EMIL ARTIN
COLLECTED PAPERS

Emil Artin
Collected Papers

Edited
by
Serge Lang, Yale University
John T. Tate, Harvard University

Springer-Verlag
New York Heidelberg Berlin

Editors

Serge Lang
Yale University
Department of Mathematics
Box 2155 Yale Station
New Haven, CT 06520
U.S.A.

John T. Tate
Harvard University
Department of Mathematics
2 Divinity Avenue
Cambridge, MA 02138
U.S.A.

AMS Classification: 01A75

This is an unaltered reprint of the edition originally released in 1965 by Addison-Wesley Publishing Company, Inc.

Library of Congress Cataloging in Publication Data

Artin, Emil, 1898–1962.
The collected papers of Emil Artin.

English and German
Reprint. Originally published: Reading, Mass.: Addison-Wesley Pub. Co., 1965.
Bibliography: p.
Includes index.
1. Mathematics—Addresses, essays, lectures.
I. Lang, Serge, 1927– . II. Tate, John Torrence, 1925– . III. Title.
[QA7.A68 1982] 510 82-701

Printed in the United States of America

9 8 7 6 5 4 3 2 1

ISBN 0-387-90686-x Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90686-x Springer-Verlag Berlin Heidelberg New York

EMIL ARTIN
COLLECTED PAPERS

Hamburg, 1935

*This watercolor was made by
Stegemann in Hamburg in 1934.
Besides playing the flute
Artin also played various
keyboard instruments.*

The Orders of the Classical Simple Groups.

by Emil Artin.

We shall extend here the result of the previous paper „The Orders of the Linear Groups" (quoted by L) to all finite classical groups. The notion of classical groups is taken in such a wide sense as to embrace all finite simple groups which are known up to now.

The situation is the following: in his book „Linear Groups" L. Dickson studied the finite simple groups known up to 1901, gave proofs of their simplicity and investigated isomorphisms among them. In the last chapter he summarizes his results and gives a list of the numerical grouporders below a billion. In two subsequent papers he adds another system of simple groups, the analogues of the exceptional Lie group E_2 with 14 parameters. These investigations were taken up again by J. Dieudonné who greatly improved on Dicksons methods, simplified and extended his proofs and finally brought order into the discussion of the orthogonal groups where confusion was supreme. No new simple finite groups was found until quite recently when C. Chevalley succeeded in defining the analogues of the remaining exceptional Lie groups E_m and in proving their simplicity. I am greatly indebted to him for communicating to me the formulas for the orders of these new simple groups. In short we mean by classical the systems of alternating, linear, unitary, symplectic and orthogonal groups, the E_m and – for good measure – the 5 Mathieu groups.

First page of Artin's manuscript on simple groups.

Preface

Emil Artin was born on March 3, 1898 in Vienna. His father was an art dealer, and his mother was an opera singer. After his father died, his mother married again, and lived in Reichenberg, Bohemia, where Artin obtained his "Reifeprüfung" in 1916. After studying one semester at the University in Vienna, he was drafted and served in an infantry regiment until the end of the war. In January 1919 he continued his studies at the University of Leipzig. He studied there with Herglotz, towards whom he kept a heartfelt appreciation throughout his life. Herglotz was the only person whom Artin recognized as having been his "teacher." Artin got his PhD in 1921, spent one year at the University of Göttingen, and then went to Hamburg University. He became Privatdozent in 1923, Ausserordentlicher Professor in 1925, and Ordentlicher Professor in 1926 at the age of 28.

He married Natalie Jasny in 1929. They had three children, Karin, Michael, both born in Hamburg, and Thomas, born later in America, to which he emigrated in 1937. He spent one year at the University of Notre Dame, then was at Indiana University in Bloomington from 1938 to 1946, at which time he moved to Princeton, where he stayed from 1946 to 1958. He returned to Hamburg in 1958, and remained there until his death, of a heart attack, on December 20, 1962.

This volume includes all of Artin's papers.

It is not our intention to discuss Artin's mathematical works, but we thought it might be worth while to mention briefly some of his conjectures, not all of which were published.

The first one was, in effect, the Riemann hypothesis in function fields. In his thesis, Artin discussed hyperelliptic fields over finite constant fields as analogues of quadratic number fields, and pointed out that the analogue of the classical Riemann hypothesis seemed to be true for them. The proof was eventually given by Hasse for fields of genus 1 (Int. Congress, Oslo, 1936) and by Weil in the general case (*Comptes Rendus*, 1941).

A little later, he defined the non-abelian L-series, and conjectured their integrality, as well as a Riemann hypothesis for them. Both of these conjectures are still unproved, but it is interesting to note that Weil's methods allowed him to prove them in the function field case, and showed the close connection between the two (exhibiting them as two aspects of a more modification is the following. For each square-free integer $m > 0$, let

$$K_m = \prod_{q|m} K_q$$

be the compositum of the fields K_q for primes q dividing m, and let k_m be the absolute degree of K_m. Then the set of primes p such that the conditions $(*)$ are satisfied for no q dividing m has density

$$\rho(m) = \sum_{d|m} \frac{\mu(d)}{k_d},$$

where μ is the Moebius function, and the sum runs over the positive divisors d of m. Hence the conjecture should be that the set of primes p for which a is a primitive root has density

$$\rho = \lim_{m} \left(\sum_{d|m} \frac{\mu(d)}{k_d} \right)$$

where the limit is taken over all square-free m, ordered by divisibility.

To get a more explicit expression for ρ, one proves that if m is odd the fields K_q for $q|m$ are completely linearly disjoint. Consequently, for odd m, we have

$$k_m = \prod_{q|m} k_q,$$

and k_{2m} is equal to k_m or to $2k_m$, according as $\sqrt{a}$ is or is not contained in the field of m-th roots of unity. Let $a = a_0 b^2$ with a_0 square free. Then the condition for $\sqrt{a}$ to be contained in the field of m-th roots of unity for odd square-free m is that a_0 divide m and be congruent to 1 (mod 4). Putting all this together one finds that the conjectured density ρ of the set of primes p for which a is a primitive root is

$$\rho = A \cdot \prod_{q} \left(1 - \frac{1}{k_q}\right),$$

with

$$A = \begin{cases} 1 & \text{if } a_0 \not\equiv 1 \pmod 4, \\ 1 - \dfrac{\mu(a_0)}{\prod\limits_{q|a_0} (k_q - 1)} & \text{if } a_0 \equiv 1 \pmod 4, \end{cases}$$

where a_0 is the square-free part of a. Here k_q is the absolute degree of the splitting field of the polynomial $x^q - a$, and consequently $k_q = q(q-1)$ unless a is of the form $\pm c^n$ for some integer c and some integer $n > 1$.

It is interesting to note that the analogue of Artin's conjecture on primitive roots in function fields over finite fields has been proved by students of Hasse, using the Riemann hypothesis in function fields (cf. Hasse's discussion, *Annales Academiae Scientiarum Fennicae*, Helsinki 1952).

The editors and publisher wish to thank the following for permission to reprint the papers in this volume as listed below:

American Journal of Mathematics, Johns Hopkins Press
(Nos. 27, 28)
American Mathematical Society
(Nos. 12, 13, 45, 46)
American Scientist
(No. 39)
Annals of Mathematics
(Nos. 16, 26, 36, 37, 38)
Centre National des Recherches Scientifiques
(Nos. 14, 30)
Communications on Pure and Applied Mathematics
(Nos. 32, 33)
Walter de Gruyter & Co.
(Nos. 4, 9, 10, 11)
Interscience (John Wiley and Sons)
(No. 29)
Jahrbuch der Akademie der Wissenschaften, Göttingen
(No. 48)
Mathematical Society of Japan
(Nos. 17, 31)
Mathematisches Seminar, Universität Hamburg
(Nos. 3, 5, 6, 7, 8, 18, 19, 20, 21, 23, 24, 25, 34, 35, 40)
Nachrichten der Gesellschaft der Wissenschaften zu Göttingen
(No. 22)
National Academy of Science, U.S.A.
(Nos. 15, 42)
Notre Dame University Press
(Nos. 41, 43)
Springer-Verlag
(Nos. 1, 2)
Tata Institute of Fundamental Research
(No. 47)
University of Indiana Press
(No. 44)

Contents

This table of contents is also a bibliography of the collected papers. It is ordered according to topics, and is chronological within each division.

REAL FIELDS

ALGEBRA AND NUMBER THEORY

TOPOLOGY

MISCELLANEOUS

GENERAL

The following is a list of books and lecture notes not reproduced in this volume.

Einführung in die Theorie der Gammafunktion,
Hamburger mathematische Einzelschriften 1 Heft (1931)

Galois Theory,
Notre Dame Lectures (1942)

Galoische Theorie,
Leipzig (1959) (a translation and expansion of the preceding item)

Modern Higher Algebra, Galois Theory,
(Notes by A. Blank) Lectures, New York University (1947)

Rings with Minimum Condition (with C. J. Nesbitt and R. M. Thrall),
Michigan (1948)

Algebraic Numbers and Algebraic Functions (Notes by I. Adamson),
Princeton-New York University (1950)

Modern Developments in Algebra (Notes by R. Stoll),
Boulder summer conference (1953)

Selected Topics in Modern Algebra,
Summer conference at University of North Carolina (1954)

Elements of Algebraic Geometry (Notes by G. Bachman),
New York University (1955)

Calculus and Analytic Geometry (Notes by G. B. Seligman),
Princeton (1957)

Algebraic Number Theory (Notes by G. Wurges),
Göttingen (1956)

Geometric Algebra,
Interscience, New York (1957)

Class Field Theory (with J. T. Tate),
Harvard (1961)

Quadratische Körper im Gebiete der höheren Kongruenzen. I.

(Arithmetischer Teil.)

Von

E. Artin in Hamburg.

§ 1.
Einleitung.

Die Dedekindschen Untersuchungen über höhere Kongruenzen[1]) legen folgende Erweiterung der Theorie nahe.

Es werde dem Körper K der rationalen Funktionen modulo p die Funktion $\sqrt{D(t)}$ adjungiert, wo $D(t)$ eine ganze im Sinne Dedekinds quadratfreie Funktion des Parameters t ist. Der entstehende quadratische Körper $K(\sqrt{D(t)})$ weist dann ähnliche Eigenschaften auf wie ein quadratischer Zahlkörper.

So gilt zum Beispiel der Satz über eindeutige Zerlegbarkeit der Ideale in Primideale, der Satz von der Endlichkeit der Klassenzahl, die Sätze über die Einheiten.

Zur Klassenzahlformel gelangt man durch Einführung der Zetafunktionen. Hier läßt sich die Frage nach der Richtigkeit der Riemannschen Vermutung in jedem speziellen Fall entscheiden. Eine Durchrechnung der ersten Fälle — es handelt sich um zirka vierzig Körper — ergab stets die Richtigkeit der Riemannschen Vermutung. Einem allgemeinen Beweis ihrer Richtigkeit scheinen sich aber noch Schwierigkeiten ähnlicher Art wie beim Riemannschen $\zeta(s)$ entgegenzustellen, doch liegen die Verhältnisse hier insofern klarer und durchsichtiger, als es sich (im wesentlichen) um ganze rationale Funktionen handelt. Auf Fragen, die damit im Zusammenhang stehen, werde ich noch zurückkommen.

Von den sonstigen Eigenschaften unserer Zetafunktionen sei noch hervorgehoben: Sie besitzen eine einfache Funktionalgleichung, welche als

[1]) Journ. für die r. u. a. Math. **54** (1857), S, 1–26.

Folge merkwürdige Reziprozitätsbeziehungen gewisser Charaktersummen nach sich zieht. Ihre Nullstellen stehen in einfachem Zusammenhang mit den Wurzeln einer algebraischen Gleichung. wodurch eben die Entscheidung über die Riemannsche Vermutung gefällt werden kann.

Setzt man die Richtigkeit der Riemannschen Vermutung für alle Körper voraus, so läßt sich für alle p der Nachweis erbringen, daß es nur endlich viele imaginäre Körper mit einklassigen Geschlechtern gibt.

Endlich sei auch noch auf den Zusammenhang mit einer Arbeit von Kornblum[2]), der am Schlusse des zweiten Teils dieser Arbeit hergestellt wird, hingewiesen. Es gelingt dabei, das Kornblumsche Resultat über die Existenz unendlich vieler Primfunktionen in arithmetischen Progressionen wesentlich zu verschärfen.

Bemerkt sei noch, daß ich der kürzeren Bezeichnung halber einige im Gebiete der Zahlen verwendete Symbole sinngemäß auf die Funktionen (mod p) übertragen habe. Dies rechtfertigt sich auch schon dadurch, daß dann die Analogie unserer Resultate mit denen in Zahlkörpern deutlicher zutage tritt. Eine Verwechslung ist dabei wohl nicht zu befürchten, da die Symbole nur gemäß unserer Definition verwendet werden.

§ 2.

Erste Erweiterung des Rechengebietes.

Nach Dedekind heißen zwei Funktionen $F_1(t) = \sum_{\nu=0}^{n} a_\nu t^\nu$ und $F_2(t) = \sum_{\nu=0}^{n} b_\nu t^\nu$ kongruent modulo p, in Zeichen

$$F_1(t) \equiv F_2(t) \pmod{p},$$

wenn für alle ν gilt

$$a_\nu \equiv b_\nu \pmod{p}.$$

Dabei bedeutet p eine in den ganzen Entwicklungen festgehaltene Primzahl.

Wir wollen in diesem Falle die Funktionen und Zahlen direkt „gleich" nennen und also einfach schreiben

$$F_1(t) = F_2(t), \quad \text{wenn} \quad a_\nu = b_\nu.$$

Von Vielfachen von p ist hierbei eben abgesehen.

Ferner verstehen wir, wenn $a \neq 0$ (d. h. nach der vorigen Festsetzung $a \not\equiv 0 \pmod{p}$), unter $\frac{b}{a}$ eine Zahl x, für welche $ax = b$ ist (d. h. wieder $ax \equiv b \pmod{p}$). Zum Beispiel ist, wenn p ungerade, unter der häufig auftretenden Zahl $\frac{1}{2}$ die ganze Zahl $\frac{p+1}{2}$ zu verstehen.

---

[2]) Mathem. Zeitschr. **5** (1919), S. 100.

Nun lassen wir — und darin besteht unsere Erweiterung — auch negative Potenzen von t in endlicher oder unendlicher Anzahl zu. Wir betrachten also Funktionen der Form

$$F(t) = \sum_{\nu=-\infty}^{n} a_\nu t^\nu = a_n t^n + a_{n-1} t^{n-1} + \dots \qquad (n \gtreqless 0),$$

wobei wieder zwei Funktionen „gleich" sein sollen, wenn die Koeffizienten entsprechender t-Potenzen „gleich" sind.

Man beachte, daß dem Buchstaben t keinerlei numerische Bedeutung zukommt, und er lediglich als Rechensymbol zu betrachten ist, so daß im Falle unendlich vieler negativer Potenzen von t der Konvergenzfrage keinerlei Bedeutung zukommt. Da er ferner im allgemeinen derselbe bleibt, unterdrücken wir künftighin seine Bezeichnung, schreiben also kurz

$$F \quad \text{statt} \quad F(t).$$

Zahlen mögen stets mit kleinen lateinischen Buchstaben und den allgemein üblichen Summationsbuchstaben μ, ν bezeichnet werden, alle übrigen Buchstaben seien den Funktionen vorbehalten.

Sei nun $F = \sum_{\nu=-\infty}^{n} a_\nu t^\nu$, wobei $a_n \neq 0$ vorausgesetzt sei.

F heiße ganz, wenn die Koeffizienten aller negativen Potenzen von t verschwinden, wenn es also eine Funktion im Dedekindschen Sinne ist.

Ferner heiße für ganzes und nicht ganzes F:

1. Wie bei Dedekind, n der Grad von F.

2. Die Zahl p^n der „Betrag" $|F| = p^n$ von F. Diese Bezeichnung wird sich in der Folge rechtfertigen. Für jetzt sei nur bemerkt, daß im Falle eines ganzen F die Zahl $p^n = |F|$ die Anzahl der Restklassen der ganzen Funktionen modulo F ist. In der Dedekindschen Bezeichnung (modd $p, F(t)$). Für von Null verschiedene Zahlen a gilt dann $|a| = 1$. Ferner werde $|0| = 0$ gesetzt.

3. Der Koeffizient a_n der höchsten Potenz von t, der schon bei Dedekind die Rolle des „Vorzeichens" von F spielt, werde mit

$$a_n = \operatorname{sgn} F$$

bezeichnet. Diese Definition hat natürlich nur einen Sinn, wenn $F \neq 0$ ist, d. h. wenn es nichtverschwindende Koeffizienten überhaupt gibt. Dann ist $\operatorname{sgn} F \neq 0$.

4. Mit Dedekind nennen wir die von Null verschiedenen Zahlen $1, 2, \dots, (p-1)$ die rationalen Einheiten, da sie in *unserem* Sinne *Teiler* der Eins sind.

5. Wenn $\operatorname{sgn} F = 1$ ist, heiße F primär. (Es entspricht dies ungefähr den positiven Zahlen.)