Can. J. Math. Vol. **43** (6), 1991 pp. 1281–1293

GROUPS, COVERINGS AND GALOIS THEORY

VAGN LUNDSGAARD HANSEN AND PETER PETERSEN, V

ABSTRACT. Finite extensions of complex commutative Banach algebras are naturally related to corresponding finite covering maps between the carrier spaces for the algebras. In the case of function rings, the finite extensions are induced by the corresponding finite covering maps, and the topological properties of the coverings are strongly reflected in the algebraic properties of the extensions and conversely. Of particular interest to us is the class of finite covering maps for which the induced extensions of function rings admit primitive generators. This is exactly the class of polynomial covering maps and the extensions are algebraic extensions defined by the underlying Weierstrass polynomials.

The purpose of this paper is to develop a suitable Galois theory for finite extensions of function rings induced by finite covering maps and to apply it in the case of Weierstrass polynomials and polynomial covering maps.

In a series of papers the relations between the algebra of a Weierstrass polynomial on the one hand and the topology of the associated polynomial covering map on the other hand have been investigated: [9], [10], [11]. The purpose of this paper is to develop a suitable Galois theory for certain extensions of function algebras naturally associated with Weierstrass polynomials and polynomial covering maps.

Throughout the paper, X is a path connected, compact Hausdorff topological space. By $C(X)$ we denote the ring of complex valued, continuous functions on X. A Weierstrass polynomial of degree $n \geq 1$ over X is then an element $P(x, z)$ of degree n in the polynomial ring $C(X)[z]$ in one complex variable $z \in \mathbb{C}$ over $C(X)$. If $P(x, z)$ is separable, in earlier papers called simple, i.e. without multiple roots for any $x \in X$, then projection of the zero set $E \subset X \times \mathbb{C}$ for $P(x, z)$ onto X defines an n-fold covering map $\pi: E \longrightarrow X$, called the associated polynomial covering map, [7],[8]. The topological equivalence class of this covering map is characterized by the quotient algebra $C(X)[z]/\left(P(x, z)\right)$, called the characteristic algebra of the polynomial covering map, [10],[11].

More generally, if $\pi: E \longrightarrow X$ is an arbitrary n-fold covering map, the dual map $\pi^*: C(X) \longrightarrow C(E)$ is a monomorphism along which we can consider $C(E)$ as a ring extension of $C(X)$, or, as an algebra over $C(X)$. Again as shown in [10], this $C(X)$-algebra characterizes the topological equivalence class of the covering map. In his thesis [17], one of the authors has studied such extensions among others, and has prepared the way for a suitable Galois theory relating subgroups of the automorphism group for the ring extension $\pi^*: C(X) \longrightarrow C(E)$ to intermediate covers of X.

The purpose of this paper is to present such a Galois theory and to apply it in the case of Weierstrass polynomials and polynomial covering maps.

Received by the editors May 28, 1990.
AMS subject classification: 57M12, 13B25, 46J10.

Earlier related work include papers of Childs [2], Magid [14], Wajnryb [19], Zame [20] and the book by DeMeyer and Ingraham [3], for the purely algebraic case of separable extensions of algebras. Of significance is also the fundamental paper of Gorin and Lin [6] where such a Galois theory is hinted at but not developed, and the important paper of Arnol'd [1] in which he proves that an entire algebraic function in $n = 2^r$, $r \geq 2$, variables cannot be represented as a superposition of entire algebraic functions of a smaller number of variables. We shall however redevelop the theory in our own context, which in our opinion is more explicit and direct.

Both authors gratefully acknowledge the University of Maryland at College Park where this collaboration was initiated. The first author also acknowledges support from the Danish Natural Science Research Council.

1. **Groups, coverings, function algebras.** Throughout the paper, X denotes a compact, path connected space with universal covering space $\tilde{X}$ and fundamental group G. If H is a subgroup of G we write $H < G$, and $H \ll G$ if H is a normal subgroup of G. In the latter case, $H\backslash G$ denotes the group of right cosets of H in G.

To each subgroup $H < G$, there corresponds a covering map $\pi: X(H) \longrightarrow X$, where $X(H)$ is path connected and has fundamental group H. The covering space $X(H)$ can be constructed as the space of H-orbits $\tilde{X}/H$ for the action of H on $\tilde{X}$ induced by viewing elements in G as deck transformations on $\tilde{X}$. The covering map $\pi: X(H) \longrightarrow X$ is finite if and only if H has finite index in G.

For any topological space Y, we denote by $C(Y)$ the ring of complex valued, continuous functions on Y.

A covering map $\pi: E \longrightarrow X$ induces a monomorphism $\pi^*: C(X) \longrightarrow C(E)$ of rings along which we can consider $C(E)$ as a ring extension of $C(X)$, or as an algebra over $C(X)$. Obviously, this algebra is commutative and has a unit element. By an automorphism of $C(E)$ over $C(X)$ we understand a ring automorphism $\phi: C(E) \longrightarrow C(E)$, which is $C(X)$-linear, or equivalently, makes the following diagram commutative

$$\begin{array}{ccc} C(E) & \xrightarrow{\phi} & C(E) \\ & {\scriptstyle \pi^*}\nwarrow \quad \nearrow{\scriptstyle \pi^*} & \\ & C(X) & \end{array}$$

Denote by $\mathcal{G} = \mathcal{G}\big(C(E)/C(X)\big)$ the group of automorphisms of $C(E)$ over $C(X)$. For a subgroup $\mathcal{H}$ in $\mathcal{G}$, let

$$\operatorname{Fix} \mathcal{H} = \{f \in C(E) \mid \phi(f) = f, \text{ all } \phi \in \mathcal{H}\}.$$

If $\operatorname{Fix} \mathcal{G} = C(X)$, then we call $C(E)$ a *normal extension* of $C(X)$, and $\mathcal{G}$ is called the *Galois group* of $C(E)$ over $C(X)$, or of the covering map $\pi: E \longrightarrow X$.

Recall that a covering map $\pi: E \longrightarrow X$ is said to be regular if the group of covering transformations of π acts transitively on the fibres of π, or equivalently, if either all or none of the liftings of a closed loop in X to paths in E are closed loops.

THEOREM 1.1. *Let H be a subgroup of finite index in the fundamental group G of X, and let $\pi: E = X(H) \longrightarrow X$ be the corresponding finite covering map. Then the following conditions are equivalent:*

(i) H is a normal subgroup of G.

(ii) $\pi: E \longrightarrow X$ is a regular covering map.

(iii) $C(E)$ is a normal extension of $C(X)$.

In case these conditions are satisfied, the Galois group $\mathcal{G}$ of $C(E)$ over $C(X)$ is anti-isomorphic to the group of right cosets $H\backslash G$.

PROOF. It is classical that (i) and (ii) are equivalent, see e.g. [15].

First assume that (i) and (ii) hold. We view $K = H\backslash G$ as a group of deck transformations on E so that $E/K \simeq X$. Define $K^* = \{\phi \in \mathcal{G} \mid \phi = k^*, k \in K\}$. We contend that $K^* = \mathcal{G} = \mathcal{G}\big(C(E)/C(X)\big)$ and that Fix $K^* = C(X)$.

For $f \in C(X)$ we have $k^*(f \circ \pi)(e) = f \circ \pi\big(k(e)\big) = f \circ \pi(e)$ since k preserves fibres. Hence K^* fixes $C(X)$.

If $f \in C(E)$ but $f \notin \pi^*\big(C(X)\big)$, then there exist $x \in X$ and $e_1, e_2 \in \pi^{-1}(x)$ with $f(e_1) \neq f(e_2)$. Now by hypothesis K acts transitively on fibres so there is a $k \in K$ with $k(e_1) = e_2$. For this $k \in K$ we have $k^*f \neq f$, since

$$(k^*f)(e_1) = f\big(k(e_1)\big) = f(e_2) \neq f(e_1).$$

Hence Fix $K^* = C(X)$, as should be proved.

Secondly suppose (iii) holds. We then prove that (ii) holds.

Denote by $\mathcal{G}$ the group of automorphisms of $C(E)$ over $C(X)$. By a theorem of Gelfand and Kolmogorov (see [5]), there is a group K of homeomorphisms of E with $K^* = \mathcal{G}$. All we have to prove then, is that K acts freely and transitively on the fibres for $\pi: E \longrightarrow X$.

STEP 1 (K PRESERVES FIBRES). Let $x \neq y$ be in X and suppose $f \in C(X)$ is a function with $f(x) \neq f(y)$. If there were an element $k \in K$, so that $k(e_x) = e_y$, where $e_x \in \pi^{-1}(x)$, $e_y \in \pi^{-1}(y)$, then we would have

$$f \circ \pi(e_y) = f \circ \pi\big(k(e_x)\big) = k^*(f \circ \pi)(e_x) = f \circ \pi(e_x),$$

as $\mathcal{G}$ fixes $C(X)$, but this is impossible.

STEP 2 (FREENESS AND TRANSITIVITY). Since E is a connected covering space of X, a covering transformation $k: E \longrightarrow E$ must be the identity if it fixes one point, and hence it follows that K acts freely. To check transitivity let $x \in X$, $e \in \pi^{-1}(x)$. Since $\pi^{-1}(x)$ is finite it is possible to find a function $f \in C(E)$ with $f(e') \neq 0$ for $e' \in \pi^{-1}(x) - \{e\}$ and $f(e) = 0$. The function $h(e) = \prod_{g \in \mathcal{G}}(gf)(e)$ is invariant under $\mathcal{G}$ and therefore it belongs to $C(X)$. Thus if $e' \in \pi^{-1}(x)$ we have

$$\prod_{g \in \mathcal{G}}(gf)(e') = h(e') = h(e) = \prod_{g \in \mathcal{G}}(gf)(e) = 0.$$

Hence $(gf)(e') = 0$ for some $g \in \mathcal{G}$. Assume $g = k^*$. Then $(k^*f)(e') = f\big(k(e')\big) = 0$, implying that $k(e') = e$. This proves transitivity of K.

During the course of proof we have also proved that $(H\backslash G)^* = \mathcal{G}$, when $\pi: E \to X$ is a regular covering map, or equivalently that $C(E)$ is normal over $C(X)$. In other words, $H\backslash G$ and $\mathcal{G}$ are anti-isomorphic. This completes the proof of Theorem 1.1.

We shall describe a Galois theory for normal extensions of $C(X)$-algebras as those in Theorem 1.1. The Galois group $\mathcal{G}$ of $C(E)$ over $C(X)$ will then of course be of central importance. Due to Theorem 1.1 we shall also refer to $H\backslash G$ as the Galois group of the covering map $\pi: X(H) \to X$.

We finish this section by collecting some known results, which establish further links between groups, coverings and function algebras.

THEOREM 1.2. *For a space X with fundamental group G as above, there are category equivalences between the following categories:*

(i) Subgroups H of finite index in G.

(ii) Finite covering maps $\pi: E \to X$ onto X.

(iii) Separable $C(X)$-algebras, which are finitely generated and projective as $C(X)$-modules and have no idempotents except 0 and 1.

Under these equivalences, a subgroup $H < G$ of finite index corresponds to the finite covering map $\pi: E = X(H) \to X$, which on the other hand corresponds to the $C(X)$-algebra $C(E)$.

The equivalence of the categories in (i) and (ii) is classical, see eg. [15]. The equivalence of the categories in (ii) and (iii) was established by Wajnryb [19] and Childs [2], see also Magid [14].

2. **Polynomial covering maps.** A substantial part of the paper shall be devoted to polynomial covering maps, [7],[8],[11],[12].

We recall that a Weierstrass polynomial of degree $n \geq 1$ over X is a polynomial function $P: X \times \mathbb{C} \to \mathbb{C}$ of the form

$$P(x, z) = z^n + \sum_{i=1}^{n} a_i(x) z^{n-i},$$

where $a_1, \ldots, a_n: X \to \mathbb{C}$ are continuous, complex valued functions. We can consider $P(x, z)$ as an element in the polynomial ring $C(X)[z]$ in one complex variable z over $C(X)$. If $P(x, z)$ is *separable,* i.e. without multiple roots for any $x \in X$, then we get an associated n-fold covering map $\pi: E \to X$ by projecting the zero set $E = \{(x, z) \in X \times \mathbb{C} \mid P(x, z) = 0\}$ for $P(x, z)$ onto X. This is the n-fold polynomial covering map associated with $P(x, z)$.

According to the embedding criterion for polynomial covering maps ([7], Theorem 5.1), a finite covering map $\pi: E \to X$ is equivalent to a polynomial covering map—we say that π is polynomial—if and only if it admits a fibrewise embedding into the trivial complex line bundle over X. On the other hand, the latter condition is equivalent to the existence of a separating function $f: E \to \mathbb{C}$ for π, i.e. a continuous function such that $f(e_1) \neq f(e_2)$, whenever $e_1 \neq e_2$ are elements in the same fibre of

π. For a polynomial covering map $\pi: E \longrightarrow X$ associated with the separable Weierstrass polynomial $P(x, z)$, the function $f(x, z) = z$ will do.

For later reference we quote the following theorem from the thesis [17] of one of the authors. See also ([18], Theorem 4.2).

THEOREM 2.1. *Let $\pi_2: E^2 \longrightarrow E^1$ and $\pi_1: E^1 \longrightarrow X$ be finite covering maps. Then the composition $\pi = \pi_1 \circ \pi_2: E^2 \longrightarrow X$ is a finite covering map, which is polynomial if and only if both $\pi_2: E^2 \longrightarrow E^1$ and $\pi_1: E^1 \longrightarrow X$ are polynomial.*

If $\pi: E \longrightarrow X$ is a regular polynomial covering map associated with the separable Weierstrass polynomial $P(x, z)$, then it is to be expected that there must be a connection between the action of the Galois group of the Weierstrass polynomial on its roots and the action of the Galois group of the covering map. This will be explored in § 5. In this connection we shall need some information concerning characteristic homomorphisms for finite covering maps, [8].

Let $\pi: E \longrightarrow X$ be an n-fold covering map onto X. We repeat that X is path connected with fundamental group G. Then there is a characteristic homomorphism $\chi(\pi): G \longrightarrow \Sigma_n$, where Σ_n is the permutation group on the n elements in the fibre of π over a base point $x_0 \in X$. The characteristic homomorphism is defined by a path lifting procedure in π and is well defined up to conjugation. It determines the equivalence class of the covering map. Let $B(n)$ denote the Artin group of braids on n strings, and let $\tau: B(n) \longrightarrow \Sigma_n$ be the epimorphism, which maps an n-braid onto the permutation of the braid. Then it is known ([8], Theorem 5.1) that $\pi: E \longrightarrow X$ is polynomial if and only if $\chi(\pi)$ lifts over τ_n, i.e.,

$$\begin{array}{ccc} & & B(n) \\ & \overset{\varphi}{\nearrow} & \big\downarrow \tau_n \\ G & \xrightarrow[\chi(\pi)]{} & \Sigma_n \end{array}$$

Suppose now that $\pi: E \longrightarrow X$ is a finite covering map associated with the subgroup $H < G$. Then the fibre over $x_0 \in X$ can be identified with the set of right cosets $H\backslash G$ and Σ_n with the group of permutations of the set $H\backslash G$. Denote by $\mathrm{Aut}(H\backslash G)$ the group of permutations of the set $H\backslash G$. Then the characteristic homomorphism of π is a homomorphism $\chi(\pi): G \longrightarrow \mathrm{Aut}(H\backslash G)$.

3. **Galois theory for extensions of function rings defined by finite covering maps.** First we prove two theorems which are essential for developing an appropriate Galois theory for extensions of function rings defined by finite covering maps. The results are valid also in the smaller category of polynomial covering maps and this is of particular interest since classical Galois theory is about polynomials over fields and their splitting fields.

THEOREM 3.1 (FUNDAMENTAL THEOREM OF GALOIS THEORY). *Let $\pi: E = X(H) \longrightarrow X$ be a regular, finite covering map onto X corresponding to a normal subgroup H in G of finite index and with Galois group G.*

https://doi.org/10.4153/CJM-1991-073-0 Published online by Cambridge University Press

If $E \longrightarrow E' \longrightarrow X$ is an intermediate covering map, then there is a subgroup $\mathcal{H}$ in $\mathcal{G}$ with $\operatorname{Fix}\mathcal{H} = C(E')$.

Conversely, if $\mathcal{H}$ is a subgroup in $\mathcal{G}$, then $\operatorname{Fix}\mathcal{H}$ *is isomorphic to $C(E')$ for some intermediate covering map $E \longrightarrow E' \longrightarrow X$.*

Finally, an intermediate covering map $E \longrightarrow E' \longrightarrow X$ is regular over X if and only if the subgroup $\mathcal{H}$ in $\mathcal{G}$ is normal, in which case $\mathcal{G}\big(C(E')/C(X)\big) \cong \mathcal{G}/\mathcal{H}$.

If $\pi: E = X(H) \longrightarrow X$ is polynomial all covering maps in the above will be polynomial.

PROOF. The theorem follows from Theorem 1.1 by observing that intermediate covering maps $E \longrightarrow E' \longrightarrow X$ correspond to intermediate subgroups $H < H' < G$. Under this correspondence it is clear that with $E' = X(H')$ we have $C(E') = \operatorname{Fix}\big((H\backslash H')^*\big)$. Conversely, if $\mathcal{H} < \mathcal{G}$, then there is a unique $H < H' < G$ with $(H\backslash H')^* = \mathcal{H}$. For the last part of the theorem it is enough to notice that $H < H' \ll G$ if and only if $(H\backslash H')^* \ll \mathcal{G}$.

The polynomial case follows from the general case of arbitrary finite covering maps, just by using Theorem 2.1 and noticing that the constructions in the proof of Theorem 1.1 work also in the smaller category of polynomial covering maps.

THEOREM 3.2 (EXISTENCE OF NORMAL CLOSURE). *Let $\pi: E = X(H) \longrightarrow X$ be a finite covering map onto X corresponding to a subgroup H in G of finite index. Then there exists a largest subgroup $\bar{H} < H$ such that $\bar{H} \ll G$ is a normal subgroup in G of finite index. The associated finite covering map $\bar{\pi}: \bar{E} = X(\bar{H}) \longrightarrow X$ has $\pi: E \longrightarrow X$ as an intermediate covering map and $C(\bar{E})$ is the smallest normal extension of $C(X)$, which contains $C(E)$.*

The group $\bar{H}$ is called the *core* of H and the algebra $C(\bar{E})$ the *normal closure* of $C(E)$.

PROOF. Define the subgroup $\bar{H}$ in G by $\bar{H} = \bigcap_{g\in G} gHg^{-1}$. Since H has finite index in G, it is easy to see that $\bar{H}$ is a finite intersection of subgroups of finite index in G. Hence $\bar{H}$ has finite index in G. By construction $\bar{H}$ is the largest subgroup in H such that $\bar{H}$ is normal in G. Granted the existence of a core $\bar{H}$ of H, the theorem is an immediate consequence of Theorem 1.1.

Before proceeding to develop the theory further, we describe the basic elements of classical Galois theory. In this theory one investigates polynomials in the polynomial ring $F[z]$ over a field F by looking at extensions of F, in which the polynomial splits into linear factors. However, it is customary to restrict attention to monic irreducibles as $F[z]$ is a unique factorization domain. If $\operatorname{char} F = 0$ it follows that all irreducibles are separable, i.e. have no multiple roots. If $\operatorname{char} F \neq 0$ then one has to decompose irreducibles into separable factors in some extension of F. Given a monic, separable, irreducible polynomial $p \in F[z]$ we know that $L = F[z]/(p)$ is an extension of F in which p has a root. There is a smallest normal extension K of F containing L, called the normal closure of L over F. Because p is irreducible it will split in K, and because p is separable, K will be a "separable" extension of F. Then K is a Galois extension of F. The Galois group of K over F is also called the Galois group of p. It is the action of this group on the roots of p that determines how complicated the polynomial is.

What we wish to do here, is to replace F by $C(X)$. As $C(X)$ is not even an integral domain, let alone a field, we can naturally not hope for an exact analogy with the classical

situation. On the other hand there is some hope that topology can help us, but maybe also set up some obstructions.

In classical Galois theory, all finite, separable extensions are primitive, i.e. they are generated by a single element, ([13], Theorem 14, p. 185). This is no longer the case for $C(X)$-algebras. In fact, primitive extensions correspond exactly to polynomial covering maps. This is the content of the following theorem due to Duchamp and Hain [4].

THEOREM 3.3 (DUCHAMP AND HAIN). *Let $\pi: E \longrightarrow X$ be a n-fold covering map. Then $C(E)$ is a primitive extension of $C(X)$, i.e. there is a function $f \in C(E)$ so that the functions $1, f, \ldots, f^{n-1}$ are a basis for $C(E)$ as a $C(X)$-module, if and only if $\pi: E \longrightarrow X$ is a polynomial covering map.*

Theorem 3.3. indicated that a successful Galois theory in the classical sense can be expected for extensions $C(E)$ of $C(X)$ corresponding to polynomial covering maps $\pi: E \longrightarrow X$. This claim is supported by the results below.

Let $P(x, z) \in C(X)[z]$ be a separable Weierstrass polynomial over X and let $\pi: E \longrightarrow X$ be the associated polynomial covering map. Then we have

THEOREM 3.4 ([10], THEOREM 2). *The $C(X)$-algebra $C(E)$ is isomorphic to the quotient algebra $C(X)[z]/\big(P(x, z)\big)$ as $C(X)$-algebras.*

THEOREM 3.5 ([9], THEOREM 5.2). *The separable Weierstrass polynomial $P(x, z)$ over X is irreducible if and only if E is connected.*

THEOREM 3.6. *The separable Weierstrass plynomial $P(x, z)$ over X splits uniquely into irreducible, separable factors.*

PROOF. If $P(x, z)$ is irreducible there is nothing to prove, so assume not. By Theorem 3.5, E is not connected. Let $E = E_1 \sqcup \cdots \sqcup E_r$ be the splitting of E into connected components. Define $P_i(x, z) = \prod_{(x,\alpha)\in E_i}(z - \alpha)$, and note that the number of factors in the product is constant in $x \in X$, since E_i is a covering space over X. Then $P_i(x, z)$ defines a separable, irreducible Weierstrass polynomial over X (with a well defined degree in z) for which the associated polynomial covering map has total space E_i. Clearly,

$$P(x, z) = P_1(x, z) \cdots P_r(x, z).$$

To prove uniqueness, let $Q(x, z)$ be a separable, irreducible Weierstrass polynomial over X, which divides $P(x, z)$. Let E' be the polynomial covering space over X associated with $Q(x, z)$. Then $E' \subset E$ and the inclusion map is continuous. Hence E' is a connected, compact subset of E. Thus $E' \subset E_i$ for some $i = 1, \ldots, r$. Any point in E' has a neighbourhood which is homeomorphic to an open set in X. This neighbourhood must therefore also be an open subset of E_i, proving that E' is also an open subset of E_i. Therefore $E' = E_i$ and $Q(x, z) = P_i(x, z)$. This proves uniqueness of the splitting.

Due the Theorem 3.6 we can without loss of generality restrict attention to irreducible Weierstrass polynomials and therefore to connected polynomial covering spaces.

4. **Weierstrass polynomials of the type $P(x,z) = z^n - a(x)$.** To illustrate Theorem 3.6 we consider the most elementary type of Weierstrass polynomials over X, namely those of the form $P(x,z) = z^n - a(x)$ for a function $a \in C(X)$. Clearly, $P(x,z)$ is separable if and only if $a(x) \neq 0$ for all $x \in X$. If $P(x,z)$ is separable, $\phi(x) = \frac{a(x)}{|a(x)|}$ defines a function $\phi: X \longrightarrow S^1$ and therefore a cohomology class in $H^1(X;\mathbb{Z})$, denoted by $|a|$. It is well known, and easy to prove ([12], Lemma IV 1.6), that $a(x)$ has a continuous n^{th}root if and only if $|a|$ is divisible by n in $H^1(X;\mathbb{Z})$. It follows that $P(x,z) = z^n - a(x)$ splits into linear factors over $C(X)$ if and only if $|a| \in H^1(X;\mathbb{Z})$ is divisible by n.

In this section we shall generalize these remarks and at the same time find a factorization of $P(x,z) = z^n - a(x)$ into irreducibles.

Let ω be an n^{th}root of unity. Suppose that the Weierstrass polynomial $P(x,z) = z^n - a(x)$ splits into a product

$$P(x,z) = P_1(x,z)P_2(x,z)$$

of Weierstrass polynomials $P_i(x,z)$ of degree p_i, $i = 1,2$. Then clearly

$$P(x,z) = \left(\omega^{-p_1}P_1(x,\omega z)\right)\left(\omega^{-p_2}P_2(x,\omega z)\right)$$

is also a splitting of $P(x,z)$ in (monic) Weierstrass polynomials over X.

Now assume that ω is a primitive n^{th}root of unity and that $P_0(x,z) = z^p + \sum_{k=1}^{p} a_k(x)z^{p-k}$ is an irreducible factor of $P(x,z) = z^n - a(x)$. Define $P_i(x,z) = \omega^{-pi}P_0(x,\omega^i z)$, $i = 1,\dots n-1$. The above analysis reveals that $P_i(x,z)$ is also an irreducible factor of $P(x,z)$. Since $P_0(x,z)$ is irreducible, $a_p(x) \neq 0$ for some $x \in X$. Therefore, if $P_i(x,z) = P_j(x,z)$ for some $i,j = 0,\dots,n-1$, we must have $\omega^{(i-j)p} = 1$, or equivalently $n|(i-j)p$.

Let $n = mp + r$ with $0 \leq r < p$. If $i \neq j$, $n|(i-j)p$ and $r > 0$, then $|i-j| > m$. But then $P_0(x,z),\dots,P_m(x,z)$ are $m+1$ different irreducible factors of $P(x,z) = z^n - a(x)$, which contradicts Theorem 3.6 since $(m+1)p > n$. We conclude that $r = 0$ and $n = mp$, so that $P_0(x,z),\dots,P_{m-1}(x,z)$ are m different irreducible factors of $P(x,z)$ for which

$$P(x,z) = P_0(x,z)\cdots P_{m-1}(x,z).$$

We shall now determine $P_0(x,z)$. By inserting the definitions of the various Weierstrass polynomials into the factorization of $P(x,z)$ we get

$$\begin{aligned} z^n - a(x) &= \prod_{i=0}^{m-1}\left(\omega^{-pi}P_0(x,\omega^i z)\right) \\ &= \prod_{i=0}^{m-1}\left(z^p + \cdots + a_k(x)\omega^{-ki}z^{p-k} + \cdots + \omega^{-pi}a_p(x)\right). \end{aligned}$$

For $z = 0$ we get the equation

$$-a(x) = a_p(x)^m \prod_{i=0}^{m-1}\omega^{-pi}.$$

https://doi.org/10.4153/CJM-1991-073-0 Published online by Cambridge University Press

Put

$$\alpha = \prod_{i=0}^{m-1} \omega^{-pi} = \omega^{-pm(m-1)/2}.$$

Then we have

$$-a(x) = a_p(x)^m \alpha.$$

We conclude that $a(x)$ has a continuous m^{th} root, that $\alpha \neq 0$ and that $a_p(x) \neq 0$ for all $x \in X$.

Assume now that the functions $a_{k+1}(x), \ldots, a_{p-1}(x)$ are identically zero on X for $k < p$. For $k = p - 1$ there is no condition. By equating coefficients to terms of degree $p - k$ in the splitting of $P(x, z)$, we then get the equation

$$\begin{aligned} 0 &= a_p(x)^{m-1} a_k(x) \left(\sum_{j=0}^{m-1} \omega^{-kj} \left(\prod_{\substack{i=0 \\ i \neq j}}^{m-1} \omega^{-pi} \right) \right) \\ &= a_p(x)^{m-1} a_k(x) \left(\sum_{j=0}^{m-1} \omega^{-kj} \omega^{pj} \alpha \right) \\ &= a_p(x)^{m-1} a_k(x) \alpha \frac{\omega^{(p-k)m} - 1}{\omega^{p-k} - 1}. \end{aligned}$$

Since $a_p(x) \neq 0$ for all $x \in X$, $\alpha \neq 0$ and $\omega^{(p-k)m} \neq 1$, we conclude that $a_k(x) = 0$ for all $x \in X$.

Altogether, it follows that

$$P_0(x, z) = z^p + a_p(x)$$

and that

$$P(x, z) = z^n - a(x) = \prod_{i=0}^{m-1} \left(z^p + \omega^{-pi} a_p(x) \right)$$

is the factorization of $P(x, z) = z^n - a(x)$ into irreducibles.

The above investigations can be summarized in the following.

THEOREM 4.1. *Let $a(x) \in C(X)$ be a continuous function on X with $a(x) \neq 0$ for all $x \in X$. Then the Weierstrass polynomial $P(x, z) = z^n - a(x)$, $n \geq 2$, is irreducible if and only if the cohomology class $|a| \in H^1(X; \mathbb{Z})$ determined by $a(x)$ is not divisible by any number $m > 1$ that divides n.*

In particular, if $n \geq 2$ is a prime number, then either $P(x, z) = z^n - a(x)$ splits completely into linear factors or is irreducible.

Assuming that the separable Weierstrass polynomial $P(x, z) = z^n - a(x)$, $n \geq 2$, over X is irreducible we can easily compute the Galois group. It has to be the cyclic group of order n, $\mathbb{Z}_n$, since the polynomial is invariant under multiplication by n^{th} roots of unity. Hence the associated polynomial covering map $\pi: E \longrightarrow X$ is regular.

In analogy with the consequence of Hilbert's Theorem 90 on cyclic field extensions ([13], Theorem 10, p. 214), it is then natural to ask whether an n-fold covering map, which is regular and has cyclic Galois group, is equivalent to a polynomial covering map associated with a separable Weierstrass polynomial of the form $P(x, z) = z^n - a(x)$. This however is not in general the case, as the following theorem of Møller explains.

THEOREM 4.2 (MØLLER [16]). *Let $\pi: E \to X$ be a regular, n-fold covering map with Galois group $\mathbb{Z}_n$. We view $\mathbb{Z}_n < S^1$ as a subgroup of the circle group S^1. Then the following statements are equivalent:*

(i) $\pi: E \to X$ *is equivalent to a polynomial covering map associated with a separable Weierstrass polynomial of the form* $P(x, z) = z^n - a(x)$.

(ii) $\pi: E \to X$ *can be equivariantly embedded into the trivial complex line bundle* $X \times \mathbb{C} \to X$.

(iii) The associated complex line bundle $\bar{\pi}: E \times_{\mathbb{Z}_n} \mathbb{C} \to X$ *is trivial.*

(iv) The associated complex line bundle $\bar{\pi}: E \times_{\mathbb{Z}_n} \mathbb{C} \to X$ *has vanishing first Chern class, i.e.* $c_1(E \times_{\mathbb{Z}_n} \mathbb{C}) = 0$.

Based on Theorem 4.2 we can appropriately say that there is an exact topological obstruction to Hilbert's Theorem 90. The only exception is 2-fold covering maps.

THEOREM 4.3. *Any 2-fold polynomial covering map $\pi: E \to X$ can be equivariantly embedded into the trivial complex line bundle $X \times \mathbb{C} \to X$.*

PROOF. Let $\pi: E \to X$ be a 2-fold polynomial covering map. Either π is trivial or E is connected. In the first case we are done. In the second case $E = X(H)$ for some subgroup H of index 2 of the fundamental group G of X. Any subgroup of index 2 is normal and hence $\pi: E \to X$ is a regular covering map. Let $T: E \to E$ be the unique nontrivial fibre preserving involution of π. If $f: E \to \mathbb{C}$ is a separating function for the polynomial covering map π, then $h(e) = \big(f(e) - f\big(T(e)\big)\big)/|f(e) - f\big(T(e)\big)|$, $e \in E$, is evidently the component into $\mathbb{C}$ of a $\mathbb{Z}_2$ equivariant embedding of $\pi: E \to X$ into the trivial complex line bundle over X, since $h\big(T(e)\big) = -h(e)$. This proves the theorem.

5. **Action of the Galois group of a Weierstrass polynomial.** Our aim in this section is to find a connection between the action of the Galois group of a Weierstrass polynomial on its roots and on the corresponding polynomial covering map.

If $\pi: E \to X$ is a covering map and $Q(x, z)$ is a Weierstrass polynomial over X, we can form the Weierstrass polynomial $Q_E(e, z)$ over E defined by $Q_E(e, z) = Q\big(\pi(e), z\big)$, $e \in E$, $z \in \mathbb{C}$.

LEMMA 5.1. *Let $\pi: E \to X$ be a regular covering map with E connected and let $Q(x, z) \in C(X)[z]$ be a separable irreducible Weierstrass polynomial over X. Suppose that $Q_E(e, z)$ has a root in $C(E)$. Then $Q_E(e, z)$ splits completely in $C(E)$.*

PROOF. Let $\alpha_1, \ldots, \alpha_m$ be the roots for $Q_E(e, z)$ in $C(E)$. Since $Q_E(e, z)$ is invariant under the action of the Galois group $\mathcal{G}$ of $C(E)$ over $C(X)$, the set $\{\alpha_1, \ldots, \alpha_m\}$ must also be invariant under $\mathcal{G}$. Therefore the polynomial $\big(z - \alpha_1(e)\big) \cdots \big(z - \alpha_m(e)\big)$, which is *a priori* a polynomial in $C(E)[z]$, is actually induced from a polynomial $R(x, z)$ in $C(X)[z]$.

Now $Q_E(e, z) = R_E(e, z)S'(e, z)$ for a Weierstrass polynomial $S'(e, z) \in C(E)[z]$. Suppose that the Weierstrass polynomials involved have the form,

$$Q_E(e, z) = z^n + a_1(e)z^{n-1} + \cdots + a_n(e)$$
$$R_E(e, z) = z^m + b_1(e)z^{m-1} + \cdots + b_m(e)$$
$$S'(e, z) = c_0(e)z^{n-m} + c_1(e)z^{n-m-1} + \cdots + c_{n-m}(e).$$

Then $c_0(e)1 = 1$ and

$$\sum_{i+j=k} c_i(e)b_j(e) = c_k(e) + c_{k-1}(e)b_1(e) + \cdots + c_0(e)b_k(e) = a_k(e).$$

It follows that $c_0(e) = 1$ and hence it can be considered as a function in $C(X)$. Suppose by induction that $c_0(e), \ldots, c_{k-1}(e)$ can actually be considered as functions in $C(X)$. Then the above formula shows that $c_k(e)$ is a function in $C(X)$. Consequently, the polynomial $S'(e,z)$ is induced from a polynomial $S(x,z) \in C(x)[z]$, that is, $S'(e,z) = S_E(e,z)$, and we have the product decomposition $Q(x,z) = R(x,z)S(x,z)$. Since $Q(x,z)$ is irreducible we conclude that $R(x,z) = 1$, or $S(x,z) = 1$. Since $R(x,z) \neq 1$ we conclude that $Q_E(x,z) = R_E(x,z)$ as desired.

LEMMA 5.2. *Let $\pi: E \longrightarrow X$ and $Q(x,z)$ be as in Lemma 5.1. Then the Galois group $\mathcal{G}$ for the ring extension $C(E)$ of $C(X)$ acts transitively on the roots for $Q_E(e,z)$ in $C(E)$.*

PROOF. We may assume that $Q_E(e,z) = \prod_{\alpha \in A}\big(z - \alpha(e)\big)$ where A is the set of roots for $Q_E(e,z)$ in $C(E)$. If $A = A_1 \cup A_2$ and A_1 is invariant under $\mathcal{G}$ then A_2 must also be invariant under $\mathcal{G}$. We can then define polynomials $Q^i_E(e,z) = \prod_{\alpha \in A_i}\big(z - \alpha(e)\big)$, $i = 1, 2$. Since A_i is invariant under $\mathcal{G}$, the polynomials $Q^i_E(e,z)$ are induced from polynomials $Q^i(x,z)$ in $C(X)[z]$, and $Q(x,z) = Q^1(x,z)Q^2(x,z)$. Since $Q(x,z)$ is irreducible either $Q^1(x,z) = 1$ or $Q^2(x,z) = 1$ and this proves the lemma.

Given a separable irreducible Weierstrass polynomial $P(x,z) \in C(X)[z]$, we have the corresponding polynomial covering map $\pi: E \longrightarrow X$, where E is connected and $E = X(H)$ for some subgroup $H < G$ in the fundamental group G of X. We form the corresponding normal closure $\bar{\pi}: \bar{E} = X(\bar{H}) \longrightarrow X$. Note that the core $\bar{H}$ of H, and hence the normal closure $\bar{E}$, is independent of the subgroup H representing the covering map π since subgroups in G representing equivalent covering maps onto X are conjugate in G.

The Weierstrass polynomial $P_E\big((x,z),z\big)$ has a root in $C(E)$, namely the function $\alpha_1\big((x,z),z\big) = z$. Therefore the Weierstrass polynomial $P_{\bar{E}}(e,z)$ has a root $\alpha_1(e) \in C(\bar{E})$ and consequently it splits completely according to Lemma 5.1. Let $A = \{\alpha_1, \ldots, \alpha_n\}$ be the roots for $P_{\bar{E}}(e,z)$ in $C(\bar{E})$. We view $K \simeq \bar{H}\backslash G$ as a group of deck transformations on $\bar{E}$, and let $\bar{g}$ denote the deck transformation corresponding to the coset $\bar{H}g$ defined by the element $g \in G$. The association $g \longrightarrow \bar{g}$ is then a group homomorphism of G into K. Denote by $\mathrm{Aut}\,A$ the group of permutations of A.

These preparatory remarks now make it possible to define a right action

$$\gamma: G \longrightarrow \mathrm{Aut}\,A$$

of G on the set of roots A for $P_{\bar{E}}(e,z)$ as the composite map

$$\begin{array}{ccccccc} G & \longrightarrow & K \simeq \bar{H}\backslash G & \overset{\text{anti}}{\underset{\simeq}{\longrightarrow}} & K^* & \longrightarrow & \mathrm{Aut}\,A \\ g & \longmapsto & \bar{g} & \longmapsto & \bar{g}^* & \longmapsto & (\alpha \longmapsto \bar{g}\alpha) \end{array}$$

The action is a right action since $K \longrightarrow K^*$ is an anti-homomorphism.

There is an obvious identification of the permutation group Σ_n on n elements (considered as the permutation group for the set of right cosets $H\backslash G$) and the group $\mathrm{Aut}\,A$. Hence the characteristic homomorphism $\chi(\pi)$ for the polynomial covering map $\pi: E \to X$ can be considered as a homomorphism $\chi(\pi): G \to \mathrm{Aut}\,A$. With this identification we have the following fundamental

THEOREM 5.3. *The action $\gamma: G \to \mathrm{Aut}\,A$ is conjugate to the characteristic homomorphism $\chi(\pi): G \to \mathrm{Aut}\,A$ for the polynomial covering map $\pi: E \to X$.*

PROOF. Define a map $\bar{\varphi}: G \to A$ by $\bar{\varphi}(g) = \bar{g}\alpha_1$ for $g \in G$. If $h \in H$ and $g \in G$ we have $\bar{\varphi}(hg) = (\overline{hg})\alpha_1 = \bar{g}(\bar{h}\alpha_1) = \bar{g}\alpha_1$, since $\alpha_1 \in C(E) = C\big(X(H)\big)$. Consequently, $\bar{\varphi}$ induces a map $\varphi: H\backslash G \to A$. By Lemma 5.2, φ is surjective, and hence it is bijective, since A and $H\backslash G$ contain the same number of elements.

The map φ provides the desired conjugation. To prove this we use that $\chi(\pi): G \to \mathrm{Aut}\,A$ is actually a homomorphism into the group of permutations of the set of right cosets $H\backslash G$. Let $a, g \in G$. Then we have

$$\varphi\big(\chi(\pi)(g)(Ha)\big) = \varphi(Hag) = (\overline{ag})\alpha_1 = \bar{g}(\bar{a}\alpha_1) = \bar{g}\big(\varphi(Ha)\big) = \gamma(g)\big(\varphi(Ha)\big).$$

This computation proves that $\varphi \circ \chi(\pi)(g) = \gamma(g) \circ \varphi$ for all $g \in G$ and the theorem is established.

Theorem 5.3 shows that the action of the Galois group of a separable irreducible Weierstrass polynomial $P(x, z)$ over X classifies the associated polynomial covering map $\pi: E \to X$. Furthermore we have the isomorphism $C(E) \simeq C(X)[z]/\big(P(x, z)\big)$ of $C(X)$-algebras from ([10, Theorem 2). This is in complete analogy with the classical Galois theory for field extensions.

From [8] it is known that an n-fold covering map $\pi: E \to X$ is polynomial if and only if the characteristic homomorphism for the covering from the fundamental group G of X into Σ_n factors through the braid group $B(n)$. The homomorphism of G into $B(n)$ is induced by the root map for π which can be expressed in terms of the coefficient map given by the coefficients in the Weierstrass polynomial $P(x, z)$. In that sense the action of the Galois group of a Weierstrass polynomial on its roots can be expressed in terms of the coefficients of the polynomial itself.

REFERENCES

1. V. I. Arnold, *Topological invariants of algebraic functions, II*, Functional Anal. i Prilozen. (2) **4**(1970), 1–9 and Functional Analysis and its Applications (2)**4**(1970), 91–98.
2. L. N. Childs, *On covering spaces and Galois extensions*, Pacific J. Math. **37**(1971), 29–33.
3. F. R. DeMeyer and E. C. Ingraham, *Separable algebras over commutative rings*. Springer Lecture Notes in Mathematics, **81**, 1971.
4. T. Duchamp and R. M. Hain, *Primitive elements in rings of holomorphic functions*, J. Reine Angew. Math. **346**(1984), 199–220.
5. L. Gillman, M. Henriksen and M. Jerison, *On a theorem of Gelfand-Kolmogoroff concerning maximal ideals in rings of continuous functions*, Proc. Amer. Math. Soc. **5**(1954), 447–455.
6. E. A. Gorin and V. Ja. Lin, *Algebraic equations with continuous coefficients, and certain questions of the algebraic theory of braids*, Mat. Sb. **78**(120)(1969), 579–610, and Math. Sbornik **7**(1969), 569–596.

7. V. L. Hansen, *Coverings defined by Weierstrass polynomials*, J. Reine Angew. Math. **314**(1980), 29–39.
8. ———, *Polynomial covering spaces and homomorphisms into the braid groups*, Pacific J. Math. **81**(1979), 399–410.
9. ———, *Algebra and topology of Weierstrass polynomials*, Expo. Math. **5**(1987), 267–274.
10. ———, *The characteristic algebra of a polynomial covering map*, Math. Scand. **64**(1989), 219–225.
11. ———, *Polynomial covering maps*. In: *Braids* (A. Libgober and J. S. Birman eds.), Contemporary Math. **78**(1988), 229–243.
12. ———, *Braids and coverings—selected topics*. London Math. Soc. Student Texts **18**, Cambridge University Press, 1989.
13. S. Lang, *Algebra*. Addison-Wesley, 1965.
14. A. R. Magid, *Algebraically separable extensions of Banach alagebras*, Michigan Math. J. **21**(1974), 137–143.
15. W. S. Massey, *Algebraic topology: an introduction*. 4th ed., Graduate Texts in Mathematics **56**, Springer-Verlag, 1977.
16. J. M. Møller, *Equivariant embeddings of principal $\mathbf{Z}_n$-bundles into complex vector bundles*, Topology Appl. **16**(1983), 279–286.
17. P. Petersen, V, *Fatness of covers*. Thesis, University of Maryland, College Park, 1987.
18. ———, *Fatness of covers*, J. Reine Angew. Math. **403**(1990), 154–165.
19. B. Wajnryb, *Projective and separable extensions of rings of continuous functions*, Bull. Acad. Pol. Sci. Sér. Sci. Math. Astr. Phys. **17**(1969), 269–271.
20. W. R. Zame, *Covering spaces and the Galois theory of commutative Banach algebras*, J. Functional Analysis **55**(1984), 151–175.

Mathematical Institute
The Technical University of Denmark
Building 303
DK-2800 Lyngby, Denmark

Department of Mathematics
University of California
Los Angeles, CA 90024
U. S. A.