Local and Global Value Sets

Shai Rosenberg

Local and Global Value Sets

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Shai Rosenberg

Submitted to the Senate of
the Technion — Israel Institute of Technology
Tevet 5782 Haifa December 2021

The research thesis was done under the supervision of Prof. Danny Neftin in the Mathematics Department.

The generous financial support of the Technion is gratefully acknowledged.

Contents

Abstract

Given a polynomial $f \in \mathbb{Z}[X]$, let f_p denote the polynomial obtained by reducing the coefficients of f modulo a prime $p \in \mathbb{Z}$. We consider two problems, concerning the extent to which f is determined by properties of f_p, where p runs over the set of prime integers. The first problem, is to compare the minimal number of preimages of values of f, with the minimal number of preimages of values of f_p. As a specific instance of this problem, consider the following question: for which polynomials $f \in \mathbb{Z}[X]$, each value of f_p has at least 2 preimages, for almost all primes $p \in \mathbb{Z}$? The second problem, is the well studied problem of Kronecker conjugate polynomials, where one asks whether a polynomial f is determined by the value sets of f_p. Two polynomials f, g are Kronecker conjugate if f_p and g_p have the same value sets for almost every prime integer. One obvious reason is when $f(X) = g(aX + b)$ for some $a, b \in \mathbb{Q}$. But there are also known nonobvious examples of Kronecker conjugate polynomials.

We discuss a close analogy between the two problems and show that they can be viewed as two complementary instances of the same problem. Each of the two problems translates to an equivalent group theoretic condition on the corresponding monodromy groups of the polynomials.

Solutions to both problems for indecomposable polynomials, that is, polynomials f that cannot be written as $f = g \circ h$ for two polynomials g, h with $\deg g > 1, \deg h > 1$, follow from the classification of monodromy groups of indecomposable polynomials. We consider the problems for decomposable polynomials, where a monodromy classification is out of reach, and solve both of the above problems in all cases where f has no decomposition $g \circ h$ for h in an explicit list.

Abbreviations and Notations

$f\|_S$	—	the reduction of a function $f : X \to Y$ to a subset $S \subseteq X$
$\mathcal{O}_K$	—	The ring of integers of a number field K
$\mathbb{P}_K$	—	The set of prime ideals of $\mathcal{O}_K$
$\overline{K_\mathfrak{p}}$	—	$\overline{K_\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ where K is a number field, and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$
$\mathrm{Mon}(f)$	—	The monodromy group of a polynomial f
$\overline{\mathrm{Mon}}(f)$	—	The geometric monodromy group of a polynomial f
$RH(\sigma)$	—	Riemann Hurwitz contribution of σ
1_G	—	The identity element of a group G
C_n	—	The cyclic group of order n
D_n	—	The dihedral group of order n
$\mathrm{AGL}_n(q)$	—	Affine group over the finite field with q elements
$\mathrm{PGL}_n(q)$	—	Projective general linear group
$\mathrm{PSL}_n(q)$	—	Projective special linear group
vm	—	Minimal value multiplicity
rvm	—	Minimal residual value multiplicity

For a group G acting on a set $\mathcal{Z}$, and $z \in \mathcal{Z}$:

$G^{\{z\}}$	—	The stabilizer of z
$G^{\{S\}}$	—	The stabilizer of S, where $S \subseteq \mathcal{Z}$
$N_G(S)$	—	The normalizer of S in G where S is a subset of G
$\theta(\sigma)$	—	$\#\{z \in \mathcal{Z} \mid \sigma \cdot z = z\}$ where $\sigma \in G$
$\tau(G)$	—	$[N_G(G^{\{z\}}) : G^{\{z\}}]$
$\tilde{\tau}(G)$	—	$\min\{\theta(\sigma) \mid \sigma \in G^{\{z\}}\}$
$G\|_\mathcal{Z}$	—	The image of the permutation representation $G \to \mathrm{Sym}(\mathcal{Z})$

Chapter 1

Introduction

1.1 General introduction

For a polynomial f over the ring of integers $\mathcal{O}_K$ of a number field K, let $f_{\mathfrak{p}}$ be the polynomial obtained by reducing the coefficients of f modulo a prime ideal $\mathfrak{p}$, in the set $\mathbb{P}_K$ of prime ideals of $\mathcal{O}_K$. One may ask to what extent are properties of f determined by properties of $f_{\mathfrak{p}}$, considered for almost all prime ideals $\mathfrak{p} \in \mathbb{P}_K$ of $\mathcal{O}_K$. We consider two such problems. The first problem is to compare the number of preimages of values of f with the number of preimages of values of $f_{\mathfrak{p}}$. The second concerns Kronecker conjugate polynomials, where one asks to what extent is f determined by the value sets of $f_{\mathfrak{p}}$. We also show that these two problems are more related than it seems at first glance.

A central invariant attached to a polynomial $f \in \mathcal{O}_K[X]$ is a permutation group $\mathrm{Mon}(f)$, called the monodromy group of f, cf. Section 2.5. Many properties of a polynomial depend merely on its monodromy group. Thus, a problem concerning polynomials is often translated first to a group theoretic equivalent problem which is given in terms of monodromy groups, and then tackled using tools from group theory. In particular, each of the two problems mentioned above, translates to an equivalent problem which is stated in group theoretic terms, cf. Sections 5.1, 4.1.

The main theorem introduced in this thesis, provides information about the minimal normal subgroup of the monodromy group of a polynomial. We apply the main theorem to the two problems mentioned above.

1.2 Minimal residual value multiplicity

Let f be a polynomial over a field $\mathbb{F}$, and let $k \in \mathbb{Z}^+$ be a positive integer. We say that f is *at least k-to-1* over $\mathbb{F}$ if each value of f has at least k preimages, counted with multiplicity. Namely, f is at least k-to-1 over $\mathbb{F}$ if:

$$f(X) - f(a) \text{ has at least } k \text{ roots (counted with multiplicity) for all } a \in \mathbb{F}. \tag{1.1}$$

An element $b \in \mathbb{F}$ is called a *branch point* of f if $f(X)-b$ has multiple roots in an algebraic closure of $\mathbb{F}$. Note that if $f(X)-b$ has a multiple root a, then a is a root of the derivative of f. Hence there are at most $\deg f - 1$ branch points. Except for the few cases where $b := f(a)$ is a branch point, the condition in (1.1) simply means that the preimage $f^{-1}(b) = \{\tilde{a} \in \mathbb{F} : f(\tilde{a}) = b\}$ of b, contains at least k elements.

Now assume f is a polynomial over the ring of integers $\mathcal{O}_K$ of a number field K. For a prime $\mathfrak{p}$ of $\mathcal{O}_K$, let $f_\mathfrak{p}$ denote the polynomial over the finite field $\mathcal{O}_K/\mathfrak{p}$ which is obtained by reducing the coefficients of f modulo $\mathfrak{p}$.

We are mainly concerned with the relation between

1. The polynomial f over K being at least k-to-1.

2. The polynomial $f_\mathfrak{p}$ over $\mathcal{O}_K/\mathfrak{p}$ being at least k-to-1 for almost all primes $\mathfrak{p} \subset \mathcal{O}_K$.

We now introduce notation that will simplify the discussion about polynomials which are at least k-to-1. When k is the maximal positive integer for which 1 holds, we say that $\mathrm{vm}_K(f) := k$ is the *minimal value multiplicity* of f. When k is the maximal positive integer for which 2 holds, we say that $\mathrm{rvm}_K(f) := k$ is the *minimal residual value multiplicity* of f. The inequality $\mathrm{vm}_K(f) \leq \mathrm{rvm}_K(f)$ is straightforward. With this notation, a polynomial f satisfies 1 but does not satisfy 2 above for some $k \in \mathbb{Z}^+$ if and only if $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$.

In Section 5.1, the problem is translated to an equivalent problem in group theoretic terms. The group theoretic characterization reveals that the polynomials f for which $\mathrm{vm}_K(f) = m$ are of the form $f = g \circ X^m \circ \ell$ for some linear polynomial $\ell(X) := aX + b$ with $a, b \in K$, and K contains all the m-th roots of unity, cf. Proposition 5.3.5.

In Section 5.4, we show that for an indecomposable polynomial f we always have $\mathrm{vm}_K(f) = \mathrm{rvm}_K(f)$. Here a polynomial f is *decomposable* over K if $f = h_1 \circ h_2$ for two nonlinear polynomials $h_1, h_2 \in K[X]$, otherwise f is *indecomposable*. This raises the question whether there exist decomposable polynomials for which $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$. The answer is affirmative: we show two examples where $\mathrm{vm}_K(f) = 1$ and $\mathrm{rvm}_K(f) = 2$, cf. Section 5.6.

In Section 5.5, we investigate $\mathrm{rvm}_K(f)$ in the case where f is decomposable. The main result is Theorem 1.2.1 below. We first introduce the relevant terminology: We say that f is *cyclic* if $f = \ell_1 \circ X^n \circ \ell_2$, and we say that f is *dihedral* if $f = \ell_1 \circ T_n \circ \ell_2$ for some linear polynomials $\ell_1, \ell_2 \in \mathbb{C}[X]$, where T_n is the degree n (normalized) *Chebyshev polynomial* satisfying $T_n(X + \frac{1}{X}) = X^n + \frac{1}{X^n}$, cf. Section 2.6. We say that $f = g \circ h$ with $g, h \in K[X]$ and h nonlinear indecomposable is a *unique right decomposition* if for any decomposition $f := \tilde{g} \circ \tilde{h}$ of $f \in K[X]$ with $\tilde{g}, \tilde{h} \in K[X]$ and $\tilde{h}$ nonlinear indecomposable, we have $\tilde{h} = \ell \circ h$ for some linear polynomial $\ell \in K[X]$.

Theorem 1.2.1 *Let $\mathcal{O}_K$ be the ring of integers of a number field K. Let $f \in \mathcal{O}_K[X]$ be a decomposable polynomial with a unique right decomposition $f = g \circ h$ for a noncyclic and nondihedral indecomposable $h \in K[X]$ of degree $\deg h \neq 4$. Then $\mathrm{rvm}_K(f) = 1$.*

Since "almost all" polynomials $h \in \mathcal{O}_K[X]$ satisfy the assumptions of the theorem above for any given g, the theorem above shows in particular, that a composition of any given polynomial g with a randomly chosen indecomposable polynomial h, almost surely yields a polynomial $f := g \circ h$ with $\mathrm{rvm}_K(f) = 1$. In particular polynomials f with $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$ are in some sense "rare".

1.3 Kronecker conjugate polynomials

Let $V_\mathfrak{p}$ denote the value set of $f_\mathfrak{p}$. That is,

$$V_\mathfrak{p} := \{f_\mathfrak{p}(a) | a \in \overline{K_\mathfrak{p}}\} \tag{1.2}$$

where $\overline{K_\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$.

We consider the following question: to what extent is f determined by the sets $V_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over the prime ideals of $\mathcal{O}_K$? This question leads to the consideration of pairs of polynomials f, g over $\mathcal{O}_K$, which have the same value sets modulo all but finitely many prime ideals of K, namely, f and g satisfy:

$$V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g) \text{ for almost all } \mathfrak{p} \in \mathbb{P}_K. \tag{1.3}$$

We say that two polynomials f and g are *Kronecker conjugate* over K, and denote $f \sim_K g$, if they satisfy (1.3) above. The polynomials f and g are obviously Kronecker conjugate if $g(X) = f(aX + b)$ for some $a, b \in K$. In such a case we say that f and g are *linearly related* over K. If f and g are Kronecker conjugate but not linearly related, we say that f and g are *properly Kronecker conjugate*. If there is no polynomial $g \in \mathcal{O}_K[X]$ such that f and g are properly Kronecker conjugate, then f is determined, up to composition with linear polynomials, by the value sets $V_{\mathfrak{p}}(f)$.

In 1968, H. Davenport posed the problem of determining the properly Kronecker conjugate pairs of polynomials over $\mathbb{Q}$. One known example of properly Kronecker conjugate polynomials over $\mathbb{Q}$ is $f(X) = X^8, g(X) = 16X^8$, cf. Section 1.5.4.

Fried showed that if f is an indecomposable polynomial with coefficients in $\mathbb{Z}$, then there is no polynomial g over $\mathbb{Z}$ such that f and g are properly Kronecker conjugate, cf. [7, Theorem 2]. The situation is slightly different if we consider indecomposable polynomials over larger number fields. A result by Fried and Feit [5] shows that for each $d \in \{7, 11, 13, 15, 21, 31\}$, there is a pair of properly Kronecker conjugate polynomials f, g over some number field K, where f is indecomposable and $\deg f = d$. For other degrees there is no polynomial g which is properly Kronecker conjugate to f. In particular, if f is indecomposable of degree greater than 31, then there is no polynomial g such that f and g are properly Kronecker conjugate. Müller [14] proved similar results for polynomials which are composition of two indecomposable polynomials. However, no similar result holds for polynomials which are composition of three indecomposable polynomials. This is shown by a construction of an infinite sequence of pairs of properly Kronecker conjugate polynomials, cf. [15]. While Kronecker conjugacy of polynomials which are composition of at most two indecomposable polynomials is well understood, the general case of decomposable polynomials has so far been widely open.

The trivial reason behind the existence of decomposable Kronecker conjugates is the following: If $h_1 \sim_K h_2$ for two polynomials $h_1, h_2 \in K[X]$, then we have $g \circ h_1 \sim_K g \circ h_2$. We prove the following theorem, which shows the converse holds, under some sufficient conditions.

Theorem 1.3.1 *Let $\mathcal{O}_K$ be the ring of integers of a number field K. Let $f \in \mathcal{O}_K[X]$ be a decomposable polynomial with a unique right decomposition $f = g \circ h$ for a noncyclic and nondihedral indecomposable $h \in K[X]$ of degree $\deg h \neq 4$.*

1. *If $f \sim_K f_2$ for $f_2 \in \mathcal{O}_K[X]$, then there exists $h_2 \in K[X]$ such that $f_2 = g \circ h_2$, and $h \sim_K h_2$.*
2. *If $f \in \mathbb{Q}[X]$ and $f \sim_{\mathbb{Q}} f_2$ for $f_2 \in \mathbb{Z}[X]$, then there exist $a, b \in \mathbb{Q}$ such that $f(X) = f_2(aX + b)$.*

Although the theorem above does not involve any group theoretic terms, the proof of the theorem is based on group theory and Galois theory. The definition of Kronecker conjugacy of polynomials over a number field has an equivalent group theoretic definition, cf. Section 4.1. The latter allows us to naturally extend the definition of Kronecker conjugacy to polynomials over any field of characteristic zero. With this definition, Theorem 1.3.1 then holds for polynomial $f, g \in K[X]$ over an arbitrary subfield $K \subseteq \mathbb{C}$. The formulation of Theorem 1.3.1 becomes even simpler when assuming $K = \mathbb{C}$.

Theorem 1.3.1 above with $K = \mathbb{C}$ is proved by Müller–Völklein [16, Theorem 4.1.2] under the following stronger assumption: There exists a decomposition $f = g_1 \circ \cdots \circ g_n$ where each of $g_1, \ldots, g_n$ is indecomposable, noncyclic, nondihedral, of degree different from 4, and is not properly Kronecker conjugate to any other polynomial. This assumption is indeed stronger: by Ritt's polynomial decomposition theorem, cf. Section 2.10, the polynomials $g_1, \ldots, g_n$ are unique in this case (up to obvious changes by composing $g_1, \ldots, g_n$ with linear polynomials). Thus the factorization $f = g \circ h$, with $g := g_1 \circ \cdots \circ g_{n-1}$ and $h := g_n$ is unique right. Roughly speaking, Theorem 1.3.1 shows it suffices to assume the right most composition factor g_n is unique, up to obvious changes, and to impose conditions on g_n, while no constrain on the other factors is imposed.

Note that h and h_2 in Theorem 1.3.1.(1) above may either be linearly related, or properly Kronecker conjugate. When h and h_2 are linearly related,

we have that f and f_2 are linearly related. That is, f and f_2 can be properly Kronecker conjugate only if the indecomposable polynomials h and h_2 are properly Kronecker conjugate, reducing to the well understood indecomposable case. In particular, Theorem 1.3.1.(2) follows from Theorem 1.3.1.(1) since there are no pairs of properly Kronecker conjugate indecomposable polynomials over $\mathbb{Q}$ by Fried's above mentioned result.

Polynomials f satisfying $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$ and Kronecker conjugacy of polynomials may be viewed as complementary instances of the same problem, as discussed in Chapter 6. This point of view explains the similiarity between Theorems 1.2.1 and 1.3.1.

1.4 Methods

The main tool we apply in this thesis, is a theorem describing a minimal normal subgroup of the monodromy group of a decomposable polynomial (namely, a polynomial f which can be decomposed as $f = g \circ h$ for some nonlinear polynomials g and h). We state and prove this theorem in Chapter 3. Since this theorem provides details about the structure of the monodromy group of a polynomial, we believe it may have further applications.

To describe the theorem, let $f \in K[X]$ be a decomposable polynomial with a unique right decomposition $f = g \circ h$ for a noncyclic and nondihedral indecomposable $h \in K[X]$ of degree $\deg h \neq 4$. Let L be the minimal normal subgroup of $U := \mathrm{Mon}(h)$, which is unique in this case, cf. Lemma 2.6.1. Here $\mathrm{Mon}(h) := \mathrm{Gal}(\Omega/K(t))$ is the monodromy group of h, where t is a transcendental over K, and Ω is the Galois closure of $K(x)$ over $K(t)$, for a root x of $f(X) - t \in K(t)[X]$.

The main result, which we state and prove in Chapter 3, is Theorem 3.1.1. It shows that under the assumptions above, $\mathrm{Mon}(f)$ contains a minimal normal subgroup isomorphic to L^m, where $m = \deg g$. To describe this minimal normal subgroup, we rely on the well known fact that the monodromy group of a decomposable polynomial $f = g \circ h \in K[X]$ can be embedded in the wreath product

$$U \wr_{\mathcal{X}} \mathrm{Mon}(g) := U^{\mathcal{X}} \rtimes \mathrm{Mon}(g), \tag{1.4}$$

where the group $U^{\mathcal{X}}$ is a direct product of m copies of U indexed by the set

$\mathcal{X}$ on which $\mathrm{Mon}(g)$ acts, cf. Section 2.4 for the definition of the semidirect product action in (1.4). Now, assume $\mathrm{Mon}(f) \leq U \wr_{\mathcal{X}} \mathrm{Mon}(g)$. Considering $U^{\mathcal{X}}$ as a subgroup of $U^{\mathcal{X}} \rtimes \mathrm{Mon}(g) = U \wr_{\mathcal{X}} \mathrm{Mon}(g)$ (in the obvious way), Theorem 3.1.1 provides sufficient conditions for $\mathrm{Mon}(f)$ to contain the subgroup $L^{\mathcal{X}}$ of $U^{\mathcal{X}}$. Namely:

$$L^{\mathcal{X}} \leq \mathrm{Mon}(f) \leq \mathrm{Mon}(h) \wr_{\mathcal{X}} \mathrm{Mon}(g). \tag{1.5}$$

Moreover, $L^{\mathcal{X}}$ is a minimal normal subgroup of $\mathrm{Mon}(f)$. Theorem 3.1.1 is an adaptation of the work of Aschbacher and König–Neftin, cf. [10, Lemma 3.1], and applies it to monodromy groups of polynomials. In Chapters 4 and 5, we deduce consequences from Condition (1.5) above.

1.5 Relation to other problems

1.5.1 A group theoretic characterization of vm and rvm

We discuss the problem from a group theoretic point of view. The relation of the discussion here to polynomials f satisfying $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$ is established in Section 5.2. Let G be a group acting transitively on a set $\mathcal{Z}$, with point stabilizer $G^{\{z\}} := \{\sigma \in G | g \cdot z = z\}$ for some $z \in \mathcal{Z}$. Let

$$\theta(\sigma) := \#\{z \in \mathcal{Z} | \sigma \cdot z = z\} \tag{1.6}$$

denote the number of elements of $\mathcal{Z}$ fixed by σ. We make the following definitions:

$$\tilde{\tau}(G) := \min_{\sigma \in G^{\{z\}}} \theta(\sigma), \text{ and} \tag{1.7}$$

$$\tau(G) := \#\{z \in \mathcal{Z} | \sigma \cdot z = z, \quad \text{for all } \sigma \in G^{\{z\}}\}. \tag{1.8}$$

Note that these definitions do not depend on the choice of z, since for a transitive action, the point stabilizers are conjugate subgroups.

In Chapter 5, we show that for any polynomial $f \in \mathcal{O}_K[X]$, we have $\mathrm{vm}_K(f) = \tau(G)$ and $\mathrm{rvm}_K(f) = \tilde{\tau}(G)$ where G is the monodromy group of f. Thus f satisfies $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$ if and only if $\tau(G) \lneqq \tilde{\tau}(G)$.

The inequality $\tau(G) \leq \tilde{\tau}(G)$ follows immediately from the definitions

above. We consider the cases where this inequality is strict, that is:

$$\tau(G) \lneqq \tilde{\tau}(G). \tag{1.9}$$

The case where G is primitive corresponds to the case where f is indecomposable, since the monodromy group of an indecomposable polynomial is primitive, cf. Section 2.9. There are examples of primitive groups G, with $\tau(G) = 1$, and arbitrary large $\tilde{\tau}(G)$. One such example is given in Chapter 5. However, for an indecomposable polynomial f we always have $\mathrm{rvm}_K(f) = \mathrm{vm}_K(f)$ as we will show indeed. That is, the problem with an arbitrary primitive G, has a different solution in nature, compared to the problem where G is restricted to be a monodromy group of an indecomposable polynomial f. This further justifies considering the existence of decomposable polynomials f with $\mathrm{vm}_K(f) \lneqq \mathrm{rvm}_K(f)$.

1.5.2 A group theoretic characterization of Kronecker conjugacy

A group theoretic characterisation of Kronecker conjugacy of polynomials, reveals a relation to the following group theoretic problem. Let G be a group, and let U_1, U_2 be two subgroups of G. Consider the following condition:

$$\bigcup_{g \in G} gU_1g^{-1} = \bigcup_{g \in G} gU_2g^{-1}. \tag{1.10}$$

The condition above was studied from a pure group theoretic perspective, cf. [25], [26] and [27]. In the next section, we elaborate about the close relation of Condition (1.10) to Kronecker conjugate polynomials and Kronecker equivalent fields.

1.5.3 Kronecker equivalent and arithmetically similar fields

We indicate an analogy between Kronecker conjugacy of polynomials, and the well studied subject of Kronecker equivalent fields and arithmetically equivalent fields, cf. [18]. Let K/k be extension of number fields. Let $f(\mathfrak{b}/\mathfrak{p})$ be the residue degree of a prime ideal $\mathfrak{b} \in \mathbb{P}_K$. Define

$$D(K/k) := \{\mathfrak{p} \in \mathbb{P}_k | f(\mathfrak{b}/\mathfrak{p}) = 1 \text{ for some } \mathfrak{b} \in \mathbb{P}_K, \text{ where } \mathfrak{b}|\mathfrak{p}\}$$

Two field extensions K_1, K_2 of k are called *Kronecker equivalent* if $D(K_1/k)$ and $D(K_2/k)$ differ by a finite set.

Let Ω be a Galois extension of k containing K_1 and K_2. Let $G := \mathrm{Gal}(\Omega/k)$, $U_1 := \mathrm{Gal}(\Omega/K_1)$ and $U_2 := \mathrm{Gal}(\Omega/K_2)$. Let $1_U^G(\sigma)$ stand for the permutation character of the action of G on the coset space G/U, for a subgroup $U \leq G$. Namely, $1_U^G(\sigma)$ equals the number of fixed points of σ with respect to the action of G on the coset space G/U. See [18] for the proof of the following theorem.

Theorem 1.5.1 *The following are equivalent*

1. $D(K_1/k) = D(K_2/k)$.

2. $D(K_1/k)$ *and* $D(K_2/k)$ *differ by a set of Dirichlet density 0.*

3. $$\bigcup_{g \in G} gU_1g^{-1} = \bigcup_{g \in G} gU_2g^{-1}. \tag{1.11}$$

4. $$1_U^G(\sigma) > 0 \Longleftrightarrow 1_{U'}^G(\sigma) > 0 \text{ for all } \sigma \in G. \tag{1.12}$$

Theorem 1.5.1.(3) provides a group theoretic characterisation of Kronecker equivalent fields. Similarly, most of the known results concerning Kronecker conjugate polynomials, are based on an equivalent characterisation of Kronecker conjugacy of polynomials in group theoretic terms, which is essentially the same as (1.11) above, cf. Section 4.1. Namely, the investigation of both Kronecker equivalent fields and Kronecker conjugate polynomials, comes down to the investigation of two subgroups U_1 and U_2 of a group G, satisfying (1.11) above. The only difference is that rather than letting G stand for a Galois group of an extension of k, as in Theorem 1.5.1, for the investigation of Kronecker conjugate polynomials, we let G stand for the Galois group of a field extension over a function field $k(t)$, where t is a transcendental over k.

Two field extensions $K/k, K'/k$ are called *arithmetically equivalent* if rather than (1.12) above, we require the stronger condition:

$$1_{U_1}^G(\sigma) = 1_{U_2}^G(\sigma) \text{ for all } \sigma \in G. \tag{1.13}$$

Arithmetically equivalent fields share many invariants. For example, if K and K' are arithmetically equivalent over k, then they have the same degree over k, the same Dedekind zeta function: $\zeta_K = \zeta_{K'}$, the same discriminant over k, and the same group of roots of unity (more invariants of K and K' which coincide are listed in [18]). For the analogous case of Kronecker conjugate polynomials, the stronger Condition 1.13 above implies that not only the value set of $f_{\mathfrak{p}}$ equals the value set of $g_{\mathfrak{p}}$, but the multiplicities of each shared value of $f_{\mathfrak{p}}$ and $g_{\mathfrak{p}}$ are the same. Namely the number of roots of $f_{\mathfrak{p}}(X) - a$ equals the number of roots of $g_{\mathfrak{p}}(X) - a$ for all $a \in \overline{K_{\mathfrak{p}}}$.

1.5.4 Intersective polynomials

Assume $f \in \mathbb{Z}[X]$ satisfies $\mathrm{vm}_{\mathbb{Z}}(f) \lneqq \mathrm{rvm}_{\mathbb{Z}}(f)$. For $a \in \mathbb{Z}$, define a polynomial

$$F_a(X) := \frac{f(X) - f(a)}{\prod_{i=1}^{s}(X - a_i)},$$

where $X - a_1, \ldots, X - a_s$ are the linear factors of $f(X) - f(a)$. For some $a \in \mathbb{Z}$ we must have $s = \mathrm{vm}_{\mathbb{Z}}(f)$. In this case, the polynomial F_a does not have a root in $\mathbb{Q}$, but it has a root modulo $\mathfrak{p}$ for almost all $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$: since $s \lneqq \mathrm{rvm}_{\mathbb{Z}}(f)$, the polynomial $f(X) - f(a)$ must have a root modulo $\mathfrak{p}$ other than $a_i (\mathrm{mod}\, \mathfrak{p})$, for almost all $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$. Similarly, if f and g are properly Kronecker conjugate, and $g(a) \neq f(b)$ for all $b \in \mathbb{Q}$, then the polynomial $F_a(X) := f(X) - g(a)$ has no rational root, but it has a root modulo $\mathfrak{p}$ for almost every prime $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$.

As an example, the polynomials $f(X) := X^8$ and $g(X) := 16X^8$ being properly Kronecker conjugate, is a direct consequence of the equation $u^8 = 16$ having a solution modulo $\mathfrak{p}$ for almost all primes $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$, while not having a solution in $\mathbb{Q}$. Conversely, f and g being properly Kronecker conjugate implies that $F_1(X) = X^8 - 16 = 0$ has a solution modulo $\mathfrak{p}$ for almost all $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$, while not having a solution in $\mathbb{Q}$. More generally, the pair $f(X) := X^n$ and $g(X) := uX^n$ for $u \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$, is Kronecker conjugate if and only if the equation $X^n = u$ has a solution modulo $\mathfrak{p}$, for all

but finitely many primes $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$. Thus Kronecker conjugacy of polynomials may be viewed as a generalization of the following problem, whose answer is given in [2]: when does the equation $X^n = u$, with $u \in \mathbb{Z}$, have a solution modulo $\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in \mathbb{P}_{\mathbb{Z}}$?

A polynomial f with coefficients in $\mathbb{Z}$ is called *intersective*, if it has no rational root, but it has a root modulo n for all $n \in \mathbb{Z}$. Thus intersective polynomials satisfy a stronger condition compared to the above. Intersective polynomials were extensively studied, cf. for example [22], [23], [12]. Let F be a Galois field over $\mathbb{Q}$, and let $G = \mathrm{Gal}(F/\mathbb{Q})$. The following are equivalent:

1. There exists an intersective polynomial f with splitting field F, which is the product of m irreducible polynomials of degree greater than 1 in $\mathbb{Q}[X]$.

2. For some proper subgroups $U_1, \ldots, U_m$ of G, one has:

$$G = \bigcup_{i=1}^{m} \Big(\bigcup_{\tau \in G} \tau U_i \tau^{-1} \Big), \tag{1.14}$$

$$\bigcap_{i=1}^{m} \Big(\bigcap_{\tau \in G} \tau U_i \tau^{-1} \Big) = \{1_G\}, \tag{1.15}$$

   and moreover for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ the decomposition group satisfies $D(\mathfrak{p}/p) \subseteq \tau U_i \tau^{-1}$ for some i and $\tau \in G$.

A relation of polynomials f with $\mathrm{vm}(f) \lneqq \mathrm{rvm}(f)$ and Kronecker conjugate polynomials to intersective polynomials can be shown also by means of the corresponding group theoretic characterisations. Roughly this is done by showing that the group theoretic characterisation of the first two problems, is related to covering a group by some of its proper subgroups as in (1.14).