TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 349, Number 3, March 1997, Pages 1269–1283
S 0002-9947(97)01695-4

RINGS WITH FZP

P. R. FUCHS, C. J. MAXSON, AND G. F. PILZ

In Memoriam Professor J. R. Clay

Abstract. In this paper we investigate the problem of characterizing those rings R such that every nonzero polynomial with coefficients from R has a finite number of zeros in R. Particular attention is directed to the class of skew polynomial domains.

1. Introduction

If $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ is a polynomial of degree n with coefficients from a commutative integral domain D, then as is well known, f has at most n zeros in D. On the other hand, the polynomial $x^2 + 1$ considered as a polynomial over the division ring of quaternions has infinitely many zeros, e.g., $(\cos\alpha)i + (\sin\alpha)j$ where α ranges over the real numbers $\mathbb{R}$. It is the purpose of this paper to initiate an investigation into the problem of characterizing those rings R (with identity) with the property that every nonzero polynomial with coefficients from R has a finite number of zeros in R. We call these rings, *rings with finite zeros property* or *rings with FZP*.

Since every finite ring has FZP, we will assume in the sequel that, unless stated to the contrary, all rings will be infinite. We also assume that our rings have an identity.

We work mainly with left polynomials over a ring R. A *left polynomial* is an expression f of the form $f = a_0 + a_1 x + \cdots + a_n x^n$ with $a_i \in R$. If we assume that x commutes with ring elements, these polynomials form a ring $R[x]$ under the usual operations of addition and multiplication. When we refer to rings with FZP we will always mean with respect to left polynomials. We also recall that, when R is a non-commutative ring, the substitution maps σ_c, for $c \in R$, $\sigma_c : R[x] \to R, f \mapsto f(c)$ are additive morphisms but not multiplicative.

For $c \in R$, if $\sigma_c(f) = 0$, i.e., $f(c) = 0$, then we say that c is a *zero* or a *root* of f. In [2], Gordon and Motzkin show that if R is a division ring, then the number of zeros in R of a (left) polynomial of degree n in $R[x]$ is either at most n or infinite. For polynomials over non-commutative domains this need not be the case. In fact, Theorem 3.12 exhibits an example of a domain R with FZP and a polynomial f of degree 2 in $R[x]$ such that f has more than 2 zeros.

Received by the editors August 15, 1994 and, in revised form, July 12, 1995.
1991 *Mathematics Subject Classification.* Primary 16S36; Secondary 16U10, 11R04.
Key words and phrases. Ring, polynomial, zero.

In a certain place, Theorem 2.3, we also will consider the ring $R_G[x]$ of general polynomials over R. A general polynomial $g \in R_G[x]$ is a finite sum of expressions of the form $a_1xa_2x \ldots a_kxa_{k+1}$, $a_1, a_2, \ldots, a_{k+1} \in R$, again with the natural operations. We give a complete characterization of those rings R such that every polynomial in $R_G[x]$ has a finite number of zeros in R.

The goal of our work is to characterize those rings with FZP. We first consider the problem of characterizing division rings with FZP. For this we use extensively the work of Gordon and Motzkin, [2], summarized in the following:

1.1. Theorem ([2])**.** *Let D be a division ring and $D[x]$ the ring of left polynomials over D.*

(i) *If D is non-commutative, then the centralizer $Z(c)$ of any element $c \in D$ is infinite.*

(ii) *An element $c \in D$ is a zero of a polynomial $f \in D[x]$ if and only if there exists $g \in D[x]$ such that $f = g \cdot (x - c)$.*

(iii) *If $f \in D[x]$ has degree n, then the zeros of f lie in at most n conjugacy classes of D. (Here the conjugacy relation is via the action of $D^* := D \setminus \{0\}$ on D.)*

(iv) *If a polynomial $f \in D[x]$ has two distinct zeros in a conjugacy class, then it has infinitely many in that class.*

As a result of (iii) and (iv) in the above theorem one sees that, for a division ring D, the number of zeros of $f \in D[x]$, where f has degree n, is either $\leq n$ or infinite ([2]).

It is clear that a subring of a ring with FZP must have FZP. However, the finite zeros property is not preserved under homomorphic images. For example, since the ring $\mathbb{Z}[x]$ of polynomials over the integers is a commutative integral domain, $\mathbb{Z}[x]$ has FZP. But the homomorphic image $\mathbb{Z}_6[x]$ does not have FZP, since, for example, the polynomial $2y \in (\mathbb{Z}_6[x])[y]$ has solutions $3x^j$, $j \in \mathbb{N}$, the positive integers.

In the next section we present some general results and solve the characterization problem for division rings with FZP. As a consequence of some of these general results, we also obtain a characterization of those rings R such that every general polynomial $g \in R_G[x]$ has only a finite number of zeros in R. In Section 3 and Section 4 we consider the characterization of FZP for certain classes of domains.

2. General Results

We first obtain some general results about rings with FZP. We recall that "ring" always means ring with identity. Also, we use "domain" to denote a ring without divisors of zero while "integral domain" is used for a commutative domain.

2.1. Theorem. *If R has FZP then R is a domain.*

Proof. Let $a \in R^* = R \setminus \{0\}$. If there exists $0 \neq b \in R$ with $ab = 0$, then the polynomial $g = ax \in R[x]$ has at least two zeros in R and, in fact, only a finite number, say $\{0 = b_1, b_2, \ldots, b_m\} = \mathrm{rann}_R(a)$, the right annihilator of a in R. For $i = 1, 2, \ldots, m$, let $S_i := \{r \in R \mid b_2r = b_i\}$. Since $\mathrm{rann}_R(r)$ is a right ideal, for each $r \in R$, $b_2r \in \mathrm{rann}_R(a)$, so $R = \bigcup_{i=1}^m S_i$. Since R is infinite, some S_i must be infinite, say S_{i_0}. But then $b_2x - b_{i_0}$ has an infinite number of zeros in R, contrary to FZP. Hence the result. □

For commutative rings we have the following characterization.

2.2. Corollary. *Let R be a commutative ring. Then R has FZP if and only if R is an integral domain.*

We can now handle the situation for general polynomials, $R_G[x]$, with coefficients in R. We suppose every nonzero polynomial in $R_G[x]$ has only a finite number of zeros in R. If R is infinite, then by the theorem above, R must be a domain. Suppose that for some $a \in R$, all powers of a are distinct. Then the polynomial $f = ax - xa$ has an infinite number of zeros, namely $a, a^2, a^3, \ldots$, a contradiction. Therefore, for each $b \in R^*$, $b^m = b^n$ for some $m, n \in \mathbb{N}$, the set of positive integers, and consequently, b is invertible, i.e., R is a division ring. If R is not commutative, from Theorem 1.1(i), for $c \in R^*$, the centralizer $Z(c)$ is infinite, which means $g = xc - cx$ has an infinite number of zeros in R, again a contradiction. Using g we also see that R must be finite. This completes the characterization.

2.3. Theorem. *Every nonzero polynomial in $R_G[x]$ has a finite number of zeros in R if and only if R is a finite ring.*

We now return to left polynomials and rings with FZP.

Let D be a division ring, not a field, and suppose D satisfies FZP. Let $a \in D \setminus Z(D)$, and so for some $d \in D$, $dad^{-1} \neq a$. We claim there exist $b, c \in D$ such that $(x - b)(x - a) = (x - c)(x - dad^{-1})$. From this claim, using Theorem 1.1(ii), we see that a and dad^{-1} are both zeros of a polynomial, and from Theorem 1.1(iv), this polynomial has an infinite number of zeros in D, a contradiction. To justify the claim we have $x^2 - (b + a)x + ba = x^2 - (c + dad^{-1})x + cdad^{-1}$. Equating coefficients and solving, one obtains

$$c = (a - dad^{-1})a(a - dad^{-1})^{-1} \text{ and } b = c - (a - dad^{-1}).$$

These kinds of computations are well-known, e.g., [7], [8]. Hence we have characterized division rings with FZP.

2.4. Theorem. *Let D be a division ring. Then D satisfies FZP if and only if D is a field.*

2.5. Corollary. *Let R be a ring with D.C.C. on (say) left ideals. Then R satisfies FZP if and only if R is a field.*

Proof. If R satisfies FZP then we know R must be a domain, and a domain with D.C.C. must be a division ring. From the above theorem, R is a field. □

Turning to domains that are not fields, we see the situation is much different, as illustrated by the following two examples.

2.6. Example. Let $R := \mathbb{C}[x; ^-]$ be the skew polynomial domain over the complex numbers $\mathbb{C}$ determined by the conjugation automorphism, $^-$, that is, $xa = \overline{a}x$, $a \in \mathbb{C}$. Consider $g = y^2 - x^2 \in R[y]$. Then for each $a \in \mathbb{C}^*$, axa^{-1} is a zero of g since $(axa^{-1})^2 = ax^2a^{-1}$ and $x^2a^{-1} = \overline{\overline{a}}^{-1}x^2 = a^{-1}x^2$. But $\{axa^{-1} \mid a \in \mathbb{C}^*\}$ is an infinite set. In fact, if $axa^{-1} = bxb^{-1}$ then $b^{-1}a \in Z(x) = \mathbb{R}[x]$, the real polynomials in x. Hence for $a, b \in \{i+1, i+2, i+3, \ldots\}$, $a \neq b$ implies $b^{-1}a \notin \mathbb{R}[x]$. Consequently, the polynomial g has an infinite number of zeros in R, so R does not satisfy FZP.

2.7. Example. Let $I(\mathbb{R})$ denote the usual quaternion division ring and let $I(\mathbb{Z})$ be the subdomain of $I(\mathbb{R})$ consisting of quaternions with integral coefficients. Further let N be the norm on $I(\mathbb{Z})$ induced by the norm on $I(\mathbb{R})$, i.e., for $b \in I(\mathbb{Z})$, $b =$

$b_0 + b_1 i + b_2 j + b_3 k$, we have $N(b) = b_0^2 + b_1^2 + b_2^2 + b_3^2$. Let $g \in (I(\mathbb{Z}))[y]$ with an infinite number of zeros. Therefore (see Theorem 1.1) there are an infinite number of zeros of g in a conjugacy class in $I(\mathbb{R})$. Thus for some zero b of g, where $b \in I(\mathbb{Z})$, there are infinitely many zeros of g in $\{dbd^{-1} \mid d \in I(\mathbb{R}) \setminus \{0\}\} \cap I(\mathbb{Z})$. However, from $dbd^{-1} = c$, $c \in I(\mathbb{Z})$, we get $N(db) = N(cd)$ or $N(b) = N(c)$, since the norm function is multiplicative. But $N(b)$ is an integer and there are only a finite number of $c \in I(\mathbb{Z})$ with $N(c) = b_0^2 + b_1^2 + b_2^2 + b_3^2$. This shows that g cannot have an infinite number of zeros in $I(\mathbb{Z})$, and since g was general, we find that $I(\mathbb{Z})$ satisfies FZP.

As these examples illustrate, some domains (not division rings) have FZP and some do not. Thus we have the remaining problem of characterizing domains D with FZP. At the moment this appears to be quite a difficult problem and remains open. However, it seems that the next step is to consider various classes of domains and to characterize within these classes the domains with FZP. With this in mind and guided by the previous two examples, we consider in the following sections skew polynomial domains and subdomains of the quaternions $I(\mathbb{R})$.

3. Skew Polynomial Domains with FZP

Throughout this section we let K denote a field with an automorphism σ, and let $R := K[x;\sigma]$ denote the domain of skew polynomials over K determined by σ, i.e., $xa = \sigma(a)x$, $a \in K$. Further, for $s \in \mathbb{N}$, let $K_s := \{a \in K \mid \sigma^s(a) = a\}$, a subfield of K.

3.1. Theorem. *If K is a finite field then $K[x;\sigma]$ has FZP.*

Proof. Let $g \in (K[x;\sigma])[y]$ and let r be any zero of $g = \sum_{i=0}^n a_i(x)y^i$; hence $\sum_{i=0}^n a_i(x)r^i = 0$. If $i_0 = \min\{i \mid a_i(x) \neq 0\}$ and $r \neq 0$, we have

$$-a_{i_0}(x) = (a_{i_0+1}(x) + a_{i_0+2}(x)r + \cdots + a_n(x)r^{n-i_0-1})r,$$

which in turn implies that $\deg r$, as a polynomial in $K[x;\sigma]$, is no larger than $\deg a_{i_0}(x)$. Since K is finite, g can have only a finite number of zeros in $K[x;\sigma]$. □

3.2. Theorem. *If $K[x;\sigma]$ has FZP then $\sigma = \mathrm{id}$ or K_1 is finite.*

Proof. Suppose K_1 is infinite and $\sigma \neq \mathrm{id}$, say $\sigma(a) \neq a$ for some $a \in K$. For $k \in K_1$ let $z(k) := (1 + ka)x(1 + ka)^{-1}$. One then verifies that $z(k) \neq z(k')$ for $k \neq k'$ in K_1. We now determine a polynomial $f \in (K[x;\sigma])[y]$ such that $f(z(k)) = 0$ for each $k \in K_1$, which contradicts the fact that $K[x;\sigma]$ has FZP. To this end let $f(y) = y^2 + (\alpha x)y + \beta x^2$. Then

$$\begin{aligned} 0 = f(z(k)) &\iff (1+ka)x^2 + \alpha x(1+ka)x + \beta x^2(1+ka) = 0 \\ &\iff \left(1 + \alpha + \beta + k(a + \alpha\sigma(a) + \beta\sigma^2(a))\right)x^2 = 0 \\ &\iff 1 + \alpha + \beta + k(a + \alpha\sigma(a) + \beta\sigma^2(a)) = 0 \end{aligned}$$

for $k \in K_1$. Since we are assuming K_1 is infinite, this latter condition is equivalent to

$$1 + \alpha + \beta = 0 \quad \text{and} \quad a + \alpha\sigma(a) + \beta\sigma^2(a) = 0.$$

Solving for α and β, we obtain

$$\alpha = \frac{\sigma^2(a) - a}{\sigma(a) - \sigma^2(a)},$$

which is well-defined since $\sigma(a) \neq a$ and hence $\beta = -1 - \alpha$. Thus the result. □

3.3. Corollary. *Let $R := K[x;\sigma]$ be such that σ has finite order. Then R satisfies FZP if and only if $\sigma = \mathrm{id}$ or K is finite.*

Proof. The sufficiency of the condition is given in Theorem 3.1. For the necessity, suppose the order of σ is $s > 1$. Consider $g = y^s - x^s \in R[y]$ and note that for each $a \in K^*$, axa^{-1} is a zero of g since $x^s \in Z(R)$. If the index of the multiplicative group $[K : K_1]$ is infinite then g has an infinite number of roots in R, hence $[K : K_1]$ is finite. But then K is finite since K_1 is finite by Theorem 3.2. □

To establish the result for the general situation, we need some further notation. From above, $K_s = \{a \in K \mid \sigma^s(a) = a\}$ is a subfield of K for each $s \in \mathbb{N}$. Define $\bar{K} := \bigcup_{s\in\mathbb{N}} K_s$, also a subfield of K. From the definition of $\bar{K}$ it is clear that the restriction $\sigma_{/\bar{K}}$ of σ to $\bar{K}$ is an automorphism of $\bar{K}$. We now state our main characterization theorem, and remark that for the remainder of this section $\sigma \neq \mathrm{id}$.

3.4. Theorem. *The following are equivalent:*

(i) *$K[x;\sigma]$ has FZP;*
(ii) (a) *If $\sigma_{/\bar{K}} = \mathrm{id}_{\bar{K}}$, then $\bar{K}$ is finite;*
(b) *If $\sigma_{/\bar{K}} \neq \mathrm{id}_{\bar{K}}$, then $\bar{K}[x;\sigma_{/\bar{K}}]$ has FZP;*
(iii) *K_1 is a finite field;*
(iv) *$\forall s \in \mathbb{N}$: K_s is a finite field;*

The proof of this theorem will be given in a sequence of lemmas. We note first that (iv) $\implies$ (iii). Since $\bar{K}$ is a subfield of K, $\bar{K}[x;\sigma_{/\bar{K}}]$ is a subring of $K[x;\sigma]$ and hence has FZP. If further $\sigma_{/\bar{K}} = \mathrm{id}_{\bar{K}}$, then $\bar{K} = K_1$ and since $\sigma \neq \mathrm{id}$, Theorem 3.2 shows that K_1 is finite. Hence (i) $\implies$ (ii). Now from (iia), K_1 is finite. If $\sigma_{/\bar{K}} \neq \mathrm{id}_{\bar{K}}$, then $\{b \in \bar{K} \mid \sigma_{/\bar{K}}(b) = b\}$ must be finite by Theorem 3.2, but this set is precisely K_1. Hence we have (ii) $\implies$ (iii). The next lemma gives the equivalence of (iii) and (iv).

3.5. Lemma. *If K_1 is finite then, $\forall s \in \mathbb{N}$: K_s is finite.*

Proof. Let $s \in \mathbb{N}$ and consider $G := \{\sigma_{/K_s}, \sigma^2_{/K_s}, \ldots, \sigma^s_{/K_s} = \mathrm{id}\}$, a subgroup of $\mathrm{Aut}(K_s)$ of order s. Since $\mathrm{Fix}(G) = \{k \in K_s \,|\, \forall\tau \in G : \tau(k) = k\}$ is equal to K_1, we know from field theory that s is the degree of K_s over K_1, hence K_s is finite. □

We now show that (iv) $\implies$ (ii), which will give us the equivalence of (ii), (iii), and (iv). If $\sigma_{/\bar{K}} = \mathrm{id}_{\bar{K}}$, then $\bar{K} = K_1$ is a finite field by condition (iv), hence it suffices to prove (iib).

Suppose $f(y) = c_n(x)y^n + \cdots + c_1(x)y + c_0(x)$ is a polynomial in $(\bar{K}[x;\sigma_{/\bar{K}}])[y]$ with an infinite number of zeros in $\bar{K}[x;\sigma_{/\bar{K}}])$, say $f(p_i) = 0$ where

$$p_i = \alpha_{i0} + \alpha_{i1}x + \cdots + \alpha_{im_i}x^{m_i}, \quad i \in \mathbb{N}.$$

3.6. Lemma. *The above polynomial $f(y)$ has an infinite number of zeros with the same degree.*

Proof. Let $R := \bar{K}[x;\sigma_{/\bar{K}}]$. From [1], we know R is a principal left ideal domain and hence an Ore domain. We let $Q(R)$ denote the division ring of left quotients and note by Theorem 1.1 that f has infinitely many zeros in the set

$$\{\beta \in R \mid \exists\gamma \in Q(R) : \beta = \gamma\alpha\gamma^{-1}\}$$

for some $\alpha \in R$. If $\alpha\gamma_1^{-1}\gamma_2 = \gamma_1^{-1}\gamma_2\beta$ for $\gamma = \gamma_1^{-1}\gamma_2 \in Q(R)$, then $\gamma_1\alpha\gamma_1^{-1}\gamma_2 = \gamma_2\beta$ and $\gamma_1\alpha\gamma_1^{-1}\gamma_2 = \delta^{-1}\eta\gamma_2$ where δ, η are chosen such that $\delta(\gamma_1\alpha) = \eta\gamma_1$. From this, $\eta\gamma_2 = \delta\gamma_2\beta$. Hence $\deg(\eta) = \deg(\delta) + \deg(\beta)$. But $\delta\gamma_1\alpha = \eta\gamma_1$ implies $\deg(\delta) + \deg(\alpha) = \deg(\eta)$, and consequently $\deg(\alpha) = \deg(\beta)$ as desired. □

Thus without loss of generality we assume all the p_i have the same degree, say m. Let j, $0 \le j \le m$, denote the greatest integer such that $\{\alpha_{ij} \mid i \in \mathbb{N}\}$ is an infinite set. We assume $j < m$ and obtain a contradiction.

To simplify notation we write "$\alpha x^\varepsilon \in p$" to denote the fact that p contains αx^ε as one of its summands. Define a set M by

$$M := \{\alpha \mid \alpha x^\varepsilon \in c_l(x) \text{ for some } l, 0 \le l \le n\} \cup \bigcup_{i\in\mathbb{N}} \{\alpha_{ij+1}, \dots, \alpha_{im}\}.$$

Since there are only a finite number of $c_l(x)$ and they are fixed, and by the choice of j, M is a finite subset of $\bar{K}$, it follows that there exists a finite subfield F of $\bar{K}$ with $M \subseteq F$. We choose F to be of the form K_s; hence F is σ-invariant.

Further, let $S := \{(s,l) \mid \gamma_s x^s \in c_l(x) \text{ for some } \gamma_s \in \bar{K}\}$ and $S_{\max} := \{(s,l) \in S \mid s + ml \text{ is maximal}\}$. From $S_{\max}$ choose (s^*, l^*) with minimal s^*. Define $\tau^* \in c_{l^*}(x)p_i^{l^*}$ by

$$\tau^* := (\gamma_{s^*}x^{s^*})(\alpha_{ij}x^j)(\alpha_{im}x^m)^{l^*-1}.$$

Since $f(p_i) = 0$, τ^* must sum to 0 with other terms $(\gamma x^{s'})(\beta x^t) \in c_l(x)p_i^l$. From $\beta x^t \in p_i^l$ we get

$$\beta x^t = (\beta_1 x^{t_1})(\beta_2 x^{t_2}) \dots (\beta_l x^{t_l}),$$

where $\beta_k x^k \in \{\alpha_{i0}, a_{i1}x, \dots, a_{im}x^m\}$. For such terms we must have $s' + t = s^* + j + m(l^* - 1)$.

Suppose t_v is the least integer among the t_k's. We show that $t_v \ge j$. Indeed, if $t_v < j$ then

$$s' + t = s' + \sum_{k=1}^{l} t_k \le s' + t_v + m(l-1)$$

since there are $l - 1$ remaining terms, all of degree at most m. Thus

$$s' + t < s' + j + m(l-1) \le s^* + j + m(l^* - 1)$$

since $(s^*, l^*) \in S_{\max}$, i.e., $s' + t < s^* + j + m(l^* - 1) = \deg(\tau^*)$, a contradiction. Hence we have $t_v \ge j$. If $t_v > j$, then for all k with $1 \le k \le l$, $\beta_k x^{t_k} \in \{\alpha_{ij+1}x^{j+1}, \dots, \alpha_{im}x^m\}$; hence $\beta_k \in F$ and since we have chosen F to be of the form K_s, F is σ-invariant, i.e., $\beta \in F$, so $(\gamma x^{s'})(\beta x^t) = \gamma\sigma^{s'}(\beta)x^{s'+t}$ with $\gamma\sigma^{s'}(\beta) \in F$. If $t_v = j$, then from the definition of τ^* (using $(s^*, l^*) \in S_{\max}$),

$$(\gamma x^{s'})(\beta x^t) = (\gamma x^{s'})(\alpha_{im}x^m)^r(\alpha_{ij}x^j)(\alpha_{im}x^m)^{l-1-r}$$

for some r. Therefore $(\gamma x^{s'})(\beta x^t) = \eta\sigma^{s'+mr}(\alpha_{ij})x^{s'+t}$ for some $\eta \in F$. By collecting the terms that sum to 0 with τ^* we arrive at an equation

$$\eta_{s_1}\sigma^{s_1}(\alpha_{ij}) + \dots + \eta_{s_w}\sigma^{s_w}(\alpha_{ij}) + \eta_{s_{w+1}} = 0,$$

$s_1 \ge s_2 \ge \dots \ge s_w \ge 0$, $\eta_{s_k} \in F$ with $w \le s^* + m(l^* - 1)$.

Note that $\eta_{s_{w+1}}$ takes care of all terms $(\gamma x^{s'})(\beta x^t)$ where $t_v > j$, i.e.,

$$(\gamma x^{s'})(\beta x^t) = \gamma\sigma^{s'}(\beta)x^{s'+t}$$

with $\gamma\sigma^{s'}(\beta) \in F$.

Thus for each $i \in \mathbb{N}$ we obtain such an equation. However, since for each $i \in \mathbb{N}$ the η_{s_k}'s $\in F$ and $w \leq s^* + m(l^* - 1)$, we find a single equation for infinitely many $i \in \mathbb{N}$, hence without loss of generality, for all $i \in \mathbb{N}$.

In the case $(\gamma x^{s'})(\beta x^t) = \eta \sigma^{s'+rm}(\alpha_{ij}) x^{s'+t}$, $\eta \in F$, if $s' + rm = s^*$, then by the minimality of s^*, $s' = s^*$, so $r = 0$, i.e., $(\gamma x^{s'})(\beta x^t)$ is τ^*. Hence the term τ^* cannot cancel, so by combining terms with the same exponent of σ, there exist, $w' \leq w$ and $s_1 > s_2 > \cdots > s_{w'} \geq 0$ with $\eta_{s_1}\sigma^{s_1}(\alpha_{ij}) + \cdots + \eta_{s_{w'+1}} = 0$.

By choosing some coefficients to be zero we can write this equation in the form

$$\sigma^{s_1}(\alpha_{ij}) + \eta_1 \sigma^{s_1 - 1}(\alpha_{ij}) + \eta_2 \sigma^{s_1-2}(\alpha_{ij}) + \cdots + \eta_{s_1}\alpha_{ij} + \eta_{s_1+1} = 0, \quad \eta_i \in F.$$

Since F is σ-invariant we see that for $s \in \mathbb{N}$, $\sigma^{s+s_1}(\alpha_{ij})$ is in the F-vector space with basis $\{\sigma^{s_1-1}(\alpha_{ij}), \ldots, \sigma(\alpha_{ij}), \alpha_{ij}, 1\}$. But F is finite, so there exists $\hat{s} \in \mathbb{N}$ such that $\sigma^{\hat{s}}(\alpha_{ij}) = \alpha_{ij}$ for all $i \in \mathbb{N}$, i.e., $\{\alpha_{ij} \mid i \in \mathbb{N}\} \subseteq K_{\hat{s}}$, contrary to the fact that $K_{\hat{s}}$ is finite. This shows we cannot have $j < m$, so we do have $j = m$.

As above, we again define S, $S_{\max}$, (s^*, l^*), and let $\tau^* = (\gamma_{s^*} x^{s^*})(\alpha_{im} x^m)^{l^*}$ and proceed as before. The situation is somewhat easier since terms which sum with τ^* to be zero are of the form $(\gamma x^{s'})(\alpha_{im}x^m)^{l'}$ where $(s', l') \in S_{\max}$. So we obtain an equation

$$(\gamma_{s_1} x^{s_1})(\alpha_{im}x^m)^{l_1} + \cdots + (\gamma_{s_w} x^{s_w})(\alpha_{im}x^m)^{l_w} = 0$$

for $i \in \mathbb{N}$, $l_1 > l_2 > \cdots > l_w > 0$, i.e., we have a polynomial $g(y) := (\gamma_{s_1}x^{s_1})y^{l_1} + \cdots + (\gamma_{s_w}x^{s_w})y^{l_w}$ with infinitely many zeros of the form (αx^m), $\alpha \in \bar{K}$. Among these zeros there are infinitely many $\beta_i x^m$ which are conjugate (in the division ring of quotients) to a fixed zero αx^m, say $\beta_i x^m = (\delta_{i_1}^{-1}\delta_{i_2})^{-1}\alpha x^m \delta_{i_1}^{-1}\delta_{i_2}$ for all $i \in \mathbb{N}$. Since $\bar{K}[x; \sigma_{/\bar{K}}]$ is an Ore domain, there exist $\gamma_i, \xi_i \in \bar{K}[x; \sigma_{/\bar{K}}]$ such that $\gamma_i \delta_{i_1} \alpha x^m = \xi_i \delta_{i_1}$, which in turn gives $\xi_i \delta_{i_2} = \gamma_i \delta_{i_2} \beta_i x^m$, hence $\deg(\xi_i) = \deg \gamma_i + m$. Let

$$\begin{aligned} \gamma_i &:= \gamma_{i_0} + \cdots + \gamma_{i_k} x^k, & \delta_{i_1} &:= \rho_0 + \cdots + \rho_s x^s, \\ \xi_i &:= \xi_{i_0} + \xi_{i_1} x + \cdots + \xi_{i_{k+m}} x^{k+m}, & \delta_{i_2} &:= \rho'_0 + \cdots + \rho'_t x^t. \end{aligned}$$

Comparing coefficients of the highest terms, we get

$$\begin{aligned} (\gamma_{i_k} x^k)(\rho_s x^s)(\alpha x^m) &= (\xi_{i_{k+m}} x^{k+m})(\rho_s x^s), \\ (\xi_{i_{k+m}} x^{k+m})(\rho'_t x^t) &= (\gamma_{i_k} x^k)(\rho'_t x^t)(\beta_i x^m). \end{aligned}$$

Calculating from these equations, we see that to obtain the conjugate $\beta_i x^m$, we may choose $\delta_{i_1} := \rho_s x^s$ and $\delta_{i_2} := \rho'_t x^t$, i.e.,

$$(\delta_{i_1}^{-1}\delta_{i_2})^{-1} = (x^{-s}\rho_s^{-1}\rho'_t x^t)^{-1} = x^{-t}\rho_t'^{-1}\rho_s x^s = \sigma^{-t}(\rho_t'^{-1}\rho_s)x^{s-t} =: \zeta_i x^z,$$

with $z \in \mathbb{Z}$, $\zeta_i \in \bar{K}$. Since $\beta_i \neq \beta_j$ for $i \neq j$, we have $\zeta_i \neq \zeta_j$, i.e., $\{\zeta_i \mid i \in \mathbb{N}\}$ is an infinite set. Consequently

$$\beta_i x^m = (\zeta_i x^z)(\alpha x^m)(\zeta_i x^z)^{-1} = \sigma^z(\alpha)\zeta_i x^m \zeta_i^{-1} = \sigma^z(\alpha)\zeta_i \sigma^m(\zeta_i^{-1})x^m;$$

hence $\beta_i = \sigma^z(\alpha)\zeta_i\sigma^m(\zeta_i^{-1})$. If $\alpha \in K_s$ then $\sigma^z(\alpha) \in \{\alpha, \sigma(\alpha), \ldots, \sigma^{s-1}(\alpha)\}$, so we may assume $z \geq 0$. We note that z depends on s and t. However, in all cases, $\sigma^z(\alpha) \in \{\alpha, \sigma(\alpha), \ldots, \sigma^{s-1}(\alpha)\}$, so we only need integers $z \in \{0, 1, \ldots, s-1\}$. Thus there is a fixed z, say $z := u$, such that $\beta_i x^m = (\zeta_i x^u)(\alpha x^m)(\zeta_i x^u)^{-1}$ for infinitely many $i \in \mathbb{N}$, so, again without loss of generality, for all $i \in \mathbb{N}$. Now for all $i \in \mathbb{N}$,

$$g(\beta_i x^m) = 0 \iff (\gamma_{s_1} x^{s_1})(\zeta_i x^u)(\alpha x^m)^{l_1} + \cdots + (\gamma_{s_w} x^{s_w})(\zeta_i x^u)(\alpha x^m)^{l_w} = 0.$$

Using an argument similar to the case for $j < m$, we find that there exists an integer $s \in \mathbb{N}$ with $\sigma^s(\zeta_i) = \zeta_i$ for all $i \in \mathbb{N}$, i.e., $\{\zeta_i \mid i \in \mathbb{N}\} \subseteq K_s$. But this again contradicts the fact that K_s is finite. Consequently no polynomial $f \in \bar{K}[x; \sigma_{/\bar{K}}][y]$ can have an infinite number of zeros in $\bar{K}[x; \sigma_{/\bar{K}}]$. This establishes the next lemma, hence (iv) $\implies$ (ii).

3.7. Lemma. *If $\sigma_{/\bar{K}} \neq \mathrm{id}_{\bar{K}}$, then $\bar{K}[x; \sigma_{/\bar{K}}]$ has FZP if and only if $\forall s \in \mathbb{N}$: K_s is a finite field.*

At this stage we can completely handle the situation in which K is an algebraic extension of K_1. For suppose this is the case and $K[x; \sigma]$ has FZP, where $\sigma \neq \mathrm{id}$. Let $k \in K \setminus K_1$. Then there exists $f \in K_1[x]$ such that $0 = f(k) = k^n + \alpha_{n-1} k^{n-1} + \cdots + \alpha_0$. If $\sigma^s(k) \neq k$ for all $s \in \mathbb{N}$, then f would have infinitely many zeros since $f(\sigma^s(k)) = 0$ for $s \in \mathbb{N}$, a contradiction. Thus $K = \bigcup_{s \in \mathbb{N}} K_s$ and $\sigma(K_s) = K_s$. Since $K[x; \sigma]$ has FZP, so does $K_s[x; \sigma_{/K_s}]$ for $s \in \mathbb{N}$. If $\sigma_{/K_s} \neq \mathrm{id}_{K_s}$, we find from Corollary 3.3 that K_s must be finite since $\sigma_{/K_s}$ has finite order s. On the other hand $\sigma_{/K_s} = \mathrm{id}_{K_s}$ implies $K_s = K_1$, and since $K[x; \sigma]$ has FZP, K_1 must be finite by Theorem 3.2. Thus when K is an algebraic extension of K_1 and $K[x; \sigma]$ has FZP, we find that $K = \bar{K}$, and K_s must be a finite field for all $s \in \mathbb{N}$.

3.8. Corollary. *Suppose $\sigma \neq \mathrm{id}$ and K is algebraic over K_1. Then $K[x; \sigma]$ has FZP if and only if $K = \bigcup_{s \in \mathbb{N}} K_s$ with each K_s being finite.*

It is clear that if every element of $K[x; \sigma]$ has only a finite number of conjugates in $K[x; \sigma]$ then $K[x; \sigma]$ has FZP. This situation arises for instance if K is a finite field, since by the proof of Lemma 3.6 two conjugate elements of $K[x; \sigma]$ have the same degree. The converse is not true, as we now show. Suppose K is infinite and the union of finite fields of the form K_s for some $\sigma \in \operatorname{Aut} K$. Let $k_1, k_2 \in K$. Then $k_1^{-1} x k_1 = k_2^{-1} x k_2 \iff k_2 k_1^{-1} x = x k_2 k_1^{-1} \iff k_2 k_1^{-1} \in K_1$. Hence x has infinitely many conjugates in $K[x; \sigma]$, but by the above corollary, $K[x; \sigma]$ has FZP.

Our next lemma is a result of linear algebra. It follows from a result of Lam and Leroy ([4, Corollary 4.13]). However we give a completely elementary proof.

3.9. Lemma. *Let K be a field, $\sigma \in \operatorname{Aut} K$, $0 \neq (c_0, c_1, \ldots, c_s) \in K^{s+1}$. Then the set of solutions of the equation $c_s \sigma^s(\xi) + \cdots + c_1 \sigma(\xi) + c_0 \xi = 0$, $s \geq 0$, is a vector space L over the field $\mathrm{Fix}(\sigma)$, with $\dim(L) \leq s$.*

Proof. Let $s \geq 1$ be minimal such that there exists an equation with $\dim L \geq s + 1$, and say $\xi_1, \xi_2, \ldots, \xi_{s+1}$ are linearly independent over $\mathrm{Fix}(\sigma)$.

For

$$A := \begin{bmatrix} \xi_1 & \sigma(\xi_1) & \ldots & \sigma^s(\xi_1) \\ \xi_2 & \sigma(\xi_2) & \ldots & \sigma^s(\xi_2) \\ \vdots & \vdots & \ddots & \vdots \\ \xi_{s+1} & \sigma(\xi_{s+1}) & \ldots & \sigma^s(\xi_{s+1}) \end{bmatrix}$$

we have $AC = 0$, where $C = (c_0, c_1, \ldots, c_s)^t$. Since $0 \neq (c_0, \ldots, c_s)$, $\mathrm{rk}(A) < s + 1$. Suppose $l \leq s$ is the maximal rank that can be achieved with linearly independent elements, and $\xi_1, \dots, \xi_{s+1} \in L$. Without loss of generality, we may assume that the first l rows of the matrix A are linearly independent. Thus if $\xi \in \{\xi_{l+1}, \dots, \xi_{s+1}\}$, there exists a vector $0 \neq (\lambda, \lambda_1, \dots, \lambda_l) \in K^{l+1}$, $\lambda \neq 0$, such that

$$\begin{aligned} \xi + \frac{\lambda_1}{\lambda}\xi_1 + \cdots + \frac{\lambda_l}{\lambda}\xi_l &= 0, \\ \sigma(\xi) + \frac{\lambda_1}{\lambda}\sigma(\xi_1) + \cdots + \frac{\lambda_l}{\lambda}\sigma(\xi_l) &= 0, \\ &\vdots \\ \sigma^l(\xi) + \frac{\lambda_1}{\lambda}\sigma^l(\xi_1) + \cdots + \frac{\lambda_l}{\lambda}\sigma^l(\xi_l) &= 0. \end{aligned}$$

Applying σ to the i-th equation and subtracting the $i+1$-th equation for $i = 1, 2, \dots, l$, we obtain

$$\begin{aligned} \left(\sigma(\frac{\lambda_1}{\lambda}) - \frac{\lambda_1}{\lambda}\right)\sigma(\xi_1) + \cdots + \left(\sigma(\frac{\lambda_l}{\lambda}) - \frac{\lambda_l}{\lambda}\right)\sigma(\xi_l) &= 0, \\ &\vdots \\ \left(\sigma(\frac{\lambda_1}{\lambda}) - \frac{\lambda_1}{\lambda}\right)\sigma^l(\xi_1) + \cdots + \left(\sigma(\frac{\lambda_l}{\lambda}) - \frac{\lambda_l}{\lambda}\right)\sigma^l(\xi_l) &= 0. \end{aligned}$$

If $\frac{\lambda_1}{\lambda}, \dots, \frac{\lambda_l}{\lambda} \in \mathrm{Fix}(\sigma)$, then $\xi \in \{\xi_{l+1}, \dots, \xi_{s+1}\}$ would be a linear combination of $\xi_1, \dots, \xi_l$, a contradiction to our assumption. Thus $(\sigma(\frac{\lambda_1}{\lambda}) - \frac{\lambda_1}{\lambda}, \dots, \sigma(\frac{\lambda_l}{\lambda}) - \frac{\lambda_l}{\lambda}) \neq (0, \dots, 0)$, which in turn implies that the columns of the matrix

$$\begin{bmatrix} \sigma(\xi_1) & \dots & \sigma^l(\xi_1) \\ \vdots & \ddots & \vdots \\ \sigma(\xi_l) & \dots & \sigma^l(\xi_l) \end{bmatrix}$$

are linearly dependent, say,

$$\begin{aligned} \eta_1\sigma(\xi_1) + \cdots + \eta_l\sigma^l(\xi_1) &= 0, \\ &\vdots \\ \eta_1\sigma(\xi_l) + \cdots + \eta_l\sigma^l(\xi_l) &= 0, \end{aligned}$$

for $(\eta_1, \dots, \eta_l) \neq (0, \dots, 0)$. Hence

$$\begin{aligned} \sigma^{-1}(\eta_1)\xi_1 + \cdots + \sigma^{-1}(\eta_l)\sigma^{l-1}(\xi_1) &= 0, \\ &\vdots \\ \sigma^{-1}(\eta_1)\xi_l + \cdots + \sigma^{-1}(\eta_l)\sigma^{l-1}(\xi_l) &= 0, \end{aligned}$$

which shows that the equation $\sigma^{-1}(\eta_1)\xi + \cdots + \sigma^{-1}(\eta_l)\sigma^{l-1}(\xi) = 0$ has l linearly independent solutions, $\xi_1, \dots, \xi_l$. But this contradicts the minimality of s, since $1 \leq l \leq s$. □

3.10. Corollary. *Let $0 \neq (c, c_0, \dots, c_s) \in K^{s+2}$. Then the set of solutions of the equation $c_s\sigma^s(\xi) + \cdots + c_1\sigma(\xi) + c_0\xi + c = 0$ has at most $s+1$ solutions which are independent over* $\mathrm{Fix}(\sigma)$*.*

Proof. This is the affine analogue of the previous lemma. In fact, if $(\xi_1, \dots, \xi_{s+2})$ were linearly independent, then $\xi_2 - \xi_1, \dots, \xi_{s+2} - \xi_1$ are $s+1$ linearly independent solutions of $c_s\sigma^s(\xi) + \cdots + c_1\sigma(\xi) + c_0\xi = 0$, a contradiction to Lemma 3.9. □

We now use the above to show that for verifying (ii) $\implies$ (i) in Theorem 3.4, we need only consider a special situation.

3.11. Lemma. *If condition* (*ii*) *in Theorem 3.4 holds but $K[x;\sigma]$ does not have FZP, then there exists a polynomial $g(y) := (\gamma_k x^{s_k})y^k + \cdots + (\gamma_1 x^{s_1})y + \gamma_0 x^{s_0}$, $0 \neq (\gamma_k, \dots, \gamma_0) \in K^{k+1}$, which has infinitely many zeros of the form $\beta_i x^m$ for some fixed $m \in \mathbb{N}$.*

Proof. The proof is similar to that of Lemma 3.7. We define $f(y)$, p_i, and $0 \leq j \leq m$ as in the discussion following Lemma 3.6. Again we suppose $j < m$ and obtain an equation $\eta_{s_1}\sigma^{s_1}(\xi) + \cdots + \eta_1\sigma(\xi) + \eta_0 = 0$, $\eta_i \in K$, which has an infinite number of zeros of the form α_{ij}. But, as we have seen before, condition (ii) holds if and only if $\mathrm{Fix}(\sigma)$ is a finite field. But this contradicts our previous two results, since finite dimensional over a finite field would mean only a finite number of zeros. So we conclude that $j = m$. Then by following the proof directly we obtain a polynomial $g(y) := (\gamma_k x^{s_k})y^k + \cdots + (\gamma_1 x^{s_1})y + \gamma_0 x^{s_0}$, which has infinitely many zeros $\beta_i x^m$ for some fixed $m \in \mathbb{N}$ if $K[x;\sigma]$ does not have FZP. □

It remains now to handle this special situation. So we assume we have an equation $g(y) := (\gamma_k x^{s_k})y^k + \cdots + (\gamma_1 x^{s_1})y + \gamma_0 x^{s_0} = 0$, $(\gamma_k, \dots, \gamma_0) \neq 0$, with an infinite number of zeros. From the proof of 3.7, if αx^m is a zero, then there are an infinite number of zeros of the form $\beta_i x^m := (\xi_i x^{e_i})(\alpha x^m)(\xi_i x^{e_i})^{-1}$ where $\alpha \in K$, $m \in \mathbb{N}$, $\xi_i \in K$, and $e_i \in \mathbb{Z}$. We do not necessarily have that all e_i are positive, but either infinitely many are positive or infinitely many are negative, so without loss of generality we can assume all are positive or all are negative. Now let $e_i = e_i' \pmod{m}$, say $e_i = c_i m + e_i'$. Then there exists e, $0 \leq e \leq m-1$, such that $e_i = c_i m + e$ for infinitely many i, hence without loss of generality for all $i \in \mathbb{N}$. We now proceed to show the existence of $\lambda_i \in K$ with $(\xi_i x^{e_i})(\alpha x^m)(\xi_i x^{e_i})^{-1} = (\lambda_i x^e)(\alpha x^m)(\lambda_i x^e)^{-1}$. This equation holds if and only if

$$\xi_i \sigma^{e_i}(\alpha)\sigma^m(\xi_i^{-1}) = \lambda_i \sigma^e(\alpha)\sigma^m(\lambda_i^{-1}),$$

which in turn holds if and only if

$$\frac{\xi_i \sigma^{e_i}(\alpha)}{\lambda_i \sigma^e(\alpha)} = \sigma^m(\frac{\xi_i}{\lambda_i}).$$

Whenever $e_i = e$, we choose $\lambda_i := \xi_i$, so now let $e_i = c_i m + e$, $c_i \neq 0$. Recall that all e_i are positive or all are negative.

Case 1. All e_i are positive. Hence $e_i \geq m$ for all $i \in \mathbb{N}$. Since

$$\sigma^m(\sigma^e(\alpha)\sigma^{e+m}(\alpha)\dots\sigma^{e_i-m}(\alpha)) = \big(\sigma^e(\alpha)\sigma^{e+m}(\alpha)\dots\sigma^{e_i-m}(\alpha)\big)\frac{\sigma^{e_i}(\alpha)}{\sigma^e(\alpha)},$$

we see that $(\sigma^e(\alpha)\sigma^{e+m}(\alpha)\dots\sigma^{e_i-m}(\alpha))$ is a solution of the equation $\sigma^m(\eta) = \eta\frac{\sigma^{e_i}(\alpha)}{\sigma^e(\alpha)}$. If η_1 and η_2 are two solutions then $\sigma^m(\frac{\eta_1}{\eta_2}) = \frac{\eta_1}{\eta_2}$, i.e., $\frac{\eta_1}{\eta_2} \in K_m$. From the fact that $\frac{\xi_i}{\lambda_i}$ is a solution we obtain $\frac{\xi_i}{\lambda_i} = \mu\sigma^e(\alpha)\sigma^{e+m}(\alpha)\dots\sigma^{e_i-m}(\alpha)$, $\mu \in K_m$, hence $\lambda_i = \xi_i/\mu\sigma^e(\alpha)\sigma^{e+m}(\alpha)\dots\sigma^{e_i-m}(\alpha)$.

Case 2. $\forall i \in \mathbb{N}$: $e_i < 0$ (therefore $e_i \leq -1$). In this case

$$\frac{1}{\sigma^{e_i}(\alpha)\sigma^{e_i+m}(\alpha)\dots\sigma^{e-m}(\alpha)}$$

is a solution of $\sigma^m(\eta) = \eta\frac{\sigma^{e_i}(\alpha)}{\sigma^e(\alpha)}$, so $\lambda_i = \mu'\xi_i\sigma^{e_i}(\alpha)\dots\sigma^{e-m}(\alpha)$ for some $\mu' \in K_m$.

The essence of the above discussion is that we are now able to construct infinitely many zeros $(\lambda_i x^e)(\alpha x^m)(\lambda_i x^e)^{-1}$, $i \in \mathbb{N}$, of $g(y)$ by using a *fixed* exponent e. From this we obtain $0 = g((\lambda_i x^e)(\alpha x^m)(\lambda_i x^e)^{-1})$ if and only if

$$\gamma_k x^{s_k}\lambda_i x^e \alpha_k x^{mk} + \gamma_{k-1}x^{s_{k-1}}\lambda_i x^e \alpha_{k-1}x^{m(k-1)} + \dots + \gamma_1 x^{s_1}\lambda_i x^e\alpha_1 x^m + \gamma_0 x^{s_0}\lambda_i x^e = 0,$$

where α_i is the coefficient of x^{mi} in $(\alpha x^m)^i$, $i = 1, 2, \dots, k$, and this in turn is true if and only if

$$\gamma_k\sigma^{s_k+e}(\alpha_k)\sigma^{s_k}(\lambda_i)x^{s_k+mk+e} + \dots + \gamma_1\sigma^{s_1+e}(\alpha_1)\sigma^{s_1}(\lambda_i)x^{m+e+s_1} + \gamma_0\sigma^{s_0}(\lambda_i)x^{s_0+e} = 0$$

if and only if

$$(1)\qquad \gamma_k\sigma^{s_k+e}(\alpha_k)\sigma^{s_k}(\lambda_i) + \dots + \gamma_1\sigma^{s_1+e}(\alpha_1)\sigma^{s_1}(\lambda_i) + \gamma_0\sigma^{s_0}(\lambda_i) = 0,$$

since from our construction we have $s_k + mk = s_{k-1} + m(k-1) = \dots = s_1 + m = s_0$. In equation (1) the coefficients are fixed elements of K.

Now suppose condition (ii) in Theorem 3.4 holds and so $\mathrm{Fix}(\sigma)$ is finite. Then from Lemma 3.9, the above equation has only a finite number of roots. But our assumption that $K[x;\sigma]$ does not have FZP gives infinitely many such λ_i. This contradiction completes the proof of Theorem 3.4. □

We conclude this section with a couple of remarks. One might ask, when a domain R satisfies FZP, if the number of zeros of a polynomial is related to the degree of the polynomial. We show that in general this is not the case.

In fact, let $K := \mathrm{GF}(p^2)$, the finite field of order p^2, and form $R := K[x;\sigma]$, where σ is the Frobenius automorphism, $\sigma(a) = a^p$, $a \in K$. Every non-zero element ω of K satisfies

$$\omega^{p^2-1} - 1 = (\omega^{p+1} - 1)(\omega^{(p+1)(p-2)} + \omega^{(p+1)(p-3)} + \dots + w^{p+1} + 1) = 0.$$

Thus there are $p+1$ elements of K satisfying $\omega^{p+1} - 1 = 0$, say $a_1, a_2, \dots, a_{p+1}$. But then $a_1x, a_2x, \dots, a_{p+1}x$ are zeros of $g(y) = y^2 - x^2 \in (K[x;\sigma])[y]$. For any $N \in \mathbb{N}$, there is a prime p, $p > N$, so for $K = \mathrm{GF}(p^2)$, g has more than N zeros. But K being finite implies that $K[x;\sigma]$ has FZP.

3.12. Theorem. *Let $N \in \mathbb{N}$. There exist a domain D with FZP and a quadratic polynomial g in $D[y]$ such that g has more than N zeros.*

On the other hand, when K is finite there is an upper bound on the number of roots of $g \in (K[x;\sigma])[y]$. Suppose $g := a_n(x)y^n + \dots + a_1(x)y + a_0(x)$. As we have seen previously, if $r \neq 0$ is a zero of g and $i_0 := \min\{i \mid a_i(x) \neq 0\}$, then $(a_{i_0+1}(x) + a_{i_0+2}(x)r + \dots + a_n(x)r^{n-i_0-1})r = -a_{i_0}(x)$, so $\deg(r) \leq \deg a_{i_0}(x)$ as polynomials in $K[x;\sigma]$. If $\deg a_{i_0}(x) = m$, then the number of zeros of g in $K[x;\sigma]$ is no more than q^{m+1}, where $|K| = q$.

4. $I(S)$ WITH FZP

In this section, let S be an integral domain, $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, and let $I(S)$ denote the ring

$$I(S) := \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in S\}.$$

In general, $I(S)$ is not a domain. For if $S = \{a + bl \mid a, b \in \mathbb{Z}, l := \sqrt{-1}\}$ is the ring of integers of the Gaussian field, $x = 1 + li$, $y = 1 - li$, then $xy = 0$. We now characterize all rings $I(S)$ with FZP in case $\mathbb{Z} \subseteq S \subseteq \mathbb{Q}$ or if S is the ring of integers of an algebraic number field. First, let $\mathbb{Z} \subseteq S \subseteq \mathbb{Q}$, i.e., $I(S)$ is a subdomain of the division ring of real quaternions.

Let p be a prime integer and suppose $\frac{1}{p} \in S$. Then $T^{-1}\mathbb{Z} \subseteq S$, where $T^{-1}\mathbb{Z}$ is the localization of $\mathbb{Z}$ by $T := \{p^n \mid n \in \mathbb{N}_0\}$. Let $R := T^{-1}\mathbb{Z}$. We first show if p is an odd prime, then $I(R)$ does not have FZP and hence $I(S)$ does not have FZP.

Case 1. $p \equiv 1 \pmod 4$. In this case, -1 is a quadratic residue of p and therefore the equation $x^2 \equiv -1 \pmod{p^n}$ has a solution for all $n \in \mathbb{N}$ [3, Par. 8.3]. From this, $p^n = x^2 + y^2$ has a primitive solution [4, p. 126]. Consequently we have a solution $a_n^2 + b_n^2 = p^n$, $\gcd(a_n, b_n) = 1$ for $n \in \mathbb{N}$. Let

$$u_n = a_n + b_n j \quad \text{and} \quad v_n = u_n i u_n^{-1} = ((a_n^2 - b_n^2)i - 2a_n b_n k)/p^n \in I(R).$$

If $v_n = v_m$ for some $n \neq m$, say $n > m$, then we obtain

$$\frac{a_m b_m}{p^m} = \frac{a_n b_n}{p^n} \quad \text{or} \quad a_m b_m p^{n-m} = a_n b_n.$$

Hence $p | a_n$ or $p | b_n$. But then, since $a_n^2 + b_n^2 = p^n$, we find that $p | a_n$ and $p | b_n$, a contradiction to $\gcd(a_n, b_n) = 1$. Consequently $\{v_n \mid n \in \mathbb{N}\}$ is an infinite set of zeros of $x^2 + 1 = 0$, so in this case $I(R)$ does not have FZP.

Case 2. $p \equiv 3 \pmod 4$. In this case, since -1 is not a quadratic residue we need an alternate approach. To this end, we define

$$R_n := \{b = \frac{b_0}{p^n} + \frac{b_1}{p^n} i + \frac{b_2}{p^n} j + \frac{b_3}{p^n} k \mid b_0, b_1, b_2, b_3 \in \mathbb{Z}, N(b) = 1\},$$

where $N : I(R) \to R$ is the usual norm on the quaternions, restricted to $I(R)$ as described in Example 2.7. Then $N(b) = 1$ implies $b_0^2 + b_1^2 + b_2^2 + b_3^2 = p^{2n}$. From [3, Par. 20.12],

$$\begin{aligned} |R_n| &= 8 \cdot (\text{sum of divisors of } p^{2n}) \\ &= 8 \cdot \frac{p^{2n+1} - 1}{p - 1} \\ &= 8 \cdot (p^{2n} + p^{2n-1} + \cdots + p + 1). \end{aligned}$$

From this we find that there are an infinite number of elements b in $I(R)$ with $N(b) = 1$.

Now let $a, b \in I(R)$ with $N(a) = N(b) = 1$, and suppose $aia^{-1} = bib^{-1}$. Then we have $b^{-1}a \in Z(i)$, the centralizer of i in $I(R)$; hence $a = bc$, $c \in Z(i)$. By calculation, $Z(i) = \{a + bi \mid a, b \in R\}$. Now let $c = \frac{c_0}{p^{n_0}} + \frac{c_1}{p^{n_1}} i$, $c_0, c_1 \in \mathbb{Z}$, and $p \nmid c_0$, $p \nmid c_1$. Without loss of generality we take $n_0 \geq n_1$. From $a = bc$, $N(c) = 1$; so

$$1 = \frac{c_0^2}{p^{2n_0}} + \frac{c_1^2}{p^{2n_1}};$$

equivalently,

$$p^{2n_0} = c_0^2 + p^{2(n_0-n_1)}c_1^2 = c_0^2 + (p^{(n_0-n_1)}c_1)^2.$$

From [3, Par. 16.9], p^{2n_0} has only 4 representations as a sum of two squares, and these then must be $c_0 = \pm p^{n_0}$ or $c_1 = \pm p_1^{n_1}$. Hence $c = \pm 1$ or $c = \pm i$, and so we see there are only 4 elements a in $I(R)$ with $N(a) = 1$ in the conjugacy class of i determined by b. But as we showed above, there are an infinite number of elements d with $N(d) = 1$. Consequently there are an infinite number of distinct conjugates of i. But now each of these bib^{-1} is a zero of $x^2 + 1 = 0$, so again, in this case as well, we see that $I(R)$ does not have FZP.

We have established the necessity of the conditions in the following theorem.

4.1. Theorem. *Let S be a domain, $\mathbb{Z} \subseteq S \subseteq \mathbb{Q}$. Then $I(S)$ has FZP if and only if $S = \mathbb{Z}$ or $S = T^{-1}\mathbb{Z}$ where $T = \{2^n \mid n \in \mathbb{N}_0\}$.*

Proof. It remains to verify the sufficiency of the conditions. In Example 2.7 we showed that $I(\mathbb{Z})$ has FZP, so we take $S = T^{-1}\mathbb{Z}$, $T = \{2^n \mid n \in \mathbb{N}_0\}$. We show that every nonzero a in $I(S)$ has a finite number of conjugates in $I(S)$, and so $I(S)$ will have FZP. To this end, let $A := \{b \in I(S) \mid N(b) = N(a)\}$. Also, for $n \in \mathbb{N}_0$, define

$$A_n := \{b = \frac{b_0}{2^n} + \frac{b_1}{2^n}i + \frac{b_2}{2^n}j + \frac{b_3}{2^n}k \mid b_0, b_1, b_2, b_3 \in \mathbb{Z}, N(b) = N(a)\}.$$

We know $N(a) = \frac{l}{2^s}$, $s \in \mathbb{N}_0$, $l \in \mathbb{N}$, and $A = \bigcup_{n=0}^{\infty} A_n$. We show that A is finite, which of course means that a has a finite number of conjugates in $I(S)$.

Suppose first that $N(a)$ is an integer. For $b \in A$, b is in some A_n, so

$$b_0^2 + b_1^2 + b_2^2 + b_3^2 = 2^{2n}N(a), \tag{2}$$

and, from [3, Par. 20.12], the number of solutions of this equation is 8·(sum of divisors of $2^{2n}N(a)$ which are not divisible by 4). But this is the same as the number of solutions of

$$b_0^2 + b_1^2 + b_2^2 + b_3^2 = 4N(a). \tag{3}$$

Thus $|A_1| = |A_n|$ for all $n \geq 1$. In fact,

$$(b_0, b_1, b_2, b_3) \mapsto (2^{n-1}b_0, 2^{n-1}b_1, 2^{n-1}b_2, 2^{n-1}b_3)$$

is a bijective map between the solutions of (3) and those of (2). Thus if $b \in A_n$, $n \geq 1$, then

$$\begin{aligned} b &= \frac{2^{n-1}}{2^n}c_0 + \frac{2^{n-1}}{2^n}c_1 i + \frac{2^{n-1}}{2^n}c_2 j + \frac{2^{n-1}}{2^n}c_3 k \\ &= \frac{c_0}{2} + \frac{c_1}{2}i + \frac{c_2}{2}j + \frac{c_3}{2}k \in A_1. \end{aligned}$$

Thus in this case, $A = A_0 \cup A_1$, a finite set.

Suppose now $N(a) = \frac{l}{2^s}$, $l \in \mathbb{N}$, $2 \nmid l$, $s \geq 1$. Modifying the above we find that, if n is even,

$$A_n = \begin{cases} \varnothing, & n < \frac{s}{2}, \\ A_{\frac{s}{2}+1}, & n \geq \frac{s}{2} + 1, \end{cases}$$

hence $A = A_{\frac{s}{2}} \cup A_{\frac{s}{2}+1}$, a finite set. If n is odd and $s \leq \lfloor \frac{s}{2} \rfloor$, then $A_n = \varnothing$, so we take $s \geq \lfloor \frac{s}{2} \rfloor + 1$. Then

$$(b_0, b_1, b_2, b_3) \mapsto 2^{n-t}(b_0, b_1, b_2, b_3)$$

where $t = \left\lfloor \frac{s}{2} \right\rfloor + 1$ is a bijection between solutions of $b_0^2 + b_1^2 + b_2^2 + b_3^2 = 2^{2t} N(a)$ and solutions of $b_0^2 + b_1^2 + b_2^2 + b_3^2 = 2^{2n} N(a)$. Therefore, in this case we have $A_n = A_{\lfloor s/2 \rfloor + 1}$ for $n \geq \left\lfloor \frac{s}{2} \right\rfloor + 1$, and again A is finite. This completes the proof of the theorem. □

For arbitrary integral domains $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, the problem of characterizing all rings $I(S)$ with FZP seems to be difficult and remains open. However, by using some results of T. Nagell [6] we are able to obtain a satisfactory answer when S is the ring of integers of an algebraic number field K. Recall that K is said to be totally real if $K \subseteq \mathbb{R}$ and all conjugate fields are real. Also $\max k$ will denote the maximum of the absolute values of the conjugates of $k \in K$.

4.2. Theorem. *Let S be the ring of integers of an algebraic number field K. Then $I(S)$ has FZP if and only if K is totally real.*

Proof. If K is totally real then $I(S)$ is a subdomain of the real quaternions, hence in order to show $I(S)$ has FZP it suffices to establish that every equation $x^2 + y^2 + z^2 + u^2 = e$ has only finitely many solutions in S for a fixed element $e \in S$. Now let $(a, b, c, d) \in S^4$ be a solution of the above equation and $u \in \{a, b, c, d\}$. Then $\max u < \max e + 1$. Indeed, if u' is a conjugate of u, then there exists a homomorphism h defined on $\mathbb{Q}(a, b, c, d)$ (= the field generated by $\mathbb{Q} \cup \{a, b, c, d\}$) such that h restricted to $\mathbb{Q}$ is the identity and $h(u) = u'$. Consequently

$$h(a)^2 + h(b)^2 + h(c)^2 + h(d)^2 = h(e) \leq \max e;$$

hence $\max u < \max e + 1$. However, by [5, Vol. 2, Thm. 2–40], there exist only finitely many $u \in S$ with this property, which shows that the number of solutions $(a, b, c, d) \in S^4$ is finite.

Conversely, suppose that $I(S)$ has FZP. As we have seen at the beginning of this section, $I(S)$ is not a domain if K is the Gaussian field; hence $I(S)$ does not have FZP by Theorem 2.1. Now suppose that K is not totally real. But then the equation $x^2 + y^2 = 1$ has infinitely many solutions $\{(x_n, y_n) \mid n \in \mathbb{N}\}$ in S by [6, Thm. 7]. Let $a_n = x_n + y_n j$, $n \in \mathbb{N}$, and $a, b \in \{a_n \mid n \in \mathbb{N}\}$. Then $aia^{-1} = bib^{-1}$ if and only if $b^{-1}a \in Z(i) = \{x + yi \mid x, y \in S\}$. Since $b^{-1}a \in \{x + yj \mid x, y \in S\}$ and $N(b^{-1}a) = 1$, it follows that $b = \pm a$; hence $x^2 + 1$ has infinitely many zeros in $I(S)$, which contradicts our assumption that $I(S)$ has FZP. □

Acknowledgement

The authors wish to thank the referee for references, in particular [4], and for pointing out a needed modification in Theorem 3.4.

References

1. K. R. Goodearl and R. B. Warfield, *An introduction to noncommutative Noetherian rings*, London Math. Soc. Student Texts, no. 16, Cambridge University Press, 1989. MR **91c:**16001
2. B. Gordon and T. S. Motzkin, *On the zeros of polynomials over division rings*, Trans. A.M.S. **116** (1965), 218–226; **122** (1966), 547. MR **33:**4050a,b
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford University Press, 1960. MR **81i:**10002
4. T. Y. Lam and A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), 308–336. MR **90f:**16005
5. W. J. LeVeque, *Topics in Number Theory*, vols. 1,2, Addison-Wesley, 1956. MR **18:**283b
6. T. Nagell, *On the number of representations of an A-number in an algebraic field*, Ark. Mat. **4** (1962), 467–478. MR **27:**128

7. L. H. Rowen, *Polynomial identities in ring theory*, Pure and Applied Math., no. 83, section 3.2, Academic Press, Boston, 1980. MR **82a:**16021

8. ———, *Wedderburn's method and algebraic elements of simple artinian rings*, Azumaya Algebras, Actions and Modules in Honor of G. Azumaya (D. Haile, ed.), Contemporary Math, no. 124, 1992, pp. 179–202. MR **92k:**16025

Institut für Mathematik, Johannes Kepler Universität, A-4040 Linz, Austria
E-mail address: `peter.fuchs@jk.uni-linz.ac.at`

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: `cjmaxson@math.tamu.edu`

Institut für Mathematik, Johannes Kepler Universität, A-4040 Linz, Austria
E-mail address: `guenter.pilz@jk.uni-linz.ac.at`