# Some non-Pólya biquadratic fields with low ramification 

Bahar Heidaryan and Ali Rajaei


#### Abstract

Pólya fields are fields with principal Bhargava factorial ideals, and as a generalization of class number one number fields, their classification might be of interest to number theorists. It is known that Pólya fields have little ramification, and the aim of this paper is to prove nonPólyaness of an infinite family of biquadratic number fields with 3 or 4 primes of ramification, correcting a minor mistake in the literature. It turns out that finer arithmetic invariants of the field such as the Hasse unit index plays a direct role in some cases.


## 1. Introduction

The notion of a Pólya field grew out of Pólya's interest in the study of entire functions with integer values at integers. Even if we restrict to the case of polynomial maps, we get rings with marvelous algebraic properties (see [2]).

Let $K$ be an algebraic number field and let $\mathcal{O}_{K}$ be its ring of integers. Consider the ring of integer-valued polynomials on $\mathcal{O}_{K}$ :

$$
\operatorname{Int}\left(\mathcal{O}_{K}\right)=\left\{f \in K[X] \mid f\left(\mathcal{O}_{K}\right) \subseteq \mathcal{O}_{K}\right\}
$$

Definition 1.1 ([13]). A number field $K$ is said to be a Pólya field if the ring $\operatorname{Int}\left(\mathcal{O}_{K}\right)$, as a $\mathcal{O}_{K}$-module, has a basis $\left(f_{n}\right)$ for $0 \leq n \in \mathbb{Z}$, such that $\operatorname{deg}\left(f_{n}\right)=n$.
(See [9], where this notion was first introduced.)
For each $n \in \mathbb{N}$, the leading coefficients of degree $n$ polynomials in $\operatorname{Int}\left(\mathcal{O}_{K}\right)$ together with zero form a fractional ideal of $\mathcal{O}_{K}$, denoted by $\mathfrak{J}_{n}(K)$, which are inverses of Bhargava factorial ideals (see [1]).

Definition 1.2. The Pólya-Ostrowski group of $K$ is the subgroup $\operatorname{Po}(K)$ of the class group of $\mathcal{O}_{K}$ generated by the classes of the ideals $\mathfrak{J}_{n}(K)$.

Note that $K$ is a Pólya field if and only if $\operatorname{Po}(K)$ is trivial (see [2]). Ostrowski [8] proved that $\operatorname{Po}(K)$ is generated by the classes of the ideals $\prod_{q}=\prod_{N(\mathrm{~m})=q} \mathrm{~m}$, where m ranges over maximal ideals in $\mathcal{O}_{K}$ and $q$ is a prime power.

Proposition 1.3 (Proposition 3.1 in [13]). If $K / \mathbb{Q}$ is Galois, the following sequence of Abelian groups is exact:

$$
1 \longrightarrow H^{1}\left(\operatorname{Gal}(K / \mathbb{Q}), \mathcal{O}_{K}^{\times}\right) \longrightarrow \underset{p \text { prime }}{\bigoplus} \mathbb{Z} / e_{p} \mathbb{Z} \longrightarrow \operatorname{Po}(K) \longrightarrow 1
$$

Quadratic Pólya fields are completely characterized:
Proposition 1.4. A quadratic field $\mathbb{Q}(\sqrt{d})$ for square-free $d$ is a Pólya field if and only if:
i) $d=-1,-2,2$, or $p$,
ii) $d=-p, 2 p, p q$ for $p \equiv q \equiv-1(\bmod 4)$,
iii) $d=2 p, p q$ for $p \equiv q \equiv 1(\bmod 4)$ when the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm +1 .

Here, $p$ and $q$ are two distinct odd primes.
Proof. See Example 3.3 in [13]; or as in Proposition 3.1 of [2], note that this follows from Hilbert's Theorems 105 and 106 in [5].

Zantema has completely characterized cyclic Pólya extensions in [13]. Biquadratic fields are the simplest non-cyclic Galois extensions, and Pólya fields among them are not yet completely characterized. However, Leriche has proved important theorems in [7], [6] about them. Here, we note that a theorem in [6] needs a minor correction.

Proposition 1.5 (Proposition 4.5 in [6]). Let p, q, r be three distinct odd primes. The following biquadratic real fields are Pólya fields:

1) $\mathbb{Q}(\sqrt{p}, \sqrt{q})$,
2) $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ with $q r \equiv 1(\bmod 4)$ when the fundamental unit in $\mathbb{Q}(\sqrt{q r})$ has norm +1 .

Note that part 2 in Proposition 4.5 of [6] is missing the above condition on the fundamental unit. However, this condition is necessary: for $p=19, q=5$ and $r=17$ we see that $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is not Pólya, since the ideals 5 and 17 factor as $(\mathfrak{p q})^{2}$, where $\mathfrak{p q}$ is not principal, i.e., $\prod_{q}$ and $\prod_{r}$ are not principal. Yet this field satisfies all the conditions of the above theorem except for the norm of the fundamental unit. Indeed, we give two infinite families of non-Pólya biquadratic fields to show that the above condition is needed.

From now on $p, q$ and $r$ will be three distinct odd primes. For $K=\mathbb{Q}(\sqrt{p}, \sqrt{q r})$, we prove the following.

Theorem A. If $p \equiv 3(\bmod 4), q \equiv 1(\bmod 4), r \equiv 1(\bmod 8),\left(\frac{q}{r}\right)=-1$ and $\left(\frac{p}{r}\right)=+1$, then $\operatorname{Po}(K)=\mathbb{Z} / 2 \mathbb{Z}$.

Theorem B. If $p \equiv q \equiv r \equiv 1(\bmod 4),\left(\frac{q}{r}\right)=-1,\left(\frac{p}{r}\right)=+1$ and the fundamental unit of $\mathbb{Q}(\sqrt{p q r})$ has norm +1 , then $\operatorname{Po}(K)=\mathbb{Z} / 2 \mathbb{Z}$.

The following two theorems give infinitely many Pólya biquadratic fields with only one Pólya subfield, again answering Leriche's question in [7] on the existence of Pólya biquadratic fields which are not a compositum of two quadratic Pólya fields, now for families of totally real biquadratic fields (the examples in [4] consisted only of imaginary biquadratic fields).

Theorem C. Let $p \equiv q \equiv-1(\bmod 4)$ and $r \equiv 5(\bmod 8)$. Then $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is a Pólya field.

Theorem D. Let $p \equiv 3(\bmod 4), q \equiv 1(\bmod 4), r \equiv 5(\bmod 8),\left(\frac{p}{r}\right)=1$, and $\left(\frac{p}{q}\right)=-1$. Then the biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is Pólya.

Our main tool is the following theorem of Setzer [10], in which $K$ is a totally real biquadratic field with quadratic subfields $K_{i}$ whose integral units are denoted by $U_{i}$. Denote $H=H^{1}\left(\operatorname{Gal}(K / \mathbb{Q}), U_{K}\right)$. For a fundamental unit $u_{i}=z_{i}+t_{i} \sqrt{\Delta_{i}}$ $\left(z_{i}>0\right)$ in $K_{i}=\mathbb{Q}\left(\sqrt{\Delta_{i}}\right)\left(\Delta_{i}\right.$ squarefree $)$, define $a_{i}=\operatorname{norm}\left(u_{i}+1\right)=2\left(z_{i}+1\right)$ if $u_{i}$ has norm +1 , and $a_{i}=1$ otherwise. Define $\bar{H}$ to be the subgroup of $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$ generated by $\Delta_{1}, \Delta_{2}, \Delta_{3}, a_{1}, a_{2}$ and $a_{3}$.

Theorem 1.6. $\bar{H} \simeq H$, except for the next two cases, in which $\bar{H}$ is canonically isomorphic to a subgroup of index 2 of $H$ :
(1) the prime 2 is totally ramified in $K / \mathbb{Q}$ and there exists integral $x_{i} \in K_{i}$ such that for $N_{i}=\operatorname{Norm}_{K_{i} / \mathbb{Q}}$,

$$
N_{1}\left(x_{1}\right)=N_{2}\left(x_{2}\right)=N_{3}\left(x_{3}\right)= \pm 2 ;
$$

(2) all the fields $K_{i}$ contain units of norm -1 and $U=U_{1} U_{2} U_{3}$.

Proof. This follows from the proof of Theorem 4 and 5 in [10], combined with the paragraph in page 171 just after the proof of Theorem 5 , for cases other than $M_{3}$ in Setzer's notation. For case $M_{3}$ (all quadratic subfields having a unit of negative norm), see the proof of Theorem 7 there. Note that in Setzer's notation, $\rho(\mathcal{G})$ corresponds to our $\bar{H}$, and $H_{u}$ denotes elements of order dividing 2 in $H$, i.e., $H_{u}=H[2]$.

Remark 1.7. Zantema mentions this theorem in Section 4 of [13], but just refers the reader to Theorem 4 in [10]. For completeness we have included more details of the proof as well as some explanation in terms of Setzer's notation.

## 2. Proof of Theorem A

Let $p, q$ and $r$ be three distinct odd primes with $p \equiv 3(\bmod 4), q \equiv r \equiv 1(\bmod 4)$, $\left(\frac{q}{r}\right)=-1$ and $\left(\frac{p}{r}\right)=1$. In this case the only ramified primes in $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ are 2 , $p, q$ and $r$. Moreover 2 is not totally ramified since it is unramified in $\mathbb{Q}(\sqrt{q r})$, and since $p \equiv 3(\bmod 4), \mathbb{Q}(\sqrt{p})$ has no units of negative norm.

Hence by Theorem 1.6 above, $H \simeq \bar{H}$ is generated by the images of $\Delta_{1}=p$, $\Delta_{2}=q r, \Delta_{3}=p q r, a_{1}, a_{2}$ and $a_{3}$ inside $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$, with $a_{i}$ as defined just before Theorem 1.6. Observe that $a_{2}=1$ since by Dirichlet's theorem [3] the fundamental unit in $\mathbb{Q}(\sqrt{q r})$ has norm -1 (that is where we use $\left(\frac{q}{r}\right)=-1$ in addition to $q \equiv r \equiv 1(\bmod 4))$.

So $|\bar{H}|=4,8$ or 16 . Lemma 2.1 below shows that in $\mathbb{Q}^{*} / \mathbb{Q}^{* 2},\left[2\left(z_{1}+1\right)\right]$ equals [2] or $[2 p]$, so it is independent from $[p]$ and $[q r]$. So $|\bar{H}|$ is at least 8 , and Lemma 2.2 below shows that $|\bar{H}|$ can not be 16. Therefore these two lemmas together show that $|H|=|\bar{H}|=8$. Hence, by Proposition $1.3, \operatorname{Po}(K)=\mathbb{Z} / 2 \mathbb{Z}$, since

$$
\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}=\bigoplus_{i=1}^{4} \mathbb{Z} / 2 \mathbb{Z}
$$

In particular, $K$ is not Pólya.
Lemma 2.1. If $u=z+t \sqrt{p}$ is a fundamental unit in $\mathbb{Q}(\sqrt{p})$ for a prime $p \equiv 3$ $(\bmod 4)$, then $1+z$ and $t$ are odd. Moreover, $1+z$ is a square if $p \equiv-1(\bmod 8)$ or $p$ times a square if $p \equiv 3(\bmod 8)$.

Proof. Since $p \equiv 3(\bmod 4)$, we have $z^{2}-p t^{2}=1$, not -1 . If $f=\operatorname{gcd}(z-1, z+1)$ (we always assume gcd to be positive) (note that $f \mid 2$ ), we have $z+\delta=f s^{2}$ and $z-\delta=f p u^{2}$ for two relatively prime integers $s$ and $u$, where $\delta= \pm 1$, since $(z+1) / f$ and $(z-1) / f$ are relatively prime and their product is $p$ times a square. Note that $2 \delta=f\left(s^{2}-p u^{2}\right)$ and $f$ can not be 2 , since that would give a unit "smaller" than the fundamental unit $\left(s^{2}-p u^{2}= \pm 1\right)$. So $f=1$ (which means $z+1$ and $t$ are odd), and $2 \delta=s^{2}-p u^{2}$. Since $p \equiv 3(\bmod 4)$, we have $\left(\frac{\delta}{p}\right)=\delta$ and so $\left(\frac{2}{p}\right)=\delta$. Since $p \equiv-1(\bmod 4), \delta=+1$ means $p \equiv-1(\bmod 8)$ and $\delta=-1$ means $p \equiv 3(\bmod 8)$.

Lemma 2.2. For $u=z+t \sqrt{p q r}$ a fundamental unit in $\mathbb{Q}(\sqrt{p q r})$ where $p$, $q$, and $r$ satisfy conditions of Theorem $\mathrm{A},[2(z+1)]$ belongs to the subgroup generated by $[2]$, $[p]$ and $[q r]$ in $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$.

Proof. As in the previous lemma, we have $z+\delta=f \epsilon s^{2}$ and $z-\delta=f r \eta u^{2}$, where $\epsilon \eta=p q, \delta= \pm 1$ and $f=\operatorname{gcd}(z+1, z-1) \mid 2$. Upon elimination of $z$, we have $2 \delta=f\left(\epsilon s^{2}-r \eta u^{2}\right)$. Since $r \equiv 1(\bmod 8), 1=\left(\frac{2 \delta}{r}\right)=\left(\frac{f}{r}\right)\left(\frac{\epsilon}{r}\right)$. So $\left(\frac{\epsilon}{r}\right)=1$, but $\epsilon$ is a divisor of $p q$, and $\left(\frac{p}{r}\right)=-\left(\frac{q}{r}\right)=1$, so $\epsilon$ must be 1 or $p$, which means $[f r \eta],[f \epsilon] \in$ $<[2],[p],[q r]>$, i.e., $[z \pm \delta] \in<[2],[p],[q r]>$. Thus $[2(z+1)] \in<[2],[p],[q r]>$.

Remark 2.3. Theorem A is far from being a characterization of Pólya $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ for $p \equiv 3(\bmod 4)$ and $q \equiv r \equiv 1(\bmod 4)$. For example, $\mathbb{Q}(\sqrt{7}, \sqrt{5 \cdot 13})$ is not Pólya, yet it is not covered by Theorem A.

## 3. Proof of Theorem B

Now let $p \equiv q \equiv r \equiv 1(\bmod 4)$. In this case, the only ramified primes in $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ are $p, q$ and $r$. The fundamental unit of $\mathbb{Q}(\sqrt{p})$ has norm -1 and since $\left(\frac{q}{r}\right)=-1$, the fundamental unit of $\mathbb{Q}(\sqrt{q r})$ also has norm -1 , both facts following from Dirichlet's theorem [3], or more generally from [12].

Since we assume $\mathbb{Q}(\sqrt{p q r})$ to have a fundamental unit of norm +1 , by Theorem 1.6, $H \simeq \bar{H}$ generated by the images of $\Delta_{1}=p, \Delta_{2}=q r, \Delta_{3}=p q r, a_{1}=1$, $a_{2}=1$ and $a_{3}$ inside $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}\left(a_{i}\right.$ as in our convention $)$. But

$$
\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}=\bigoplus_{i=1}^{3} \mathbb{Z} / 2 \mathbb{Z}
$$

Hence $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is Pólya if and only if $a_{3}$ is independent of $\Delta_{i}$ 's inside $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$.
So we need the following lemma to finish the proof of Theorem B.
Lemma 3.1. If $u=\frac{1}{2}(z+t \sqrt{p q r})$ is a fundamental unit in $\mathbb{Q}(\sqrt{p q r})$ with $p, q$ and $r$ as in Theorem B , then in $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$, $a_{3}$ belongs to the subgroup generated by $[p]$ and $[q r]$.

Proof. By assumption, the fundamental unit $u=\frac{1}{2}(z+t \sqrt{p q r})$ in $\mathbb{Q}(\sqrt{p q r})$ has norm +1 (where $z$ and $t$ are integers of the same parity), i.e., $z^{2}-p q r t^{2}=4$.

If $f=\operatorname{gcd}(z-2, z+2)$, as in the proof of Lemma 2.1, we have $z+2 \delta=f \epsilon s^{2}$ and $z-2 \delta=f r \eta u^{2}$, where $\epsilon \eta=p q$ and $\delta= \pm 1$.

Note that $f \mid 4$, but both $[z+2 \delta]=[f \epsilon]$ and $[z-2 \delta]=[f r \eta]$ belong to

$$
\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z} \cong<[p],[q],[r]>
$$

so $f=1$ or 4 .
Eliminating $z$ gives us $f\left(\epsilon s^{2}-r \eta u^{2}\right)=4 \delta$. So $\left(\frac{\epsilon}{r}\right)=\left(\frac{\delta}{r}\right)=+1$, but $\epsilon$ is a divisor of $p q$ and $\left(\frac{p}{r}\right)=-\left(\frac{q}{r}\right)=+1$, so $\epsilon$ must be 1 or $p$. Thus

$$
[z+2 \delta]=[f \epsilon]=[\epsilon] \in<[p],[q r]>
$$

but

$$
[z+2 \delta][z-2 \delta]=[p q r] \in<[p],[q r]>
$$

so both $[z+2 \delta]$ and $[z-2 \delta]$ are in $<[p],[q r]>$. So $a_{3}=\left[2\left(\frac{z}{2}+1\right)\right]$ is in $<$ $[p],[q r]>$.

Remark 3.2. It has been conjectured that for $p \equiv q \equiv r \equiv 1(\bmod 4)$, in one third of cases $\mathbb{Q}(\sqrt{p q r})$ has only units of positive norm (see Section 3, page 127 of [11]).

If the fundamental unit in $\mathbb{Q}(\sqrt{p q r})$ has norm -1 with $p, q, r$ as in Theorem B, then we might be in the situation of part (2) of Theorem 1.6. Therefore the above proof can not rule out $H^{1}\left(\operatorname{Gal}(K / \mathbb{Q}), U_{K}\right)$ being the whole $\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}$. This happens exactly when $U=U_{1} U_{2} U_{3}$, in the notation of Theorem 1.6. Therefore we have a dichotomy: either $K$ is Pólya or $\operatorname{Po}(K)=\mathbb{Z} / 2 \mathbb{Z}$.

Remark 3.3. When $p \equiv q \equiv r \equiv 1(\bmod 4)$ and all quadratic subfields of $K=$ $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ have a fundamental unit of norm $-1,\left|U: U_{1} U_{2} U_{3}\right|=1$ is equivalent to being Pólya, and non-Pólyaness is equivalent to $\operatorname{Po}(K)=\mathbb{Z} / 2 \mathbb{Z}=U / U_{1} U_{2} U_{3}$ (for the second equality, see Theorem 7 in [10]). Note that a fundamental unit of negative norm in all quadratic subfields of $K$ can happen frequently: if we have $\left(\frac{q}{r}\right)=-1$ and at most one of the $\left(\frac{p}{r}\right)$ or $\left(\frac{p}{q}\right)$ is +1 , then automatically all quadratic subfields have units of norm -1 by [12].

## 4. Proofs of Theorems C and D

In this section, we prove two theorems on the existence of totally real biquadratic Pólya fields with only one quadratic Pólya subfield. In both theorems, $p \equiv-1$ $(\bmod 4)$, and $r \equiv 5(\bmod 8)$.

First, the case where $q \equiv-1(\bmod 4)$.
Theorem C. Let $p \equiv q \equiv-1(\bmod 4)$, and $r \equiv 5(\bmod 8)$. Then the biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is a Pólya field.

Proof. Under the above assumptions, we have

$$
\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}=\bigoplus_{i=1}^{4} \mathbb{Z} / 2 \mathbb{Z}
$$

and $\left[2\left(z_{1}+1\right)\right]$ equals [2] or [2p], by Lemma 2.1. Therefore it is sufficient to check $\left[a_{2}\right]$ and $\left[a_{3}\right]$. Let $z_{2}+t_{2} \sqrt{q r}$ be a fundamental unit in $\mathbb{Q}(\sqrt{q r})$. We claim that $\left[a_{2}\right]=\left[2\left(z_{2}+1\right)\right]$ is independent of $[2],[p]$, and $[q r]$. Notice that $z_{2}^{2}-q r t_{2}^{2}=1$, since $q \equiv 3(\bmod 4)$. So $z_{2}+\delta=f \epsilon r s^{2}$ and $z_{2}-\delta=f \eta u^{2}$ where $\epsilon \eta=q$ and $\delta= \pm 1$. Thus $2 \delta=f\left(\epsilon r s^{2}-\eta u^{2}\right)$. Since $\left[2\left(z_{2}-\delta\right)\right]\left[2\left(z_{2}+\delta\right)\right]=[q r], a_{2} \in<[2],[p],[q r]>$ if and only if $\left[2\left(z_{2}+\delta\right)\right]=[2 f \epsilon r] \in<[2],[p],[q r]>$, if and only if $\epsilon=q$, since $\epsilon \mid q$.

So we must show that $\epsilon \neq q$. But if $\epsilon=q$, then $2 \delta=f\left(q r s^{2}-u^{2}\right)$. Now, $f=2$ gives a unit smaller than the fundamental unit, so $f=1$. This means $2 \delta=q r s^{2}-u^{2}$, which upon reduction modulo $r$ gives $\left(\frac{2}{r}\right)=\left(\frac{2 \delta}{r}\right)=\left(\frac{-1}{r}\right)=1$ contradicting $r \equiv 5(\bmod 8)$. Therefore, $H$ is generated by $[p]$, $[q r]$, [2], and $\left[a_{2}\right.$ ] independently. So $|H|=\left|\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}\right|$, and therefore $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is a Pólya field.

Theorem D. Let $p \equiv 3(\bmod 4), q \equiv 1(\bmod 4), r \equiv 5(\bmod 8),\left(\frac{p}{r}\right)=1$, and $\left(\frac{p}{q}\right)=-1$. Then the biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{q r})$ is Pólya.

Proof. Since $p \equiv 3(\bmod 4), \mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{p q r})$ can not have a unit of negative norm. Moreover, 2 is unramified in $\mathbb{Q}(\sqrt{q r})$, so by Theorem 1.6, $H \simeq \bar{H}$ is generated by the classes $[p],[q r],\left[a_{1}\right],\left[a_{2}\right]$, and $\left[a_{3}\right]$ inside $\mathbb{Q}^{*} / \mathbb{Q}^{* 2}$ in which $\left[a_{1}\right]=[2]$ or $[2 p]$ (by Lemma 2.1). Thus, since

$$
\bigoplus_{p \text { prime }} \mathbb{Z} / e_{p} \mathbb{Z}=\bigoplus_{i=1}^{4} \mathbb{Z} / 2 \mathbb{Z}
$$

it is sufficient to prove that $\left[a_{3}\right]$ is independent of $[2],[p]$ and $[q r]$.

Now let $z+t \sqrt{p q r}$ be a fundamental unit in $\mathbb{Q}(\sqrt{p q r})$, i.e., $z^{2}-p q r t^{2}=1$ since $p \equiv 3(\bmod 4)$. If $f=\operatorname{gcd}(z+1, z-1)(f=1$, or 2$)$, then for two integers $s$ and $u$ we have $z+\delta=f \epsilon r s^{2}$ and $z-\delta=f \eta u^{2}$, where $\epsilon \eta=p q$. Since $[2(z+$ $\delta)][2(z-\delta)]=[p q r] \in<[2],[p],[q r]>$, we have $a_{3} \in<[2],[p],[q r]>$ if and only if $[2(z+\delta)]=[2 f \epsilon r] \in<[2],[p],[q r]>$ if and only if $\epsilon=q, p q$ since $\epsilon \mid p q$.

So we have to rule out $\epsilon=q$ or $p q$. But $2 \delta=f\left(\epsilon r s^{2}-\eta u^{2}\right)$ and reduction modulo $r$ gives

$$
\left(\frac{2}{r}\right)=\left(\frac{2 \delta}{r}\right)=\left(\frac{f}{r}\right)\left(\frac{-\eta}{r}\right)=\left(\frac{f}{r}\right)
$$

since $\eta=p q / \epsilon=p$ or 1 . This means $f=2$ and we have $\delta=\epsilon r s^{2}-\eta u^{2}$. Observe that $\epsilon=p q$ gives a unit smaller than the fundamental unit, so $\epsilon=q$ and $\eta=p$. As $q \equiv 1(\bmod 4)$, reduction modulo $q$ gives

$$
1=\left(\frac{\delta}{q}\right)=\left(\frac{-p}{q}\right)=\left(\frac{p}{q}\right)=-1
$$

which yields the desired contradiction.
Acknowledgment. The authors wish to thank the anonymous referee for useful comments which corrected and improved an earlier draft of this paper.

## References

[1] Bhargava, M.: $P$-orderings and polynomial functions on arbitrary subsets of Dedekind rings. J. Reine Angew. Math. 490 (1997), 101-127.
[2] Cahen, P. J. and Chabert, J. L.: Integer-valued polynomials. Mathematical Surveys and Monographs 48, American Mathematical Society, Providence, RI, 1997.
[3] Dirichlet, P. G. L.: Einige neue Sätze über unbestimmte Gleichungen. Abh. K. Preuss. Akad. d. Wiss. (1834), 649-664.
[4] Heidaryan, B. and Rajaei, A.: Biquadratic Pólya fields with only one quadratic Pólya subfield. J. Number Theory 143 (2014), 279-285.
[5] Hilbert, D.: Die Theorie der algebraischen Zahlkörper. Jahresbericht der Deutschen Mathematiker-Vereinigung 4 (1897), 175-546.
[6] Leriche, A.: Pólya fields, Pólya groups and Pólya extensions: A question of capitulation. J. Théor. Nombres Bordeaux 23 (2011), no. 1, 235-249.
[7] Leriche, A.: Cubic, quartic and sextic Pólya fields. J. Number Theory 133 (2013), no. 1, 59-71.
[8] Ostrowski, A.: Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. 149 (1919), 117-124.
[9] Pólya, G.: Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. 149 (1919), 97-116.
[10] Setzer, C. B.: Units over totally real $C_{2} \times C_{2}$ fields. J. Number Theory 12 (1980), no. 2, 160-175.
[11] Stevenhagen, P.: The number of real quadratic fields having units of negative norm. Experiment. Math. 2 (1993), no. 2, 121-136.
[12] Trotter, H. F.: On the norms of units in quadratic fields. Proc. Amer. Math. Soc. 22 (1969), 198-201.
[13] Zantema, H.: Integer valued polynomials over a number field. Manuscripta Math. 40 (1982), no. 2-3, 155-203.

Received September 2, 2015; revised June 26, 2016.
Bahar Heidaryan: Department of Mathematics, Tarbiat Modares University, 14115134, Tehran, Iran.
E-mail: b.heidaryan@modares.ac.ir
Ali Rajaei (corresponding author): Department of Mathematics, Tarbiat Modares University, 14115-134, Tehran, Iran.
E-mail: alirajaei@modares.ac.ir

The second author's research was in part supported by a grant from IPM (No. 95110131).

