sciendo

Annales Mathematicae Silesianae **33** (2019), 106–120
DOI: 10.2478/amsil-2019-0012

n-TH ROOT SELECTIONS IN FIELDS

Paweł Gładki

Dedicated to Prof. Andrzej Sładek on the occasion of his retirement

Abstract. In this work we generalize the results of [9] to the higher level case: we define n-th root selections in fields of characteristic $\neq 2$, that is subgroups of the multiplicative group of a field whose existence is equivalent to the existence of a partial inverse of the $x \mapsto x^n$ function, provide necessary and sufficient conditions for such a subgroup to exist, study their existence under field extensions, and give some structural results describing the behaviour of maximal n-th root selection fields.

1. Introduction

During the last talk before his (formal) retirement at the Algebra and Number Theory Seminar of the Institute of Mathematics of the University of Silesia, a dear friend and a colleague of mine, Prof. Andrzej Sładek, presented results of Waterhouse [9], who defined root selections in fields and investigated some of their properties. Roughly speaking, root selections are partial inverses of the square function, whose existence is equivalent to the existence of certain subgroups of the multiplicative group of a field, which, in turn, can be viewed as somewhat weaker versions of positive cones of orderings in fields. Following

Received: 05.04.2018. Accepted: 01.06.2019. Published online: 22.06.2019.
(2010) Mathematics Subject Classification: 12F05, 12J15.
Key words and phrases: root selections, root selections of higher level, half-orderings, pre-orderings and orderings of higher level.

Waterhouse, Prof. Sładek encouraged us to generalize these results to the higher level case, and in this paper we do the assigned homework.

In Section 2 we formally define n-th root selections in a field F as partial inverses of the $x \mapsto x^n$ function and show that their existence is equivalent to the existence of a multiplicative subgroup R of $F^* = F \setminus \{0\}$ such that for every element $a \in F^*$ there exists a unique element $r \in R$ and a unique n-th root of unity ω such that $a = \omega r$. In other words, we study subgroups R of F^* such that

$$F^* = R \cdot \mu_n(F) \quad \text{and} \quad R \cap \mu_n(F) = \{1\},$$

where $\mu_n(F)$ denotes the group of n-th roots of unity of F. As every finite subgroup of F^* is a group of roots of unity, this is a more general case of a special situation concerned with studying subgroups R of F^* with a finite factor group F^*/R which admit a complement, that is a subgroup S of F^* such that

$$F^* = R \cdot S \quad \text{and} \quad R \cap S = \{1\}.$$

In Section 3 we study extensions of n-th root selections, and prove that a n-th root selection R of a field F can be extended to a n-th root selection of a field extension $E \supset F$ regardless of the parity of the degree of this field extension. This naturally leads to the notion of a maximal n-th root selection, which is somewhat analogous to the one of a real closure of a field. Maximal selections are further studied in Section 3, where some of their basic properties are investigated, and equivalent conditions for a root selection to be maximal are given. The case of $n = 2^p$ is especially interesting.

2. Existence of n-th root selections

Throughout the paper assume F is a field and denote, for any subset $A \subset F$, by A^* the set $A \setminus \{0\}$. Also, denote by $\mu_n(F)$ the group of n-th roots of unity of F.

Intuitively, we want to define n-th root selections as homomorphisms that assign to n-th powers of a field F some elements of the multiplicative group of F. The existence of these homomorphisms is equivalent to the existence of certain subgroups of F^*, as shown in the following lemma:

LEMMA 2.1. *A multiplicative homomorphism ϕ from the group F^{*n} of n-th powers of F to F^* such that $\phi(c^n) = \omega c$, for some $\omega \in \mu_n(F)$, exists if*

and only if there exists a multiplicative subgroup R of F^* such that for every element $a \in F^*$ there exist a unique element $r \in R$ and a unique element $\omega \in \mu_n(F)$ such that $a = \omega r$.

Proof. ($\Rightarrow$) Assume that there exists ϕ as desired. Let $R = \operatorname{Im}\phi$. Then, automatically, R is a subgroup of F^*. Fix $a \in F^*$. Say $\mu_n(F) = \{\omega_1, \ldots, \omega_n\}$. Then, clearly, for some $k \in \{1, \ldots, n\}$, $R \ni \phi(a^n) = \omega_k a$, and hence $F^* = \omega_1 R \cup \omega_2 R \cup \ldots \cup \omega_n R$. Suppose that, for some $r_1, r_2 \in R$ and some $k_1, k_2 \in \{1, \ldots, n\}$, $\omega_{k_1} r_1 = \omega_{k_2} r_2$. Say $\omega_l = \omega_{k_1}/\omega_{k_2}$. Then $\omega_l \in R$, say $\omega_l = \phi(c^n)$, for some $c \in F^*$. On the other hand $\phi(c^n) = \omega_k c$, for some $k \in \{1, \ldots, n\}$, so that $c = \omega_l/\omega_k \in \mu_n(F)$ and $c^n = 1$. Since ϕ is a homomorphism, $\phi(1) = 1$. In particular, $\omega_l = 1$, so that $\omega_{k_1} = \omega_{k_2}$, which leads to also $r_1 = r_2$.

($\Leftarrow$) Assume that there exists R as desired. Then, for a fixed $c^n \in F^{*n}$, there exist a unique element $r \in R$ and a unique $\omega \in \mu_n(F)$ such that $\omega c = r$. The assignment $\phi(c^n) := r$ declares a well-defined function that satisfies the desired condition and it remains to check that it is a homomorphism: this is, indeed, the case, for if $c_1^n, c_2^n \in F^{*n}$ and $\omega_1, \omega_2 \in \mu_n(F)$, $r_1, r_2 \in R$ are the unique integers and elements of R such that $\omega_1 c_1 = r_1$ and $\omega_2 c_2 = r_2$, then $\omega_1\omega_2 c_1 c_2 = r_1 r_2$, which, by the uniqueness, yields $\phi(c_1^n c_2^n) = r_1 r_2 = \phi(c_1^n)\phi(c_2^n)$. □

We are now in a position to formally define n-th root selections:

Definition 2.2. A multiplicative subgroup R of F^* such that for every element $a \in F^*$ there exist a unique element $r \in R$ and a unique $\omega \in \mu_n(F)$ such that $a = \omega r$ shall be called a *n-th root selection for F*. Moreover, if $|\mu_n(F)| = n$, then such a subgroup R shall be called an *exact n-th root selection for F*.

Remark 2.3.

1. A multiplicative subgroup R of F^* is a n-th root selection for F if and only if

$$F^* = R \cdot \mu_n(F) \quad \text{and} \quad R \cap \mu_n(F) = \{1\};$$

indeed, by definition, that R is a n-th root selection is just equivalent to F^* being the direct product of R and $\mu_n(F)$.

2. If $|\mu_n(F)| = k$, then n-th root selections are at the same time k-th root selections; this is clear, as then $\mu_n(F) = \mu_k(F)$: order of every element ω of $\mu_n(F)$ is divisible by k, so that $\omega \in \mu_k(F)$, and since $\omega^n = 1$, also $k \mid n$, so that every k-th root of unity is necessarily a n-th root of unity.

EXAMPLE 2.4. Consider the field $\mathbb{R}$. Here $\mu_2(\mathbb{R}) = \{1, -1\}$, and the group $R = \mathbb{R}^+ = \{a \in \mathbb{R} \mid a > 0\}$ is a 2-nd root selection for $\mathbb{R}$, as $\mathbb{R}^* = R \cdot \mu_2(\mathbb{R})$ and $R \cap \mu_2(\mathbb{R}) = \{1\}$. At the same time it is also a 4-th root selection for $\mathbb{R}$, which is, however, not exact, as $|\mu_4(\mathbb{R})| = 2$.

On the other hand, for the field of Gaussian rationals $\mathbb{Q}(i)$, where $i = \sqrt{-1}$, one has $\mu_4(\mathbb{Q}(i)) = \{1, -1, i, -i\}$, which coincides with the group of units of the ring of Gaussian integers. As this ring is a unique factorization domain, it follows that $\mathbb{Q}(i)^* = R \cdot \mu_4(\mathbb{Q}(i))$ and $R \cap \mu_4(\mathbb{Q}(i)) = \{1\}$, where R is the subgroup of $\mathbb{Q}(i)^*$ generated by the element $(1 + i)$ and Gaussian primes of the form $a + bi$ with a odd and positive, and b even. R is thus a 4-th root selection, which is exact.

The first issue to consider is the existence of n-th root selections. First of all, we shall note that we can restrict our considerations to the case when n is a power of a prime number, which reflects the usual handling of taking n-th roots for composite n's – we will, however, continue to provide arguments without this additional assumption, at least when it will not lead to too much extra work:

PROPOSITION 2.5. *Let $n = r \cdot s$ with $\gcd(r, s) = 1$. A n-th root selection for F (containing a subset $T \subset F^*$) exists if and only if both r-th and s-th root selections exist for F (containing a subset $T \subset F^*$).*

PROOF. Note that $\mu_n(F) = \mu_r(F) \cdot \mu_s(F)$.

($\Rightarrow$) Assume there exists a multiplicative subgroup R of F^* (containing a subset $T \subset F^*$) such that $F^* = R \cdot \mu_n(F)$ and $R \cap \mu_n(F) = \{1\}$. Then $F^* = R \cdot \mu_r(F) \cdot \mu_s(F)$ and we shall show that $(R \cdot \mu_r(F)) \cap \mu_s(F) = \{1\}$. But this is clear: if $\omega \in (R \cdot \mu_r(F)) \cap \mu_s(F)$, say $\omega = a \cdot \omega'$ with $a \in R$ and $\omega' \in \mu_r(F)$, then $\omega, \omega' \in \mu_n(F)$ and hence $\frac{\omega}{\omega'} = a \in R \cap \mu_n(F)$, so that $\frac{\omega}{\omega'} = 1$ and $\mu_s(F) \ni \omega = \omega' \in \mu_r(F)$: as $\gcd(r, s) = 1$, this yields $\omega = 1$. Similarly, $(R \cdot \mu_s(F)) \cap \mu_r(F) = \{1\}$.

($\Leftarrow$) Assume there exist groups R_1 and R_2 (containing a subset $T \subset F^*$) such that $F^* = R_1 \cdot \mu_s(F) = R_2 \cdot \mu_r(F)$ and $R_1 \cap \mu_s(F) = R_2 \cap \mu_r(F) = \{1\}$. Thus, for every $a \in F^*$ there are unique $s_a \in R_1$ and $\omega \in \mu_s(F)$ such that $a = s_a\omega$, and for this choice of $s_a \in R_1$ there are unique $t_a \in R_2$ and $\omega' \in \mu_r(F)$ such that $s_a = t_a\omega'$. That $R = \{t_a \mid a \in F^*\}$ is a group (containing $T \subset F^*$) is apparent, so we have shown that $F^* = R \cdot \mu_r(F) \cdot \mu_s(F)$ and $R \cdot \mu_r(F) \cap \mu_s(F) = \{1\}$, which finishes the proof. □

In order to establish criteria for the existence of n-th root selections, we shall start with a slightly more general result:

THEOREM 2.6. *Let $T \subset F^*$ be a set of nonzero elements of F. Then there exists a n-th root selection for F containing T if and only if the subgroup $F^{*n}[T] < F^*$ generated by T and the group of all n-th powers intersects with $\mu_n(F)$ trivially.*

PROOF. ($\Rightarrow$) Assume that there exists a n-th root selection for F containing T, call it R. Observe that $F^{*n} \subset R$: indeed, for a fixed $c^n \in F^{*n}$, there exist $r \in R$ and $\omega \in \mu_n(F)$ such that $c = \omega r$, hence $c^n = \omega^n r^n = r^n \in R$. Therefore $F^{*n}[T] \subset R$. By Remark 2.3.1 $F^{*n}[T] \cap \mu_n(F) = \{1\}$.

($\Leftarrow$) Assume that $\mu_n(F) \cap F^{*n}[T] = \{1\}$. Say $n = 2^k l$ with $2 \nmid l$. By Proposition 2.5 it suffices to show that there exist both 2^k-th root selection containing T and l-th root selection containing T. Firstly, observe that $\mu_{2^k}(F) \cap F^{*2^k}[T] = \{1\}$ and $\mu_l(F) \cap F^{*l}[T] = \{1\}$: indeed, suppose that there exists $1 \neq \omega \in \mu_{2^k}(F)$ with $\omega \in F^{*2^k}[T]$, say $\omega = a^{2^k} t_1 \dots t_m$, $t_1, \dots, t_m \in T$ – then $\omega^l = a^{2^k l} t_1^l \dots t_m^l \in F^{*n}[T]$ and $(\omega^l)^{2^k l} = 1^{l^2}$, but $\omega^l \neq 1$, as the order of ω is a power of 2 and $2 \nmid l$, which yields a contradiction. Similar argument shows that $\mu_l(F) \cap F^{*l}[T] = \{1\}$.

Let $\mathcal{S} = \{S \mid S < F^*, F^{*2^k}[T] \subset S, \mu_{2^k}(F) \cap S = \{1\}\}$. Union of any chain $\mathcal{C}$ of elements of $\mathcal{S}$ is again an element of $\mathcal{S}$, so, by Zorn's Lemma, let R be a maximal element of $\mathcal{S}$. We shall show that R is the desired 2^k-th root selection.

Firstly, we claim that, for an element $b \in F^*$, if $b^2 \in R$, then either $b \in R$ or $-b \in R$. Indeed, assume that $b \notin R$. Then $R \cup bR$ is easily seen to be a group containing $F^{*2^k}[T]$ which, by maximality of R, intersects with $\mu_{2^k}(F)$ at some $\omega \neq 1$. Hence $\omega = br$, for some $r \in R$, and if $2^{k'}$ is the order of ω in $\mu_{2^k}(F)$, then $-1 = \omega^{2^{k'-1}} = b^{2^{k'-1}} r^{2^{k'-1}}$: if $k' > 1$ this leads to $-1 \in R$, which yields a contradiction, and if $k' = 1$ we get $-1 = br$, so that $-b \in R$.

By design $\mu_{2^k}(F) \cap R = \{1\}$ and it suffices to show that $F^* = \mu_{2^k}(F) \cdot R$. Suppose, *a contrario*, that there is an element $a \in F^*$ such that, for all $\omega \in \mu_{2^k}(F)$, $a\omega \notin R$. Let ω_0 be a generator of the cyclic group $\mu_{2^k}(F)$ and let $\operatorname{ord}(\omega_0) = 2^{k'}$, $k' \in \{1, \dots, k\}$. By the above claim, as $\omega_0^{2^{k'}} = 1 \in R$, necessarily $-\omega_0^{2^{k'-1}} \in R$. On the other hand $(a\omega_0)^{2^k} \in R$, so that either $(a\omega_0)^{2^{k-1}} \in R$ or $-(a\omega_0)^{2^{k-1}} \in R$. If the latter is the case, then

$$R \ni (-\omega_0^{2^{k'-1}})(-(a\omega_0)^{2^{k-1}}) = \omega_0^{2^{k-1}2^{k'-k}} (a\omega_0)^{2^{k-1}} = (a\omega_0^{2^{k'-k}+1})^{2^{k-1}}.$$

At any rate, $(a\omega)^{2^{k-1}} \in R$, for some $\omega \in \mu_{2^k}(F)$. Repeating the argument k times we eventually arrive at $a\omega \in R$, for some $\omega \in \mu_{2^k}(F)$, which yields a contradiction. This shows that F admits a 2^k-th root selection containing T.

For the proof of existence of an l-th root selection containing T, let now $\mathcal{S} = \{S \mid S < F^*, F^{*l}[T] \subset S, \mu_l(F) \cap S = \{1\}\}$. As before, let R be a

maximal element of $\mathcal{S}$, and it suffices to show that $F^* = \mu_l(F) \cdot R$. Suppose that for some $a \in F^*$, $a\omega \notin R$, for all possible $\omega \in \mu_l(F)$. As $a^l \in R$, the set $R \cup aR \cup a^2R \cup \ldots \cup a^{l-1}R$ is easily seen to be a group which, by maximality of R, intersects with $\mu_l(F)$ at some $\omega \neq 1$. Say $l' \in \{2, \ldots, l-1\}$ is the least integer such that $a^{l'}\omega \in R$, for some $\omega \in \mu_l(F) \setminus \{1\}$.

We claim that $l' \mid l$. Indeed, if $l = ql' + r$, for some $q, r \in \mathbb{Z}$, $0 < r < l'$, then

$$R \ni (a\omega)^l = (a\omega)^{ql'+r} = (a^{l'}\omega\omega^{l'-1})^q(a\omega)^r = (a^{l'}\omega)^q a^r \omega^{(l'-1)q+r},$$

so that $a^r\omega^{(l'-1)q+r} \in R$. By the minimality of l', this yields $\omega^{(l'-1)q+r} = 1$. Therefore $a^r \in R$ and, consequently, $a^{l'-r}\omega \in R$ with $l' - r \in \{1, \ldots, l'-1\}$. But $l' - r \neq 1$ by our assumptions, hence $l' - r \in \{2, \ldots, l'-1\}$ contradicting the minimality of l'.

Thus let $l = l'q$ for some $q \in \{2, \ldots, l-1\}$. But then

$$R \ni (a\omega)^l = (a\omega)^{l'q} = (a^{l'}\omega\omega^{l'-1})^q = (a^{l'}\omega)^q\omega^{(l'-1)q},$$

so that $\omega^{(l'-1)q} \in R$ and thus $\omega^{(l'-1)q} = 1$. As $(l'-1)q = l'q - q < l$ this implies $(l'-1)q \mid l$ and, in particular, $l' - 1 \mid l$. Since, at the same time, $l' \mid l$, this forces l to be even. But $2 \nmid l$ – a contradiction. □

A necessary and sufficient condition for a n-th root selection to exist now easily follows:

Corollary 2.7. *A multiplicative homomorphism ϕ from the group F^{*n} of n-th powers of F to F^* such that $\phi(c^n) = \omega_k c$, for some $k \in \{1, \ldots, n\}$, exists if and only if F^{*n} intersects with $\mu_n(F)$ trivially.*

Proof. In Theorem 2.6 take T to be empty. □

Corollary 2.8. *F admits a n-th root selection if and only if $\mu_n(F) = \mu_{n^2}(F)$.*

Proof. By Corollary 2.7 it suffices to observe that $\mu_n(F) = \mu_{n^2}(F)$ if and only if $\mu_n(F) \cap F^{*n} = \{1\}$. This is indeed the case: suppose $1 \neq \omega \in \mu_n(F)$ and $\omega = a^n$, for some $a \in F^*$ – then $a \in \mu_{n^2}(F)$ but $a \notin \mu_n(F)$; conversely, say $a \in \mu_{n^2}(F)$ and $a \notin \mu_n(F)$ – then $1 \neq a^n \in \mu_n(F)$. □

Remark 2.9.

1. Corollary 2.8 shows, in particular, that no algebraically closed field admits a n-th root selection.

2. Proposition 2.5 combined with Corollary 2.8 provide a convenient criterion to determine whether, for a given integer n and a field F, there exists a n-th root selection: let $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ be the prime decomposition of n with $k_1, k_2, \ldots, k_m \in \mathbb{N}$ and $p_1, p_2, \ldots, p_m$ pairwise disjoint primes. Then a n-th root selection for F exists if and only if:

$$\mu_{p_i^{k_i}}(F) = \mu_{p_i^{2k_i}}(F), \text{ for all } i \in \{1, \ldots, m\}.$$

This is equivalent to the condition that, for some $l_1, l_2, \ldots, l_m \in \mathbb{N}$ with $l_1 \leqslant k_1, l_2 \leqslant k_2, \ldots, l_m \leqslant k_m$:

$$F \text{ contains a } p_i^{l_i}\text{-th primitive root of unity}$$

and does not contain a $p_i^{l_i+1}$-th primitive root of unity, $i \in \{1, \ldots, m\}$.

Moreover, if $l_1 = k_1, l_2 = k_2, \ldots, l_m = k_m$, then the n-th root selection under consideration is exact. This is, more or less, clear; indeed, for the implication ($\Rightarrow$) fix $i \in \{1, \ldots, m\}$ and assume $\mu_{p_i^{k_i}}(F) = \mu_{p_i^{2k_i}}(F)$. Let ω be the generator of $\mu_{p_i^{k_i}}(F)$. Then $\omega \neq 1$, so that $\mathrm{ord}(\omega) = p_i^{l_i}$, for some $l_i \in \{1, \ldots, k_i\}$, and ω is a primitive $p_i^{l_i}$-th root of unity. If there existed $p_i^{l_i+1}$ roots of unity of degree $p_i^{l_i+1}$, then any such root would be also a $p_i^{2k_i}$-th root, and, consequently, $p_i^{k_i}$-th, and hence a $p_i^{l_i}$-th root, which is impossible, as there are only $p_i^{l_i}$ of them. Conversely, for the implication($\Leftarrow$) assume that, for $i \in \{1, \ldots, m\}$, F contains a $p_i^{l_i}$-th primitive root of unity and does not contain a $p_i^{l_i+1}$-st primitive root of unity, for some $l_i \leqslant k_i$. Thus $\mu_{p_i^{l_i}}(F) = \mu_{p_i^{l_i+1}}(F)$. Observe, that then F does not contain a $p_i^{l_i+2}$-nd primitive root of unity, for if such a root ω existed, then $\omega^{p_i}, \omega^{2p_i}, \ldots, \omega^{p_i^{l_i+1} p_i}$ would form $p_i^{l_i+1}$ roots of unity of degree $p_i^{l_i+1}$ which, as $\mathrm{ord}(\omega) = p_i^{l_i+2}$, would be pairwise disjoint, which is impossible. Thus $\mu_{p_i^{l_i+1}}(F) = \mu_{p_i^{l_i+2}}(F)$, and, consequently, $\mu_{p_i^{l_i+1}}(F) = \mu_{p_i^{2k_i}}(F)$, which implies $\mu_{p_i^{k_i}}(F) = \mu_{p_i^{2k_i}}(F)$, and

$$\omega^{p_i^{l_i}} = \omega^{p_i^{\ell s}} = \omega^{(p_i^{\ell})^s} = \omega^{(p_i^{\ell})(p_i^{\ell})^{s-1}} = (\omega^{p_i^{\ell}})^{(p_i^{\ell})^{s-1}} = 1.$$

Example 2.10. Consider the finite field $\mathbb{F}_{41}$ with 41 elements. As is well-known, $\mathbb{F}_{41}$ contains a n-th primitive root of unity if and only if $n \mid 41 - 1 = 2^3 \cdot 5$. Thus $\mathbb{F}_{41}$ contains primitive roots of degree $2, 2^2$ and 2^3 but not 2^k, $k \geq 4$, and of degree 5 but not 5^l, $l \geq 2$. Therefore, by Remark 2.9.2, $\mathbb{F}_{41}$ contains $20 = 2^2 \cdot 5$-th root selection (which is not exact) and $40 = 2^3 \cdot 5$-th root selection (which is exact), but does not contain $10 = 2 \cdot 5$-th root selection.

COROLLARY 2.11. *Let $a \in F^*$ and assume that $\mu_n(F) \cap F^{*n} = \{1\}$. Then there exists a n-th root selection R such that $a \in R$ if and only if $\omega a^k \notin F^{*n}$, for $\omega \in \mu_n(F) \setminus \{1\}$, $k \in \{1, \ldots, n-1\}$.*

PROOF. In Theorem 2.6 take $T = \{a\}$. Then $\mu_n(F) \cap F^{*n}[a] = \{1\}$ if and only if $\omega \neq c^n a^k$, for $c \in F^*$ and $\omega \in \mu_n(F) \setminus \{1\}$, $k \in \{1, \ldots, n-1\}$, or, equivalently, $\omega a^k \notin F^{*n}$, for $\omega \in \mu_n(F) \setminus \{1\}$, $k \in \{1, \ldots, n-1\}$. □

COROLLARY 2.12. *Let $a \in F^*$ and assume that $\mu_n(F) \cap F^{*n} = \{1\}$. Then a belongs to all n-th root selections in F if and only if $a \in F^{*n}$.*

REMARK 2.13.

1. We recall that an *ordering of level n* of a field F is a subset $P \subset F$ such that $P + P \subset P$, P^* is a subgroup of F^*, $-1 \notin P$ and F^*/P^* is a cyclic group with $|F^*/P^*| \mid n$. If $|F^*/P^*| = n$, we say that P has the *exact level* n. Orderings of higher level were first introduced in the case when $n = 2^p$, $p \in \mathbb{N}$ (see the classical monographs [1] and [5]), and soon generalized to the case of an arbitrary n (see [2]), where, at least when n is even, a version of the Artin-Schreier theory can be built. In particular, orderings of level n, with n even, exist in a field F if and only if F is *formally real*, that is when -1 is not a sum of squares in F. Clearly, for a formally real field F and for any n there exists a n-th root selection: if n is even, then $\mu_n(F) = \{1, -1\}$ and an ordering of level 1 is an example of a n-th root selection, whereas if n is odd, then $\mu_n(F) = \{1\}$ and F^* is trivially a n-th root selection.
2. Orderings of exact level 2 are simply called *orderings* and can be thought of as subsets $P \subset F$ such that $P + P \subset P$ and P^* is a subgroup of F^* of index 2. Now, subsets $P \subset F$ such that P^* is a subgroup of index 2 of F^* which fail to be orderings, i.e. such that the additive condition $P + P \subset P$ is not satisfied, are called *half-orderings*. Half-orderings were investigated in [4], and the concept was first introduced in [8] in a geometrical context; orderings and half-orderings are the easiest to understand examples of H-orderings associated to a subgroup H of the W-group of a field, which, in turn, is the Galois-theoretic analogue of the Witt ring that allows to extend methods and techniques from formally real fields to general fields of characteristic not 2 (see [7] for details). Readily, for a half-ordered field F and for any n there exists a n-th root selection: as we only deal with the multiplicative structure of F as far as root selections and half-orderings are concerned, the argument is, more or less, the same as for orderings – if n is even and $\mu_n(F) \cap F^{*n} \neq \{1\}$, then $-1 \in F^{*2}$; thus, if P is a conceivable half-ordering, $-1 \in P$, as P contains all squares of F (for $a^2 \in F^{*2}$, if $a \in P^*$ this is clear, and if $a \notin P^*$, then $P^* = (aP^*)^2 = a^2 P^*$, so that $a^2 \in P^*$ as well), but then $P = F$ (for $a \in F^*$, as $a^2 \in P^*$ and $|F^*/P^*| = 2$, either $a \in P^*$ or $-a \in P^*$, and in the latter case $a = (-1) \cdot (-a) \in P^*$), so

that P^* can not be a subgroup of F^* of index 2; for odd n, again, one uses Proposition 2.5.

3. In view of the above, it seems that what appears to be a common denominator for the theory of n-th root selections, the theory of orderings of level n and the theory of half-orderings is that they all lead to the study of subgroups $H^* < F^*$ such that F^*/H^* is cyclic. These subgroups (or, more generally, subgroups of finite index of the multiplicative group of a field) exhibit some interesting arithmetical properties and were studied by a number of authors (see, for example, [3]).

3. Extensions of 2^p-th root selections

In this Section we turn our attention to extensions of root selections.

Definition 3.1. Let $E \supset F$ be a field extension, let R be a n-th root selection for F. We say that R can be *extended* to a n-th root selection for E, if there exists a n-th root selection S for E such that $S \supset R$.

Alternatively, an extension of a n-th root selection R can be viewed as an extension of the homomorphism $F^{*n} \to F^*$ that defines R as in Lemma 2.1:

Lemma 3.2. *Let $E \supset F$ be a field extension. Let R be a n-th root selection for F and let S be a n-th root selection for E with $S \supset R$. Let $\phi : F^{*n} \to F^*$ be the homomorphism defined by R such that, for $c \in F^*$, $\phi(c^n) = \omega c$, for some $\omega \in \mu_n(F)$, and let $\psi : E^{*n} \to E^*$ be the homomorphism defined by S such that, for $\chi \in E^*$, $\psi(\chi^n) = \omega\chi$, for some $\omega \in \mu_n(E)$. Then $\psi \restriction_{F^{*n}} = \phi$.*

Proof. If, for a $c \in F^*$, $\phi(c^n) = \omega c \in \operatorname{Im}\phi = R \subset S, \omega \in \mu_n(F) \subset \mu_n(E)$, and $\psi(c^n) = \omega' c \in \operatorname{Im}\psi = S$, $\omega' \in \mu_n(E)$, with $\omega \neq \omega'$, then $1 \neq \frac{\omega}{\omega'} \in S$, contrary to Remark 2.3. □

Remark 3.3. It might, in principle, happen that when $E \supset F$ is a field extension, then E has more n-th roots of 1 than F, so that if S is a n-th root selection for E and $R = S \cap F$ is a n-th root selection for F, then $[E^* : S] > [F^* : R]$. In what follows this will cause us, on occasions while considering root selections in field extensions, to make an additional assumption that $|\mu_n(F)| = n$. Note that since $|\mu_n(F)| = n$, either $\operatorname{char}(F) = 0$ or $\operatorname{char}(F) = p$, $p \nmid n$, so, in particular, $\operatorname{char}(F) \neq 2$.

The existence of n-th root selections in field extensions is handled by the following result:

THEOREM 3.4. *Let $E \supset F$ be a field extension, let R be a n-th root selection for F with n even. Moreover, let $|\mu_n(F)| = n$.*

(1) *If $(E : F)$ is odd with $\gcd(n, (E : F)) = 1$, then R can be extended to a n-th root selection for E.*
(2) *If $s \in R$ and $M = F(\sqrt{s})$ with $(M : F) = 2$, then R can be extended to a n-th root selection for M.*

PROOF. Assume $(E : F)$ is odd. By Theorem 2.6 it suffices to show that $\mu_n(E) \cap E^{*n}[R] = \{1\}$. Suppose that for some $1 \neq \omega \in \mu_n(E)$, for $e \in E^*$ and for $r \in R$ one indeed has $\omega = e^n r$. Clearly $e \notin F^*$. Moreover, $F(e) \supset F$ is a Kummer extension with $(F(e) : F) = m$, $m \mid n$. But as $F \subsetneq F(e) \subset E$, $m \mid (E : F)$, contrary to the assumption that $\gcd(n, (E : F)) = 1$.

Assume $s \in R$ and $M = F(\sqrt{s})$. By Remark 3.3, $\mathrm{char}(F) \neq 2$. Since $|\mu_n(F)| = n$, $\mu_n(F) = \mu_n(M)$. Fix $r \in R$ and suppose that, for some $\omega \in \mu_n(M) = \mu_n(F)$ and for $a, b \in F$ one has $r = \omega(a + b\sqrt{s})^n$ with $\omega \neq 1$. In particular $(a + b\sqrt{s})^n \in F$, so that $b \neq 0$. But

$$(a + b\sqrt{s})^n = \left(\sum_{i=0}^{n/2} \binom{n}{2i} a^{n-2i} b^{2i} s^i\right) + \left(\sum_{j=0}^{n/2-1} \binom{n}{2j+1} a^{n-(2j+1)} b^{2j+1} s^j\right)\sqrt{s},$$

forcing $\left(\sum_{j=0}^{n/2-1} \binom{n}{2j+1} a^{n-(2j+1)} b^{2j+1} s^i\right) = 0$. Hence $(a + b\sqrt{s})^n = (a - b\sqrt{s})^n$, so that $\frac{a+b\sqrt{s}}{a-b\sqrt{s}} = \omega'$ for some $\omega' \in \mu_n(M) = \mu_n(F)$. Thus $(a + b\sqrt{s})^2 = \omega'(a^2 - b^2 s)$ yielding $a^2 + b^2 s + 2ab\sqrt{s} \in F$. This forces $2ab = 0$, which, in turn, as $b \neq 0$, yields $a = 0$. Therefore $r = \omega b^n s^{n/2}$, so that $\omega \in R$ – a contradiction. □

It is now natural to consider maximal n-th root selection fields, which should serve as analogs of real closed fields of higher level of [1] and [5]:

DEFINITION 3.5. F is called a *maximal n-th root selection field* if it contains a n-th root selection that cannot be extended to any larger algebraic extension of F.

The existence of maximal n-th root selection fields in characteristic $\neq 2$ is now pretty obvious:

THEOREM 3.6. *Let F be a field with $\mathrm{char}(F) \neq 2$ and let n be even. Let R be a n-th root selection for F. Then there exists a maximal n-th root selection field E such that $E \supset F$ and with n-th root selection extending R.*

PROOF. Let $\mathcal{S} = \{(E, S) \mid F^{\text{alg}} \supset E \supset F, S \text{ is } n\text{-th root selection for } E, S \supset R\}$. $\mathcal{S}$ is partially ordered by

$$(E, S) \prec (E', S') \Longleftrightarrow (E \subset E') \wedge (S \subset S')$$

and union of any chain $\mathcal{C}$ in $\mathcal{S}$ is again an element of $\mathcal{S}$, so by Zorn's Lemma $\mathcal{S}$ has a maximal element, which is the desired maximal n-th root selection field. □

4. Structure of maximal 2^p-th root selection fields

In this Section we shall investigate selected properties of maximal n-th root selection fields. We restrict to the special case $n = 2^p$ with the additional assumption that the fields under consideration contain primitive roots of unity of degree n. We start with some easy consequences of the results of the previous Section:

THEOREM 4.1. *Let F be a maximal n-th root selection field with n-th root selection R, n even. Let $|\mu_n(F)| = n$.*

(1) $R \subset F^{*2}$.
(2) *If $n = 2^p$, then $R \subset F^{*n}$.*
(3) *F is perfect.*
(4) *Finite extensions of F are of degree 2^m, for some $m \in \mathbb{N}$.*
(5) *In finite and proper extensions of F n-th powers and n-th roots of 1 intersect non-trivially.*
(6) *If $n = 2^p$, $p > 1$, then the absolute Galois group of F is isomorphic to the additive group of 2-adic integers.*
(7) *If $n = 2^p, p > 1$, and if F_r denotes the unique extension of F of degree 2^r,then F_r is a maximal 2^{p+r} root selection field.*

PROOF. By Remark 3.3, we may assume $\text{char}(F) \neq 2$.

(1) Suppose that there exists $s \in R$ such that $\sqrt{s} \notin F$. Then $F(\sqrt{s}) \supset F$ is of degree 2 and, by Theorem 3.4, R can be extended to a n-th root selection of $F(\sqrt{s})$, contrary to the maximality of F.
(2) Fix $r \in R$. By *1.* $r = a^2$, for some $a \in F^*$. We claim that either $a \in R$ or $-a \in R$: indeed, $\omega a \in R$, for some $\omega \in \mu_n(F)$, and thus $\omega^2 a^2 \in R$ leading to $\omega^2 \in R$. Thus $\omega^2 = 1$ and hence $\omega = 1$ or $\omega = -1$.
Now, by *1.*, either a is a square or $-a$ is a square, so that r is a 4-th power equal to either $\left(\sqrt{a}\right)^4$ or $\left(\sqrt{-1}\sqrt{a}\right)^4$. Repeating the argument p times we eventually show that r is a 2^p-th power.

(3) All fields of characteristic 0 are perfect. If $\operatorname{char} F = q > 2$, suppose that there exists $a \in F$ such that $\sqrt[q]{a} \notin F$. Then $F(\sqrt[q]{a}) \supset F$ is of odd degree and, by Theorem 3.4, R can be extended to a n-th root selection of $F(\sqrt[q]{a})$ – a contradiction.

(4) Let $E \supset F$ be a finite extension. Since F is perfect, every algebraic extension of F is separable. In particular, the normal closure of $E \supset F$, call it L, is separable, and hence Galois. Let H be the Sylov 2-subgroup of $\operatorname{Gal}(L/F)$. If the fixed field of H was different from F, it would be an extension of odd degree of F, hence it would admit a n-th root selection, contrary to the maximality of F. Therefore H is the full Galois group, and hence $(L : F)$ is a power of 2, and so is $(E : F)$.

(5) Let $E \supset F$ be a proper finite extension. Let L be the normal closure of $E \supset F$, which is hence Galois. As before, $(L : F)$ is a power of 2. Let P be the subgroup of $\operatorname{Gal}(L/F)$ that fixes E, and let M be a maximal proper subgroup of $\operatorname{Gal}(L/F)$ that contains P. Then the index of M in $\operatorname{Gal}(E/F)$ is equal to 2, and thus the fixed field of M is a quadratic extension of F contained in E. This fixed field cannot admit a n-th root selection, as that would contradict the maximality of F, and hence, by Theorem 2.7, n-th powers and n-th roots of 1 intersect non-trivially.

(6) Since F is perfect, the separable closure of F is the same as the algebraic closure F^{alg}. If $[F^{\mathrm{alg}} : F]$ was finite, then F would be real closed, which is impossible, since $|\mu_n(F)| = n$ with $n \geq 4$, so that, in particular, -1 is a square in F. Hence $[F^{\mathrm{alg}} : F]$ is infinite. Let L be any nontrivial finite Galois extension of F with Galois group G. By *5.* in L n-th roots of unity and n-th powers intersect non-trivially, but since $n = 2^p$, $p > 1$, this means that $\sqrt{-1} \in L$. Thus all proper subgroups of G contain the subgroup M fixing $\sqrt{-1}$. Therefore no automorphism τ in G outside of M can fix a nontrivial extension, and hence it generates the whole Galois group G. As before, G is cyclic whose order is a power of 2, so that we have the same structure for all intermediate fields, unique for each power of 2. Therefore $\operatorname{Gal}(F^{\mathrm{alg}}/F)$ is the inverse limit of some $\mathbb{Z}/2^m\mathbb{Z}$, that is the additive group of 2-adic numbers.

(7) We proceed by induction. If $r = 1$, then $F_1 = F\left(\sqrt{a}\right)$. By Corollary 2.7, suppose that $\mu_{2^{p+1}}(F_1)$ and $F_1^{*2^{p+1}}$ intersect non-trivially at $\alpha \neq 1$. Say $\alpha = \beta^{2^{p+1}}$ for some $\beta \in F_1$, consider the norm map $N_{F_1/F} : F_1 \to F$, and denote by $\overline{\gamma}$ the conjugate of an element $\gamma \in F_1$. As $N_{F_1/F}(\alpha)^{2^{p+1}} = N_{F_1/F}(\alpha^{2^{p+1}}) = N_{F_1/F}(1) = 1$, either $N_{F_1/F}(\alpha)^{2^p} = 1$ or $N_{F_1/F}(\alpha)^{2^p} = -1$. The latter case cannot occur, as -1 is a 2^p-th root of unity and $\mu_{2^p}(F) \cap F^{*2^p} = \{1\}$. Hence $N_{F_1/F}(\alpha)^{2^p} = 1$. On the other hand,

$$N_{F_1/F}(\alpha) = N_{F_1/F}(\beta^{2^{p+1}}) = N_{F_1/F}(\beta)^{2^{p+1}} = (N_{F_1/F}(\beta)^2)^{2^p},$$

leading to $N_{F_1/F}(\alpha) = 1$. Therefore

$$\left(\frac{\alpha}{\overline{\alpha}}\right)^{2^p} = \left(\frac{\alpha^2}{\alpha\overline{\alpha}}\right)^{2^p} = \frac{\alpha^{2^{p+1}}}{N_{F_1/F}(\alpha)} = 1,$$

so that $\frac{\alpha}{\overline{\alpha}}$ is a 2^p-th root of unity, and thus an element of F. Say $\alpha = x + y\sqrt{a}$ for some $x, y \in F$. Then

$$F \ni \frac{\alpha}{\overline{\alpha}} = \frac{\alpha^2}{\alpha\overline{\alpha}} = \frac{(x + y\sqrt{a})^2}{N_{F_1/F}(\alpha)} = (x^2 + y^2 a) + 2xy\sqrt{a},$$

leading to either $x = 0$ or $y = 0$. If $y = 0$, then $1 = N_{F_1/F}(\alpha) = N_{F_1/F}(x) = x^2$, so that either $x = -1$ or $x = 1$. The latter case cannot occur, as $\alpha = x \neq 1$. If $\alpha = x = -1$, then, as $1 = N_{F_1/F}(\alpha) = (N_{F_1/F}(\beta)^{2^p})^2$, either $N_{F_1/F}(\beta)^{2^p} = 1$ or $N_{F_1/F}(\beta)^{2^p} = -1$, and the latter case cannot occur as -1 is a 2^p-th root of unity. Therefore $N_{F_1/F}(\beta)^{2^p} = 1$, and thus

$$\left(\frac{\beta}{\overline{\beta}}\right)^{2^p} = \left(\frac{\beta^2}{\beta\overline{\beta}}\right)^{2^p} = \frac{\beta^{2^{p+1}}}{N(\beta)^{2^p}} = \frac{\alpha}{1} = -1,$$

so that $\beta^{2^p} = -\overline{\beta^{2^p}}$. Hence $\beta^{2^p} = z\sqrt{a}$ for some $z \in F$. Then $-1 = \alpha = \beta^{2^{p+1}} = z^2 a$, but as $p > 1$, $\sqrt{-1} \in F$, so that a is a square, which yields a contradiction. Hence $x = 0$, but this implies $1 = N_{F_1/F}(\alpha) = -y^2 a$, so that, again, a is a square yielding a contradiction. We have thus shown that F_1 admits a 2^{p+1}-st root selection R and it remains to prove that no algebraic extension of F_1 admits a 2^{p+1}-st root selection extension of R.

By 3. and 4. it suffices to show that no quadratic extension $E = F_1(\sqrt{\alpha})$ of F_1 admits a 2^{p+1}-st root selection extension of R. Firstly, observe that all 2^{p+1}-st roots of unity are already in F_1: take a nontrivial 2^p-th root of unity $\omega \in F_1$ which is also a 2^p-th power in F_1, say $\omega = \gamma^{2^p}$. Then $\omega^2 = \gamma^{2^{p+1}}$ and $(\omega^2)^{2^{p+1}} = (\omega^{2^p})^4 = 1$, so that $\omega^2 = 1$, as $\mu_{2^{p+1}}(F_1) \cap F_1^{*2^{p+1}} = \{1\}$. Hence either $\omega = -1$ or $\omega = 1$, the latter case being impossible due to nontriviality of ω. But this means $\gamma^{2^p} = -1$ and $\gamma^{2^{p+1}} = 1$, that is γ is a primitive 2^{p+1}-st root of unity in F_1.

Secondly, we claim that if $\alpha \in F_1$ is such an element that $\sqrt{\alpha} \notin F_1$, then the unique $\omega \in \mu_{2^p}(F)$ such that $\omega\alpha\overline{\alpha}$ is in the maximal 2^p-th root selection of F is a primitive root of unity in F. Indeed, suppose that, for some $\alpha \in F_1$ with $\sqrt{\alpha} \notin F_1$, $\omega\alpha\overline{\alpha} = b^{2^p}$, for some $b \in F^*$ and $\omega^{2^{p-1}} = 1$.

Thus $\alpha\overline{\alpha} = N_{F_1/F}(\alpha)$ is a square. Consider the square class exact sequence ([6], Theorem VII.3.8):

$$F^*/F^{*2} \xrightarrow{r} F_1^*/F_1^{*2} \xrightarrow{\overline{N_{F_1/F}}} F^*/F^{*2},$$

where $\overline{N_{F_1/F}}$ is induced by the norm map and $r\colon F^*/F^{*2} \to F_1^*/F_1^{*2}$ is given by $r(\beta F^{*2}) = \beta F_1^{*2}$. $N_{F_1/F}(\alpha)$ being a square means $\alpha F_1^{*2} \in \operatorname{Ker}\overline{N_{F_1/F}} = \operatorname{Im} r$, so that $\alpha F_1^{*2} = cF_1^{*2}$, for some $c \in F^*$, or, equivalently, $\alpha = c\beta^2$, for some $c \in F^*$ and $\beta \in F_1$. In order to obtain a contradiction, it suffices to show that c is, in fact, a square in F_1: if $\sqrt{c} \notin F^*$ then, by the already proven part of the theorem, the field $F(\sqrt{c})$ admits a 2^{p+1}-st root selection R'. In particular, $\omega'\sqrt{c} \in R'$, for some $\omega' \in \mu_{2^{p+1}}(F(\sqrt{c}))$. As F_1 contains a primitive 2^{p+1}-st root of unity, this really means $\omega' \in \mu_{2^{p+1}}(F_1)$. On the other hand, let $\omega'' \in \mu_{2^p}(F)$ be such that $\omega''c = d^{2^p}$, for some $d \in F^*$. Then $(\omega'')^2c^2 = d^{2^{p+1}} \in R'$ but, at the same time, $(\omega')^4c^2 = (\omega'\sqrt{c})^4 \in R'$ as well, so by the uniqueness of the choice of a 2^{p+1}-st root of unity in such a representation, $(\omega'')^2 = (\omega')^4$, so that $\omega'' = \pm(\omega')^2$: since $\sqrt{-1} \in F$, in both cases this leads to ω'' being a square of an element of F_1 and likewise c. This proves the claim.

To finish the proof suppose that $E = F_1(\sqrt{\alpha})$ admits a 2^{p+1}-st root selection extension S of R, where $\alpha \in F_1$ and $\sqrt{\alpha} \notin F_1$. Let $\omega_1, \omega_2 \in \mu_{2^{p+1}}(E) = \mu_{2^{p+1}}(F_1)$ be such that $\omega_1\sqrt{\alpha} \in S$ and $\omega_2\sqrt{\overline{\alpha}} \in S$. By the above claim, $\omega\alpha\overline{\alpha} = b^{2^p}$, for some $b \in F^*$ and $\omega \in \mu_{2^p}(F)$ with $\omega^{2^{p-1}} = -1$. Thus $\omega^2\alpha^2\overline{\alpha}^2 = b^{2^{p+1}} \in R$ and $\omega_1^4\omega_2^4\alpha^2\overline{\alpha}^2 \in S \cap F_1 = R$, so that $\omega = \pm\omega_1^2\omega_2^2$. As $\sqrt{-1} \in F$, this yields a contradiction.

Now, the inductive step is really no different from the $r = 1$ case. □

Finally, we are able to give equivalent definitions of maximal n-th root selection fields.

THEOREM 4.2. *Let F be a field and assume that F contains the n-th primitive root of unity ω_n, n even. Let F^{alg} denote the algebraic closure of F. The following conditions are equivalent:*

(1) *F is a maximal n-th root selection field;*
(2) *F is maximal among subfields E of F^{alg} such that $\mu_n(E) \cap E^{*n} = \{1\}$;*
(3) *F has a n-th root selection and no nontrivial finite extension of F does.*

PROOF. The sequence of implications 1. ⇒ 2. ⇒ 3. ⇒ 1. follows from the already proven results: 1. ⇒ 2. is Theorem 4.1.5, in 2. ⇒ 3. both the existence of a n-th root selection in F and the non-existence of a n-th root selection in E with $F^{\mathrm{alg}} \supset E \supsetneq F$ follows from Corollary 2.7, and 3. ⇒ 1. is basically just the definition of a maximal root selection field. □

References

[1] E. Becker, *Hereditarily Pythagorean Fields and Orderings of Higher Level*, Monografías de Matemática, 29, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1978.
[2] E. Becker, *Summen n-ter Potenzen in Körpern*, J. Reine Angew. Math. **307/308** (1979), 8–30.
[3] P. Berrizbeitia, *Additive properties of multiplicative subgroups of finite index in fields*, Proc. Amer. Math. Soc. **112** (1991), 365–369.
[4] J. Königsmann, *Half-ordered fields*, PhD thesis, Universität Konstanz, Konstanz, 1993.
[5] T.Y. Lam, *The theory of ordered fields*, in: B.R. McDonald (ed.), *Ring Theory and Algebra,* III, Lecture Notes in Pure and Appl. Math., 55, Dekker, New York, 1980, pp. 1–152.
[6] T.Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, 67, American Mathematical Society, Providence, RI, 2005.
[7] L. Mahé, J. Mináč and T.L. Smith, *Additive structure of multiplicative subgroups of fields and Galois theory*, Doc. Math. **9** (2004), 301–355.
[8] E. Sperner, *Die Ordnungsfunktionen einer Geometrie*, Math. Ann. **121** (1949), 107–130.
[9] W.C. Waterhouse. *Square root as a homomorphism*, Amer. Math. Monthly **119** (2012), 235–239.

Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice
Poland
e-mail: pawel.gladki@us.edu.pl