Symmetries of various sets of polynomials

Béranger Seguin*

Abstract. Let K be a field of characteristic 0, and let $k \geq 2$ be an integer. We prove that every K-linear bijection $f\colon K[X] \to K[X]$ strongly preserving the set of k-free polynomials (or the set of polynomials with a k-fold root in K) is a constant multiple of a K-algebra automorphism of $K[X]$, i.e., that there are elements $a, c \in K^\times$ and $b \in K$ such that $f(P)(X) = cP(aX + b)$. When K is a number field or $K = \mathbb{R}$, we prove that similar statements hold when f preserves the set of polynomials with a root in K.

Keywords: Linear preservers · Squarefree polynomials · Diophantine equations
Mathematics Subject Classification (MSC 2020): 47B49 · 15A86 · 12E05 · 26C10 · 12E25

Contents

1. Introduction 1
2. Root-permuting maps 4
3. Symmetries of the set of k-free polynomials 7
4. Symmetries of the set of polynomials with a root in a number field 12
5. Symmetries of the set of polynomials with a real root 13

1. Introduction

1.1. Introduction to linear preserver problems

An element of a ring B is *k-free* if it does not belong to m^k for any maximal ideal m of B. In [GK24, Theorem 1.1], Gundlach and Klüners show that if K is a number field and $f\colon \mathcal{O}_K \to \mathcal{O}_K$ is a $\mathbb{Z}$-linear map preserving the set of k-free elements of $\mathcal{O}_K$ for some $k \geq 2$, then f is of the form $x \mapsto c \cdot \sigma(x)$ where $c \in \mathcal{O}_K^\times$ is a unit and $\sigma \in \mathrm{Aut}(K)$ is a field automorphism of K. In other words, f is, up to a constant factor, an automorphism of the $\mathbb{Z}$-algebra $\mathcal{O}_K$. The motivation for that question comes from the study of dynamical systems and shift spaces associated to the set of k-free integers in a number field.

Our goal is to examine similar questions in different contexts. A general setting for these questions is the following:

Question 1.1. Let A be a ring and B be an A-algebra. Let S be a subset of B invariant under multiplication by units and under A-algebra automorphisms of B, i.e., invariant under the action of $B^\times \rtimes \mathrm{Aut}_{A\text{-alg}}(B)$. Let $\mathrm{Aut}^S_{A\text{-mod}}(B)$ be the set of A-module automorphisms $f\colon B \xrightarrow{\sim} B$ such that $f(S) = S$ (we say that f *preserves* S). When do $\mathrm{Aut}^S_{A\text{-mod}}(B)$ and $B^\times \rtimes \mathrm{Aut}_{A\text{-alg}}(B)$ coincide?

*Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany. Email: bseguin@math.upb.de.

Question 1.1 is similar to the family of "linear preserver problems" considered in matrix and operator theory [MM59, LP01, LT92, RdSP11]. An example is the following result of Dieudonné [Die48]: let K be a field and f be an endomorphism of the space of $n \times n$ matrices over K, such that a matrix M is invertible if and only if $f(M)$ is invertible; then, there are matrices $U, V \in \mathrm{GL}_n(K)$ such that f is either of the form $M \mapsto UMV$, or of the form $M \mapsto UM^TV$. The answer to Question 1.1 is then negative: up to multiplication by VU^{-1}, the former maps do correspond to K-algebra automorphisms, but the latter correspond to antiautomorphisms.

In situations where Question 1.1 does admit a positive answer, we can interpret this as saying that the additive structure of B as an A-module together with the subset S are "enough information" to reconstruct the multiplicative structure of B up to a scaling factor. Typically, Question 1.1 has a negative answer when the set S can be defined in terms of the additive structure of B only (for example, if S is $\varnothing$, $\{0\}$, B or $B \setminus \{0\}$), as then every A-module automorphism of B preserves S. Instead, we should consider sets S defined in terms of the multiplicative structure of B, e.g., the sets of units, squarefree or k-free elements, irreducible elements, etc.

1.2. Main results

In this article, we study instances of Question 1.1 where A is a field and B is a ring of polynomials in one variable over (an extension of) A. Our results are positive answers in three situations:

- (Theorem 3.1) K is a field of characteristic zero, $k \geq 2$ is an integer, and $S \subseteq K[X]$ is either the set of k-free polynomials, or the set of polynomials with a k-fold root in K.
- (Theorem 4.1) K is a number field and $S \subseteq K[X]$ is the set of polynomials with a root in K.
- (Theorem 5.1) $K = \mathbb{R}$ and $S \subseteq \mathbb{R}[X]$ is the set of polynomials with a real root.

In these three cases, we show that every K-linear bijection $f\colon K[X] \to K[X]$ such that $f(S) = S$ is of the form $P \mapsto c \cdot P \circ (aX + b)$ for constants $a, c \in K^\times$ and $b \in K$.

In fact, Theorem 4.1 is stronger than the statement above, as we consider more generally the case of a finite separable extension $L|K$ of Hilbertian fields and describe every K-linear bijection $L[X] \to L[X]$ preserving the set of polynomials with a root in L.

Relation with previous work. Linear preserver problems for polynomials have been considered in [Fis08, GS08, Mel15], mostly focusing on real polynomials and the location of their roots, and interpreting "f preserves S" in the weaker sense $f(S) \subseteq S$. There is also a large body of work on linear preservers of algebraic sets — notably zeros of matrix polynomials, cf. [How80, BGLS05]. For polynomials of fixed degree, our results about squarefree polynomials are somewhat related to the linear preservers of the algebraic set defined by the vanishing of the discriminant. However, the fact that we do not assume that our maps preserve degrees makes it difficult to use the language of algebraic geometry and of (finite-dimensional) algebraic varieties to think about this problem.

Polynomial rings are quite different from the rings of integers of number fields studied in [GK24], as they are not finite-dimensional. However, the fact that we obtain similar results in both cases is intriguing, and we may wonder whether these observations have a hidden common cause:

Question 1.2. Is there a negative answer to Question 1.1 satisfying the three following conditions?

- A is a Jacobson ring of characteristic 0 and B is a finitely generated commutative A-algebra, with $A \to B$ injective;
- The intersection of all maximal ideals m of B such that $A/(m \cap A) \simeq B/m$ is the zero ideal;
- S is the set of k-free elements of B for some $k \geq 2$.

(These hypotheses were chosen to mimic the existence of "enough" primes which split completely, as they are central in the argument of [GK24], while also including the case $A = K$, $B = K[X]$. See also Proposition 2.1.)

Other natural questions which are left for further study are the following:

- Does Theorem 3.1 hold in positive characteristic?
- Is there a field K which is not algebraically closed, and such that there is a K-linear bijection $K[X] \to K[X]$, preserving the set of polynomials with a root in K, which is not in $K^\times \rtimes \mathrm{Aut}_{K\text{-alg}}(K[X])$? Settling the case of non-Archimedean local fields would be a good start.

1.3. Notation

In this paper, the phrase "the map f preserves the set S" always means $f(S) = S$. A *k-fold root* of a polynomial P is a root of multiplicity $\geq k$. For a field extension $L|K$, we define the following groups:

$$\mathrm{Aut}_{K\text{-Vect}}(L[X]) \coloneqq \{f\colon L[X] \to L[X] \mid f \text{ is a } K\text{-linear bijection}\}$$

$$\mathrm{Aut}^{k\text{-free}}_{K\text{-Vect}}(L[X]) \coloneqq \left\{ f \in \mathrm{Aut}_{K\text{-Vect}}(L[X]) \;\middle|\; \forall P \in L[X],\ \begin{array}{c} P \text{ is } k\text{-free} \\ \Updownarrow \\ f(P) \text{ is } k\text{-free} \end{array} \right\}$$

$$\mathrm{Aut}^{k\text{-root}}_{K\text{-Vect}}(L[X]) \coloneqq \left\{ f \in \mathrm{Aut}_{K\text{-Vect}}(L[X]) \;\middle|\; \forall P \in L[X],\ \begin{array}{c} P \text{ has a } k\text{-fold root in } L \\ \Updownarrow \\ f(P) \text{ has a } k\text{-fold root in } L \end{array} \right\}$$

$$\mathrm{Aut}^{\mathrm{root}}_{K\text{-Vect}}(L[X]) \coloneqq \mathrm{Aut}^{1\text{-root}}_{K\text{-Vect}}(L[X])$$

1.4. Organization of the paper

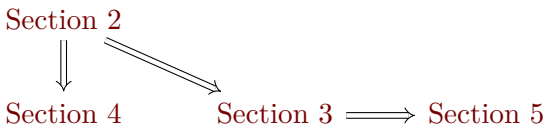
Section 2 consists of "technical" results (Theorem 2.2 and Corollary 2.3) which are used in the proofs of all main theorems.

In Section 3, we prove Theorem 3.1, which states that $\mathrm{Aut}^{k\text{-free}}_{K\text{-Vect}}(K[X]) = \mathrm{Aut}^{k\text{-root}}_{K\text{-Vect}}(K[X]) = K^\times \rtimes \mathrm{Aut}_{K\text{-alg}}(K[X])$ for all fields K of characteristic 0 and all integers $k \geq 2$. The proof is by induction on k, using Corollary 2.3 as a "replacement" for the case $k = 1$.

In Section 4, we prove Theorem 4.1, which states that $\mathrm{Aut}^{\mathrm{root}}_{K\text{-Vect}}(L[X]) = L^\times \rtimes \mathrm{Aut}_{K\text{-alg}}(L[X])$ for all extensions $L|K$ of number fields. The proof uses Hilbert's irreducibility theorem and Theorem 2.2.

In Section 5, we prove Theorem 5.1, which states that $\mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X]) = \mathbb{R}^\times \rtimes \mathrm{Aut}_{\mathbb{R}\text{-alg}}(\mathbb{R}[X])$. The proof proceeds by showing that $\mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X]) \subseteq \mathrm{Aut}^{2\text{-root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$, and applying Theorem 3.1 (or the weaker Theorem 3.8) to conclude.

The dependencies between the sections are summed up by the following diagram:



1.5. Acknowledgements

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) — Project-ID 491392403 — TRR 358. I thank Fabian Gundlach for listening to my endless discussions about this problem, and for suggesting the idea of using linear subspaces of fixed codimension to "track" the roots, and I thank the anonymous referee for their careful proofreading and their helpful corrections, and in particular for simplifying the final computation in the proof

of Theorem 3.8. I also thank Philippe Caldero for making a video version of the proof of the case $k = 2$ of Theorem 3.1 on his YouTube channel, which I highly recommend for French speakers: https://www.youtube.com/watch?v=2oF32X3UHK0.

2. Root-permuting maps

In this section, we characterize maps which preserve roots "up to a fixed permutation of the base field" (see Corollary 2.3 for a precise statement). The main results of this section are Theorem 2.2 and Corollary 2.3, which we use in all further sections. We begin with the following proposition, which is stated in an abstract way as it may be used to answer Question 1.1 in more general settings:

Proposition 2.1. *Let A be a ring, let B, B' be commutative A-algebras, and let f be an A-linear map $B \to B'$. Denote by $M_{\deg=1}(B)$ the set of maximal ideals m of B such that the canonical map $A \to B/m$ is surjective. For $m \in M_{\deg=1}(B)$, let $\mu(m)$ be the ideal of B' generated by $f(m)$, and assume that the intersection of all ideals $\mu(m)$ for $m \in M_{\deg=1}(B)$ is the zero ideal of B'. Then:*

$$\forall x, y \in B, \quad f(1)f(xy) = f(x)f(y).$$

If moreover $B = B'$ and f is bijective, then $f \in B^\times \rtimes \mathrm{Aut}_{A\text{-alg}}(B)$.

Proof. For each $m \in M_{\deg=1}(B)$, f induces a well-defined A-linear map $f_m \colon B/m \to B'/\mu(m)$ which fits in the following commutative diagram of A-linear maps:

$$\begin{array}{ccccc} A & \longrightarrow & B & \xrightarrow{f} & B' \\ & \searrow & \downarrow & & \downarrow \\ & & B/m & \xrightarrow[f_m]{} & B'/\mu(m) \end{array}$$

Fix $x, y \in B$. For each $m \in M_{\deg=1}(B)$, use surjectivity to choose elements $x_m, y_m \in A$ whose images in B/m coincide respectively with those of x and y. By A-linearity, we have $f(1)f(x_m y_m) = x_m y_m f(1)^2 = f(x_m)f(y_m)$, and thus $f_m(1)f_m(xy)$ equals $f_m(x)f_m(y)$ in $B'/\mu(m)$. The element $f(1)f(xy) - f(x)f(y)$ then belongs to $\bigcap_{m \in M_{\deg=1}(B)} \mu(m) = 0$ and hence $f(1)f(xy) = f(x)f(y)$.

Assume now that f is surjective and pick u such that $f(u) = 1$. Then, $f(1)f(u^2) = f(u)f(u) = 1$ and thus $f(1) \in B'^\times$. The A-linear map $g \colon B \to B'$ defined by $x \mapsto f(1)^{-1}f(x)$ satisfies $g(xy) = g(x)g(y)$ and hence is a morphism of A-algebras $B \to B'$. The last statement follows. □

(The proof can be summed up by the following slogan: at primes of degree 1, A-linearity implies local multiplicativity by unidimensionality; if there are enough primes of degree 1, then the local multiplicativity at all those primes implies multiplicativity.)

We now characterize linear maps which preserve roots of polynomials up to a fixed permutation of the base field. We include the case of a nontrivial algebraic field extension $L|K$ as we need it for the proof of Theorem 4.1. We include the possibility of a finite set S of exceptional elements of K because we need this generalization for the proof of Theorem 3.8.

Theorem 2.2. *Let $L|K$ be an algebraic field extension, with K infinite. Let S be a finite subset of L, and let $L' \coloneqq L \setminus S$. Let $\mu \colon L' \to L$ be an injective map and $f \colon L[X] \to L[X]$ be a K-linear map such that $f(1)$ does not vanish on $\mu(L')$, and such that*

$$\forall P \in L[X], \quad \forall x \in L', \quad [P(x) = 0] \Rightarrow [f(P)(\mu(x)) = 0].$$

Then, there is a polynomial $Y \in L[X]$ and an automorphism $\sigma \in \mathrm{Aut}(L|K)$ such that

$$\forall P \in L[X], \quad f(P) = f(1) \cdot (\sigma(P) \circ Y).$$

Moreover, the maps σ and $Y \circ \mu$ coincide on L'.

Proof. Let $K' \coloneqq K \cap L'$. For every element $u \in L^\times$, let f_u be the K-linear map $K[X] \to L[X]$ defined by $P \mapsto f(uP)$. By hypothesis, for any $x \in K'$, the image under f_u of the maximal ideal $(X-x) \in M_{\deg=1}(K[X])$ is contained in the ideal $(X-\mu(x))$ of $L[X]$. An element of $\bigcap_{x\in K'}(X-\mu(x))$ is a polynomial vanishing on the set $\mu(K')$ (which is infinite as μ is injective and K' is infinite) and hence is the zero polynomial. By Proposition 2.1, we have

$$\forall u \in L, \quad \forall P, Q \in K[X], \quad f(u)f(uPQ) = f(uP)f(uQ). \tag{2.1}$$

Consider arbitrary $x \in L$ and $P \in K[X]$, and apply Equation (2.1) with $Q = P$ and $u \in \{1, x, x+1\}$. We obtain

$$\begin{aligned} f(x+1)f((x+1)P^2) &= f(x)f(xP^2) + f(x)f(P^2) + f(1)f(xP^2) + f(1)f(P^2) \\ &= f(xP)^2 + f(x)f(P^2) + f(1)f(xP^2) + f(P)^2 \end{aligned}$$

but also

$$\begin{aligned} f(x+1)f((x+1)P^2) &= f((x+1)P)^2 \\ &= f(xP)^2 + 2f(xP)f(P) + f(P)^2 \end{aligned}$$

and thus

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

Multiplying both sides by $f(1)f(x)$ and applying Equation (2.1) again yields

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

which rewrites as $[f(1)f(xP) - f(x)f(P)]^2 = 0$. We have shown

$$\forall x \in L, \quad \forall P \in K[X], \quad f(1)f(xP) = f(x)f(P).$$

In other words, the K-linear map $g\colon L[X] \to L(X)$ defined by $P \mapsto \frac{f(P)}{f(1)}$ (the polynomial $f(1)$ is nonzero as it does not vanish on $\mu(L')$) satisfies:

$$\forall x \in L, \quad \forall P \in K[X], \quad g(xP) = g(x)g(P). \tag{2.2}$$

Moreover, by Equation (2.1) with $u = 1$, the restriction of g to $K[X]$ is a morphism of K-algebras $K[X] \to L(X)$. We define $Y \coloneqq g(X)$. Note that for any $x \in L'$, the polynomial $X - x$ vanishes at x and hence $g(X - x) = Y - g(x)$ vanishes at $\mu(x)$.

Consider arbitrary elements $u, v \in L$. We are going to prove that $g(uv) = g(u)g(v)$. If $v = 0$, then $g(uv) = g(u)g(v) = 0$; thus, we assume that $v \in L^\times$. Let $W(v)$ be the infinite set of elements $t \in K^\times$ such that $tv \in L'$. For $t \in W(v)$, the polynomial $(X-u)(X-tv) \in L[X]$ vanishes at tv, and thus the polynomial $g((X-u)(X-tv))$ vanishes at $\mu(tv)$. We have

$$\begin{aligned} g((X-u)(X-tv)) &= g\Big(X^2 - (u+tv)X + utv\Big) \\ &= Y^2 - g(u+tv)Y + tg(uv) \\ &= (Y - g(u))(Y - g(tv)) + t[g(uv) - g(u)g(v)]. \end{aligned}$$

Evaluating at $\mu(tv)$, we find that $0 = 0 + t[g(uv)(\mu(tv)) - g(u)(\mu(tv)) \cdot g(v)(\mu(tv))]$, so the rational function $g(uv) - g(u)g(v) \in L(X)$ vanishes on the infinite set $\{\mu(tv) \mid t \in W(v)\}$, and therefore it is zero. We have shown:

$$\forall u, v \in L, \quad g(uv) = g(u)g(v). \tag{2.3}$$

Now, consider a K-basis $(\beta_i)_{i\in I}$ of L and arbitrary polynomials $P, Q \in L[X]$, written as $P = \sum_{i\in I} \beta_i P_i$ and $Q = \sum_{i\in I} \beta_i Q_i$ with $P_i, Q_i \in K[X]$. We have:

$$\begin{aligned}
g(PQ) &= g\left(\sum_{i,j} \beta_i\beta_j P_i Q_j\right) \\
&= \sum_{i,j} g(\beta_i\beta_j) g(P_i Q_j) && \text{by Equation (2.2)} \\
&= \sum_{i,j} g(\beta_i) g(\beta_j) g(P_i) g(Q_j) && \text{by } \begin{cases}\text{Equation (2.3)}\\ \text{Equation (2.1) with } u = 1\end{cases} \\
&= \left(\sum_i g(\beta_i) g(P_i)\right)\left(\sum_j g(\beta_j) g(Q_j)\right) \\
&= g(P) g(Q) && \text{by Equation (2.2).}
\end{aligned}$$

We have shown that $g\colon L[X] \to L(X)$ is a morphism of K-algebras. As elements of L are algebraic over K, their images in $L(X)$ are algebraic over K and hence constant (i.e., they belong to L); this implies that g restricts to an automorphism $\sigma \in \mathrm{Aut}(L|K)$. We then have:

$$\forall P \in L[X], \quad g(P) = \sigma(P) \circ Y.$$

This implies:

$$\forall P \in L[X], \quad f(P) = f(1) \cdot (\sigma(P) \circ Y).$$

The fact that $f(X^n) = f(1)Y^n$ is a polynomial for all $n \geq 1$ implies that $Y \in L[X]$. It remains only to show that σ coincides with $Y \circ \mu$ on L'. For this, notice that for any $x \in L'$, the polynomial $X - x$ has a root at x, and hence $g(X - x) = Y - \sigma(x)$ has a root at $\mu(x)$ as $\mu(x) \in \mu(L')$ is not a root of $f(1)$. Evaluating at $\mu(x)$, we obtain $Y(\mu(x)) = \sigma(x)$. □

Corollary 2.3. *Let K be an infinite field. Let S be a finite subset of K and $K' \coloneqq K \setminus S$. Let $\mu\colon K \to K$ be a bijective map and $f_1, f_2\colon K[X] \to K[X]$ be two K-linear maps such that:*

$$\forall P \in K[X], \quad \forall x \in K', \quad P(x) = 0 \iff f_1(P)(\mu(x)) = 0 \iff f_2(P)(\mu^{-1}(x)) = 0.$$

Then, there are constants $a \in K^\times$ and $b \in K$ such that:

1. *$\mu(x) = \frac{x-b}{a}$ for all $x \in K'$*
2. *$f_1(P)(X) = f_1(1)P(aX + b)$ and $f_2(P)(X) = f_2(1)P\left(\frac{X-b}{a}\right)$, for all $P \in K[X]$*
3. *$f_1 \circ f_2 = f_2 \circ f_1 = f_1(1)f_2(1) \cdot \mathrm{id}$.*

Proof. Note that the hypothesis implies that $f_1(1)$ does not vanish on $\mu(K')$ and that $f_2(1)$ does not vanish on $\mu^{-1}(K')$. Applying Theorem 2.2 (with $L = K$) to the triples $(S, \mu|_{K'}, f_1)$ and $(S, \mu^{-1}|_{K'}, f_2)$, we deduce that there are polynomials $Y_1, Y_2 \in K[X]$ such that, for all $P \in K[X]$:

$$f_1(P) = f_1(1) \cdot (P \circ Y_1) \qquad \text{and} \qquad f_2(P) = f_2(1) \cdot (P \circ Y_2)$$

and such that both $Y_1 \circ \mu$ and $Y_2 \circ \mu^{-1}$ coincide with the identity on K'. In particular, the polynomial maps Y_1 and Y_2 coincide respectively with the maps μ^{-1} and μ outside the finite set $\mu(S) \cup \mu^{-1}(S)$. Since $\mu^{-1} \circ \mu = \mathrm{id}$, the algebraic equality $Y_1 \circ Y_2 = X$ holds in $K[X]$, and hence both Y_1 and Y_2 have degree 1. Writing Y_1 as $aX + b$, we have $Y_2 = \frac{X-b}{a}$ and $\mu(x) = Y_2(x)$ for $x \in K'$, and all points follow. □

Remark 2.4. When $L|K$ is a nontrivial extension, the conclusion of Theorem 2.2 could not follow directly from an application of Proposition 2.1 as the set $M_{\deg=1}(L[X])$ is empty when $L[X]$ is seen as a K-algebra.

3. Symmetries of the set of k-free polynomials

The goal of this section is to prove the following theorem:

Theorem 3.1. *Let K be a field of characteristic zero and $k \geq 2$ be an integer. Assume that $f\colon K[X] \to K[X]$ is a K-linear bijection preserving the set of k-free polynomials, or preserving the set of polynomials with no k-fold root in K. Then, there are constants $a, c \in K^\times$, $b \in K$ such that:*

$$\forall P \in K[X], \quad f(P) = c \cdot P \circ (aX + b).$$

In other words, $\mathrm{Aut}^{k\text{-free}}_{K\text{-Vect}}(K[X]) = \mathrm{Aut}^{k\text{-root}}_{K\text{-Vect}}(K[X]) = K^\times \rtimes \mathrm{Aut}_{K\text{-alg}}(K[X])$.

The proof of Theorem 3.1 is in two steps. First, we establish in Subsection 3.1 that maps in $\mathrm{Aut}^{k\text{-root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$ or in $\mathrm{Aut}^{k\text{-free}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$ preserve the set of polynomials with a given k-fold root "up to a fixed permutation of K". In Subsection 3.2, we show that maps with that property are of the expected form, by induction on k, reducing to Corollary 2.3 for the case $k = 1$. These pieces are put together in Subsection 3.3 to prove Theorem 3.1.

3.1. From non-k-free polynomials to k-fold roots

We fix an integer $k \geq 2$ and an infinite field K of characteristic zero or $> k$. The main result of this subsection is Corollary 3.4, which states that K-linear bijections preserving the set of k-free polynomials or the set of polynomials with no k-fold root in K actually preserve the set of polynomials with a given k-fold root "up to a fixed permutation of K". The starting point is the following lemma:

Lemma 3.2. *Let $x \in K$ and $P \in K[X]$. Let K' be the set of elements $\lambda \in K$ such that $P + \lambda(X-x)^k$ is not k-free. Assume that the cardinality of K' is at least $1 + \deg P$ (for example, if K' is infinite). Then, the polynomial $(X-x)^k$ divides P.*

Proof. By hypothesis, the following polynomial has positive degree for all $\lambda \in K'$:

$$\begin{aligned} g(\lambda) &\coloneqq \gcd\Big(P + \lambda(X-x)^k, P' + \lambda k(X-x)^{k-1}, \dots, P^{(k-1)} + \lambda k!(X-x)\Big) \\ &= \gcd\Big(P - \frac{1}{k}(X-x)P', P' + \lambda k(X-x)^{k-1}, \dots, P^{(k-1)} + \lambda k!(X-x)\Big) \end{aligned}$$

Denote by $\widetilde{P}$ the polynomial $P - \frac{1}{k}(X-x)P'$, which is independent of λ.

First assume that $\widetilde{P} = 0$, i.e., that $P = \frac{1}{k}(X-x)P'$. Let R be the monic greatest common divisor of P and $(X-x)^k$. We have $R = (X-x)^r$ for some integer $r \leq k$. If $r = k$, then $(X-x)^k$ divides P and we are done, so we assume that $r < k$. In particular, $k - r \in \{1, \dots, k\}$ is nonzero in K. Write $P = (X-x)^r Q$, where Q is not divisible by $(X-x)$. The differential equation $kP = (X-x)P'$ rewrites as $(k-r)Q = (X-x)Q'$, which implies that $(X-x)$ divides Q, a contradiction.

Assume now that $\widetilde{P} \neq 0$, and let $\widetilde{P}_1, \dots, \widetilde{P}_r$ be the monic irreducible factors of $\widetilde{P}$, of which there are at most $\deg P$. For each $\lambda \in K'$, $g(\lambda)$ is not constant and divides $\widetilde{P}$, and thus is a multiple of $\widetilde{P}_{i(\lambda)}$ for some $i(\lambda) \in 1, \dots, r$. Then, $(\widetilde{P}_{i(\lambda)})^k$ divides $P + \lambda(X-x)^k$. Since $|K'| > \deg P \geq r$, there are two distinct $\lambda_1, \lambda_2 \in K'$ such that $i(\lambda_1) = i(\lambda_2)$; we denote this common value by i_0. Then, $(\widetilde{P}_{i_0})^k$ divides $P + \lambda_1(X-x)^k$ and $P + \lambda_2(X-x)^k$, and hence divides both P and $(X-x)^k$. Since $(X-x)^k$ has no irreducible factor besides $X - x$, we have $\widetilde{P}_{i_0} = X - x$ and finally $(X-x)^k$ divides P. □

Corollary 3.3. *Let V be a K-linear subspace of $K[X]$ of codimension k containing only polynomials which are not k-free. Then, there is some $x \in K$ such that $V = (X-x)^k K[X]$.*

Proof. Since V has codimension k, the space V_k of polynomials of degree $\leq k$ in V has dimension at least 1. Since polynomials of degree $< k$ are k-free, they are not in V and thus V_k has dimension exactly 1. We have $V_k = K \cdot P$ for a monic polynomial P of degree k which is not k-free, and which is therefore of the form $(X-x)^k$ for some $x \in K$. For all $Q \in V$ and $\lambda \in K$, the polynomial $Q + \lambda(X-x)^k \in V$ is not k-free and thus $(X-x)^k$ divides Q by Lemma 3.2, as K is infinite. This establishes $V \subseteq (X-x)^k K[X]$. Since both spaces have codimension k, they are equal. □

Corollary 3.4. *Let $f\colon K[X] \to K[X]$ be a linear bijection mapping polynomials with a k-fold root in K to non-k-free polynomials. Then, there is a map $\mu_f\colon K \to K$ such that $x \in K$ is a k-fold root of P if and only if $\mu_f(x)$ is a k-fold root of $f(P)$. Moreover, if f^{-1} also maps polynomials with a k-fold root in K to non-k-free polynomials, then μ_f is bijective of inverse $\mu_{f^{-1}}$, and in particular f preserves the number of distinct k-fold roots that a given polynomial has in K.*

Proof. Let $x \in K$. The hypothesis implies that $f((X-x)^k K[X])$ is a subspace of $K[X]$ of codimension k consisting only of polynomials which are not k-free. By Corollary 3.3, there is a unique $\mu_f(x) \in K$ such that $f((X-x)^k K[X]) = (X-\mu_f(x))^k K[X]$. The other points follow. □

Remark 3.5. The hypothesis that the characteristic of K is zero or greater than k in Lemma 3.2 is crucial. For instance, assume that K is an infinite field of characteristic p and that k is a power of p. Let $x \in K^\times$. Then $(X-x)^k$ does not divide X^{2k} but, for any $\lambda \in K$ which is a k-th power, the polynomial $X^{2k} + \lambda(X-x)^k$ is not k-free as it equals $\left(X^2 + \sqrt[k]{\lambda}(X-x)\right)^k$.

3.2. From k-fold roots to $(k-1)$-fold roots

We fix a field K of characteristic zero. In this subsection, we prove Theorem 3.8, which characterizes K-linear bijections $K[X] \to K[X]$ preserving k-fold roots up to a fixed permutation of K. The proof is by induction on k, using the results of Section 2 for the case $k = 1$, and using the following lemma to relate the cases k and $k-1$:

Lemma 3.6. *Let $k \geq 2$ be an integer, let $P, Q \in K[X]$, and let $x \in K$ be such that at least one of $P(x)$ and $Q(x)$ is nonzero. Then, x is a $(k-1)$-fold root of $PQ' - P'Q$ if and only if x is a k-fold root of $\lambda P + \nu Q$ for some $(\lambda, \nu) \in K^2 \setminus \{(0,0)\}$.*

Proof. Using the equality $\left(\det\begin{pmatrix} A & B \\ C & D \end{pmatrix}\right)' = \det\begin{pmatrix} A' & B' \\ C & D \end{pmatrix} + \det\begin{pmatrix} A & B \\ C' & D' \end{pmatrix}$ repeatedly, we obtain:[1]

$$\forall n \in \mathbb{N}, \quad (PQ' - P'Q)^{(n)} = \left(\det\begin{pmatrix} P & Q \\ P' & Q' \end{pmatrix}\right)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} \cdot \det\begin{pmatrix} P^{(i)} & Q^{(i)} \\ P^{(n+1-i)} & Q^{(n+1-i)} \end{pmatrix}.$$

Now, assume that there exists $(\lambda, \nu) \in K^2 \setminus \{(0,0)\}$ such that $x \in K$ is a k-fold root of $\lambda P + \nu Q$, i.e., that the vectors $\left(P(x), P'(x), \ldots, P^{(k-1)}(x)\right)$ and $\left(Q(x), Q'(x), \ldots, Q^{(k-1)}(x)\right)$ are colinear. Then, all the determinants $\det\begin{pmatrix} P^{(i)}(x) & Q^{(i)}(x) \\ P^{(n+1-i)}(x) & Q^{(n+1-i)}(x) \end{pmatrix}$ vanish for $0 \leq i \leq n \leq k-1$, so x is a $(k-1)$-fold root of $PQ' - P'Q$.

Conversely, assume that x is a $(k-1)$-fold root of $PQ' - P'Q$. We show by induction on $n \in \{0, \ldots, k-1\}$ that $\left(Q(x), Q'(x), \ldots, Q^{(n)}(x)\right)$ and $\left(P(x), P'(x), \ldots, P^{(n)}(x)\right)$ are colinear, and more precisely that:

$$P(x) \cdot \left(Q(x), Q'(x), \ldots, Q^{(n)}(x)\right) - Q(x) \cdot \left(P(x), P'(x), \ldots, P^{(n)}(x)\right) = 0.$$

Note that $(-Q(x), P(x)) \in K^2 \setminus \{(0,0)\}$ as x is not a common root of P and Q. The result for $n = 0$ is clear. Fix an $n \in \{1, \ldots, k-1\}$, and assume that $P(x) \cdot (Q(x), Q'(x), \ldots, Q^{(n-1)}(x)) -$

[1] If we take cancellations of determinants into account, we can be more precise:

$$\left(\det\begin{pmatrix} P & Q \\ P' & Q' \end{pmatrix}\right)^{(n)} = \sum_{i=0}^{\lceil n/2 \rceil} C(n-i, i) \cdot \det\begin{pmatrix} P^{(i)} & Q^{(i)} \\ P^{(n+1-i)} & Q^{(n+1-i)} \end{pmatrix}$$

where $C(n,p)$ denotes Catalan numbers.

$Q(x) \cdot (P(x), P'(x), \dots, P^{(n-1)}(x)) = 0$. In particular, all determinants $\det\begin{pmatrix} P^{(i)}(x) & Q^{(i)}(x) \\ P^{(j)}(x) & Q^{(j)}(x) \end{pmatrix}$ for $i, j \in \{0, \dots, n-1\}$ vanish. We have:

$$\begin{aligned} 0 = (PQ' - P'Q)^{(n-1)}(x) &= \sum_{i=0}^{n-1} \binom{n-1}{i} \cdot \det\begin{pmatrix} P^{(i)}(x) & Q^{(i)}(x) \\ P^{(n-i)}(x) & Q^{(n-i)}(x) \end{pmatrix} \\ &= \det\begin{pmatrix} P(x) & Q(x) \\ P^{(n)}(x) & Q^{(n)}(x) \end{pmatrix} \end{aligned}$$

and hence $P(x)Q^{(n)}(x) - Q(x)P^{(n)}(x) = 0$. By induction, we have shown:

$$P(x) \cdot \Big(Q(x), Q'(x), \dots, Q^{(k-1)}(x)\Big) - Q(x) \cdot \Big(P(x), P'(x), \dots, P^{(k-1)}(x)\Big) = 0.$$

Hence, there is a pair $(\lambda, \nu) \in K^2 \setminus \{(0,0)\}$ such that x is a k-fold root of $\lambda P + \nu Q$, namely $\lambda = -Q(x)$ and $\nu = P(x)$. □

We also need the following small lemma:

Lemma 3.7. *Let $P, Q \in K[X]$ be polynomials satisfying $PQ' = P'Q$, with $P \neq 0$. Then, there is a constant $\lambda \in K$ such that $Q = \lambda P$.*

Proof. If $Q = 0$, we can take $\lambda = 0$. Hence, we assume that $Q \neq 0$. Comparing the leading monomials of PQ' and $P'Q$ shows that P and Q must have the same degree, so $Q = \lambda P + \widetilde{Q}$ for some $\lambda \in K^\times$ and some $\widetilde{Q} \in K[X]$ of degree $< \deg P$. The equality $PQ' = P'Q$ implies $P\widetilde{Q}' = P'\widetilde{Q}$. By the same arguments as those used for Q, this can only occur if $\deg \widetilde{Q} = \deg P$, which is not true, or if $\widetilde{Q} = 0$, which implies the claim. □

Let $\int : K[X] \to K[X]$ be the linear map taking a polynomial to its formal antiderivative vanishing at 0, i.e., the linear map induced by $X^n \mapsto \frac{X^{n+1}}{n+1}$, which is well-defined as K has characteristic zero. For all polynomials $P \in K[X]$, we have $(\int P)' = P$ and $\int (P') = P - P(0)$.

Theorem 3.8. *Let $k \geq 1$ be an integer. Let S be a finite subset of K and $K' := K \setminus S$. Let $\mu : K \to K$ be a bijective map and let $f_1, f_2 : K[X] \to K[X]$ be two K-linear maps such that, for all $P \in K[X]$ and $x \in K'$:*

$$x \text{ is a } k\text{-th root of } P \iff \mu(x) \text{ is a } k\text{-th root of } f_1(P) \iff \mu^{-1}(x) \text{ is a } k\text{-th root of } f_2(P). \quad (3.1)$$

Then, there are constants $a \in K^\times$ and $b \in K$ such that:

1. *$\mu(x) = \frac{x-b}{a}$ for all but finitely many $x \in K$*
2. *$f_1(P)(X) = f_1(1)P(aX + b)$ and $f_2(P)(X) = f_2(1)P\Big(\frac{X-b}{a}\Big)$, for all $P \in K[X]$*
3. *$f_1 \circ f_2 = f_2 \circ f_1 = f_1(1)f_2(1) \cdot \mathrm{id}$.*

Proof. We reason by induction on k. The case $k = 1$ is Corollary 2.3. Let $k \geq 2$, and assume that the theorem holds for $k - 1$.

Let $P \in K[X]$. Note that $P = (\int P)' = \det\begin{pmatrix} 1 & \int P \\ 1' & (\int P)' \end{pmatrix}$.

Let $x \in K'$, and assume that x does not belong to the finite set $S_2' \coloneqq \{\mu(y) \mid y \text{ root of } f_2(1)\}$. Then:

$$\begin{aligned}
&\Big[x \text{ is a } (k-1)\text{-fold root of } P\Big] \\
\Leftrightarrow &\Big[\exists(\lambda,\nu) \in K^2 \setminus \{(0,0)\},\ x \text{ is a } k\text{-fold root of } \lambda \cdot 1 + \nu \cdot \textstyle\int P\Big] && \text{by Lemma 3.6} \\
\Leftrightarrow &\Big[\exists(\lambda,\nu) \in K^2 \setminus \{(0,0)\},\ \mu^{-1}(x) \text{ is a } k\text{-fold root of } \lambda \cdot f_2(1) + \nu \cdot f_2(\textstyle\int P)\Big] && \text{by } \begin{cases} x \in K' \\ \text{Equation (3.1)} \end{cases} \\
\Leftrightarrow &\Big[\mu^{-1}(x) \text{ is a } (k-1)\text{-fold root of } f_2(1)f_2(\textstyle\int P)' - f_2(1)'f_2(\textstyle\int P)\Big] && \text{by } \begin{cases} x \notin S_2' \\ \text{Lemma 3.6} \end{cases}
\end{aligned}$$

Define the K-linear map $\widetilde{f_2}\colon P \mapsto f_2(1)f_2(\int P)' - f_2(1)'f_2(\int P)$. We have shown:

$$\forall x \in K' \setminus S_2', \quad [x \text{ is a } (k-1)\text{-fold root of } P] \iff [\mu^{-1}(x) \text{ is a } (k-1)\text{-fold root of } \widetilde{f_2}(P)]$$

Symmetrically, the K-linear map $\widetilde{f_1}\colon P \mapsto f_1(1)f_1(\int P)' - f_1(1)'f_1(\int P)$ and the finite set $S_1' \coloneqq \{\mu(y) \mid y \text{ root of } f_1(1)\}$ satisfy:

$$\forall x \in K' \setminus S_1', \quad [x \text{ is a } (k-1)\text{-fold root of } P] \iff [\mu(x) \text{ is a } (k-1)\text{-fold root of } \widetilde{f_1}(P)]$$

Define the finite set $S' = S \cup S_1' \cup S_2'$. By the induction hypothesis, applied to $(S', \mu, \widetilde{f_1}, \widetilde{f_2})$, there are constants $a \in K^\times$ and $b \in K$ such that $\mu(x) = \frac{x-b}{a}$ for all but finitely many $x \in K$ and such that, for all $P \in K[X]$:

$$\widetilde{f_1}(P)(X) = \widetilde{f_1}(1)P(aX+b) \qquad \text{and} \qquad \widetilde{f_2}(P)(X) = \widetilde{f_2}(1)P\Big(\frac{X-b}{a}\Big).$$

The first equation implies:

$$f_1(1)f_1(P)' - f_1(1)'f_1(P) = \widetilde{f_1}(1)P'(aX+b) \tag{3.2}$$

To simplify notations, we replace f_1 by the map $P \mapsto f_1\Big(P \circ \frac{X-b}{a}\Big)$, so that $a = 1$ and $b = 0$. Our goal then becomes to prove that $f_1(P) = f_1(1)P$ for all polynomials $P \in K[X]$ (the case of f_2 is symmetrical, and the third point follows from the second point).

Using Euclidean division, write $\widetilde{f_1}(1) = Q \cdot f_1(1)^2 + R$ for polynomials $Q, R \in K[X]$ satisfying $\deg R < 2\deg f_1(1)$, and define the K-linear map $h_Q\colon K[X] \to K[X]$ by:

$$h_Q(P) \coloneqq f_1(1) \cdot [QP - Q'(\textstyle\int P) + Q''(\int^2 P) - \dots]$$

which is a finite sum as Q is a polynomial. Note that:

$$\begin{aligned}
f_1(1)h_Q(P)' - f_1(1)'h_Q(P) =& f_1(1)^2 \cdot [QP' + Q'P - Q'P - Q''(\textstyle\int P) + Q''(\int P) + Q'''(\int^2 P) - \dots] \\
&+ f_1(1)f_1(1)' \cdot [QP - Q'(\textstyle\int P) + Q''(\int^2 P) - \dots] \\
&- f_1(1)'f_1(1) \cdot [QP - Q'(\textstyle\int P) + Q''(\int^2 P) - \dots] \\
=& f_1(1)^2 QP'.
\end{aligned}$$

Now define $g_1 \coloneqq f_1 - h_Q$. For all polynomials $P \in K[X]$, we have:

$$\begin{gathered}
f_1(1)g_1(P)' - f_1(1)'g_1(P) = RP' \\
\deg R < 2\deg f_1(1).
\end{gathered} \tag{3.3}$$

We prove by contradiction that $R = 0$. Assume that R is nonzero. Then, $2\deg f_1(1) > \deg R$ implies that $f_1(1)$ is non-constant. Let P be any polynomial of degree $2\deg f_1(1) - \deg R$ (which is a positive integer). Using Equation (3.3), we get:

$$\deg\Big(f_1(1)g_1(P)' - f_1(1)'g_1(P)\Big) = \deg(RP') = 2\deg f_1(1) - 1.$$

We can also compute the degree directly:

$$\deg\Big(f_1(1)g_1(P)' - f_1(1)'g_1(P)\Big) \leq \deg f_1(1) + \deg g_1(P) - 1$$

with equality if and only if $\deg f_1(1) \neq \deg g_1(P)$. But this means that $\deg f_1(1)$ and $\deg g_1(P)$ are equal if and only if they are not equal, which is absurd. We have shown that $R = 0$.

For all $P \in K[X]$, Equation (3.3) then becomes $f_1(1)g_1(P)' = f_1(1)'g_1(P)$, so by Lemma 3.7 there is a linear form $u\colon K[X] \to K$, mapping a polynomial P to the constant $u(P) = \frac{g_1(P)}{f_1(1)}$. Unfolding the definitions of g_1 and h_Q, the equality $g_1(P) = u(P)f_1(1)$ rewrites as:

$$f_1(P) = f_1(1) \cdot [QP - Q'(\textstyle\int P) + Q''(\int^2 P) - \cdots + u(P)]. \tag{3.4}$$

Let $\widetilde{S}$ be the finite set obtained by adding the roots of $f_1(1)$ to S. Let x be an element of $K \setminus \widetilde{S}$, and let $\ell \geq k$. Since $x \notin S$, x is a (k-fold) root of the polynomial

$$f_1\Big((X-x)^\ell\Big) = f_1(1) \cdot \left[\sum_{i\geq 0} \ell! Q^{(i)} \frac{(X-x)^{\ell+i} - \sum_{j=0}^{i-1} \binom{\ell+i}{j} X^j (-x)^{\ell+i-j}}{(\ell+i)!} + \sum_{i=0}^{\ell} \binom{\ell}{i} (-x)^{\ell-i} u(X^i)\right].$$

Evaluating at x and dividing by $f_1(1)(x)$ (which we may do as $x \notin \widetilde{S}$), we obtain:

$$\begin{aligned} 0 &= \sum_{i\geq 0} -\ell! Q^{(i)}(x) \sum_{j=0}^{i-1} \binom{\ell+i}{j} \frac{(-1)^j (-x)^{\ell+i}}{(\ell+i)!} + \sum_{i=0}^{\ell} \binom{\ell}{i} (-x)^{\ell-i} u(X^i) \\ &= -\ell! \sum_{i\geq 1} Q^{(i)}(x) \sum_{j=0}^{i-1} \frac{(-1)^j}{j!(\ell+i-j)!} (-x)^{\ell+i} + \sum_{i=0}^{\ell} \binom{\ell}{i} (-x)^{\ell-i} u(X^i). \end{aligned}$$

This equality holds for all $x \in K \setminus \widetilde{S}$. Since $K \setminus \widetilde{S}$ is infinite, the corresponding polynomial in x equals the zero polynomial. In particular, $u(1) = u(X) = \cdots = u(X^{\ell-1}) = u(X^\ell) = 0$ (coefficients in front of $x^\ell, x^{\ell-1}, \ldots, x^0$). Since this holds for all $\ell \geq k$, the linear form u is identically zero. Thus, we have the following equality of polynomials for all $\ell \geq k$:

$$0 = \sum_{i\geq 1} Q^{(i)} \sum_{j=0}^{i-1} \frac{(-1)^j}{j!(\ell+i-j)!} (-X)^{\ell+i}. \tag{3.5}$$

For any fixed $i \geq 1$, the formula $\binom{\ell+i}{j} = \binom{\ell+i-1}{j} + \binom{\ell+i-1}{j-1}$ lets us simplify the inner (telescoping) sum

$$\sum_{j=0}^{i-1} \frac{(-1)^j}{j!(\ell+i-j)!} = \frac{1}{(\ell+i)!} \sum_{j=0}^{i-1} (-1)^j \binom{\ell+i}{j} = \frac{1}{(\ell+i)!} (-1)^i \binom{\ell+i-1}{i-1} = \frac{(-1)^i}{\ell!(\ell+i)(i-1)!}$$

so the right-hand side of Equation (3.5) rewrites as

$$\sum_{i\geq 1} Q^{(i)} \sum_{j=0}^{i-1} \frac{(-1)^j}{j!(\ell+i-j)!} (-X)^{\ell+i} = \sum_{i\geq 1} \frac{Q^{(i)}(-1)^i}{\ell!(\ell+i)(i-1)!} (-X)^{\ell+i} = \frac{(-X)^\ell}{\ell!} \sum_{i\geq 1} \frac{Q^{(i)} X^i}{(\ell+i)(i-1)!}.$$

Assume that Q is non-constant, and let $a_d X^d$ be the leading monomial of Q (with $d \geq 1$, $a_d \neq 0$). The coefficient in front of $X^{\ell+d}$ in the right-hand side of Equation (3.5) is then

$$\frac{(-1)^\ell}{\ell!} \sum_{1\leq i\leq d} \frac{d!}{(d-i)!(\ell+i)(i-1)!} \cdot a_d$$

which is nonzero (a_d is nonzero, and the rational number by which it is multiplied is nonzero, as a nonempty sum of nonzero rational numbers of same sign), contradicting Equation (3.5).

We have shown by contradiction that Q is constant. Letting $P = 1$ in Equation (3.4) shows that $Q = 1$. Finally, Equation (3.4) rewrites as $f_1(P) = f_1(1)P$. □

3.3. Proof of Theorem 3.1

Let $f \in \mathrm{Aut}^{k\text{-free}}_{K\text{-Vect}}(K[X])$ or $f \in \mathrm{Aut}^{k\text{-root}}_{K\text{-Vect}}(K[X])$. By Corollary 3.4, there is a bijective map $\mu\colon K \to K$ such that $f\big((X-x)^k K[X]\big) = \big(X-\mu(x)\big)^k K[X]$ for all $x \in K$. By Theorem 3.8, applied to $S = \varnothing$, $f_1 = f$ and $f_2 = f^{-1}$, there are constants $a \in K^\times$ and $b \in K$ such that $f(P) = f(1)\cdot P\circ(aX+b)$ for all $P \in K[X]$. Since f is surjective, $f(1)$ is a nonzero constant $c \in K^\times$. This concludes the proof of Theorem 3.1.

4. Symmetries of the set of polynomials with a root in a number field

Fix a number field K (or any Hilbertian field, such as $\mathbb{Q}^{\mathrm{ab}}$ or any function field in at least one variable over a field) and a finite (separable) extension $L|K$. In this section, we prove the following theorem:

Theorem 4.1. *Let $f\colon L[X] \to L[X]$ be a K-linear bijection preserving the set of polynomials with a root in L. Then, there are constants $a, c \in L^\times$, $b \in L$, and an automorphism $\sigma \in \mathrm{Aut}(L|K)$ such that*

$$\forall P \in L[X], \quad f(P) = c\cdot\sigma(P)\circ(aX+b).$$

In other words, $\mathrm{Aut}^{\mathrm{root}}_{K\text{-Vect}}(L[X]) = L^\times \rtimes \mathrm{Aut}_{K\text{-alg}}(L[X])$.

First, we prove the following lemma using Hilbert's irreducibility theorem:

Lemma 4.2. *Let $P, Q \in L[X]$ be coprime polynomials, and assume that for all $\lambda \in K$, the polynomial $P+\lambda Q$ has a root in L. Then, both P and Q have degree at most 1.*

Proof. Let $f = \frac{P}{Q} \in L(X)$ and $D = \max(\deg P, \deg Q)$. Then, f defines a morphism $\mathbb{P}^1_L \to \mathbb{P}^1_L$ of degree D and, by hypothesis, all of K is contained in $f(\mathbb{P}^1(L))$. Assume that $D > 1$, so that $f(\mathbb{P}^1(L))$ is a thin set, and its complement is a Hilbertian subset of $\mathbb{P}^1(L)$ containing no element of K. By [FJ08, Corollary 12.2.3], this Hilbertian set contains a Hilbertian subset of $\mathbb{P}^1(K)$. Thus, the empty set (in $\mathbb{P}^1(K)$) is Hilbertian, contradicting the fact that K is Hilbertian. We have shown that $D = 1$. □

As a consequence, a version of Corollary 3.3 holds also for $k = 1$ in the case of Hilbertian fields:

Corollary 4.3. *Linear K-subspaces of $L[X]$ of codimension $[L:K]$ containing only polynomials with a root in L are exactly subspaces of the form $(X-x)L[X]$ for some $x \in L$.*

Proof. Let V be such a linear subspace. Since V has codimension $[L:K]$, which is the dimension of the space of polynomials of degree ≤ 0, and since nonzero polynomials of degree ≤ 0 do not have a root in L, we have $V \oplus L = L[X]$. The space V' of polynomials of degree ≤ 1 in V has dimension exactly $[L:K]$, and nonzero elements of V' are polynomials with degree exactly 1.

Let $P \in V' \setminus \{0\}$ and $Q \in V$ of degree ≥ 2, and assume that P does not divide Q. Then, Q is coprime to P since $\deg P = 1$. Moreover, $P+\lambda Q$ belongs to V and hence has a root in L, for all $\lambda \in K$. But then, Lemma 4.2 implies $\deg Q \leq 1$, which contradicts the hypothesis. Therefore, every element of $V' \setminus \{0\}$ divides every element of V of degree ≥ 2.

Fix any polynomial $Q_0 \in V$ of degree 2, which is split since it has a root in L, and let x_1, x_2 be its roots in L (which may be equal). As seen previously, any $P \in V' \setminus \{0\}$ divides Q_0, which means that V' is covered by the two vector spaces $L\cdot(X-x_1)$ and $L\cdot(X-x_2)$. As the field K is infinite, this implies $V' \subseteq L\cdot(X-x_i)$ for some $i \in \{1,2\}$. Since these spaces both have dimension $[L:K]$, we have the equality $V' = L\cdot(X-x_i)$. To show that all polynomials in V are divisible by $X-x_i$, remark that they either belong to $V' = L\cdot(X-x_i)$, or they are of degree ≥ 2 and are then divisible by $X-x_i \in V'\setminus\{0\}$. We have proved that $V \subseteq (X-x_i)L[X]$. Since these spaces have the same codimension $[L:K]$, this is an equality. □

Finally, we prove Theorem 4.1:

Proof of Theorem 4.1. Let $f \in \mathrm{Aut}^{\mathrm{root}}_{K\text{-Vect}}(L[X])$. For all $x \in L$, the image of $(X-x)L[X]$ under f is a K-subspace of $L[X]$ of codimension $[L:K]$ consisting only of polynomials with a root in L. By Corollary 4.3, this implies that there is a map $\mu\colon L \to L$ such that $f((X-x)L[X]) = (X-\mu(x))L[X]$ for all $x \in K$. Doing the same for f^{-1} shows that μ is bijective. Let S be the finite set $\{\mu^{-1}(x) \mid f(1)(x)=0\} \cup \{\mu(x) \mid f^{-1}(1)(x)=0\}$ and $L' = L \setminus S$. Applying Theorem 2.2 to the triples $(S, \mu|_{L'}, f)$ and $(S, \mu^{-1}|_{L'}, f^{-1})$ shows that there are polynomials $Y_1, Y_2 \in L[X]$ and automorphisms $\sigma, \tau \in \mathrm{Aut}(L|K)$ such that:

$$\forall P \in L[X], \quad f(P) = f(1)\cdot(\sigma(P)\circ Y_1) \qquad \text{and} \qquad f^{-1}(P) = f^{-1}(1)\cdot(\tau(P)\circ Y_2)$$

and such that $\begin{cases} \sigma & \text{coincides with} \quad Y_1 \circ \mu \\ \tau & \text{coincides with} \quad Y_2 \circ \mu^{-1} \end{cases}$ on L'. Since f is surjective, $f(1)$ is a nonzero constant $c \in L^\times$, and $f^{-1}(1) = \frac{1}{\sigma^{-1}(c)}$. At all but finitely many points, we have the equality $\sigma \circ \tau = \sigma \circ Y_2 \circ \mu^{-1} = \sigma(Y_2) \circ \sigma \circ \mu^{-1} = \sigma(Y_2) \circ Y_1$. But then the polynomial $\sigma(Y_2)\circ Y_1 \in L[X]$ coincides with the identity $X \in L[X]$ when evaluated at all but finitely many elements of K (forming an infinite subset of L). This implies the algebraic equality $\sigma(Y_2)\circ Y_1 = X$ and thus $\sigma \circ \tau = \mathrm{id}$, i.e., $\tau = \sigma^{-1}$. Moreover, the equality $\sigma(Y_2)\circ Y_1 = X$ in $L[X]$ implies that both Y_1 and Y_2 are polynomials of degree 1. If we write $Y_1 = aX+b$, then $Y_2 = \sigma^{-1}\left(\frac{X-b}{a}\right) = \frac{X-\sigma^{-1}(b)}{\sigma^{-1}(a)}$. □

5. Symmetries of the set of polynomials with a real root

The goal of this section is to prove the following theorem:

Theorem 5.1. *Let f be a $\mathbb{R}$-linear bijective map $\mathbb{R}[X] \to \mathbb{R}[X]$ preserving the set of polynomials with a real root. Then, there are real numbers $a, c \in \mathbb{R}^\times$ and $b \in \mathbb{R}$ such that:*

$$\forall P \in \mathbb{R}[X], \quad f(P) = c \cdot P \circ (aX+b).$$

In other words, $\mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X]) = \mathbb{R}^\times \rtimes \mathrm{Aut}_{\mathbb{R}\text{-alg}}(\mathbb{R}[X])$.

In Subsection 5.1, we prove lemmas which imply that maps in $\mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$ preserve the set of polynomials with a given degree, and in Subsection 5.2 we show that these maps preserve the set of polynomials which have a real double root. In Subsection 5.3, we prove Theorem 5.1 by combining the lemmas from the first two subsections with Theorem 3.8.

Remark 5.2. Without the bijectivity hypothesis, there are additional maps even if we require $f(1) = 1$. For instance, the map $f\colon P \mapsto P \circ Q$, where $Q \in \mathbb{R}[X]$ is a non-constant polynomial whose derivative has no real roots of odd multiplicity (e.g. $Q = X^3$), preserves the set of polynomials with a real root.

Remark 5.3. The naive variant of Corollary 3.3/Corollary 4.3 does not hold for real roots: there are many linear subspaces of $\mathbb{R}[X]$ of codimension 1 consisting only of polynomials with a real root, and which are not of the form $(X-x)\mathbb{R}[X]$. Here is a way to construct such subspaces: let μ be a nonzero positive measure on $\mathbb{R}$ with all moments finite (for example, such that its support $\mathrm{Supp}(\mu)$ is compact), and let L be the subspace (of codimension 1) of polynomials $P \in \mathbb{R}[X]$ such that $\int_{\mathbb{R}} P \,\mathrm{d}\mu = 0$. If $P \in L$, then either P vanishes everywhere on $\mathrm{Supp}(\mu)$ in which case P has a real root, or P must take values of both signs on $\mathrm{Supp}(\mu)$ for the integral to vanish, so P has a zero in the convex hull of $\mathrm{Supp}(\mu)$ by the intermediate value theorem. Thus, all polynomials $P \in L$ have a real root. For instance, if μ is the sum of two Dirac measures concentrated respectively at -1 and 1, then L is the space of polynomials P satisfying $P(1)+P(-1)=0$, which all have a real root; that space is spanned by the polynomials $X, X^2-1, X^3, X^4-1, X^5, X^6-1, \ldots$

5.1. The sets $V(P,Q)$ and $S(P)$

In this subsection, we describe properties of the following sets:

- for $P, Q \in \mathbb{R}[X]$, we let $V(P,Q) \coloneqq \{\lambda \in \mathbb{R} \mid P - \lambda Q \text{ has a real root}\}$
- for $P \in \mathbb{R}[X]$, we let $S(P) \coloneqq \{Q \in \mathbb{R}[X] \mid V(Q,P) \text{ is bounded}\}$

In Lemma 5.6, we characterize the set of polynomials of degree $\leq n$ for any even n in terms of the sets $S(P)$. This is later used to prove that any map $f \in \mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$ preserves the set of polynomials of a given degree.

Lemma 5.4. *Let $P, Q \in \mathbb{R}[X]$. If P and Q have a common real root, then $V(P,Q) = \mathbb{R}$. Otherwise, $V(P,Q)$ is the image of $\frac{P}{Q}$.*

Proof. If $P(x) = Q(x) = 0$, then $P - \lambda Q$ has the real root x for all $\lambda \in \mathbb{R}$, which shows $V(P,Q) = \mathbb{R}$. Assume now that P and Q have no common real root. Let y be in the image of $\frac{P}{Q}$, i.e., $P(x) = yQ(x)$ for some real number x such that $Q(x) \neq 0$. Then, $P - yQ$ has the real root x. Conversely, if $P - yQ$ has the real root x, then $P(x) = yQ(x)$. If $Q(x) = 0$, then $P(x) = 0$ contradicts the fact that P and Q have no common real root. Therefore, $Q(x) \neq 0$ and $\frac{P(x)}{Q(x)} = y$. □

Lemma 5.5. *Let $P \in \mathbb{R}[X]$. If P has a real root, then $S(P)$ is empty. Otherwise, $S(P)$ is the space of polynomials of degree $\leq \deg P$.*

Proof. By Lemma 5.4, the set $S(P)$ is the set of polynomials having no common real root with P, and such that the function $\frac{Q}{P}$ is bounded. If P has a real root x, then for every polynomial Q sharing no real root with P, the function $\frac{Q}{P}$ has asymptotes at x and hence takes unbounded values; thus, $S(P) = \varnothing$. Now, assume that P has no real root. Then, $S(P)$ is the set of polynomials Q such that the function $\frac{Q}{P}$ (which has no asymptotes at any real number) is bounded on $\mathbb{R}$; this amounts to the fact that it does not become infinite at $\pm\infty$, i.e., that $\deg Q \leq \deg P$. □

Lemma 5.6. *Let n be an even integer and V be a subspace of $\mathbb{R}[X]$. Then, V is the space of polynomials of degree at most n if and only if $\dim(V) = n+1$ and $V = S(P_0)$ for some $P_0 \in V$.*

Proof. If V is the space of polynomials of degree at most n, which has dimension $n+1$, then the polynomial $P_0 = X^n + 1 \in V$ has no real root and has degree n, and hence $S(P_0) = V$ by Lemma 5.5. Conversely, assume that $\dim(V) = n+1$ and that $V = S(P_0)$ for some $P_0 \in V$. By Lemma 5.5, the polynomial P_0 has no real root and V is the space of polynomials of degree $\leq \deg P_0$. Since $\dim V = n+1$, we have $\deg P_0 = n$. □

5.2. Quadratic polynomials and double roots

In this subsection, we characterize polynomials having a given $x \in \mathbb{R}$ as a double root using only the "additive" structure of polynomials and the property of having a real root (assuming we can "recognize" polynomials of degrees 0, 1 and 2, and nonnegative polynomials).

Lemma 5.7. *Let $x \in \mathbb{R}$, and let P be a polynomial of degree 2 such that $P + b(X-x) + c$ has a real root if and only if $b^2 \geq 4c$. Then, $P = (X-x)^2$.*

Proof. Write $P = \alpha(X-x)^2 + \beta(X-x) + \gamma$ with $\alpha \neq 0$. The hypothesis says that

$$[(\beta + b)^2 \geq 4\alpha(\gamma + c)] \iff [b^2 \geq 4c],$$

i.e., the affine transformation $\begin{cases} b & \mapsto & b + \beta \\ c & \mapsto & \alpha c + \alpha\gamma \end{cases}$ preserves the set $\{(b,c) \mid b^2 \geq 4c\}$, and hence preserves its boundary, the parabola $b^2 = 4c$. This implies $(b+\beta)^2 = \alpha b^2 + 4\alpha\gamma$ for all $b \in \mathbb{R}$. Equating the coefficients of the corresponding polynomials in b, we obtain $1 = \alpha$, $2\beta = 0$ and $\beta^2 = 4\alpha\gamma$, from which follows that $(\alpha, \beta, \gamma) = (1, 0, 0)$ and thus $P = (X-x)^2$. □

Lemma 5.8. *Let P be a polynomial of even degree with positive leading coefficient, and $x \in \mathbb{R}$. Then, x is a double root of P if and only if there is a $\lambda_0 \in \mathbb{R}$ such that the polynomial $P + \lambda(X-x)^2$ has image $\mathbb{R}^+$ for any $\lambda > \lambda_0$.*

Proof. First assume that x is a double root of P, and write $P = (X-x)^2\widetilde{P}$. Then, $P + \lambda(X-x)^2 = (\widetilde{P} + \lambda)(X-x)^2$. Since $\widetilde{P}$ is a polynomial of even degree and positive leading coefficient, it has a global minimum $m \in \mathbb{R}$. Taking $\lambda_0 = -m$, we have $\widetilde{P}(t) + \lambda \geq 0$ for all $\lambda > \lambda_0$ and all $t \in \mathbb{R}$, and then the polynomial $P + \lambda(X-x)^2$ has image $\mathbb{R}^+$ (it is nonzero, everywhere nonnegative, and vanishes at x).

Conversely, assume that there is a $\lambda_0 \in \mathbb{R}$ such that the polynomial $P + \lambda(X-x)^2$ has image $\mathbb{R}^+$ for any $\lambda > \lambda_0$. In particular, for any $\lambda > \lambda_0$, the polynomial $P + \lambda(X-x)^2$ has a root and since that polynomial is nonnegative, that root is of even multiplicity — in particular, it has multiplicity at least 2. Then, Lemma 3.2 (with $k = 2$) implies that $(X-x)^2$ divides P. □

Lemma 5.9. *Let $P \in \mathbb{R}[X]$ and $x \in \mathbb{R}$. Then, x is a double root of P if and only if there are polynomials $P_1, P_2 \in \mathbb{R}[X]$ of even degree and positive leading coefficient such that $P = P_1 - P_2$ and such that x is a double root of both P_1 and P_2.*

Proof. If $P = P_1 - P_2$ and both P_1 and P_2 have x as a double root, then x is a double root of P. Conversely, assume that x is a double root of P. If $P = 0$, take $P_1 = P_2 = (X-x)^2$. If P has even degree, take $(P_1, P_2) = (P, 0)$ if P has positive leading coefficient and $(P_1, P_2) = (0, -P)$ otherwise. If P has odd degree n, take $P_1 = (X-x)^{n+1} + P$ and $P_2 = (X-x)^{n+1}$. □

5.3. Proof of Theorem 5.1

Let $f \in \mathrm{Aut}^{\mathrm{root}}_{\mathbb{R}\text{-Vect}}(\mathbb{R}[X])$. Note that, for all polynomials $P, Q \in \mathbb{R}[X]$:

$$V(f(P), f(Q)) = V(P, Q) \qquad \text{and} \qquad S(f(P)) = f(S(P)). \tag{5.1}$$

By Lemma 5.6, this implies that f preserves the set of polynomials of degree $\leq n$ when n is even. In particular, the case $n = 0$ implies that f maps constant polynomials to constant polynomials. We reduce to the case $f(1) = 1$ by replacing f by $\frac{f}{f(1)}$.

Let $P \in \mathbb{R}[X]$. Then, Equation (5.1) implies that $V(f(P), 1) = V(P, 1)$, which by Lemma 5.4 means that the polynomials P and $f(P)$ have the same image. In particular:

- f maps polynomials of odd degree (surjective polynomials) to polynomials of odd degree;
- f maps polynomials of even degree to polynomials of even degree, with a leading coefficient of the same sign, and with the same global minimum/maximum. In particular, f preserves the set of nonnegative polynomials.

The map f then preserves the set of polynomials of degree n:

- when n is odd, because they are the polynomials whose degree is odd, $\leq n+1$ and not $\leq n-1$.
- when n is even, because they are the polynomials whose degree is even, $\leq n$ and not $\leq n-2$.

In particular, $f(X)$ is a polynomial of degree 1, which we write as $aX + b$ with $a \in \mathbb{R}^\times$ and $b \in \mathbb{R}$. We reduce to the case $f(X) = X$ by replacing f by $P \mapsto f\left(P \circ \left(\frac{X-b}{a}\right)\right)$.

Let $u \in \mathbb{R}$. By Lemma 5.7, f maps $(X-u)^2$ to $(X-u)^2$. Then, Lemma 5.8 implies that f preserves the set of polynomials with even degree and positive leading coefficient having u as a double root. By Lemma 5.9, this implies that f preserves the set $(X-u)^2\mathbb{R}[X]$ of all polynomials having u as a double root. We conclude using Theorem 3.8 with $k = 2$, $S = \varnothing$, $\mu = \mathrm{id}_{\mathbb{R}}$ and $(f_1, f_2) = (f, f^{-1})$.

References

[BGLS05] LeRoy B. Beasley, Alexander E. Guterman, Sang-Gu Lee, and Seok-Zun Song. Linear preservers of zeros of matrix polynomials. *Linear Algebra and its Applications*. 401, pp. 325–340. 2005. DOI: 10.1016/j.laa.2004.08.015.

[Die48] Jean Dieudonné. Sur une généralisation du groupe orthogonal à quatre variables. *Archiv der Mathematik*. 1, pp. 282–287. 1948. DOI: 10.1007/BF02038756.

[Fis08] Steve Fisk. Polynomials, roots, and interlacing. 2008. arXiv: math/0612833.

[FJ08] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Berlin, Heidelberg. 2008. DOI: 10.1007/978-3-031-28020-7. ISBN: 978-3-031-28019-1.

[GK24] Fabian Gundlach and Jürgen Klüners. Symmetries of power-free integers in number fields and their shift spaces. 2024. arXiv: 2407.08438.

[GS08] Alexander Guterman and Boris Shapiro. On linear operators preserving the set of positive polynomials. *Journal of Fixed Point Theory and Applications*. 3(2), pp. 411–429. 2008. DOI: 10.1007/s11784-008-0084-3.

[How80] Ralph Howard. Linear maps that preserve matrices annihilated by a polynomial. *Linear Algebra and its Applications*. 30, pp. 167–176. 1980. DOI: 10.1016/0024-3795(80)90192-5.

[LP01] Chi-Kwong Li and Stephen Pierce. Linear preserver problems. *The American Mathematical Monthly*. 108(7), pp. 591–605. 2001. DOI: 10.2307/2695268.

[LT92] Chi-Kwong Li and Nam-Kiu Tsing. Linear preserver problems: A brief introduction and some special techniques. *Linear Algebra and its Applications*. 162–164, pp. 217–235. 1992. DOI: 10.1016/0024-3795(92)90377-M.

[Mel15] Eugeny Melamud. Linear operators on polynomials preserving roots in open circular domains. *Proceedings of the American Mathematical Society*. 143(12), pp. 5213–5218. 2015. DOI: 10.1090/proc/12109.

[MM59] Marvin Marcus and Benjamin N. Moyls. Linear transformations on algebras of matrices. *Canadian Journal of Mathematics*. 11, pp. 61–66. 1959. DOI: 10.4153/CJM-1959-008-0.

[RdSP11] Bernard Randé and Clément de Seguins Pazzis. The linear preservers of real diagonalizable matrices. *Linear Algebra and its Applications*. 435(6), pp. 1257–1266. 2011. DOI: 10.1016/j.laa.2011.03.014.