Radicals in arithmetic

Palenstijn, W.J.

Preface

This manuscript consists of two parts. In the first part, comprising Chapters 1 to 6, we build a theory for *entangled radicals*, and apply this to generalizations of Artin's primitive root conjecture. In the second part, consisting of Chapter 7, we give an algorithm for enumerating so-called *ABC triples* and report results from the ABC@home project, a volunteer computing project that has enumerated all ABC triples up to 10^{18}.

Artin's primitive root conjecture, first stated in 1927 and adapted in the 1950s, concerns the density of prime numbers q for which a fixed integer $x \neq 0$ generates the cyclic group $\mathbf{F}_q^*$. Artin conjectured that this density exists and is equal to a constant A times a rational correction factor depending on x that can be given explicitly [2], with A defined as

$$A = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558\ldots$$

In 1967 this conjecture was proved by Hooley [16] assuming the Generalized Riemann Hypothesis.

The algebraic number theory argument behind the conjecture, which we give in its entirety in Chapter 1, revolves around the degrees of splitting fields K_p of the polynomials $X^p - x$ and their composita. These degrees are reflected in the expression $p(p-1)$ in the constant above.

If we for the moment assume that x is not a perfect power, the mentioned correction factor is necessary to compensate for the fact that the fields K_p are not always linearly disjoint. For $x = 3$ the fields K_p *are* all linearly disjoint, and in this case the correction factor is 1. However, for $x = 5$, the splitting field of $X^2 - 5$ is contained in the splitting field of $X^5 - 5$ since we have $\mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\zeta_5)$.

These unexpected additive relations determine the value of the correction factor. In 2003, H.W. Lenstra, P. Moree and P. Stevenhagen [31] gave an interpretation of this factor which served as the basis for the treatment in the present manuscript.

Roots of polynomials of the form $X^n - a$ are called *radicals*, and following H.W. Lenstra [19], we shall refer to these unexpected additive relations as *entanglement* between radicals.

In Chapter 1, Theorem 1.5, we give a **generalization of Artin's primitive root conjecture to number fields**. We give the density as a similar product of a

constant independent of x, times an explicit rational correction factor. Chapter 1 is self-contained, and, besides containing the generalization of Artin's conjecture, acts as a prelude to the more general theory of entangled radicals covered in Chapter 2.

Let K be a field, $\bar{K}$ an algebraic closure of K, and $B \supset K^*$ a multiplicative group of radicals in $\bar{K}^*$ over K, i.e., elements of $\bar{K}^*$ of which a power is in K^*. Let us also assume that $K(B)$ is a Galois extension of K. Then determining the entanglement is a key ingredient for the computation of the field degree $[K(B) : K]$ and the Galois group $\mathrm{Gal}(K(B)/K)$. The strictly multiplicative structure of B is much more straightforward. In particular, the index of K^* in B and the structure of the automorphism group $\mathrm{Aut}_{K^*}(B)$ of automorphisms of B that are the identity on K^* are much simpler to analyze. This is also apparent in the context of Artin's conjecture: if we define $B_p = \langle \mathbf{Q}^*, \zeta_p, \sqrt[p]{x} \rangle$ for primes p, and B as the group generated by all B_p, then the structure of $\mathrm{Aut}_{\mathbf{Q}^*}(B)$ is independent of x (again assuming for the moment that x is not a perfect power), and in fact we have natural isomorphisms

$$\mathrm{Aut}_{\mathbf{Q}^*}(B) \cong \prod_{p \text{ prime}} \mathrm{Aut}_{\mathbf{Q}^*}(B_p) \cong \prod_{p \text{ prime}} (\mathbf{Z}/p\mathbf{Z}) \rtimes (\mathbf{Z}/p\mathbf{Z})^*.$$

Chapter 2 takes one further step back, and covers the setting of any group (in applications usually a Galois group) acting on a group B of radicals. Groups of radicals over a field have the property that all finite subgroups (i.e., those consisting of roots of unity) are cyclic. This property is sufficient for the automorphism group of the torsion subgroup of B to be abelian, and it turns out to be an essential part of the theory. In fact, this property is not only sufficient, but also necessary for the torsion subgroup of B to have an abelian automorphism group. (See Dixon [12], exercise 3.12 for this result due to G.A. Miller.)

Let B therefore be an abelian group of which all finite subgroups are cyclic, and let G be a profinite group acting continuously on B, where we give B the discrete topology. We write B^G for the subgroup of B consisting of the invariants under the action of G, and assume that B/B^G is torsion. This extension $B^G \subset B$ is what we shall call a Galois radical group extension (Definition 2.7). The condition of B/B^G being torsion encodes that the elements of B are radicals over B^G.

One of the main results of this thesis (Theorem 2.25) is that in this generality, **the image of G in $\mathrm{Aut}(B)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ and $E = \mathrm{Aut}_{B^G}(B)/\mathrm{im}(G)$ is abelian**. We call E the *entanglement group* of the action of G on B.

This result builds on analogues of Kummer theory, Schinzel's theorem, and other theorems traditionally used to describe radical field extensions, which we state and prove in Chapter 2.

A case of special interest is the entanglement group of the maximal radical extension of a field. We call this the **absolute entanglement group**, and compute it in Chapter 3 based on the theory of Chapter 2. The characteristic 0 case of these results has been announced in the lecture notes for a series of Colloquium Lectures by H.W. Lenstra [19] at the AMS Annual Meeting in 2006.

In Chapter 4 we explicitly compute entanglement groups over $\mathbf{Q}$, and apply that

to **compute field degrees of radical field extensions of Q**. We use the expressions for the entanglement group derived in Chapter 2 to construct a polynomial time algorithm to compute these degrees, up to an evaluation of Euler's totient function φ.

In Chapter 5 we then return to Artin's conjecture. Many variants of Artin's conjecture have been described and studied in the literature (see, e.g., [18, 20, 22, 24]). In many of these generalizations, the theory from Chapter 1 can no longer directly be used, since that only considered roots of square-free order. In Chapter 5 we apply the more general theory of Chapters 2 and 4 to a number of generalizations of Artin's conjecture over number fields.

Specifically, we look at so-called **near-primitive roots**, where we consider the density of primes $\mathfrak{q}$ of a number field K where a fixed $x \in K^*$ generates a subgroup of $(\mathcal{O}_K/\mathfrak{q})^*$ of index dividing a given integer t. For the case $K = \mathbf{Q}$, this has been treated by P. Moree [23] building on a result by Wagstaff [35]. Another extension we study is that of **higher rank analogues of Artin's conjecture**, where we take multiple non-zero elements $x_1, \ldots, x_k$ and consider the set of primes $\mathfrak{q}$ of K for which $\bar{x}_1, \ldots \bar{x}_k$ together generate $(\mathcal{O}_K/\mathfrak{q})^*$. Over the rationals, this is covered by P. Moree and P. Stevenhagen [24].

Due to the generality of the results of Chapter 2, we can also apply them outside of the setting of radicals in unit groups of (number) fields. The setting we turn to in Chapter 6 is that of tori. A torus is an algebraic group closely related to the multiplicative group $\mathbf{G}_{\mathrm{m}}$, which we considered in Chapters 1 and 5. To satisfy the requirement that finite subgroups are cyclic, we specifically restrict to **rank one tori over number fields**. A point on such a torus can be reduced at almost all primes, and as a consequence there is an analogue of Artin primitive root densities in this setting, studied for tori over $\mathbf{Q}$ by Chen [7]. We show that our theory of entangled radicals also applies to this setting, and use it to obtain a generalization of Artin's conjecture to rank one tori over number fields.

The final chapter of this manuscript covers an entirely different topic, and is independent of the first six chapters — except for the central role the word radical plays in both parts. Here, the *radical* of a positive integer is defined to be the product of its prime divisors, without multiplicity. An *ABC triple* is a triple (a, b, c) of coprime positive integers satisfying $a + b = c$ and $a \leq b$, and for which the radical of abc is smaller than c. For example, the smallest such triples are $1 + 8 = 9$ and $5 + 27 = 32$. In this chapter, we give bounds for the number of ABC triples, describe an **algorithm for enumerating all ABC triples** below a given bound, and report results from ABC@home, **a distributed volunteer computing project** that has enumerated all ABC triples with $c < 10^{18}$.