Introduction to the Third Edition

The third edition of "Field Arithmetic" improves the second edition in two ways. First it removes many typos and mathematical inaccuracies that occur in the second edition. In particular, it fills out a big gap in the References of the second edition, where unfortunately all references between "Gilmore and Robinson" and "Kantor and Lubotzky" are missing. Secondly, the third edition reports on five open problems of the second edition that were solved since that edition appeared in 2005.

János Kollár solved Problem 2 by proving that if each projective plane curve defined over a field K has a K-rational point, then K is PAC.

János Kollár also solved Problem 3 and proved that if K is a PAC field, w is a valuation of $\tilde{K}$, and V is a variety defined over K, then $V(K)$ is w-dense in $V(\tilde{K})$.

János Kollár partially settled Problem 21. He proved that every PAC field of characteristic 0 is C_1.

Problem 31 was affirmatively solved by Lior Bary-Soroker by establishing an analog of the diamond theorem for the finitely generated non-Abelian free profinite groups.

Finally, Eric Rosen suggested to reorganize Corollary 28.5.3 of the second edition that led to an affirmative solution of Problem 33.

Unfortunately, a full account of the first four solutions is out of the scope of the present volume.

Much of the improvment made in the present edition is due to Arno Fehm and Dan Haran. I am really indebted to them for their contribution.

Tel Aviv, Autumn 2007 Moshe Jarden

Introduction to the Second Edition

The first edition of "Field Arithmetic" appeared in 1986. At the end of that edition we gave a list of twenty-two open problems. It is remarkable that since then fifteen of them were partially or fully solved. Parallel to this, Field Arithmetic has developed in many directions establishing itself as an independent branch of Algebra and Number Theory. Some of these developments have been documented in books. We mention here "Groups as Galois groups" [Völklein] on consequences of the Riemann existence theorem, "Inverse Galois Groups" [Malle-Matzat] with a comprehensive report on finite Galois groups over number fields, "Profinite groups" [Ribes-Zalesskii] including the cohomology of profinite groups, "Analytic pro-p Groups" [Dixon-du.Sautoy-Mann-Segal] on closed subgroups of $\mathrm{GL}(n, \mathbb{Z}_p)$, "Subgroup Growth" [Lubotzky-Segal] on counting the number of subgroups of finitely generating groups, and "Multi-Valued Fields" [Ershov7] on the model theory of fields with several valuations. This led to an official recognition of Field Arithmetic by the Mathematical Reviews in the form of MSC number 12E30.

The extent which Field Arithmetic has reached makes it impossible for us to report in one extended volume about all exciting results which have been achieved. We have therefore made several choices which best suit the spirit of this book but do not extend beyond the scope of one volume.

The new results and additional topics have made it necessary to reorganize and to enlarge the sections dealing with background material. Of course, we took the opportunity afforded by editing a second edition to correct flaws and mistakes which occurred in the first edition and to add more details to proofs wherever it seemed useful.

We list the major changes and additions we made in the book:

Chapter 2 has been reorganized. Sections 2.5–2.9 of the first edition, which survey the theory of algebraic function fields of one variable, were moved to Chapter 3. Sections 2.5–2.8 dealing with linear disjointness, regular extensions, and separability appeared in the first edition as sections 9.1–9.3. A nice application of linear disjointness is Leptin's construction (which preceded that of Warehouse) of a Galois group isomorphic to a given profinite group (Proposition 2.6.12).

In addition to the introductory material about the theory of algebraic function fields of one variable, Chapter 3 now includes a proof of the Riemann-Hurwitz formula and a discussion of hyperelliptic curves.

The proof of Theorem 4.9 of the first edition, estimating the number of zeros of an absolutely irreducible polynomial over a finite field, had a flaw. This has been fixed in the proof of Theorem 5.4.1.

Likewise, the inequality given by [Fried-Jarden3, Prop. 5.16] is inaccurate. This inaccuracy is fixed in Proposition 6.4.8.

We find it more convenient to use the language of algebraic sets as introduced in [Weil5] for model theoretic applications. Section 10.8 translates the basic concepts of that language to the now more commonly used language of schemes.

Theorem 10.14 of the first edition (due to Frey-Prestel) says that the Henselian hull of a PAC field K is K_s. Proposition 11.5.3 (due to Prestel) strengthens this theorem. It says that K is w-dense in $\tilde{K}$ for every valuation w of $\tilde{K}$.

What we called "a separably Hilbertian field" in the first edition, is now called "a Hilbertian field" (Section 12.1). This agrees with the common usage and seems more appropriate for applications.

Section 13.5 gives an alternative definition of Hilbertianity via coverings leading to the notion of "g-Hilbertianity". This sets the stage for a generalization of a theorem of Zannier: Every global field has an infinite normal extension N which is g-Hilbertian but not Hilbertian (Theorem 13.6.2). Moreover, there is a unique factorization subring R of N with infinitely many irreducible elements (Example 15.5.8). This answers negatively Problems 14.20 and 14.21 of the first edition.

Chapter 13 includes now one of the major results of Field Arithmetic which we call "Haran's diamond theorem": Let M_1 and M_2 be Galois ex-

tensions of a Hilbertian field K and M a field between K and M_1M_2 not contained in M_1 nor in M_2. Then M is Hilbertian (Theorem 13.8.3). In particular, if N is a Galois extension of K, then N is not the compositum of two Galois extensions of K neither of which is contained in the other. This settles Problems 12.18 and 12.19 of the first edition.

The immediate goal of Hilbert's irreducibility theorem was to realize the groups S_n and A_n as Galois groups over $\mathbb{Q}$. Chapter 16 is dedicated to realizations of Galois groups over arbitrary Hilbertian fields. One of the most important of these results is due to Harbater (Proposition 16.12.1): Let K be a complete valued field, t an indeterminate, and G a finite group. Then G is **regular** over K, that is, $K(t)$ has a finite Galois extension F, regular over K, with $\mathrm{Gal}(F/K(t)) \cong G$. Unfortunately, none of the three proofs of this theorem fits into the scope of this book.

Section 16.6 proves a theorem of Whaples: Let K be a field and p a prime number. Suppose $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}/4\mathbb{Z}$ if $p = 2$) occurs as a Galois group over K. Then $\mathbb{Z}_p$ is realizable over K.

Section 16.7 generalizes a theorem of Hilbert: Let K be a field and $n \geq 2$ an integer with $\mathrm{char}(K) \nmid (n-1)n$. Then A_n is regular over K.

One of the most far-reaching attempts to realize arbitrary finite Galois groups over Hilbertian fields uses Matzat's notion of GAR realization of simple finite groups: Let K be a Hilbertian field and $\alpha\colon G \to \mathrm{Gal}(L/K)$ a finite embedding problem over K. Suppose every composition factor of $\mathrm{Ker}(\alpha)$ has a GAR realization over K. Then the embedding problem is solvable. This leads in particular to the realization of many finite groups over $\mathbb{Q}$ (Remark 16.9.5).

Chapter 17 deals mainly with **Melnikov's formations** $\mathcal{C}$ (i.e. sets consisting of all finite groups whose composition factors belong to a given set of finite simple groups). We prove that every free abstract group F is residually-$\mathcal{C}$. Thus, if the free pro-$\mathcal{C}$ group with a given rank m exists, then the canonical injection of F into $\hat{F}_m(\mathcal{C})$ is injective (Proposition 17.5.11 – Ribes-Zalesskii).

Konrad Neumann improved former results of Fried-Geyer-Jarden and proved that every field is stable (Theorem 18.9.3). This allows the construction of PAC Hilbertian Galois extensions of arbitrary countable Hilbertian fields (Theorems 18.10.2 and 18.10.3). We survey Neumann's proof in Section 18.9. The full proof unfortunately falls outside the scope of this book.

It seemed to be well known that the concept of absolute irreducibility of a variety is elementary. Unfortunately, we could find no solid proof for it in the literature. Proposition 19.5.9 fills in the gap by proving that result.

Section 21.2 includes now the classical results about C_i-fields and not only the corresponding results about weakly C_i-fields as was the case in Section 19.2 of the first edition.

Sections 21.8 gives a complete proof of Schur's Conjecture: If $f(X)$ is a polynomial with coefficients in a global field K with $\mathrm{char}(K) \nmid \deg(f)$ and f permutes $O_K/\mathfrak{p}$ for infinitely many primes $\mathfrak{p}$ of K, then each composition factor of f is linearly related over K to a Dickson polynomial of a prime

degree. Section 21.7 proves all lemmas about permutation groups which are used in the proof of Schur's Conjecture (Theorem 21.8.13). This includes the classification of subgroups of $\mathrm{AGL}(1,\mathbb{F}_l)$ (Lemma 21.7.2), and the theorems of Schur (Proposition 21.7.7) and Burnside (Proposition 21.7.8) about doubly transitive permutation groups.

Section 21.9 contains the Fried-Cohen version of Lenstra's proof of the generalized Carlitz's Conjecture: Let p be a prime number, q a power of p, and $f \in \mathbb{F}_q[X]$ a polynomial of degree $n > 1$ which is not a power of p. Suppose f permutes infinitely many finite extensions of $\mathbb{F}_q$. Then $\gcd(n, q-1) = 1$.

The universal Frattini p-cover of a finite group plays a central role in Fried's theory of modular towers. Section 22.11 introduces the former concept and proves its basic properties. Corollary 22.13.4 shows then that $\mathrm{PSL}(2,\mathbb{Z}_p)$ is a p-Frattini cover of $\mathrm{PSL}(2,\mathbb{F}_p)$ although it is not the universal p-Frattini cover.

Chapter 23 puts together material on PAC fields which appeared in Section 20.5 and Chapter 21 of the first edition.

The Beckmann-Black Problem is a refinement of the inverse problem of Galois Theory. Débes proved that the problem has an affirmative solution over PAC fields (Theorem 24.2.2).

Chapter 25 substantially extends the study of free profinite groups F of infinite rank which appeared in Section 24.4 of the first edition. Most of the material goes back to Melnikov. We characterize closed normal subgroups of F by their S-ranks, and prove that a closed subgroup of F is accessible if and only if it is homogeneous.

The first part of Chapter 25 reproduces the group theoretic version of Haran's diamond theorem.

Chapter 26 is completely new. It describes the properties of the closed subgroup $\langle \mathbf{x} \rangle$ and the closed normal subgroup $[\mathbf{x}]$ generated by a random e-tuple $\mathbf{x} = (x_1, \ldots, x_e)$ of elements of a finitely generated free profinite group F of finite rank $n \geq 2$. For example, with probability 1, $\langle \mathbf{x} \rangle \cong \hat{F}_e$ (Proposition 26.1.7). This solves Problem 16.16 of the first edition. In addition, with a positive probability, $[\mathbf{x}]$ has infinite rank and is isomorphic to $\hat{F}_\omega$ (Theorem 26.4.5 and Corollary 26.5.7). The latter result is based on the Golod-Shafarevich Inequality.

Chapter 28 considers an infinite field K which is finitely generated over its base field. It proves that for $e \geq 2$ the theory of all sentences θ which hold in almost all structures $\langle \tilde{K}, \sigma_1, \ldots, \sigma_e \rangle$ with $(\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ is undecidable. Moreover, the probability that a sentence θ hold in $\langle \tilde{K}, \sigma_1, \ldots, \sigma_e \rangle$ is in general a nonrational number.

Perhaps the most significant achievement of Field Arithmetic since the first edition appeared is the solution of Problem 24.41 of that edition: The absolute Galois group of a countable PAC Hilbertian field is free of rank $\aleph_0$. It was originally proved in characteristic 0 with complex analysis by Fried-Völklein. Then it was proved in the general case by Pop using rigid geometry and by Haran-Jarden-Völklein using "algebraic patching". The two

latter methods also lead to the proof that $\mathrm{Gal}(C(t))$ is a free profinite group if C is an arbitrary algebraically closed field (Harbater, Pop, Haran-Jarden). The method of Fried-Völklein led to the theory of modular towers of Fried.

A remote goal in Galois theory is the classification of absolute Galois groups among all profinite groups. In this framework, one tries to construct new absolute Galois groups out of existing ones. For example, for all fields $K_1, \ldots, K_n$ there exists a field K with $\mathrm{Gal}(K)$ isomorphic to the free product of $\mathrm{Gal}(K_1), \ldots, \mathrm{Gal}(K_n)$ (Pop, Melnikov, Ershov, Koenigsmann). Generalization of this result to infinite families of closed subgroups generalize the concepts "projective groups" and "PRC fields" or "PpC fields" to "relatively projective groups" and "pseudo closed fields" (Haran-Jarden-Pop). They generalize the classification of projective groups as those profinite groups appearing as absolute Galois groups of PAC fields.

All of the exciting material mentioned in the preceding two paragraphs lie unfortunately outside the scope of this volume.

It is my pleasure to thank colleagues and friends who critically read parts of the manuscript of the present edition of "Field Arithmetic": Michael Bensimhoun, David Brink, Gregory Cherlin, Michael Fried, Wulf-Dieter Geyer, Peter Müller, Dan Haran, Wolfgang Herfort, Alexander Lubotzky, Nikolay Nikolov, Dan Segal, Aharon Razon, and Irene Zimmermann.

Tel Aviv, Spring 2004 Moshe Jarden

Introduction to the First Edition

Our topic is the use of algebraic tools — coming mainly from algebraic geometry, number theory, and the theory of profinite groups — in the study of the elementary properties of classes of fields, and related algorithmic problems. (We take the precise definition of "elementary" from first order logic.) This subject has its more distant roots in Tarski's observation that, as a consequence of elimination theory, the full elementary theory of the class of all algebraically closed fields is decidable; this relies on the Euclid algorithm of finding the greatest common divisor of two polynomials in one variable over a field. In its first phase this line of thought led to similar results on real closed fields and p-adic fields.

The subject took a new turn with the work of James Ax [Ax2] on the elementary theory of the class of finite fields, which represents a radical departure in terms of the algebraic methods used. The analysis is based entirely on three properties of a finite field K:

(1a) K is perfect.

(1b) K has a unique extension of each degree.

(1c) There is an explicitly computable function $q(d, m)$ such that any absolutely irreducible variety V defined over K will have a K-rational point if $|K| > q(\dim(V), \deg(V))$.

The validity of the third condition for finite fields is a consequence of Riemann's hypothesis for curves over finite fields. Methods of logic, specifically ultraproducts, led Ax to consider this condition for infinite fields as well, in which case the lower bound afforded by the function q is vacuous, and the condition becomes:

(2) Every absolutely irreducible variety over K has a K-rational point.

Fields satisfying (2) are said to be pseudo algebraically closed, or PAC.

The second condition may be interpreted as a description of the absolute Galois group $\mathrm{Gal}(K)$ as a profinite group: $\mathrm{Gal}(K)$ is the free profinite group on one generator. In Ax' approach it was convenient to have an Abelian absolute Galois group, but a strong trend in later work has been the systematic analysis of situations involving progressively more general Galois groups. One of our central goals here is the presentation of the general theory of PAC fields in its modern form, and its connections with other branches of algebra. From what we have said so far, some connections with algebraic geometry and profinite groups are visible; a number theoretic connection will appear shortly.

One important feature of PAC fields is that they occur in profusion in nature and are in fact typical in the following sense. Since the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ of the rationals is a compact topological group, it carries a canonical invariant probability measure, the Haar measure. We can therefore ask for the probability that the fixed field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ of a sequence $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_e)$ of automorphisms of $\tilde{\mathbb{Q}}$ will be PAC; and we find that this occurs with probability 1. In addition, the absolute Galois group of $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is free on the e generators $\sigma_1, ..., \sigma_e$, again with probability 1. These facts are consequences of Hilbert's irreducibility theorem for $\mathbb{Q}$ (Chapter 13), at least in the context of countable fields. We will develop other connections between the PAC property and Hilbertianity.

There are also remarkable connections with number theory via the Chebotarev density theorem (Chapters 6, 13, 16, 20, 21, 31). For example, the probability that a given elementary statement ψ holds for the field $\tilde{\mathbb{Q}}(\sigma)$ coincides with the Dirichlet density of the set of primes for which it holds for the field $\mathbb{F}_p$, and this density is rational. Thus, the "probability 1" theory of the fixed fields $\tilde{\mathbb{Q}}(\sigma)$ coincides with the theory of "all sufficiently large" finite fields, which by Ax' work is an algorithmically decidable theory.

Ax' results extend to the "probability 1" theory of the fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ for $\boldsymbol{\sigma}$ of length $e > 1$, by somewhat different methods (Chapter 20), although the connection with finite fields is lost. The elementary theories of such fields are largely determined by three properties: PAC, characteristic zero, and having an absolute Galois group which is free on e generators. To determine the full elementary theory of one such field K, it is also necessary to describe the intersection $K \cap \tilde{\mathbb{Q}}$.

Although the absolute Galois group of a PAC field need not be free, it can be shown to be projective in a natural sense, and conversely any

projective profinite group occurs as the Galois group of some PAC field. In extending the theory from PAC fields with free Galois group to the general (projective) case, certain obstacles arise: for example, the algorithmic results do not extend. There is nonetheless a quite general theory, which enables us to identify some broad classes of projective profinite groups for which the associated classes of profinite groups behave well, and also to pinpoint unruly behavior in other case.

One approach to the algorithmic problems associated with PAC fields leads to the study of profinite groups G with the embedding property (the terminology reflects a preoccupation with the corresponding fields): for each pair of continuous epimorphisms $\varphi\colon G \to A$, $\alpha\colon B \to A$, where B is a finite quotient of G, we require that φ should factor through α. A perfect PAC field whose absolute Galois group is a group with the embedding property is called a Frobenius field. The elementary theory of all Frobenius fields can be computed quite explicitly. The algorithm has some relationship with elimination theory as used by Tarski. We associate to each elementary statement in the language of PAC fields a stratification of affine space into basic normal locally closed algebraic sets, each equipped with a Galois extension of its function field, and the given statement is reinterpreted as a statement about conjugacy classes of subgroups of the specified Galois groups. When the initial statement has no quantifiers this is a fairly trivial procedure, but addition of quantifiers corresponds to a special kind of "projection" of these Galois stratifications.

This procedure has not yet been closely examined from the point of view of computational complexity. Like most procedures which operate by tracing through a series of projections, it is effective but hopelessly inefficient in its present form. It is not yet clear whether it is substantially less efficient than Tarski's procedure for algebraically closed fields, nor whether, like that procedure, it can significantly reorganized and sped up.

The Galois stratification algorithm relies on techniques of effective algebraic geometry, and also involves substantial algorithmic problems of a new type connected with the theory of profinite groups. Specifically, it is necessary to determine, given two collections $A_1, ..., A_m$ and $B_1, ..., B_n$ of finite groups, whether or not there is a projective group with the embedding property which has each A_i as (continuous) image, but none of the groups B_j. The solution to this problem depends on recent work on projective covers (Chapter 22) and embedding covers (Chapter 24). Ultimately our decision problem reduces to the determination of the finite quotients of the projective cover of the embedding cover of a single finite group.

The theory of projective covers leads also to the undecidability results alluded to earlier. A fairly natural encoding of graphs into profinite groups is lifted by this theory into the class of projective profinite groups, and then by looking at the corresponding PAC fields we see that their elementary theories encode algorithmically undecidable problems (the analogous results for graphs are well known).

In the final chapter we return to our point of departure, the theory of finite fields. The zeta function of a Galois formula over a finite field is defined, and using a result of Dwork and Bombieri we show that some integral power of each such function is a product of an exponential and a rational function over $\mathbb{Q}$.

One of the goals of this book is to serve as a bridge between algebraists and logicians. For the algebraist there is a self contained introduction to the logic and model theory background for PAC fields (Chapter 7). Chapter 14 gives the "nonstandard" framework that suffices for Weissauer's proof of Hilbert's irreducibility theorem (Chapter 15), and Chapters 8 and 28 include basic recursion theory. On the other hand, for logicians with basic algebraic background (e.g. Lang's book "Algebra") Chapter 4 has the Stepanov-Bombieri elementary proof of the Riemann hypotheses for curves, and Chapter 6 gives an elementary proof of the Chebotarev density theorem. Both groups of readers may find the extensive treatment of profinite groups (Chapters 1, 17, 18, 22, 24, 25 and 26) and of Hilbertian fields (Chapters 12, 13, 15, and 16) valuable.

Although PAC fields arise over arithmetically rich fields, they themselves lack properties that we associate with the arithmetic, say, of the rationals. For example, a PAC field F admits no orderings and all Henselizations of F are separably closed (Section 11.5). Many PAC field results generalize to pseudo real closed (PRC) fields.

A field F is **PRC** if each absolutely irreducible variety defined over F has an F-rational point provided it has a nonsingular $\hat{F}$-rational point in each real closure $\hat{F}$ of F. Thus, a PRC field without orderings is PAC. This, and the development of the theory of **pseudo p-adically closed** PpC **fields** are outside the scope of this book. We refer to [Prestel1], to [Jarden12], [Haran-Jarden2], and to [Haran-Jarden3] for literature about PRC fields and to [Haran-Jarden4] for PpC fields. Similarly, we give no account of the theories of real closed fields and p-adically closed fields that preceded the development of the theory of PAC fields. In particular, for Hilbert's 17th problem and the Ax-Kochen-Ershov p-adic theory, we refer the reader to [Prestel2], [Ax-Kochen1, Ax-Kochen2, and Ax-Kochen3], and [Prestel-Roquette].

Acknowledgement: We are indebted to several colleagues who corrected errors in the process of critically reading the manuscript. In particular, Wulf-Dieter Geyer, Gregory L. Cherlin, and Dan Haran made crucial contributions.

Michael D. Fried, Gainesville, Florida
Moshe Jarden, Tel Aviv, Israel
Summer 1986

http://www.springer.com/978-3-540-77269-9

Field Arithmetic
Fried, M.D.; Jarden, M.
2008, XXIV, 792 p., Hardcover
ISBN: 978-3-540-77269-9