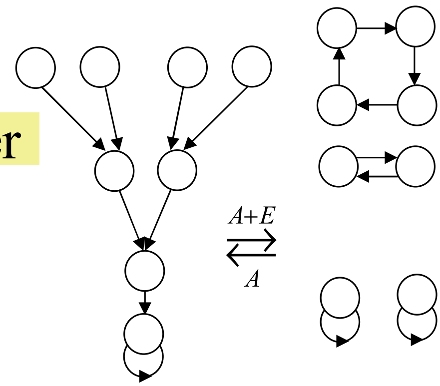
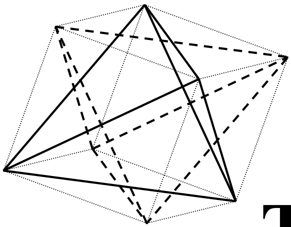
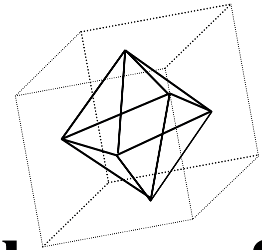
$\mathrm{SU}(2;\mathbb{F}_{\mathbb{C}}(q^2)) \to \mathrm{SO}(3;\mathbb{F}_{\mathbb{R}}(q))$

Wolf-Michael Wendler



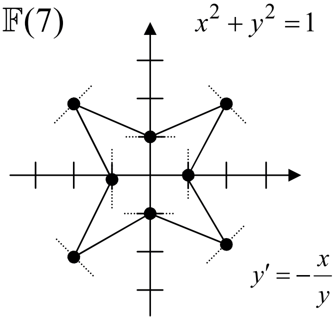


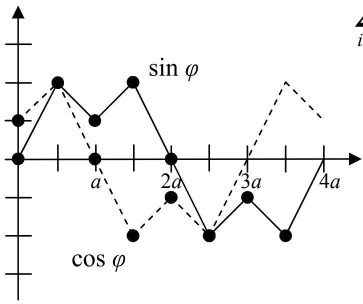


Theory of Finite Fields

$$\frac{q-1}{2}(N_{n,r^2\equiv R} + N_{n,r^2\equiv NR}) + N_{n,r^2\equiv 0} = q^n$$

$\mathbb{F}(7)$

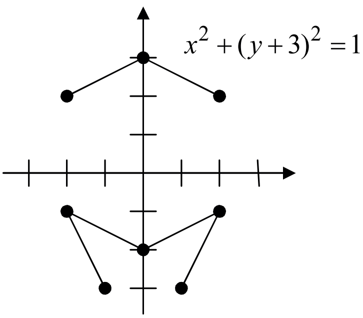




$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x},\ x \neq 1$$

$\mathrm{Ord}\ \mathrm{O}(n;\mathbb{F}(q))$

$$j^2 = -\alpha \equiv NR \in \mathbb{F}(q)$$



$$(a+b)^p = a^p + b^p$$

$$e^A = \varphi(A) = \begin{pmatrix} e^2 & e^2 & 0 \\ 0 & e^2 & 0 \\ 0 & 0 & e^4 \end{pmatrix} =: B$$

$E = mc^2$

SHAKER VERLAG

$\square \underline{E} = 0$

$$\overline{211}:\ \mathcal{A}^{-1}\{F(a)\} = f(k) = 3 + 2\left[(2+2j)^k + (2-2j)^k\right]$$

Wolf-Michael Wendler

Theory of Finite Fields

and a Comparison with Characteristic 0

Contact:

Professor i.R. Dr. rer. nat. Wolf-Michael Wendler

Am Soltkamp 13
38126 Braunschweig

FRG

e-mail: wolfmichael.wendler@t-online.de
wolfmichael.wendler@gmail.com

Berichte aus der Mathematik

Wolf-Michael Wendler

Theory of Finite Fields

and a Comparison with Characteristic 0

Shaker Verlag
Düren 2020

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Printed in Germany.

ISBN 978-3-8440-7614-1
ISSN 0945-0882

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

Preface to the German Edition

The theory of finite fields is a solid part of algebra and has numerous applications like coding theory and cryptography to name two of them. It is also part of discrete mathematics, frequently in conjunction with Latin squares and combinatory designs. If we restrict us to the field $\mathbb{F}(2)$, which is the smallest field with elements 0, 1 only, then this is basic for the mathematical investigation of electrical circuits in a broad sense.

But we may carry over linear systems theory over characteristic 0 to finite fields, indicating a somewhat unified representation of both worlds, which on a first glimpse are rather different. The comparison of mathematical relations in characteristic 0 and p gives a guide line, which in turn justifies the subtitle of the book. We use without exception textbooks as well as a variety of contributions of the author to the Proceedings of the Boolean Workshops in the years 2000 to 2014. These are briefly discussed (almost) chronologically in the following, because we cite them in the book, but do not give any further remarks.

The works [0], … , [4] contain the formulation of linear and mostly time-invariant systems theory and the complete solution of the homogeneous and autonomous equations. While [0], … , [3] exceptionally are formulated in characteristic $p = 2$, [4] gives for the first time a treatment for all primes $p > 2$. In addition, the works [5], [8] are formulated in char $p = 2$, they contain the Maxwell equation of electrodynamics as well classical mechanics. Thereby, we use a generalization of the well known numerical Boolean functions over $\mathbb{F}(2)$, which obey a differential calculus differing from characteristic 0. The arguments of these functions are assumed to be natural numbers. We mention that there is still almost total agreement with the result of characteristic 0.

[6], [7] treat the introduction to complex numbers of finite fields in characteristic $p \geq 2$ as well as their application to the formulation of quantum mechanics. As a matter of fact, these works partly are incomplete and not reasonable. In later works we introduce the terms number theoretical and algebraic approach in conjunction with quadratic field extensions. Complex numbers in the sense of the number theoretical approach are given in [9].

The investigation of conic sections may be found in [10]. There distinction is to be made between the two cases of odd primes and prime powers, namely $p^k \equiv 1 \bmod 4$ (I) and $p^k \equiv 3 \bmod 4$ (II), which appear throughout the book. Real functions, like powers, polynomials, and in particular transcendent functions are subject to [11]. Finally, we give in [12] a real analysis, which nicely goes along with the results we know from characteristic 0. Thereby we use a "set-operation" $\Delta x = 0$, which circumvents the term "limes".

The works [13], [14] contain again complex numbers, but within the algebraic approach as compare to the number theoretical approach as well as the formulation of the fundamental theorem of algebra. On this basis, in [14] Clifford-algebras and quaternions are treated, by which means than Dirac's theory may be carried over to characteristic $p \geq 2$.

In [15] we treat geometric and analytic properties of complex transcendental functions based on the complex exponential function in our Gaussian plane. The structure and meaning of these functions is recovered by investigating the multiplicative group of the field under consideration as wells the subgroups and cosets.

[16] contains classical Lie-groups and -algebras where in advance, manifolds on finite fields are introduced. This also is essential for [19], where the calculus of differential forms is worked out on the basis of the Grassmann-algebra. Moreover, in [17] we derive the matrix exponential function and its inverse which in turn is required for the classical Lie-groups and -algebras. This is accomplished by using the substitution polynomial, which may be carried over from characteristic 0.

By introducing rotation matrices in [18], the structure on ball of arbitrary dimension is explained: We derive the number of points of n-balls and moreover the number of circles and rotationally invariant points contained in them. As an aside we obtain the numbers of points (vector) with real, complex, and vanishing distance from the origin. The later are isotropic vectors, which are characteristic and natural over finite fields.

One aim of this brief discussion consists of showing that the development is all but linear and has its origin in the treatment of linear systems theory. Over the years, it spread out to a variety of disciplines in mathematics. Consequently, we arrive at the following arrangement of the Chapters.

Chapter 1 gives elements of algebra and number theory necessary for what follows and moreover supports those readers which not acquainted with these topics. Chapter 2 we have entitled as Algebraic Analysis, because the contents of definitions and investigation of in our sense transcendental functions is dominated by algebraic methods. First we treat complex functions and then come to the special case of real functions. The set-operation $\Delta x = 0$ mentioned above then yields a differential and integral calculus as we know from characteristic 0. The Sections on sequences and series as well as complex integration [20] are not published yet. In our case the division between real and complex analysis seems some what weaker, because it is more or less a matter of definition whether an even field is interpreted as real or complex.

Chapter 3 contains usual topics of linear algebra, i.e. vectors, matrices, linear systems of equations, eigenvalue problems, Jordan canonical form, and the derivation of the matrix exponential function and its inverse. The Chapter ends with a Section on tensor algebra and -analysis. It is noted that in the textbook literature there exist some examples for using instead of the fields $\mathbb{R}, \mathbb{C}$ in conjunction with vector spaces, more generally a $\mathbb{K}$-vector space is assumed. Usually this ends, if complex numbers for vectors and matrices come into play. Hence, our work gives a certain unification.

Chapter 4 deals with geometry, i.e. conic sections, balls, and n-balls and hyperboloids in the frame of Euclidean geometry, where we briefly also treat pseudo-Euclidean geometry. The Section on spinors gives an example for symplectic geometry. Within the Section on differential geometry we treat elementary theories of curves and surfaces. The last two Sections are not published yet [21], [22], too.

Chapter 5 contains classical Lie-groups and -algebras, Clifford algebras, and the Grassmann algebra and its application to differential forms.

Chapter 6 gives an application of finite fields to linear systems theory, where at the beginning of the Chapter we show briefly the corresponding theories in characteristic 0 in the continuum and time-discrete case for better comparison. In characteristic p we rely on the works of [Gössel] and [Wunsch], for which the idea of unification also plays a role. By transforming the system matrix of the state space equations to its Jordan canonical form, we obtain complete solution of the homogeneous and autonomous case. Moreover, we see close analogies to characteristic 0.

Finally, Chapter 7 deals with the formulation of elementary theories of physics, namely mechanics, electrodynamics, and quantum mechanics, all in the classical and special relativistic case.

Now we come to some general aspects of the book. In Chapter 1 to 6 we use throughout a mathematical oriented style, i.e. we give definitions, formulate theorems and prove them, which makes sense in view of the number of assertions as well as the number of terms to be introduced. In Chapter 7 we regret to do so, in physics it is not as pronounced. All Chapters are given uniformly in characteristic p. Discarding the new Sections with respect to the publications we have added numerous definitions, specifications, and supplements. Moreover, Chapters 2, 4, 6 contain a variety of figures, where we choose one out of $q!$ possible orderings of the numbers of finite fields. They are supposed to represent certain results in a more pictorial way, which for a skilled physicist may be allowed. In conjunction to some figures, we also give elementary graph theoretical interpretations.

In addition, Chapter 6 and 7 may be viewed as test cases: We intend to show that prominent and well known theories in characteristic may be *formulated* over finite fields. This does not say that for instance classical mechanics in characteristic p is physically useful. On the other hand, the Maxwell equations yield a reasoning for transversal waves, which per se could be an interesting object of investigation. Possibly, quantum mechanics over finite fields may have relations to quantum computing.

Finally we remark that the average size of a Chapter is about 70 pages. On the contrary, for each topic there exist textbooks with up to several hundred pages. From this sight we can not in a first step map all what we know in characteristic 0 to finite fields. One may also think of the fact that the huge area of differential equations here is almost neglected.

The preconditions for reading this book are little: With the fourth or fifth semester of a bachelor study in physics/mathematics the book may be read, lectures on analysis and linear algebra are elementary. A variety of things, like trigonometric functions are usually a matter of high school knowledge, but indeed one has to get used to our functions. The book is readable also by theoretical physicists or theoretically interested engineers.

At last I like to thank in chronological ordering: Thanks to Prof. Dr. D. Bochmann for encouraging me to publish the work [0] at the 4th International Workshop on Boolean Problems in 2000 and to continue this work further. Thanks to Prof. Dr. W. Borho for the idea, to employ the Jordan canonical form to resolve the structure of the solution of the homogeneous state equations in systems theory. He also suggested to generalize these works such that they are valid for all primes and prime powers. Finally, I thank Prof. Dr. B. Steinbach for his generosity, that I could present my work in a predominantly Boolean community. Also thanks to him for his question at the last workshop in 2012, if it would be possible to comprise all my works in a systematic manner. This is may be judged by the editor and the reader.

Braunschweig, Spring 2014

Wolf-Michael Wendler

Preface to the English Edition

This edition mainly is a translation into English as compared to the German edition, but has gained some pages too. These arise by including in Chapter 5 an additional Section 5 on elements of graph theory. This is felt adequate because in Chapter 7 on systems theory graph theoretical considerations are valuable with respect to the various state graphs given. Also this Section contains in Subsection 5.2 polyhedrons and in particular the planar graphs of the Platonic solids. We come to them in Chapter 6, Section 4. In addition we treat rudimentary in Subsection 5.3 elements of algebraic graph theory, which is used also in [Wendler_2] with respect to the hypercycles of M. Eigen.

Chapter 6 is new and is concerned with the orders of classical matrix Lie-groups. It is inserted such that the old Chapters 6, 7 now become Chapters 7 and 8. As preliminaries in Section 1 some supplements to groups are given, while in Section 2 the results for the number of points of balls and hyperboloids are generalized such that we are dealing now with m-dimensional balls and n-dimensional hyperboloids. Section 3 gives the order of the general linear group $\mathrm{GL}(n;\, \mathbb{F}(q))$, for which H. Weyl suggested the name “Her All-embracing Majesty” [Grove]. This Section also gives a reordering of the factors for the order, such that the formulae of the orders of the classical Lie-groups may be rewritten and reproved by using our results in Chapter 4, Subsection and Chapter 6, Section 2.

Section 4 of Chapter 6 contains the orders of the orthogonal groups $\mathrm{O}(n; \mathbb{F}(q))$ and $\mathrm{SO}(n; \mathbb{F}(q))$. In Subsection 4.2 the 3-dimensional case is investigated in particular over $\mathbb{F}(3)$. Thereby, we rediscover the octahedron group and its isomorphic counterpart, i.e. the group of the cube, as well as the tetrahedron subgroup. Platonic solids are tightly connected to quaternions, where the latter are investigated in Section 4, Chapter 5.

Section 5 treats the unitary groups $\mathrm{U}(n;\, \mathbb{F}(q))$ and $\mathrm{SU}(n;\, \mathbb{F}(q))$, where we investigate in Subsection 5.2 again the 3-dimensional case. Unitary matrices of format (3, 3), (4, 4) play an important role in elementary particle physics. Besides we resolve the little obstacle that $(3, 3)$-matrices must contain at least one zero entry, which is also the case for $(3, 3)$- rotation matrices over $\mathbb{F}(4)$ [Wendler_2], where we recovered the icosahedron group.

The last Section 6 contains the orders of the Euclidean group of motions $\mathrm{E}(n)$, the generalized orthogonal group $\mathrm{O}(m, n; \mathbb{F}(4))$, and the symplectic group $\mathrm{Sp}(2n; \mathbb{F}(q))$.

Of course as compared to the German edition there are a variety of minor changes, clarifications, and supplements. We wish to mention only one of them, because it gives a somewhat different sight and is found in the course of working out the book "Mathematics and Codons" [Wendler_2]: Despite the fact that we use linear state equations in the scope of systems theory in Chapter 7, their solutions show self-reproducing behaviour as well as period doubling, which both usually are obtained in characteristic 0 by non-linear equations. The reason lays in the fact that over finite fields the term non-linear is considerably different than in char 0. An example for powers of the elements of $\mathbb{F}(25)$ is given in Chapter 2, Subsection 1.1.

Braunschweig, Autumn 2020

Wolf-Michael Wendler

Contents