have $f(x + 1) = f(x - 1) = 0$, as desired.

Now note that (9.1) yields $f(x + 1) + f(x - 1) - 2f(x) = f(x + 2) + f(x) - 2f(x + 1)$. Thus, (9.4) yields a stronger result:

$$f(x + 1) + f(x - 1) = 2f(x) + 2 \text{ or } f(x + 1) = f(x) = f(x - 1) = 0 \quad \forall x \in R. \tag{9.5}$$

Finally, we show that the latter yields a contradiction. For the case $\mathrm{char}(S) = 3$, we have $f(2) = 3 = 0$. We can then borrow (7.4) from Step 7, which does not require $f(2) \neq 3$. It directly yields a contradiction. It remains to consider the case $\mathrm{char}(S) \neq 3$.

By (6.2) and (*), we have $f(2x + 1) = f(2x - 1) = 0$. So (9.5) with $\mathrm{char}(S) \neq 2$ tells us that $f(2x) \in \{-1, 0\}$. On the other hand, we will show that $f(2x) = -3$, which is a contradiction since $\mathrm{char}(S) \neq 2, 3$. Indeed, by (6.2) and (*),

$$f(x^2 - 2) = f(x + 1)f(x - 1) + f(2) = 3,$$
$$f(x^2 - 1) = f(x)^2 - 1 = -1,$$
$$f(x^2) = f(x + 1)f(x - 1) + f(2x) = f(2x),$$
$$f(x^2 + 1) = f(x)^2 + f(2x) = f(2x),$$

so (9.1) implies

$$f(2x) = 3(f(2x) + 1) + 3 \iff 2(f(2x) + 3) = 0 \iff f(2x) = -3,$$

9

since char$(S) \neq 2$. This proves
$$f(x+1) + f(x-1) = 2f(x) + 2 \quad \forall x \in R. \tag{9.6}$$

For the rest of the subsection, we assume that S is a field.

Consider the function $g : R \to S$ defined by
$$g(x) = \frac{f(x) - f(x-1) + 1}{2}.$$

Since $f(1) = 0$ and $f(0) = -1$, we have
$$g(0) = 0. \tag{9.g1}$$

By (9.6), we have
$$g(x+1) = g(x) + 1 \quad \forall x \in R, \tag{9.g2}$$

By (9.6) and (6.1), we have
$$g(-x) = -g(x) \quad \forall x \in R, \tag{9.g3}$$

We claim that g is the desired homomorphism.

We first prove that
$$f(x) = g(x)^2 - 1 \quad \forall x \in R. \tag{9.g4}$$

We plug (9.6) to (9.2). After some rearranging, we get
$$(f(x) - f(x-1) - 1)^2 + 4 = 4f(x),$$

which implies (9.g4) after division by $4 = 2^2 \neq 0 \in S$.

Now, by (9.g2), (*) becomes
$$(g(xy) + 1)^2 - g(x+y)^2 = (g(x)^2 - 1)(g(y)^2 - 1) \quad \forall x, y \in R. \tag{9.g5}$$

On the other hand, (6.2) becomes
$$(g(xy) - 1)^2 - g(x-y)^2 = (g(x)^2 - 1)(g(y)^2 - 1) \quad \forall x, y \in R. \tag{9.g6}$$

Subtracting the two equalities and using (9.g2) gives
$$4g(xy) = g(x+y)^2 - g(x-y)^2 \quad \forall x, y \in R. \tag{9.g7}$$

Now adding (9.g5) and (9.g6) gives
$$2g(xy)^2 + 2 - (g(x+y)^2 + g(x-y)^2) = 2(g(x)^2 - 1)(g(y)^2 - 1).$$

Multiplying by $2^3 = 8$ and using (9.g7) gives
$$(g(x+y)^2 - g(x-y)^2)^2 + 16 = 8(g(x+y)^2 + g(x-y)^2) + 16(g(x)^2 - 1)(g(y)^2 - 1). \tag{9.g8}$$

Consider the following identity, which holds due to (9.g2):
$$g(x+1)^2 + g(x-1)^2 = 2g(x)^2 + 2 \quad \forall x \in R.$$

We use this identity as follows. Consider (9.g8) with y replaced by $y + 1$ and also by $y - 1$. Add the two equations, and then subtract with twice of (9.g8). Due to the above identity, after some heavy rearrangement and simplification, we get
$$8(g(x+y) + g(x-y))^2 = 32g(x)^2.$$

That is, we get
$$g(x + y) + g(x - y) = \pm 2g(x) \quad \forall x, y \in R.$$

We now remove the sign constrain and prove
$$g(x + y) + g(x - y) = 2g(x) \quad \forall x, y \in R. \tag{9.g9}$$

Suppose for the sake of contradiction that the above equality does not hold for some $x, y \in R$. Then we have
$$g(x + y) + g(x - y) = -2g(x) \text{ and } g(x + y + 1) + g(x - y + 1) = -2g(x + 1),$$

since $g(x+y+1)+g(x-y+1) = 2g(x+1)$ implies (9.g9). The two equalities yield $4 = 0$ in S; a contradiction.

Now (9.g3) also yields $g(x + y) - g(x - y) = 2g(y)$. Thus, (9.g7) becomes $4g(xy) = 4g(x)g(y)$ for all $x, y \in R$. Since char$(S) \neq 2$, we get that
$$g(xy) = g(x)g(y) \quad \forall x, y \in R. \tag{9.g10}$$

Finally, we prove that g is additive. Plugging $x = 2$ yields $g(2y) = 2g(y)$ for all $y \in R$ since $g(2) = 2$. Now replace x and y in (9.g9) with $x+y$ and $x-y$, respectively. We get $2g(x)+2g(y) = 2g(x+y)$, and thus
$$g(x) + g(y) = g(x + y) \quad \forall x, y \in R$$

since char$(S) \neq 2$. Thus g is indeed a ring homomorphism. The formula (9.4) now proves that f can be written as $g^2 - 1$, where $g : R \to S$ is a ring homomorphism.

Step 10: Subcase 2.4: $f(2) = -1$

Finally, we consider the subcase where $f(2) = -1$. The solution in this subcase corresponds to four class of solutions: 2, 4, 8, 9. More precisely, class 2 solutions occur when char$(S) = 2$, so that $1 = -1$ in S. The other three classes occur in the case char$(S) \neq 2$.

Again, recall the definition of the set I as in (2.2):
$$I = \{c \in R : \forall x \in R, f(c + x) = f(x)\}.$$

As in Step 5, we can assume WLOG that $I = 0$. Our first step here is proving that
$$2 \in I \iff f(x + 1) = f(x - 1) \quad \forall x \in R.$$

The equation (6.5) reads as
$$f(x + 2) = f(x) - f(x + 1) + f(x - 1).$$

Using the above equation, (6.6) reads as
$$f(x)f(x + 1) - f(x - 1)(f(x) - f(x + 1) + f(x - 1)) = f(x - 1) - f(x + 1).$$

Rearranging yields
$$(f(x) + f(x - 1))(f(x + 1) - f(x - 1)) = -(f(x + 1) - f(x - 1)).$$

Thus, we have
$$f(x + 1) = f(x - 1) \text{ or } f(x) + f(x - 1) = -1 \quad \forall x \in R.$$

11

Now we are ready to prove that $2 \in I$. Fix $x \in R$. Replace x with $-x$ in the above equation. Using the fact that f is even (that is, (6.1)), we get

$$f(x+1) = f(x-1) \text{ or } f(x) + f(x+1) = -1.$$

If $f(x+1) \neq f(x-1)$, then we get $f(x)+f(x-1) = f(x)+f(x+1) = -1$. This still leads to $f(x+1) = f(x-1)$. This proves that $2 \in I$. From now on, we may assume that $2 = 0$ in R.

The two equations (6.4) and (6.3), respectively, becomes

$$f(x(x+1)+1) = f(x)f(x+1) \quad \forall x \in R. \tag{10.1}$$

$$f(x^2+1) = f(x)^2 - 1 \quad \forall x \in R, \tag{10.2}$$

The latter yields

$$f(x^2) = f(x+1)^2 - 1 \quad \forall x \in R, \tag{10.3}$$

Next, we prove the following lemma.

Lemma 4. *For any $x \in R$, either $f(x)^2 + f(x+1)^2 = 1$ or $f(x) + f(x+1) = 1$ holds.*

Proof. We start by proving the following equality statement:

$$(f(x+1)^2 - 1)(f(x+1) - 1) + f(x)f(x+1) = f(x)f(x^2 + x) \quad \forall x \in R. \tag{10.L1.1}$$

The equality is based on factoring $x^2(x+1)$ in two ways, as $x^2 \cdot (x+1)$ and $x \cdot x(x+1)$. For any $x \in R$, (*) yields

$$f(x^2)f(x+1) + f(x^2 + x + 1) = f(x^2 + x)f(x) + f(x^2),$$

as both sides are equal to $f(x^2(x+1)+1)$. By (10.1), (10.3), and some algebraic manipulation, (10.L1.1) follows.

Now fix x and let $a = f(x)$ and $b = f(x+1)$. Then (10.L1.1) gives us

$$(b^2 - 1)(b - 1) + ab = af(x^2 + x),$$

$$(a^2 - 1)(a - 1) + ab = bf(x^2 + x).$$

Eliminating terms containing $f(x^2 + x)$ gives us

$$b((b^2 - 1)(b - 1) + ab) = a((a^2 - 1)(a - 1) + ab).$$

After some factoring, this is equivalent to

$$(b - a)(a^2 + b^2 - 1)(a + b - 1) = 0.$$

That is, we have either $f(x)^2 + f(x+1)^2 = 1$, $f(x) + f(x+1) = 1$. It remains to show that the $f(x) = f(x+1)$ has to yield $f(x) + f(x+1) = 1$.

Now suppose for the sake of contradiction that Lemma 4 does not hold. Then we have $a = b$, and (10.L1.1) yields

$$af(x^2 + x) = (a^2 - 1)(a - 1) + a^2 = a^3 - a + 1.$$

By (10.1), (10.3), and (10.2),

$$f(x^4 + x^2 + 1) = f(x^2)f(x^2 + 1) = (a^2 - 1)^2.$$

On the other hand, by (10.2) directly,

$$f(x^4 + x^2 + 1) = f(x^2 + x)^2 - 1.$$

As a result, we have $(a^2 - 1)^2 = f(x^2 + x)^2 - 1$, and thus

$$a^2(a^2 - 1)^2 = (a^3 - a + 1)^2 - a^2,$$

which is equivalent to $(1 - 2a)(a^2 - 1) = 0$. So we have either $1 = 2a = a + b$, which still implies Lemma 4, or $a = \pm 1$.

It remains to show that $a = b = \pm 1$ is impossible. Indeed, it yields $f(x^2) = f(x^2 + 1) = a^2 - 1 = 0$. This contradicts (10.L1.1) with x replaced by x^2. □

We are now ready to finish for the case $\operatorname{char}(S) = 2$. We prove that $f + 1$ is a ring homomorphism.

Claim. *If* $\operatorname{char}(S) = 2$, *then* $f + 1 : R \to S$ *is a ring homomorphism.*

Proof. For the case $\operatorname{char}(S) = 2$, Lemma 4 simplifies to

$$f(x + 1) = f(x) + 1 \quad \forall x \in R. \tag{10.L2.1}$$

This means that (*) can be written as

$$f(xy) = f(x)f(y) + f(x + y) + 1 \quad \forall x, y \in R. \tag{10.L2.2}$$

First suppose that $f + 1$ is additive, i.e.,

$$f(x + y) = f(x) + f(y) + 1 \quad \forall x, y \in R.$$

Then (10.L2.2) yields
$$f(xy) + 1 = (f(x) + 1)(f(y) + 1) \quad \forall x, y \in R,$$

and thus $f + 1$ is both additive and multiplicative. Thus, we only need to prove that $f + 1$ is additive.

We write $f(xy(x + 1)(y + 1) + 1)$ in two ways using (10.L2.2). We get

$$f(xy)f((x + 1)(y + 1)) + f(x + y + 1) = f(x(y + 1))f(y(x + 1)) + f(x + y).$$

Using (10.L2.1), we get

$$f(xy)f((x + 1)(y + 1)) + 1 = f(x(y + 1))f(y(x + 1)).$$

For convenience, set $a = f(x)$, $b = f(y)$, and $c = f(x + y)$. Then, using (10.L2.2) repeatedly gives

$$(ab + c)((a + 1)(b + 1) + c) + 1 = (a(b + 1) + c + 1)(b(a + 1) + (c + 1)),$$

which is equivalent to $c = a + b + 1$ after some heavy algebraic manipulation. This is the equation we wanted to prove, so we are done. □

The rest of the solution is going to focus on the case $\operatorname{char}(S) \neq 2$. The main goal is to prove that $f(c) = -1$ implies $c = 0$. We have useful statements along that way that also helps solving the subcase after proving the main goal.

Lemma 5. *For any* $x \in R$, *we have either* $f(x)f(x + 1) = 0$, *or* $f(x) + f(x + 1) = 1$ *and* $f(x)f(x + 1) = -1$.

Proof. We start by rewriting $f(x^4)$ using (10.2) and (10.3):

$$f(x^4) = f(x)^2(f(x)^2 - 2) = f(x)^4 - 2f(x)^2.$$

Now we write $f(x^8 + x^4 + 1)$ in two ways, using the above equality and (10.1) in different order. For convenience, denote $a = f(x)$ and $b = f(x + 1)$. Then we have

$$f(x^8 + x^4 + 1) = f(x^4)f(x^4 + 1) = (a^4 - 2a^2)(b^4 - 2b^2),$$

$$f(x^8 + x^4 + 1) = f(x^2 + x + 1)^4 - f(x^2 + x + 1)^2 = a^4b^4 - 2a^2b^2.$$

Thus, we have

$$(a^4 - 2a^2)(b^4 - 2b^2) = a^4b^4 - 2a^2b^2 \iff 2(ab)^2(a^2 + b^2 - 3) = 0.$$

Since $2 \neq 0$ in S, this reduces to either $ab = 0$ or $a^2 + b^2 = 3$.

Now we assume the latter. Lemma 4 tells us that either $a^2 + b^2 = 1$ or $a + b = 1$ holds. Since $a^2 + b^2 = 3 \neq 1$, we get $a + b = 1$, and

$$2ab = (a + b)^2 - (a^2 + b^2) = -2.$$

Since $\text{char}(S) \neq 2$, we get $ab = -1$, as desired. $\qquad\square$

Lemma 6. *For any $c \in R$, $f(c) = -1$ implies $c = 0$.*

Proof. First, by Lemma 5, we have

$$f(x) = -1 \text{ implies } f(x + 1) = 0 \quad \forall x \in R. \tag{10.L3.1}$$

Another important observation is the following statement:

$$\text{if } f(c) = -1, \text{ then } f(c^2 + cx + 1) = -f(cx + 1) \quad \forall x \in R, \tag{10.L3.2}$$

which follows from applying (*) twice on both sides.

Now fix some $c \in R$ with $f(c) = -1$. By (10.L3.1) and (10.3), we get

$$f(c + 1) = 0 \implies f(c^2) = 0^2 - 1 = -1.$$

Now, apply (10.L3.2) twice to get

$$f(c^4 + c^2 + c^2x + 1) = f(c^2x + 1) \quad \forall x \in R.$$

By (10.L3.1) and (10.1), we have

$$f(c^2 + c + 1) = f(c)f(c + 1) = 0.$$

Then by (10.3), we get $f(c^4 + c^2) = -1$. Thus, the above equation yields

$$f((c^6 + c^4)x + (c^4 + c^2) + 1) = 0 \quad \forall x \in R.$$

Using the above equation again yields $c^6 + c^4 \in J$.

Notice that $c^6 + c^4 = (c^2 + c^3 + 1)^2 - 1$. But we also have

$$f(c^3 + c^2 + 1) = f(c^2)f(c + 1) + f(c^2 + c + 1) = 0.$$

Thus $f(c^6 + c^4) = -1$. By Lemma 2, we have $c^6 + c^4 \in I$, so $c^6 + c^4 = 0$.

Now we reduce from $c^6 + c^4 = 0$ to $c = 0$. By (10.L3.2) and the fact that $\text{char}(S) \neq 2$, it suffices to show that $c^2 = 0$. Repeating the same argument again, it suffices to show that $c^4 = 0$.

Consider that for any $x \in R$,

$$f((c^2 + 1)(c^4x + 1) + 1) = f(c^2 + 1 + 1) = f(c^2) = -1.$$

14

On the other hand, (10.2) yields $f(c^2 + 1) = 0$, and (*) then yields

$$f((c^2 + 1)(c^4 x + 1) + 1) = f((c^2 + 1) + (c^4 x + 1)) = f(c^4 x + c^2).$$

Thus $f(c^4 x + c^2) = -1$. Applying (10.L3.1), we get

$$f(c^4 x + c^2 + 1) = 0 \quad \forall x \in R.$$

Applying (10.L3.2), we get $f(c^4 x + 1) = 0$ for any $x \in R$, so $c^4 \in J$. By Lemma 2, it remains to show that $f(c^4) = -1$. Since $f(c^2) = -1$, this follows by (10.L3.1) and (10.3). $\qquad \square$

Lemma 7. *For any $x \in R$, we have either $x^2 = 0$, $(x+1)^2 = 0$, or $f(x) + f(x+1) = 1$ and $x^2 + x + 1 = 0$.*

Proof. If $ab = 0$, then either $f(x) = 0$ or $f(x+1) = 0$. By (10.2) and Lemma 6, they yield $(x+1)^2 = 1$ and $x^2 = 0$, respectively.

Now suppose that $a^2 + b^2 = 3$. Lemma 4 yields $a + b = 1$. Thus $2ab = 1^2 - 3 = -2$. Since char$(S) \neq 2$, this yields $f(x)f(x+1) = ab = -1$. By (10.1) and Lemma 6, we get $x^2 + x + 1 = 0$. $\qquad \square$

Now we just consider the above lemma and split into several subsubcases. The three subsubcases yield three distinct solution classes.

First suppose that there exists $c \in R$ such that $c \neq 0$ and $c^2 = 0$. By (10.3), we have

$$-1 = f(0) = f(c^2 x^2) = f(cx + 1)^2 - 1 \quad \forall x \in R.$$

In particular, $f(cx + 1) = 0$ for all $x \in R$, i.e., $c \in J$. Since $f(c^2 + 1) = f(1) = 0$, (10.2) yield $f(c) = -1$. But $f(c) = -1$ implies $c = 0$, so this necessarily implies $f(c) = 1$. Lemma 3 yields $R \cong \mathbb{F}_2[X]/\langle X^2 \rangle$ with $c \mapsto X$. Also, we have computed $f(0) = -1$, $f(1) = 0$, $f(c) = 1$, and $f(c + 1) = 0$.

Now suppose that in R, $x^2 = 0$ implies $x = 0$. Then, $x^2 = 1$ implies $(x - 1)^2 = 0$ and thus $x = 1$. That is, Lemma 7 simplifies to

$$x = 0 \text{ or } x = 1 \text{ or } x^2 + x + 1 = 0 \quad \forall x \in R.$$

If the case $x^2 + x + 1 = 0$ never occurs, then clearly $R \cong \mathbb{F}_2$ and we are done. It remains to consider the case where $f(c) + f(c + 1) = 1$ and $c^2 + c + 1 = 0$ for some $c \in R$.

Fix such c, and consider an arbitrary $d \in R$ such that $d^2 + d + 1 = 0$. Then $c + d \in \{0, 1\}$, since

$$(c + d)^2 + (c + d) + 1 = (c^2 + c + 1) + (d^2 + d + 1) + 1 = 1 \neq 0.$$

That is, we have $d \in \{c, c + 1\}$. In summary, any $x \in R$ satisfies $x \in \{0, 1, c, c + 1\}$. This yields $R \cong \mathbb{F}_4$, and it remains to check that $f(c) + f(c + 1) = 1$ and $f(c)f(c + 1) = -1$. The former is given, and the latter follows by (10.1).