Number Theory in Progress

Andrzej Schnzel

# Number Theory in Progress

Proceedings of the International Conference
on Number Theory organized by the
Stefan Banach International Mathematical Center
in Honor of the 60th Birthday of Andrzej Schinzel
Zakopane, Poland, June 30–July 9, 1997


## Volume 1
## Diophantine Problems and Polynomials

*Editors*

Kálmán Győry
Henryk Iwaniec
Jerzy Urbanowicz


Walter de Gruyter · Berlin · New York 1999

*Editors*

K. Győry
Institute of Mathematics
and Informatics
Lajos Kossuth University
4010 Debrecen, Hungary

H. Iwaniec
Department of Mathematics
Rutgers University
New Brunswick, NJ 08903-2101
USA

J. Urbanowicz
Institute of Mathematics
Polish Academy of Sciences
P.O. Box 137
00-950 Warszawa
Poland

*1991 Mathematics Subject Classification:*
11-02, 11-06, 11Axx, 11Bxx, 11Cxx, 11Dxx, 11Exx, 11Fxx, 11Gxx, 11Hxx, 11Jxx, 11Kxx, 11Lxx, 11Mxx, 11Nxx, 11Pxx, 11Rxx, 11Sxx, 11Txx, 11Yxx, 14Gxx, 14Hxx, 14Jxx, 20Bxx, 30Dxx, 32Axx, 33Exx, 40Gxx, 52Cxx, 60Cxx

*Keywords:*
*abc*-conjecture, arithmetic algebraic geometry, automorphic forms, Baker's method, computational number theory, diophantine equations and inequalities, diophantine approximation, elliptic curves, estimates of exponential and character sums, Hecke operators, $L$-functions and zeta functions, lattices and convex bodies, linear independence, Mahler's measure, Pisot and Salem numbers, polynomials, quadratic forms, sequences and sets, Schinzel's hypothesis, sieves and their applications, spectral theory, transcendental numbers

♾ Printed on acid-free paper which falls within the guidelines of the ANSI to ensure permanence and durability.

*Library of Congress – Cataloging-in-Publication-Data*

International Conference on Number Theory (1997 : Zakopane, Poland)
Number theory in progress : proceedings of the International Conference on Number Theory organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Zakopane, Poland, June 30–July 9, 1997 / editors, Kálmán Győry, Henryk Iwaniec, Jerzy Urbanowicz.
p. cm.
Contents:
v. 1. Diophantine problems and polynomials –
v. 2. Elementary and analytic number theory.
ISBN 3-11-015715-2 (set : acid-free paper)
1. Number theory – Congresses. I. Schinzel, Andrzej. II. Győry, Kálmán. III. Iwaniec, Henryk. IV. Urbanowicz, Jerzy. V. Title
QA241.I584 1997
512'.7–dc21 99-19358
CIP

*Die Deutsche Bibliothek – Cataloging-in-Publication-Data*

**Number theory in progress** : proceedings of the International Conference on Number Theory organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Zakopane, Poland, June 30–July 9, 1997 / ed. Kálmán Győry ... – Berlin ; New York : de Gruyter
ISBN 3-11-015715-2
Vol. 1. Diophantine problems and polynomials. – 1999


Typeset using the authors' TEX files: I. Zimmermann, Freiburg. Printing: WB-Druck GmbH & Co., Rieden/Allgäu. Binding: Lüderitz & Bauer, Berlin. Cover design: Thomas Bonnie, Hamburg.

# Preface

These are the Proceedings of the International Conference on Number Theory held in Zakopane-Kościelisko, Poland, from June 30 to July 9, 1997. The conference was organized by the Stefan Banach International Mathematical Center to celebrate the 60th birthday of Professor Andrzej Schinzel.

Andrzej Schinzel is the editor-in-chief of *Acta Arithmetica*—the first international journal devoted exclusively to number theory—for over 28 years. He is also well known for many original results in various areas of number theory appearing in nearly 200 research papers. His main contributions are described in the article of Władysław Narkiewicz in these Proceedings.

About 130 mathematicians from 21 countries attended the conference. The focus of the meeting was twofold: Diophantine Problems and Polynomials, and Elementary and Analytic Number Theory. Bogdan Bojarski, Director of the Institute of Mathematics of the Polish Academy of Sciences opened the conference with an address to the participants, and Władysław Narkiewicz delivered the opening lecture on selected works of Andrzej Schinzel. The scientific program was supplemented by a banquet and a one-day excursion, to Cracow, the former capital of Poland. After the excursion, Andrzej Schinzel presented a requested lecture on the history of Poland—a subject which is close to his heart.

The Proceedings contain 71 selected, refereed research and survey papers by conference speakers and a few invited mathematicians who were unable to come to the conference. The material is divided into two volumes according to the conference subjects. The articles of the first volume are concerned with diophantine problems and polynomials (diophantine equations, diophantine approximation, transcendental number theory and polynomials). The second volume contains the papers related to elementary and analytic number theory (sieve methods, modular and automorphic forms, Hecke operators, estimates on exponential and character sums, zeta functions and $L$-functions). A noteworthy feature of these volumes is the large number of papers written by leading mathematicians. Most of the contributions are in English while a few are in French. We thank all the authors and referees for all their contributions to the Proceedings.

Many people helped in the organization of the conference or in the editing of the Proceedings. Special thanks are due to Bogdan Bojarski for his guidance and help. We also thank Robert Tijdeman, who played an important role from the initial planning of the conference to the publication of the Proceedings. We thank Lajos Hajdu and Jan K. Kowalski for their efficient secretarial assistance. Special thanks go to Jan K. Kowalski, who looked through the manuscripts, made corrections, and offered valuable suggestions for improving the presentation. The staff of Walter de Gruyter & Co., especially Manfred Karbe, deserve our thanks for an excellent co-operation.

We gratefully acknowledge the support of our sponsors: the Stefan Banach Center, the State Committee for Scientific Research of Poland (KBN), the Department of Defense of the Polish government, the Foundation for Polish-German Coopera-

tion, the Max-Planck-Institut für Mathematik in Bonn, Germany, and the Stefan Batory Foundation.

The organizers want to thank Don Zagier, Director of the Max-Planck-Institut, our first sponsor, for his help and friendly interest. The wonderful blackboards and some electronic equipment, purchased partially from money received from the Max-Planck-Institut, were passed on as a gift to the Mathematical Conference Center in Będlewo, Poland.

September, 1998

*Kálmán Győry*
*Henryk Iwaniec*
*Jerzy Urbanowicz*

# List of participants

Scott Ahlgren, Denison University, Granville, USA

Francesco Amoroso, University of Torino, Italy

Johan Andersson, Stockholm University, Sweden

Alan Baker, University of Cambridge, United Kingdom

Antal Balog, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary

Grzegorz Banaszak, Adam Mickiewicz University, Poznań, Poland

Bruce Berndt, University of Illinois at Urbana-Champaign, USA

Vasily Bernik, Institute of Mathematics, Academy of Sciences of Belarus, Minsk, Belarus

Marie José Bertin, Université Pierre et Marie Curie, Paris, France

Frits Beukers, University of Utrecht, The Netherlands

Yuri Bilu, ETH Zürich, Switzerland

Bryan J. Birch, Oxford University, United Kingdom

David W. Boyd, University of British Columbia, Vancouver, Canada

Béla Brindza, Kossuth Lajos University, Debrecen, Hungary

Jerzy Browkin, Warsaw University, Poland

W. Dale Brownawell, Penn State University, USA

Joerg Brüdern, Universität Stuttgart, Germany

Roelof W. Bruggeman, University of Utrecht, The Netherlands

V. A. Bykovsky, Russian Academy of Sciences, Far Eastern Branch, Khabarovsk, Russia

Mark Coleman, UMIST, Manchester, United Kingdom

Jean-Louis Colliot-Thélène, Université de Paris-Sud, France

Giovanni Coppola, DIIMA, Università degli Studi di Salerno, Italy

Daniel Coray, University of Geneva, Switzerland

Jean-Marc Couveignes, Université de Bordeaux, France

Alfred Czogała, Silesian University, Katowice, Poland

Andrzej Dąbrowski, University of Szczecin, Poland

Pierre Dèbes, Université Lille, France

Hubert Delange, University of Paris 11, France

Ulrich Dieter, Technische Universität Graz, Austria

Edward Dobrowolski, College of New Caledonia, Prince George, Canada

Arturas Dubickas, Vilnius University, Lithuania

E. H. Dubois, Université de Basse-Normandie, Caen, France

William D. Duke, Rutgers University, New Brunswick, USA

Roberto Dvornicich, Università di Pisa, Italy
Peter D. T. A. Elliott, University of Colorado at Boulder, USA
Jan-Hendrik Evertse, University of Leiden, The Netherlands
Michael Filaseta, University of South Carolina, USA
Kevin Ford, University of Texas at Austin, USA
Etienne Fouvry, Université de Paris-Sud, France
Gregory A. Freiman, Tel Aviv University, Israel
Michael D. Fried, University of California, Irvine, USA
J. B. Friedlander, University of Toronto, Canada
Dorian Goldfeld, Columbia University, USA
Peter J. Grabner, Technische Universität Graz, Austria
George Greaves, University of Wales, Cardiff, United Kingdom
Kálmán Győry, Kossuth Lajos University, Debrecen, Hungary
Lajos Hajdu, Kossuth Lajos University, Debrecen, Hungary
Gabor Halász, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary
Heini Halberstam, University of Illinois at Urbana-Champaign, USA
Franz Halter-Koch, Universität Graz, Austria
Adolf Hildebrand, University of Illinois at Urbana-Champaign, USA
Jürgen Hurrelbrink, Louisiana State University, USA
Martin N. Huxley, University of Wales, Cardiff, United Kingdom
Henryk Iwaniec, Rutgers University, New Brunswick, USA
Anna Iwaszkiewicz-Rudoszańska, Adam Mickiewicz University, Poznań, Poland
Stanislav Jakubec, Institute of Mathematics, Slovak Academy of Sciences, Bratislava, Slovakia
Jerzy Kaczorowski, Adam Mickiewicz University, Poznań, Poland
Przemysław Kamiński, Adam Mickiewicz University, Poznań, Poland
Takeshi Kano, Yamagata University, Japan
Winfried Kohnen, Universität Heidelberg, Germany
Sergei Konyagin, Moscow State University, Russia
Katalin Pappne Kovacs, Eötvös University, Budapest, Hungary
Emmanuel Kowalski, Rutgers University, New Brunswick, USA
Jonas Kubilius, Vilnius University, Lithuania
Mieczysław Kulas, Adam Mickiewicz University, Poznań, Poland
Michel Langevin, Université de Bordeaux, France
Don J. Lewis, National Science Foundation, USA
John B. Lewis, Framingham State College, USA
Andrzej Mąkowski, Warsaw University, Poland
Eugenijus Manstavičius, Vilnius University, Lithuania

David Masser, University of Basel, Switzerland
Michel Mendès France, Université Bordeaux I, France
Philippe Michel, Université de Paris-Sud, France
Maurice Mignotte, Université Louis Pasteur, Strasbourg, France
Pieter Moree, Max-Planck-Institut für Mathematik, Bonn, Germany
Yoichi Motohashi, Nihon University, Japan
Władysław Narkiewicz, Wrocław University, Poland
Yu. Nesterenko, Moscow State University, Russia
Jean-Louis Nicolas, Université Claude Bernard, Villeurbanne, France
Harald Niederreiter, Austrian Academy of Sciences, Vienna, Austria
Werner Georg Nowak, Universität für Bodenkultur, Vienna, Austria
Andrew Odlyzko, AT&T Labs – Research, USA
Ken Ono, Penn State University, USA
Aleksander Pełczyński, Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland
Alberto Perelli, Università di Genova, Italy
Robert Perlis, Louisiana State University, USA
Patrice Philippon, CNRS, Paris, France
János Pintz, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary
Andrew D. Pollington, Brigham Young University, USA, and Imperial College, London, United Kingdom
Carl Pomerance, University of Georgia, USA
Jacek Pomykała, Warsaw University, Poland
Štefan Porubský, Institute of Chemical Technology, Prague, Czech Republic
Maciej Radziejewski, Adam Mickiewicz University, Poznań, Poland
Piotr Rejmenciak, Adam Mickiewicz University, Poznań, Poland
Szilard Révész, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary
Georges Rhin, Université de Metz, France
Paulo Ribenboim, Queen's University, Kingston, Ontario, Canada
Herman te Riele, Centre for Mathematics and Computer Science (CWI), Amsterdam, The Netherlands
Andrzej Rotkiewicz, Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland
Michael Rubinstein, Princeton University, USA
Zeév Rudnick, Tel Aviv University, Israel
Imre Z. Ruzsa, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary
András Sárközy, Eötvös Lorand University, Budapest, Hungary

Andrzej Schinzel, Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland

Hans Peter Schlickewei, Universität Marburg, Germany

Wolfgang M. Schmidt, University of Colorado, USA

Wolfgang Schwarz, University of Frankfurt, Germany

Hakim Smati, Université de Limoges, France

Chris Smyth, Edinburgh University, United Kingdom

Lawrence Somer, Catholic University of America, Washington, USA

Vera Sós, Mathematical Institute, Hungarian Academy of Sciences, Budapest, Hungary

Cameron L. Stewart, University of Waterloo, Canada

Leo Summerer, University of Vienna, Austria

Peter Swinnerton-Dyer, Isaac Newton Institute, Cambridge University, United Kingdom

Janusz Szmidt, Military University of Technology, Warsaw, Poland

Bogdan Szydło, Adam Mickiewicz University, Poznań, Poland

Kazimierz Szymiczek, Silesian University, Katowice, Poland

Jörg Maximilian Thuswaldner, Montanuniversität Leoben, Austria

Robert F. Tichy, Technische Universität Graz, Austria

Robert Tijdeman, University of Leiden, The Netherlands

Gerhard Turnwald, University of Tübingen, Germany

Yoichi Uetake, Adam Mickiewicz University, Poznań, Poland

Jerzy Urbanowicz, Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland

Jeffrey D. Vaaler, The University of Texas at Austin, USA

Carlo Viola, Università di Pisa, Italy

Michel Waldschmidt, Université Pierre et Marie Curie, Paris, France

Gary Walsh, University of Ottawa, Canada

Eduard Wirsing, Universität Ulm, Germany

Kunrui Yu, Hong Kong University of Science and Technology, Hong Kong / China

Don Zagier, Max-Planck-Institut für Mathematik, Bonn, Germany

Umberto Zannier, Istituto Universitario di Architettura, Venezia, Italy

Tao Zhan, Shandong University, Jinan, China

# Table of contents of Volume I

# Table of contents of Volume II

# Quelques nouveaux résultats sur les nombres de Pisot et de Salem

*M.J. Bertin*

*Au Professeur Schinzel, pour son soixantième anniversaire*

**Résumé.** Après un court historique sur le problème de Lehmer, nous montrons l'importance de la répartition des conjugués d'un entier algébrique pour l'évaluation de sa mesure de Mahler.

Les nombres de Pisot et de Salem apparaissent déjà dans le célèbre article de D.H. Lehmer (1933) [Le].

Motivé par la recherche de grands nombres premiers à partir des quantités $\Delta_n(P) = \prod_{i=1}^{r} (\alpha_i^n - 1)$ où $P$ est un polynôme unitaire, irréductible, à coefficients entiers rationnels possédant les racines $\alpha_1, \ldots, \alpha_r$, Lehmer observa que pour obtenir sans trop de calculs de très grands nombres premiers, les quantités $\frac{\Delta_{n+1}(P)}{\Delta_n(P)}$ ne devaient pas croître trop vite.

Or si $P$ ne possède pas de racine de module 1, on déduit aisément que

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(P)}{\Delta_n(P)} \right| = \prod_{i=1}^{r} \max(|\alpha_i|, 1) = M(P),$$

où $M(P)$ désigne la mesure de Mahler du polynôme unitaire $P$.

Lehmer s'intéressa d'abord aux mesures de Mahler des polynômes unitaires irréductibles non réciproques.

Il montra que:

en degré 1, celui de plus petite mesure est $X - 2$ de mesure 2;
en degré 2, celui de plus petite mesure est $X^2 - X - 1$ de mesure $\frac{1+\sqrt{5}}{2}$;
en degré 3, celui de plus petite mesure est $X^3 - X - 1$ de mesure 1,3247...;
en degré 4, celui de plus petite mesure est $X^4 - X - 1$ de mesure 1,38027...

Faute d'outils de calcul et parce que les plus petites mesures obtenues jusqu'au degré 4 étaient obtenues avec des trinômes, Lehmer se contenta d'étudier les trinômes en degré 5, 6 et 7.

Il obtint pour plus petites mesures de Mahler:

en degré 5, le polynôme $X^5 - X^3 - 1$ de mesure 1,3625...;

en degré 6, le polynôme $X^6 - X - 1$ de mesure 1,3707...;
en degré 7, le polynôme $X^7 - X^3 - 1$ de mesure 1,3797...

Observons que jusqu'au degré 4 les polynômes cités ne possèdent qu'une seule racine $\theta$, $\theta > 1$, extérieure au disque unité.

Cette racine $\theta$ *est un nombre de Pisot* (on trouve aussi dans la littérature P–V nombre, P pour Pisot et V pour Vijayaraghavan [V] qui étudia également ces nombres).

*Un nombre de Pisot est donc un entier algébrique $\theta$, $\theta > 1$, dont tous les autres conjugués ont un module strictement inférieur à 1. L'ensemble des nombres de Pisot est noté $S$.*

Observons également que vers les années 1960, les résultats suivants furent obtenus:

$$2 = \inf S'', \quad \frac{1+\sqrt{5}}{2} = \inf S', \quad \theta_0 = 1{,}3247\ldots = \inf S.$$

$\theta_1 = 1{,}38027\ldots$ est le deuxième plus petit nombre de Pisot [G], [D-P 1, 2, 3]. (L'ensemble $S'$ désigne l'ensemble dérivé de l'ensemble $S$).

Lehmer observa encore que les polynômes réciproques non cyclotomiques de plus petite mesure sont ceux qui possèdent toutes leurs racines sauf 2 sur le cercle unité. Ces entiers algébriques deviendront vite célèbres: ce sont les nombres de Salem. Leur ensemble est noté $T$.

*Un nombre de Salem est donc un entier algébrique $\tau$, $\tau > 1$, dont tous les autres conjugués ont un module inférieur ou égal à 1, avec effectivement des conjugués de module 1.*

Lehmer donna les plus petites mesures pour les polynômes réciproques par degré croissant:

$X^2 - 3X + 1$ de mesure 2,618...;
$X^4 - X^3 - X^2 - X + 1$ de mesure 1,7220...;
$X^6 - X^4 - X^3 - X^2 + 1$ de mesure 1,4012...;
$X^8 - X^5 - X^4 - X^3 + 1$ de mesure 1,2806...

Ces trois dernières mesures sont les plus petits nombres de Salem de degré 4, 6, 8 respectivement. On le vérifie aisément dans les tables de Boyd [Bo 2] (1980).

En degré 10, Lehmer avoua n'avoir pu tout examiner mais donna sa meilleure mesure obtenue, 1,1762... Ce nombre est l'unique racine de module supérieur à 1 du polynôme:

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

Ce nombre est appelé aujourd'hui *nombre de Lehmer.*

*Alors, tout naturellement, Lehmer posa la question suivante: existe-t-il des polynômes unitaires, irréductibles, à coefficients entiers de mesure inférieure à* 1,1762...?

C'est la fameuse question de Lehmer que certains auteurs tournent parfois en conjecture de Lehmer ou généralisent à diverses situations.

En dépit de toutes les investigations de nombreux mathématiciens, ce nombre demeure toujours le plus petit nombre de Salem connu et sa mesure, qui est le nombre lui-même, la plus petite mesure de Mahler actuellement connue.

Remarquons maintenant la répartition des conjugués dans $\mathbb{C}$ du plus petit nombre de Pisot $\theta_0 = 1{,}32\ldots$ ainsi que du plus petit nombre de Salem connu $\tau_0 = 1{,}1762\ldots$

Le nombre $\theta_0$ a deux conjugués de module $\frac{1}{\sqrt{\theta_0}}$ et d'arguments $\pm 139°67$.

Le nombre $\tau_0$ possède un conjugué $\frac{1}{\tau_0}$ et ses autres conjugués de module 1 et d'arguments $\pm 62°8, \pm 106°9, \pm 137°2, \pm 160°6$.

Pourquoi regarder aussi attentivement les conjugués de ces nombres?

Au début de leur étude, lors de la thèse de Pisot [P] et dans les quelques 30 ans qui suivirent, on s'intéressait essentiellement au nombre lui-même, c'est-à-dire aux propriétés du plus grand des conjugués $\theta$ ou $\tau$.

Il y a d'ailleurs des résultats célèbres:

*$S$ est un ensemble fermé pour la topologie de* $\mathbb{R}$ (Salem [S 1] (1944));

*$S$ est contenu dans l'ensemble dérivé $T'$ des nombres de Salem* (Salem [S 2] (1945));

*$M(\alpha) \geq \theta_0 = 1{,}32\ldots = \inf S$ si $\alpha$ est un entier algébrique non réciproque* (Smyth [Sm] (1970));

*tout nombre de Salem peut être obtenu à partir d'un nombre de Pisot par la construction de Salem* (Boyd [Bo 1] (1977)).

Cependant, si l'on s'intéresse à la question de Lehmer, la répartition des conjugués est très importante. J'en veux pour preuve deux résultats.

Le premier est un résultat de Zagier (1993) [Za]:

*Tout nombre algébrique $\alpha$, de degré $d$, $\alpha \neq 0$, $\alpha \neq 1$, $\alpha \neq (1+\sqrt{-3})/2$, vérifie l'inégalité*:

$$M(\alpha)M(\alpha-1) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}.$$

Une telle formule renseigne sur la localisation des zéros des entiers algébriques de petite mesure.

Par exemple, on déduit du résultat de Zagier qu'un nombre de Pisot $\alpha$ de degré 3, de mesure inférieure à 2, a ses conjugués de module inférieur à 1 à l'extérieur du cercle de centre 1 et de rayon 1.

Parmi ces nombres, il y a le plus petit nombre de Pisot $\theta_0 = 1{,}32\ldots$ racine de l'équation $X^3 - X - 1 = 0$ ainsi que le quatrième plus petit nombre de Pisot $\theta = 1{,}46557\ldots$ racine de l'équation $X^3 - X^2 - 1$ dont les autres conjugués ont pour module $\frac{1}{\sqrt{\theta}}$ et argument $\pm 106°, 36$.

On déduit également du résultat de Zagier qu'il n'existe pas de nombre de Salem $\tau \leq 2$ dont les conjugués de module 1 aient un argument $\leq \frac{\pi}{3}$ en module. En outre, pour $\tau > 2$, on a $\tau \geq C(d)$, la constante $C(d)$ dépendant du degré $d$ de $\tau$ et tendant vers l'infini lorsque $d$ tend vers l'infini.

Ces exemples montrent que la répartition des conjugués et donc la trace et la norme de l'entier algébrique ont une influence sur la mesure.

C'est le deuxième résultat évoqué précédemment, le résultat de Matveev, qui m'a permis de concrétiser cette remarque.

Citons d'abord le résultat de Matveev [M].

Soit $K$ un corps de nombres de degré $d$. Notons $K^{(\sigma)}$ les corps conjugués de $K$ sur $\mathbb{C}$. Il leur correspond les valeurs absolues archimédiennes normalisées, $|\alpha|_\sigma = |\alpha^{(\sigma)}|$, $1 \leq \sigma \leq d$, $\alpha \in K^*$, tous les plongements étant considérés, bien que deux plongements complexes conjugués définissent la même valeur absolue.

Désignons les idéaux premiers de $K$ avec des indices $\sigma$, $\sigma > d$. Il leur correspond des valeurs absolues non archimédiennes $|\alpha|_\sigma = N(\mathcal{P})^{-m}$, $\mathcal{P} = \mathcal{P}_\sigma$, $\sigma > d$, $m$ étant l'exposant de $\mathcal{P}$ dans la décomposition en idéaux premiers de l'idéal $(\alpha)$.

Nous avons alors pour $\alpha \neq 0$ la formule du produit $\prod_\sigma |\alpha|_\sigma = 1$, où seulement un nombre fini de facteurs diffère de 1.

Notons $\mathcal{D} = \mathcal{D}(K)$ l'ensemble $\{1, 2, \ldots, d\}$ et choisissons un sous-ensemble $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{D}$ et pour tout $\sigma \in \mathcal{S}$, une détermination de $\ln \alpha^{(\sigma)}$.

Définissons

$$\mu = \mu(\alpha, \mathcal{S}) = (1/2) \sum_{\sigma \notin \mathcal{S}} \left| \ln |\alpha|_\sigma \right|, \quad \lambda = \lambda(\alpha, \mathcal{S}) = (1/S) \sum_{\sigma \in \mathcal{S}} \left| \ln \alpha^{(\sigma)} \right|,$$

où $S = \mathrm{Card}(\mathcal{S})$.

**Théorème 0.** *Avec les notations précédentes, on a, pour $\alpha \neq 1$, l'inégalité*

$$\mathrm{sh}(\lambda/2) \geq \exp(-(d \ln 2 + \mu)/S).$$

**Corollaire 0.** *Avec les notations du théorème, il en résulte l'inégalité*

$$\lambda \geq (2 \ln \beta) \exp(-(d \ln 2 + \mu)/S),$$

*où $\beta = (3 + \sqrt{5})/2$ est le carré du nombre d'or.*

Avant de donner nos résultats, rappelons également la célèbre inégalité de Schinzel [Sc] (1973) :

$$M(\alpha) \geq \left( \frac{1 + \sqrt{5}}{2} \right)^{d/2}$$

*si $\alpha$ est un entier algébrique totalement réel.*

**Théorème 1** [Be 3]. *Soit $\theta$ un entier algébrique totalement réel de degré $d$, de norme $N(\theta)$. Si $\theta$ est totalement positif, on a :*

$$M(\theta) \geq \mathrm{Max} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^d, \sqrt{N(\theta)} \left( \frac{1 + \sqrt{5}}{2} \right)^{d/N(\theta)^{1/2d}} \right).$$

*Sinon,*

$$M(\theta) \geq \mathrm{Max} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^{d/2}, \sqrt{|N(\theta)|} \left( \frac{1 + \sqrt{5}}{2} \right)^{d/2|N(\theta)|^{1/d}} \right).$$

Nous allons maintenant étudier une classe particulière d'entiers algébriques.

Désignons par $\Theta_\nu$ l'ensemble des entiers algébriques réciproques $\theta$ ayant au moins un conjugué de module 1 et les $2\nu$ conjugués de module différent de 1 réels.

Le théorème suivant montre que certaines classes de nombres de $\Theta_\nu$ se comportent presque comme des entiers algébriques réciproques totalement réels.

**Théorème 2.** *On considère l'ensemble des $\theta \in \Theta_\nu$ de degré $2d$ tels que $d/\nu$ tende vers $\gamma \geq 1$ lorsque $d$ tend vers $+\infty$. Soit $X_0$ la racine supérieure à 1 de l'équation*

$$X^2 - (2 + 2^{-2(\gamma-1)})X + 1 = 0.$$

*Alors, pour tout $\varepsilon > 0$, il existe un entier $d_0$ tel que pour tout $d$, $d \geq d_0$, l'on ait*

$$\inf_{\deg \theta = d} M(\theta) \geq X_0^{\nu(1-\varepsilon)/2}.$$

*Si $\gamma = 1$, on retrouve asymptotiquement le résultat de Schinzel.*

*Preuve.* On peut supposer $\theta \in \Theta_\nu$ totalement positif.

Considérons $K = \mathbb{Q}(\theta)$ et prenons pour $\mathcal{S}$ l'ensemble des valeurs absolues archimédiennes de $K$ sauf celles correspondant aux conjugués de module 1. On a donc $S = 2\nu$, $\mu = 0$, $\lambda = (1/\nu) \ln M(\theta)$.

La fonction $(1/\lambda)\,\mathrm{sh}(\lambda/2)$ étant décroissante, si $\lambda \leq \ln X_0$, alors

$$(1/\lambda)\,\mathrm{sh}(\lambda/2) \leq 2^{-\gamma}/\ln X_0,$$

d'où l'inégalité. □

Les nombres de Salem sont très loin de vérifier la condition du théorème 2. Cependant, on peut déduire pour eux un résultat sur la répartition sur le cercle unité de leurs conjugués de module 1.

**Théorème 3.** *Soit $\tau$ un nombre de Salem de degré $2d$. Soient $\theta_1, \ldots, \theta_{d-1}$ les arguments des conjugués de module 1 de $\tau$ compris entre 0 et $\pi$. Alors si $\beta = (3 + \sqrt{5})/2$, on a l'inégalité suivante*

$$\frac{1}{d-1} \sum_{i=1}^{d-1} \theta_i \geq (2 \ln \beta) \exp\left( - \frac{2d \ln 2 + \ln \tau}{2(d-1)} \right).$$

*En particulier, si $\tau$ appartient à l'ensemble des nombres de Salem inférieurs à 1,3 on a pour $d$ assez grand,*

$$\frac{1}{d-1} \sum_{i=1}^{d-1} \theta_i \geq 0{,}96.$$

*Preuve.* Si $K = \mathbb{Q}(\tau)$, $\mathcal{S} = \mathcal{D} - \{1, \sigma\}$ où $\sigma(\tau) = 1/\tau$, alors $\mu = ln\tau$, $S = 2(d-1)$, $\lambda = \frac{1}{d-1} \sum_{i=1}^{d-1} \theta_i$. L'inégalité résulte alors du corollaire 0. □

**Remarque.** Ce type de résultats est à rapprocher des résultats de Bertin–Boyd [B-B 1, 2].

*Nous pouvons maintenant expliquer pourquoi les conjugués extérieurs au cercle unité des entiers algébriques réciproques de petite mesure sont autant que possible imaginaires.*

**Définition.** On appelle $\nu$-Salem un entier algébrique réciproque ayant $\nu$ conjugués extérieur au cercle unité et au moins un conjugué de module 1. Nous dirons que le $\nu$-Salem est *totalement réel* si ses conjugués extérieurs au cercle unité sont tous réels.

On déduit alors directement du corollaire 0 le théorème suivant.

**Théorème 4.** *La mesure de Mahler d'un $\nu$-Salem $\theta$ de degré $2\nu+2k$, totalement réel, vérifie l'inégalité*

$$M(\theta) \geq ((1+\sqrt{5})/2)^{\nu/2^{k/\nu}} = C(\nu,k).$$

*Les $\nu$-Salem totalement positifs, en particulier les nombres de Salem qui sont des 1-Salem, vérifient*

$$M(\theta) \geq (C(\nu,k))^2.$$

**Corollaire.**

(1) *Un nombre de Salem de degré* 4 *est supérieur à* 1,618033... *Le plus petit d'entre eux est donné par la table de Boyd et vaut* 1,722683...

(2) *Un* 2*-Salem de degré* 6*, de mesure inférieure à* 1,9749... *est totalement imaginaire. Le seul* 2*-Salem de mesure inférieure à* 2 *est de mesure* 1,9962... *et est encore totalement imaginaire.*

(3) *Un* 2*-Salem de degré* 8*, de mesure inférieure à* 1,618033... *est totalement imaginaire et tous ceux de mesure inférieure à* 2 *sont ou bien totalement imaginaires ou bien ont leurs conjugués extérieurs au cercle unité de signes contraires.*
*Le seul* 2*-Salem de degré* 8 *de mesure* 1,8475... *inférieure à* 2 *possède deux conjugués extérieurs au cercle unité réels et de signes contraires. Tous les autres de mesure inférieure à* 2 *sont totalement imaginaires.*

(4) *Un* 2*-Salem de degré* 10*, de mesure inférieure à* 1,4053... *est totalement imaginaire, de mesure inférieure à* 1,9749... *est soit totalement imaginaire soit possède ses deux conjugués extérieurs au cercle unité de signes contraires. Les seuls* 2*-Salem de mesure inférieure à* 2 *ayant deux conjugués extérieurs au cercle unité réels de signes contraires sont les* 2*-Salem de mesure* 1,835053..., 1,836868..., 1,953585..., 1,961647... *et* 1,994976...
*Les* 3*-Salem et les* 4*-Salem de degré* 10 *de mesure inférieure à* 2 *ont au moins deux conjugués extérieurs au cercle unité imaginaires conjugués.*

*Preuve.* Ces résultats découlent immédiatement du théorème 4 et du calcul des conjugués des entiers réciproques de petite mesure donnés par la table de Boyd [Bo 2].

Nous laissons au lecteur le soin de compléter ce corollaire en degré supérieur grâce à [Bo 3], [Bo 4]. □

J'en viens maintenant aux résultats de mes élèves: ceux de Zaïmi (1994–1997) concernent plus particulièrement les nombres de Pisot et ceux de Lalande (1996–1997) les nombres de Salem.

Le travail de Zaïmi porte sur une généralisation des nombres de Pisot.

Etant donné un corps de nombres $K$ et un entier algébrique $\theta$, $\theta > 1$, de polynôme minimal $P$ sur $K$, on dit que $\theta$ est un $K$-nombre de Pisot ou encore appartient à $S_K$ si pour tout plongement de $K$ dans $\mathbb{C}$, $\sigma(P_K)$ possède une unique racine de module supérieur à 1 et aucune racine de module 1. La définition est due à A.M. Bergé et J. Martinet [B-M].

J'avais remarqué que si $K$ est un corps quadratique réel, les éléments de $S_K$ de mesure inférieure à 2,6 sont en nombre fini et leur mesure croît avec le discriminant du corps de nombres [Be 2].

Zaïmi a continué l'étude pour les corps quadratiques imaginaires et les corps cubiques totalement réels. Il a prouvé dans sa thèse (1994) [Z 1] que la mesure d'un $K$-nombre de Pisot $\theta$ vérifie l'inégalité:

$$M(\theta) \geq \frac{\sqrt{|\Delta|}}{2}$$

si $K$ est quadratique, et

$$M(\theta) \geq \frac{\Delta^{1/4}}{\sqrt{6}}$$

si $K$ est cubique totalement réel, $\Delta$ désignant le discriminant de $K$.

Il a ensuite prouvé [Z 2] le théorème suivant:

*Soient $K$ un corps de nombres totalement réel primitif de degré $d$ ou bien un corps quadratique de discriminant $D$ et $P$ le polynôme minimal sur $K$ d'un entier algébrique $\theta$. Si le polynôme minimal de $\theta$ sur $K$ est non réciproque et si pour tout plongement $\sigma$ de $K$ dans $\mathbb{C}$ les polynômes $P$ et $\sigma P$ sont premiers entre eux, alors*

$$M(\theta)^{2(d-1)} \geq \frac{|D|}{d^d}.$$

Une question demeurait cependant ouverte depuis 1989 [B-M].

Plongeons $S_K$ dans l'algèbre $A = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ par la suite $(\theta_\sigma)_\sigma$ des conjugués de $\theta$ de module supérieur à 1, $(r_1, r_2)$ désignant la signature de $K$.

*L'ensemble $S_K$ est-il fermé dans $A$?*

*Lorsque $S_K$ est fermé, quels sont les éléments de mesure minimale?*

Zaïmi vient de démontrer (1997) [Z 3] l'équivalence suivante:

*$S_K$ est fermé dans $A$ si et seulement si $K = \mathbb{Q}$ ou $K$ quadratique imaginaire.*

(On savait déjà, grâce à Salem [S 1] pour $K = \mathbb{Q}$ et à Zaïmi [Z 1] pour $K$ quadratique imaginaire, que $S_K$ est fermé.)

Zaïmi a également prouvé [Z 3], que si $K$ est quadratique imaginaire ou totalement réel, alors:

$$\inf S_K = \theta_0 = 1{,}32\ldots$$

et

$$\inf S'_K = \frac{1+\sqrt{5}}{2}.$$

La preuve utilise encore le résultat de Schinzel précédemment cité ainsi que la remarquable propriété des nombres de Pisot :

*Tout corps de nombres réel peut être engendré par un nombre de Pisot qui est une unité du corps.*

On peut alors se demander si les corps de nombres imaginaires ayant seulement deux corps conjugués réels possède une pareille propriété, à savoir d'être engendré par un nombre de Salem.

*Lalande* (1996–1997) [La] *a caractérisé à l'aide de leur groupe de Galois les corps de nombres engendrés par un nombre de Salem et plus généralement les corps de nombres non totalement imaginaires engendrés par une unité réciproque.*

## Références


[B-M] Bergé, A.M., Martinet, J., Notions relatives de régulateurs et de hauteurs. Acta Arith. 54 (1989), 155–170.

[Be 1] Bertin, M.J., $K$-nombres de Pisot et de Salem. Acta Arith. 68 (1994), 113–131.

[Be 2] — $K$-nombres de Pisot et de Salem. In : Advances in number theory (éd. par F.Q. Gouvêa et N. Yui), 391–397. Oxford University Press, New York 1993.

[Be 3] — The operator $x + (1/x) - 2$ and the reciprocal integers. In: Proceedings of the 5th Conference of the Canadian Number Theory Association, Ottawa 1996, à paraître.

[B-B 1] Bertin, M.J., Boyd, D.W., Une caractérisation de certaines classes de nombres de Salem. C. R. Acad. Sci. Paris Sér. I Math. 303 (1986), 837–839.

[B-B 2] — A characterization of two related classes of Salem numbers. J. Number Theory 50 (1995), 309–317.

[Bo 1] Boyd, D.W., Small Salem numbers. Duke Math. J. 44 (1977), 315–327.

[Bo 2] — Reciprocal polynomials having small measure. Math. Comp. 35 (1980), 1361–1377.

[Bo 3] — Reciprocal polynomials having small measure II. Math. Comp. 53 (1989), 355–357, S1–S5.

[Bo 4] — Small measures of reciprocal polynomials. Correspondance privée, Avril 1995.

[D-P 1] Dufresnoy, J., Pisot, Ch., Sur les petits éléments d'un ensemble remarquable d'entiers algébriques. C. R. Acad. Sci. Paris 238 (1954), 1551–1553.

[D-P 2] — Etude de certaines fonctions méromorphes bornées sur le cercle unité. Application à un ensemble fermé d'entiers algébriques. Ann. Sci. École Norm. Sup. (3) 72 (1955), 69–92.

[D-P 3] — Sur les éléments d'accumulation d'un ensemble fermé d'entiers algébriques. Bull. Sci. Math. (2) 79 (1955), 54–64.

[G] Grandet-Hugot, M., Ensembles fermés d'entiers algébriques. Ann. Sci. École Norm. Sup. (3) 82 (1965), 1–35.

[La] Lalande, F., Corps de nombres engendrés par un nombre de Salem. Exposé au Séminaire d'Arithmétique, 1996, non publié.

[Le] Lehmer, D.H., Factorization of certain cyclotomic functions. Ann. of Math. (2) 34 (1933), 461–479.

[M] Matveev, E.M., On algebraic numbers of small logarithmic height. Mat. Zametki, à paraître.

[P] Pisot, Ch., La répartition modulo 1 et les nombres algébriques. Ann. Scuola Norm. Sup. Pisa (2) 7 (1938), 205–248.

[S 1] Salem, R., A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan. Duke Math. J. 11 (1944), 103–107.

[S 2] — Power series with integral coefficients. Duke Math. J. 12 (1945), 153–171.

[Sc] Schinzel, A., On the product of the conjugates outside of the unit circle of an algebraic number. Acta Arith. 24 (1973), 385–399. Addendum: ibid. 26 (1974/75), 329–331.

[Sm] Smyth, C.J., On the product of the conjugates outside the unit circle of an algebraic integer. Bull. London Math. Soc. 3 (1971), 169–175.

[V] Vijayaraghavan, T., On fractional part of the powers of a number:
I, J. London Math. Soc. 15 (1940), 159–160.
II, Proc. Cambridge Philos. Soc. 37 (1941), 349–357.
III, J. London Math. Soc. 17 (1942), 137–138.
IV, J. Indian Math. Soc. (N.S.) 12 (1948), 33–39.

[Za] Zagier, D., Algebraic numbers close to both 0 and 1. Math. Comp. 61 (1993), 485–491.

[Z 1] Zaïmi, T., Sur les nombres de Pisot relatifs. Thèse de Doctorat de l'Université Paris 6, Mai 1994.

[Z 2] — Sur les $K$-nombres de Pisot de petite mesure. Acta Arith. 77 (1996), 103–131.

[Z 3] — Sur la fermeture de l'ensemble des $K$-nombres de Pisot. Acta Arith. 83 (1998), 363–367.

# Irreducibility of polynomials and arithmetic progressions with equal products of terms

*F. Beukers, T.N. Shorey and R. Tijdeman*

*To Andrzej Schinzel on the occasion of his sixtieth birthday*

**Abstract.** In some fundamental papers Davenport, Lewis and Schinzel [DLS], Schinzel [Sch1, Sch3] and Fried [Fr1, Fr2, Fr3] have shown how irreducibility criteria for polynomials $f(X) - g(Y)$ in combination with results of Runge or Siegel can be used to prove the finiteness of the solutions of the corresponding diophantine equation $f(x) = g(y)$ in integers $x, y$. In the present paper we are particularly interested in the case $f(X) = X(X+d_1)\cdots(X+(m-1)d_1)$, $g(Y) = Y(Y+d_2)\cdots(Y+(n-1)d_2)$, i.e. the diophantine equation

$$x(x+d_1)\cdots(x+(m-1)d_1) = y(y+d_2)\cdots(y+(n-1)d_2). \tag{0.1}$$

We first give some history on this equation and indicate how results for this equation can be derived from general irreducibility theory in the literature. Then we give direct proofs of the results using only basic facts on algebraic curves.

1991 Mathematics Subject Classification: 11D57.

## 1. When do finite arithmetic sequences have equal products of terms?

The question, under the restriction that the arithmetic progressions have equal lengths, was posed in Poland by Gabovich in 1966 [Ga]. He mentioned the example $2 \cdot 6 \cdot 10 = 4 \cdot 5 \cdot 6$ and gave an infinite class of examples of length 4 including $7 \cdot 20 \cdot 33 \cdot 46 = 20 \cdot 21 \cdot 22 \cdot 23$ and $18 \cdot 37 \cdot 56 \cdot 75 = 24 \cdot 37 \cdot 50 \cdot 63$. Some infinite classes of solutions of length 5 were given by Szymiczek [Sz] and Choudhry [Ch]. In 1968 Mąkowski [Mą] observed that for every positive integer $m$

$$2 \cdot 6 \cdot 10 \cdots (4m-2) = (m+1)(m+2)\cdots(2m). \tag{1.1}$$

An opposite result was obtained by Saradha, Shorey and Tijdeman [SaST1].

**Theorem A.** *For fixed integers $d_1 > d_2 > 0$ there are only finitely many positive integers $m > 2$, $x, y$ $\gcd(x, y, d_1, d_2) = 1$ and*

$$x(x + d_1) \cdots (x + (m-1)d_1) = y(y + d_2) \cdots (y + (m-1)d_2) \tag{1.2}$$

*except for the solutions* (1.1). *The other solutions are effectively computable.*

The special case of equal products of arithmetic progressions of different lengths, but both with difference 1, was also considered by some authors. This is the same as equality of the products of two blocks of positive integers

$$x(x+1) \cdots (x+m-1) = y(y+1) \cdots (y+n-1), \qquad m < n. \tag{1.3}$$

In 1963 Mordell [Mo] showed that $(x, y) = (2, 1)$ and $(14, 5)$ are the only solutions of (1.3) in case $(m, n) = (2, 3)$. MacLeod and Barrodale [MaB] proved that there are no solutions for $(m, n) = (2, 4), (2, 6), (2, 8), (2, 12), (4, 8)$ and $(5, 10)$ and only one solution $(x, y) = (8, 1)$ if $(m, n) = (3, 6)$. Boyd and Kisilevsky [BoK] found that there are just three solutions when $(m, n) = (3, 4)$, namely $(x, y) = (2, 1), (4, 2)$ and the remarkable $(55, 19)$. Other known solutions occur when $(m, n) = (3, 5)$, namely $(x, y) = (4, 1), (8, 2)$, and when $(m, n) = (4, 7)$ we find $(x, y) = (7, 1), (63, 8)$.

In the years 1990–1996 Shorey and coworkers studied the equation (0.1) subject to $n > m > 1$ with $d_1, d_2$ and $n/m$ fixed. Saradha and Shorey [SaS1] showed that $(m, n, x, y) = (3, 6, 8, 1)$ is the only solution of (0.1) with $d_1 = d_2 = 1$ and $n = 2m$. They proved in [SaS2] that (0.1) has no solutions with $d_1 = d_2 = 1$ and $n = 3m$ or $n = 4m$. Mignotte and Shorey [MiS] proved that there are no solutions with $d_1 = d_2 = 1$ and $n = 5m$ or $n = 6m$. The case $d_1 = 1$, $d_2 > 1$, $n = m$ or $n = 2m$ was considered by Saradha, Shorey and Tijdeman [SaST3]. In the paper all the solutions of equation (0.1) with $n = m$, $d_1 = 1$, $d_2 = 2, 3, 5, 6, 7, 9, 10$ and equation (0.1) with $n = 2m$, $d_1 = 1$, $d_2 = 5, 6$ have been given. In [SaST4] extensions to more general equations on the products of values of a polynomial at points in arithmetic progressions have been treated.

Some general finiteness results were obtained by Saradha and Shorey [SaS3] and Saradha, Shorey and Tijdeman [SaST2]. They proved that if $n > m$ and $\gcd(m, n) > 1$, then the positive solutions $m, n, x, y$ of equation (0.1) can be effectively bounded in terms of $d_1$, $d_2$ and $n/m$ with the exception of the infinite class of solutions

$$m = 2, \quad n = 4, \quad d_1 = 2d_2^2, \quad x = y^2 + 3d_2 y.$$

They further proved that if $m = 2$ or 4 and $n > 2$ is odd, then the solutions $n, x, y$ of (0.1) can be effectively bounded in terms of $d_1$ and $d_2$.

For the remaining case $\gcd(m, n) = 1$ no general effective method is available. In that case, with $m, n$ fixed, we have to resort to Siegel's famous result on integral points on algebraic curves, which is, unfortunately, ineffective. In addition, we can use Faltings's work on Mordell's conjecture to make a similar statement for rational solutions as well. We summarize this in the following theorem, whose proof is the main goal of this paper.

**Theorem 1.1.** *Let $m$ and $n$ be integers with $1 < m \leq n$. Let $d_1$ and $d_2$ be positive rational numbers with $d_1 \neq d_2$, if $m = n$. The equation*

$$x(x+d_1)\cdots(x+(m-1)d_1) = y(y+d_2)\cdots(y+(n-1)d_2)$$

*admits only finitely many integral solutions $x, y$ except for the infinite class of solutions $x = y^2+3d_2y, -2d_2^2-3d_2y-y^2$ when $m = 2$, $n = 4$ and $d_1 = 2d_2^2$. Moreover, the equation admits infinitely many rational solutions $x, y$ when $(m,n) = (2,2),(2,3),(2,4),(3,3)$ and $m = 2$, $n = 6$, $d_1 = 15d_2^3/4$. In all other cases there are only finitely many rational solutions.*

Note that in the above considerations $d_1$ and $d_2$ were given as fixed numbers. Quite recently Choudhry [Ch] provided an infinite class of solutions of (1.2) with arbitrary length and unbounded $d_1, d_2$. He observed that for arbitrary positive integers $m, r, s$ with $r > s$, solutions of (1.2) are given by

$$x = mrs^m, \quad d_1 = r(r^m - s^m), \quad y = s\{r^m + (m-1)s^m\}, \quad d_2 = s(r^m - s^m).$$

As a generalisation in another direction Erdős [Er] conjectured in 1975 that for every rational number $\lambda$ the number of integral solutions $(x, y, m, n)$ of

$$x(x+1)\cdots(x+m-1) = \lambda y(y+1)\cdots(y+n-1) \quad \text{with } y \geq x+m,$$
$$\min(m,n) \geq 3, \quad m > 1, \quad n > 1$$

is finite. The combination of Theorem 2.2 and Siegel's Theorem B, both to be stated in the next section, yields a finiteness statement in case $m$ and $n$ are fixed. Actually Theorem 2.2 describes more accurately which triples $(m, n, \lambda)$ are exceptional. The combination of Theorem 2.2 and Faltings's Theorem C gives a list of triples $(m, n, \lambda)$ such that the number of rational solutions $x, y$ for every other triple is finite.

## 2. Diophantine equations and irreducibility of polynomials

Throughout the paper we shall mean irreducible over the field of complex numbers if we merely write irreducible. The relation between irreducibility of polynomials $f(X) - g(Y)$ $(f(X), g(X) \in \mathbb{Z}[X])$ and solvability of diophantine equations $f(x) = g(y)$ becomes clear from the following fundamental results.

**Theorem B** (Siegel). *The number of integral points on an irreducible algebraic curve of genus $> 0$ is finite.*

Actually Siegel gave a more refined condition which we do not state here, but refer to [Si]. In [Fa] we have the following celebrated theorem.

**Theorem C** (Faltings). *The number of rational points on an irreducible algebraic curve of genus $> 1$ is finite.*

Both results are ineffective. An effective result on the finiteness of the number of integral solutions of $f(x,y) = 0$ if the polynomial $f(X,Y)$ is irreducible over the field of rational numbers, was given by Runge [Ru], cf. [Sk, pp. 89–91].

So basic questions are to decide if a polynomial $f(X) - g(Y)$ is irreducible and to compute its genus. In 1958 Ehrenfeucht [Eh] proved that $f(X) - g(Y)$ is irreducible if the degrees of $f$ and $g$ are coprime. Three years later Davenport, Lewis and Schinzel [DLS] gave two classes of reducible polynomials $f(X) - g(Y)$, namely

1. $f(X) = F(f_1(X))$, $g(Y) = F(g_1(Y))$ where $F, f_1, g_1$ are arbitrary polynomials, subject to $\deg F > 0$, in which case $f_1(X) - g_1(Y)$ is a factor of $f(X) - g(Y)$,
2. $f(X) = cF_k(f_1(X))$, $g(Y) = -cF_k(g_1(Y))$ where $c$ is a constant, $f_1$, $g_1$ are arbitrary polynomials, $k$ is an even integer $> 2$ and $F_k$ is defined by $F_k(\cosh\theta) = \cosh k\theta$.

In this case $u^2 - 2uv\cos\frac{\pi}{k} + v^2 - \sin^2\frac{\pi}{k}$ is a factor of $F_k(f_1(X)) + F_k(g_1(Y))$ where $u = f_1(X)$, $v = g_1(Y)$. They further provided a criterion on the discriminants $D(\lambda) = \operatorname{disc}(f(x) + \lambda)$ and $E(\lambda) = \operatorname{disc}(g(y) + \lambda)$ which implies that $f(X) - g(Y)$ is irreducible and has positive genus and applied their criterion to the case $f(X) = X^m + X^{m-1} + \ldots + X$, $g(Y) = Y^n + Y^{n-1} + \ldots + Y$. In this way they showed that for these $f$ and $g$ and for integers $n > m > 1$ the equation $f(x) = g(y)$ has only finitely many integral solutions. They further showed that Runge's theorem could be used to compute upper bounds for the solutions in terms of the degrees $m$ and $n$ of $f$ and $g$, respectively, if they are not coprime. Further Nesterenko and Shorey [NeS] showed that the preceding upper bounds for the solutions can be computed in terms of $m/\gcd(m,n)$ and $n/\gcd(m,n)$ if $\gcd(m,n) > 1$. Quite recently Brindza and Pintér [BrP] applied the criterion of Davenport, Lewis and Schinzel to

$$f(X) = X(X + d_1)\cdots(X + (m-1)d_1), \quad g(Y) = Y(Y + d_2)\cdots(Y + (n-1)d_2),$$

but they only obtained a conditional result, which is satisfied if $m$ and $n$ are prime or less than 31.

Schinzel [Sch1] extended Ehrenfeucht's theorem in the following way. Suppose $f(X), g(X) \in \mathbb{Q}[X]$ and $f$ is of prime degree. Then $f(X) - g(Y)$ is reducible over the complex field if and only if $g(Y) = f(h(Y))$ and either $h(X) \in \mathbb{Q}[X]$ or $f(X) - g(Y)$ is of the form $a(X + b)^p + c(\ell(X))^p$ where $a, b, c \in \mathbb{Q}$ and $\ell(X) \in \mathbb{Q}[X]$. The paper contains examples of the latter case with $p = 7$ and 11 due to Birch, Cassels and Guy, cf. [Ca]. Furthermore, Schinzel [Sch2] obtained the following improvement of the theorems of Runge [Ru] and Siegel [Si]. If $f(X,Y) \in \mathbb{Z}[X,Y]$ is irreducible over the rationals and the equation $f(x,y) = 0$ has an infinity of integer solutions, then the highest homogeneous part of $f(X,Y)$ is, up to a constant factor, a power of a linear or an irreducible indefinite quadratic form. In his book, published in 1982, Schinzel [Sch3, Section 8, Theorem 11] gave another classification of polynomials $f(X), g(X) \in \mathbb{Z}[X]$ such that $f(X) - g(Y)$ is reducible.

Fried made a deep study of the structure of the factors of $f(X) - g(Y)$. We mention some special cases of his results which are relevant to our work. For

a survey we refer to Fried's own contribution to these Proceedings. Fried and MacRae [FrM] showed that $f_1(X) - g_1(Y)$ divides $f(X) - g(Y)$ in $\mathbb{C}[X, Y]$ if and only if there exists a polynomial $F(T) \in \mathbb{C}[T]$ such that $f(X) = F(f_1(X))$ and $g(Y) = F(g_1(Y))$. This is due to Schinzel in case $\deg(f)$ is prime.

The decomposition properties were elaborated in [Fr1]. Fried proved (cf. [Fr1, Propositions 2 and 3]) that if $f(X)$, $g(X) \in \mathbb{Z}[X]$, then there exist polynomials $f_1, f_2, g_1, g_2 \in \mathbb{Z}[X]$ such that

1. $f(X) = f_1(f_2(X))$, $g(Y) = g_1(g_2(Y))$,
2. $\deg(f_1) = \deg(g_1)$,
3. the splitting fields of $f_1(X) - X$ and $g_1(X) - X$ are the same,
4. the irreducible factors of $f(X) - g(Y)$ are in one-to-one correspondence with the irreducible factors of $f_1(X) - g_1(Y)$.

In Proposition 1 of [Fr2] Fried used the Riemann-Hurwitz formula to give expressions for the genus of $f(X) - g(Y)$. Fried used the formulas to describe the structure of polynomials $f, g \in K[X]$, $K$ a number field, such that $f(X) - g(Y)$ has an irreducible factor which defines a curve having infinitely many $K$-integral points (cf. Corollary of Theorem 3 of [Fr2]).

By using Schinzel's characterization of reducible polynomials $f(X) - g(Y)$ [Sch3] and by using Fried's decomposition theorem on such polynomials it is possible to derive the following result.

**Theorem 2.1.** *Let $m$ and $n$ be positive integers with $m \leq n$ and let $\lambda \in \mathbb{C}^*$. If $X(X+1)\cdots(X+m-1) - \lambda Y(Y+1)\cdots(Y+n-1)$ is reducible in $\mathbb{C}[X, Y]$ then one of the following possibilities holds:*

1. *$m = n$, $\lambda = 1$, in which case $X - Y$ is a factor,*
2. *$m = n$ is odd, $\lambda = -1$, in which case $X + Y + m - 1$ is a factor,*
3. *$m = 2$, $n = 4$, $\lambda = \frac{1}{4}$, in which case we have*

$$4X(X+1) - Y(Y+1)(Y+2)(Y+3) = (2X - Y^2 - 3Y)(2X + 2 + 3Y + Y^2).$$

In the next section we shall give a selfcontained proof of this theorem. The following genus computation allows us to apply Theorems B and C.

**Theorem 2.2.** *Consider the curve*

$$X(X+1)\cdots(X+m-1) = \lambda Y(Y+1)\cdots(Y+n-1)$$

*with $n \geq m > 1$ and $\lambda \in \mathbb{C}^*$. Suppose it is irreducible. Then its genus is zero in the following cases:*

1. $m = 2$, $n = 2$,
2. $m = 2$, $n = 3$, $\lambda = \pm 3\sqrt{3}/8$,
3. $m = 2$, $n = 4$, $\lambda = -4/9$,
4. $m = 2$, $n = 6$, $\lambda = (-10 \pm 7\sqrt{7})/576$.

*The genus is one in the following cases:*

1. $m = 2$, $n = 3$, $\lambda \neq \pm 3\sqrt{3}/8$,
2. $m = 2$, $n = 4$, $\lambda \neq -4/9$,

3. $m = 2$, $n = 5$, $\lambda = -1/4t, 3125t^4 - 47500t^2 + 82944 = 0$,
4. $m = 2$, $n = 6$, $\lambda = 16/225$,
5. $m = 2$, $n = 8$, $\lambda = -1/4t, t^3 + 567t^2 - 54432t - 4665600 = 0$,
6. $m = 3$, $n = 3$,
7. $m = 3$, $n = 4$, $\lambda = \pm 3\sqrt{3}/2$,
8. $m = n = 4$, $\lambda = -9/16, -16/9$.

*In all other cases the genus is strictly bigger than one.*

# 3. Proof of Theorem 2.1

Let $f \in \mathbb{C}[X]$ and let $S_f, S_g$ be the set of stationary points of $f, g$ which we assume to be simple. Let $m = \deg(f)$ and $n = \deg(g)$. For any $a \in \mathbb{C}$ let

$$m_a = \#\{\alpha \in S_f \mid f(\alpha) = a\}$$
$$n_a = \#\{\beta \in S_g \mid g(\beta) = a\}$$

Consider the polynomial $f(X) - g(Y)$ and suppose it is reducible.

**Proposition 3.1.** *Suppose $m = n$ and $f(X) - g(Y) = F(X,Y)G(X,Y)$ with $\deg(F) = m_1$, $\deg(G) = m_2$ with $m_1, m_2 \geq 1$ and $m_1 + m_2 = m$. Then*

$$m_1 m_2 \leq \sum_{a \in \mathbb{C}} m_a n_a.$$

*Proof.* Geometrically the curve $C$ given by $f(X) - g(Y) = 0$ consists of two components $C_1, C_2$ given by $F(X,Y) = 0$ and $G(X,Y) = 0$. By homogenisation of the coordinates we can assume that $C$ is embedded in projective space $\mathbb{P}^2$. Let $f(X) = \sum_{r=0}^{m} f_r X^r$ and $g(Y) = \sum_{r=0}^{m} g_r Y^r$. The points of intersection of $C$ with the line at infinity are given by $f_m X^m = g_m Y^m$. These are distinct points with multiplicity one. So $C$ has no singularities at infinity.

The finite singular points of $C$ are given by the pairs $(\alpha, \beta)$ such that $f'(\alpha) = g'(\beta) = 0$ and $f(\alpha) = g(\beta)$. The local equation of $C$ around such a point looks like

$$0 = f''(\alpha)(X - \alpha)^2 - g''(\beta)(Y - \beta)^2 + \ldots$$

Since $f''(\alpha), g''(\beta) \neq 0$ we conclude that the singularities are simple. In total there are $\sum_{a \in \mathbb{C}} m_a n_a$ singular points.

Any point of intersection between $F = 0$ and $G = 0$ is a singular point of $C$. Since all singularities are simple, the order of intersection is one. By Bezout's theorem there are $m_1 m_2$ points of intersection, hence $m_1 m_2 \leq \sum_{a \in \mathbb{C}} m_a n_a$. □

We next consider the case of unequal degrees $m, n$. Let us introduce the weighted degree $\delta$ given by $\delta(X^a Y^b) = na + mb$ and notice that $\delta(AB) = \delta(A) + \delta(B)$ for all $A, B \in \mathbb{C}[X,Y]$, $AB \neq 0$. For any $A \in \mathbb{C}[X,Y]$ we denote the highest degree part with respect to $\delta$ by $(A)_h$. We also have $(AB)_h = (A)_h (B)_h$. Assume that

$$f(X) - g(Y) = F(X,Y)G(X,Y)$$

where $F, G$ have positive degree. From comparison of the highest degree parts we get

$$f_m X^m - g_n Y^n = (F)_h (G)_h.$$

So $(F)_h$ must be of the form $aX^r + \ldots + bY^s$ with $a, b \neq 0$. The monomials $X^r, Y^s$ have equal weighted degree, i.e. $nr = ms$ and so, $r, s$ must be multiples of $m/d, n/d$ respectively, where $d = \gcd(m, n)$. In particular the weighted degrees of $F$ and $G$ are multiples of $mn/d$ and also $d \geq 2$. Note, by the way, that this immediately implies Ehrenfeucht's theorem.

**Proposition 3.2.** *Let the notation be as above and let $m_1, m_2$ be the weighted degrees of $F$, $G$ respectively. Then,*

$$m_1 m_2 \leq mn \sum_{a \in \mathbb{C}} m_a n_a.$$

*Moreover, $m_1, m_2$ are multiples of $mn/d$ and $m_1 + m_2 = mn$.*

*Proof.* Choose $b \in \mathbb{C}$ such that $b \notin S_f \cup S_g$, $f(b) \notin \{g(b), g(S_g)\}$ and $g(b) \notin \{f(b), f(S_f)\}$. Consider the polynomials $\widetilde{f}(X) = f(X^n + b)$, $\widetilde{g}(Y) = g(b + Y^m)$. We define

$$\widetilde{m}_a = \#\{\alpha \in S_{\widetilde{f}} \mid \widetilde{f}(\alpha) = a\},$$
$$\widetilde{n}_a = \#\{\beta \in S_{\widetilde{g}} \mid \widetilde{g}(\beta) = a\}.$$

Notice that $\widetilde{m}_a = nm_a$ whenever $a \in f(S_f)$ and $\widetilde{m}_a = 0$ if $a \notin \{f(S_f), f(b)\}$. Above $f(b)$ the polynomial $\widetilde{f}$ has the higher order stationary point $X = 0$. But since $f(b)$ is not the image under $\widetilde{g}$ of $S_{\widetilde{g}}$, this point is not a singular point of the curve $\widetilde{f}(X) - \widetilde{g}(Y) = 0$ and we can ignore it. Similar remarks hold for $g(b)$ and the values of $\widetilde{n}_a$. We now apply our previous proposition to the factorisation

$$\widetilde{f}(X) - \widetilde{g}(Y) = F(X^n + b, Y^m + b) G(X^n + b, X^m + b)$$

to obtain

$$m_1 m_2 \leq \sum_{a \in \mathbb{C}} \widetilde{m}_a \widetilde{n}_a.$$

Hence

$$m_1 m_2 \leq mn \sum_{a \in \mathbb{C}} m_a n_a. \qquad \square$$

**Proposition 3.3.** *Let notations be as above and suppose that $n_a \leq 1$ for all $a$. Then $n = d$ and $f(X) - g(Y)$ has a factor of degree one in $Y$.*

*Proof.* From Proposition 3.2 we get

$$m_1 m_2 \leq mn \sum_a m_a \leq mn(m-1).$$

Using $m_1, m_2 \geq mn/d$ and $m_1 + m_2 = mn$ we get

$$\frac{mn}{d}\left(mn - \frac{mn}{d}\right) \leq mn(m-1),$$

hence

$$\frac{n}{d} \leq \frac{d}{d-1}\Big(1-\frac{1}{m}\Big) < \frac{d}{d-1} \leq 2.$$

So we see that $n = d$. Suppose now that $f(X) - g(Y)$ has no factors of degree one in $Y$. Then, $m_1, m_2 \geq 2mn/d$ and hence

$$2\,\frac{mn}{d}\Big(mn - \frac{2mn}{d}\Big) \leq mn(m-1).$$

We obtain

$$2\,\frac{n}{d} \leq \frac{d}{d-2}\Big(1-\frac{1}{m}\Big) < \frac{d}{d-2} \leq 2$$

and we conclude $n/d < 1$ which is impossible. □

We apply the previous results to the case where

$$f(X) = X(X+1)\cdots(X+m-1), \quad g(Y) = \lambda Y(Y+1)\cdots(Y+n-1)$$

with $\lambda \neq 0$. Without loss of generality we may assume that $m \leq n$. We shall use the following proposition

**Proposition 3.4.** *Let $f(X) = X(X+1)\cdots(X+m-1)$. Then, for all $a \in \mathbb{C}$, $m_a \leq 2$. Moreover, if $m$ is odd, then $m_a \leq 1$ for all $a \in \mathbb{C}$.*

*Proof.* Let $\alpha_1, \alpha_2, \ldots, \alpha_{d-1}$ be the stationary points of $f$. By Rolle's theorem they are simple and real and can be ordered such that $-(d-1) < \alpha_{d-1} < -(d-2) < \alpha_{d-2} < \ldots < -1 < \alpha_1 < 0$. Note that $|f|$ has a symmetry axis $\operatorname{Re} X = -(d-1)/2$ so that $|f(\alpha_i)| = |f(\alpha_{d-i})|$ for each $i$. Observe that $|f(X)|$ assumes its unique maximal value on the interval $[-i, -i+1]$ at $\alpha_i$ so that

$$\frac{|f(\alpha_{i-1})|}{|f(\alpha_i)|} \geq \frac{|f(\alpha_i+1)|}{|f(\alpha_i)|} = \frac{|\alpha_i+1|\,|\alpha_i+2|\cdots|\alpha_i+d|}{|\alpha_i|\,|\alpha_i+1|\cdots|\alpha_i+d-1|} = \frac{|\alpha_i+d|}{|\alpha_i|}$$

for $i = 1, \ldots, d-1$. For $i \leq d/2$ we have $|\alpha_i - (-d)| > |\alpha_i - 0|$ whence $|f(\alpha_{i-1})| > |f(\alpha_i)|$. By symmetry, $|f(\alpha_{i-1})| < |f(\alpha_i)|$ for $i \geq (d+2)/2$. Thus $m_a \leq 2$ for every $a$. If $d$ is odd, then $f(\alpha_i) = -f(\alpha_{d-i})$ and $m_a \leq 1$ for every $a$. □

**Corollary 3.5.** *Let $d$ be an even positive integer. Put $\widetilde{f}(X) = (X-1^2)(X-3^2)\times \ldots \times (X-(d-1)^2)$. Put $\widetilde{m}_a = \#\{\alpha \in S_{\widetilde{f}} \mid \widetilde{f}(\alpha) = a\}$. Then $\widetilde{m}_a \leq 1$ for every $a \in \mathbb{C}$.*

*Proof.* We use the notation of Proposition 3.4 and its proof. Note that $f(X) = 2^{-d}\widetilde{f}((2X+d-1)^2)$. Let $\beta_1, \ldots, \beta_{(d/2)-1}$ be the (simple) stationary points of $\widetilde{f}$ ordered in such a way that

$$1^2 < \beta_{(d/2)-1} < 3^2 < \ldots < (d-3)^2 < \beta_1 < (d-1)^2.$$

Then $\beta_i = (2\alpha_i + d - 1)^2$ for $i = 1, 2, \ldots, (d/2) - 1$. Hence $\widetilde{f}(\beta_i) = 2^d f(\alpha_i)$. It follows that

$$|\widetilde{f}(\beta_1)| > |\widetilde{f}(\beta_2)| > \ldots > |\widetilde{f}(\beta_{(d/2)-1})|$$

so that $\widetilde{m}_a \leq 1$ for every $a \in \mathbb{C}$. □

*Proof of Theorem* 2.1. Suppose that $n$ is odd. According to Propositions 3.3 and 3.4 we get that $n = d$ and $f(X)-g(Y)$ has a factor linear in $Y$. From $n = d = \gcd(m, n)$ and $m \leq n$ we get $m = n$ and so our factor is also linear in $X$. It is not hard to see that the only linear factors that can occur are $Y-X$ when $\lambda = 1$ and $Y+X-(m-1)$ when $\lambda = (-1)^m$.

Now suppose that $n$ is even. Since $g(Y) = g(n-1-Y)$ we see that

$$g((U-n+1)/2) = \lambda 2^{-n}(U^2-1^2)(U^2-3^2)\cdots(U^2-(n-1)^2).$$

Let us write $h(V) = \lambda 2^{-n}(V-1^2)(V-3^2)\cdots(V-(n-1)^2)$. Using Corollary 3.5 we note that $h$ is a polynomial such that $\#\{\alpha \in S_h \mid h(\alpha) = a\}$ is at most 1 for every $a \in \mathbb{C}$. Suppose that $f(X)-g(Y)$ contains an irreducible factor $K(X,Y)$ of degree $< n/2$ in $Y$. Then either $K(X,Y)$ or $K(X,Y)K(X,-n+1-Y)$ is symmetric with respect to $Y \to -n+1-Y$ and is a non-trivial factor of $f(X)-g(Y)$. Hence $f(X)-h(V)$ has a non-trivial factor in $\mathbb{C}[X,V]$. Application of Proposition 3.3 now yields that $f(X)-h(V)$ has a divisor linear in $V$ and $n/2 = \gcd(m, n/2)$. So either $m = n$ or $n = 2m$.

Suppose $m = n$. We know that $f(X)-h(V)$ has a factor linear in $V$ and quadratic in $X$. Hence there is a quadratic polynomial $Q \in \mathbb{C}[X]$ such that $f(X) = h(Q(X))$. More particularly, $Q$ maps the set of points $A = \{0, -1, \ldots, 1-m\}$ to $B = \{1^2, 3^2, \ldots, (m-1)^2\}$. Suppose $Q(X) = aX^2+bX+c$. Each element of $B$ is the image of precisely two points of $A$ under $Q$. Hence the set $A$ is stable under the substitution $X \to -b/a - X$. So we see that $b/a = m-1$ and $Q$ has an extremal value at $(1-m)/2$. If this point is a minimum then $Q(0) = (m-1)^2$ and $Q(-m/2) = 1^2$. Since $m = n > 2$ this gives two independent conditions and a short calculation yields $Q(X) = (2X+m-1)^2$. The equality $f(X) = h(Q(X))$ then implies that $\lambda = 1$. Suppose that $Q$ has a maximum at $(1-m)/2$. Then, $Q(0) = 1$ and $Q(-m/2) = (m-1)^2$. A short calculation yields $Q(X) = -(2X+m-1)^2 + m^2 - 2m + 2$. In addition we have $Q(-1) = 3^2$ and hence $4m-7 = 9$, i.e. $m = 4$. From $f(X) = h(Q(X))$ we again infer $\lambda = 1$.

Suppose $n = 2m$. We know that $f(X)-h(V)$ has a factor linear in both $X$ and $V$. Hence there is a linear polynomial $L \in \mathbb{C}[X]$ such that $f(X) = h(L(X))$. More particularly, $L$ maps the set of points $A = \{0, -1, \ldots, 1-m\}$ to $B = \{1^2, 3^2, \ldots, (2m-1)^2\}$. Suppose $L(X) = aX+b$ and $m > 2$. Then either $L(0) = 1^2$, $L(-1) = 3^2$, $L(-2) = 5^2$ or $L(0) = (2m-1)^2$, $L(-1) = (2m-3)^2$, $L(-2) = (2m-5)^2$. In both cases these function values cannot be assumed by a linear function. Hence $m = 2$, $n = 4$. But in that case there cannot be a factor of $f(X)-g(Y)$ of degree $< n/2 = 2$ in $Y$.

The case that remains is when $f(X)-g(Y)$ has only factors of degree $n/2$ in $Y$. Then we can apply Proposition 3.2 with $m_1 = m_2 = mn/2$. Hence, by $n_a \leq 2$,

$$(mn/2)^2 \leq mn \sum_a m_a n_a \leq 2mn(m-1).$$

We find $n \leq 8(1-1/m) < 8$. Hence $n = 2, 4, 6$. Since $mn/2$ is a multiple of $mn/d$ we see that $d$ is even, and hence $m = 2, 4, 6$. By the stationary values of a polynomial $p$ we mean the set $\{p(\alpha) \mid p'(\alpha) = 0\}$. Here is a table of the stationary

values of $X(X+1)\cdots(X+k-1)$,

$$\begin{aligned} k=2: &\quad -1/4 \\ k=4: &\quad 9/16, -1 \\ k=6: &\quad -225/64, -(160 \pm 112\sqrt{7})/27. \end{aligned}$$

Using this table it is readily seen that the only instances in which the inequality $(mn/2)^2 \leq mn\sum_a m_a n_a$ holds are given by $m=n$, $\lambda=1$ or $m=2$, $n=4$, $\lambda=1/4$. □

# 4. Proof of Theorem 2.2

**Proposition 4.1.** *Let $f, g \in \mathbb{C}[X]$ be polynomials of degree $m, n$ respectively and suppose $f(X)-g(Y)$ is irreducible. Suppose that the stationary points of $f$ and $g$ are simple. For $\alpha \in S_f$ we put $r_\alpha = \#\{y \in S_g \mid f(\alpha)=g(y)\}$. Let $g_C$ be the genus of the curve $C: f(X)=g(Y)$. Then*

$$2g_C = \sum_{\alpha \in S_f}(n-2r_\alpha) - m + 2 - \gcd(m,n).$$

*Proof.* Consider the function field extension $\mathbb{C}(X,Y)/\mathbb{C}(Y)$ given by $f(X)-g(Y)$. Its genus is given by

$$2-2g_C = 2m - \sum_i (e_i - 1),$$

where the $e_i$ are the ramification indices of our extension $\mathbb{C}(X,Y)/\mathbb{C}(Y)$ (see [GrH, p. 218]). Note that we have only ramification above $Y=\infty$ and above those $Y=y_0$ for which $g(y_0) \in \{f(\alpha) \mid \alpha \in S_f\}$. Above $Y=\infty$ we have $d$ branches of ramification index $m/d$ where we have written $d=\gcd(m,n)$. A local parameter at such a branch is given by $t = X^p Y^q$ where $p, q \in \mathbb{Z}$ are chosen so that $-d = p(n/d)+q(m/d)$. Let $\zeta$ be any $d$-th root of unity. Then $X = \zeta t^{-n/d} + O(t^{-(n/d-1)})$ and $Y = t^{-m/d} + O(t^{-(m/d-1)})$ around $t=0$. The $d$ branches correspond to the $d$ different choices of $\zeta$.

Now let $Y=y_0$ with $g(y_0)=f(\alpha)$ for some $\alpha \in S_f$. Clearly the point $(\alpha, y_0)$ is only ramified above $y_0$ if $g'(y_0) \neq 0$. So we obtain

$$\begin{aligned} \sum_i (e_i - 1) &= d(m/d-1) + \sum_{\alpha \in S_f} \sum_{\substack{y_0 : g(y_0)=f(\alpha) \\ g'(y_0)\neq 0}} 1 \\ &= m - d + \sum_{\alpha \in S_f}(n-2r_\alpha) \end{aligned}$$

Hence

$$2g_C = 2-2m+\sum_i (e_i-1) = \sum_{\alpha \in S_f}(n-2r_\alpha) - m + 2 - \gcd(m,n). \qquad \square$$

*Proof of Theorem* 2.2. We shall apply Proposition 4.1 to the curve $f(X) - g(Y) = 0$ with $f(X) = X(X+1)\cdots(X+m-1)$ and $g(Y) = \lambda Y(Y+1) \times \ldots \times (Y+m-1)$. We may assume that $1 < m \leq n$. By Proposition 3.4 we know that $r_\alpha \leq 2$ in all cases and $r_\alpha \leq 1$ if $n$ is odd. Write $\delta(n) = 2$ when $n$ is odd and $\delta(n) = 4$ when $n$ is even. Since $|S_f| = m - 1$, we get

$$\begin{aligned} 2g_C &= \sum_{\alpha \in S_f} (n - 2r_\alpha) - m + 2 - \gcd(m,n) \\ &\geq (n - \delta(n))(m-1) + 2(1-m) + m - \gcd(m,n) \\ &= (n - \delta(n) - 2)(m-1) + m - \gcd(m,n) \end{aligned}$$

Suppose $n \geq 9$ or $n = 7$. Then $n - \delta(n) - 2 \geq 3$ and we get $2g_C \geq 3(m-1)$, hence $g_C > 1$. Suppose $n = 8$, then $n - \delta(n) - 2 = 2$ and $2g_C \geq 2(m-1) + m - \gcd(m,8) \geq 2(m-1)$. Hence $g_C > 1$ if $m \geq 3$. This leaves us the case $m = 2$, $n = 8$. Suppose $n = 5$. Then $2g_C \geq m - 1 + m - \gcd(m,5)$. We easily check that for all choices of $m = 3,4,5$ we get $g_C > 1$. This leaves us with $m = 2$, $n = 5$.

We must now determine the genera in the following remaining cases:

1. $m = 2$, $n = 2,3,4,5,6,8$
2. $m = 3$, $n = 3,4,6$
3. $m = 4$, $n = 4,6$
4. $m = 5$, $n = 6$
5. $m = 6$, $n = 6$.

To get $g_C$ for these cases we must compute the set of stationary values of each of the polynomials $h_m = X(X+1)\cdots(X+m-1)$ with $m = 2,3,4,5,6,8$. In other words, we compute $\{h_m(\alpha) \mid h_m'(\alpha) = 0\}$ for $m = 2,3,\ldots,8$.

$$\begin{aligned} m = 2: &\quad \{-1/4\}\ (\textit{once}) \\ m = 3: &\quad \{\text{zeros of } 27x^2 - 4\}\ (\textit{once}) \\ m = 4: &\quad \{9/16\ (\textit{once}), -1\ (\textit{twice})\} \\ m = 5: &\quad \{\text{zeros of } 3125x^4 - 47500x^2 + 82944\ (\textit{once})\} \\ m = 6: &\quad \{-225/64\ (\textit{once}) \text{ and zeros of } 27x^2 + 320x - 2304\ (\textit{twice})\} \\ m = 8: &\quad \{11025/256\ (\textit{once}) \\ &\quad \text{and zeros of } x^3 + 567x^2 - 54432x - 4665600\ (\textit{twice})\}. \end{aligned}$$

The adjective 'twice' indicates that there are two stationary points above the stationary value involved. Let $m = 2$. Then $S_f$ consists of a single point and $f(S_f) = -1/4$. If $g(S_g)$ does not contain this point then $2g_C = n - m + 2 - \gcd(m,n) = n - \gcd(n,2)$. Hence $g_C > 1$ if $n = 5,6,8$, $g_C = 1$ if $n = 3,4$ and $g_C = 0$ if $n = 2$. If $-1/4$ is an element of $g(S_g)$ then the value $\lambda$ is determined by this and we can easily compute the genus. The result is in the statement of our theorem. Note that $m = 2$, $n = 4$, $\lambda = 1/4$ is excluded since it is reducible.

Let $m = 3$. If $f(S_f)$ is disjoint with $g(S_g)$ we get $2g_C = 2n - m + 2 - \gcd(m,n) = 2n - 1 - \gcd(n,3)$. Hence $g_C > 1$ if $n = 4,6$ and $g_C = 1$ if $n = 3$. If $f(S_f) \cap g(S_g)$

is non-empty we get explicit values for $\lambda$ which are enumerated in the theorem. The cases $m = n = 3, \lambda = \pm 1$ are excluded because they are reducible.

When $m = 4, 5, 6$ we argue in exactly the same way as above. □

# 5. Proof of Theorem 1.1

**Proposition 5.1.** *Let $l \in \mathbb{Q}^*$. Then each of the following genus one curves*

1. $y(y+1) = lx(x+1)(x+2)$
2. $y(y+1)(y+2) = l^3x(x+1)(x+2)$ *with* $l \neq \pm 1$
3. $y(y+1) = l^2x(x+1)(x+2)(x+3)$
4. $225y(y+1) = 16x(x+1)(x+2)(x+3)(x+4)(x+5)$

*contains infinitely many rational points.*

*Proof.* We use a deep result of B. Mazur [M] which says that the rational torsion group of an elliptic curve over $\mathbb{Q}$ is either $\mathbb{Z}/N\mathbb{Z}$ with $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $N = 1, 2, 3, 4$. In particular, if an elliptic curve contains finitely many points, this number is at most 16. The number of torsion points whose orders do not divide 2 is at most 12.

Let us apply this principle to the first curve $y(y+1) = lx(x+1)(x+2)$. There we have the six obvious rational points $(a, b)$ with $a = 0, -1$ and $b = 0, -1, -2$. By using the cord method for elliptic curves we find the additional points

$$\Big(-2+\frac{1}{l}, 1-\frac{1}{l}\Big), \Big(-2+\frac{1}{l}, -2+\frac{1}{l}\Big), \Big(-1+\frac{1}{4l}, -\frac{4l+1}{8l}\Big),$$
$$\Big(-1+\frac{1}{4l}, -\frac{4l-1}{8l}\Big), \Big(\frac{1}{l}, -2-\frac{1}{l}\Big), \Big(\frac{1}{l}, 1+\frac{1}{l}\Big),$$
$$(l-1, l^2-1), (l-1, -l^2).$$

A straightforward check, long and boring by hand, but swiftly done using a computer algebra system, reveals that if $l \neq \pm 1/4, \pm 1/2, \pm 1, \pm 3/4, \pm 2/3$ then none of the rational points coincide or coincide with a 2-torsion point. Note that 2-torsion points can be recognized by the fact that their $y$-coordinate is $-1/2$ in our curve. Hence we have found more than 12 rational points whose order does not divide 2 and so our curve must have infinitely many rational points. The remaining cases can be checked simply by finding at least 13 points whose orders do not divide 2. We exhibit our finds here. For $l = 1$ we found

$$(0,0), (0,-1), (-1,0), (-1,-1), (-2,0), (-2,-1), (1,2), (1,-3), (5,14), (5,-15),$$
$$(-3/4, -3/8), (-3/4, -5/8), (-14/9, -35/27), (-14/9, 8/27).$$

For $l = 1/4$ we found

$$(0,0), (0,-1), (-1,0), (-1,-1), (-2,0), (-2,-1), (2,-3), (4,-6), (4,5), (2,2),$$
$$(-20/9, -22/27), (-20/9, -5/27), (-3/4, -15/16), (-3/4, -1/16).$$

For $l = 1/2$ we found

$$(0,0),(0,-1),(-1,0),(-1,-1),(-2,0),(-2,-1),(2,3),(2,-4),(3,5),(3,-6),$$
$$(-1/2,-3/4),(-1/2,-1/4),(-4/9,-20/27),(-4/9,-7/27).$$

For $l = 3/4$ we found

$$(0,0),(0,-1),(-1,0),(-1,-1),(-2,0),(-2,-1),(4,9),(4,-10),(4/3,-10/3),$$
$$(4/3,7/3),(-1/4,-7/16),(-1/4,-9/16),(-2/3,-1/3),(-2/3,-2/3).$$

For $l = 2/3$ we found

$$(0,0),(0,-1),(-1,0),(-1,-1),(-2,0),(-2,-1),$$
$$(-1/3,-4/9),(-1/3,-5/9),(11/3,-77/9),(11/3,68/9),$$
$$(-5/8,-11/16),(-5/8,-5/16),(3/2,5/2),(3/2,-7/2).$$

For negative $l$ we can remark that the curves with $l$ and $-l$ are isomorphic via $(x,y) \mapsto (-3-x,y)$.

Consider the curve $y(y+1)(y+2) = l^3x(x+1)(x+2)$ with $l \neq \pm 1$. The point $(-1,-1)$ is a point of inflexion and can be used as the zero of our addition law. It turns out that the order 2 points all lie on the line at infinity. Obvious rational points on the curve are given by $(a,b)$ with $a,b \in \{0,-1,-2\}$. Further rational points are given by

$$\left(\frac{12}{l^3-8}, 2\frac{l^3+4}{l^3-8}\right), \quad \left(-4\frac{2l^3+1}{8l^3+1}, \frac{-12l^3}{8l^3+1}\right)$$
$$\left(\frac{-3}{l^3+1}, \frac{-3l^3}{l^3+1}\right), \quad \left(\frac{3}{l^3-1}, \frac{l^3+2}{l^3-1}\right), \quad \left(-4\frac{2l^3-1}{8l^3-1}, -2\frac{2l^3-1}{8l^3-1}\right).$$

So when $l \neq \pm 2, \pm 1/2$ we have found 13 finite points whose orders do not divide 2. Again, a long and boring check reveals that there are no rational values of $l$ for which two of these points coincide. For $l = 2$ we found the points

$$(0,0),(0,-1),(0,-2),(-1,0),(-1,-2),(-2,0),(-2,-1),(-2,-2),$$
$$(-1/3,-8/3),(-5/3,2/3),(3/7,10/7),(-17/7,-24/7),(-20/21,-10/21).$$

The curves with $l = -2, \pm 1/2$ are trivially isomorphic to the one with $l = 2$. So in all cases we find at least 13 finite rational points beside $(-1,-1)$. Hence our proposition is proved again in this case.

Now consider the curve $y(y+1) = l^2x(x+1)(x+2)(x+3)$. This curve has two involutions given by $y \to -1-y$ and $x \to -3-x$. They generate a group of order 4. At infinity we have two rational points. Consider the four points

$$(0,0),(-1,0),\left(-\frac{3l-1}{2l}, -\frac{(l+1)(3l-1)}{4l}\right),\left(-\frac{2l^2+3l+1}{2l}, -\frac{4l^4-l^2+2l-1}{4l}\right).$$

The only rational values of $l$ for which any such point can lie in the orbit of another point are given by $l = \pm 1, \pm 1/3, \pm 1/2$. In all other cases we have now, after application of the group action, 16 rational points on the curve plus two points at infinity. Hence there are infinitely many rational points. In the exceptional cases

$l = \pm 1, \pm 1/3$ we exhibit at least 16 finite rational points. For $l = \pm 1$ we find

$$(0,0),(0,-1),(-1,0),(-1,-1),(-2,0),(-2,-1),(-3,0),(-3,-1),$$
$$(4/3,-65/9),(4/3,56/9),(-13/3,56/9),(-13/3,-65/9),$$
$$(-5/4,5/16),(-5/4,-21/16),(-7/4,-21/16),(-7/4,5/16).$$

For $l = \pm 1/3$ we find

$$(0,0),(0,-1),(-1,0),(-1,-1),(-2,0),(-2,-1),(-3,0),(-3,-1),$$
$$(-9/4,-15/16),(-9/4,-1/16),(-3/4,-1/16),(-3/4,-15/16),$$
$$(1/3,8/27),(1/3,-35/27),(-10/3,-35/27),(-10/3,8/27).$$

The case $l = \pm 1/2$ corresponds to a reducible curve which has infinitely many rational points in a trivial way.

Finally consider the genus one curve $225y(y+1) = 16x(x+1)(x+2)(x+3) \times (x+4)(x+5)$. There are two rational points at infinity and we have the finite rational points $(a,b)$ with $a = 0,-1,-2,-3,-4,-5$, $b = 0,-1$ and

$$(-43/5,33024/625), \quad (-43/5,-33649/625),$$
$$(9/5,9728/625), \quad (9/5,-10353/625).$$

Hence we have at least 18 rational points so there must be infinitely many. □

*Proof of Theorem* 1.1. Let $C$ be the plane algebraic curve given by

$$X(X+d_1)\cdots(X+(m-1)d_1) = Y(Y+d_2)\cdots(Y+(n-1)d_2).$$

After the replacements $X \to d_1X, Y \to d_2Y$ we see that $C$ is isomorphic to

$$X(X+1)\cdots(X+m-1) = \lambda Y(Y+1)\cdots(Y+n-1)$$

with $\lambda = d_2^n/d_1^m$. We know that this curve is irreducible unless $m = n$, $\lambda = \pm 1$ or $m = 2$, $n = 4$, $\lambda = 1/4$. The first case does not occur since $\lambda \neq \pm 1$. The latter case gives rise to the factorisation

$$X(X+2d^2) - Y(Y+d)(Y+2d)(Y+3d) = (X - Y^2 - 3dY)(X + Y^2 + 3dY + 2d^2)$$

which induces the infinite set of integral solutions given in our theorem. In all other cases $C$ is irreducible.

From our Theorem 2.1 we know that the genus of $C$ can only be zero if $m = n = 2$. In that case our equation can be rewritten as $(2x+d_1)^2 - (2y+d_2)^2 = d_1^2 - d_2^2$ which has clearly only finitely many solutions. In all other cases the genus of $C$ is positive and by Siegel's Theorem B the number of integral points is finite. This proves the first part of our theorem.

We now consider rational solutions. When $m = n = 2$ there are clearly infinitely many rational solutions since we have a conic with at least one rational point on it. By Theorem 2.1 there are no other cases of genus zero. We now proceed to the genus one cases. According to Theorem 2.1 these are given by $(m,n) = (2,3),(2,4),(3,3)$ and $(m,n) = (2,6)$ with $\lambda = 16/225$. According to Proposition 5.1 we have infinitely many rational solutions in all cases. This gives

rise to the second assertion of our theorem. Finally, according to Theorem 2.1 the remaining cases have all genus at least two and hence, by Faltings's Theorem C, we have finitely many rational solutions. □

**Acknowledgement.** We thank B. Brindza, M.D. Fried, M. Nori and A. Schinzel for their valuable remarks on the background of the solutions of our problems. They alerted us to most of the papers mentioned in Section 2. The paper would not have had its present form without the lively conference in wet Zakopane.

## References

[BoK] Boyd, D.W., Kisilevsky, H.H., The diophantine equation $u(u+1)(u+2)(u+3) = v(v+1)(v+2)$. Pacific J. Math. 40 (1972), 23–32.

[BrP] Brindza, B., Pintér, Á., On the irreducibility of some polynomials in two variables. Preprint.

[Ca] Cassels, J.W.S., Factorization of polynomials in several variables. In: Proceedings of the Fifteenth Scandinavian Congress (Oslo, 1968) (Lecture Notes in Math. 118), 1–17. Springer, Berlin 1970.

[Ch] Choudhry, A., On arithmetic progressions of equal lengths and equal products of terms. Acta Arith. 82 (1997), 95–97.

[DLS] Davenport, H., Lewis, D.J., Schinzel, A., Equations of the form $f(x) = g(y)$. Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[Eh] Ehrenfeucht, A., A criterion of indecomposability of polynomials (in Polish). Prace Mat. 2 (1958), 167–169.

[Er] Erdős, P., Problems and results on number theoretic properties of consecutive integers and related questions. In: Proceedings of the Fifth Manitoba Conference on Numerical Mathematics (Congressus Numerantium No. XVI), 25–44. Utilitas Math., Winnipeg 1976.

[Fa] Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73 (1983), 349–366.

[Fr1] Fried, M., The field of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J. Math. 17 (1973), 128–146.

[Fr2] — On a theorem of Ritt and related diophantine problems. J. Reine Angew. Math. 264 (1973), 40–55.

[Fr3] — Irreducibility results for separated variables equations. J. Pure Appl. Algebra 48 (1987), 9–22.

[FrM] Fried, M., MacRae, R.E., On curves with separated variables. Math. Ann. 180 (1969), 220–226.

[Ga] Gabovich, Ya., On arithmetic progressions with equal products of terms (in Russian). Colloq. Math. 15 (1966), 45–48.

[GrH] Griffiths, P., Harris, J., Principles of algebraic geometry. Wiley, New York 1978.

[MaB] MacLeod, R.A., Barrodale, I., On equal products of consecutive integers. Canad. Math. Bull. 13 (1970), 255–259.

[Mą] Mąkowski, A., Problèmes P543 et P545, R1. Colloq. Math. 19 (1968), 179–180.

[M] Mazur, B., Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[MiS] Mignotte, M., Shorey, T.N., The equations $(x+1)\cdots(x+k) = (y+1)\cdots(y+mk)$ with $m = 5, 6$. Indag. Math. (N.S.) 7 (1996), 215–225.

[Mo] Mordell, L.J., On the integer solutions of $y(y+1) = x(x+1)(x+2)$. Pacific J. Math. 13 (1963), 1347–1351.

[NeS] Nesterenko, Yu.V., Shorey, T.N., An equation of Goormaghtigh. Acta Arith. 83 (1998), 381–389.

[Ru] Runge, C., Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. J. Reine Angew. Math. 100 (1887), 425–435.

[SaS1] Saradha, N., Shorey, T.N., On the ratio of two blocks of consecutive integers. Proc. Indian Acad. Sci. Math. Sci. 100 (1990), 107–132.

[SaS2] — The equations $(x+1)\cdots(x+k) = (y+1)\cdots(y+mk)$ with $m = 3, 4$. Indag. Math. (N.S.) 2 (1991), 489–510.

[SaS3] — On the equation $x(x+d_1)\cdots(x+(k-1)d_1) = y(y+d_2)\cdots(y+(mk-1)d_2)$. Proc. Indian Acad. Sci. Math. Sci. 104 (1994), 1–12.

[SaST1] Saradha, N., Shorey, T.N., Tijdeman, R., On arithmetic progressions of equal lengths with equal products. Math. Proc. Cambridge Philos. Soc. 117 (1995), 193–201.

[SaST2] — On arithmetic progressions with equal products. Acta Arith. 68 (1994), 89–100.

[SaST3] — On the equation $x(x+1)\cdots(x+k-1) = y(y+d)\cdots(y+(mk-1)d)$, $m = 1, 2$. Acta Arith. 71 (1995), 181–196.

[SaST4] — On values of a polynomial at arithmetic progressions with equal products. Acta Arith. 72 (1995), 67–76. Correction: ibid. 84 (1998), 385–386.

[Sch1] Schinzel, A., Reducibility of polynomials of the form $f(x) - g(y)$. Colloq. Math. 18 (1967), 213–218.

[Sch2] — An improvement of Runge's theorem on diophantine equations. Comment. Pontificia Acad. Sci. 2 (1969), no. 20, 1–9.

[Sch3] — Selected topics on polynomials. University of Michigan Press, Ann Arbor 1982.

[Si] Siegel, C.L., Über einige Anwendungen diophantischer Approximation. Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. 1929, Nr. 1, 70 pp. Gesammelte Abhandlungen, vol. I, 209–266. Springer, Berlin 1966.

[Sk] Skolem, Th., Diophantische Gleichungen. Springer, Berlin 1938.

[Sz] Szymiczek, K., Note on arithmetical progressions with equal products of five terms. Elem. Math. 27 (1972), 11–12.

# Mahler's measure and special values of $L$-functions — some conjectures

*David W. Boyd*

*To Andrzej Schinzel on the occasion of his 60th birthday*

**Abstract.** If $P(x_1, \ldots, x_n)$ is a polynomial with integer coefficients, the Mahler measure of $P$, $M(P)$ is defined to be the geometric mean of $|P|$ over the $n$-torus $\mathbb{T}^n$. We are interested in formulas that generalize a formula of Smyth, that $\log M(1+x+y) = L'(\chi_{-3}, -1)$, where $\chi_{-3}$ is the odd Dirichlet character of conductor 3. We will describe some results of a systematic search for polynomials $P(x,y)$ for which $\log M(P)$ is a rational multiple of $L'(\chi_{-f}, -1)$ for various other values of the conductor $f$, and another class of examples for which $\log M(P)$ seems to be a multiple of $L'(E,0)$, where $E$ is an elliptic curve. The formulas have been verified to high numerical accuracy but most have not been rigorously proved. However, we have some conjectures about necessary and/or sufficient conditions under which such formulas can hold. The results for Dirichlet characters are related to $K_2(\mathcal{O}_F)$ for certain number fields $F$ while the results for elliptic curves $E$ are related to $K_2(E)$. Thus there are clearly some connections with the wide-ranging Beilinson conjectures, some of which have been made explicit by Hubert Bornhorn and Fernando Rodriguez Villegas.

1991 Mathematics Subject Classification: Primary 11R06, 11K16; Secondary 11Y99.

Key words: Mahler measure, polynomials, computation, $L$-functions, Beilinson conjecture, elliptic curve.

## 1. Formulas involving Dirichlet $L$-functions

If $P(x_1, \ldots, x_n)$ is a polynomial with complex coefficients, then the *logarithmic Mahler measure* of $P$ is defined by

$$m(P) = \int_0^1 \cdots \int_0^1 \log |P(e(t_1), \ldots, e(t_n))| \, dt_1 \cdots dt_n,$$

where $e(t) = \exp(2\pi i t)$. The *Mahler measure* of $P$ is then defined as $M(P) = \exp(m(P))$. So $M(P)$ is the geometric mean of $|P|$ over the $n$-torus. This was introduced by Mahler [Ma] in order to give a simple proof of the "Gel'fond-Mahler inequality". It will be more natural to deal directly with $m(P)$ here.

This research was supported by a grant from NSERC.

For $n = 1$, if $P(x) = a_0 \prod_{j=1}^{d}(x - \alpha_j)$, Jensen's formula shows that

$$m(P(x)) = \log|a_0| + \sum_{j=1}^{d} \log^+ |\alpha_j|,$$

where $\log^+ v = \max(\log v, 0)$, for $v > 0$, and $\log^+ 0 = 0$.

For polynomials with integer coefficients, clearly $m(P(x)) \geq 0$ with the equality only if $P(x)$ is monic and has all its zeros inside the unit circle, and hence is a product of a monomial $x^a$ and a cyclotomic polynomial, by Kronecker's theorem. In [Le], Lehmer noted that $m(P(x))$ measures the growth rate of the sequence $\Delta_n = \prod_{j=1}^{d}(\alpha_j^n - 1)$, and asked whether $m(P)$ can be arbitrarily small but positive for $P(x) \in \mathbb{Z}[x]$. The smallest value he was able to find was

$$\begin{aligned} m(x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1) \\ = \log(1.17628081\ldots) = .16235761\ldots. \end{aligned} \tag{1}$$

As we pointed out in [Bo1], Lehmer's question leads in a natural way to the consideration of $m(P(x_1, \ldots, x_n))$ since one has

$$\lim_{n\to\infty} m(P(x, x^n)) = m(P(x, y)).$$

This formula, and its generalization to $n$ variables by Lawton [La] show that measures of polynomials in many variables are limit points of measures of polynomials in one variable. We conjectured in [Bo1] that the set $\mathbb{L}$ of all measures $m(P(x_1, \ldots, x_n))$ for polynomials with integer coefficients should be a closed set. This would imply a positive answer to Lehmer's question.

Smyth [Sm] showed that the values of $m(P)$ could be interesting even for very simple polynomials by proving that

$$m(1 + x + y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2) = L'(\chi_{-3}, -1), \tag{2}$$

where the second form follows from the functional equation for $L'(\chi_{-3}, s)$.

It is interesting that (1) can also be written in a similar way. Lehmer's polynomial $P(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ is the minimal polynomial of a Salem number (a real algebraic integer $\sigma > 1$ for which $1/\sigma$ is a Galois conjugate and all other conjugates lie on the unit circle). Thus $m(P(x)) = \log\sigma$. Chinburg [Ch], using a result of Stark [St], showed that for every Salem number $\sigma$, if $K = \mathbb{Q}(\sigma)$ and $k = \mathbb{Q}(\sigma + 1/\sigma)$, if $\chi$ is the nontrivial character of $\mathrm{Gal}(K/k)$ and if $L(\chi, s)$ is the Artin $L$-function of $\chi$, then

$$\log\sigma = rL'(\chi, 0),$$

where $r$ is an explicit rational number (in which the class numbers $h(K)$ and $h(k)$ appear).

Perhaps motivated by this, and certainly motivated by Smyth's result (2), Chinburg was led to ask, for each real odd Dirichlet character $\chi_{-f}$, whether there is a polynomial $P_f(x,y)$ with integer coefficients such that $m(P_f(x,y))$ is a rational multiple of $L'(\chi_{-f},-1)$, i.e. does Smyth's formula generalize. His student, Ray [Ra] constructed such polynomials for the six values 3, 4, 7, 8, 20 and 24 using the theory of dilogarithms. In fact, his proof for $f=7$ requires the proof of a new multivariable dilogarithm identity and gives:

$$m(\Phi_7(x)(y-1)^2+7x^2(x+1)^2y)=\frac{8}{7}L'(\chi_{-7},-1), \tag{3}$$

where $\Phi_7(x)=(x^7-1)/(x-1)$ is the 7th order cyclotomic polynomial.

Recently, we have found rather simpler formulas than Ray's and extended the list of conductors by adding 11, 15, 35, 39, 55 and 84. However, most of our formulas have only been verified numerically to 50 decimal places rather than being proved. For example, in contrast to (3), we have

$$m((x+1)^2y+(x^2+x+1))\stackrel{?}{=}\frac{1}{3}d_7, \tag{4}$$

and

$$m((x^2+x+1)y+(x^2+1))\stackrel{?}{=}\frac{1}{12}d_{15}, \tag{5}$$

and

$$m((x+1)^2(x^2+x+1)y+(x^2-x+1)^2)\stackrel{?}{=}\frac{2}{3}d_{11}. \tag{6}$$

Our notation here is that

$$d_f=L'(\chi_{-f},-1)=\frac{f^{3/2}}{4\pi}L(\chi_{-f},2), \tag{7}$$

and the symbol $\stackrel{?}{=}$, read "conjectured to be equal to" means that the two members of the equation are equal to many decimal places (usually 50). Our examples are of the form $m(A(x)y+B(x))$ where $A$ and $B$ are cyclotomic polynomials, so that

$$m(A(x)y+B(x))=m^+(B(x)/A(x)),$$

where

$$m^+(P)=\int_0^1\cdots\int_0^1\log^+|P(e(t_1),\ldots,e(t_n))|\,dt_1\cdots dt_n. \tag{8}$$

In this case $m(A(x)y+B(x))$ can be written as a sum of values of the Bloch-Wigner dilogarithm evaluated at those roots of $|A(x)|=|B(x)|$ that lie on the circle $|x|=1$. (Note that these are algebraic numbers since they are the roots of $A(x)A(1/x)=B(x)B(1/x)$.)

For example, in (4), if $\alpha=(-3+\sqrt{-7})/2$ and $\mathcal{D}(z)$ is the Bloch-Wigner dilogarithm, then

$$m((x+1)^2y+(x^2+x+1))=\frac{1}{\pi}\big(\mathcal{D}(\alpha)-\mathcal{D}(\alpha^2)+\frac{1}{3}\mathcal{D}(\alpha^3)\big),$$

which is known to be of the form $rd_7$ where $r$ is a non-zero rational by a result of Zagier [Z]. By computation, $r \stackrel{?}{=} 1/3$. These results, and those for the other conductors mentioned are closely related to the results computed by Browkin [Br] related to Lichtenbaum's conjecture for $K_2(\mathcal{O}_F)$ where $\mathcal{O}_F$ is the ring of integers of an imaginary quadratic field $F$.

Typically, the equation $|A(x)| = |B(x)|$ will have more than one pair of roots on the unit circle and then the formulas have more terms, e.g.

$$m(y + \Phi_{11}(x)) = m^+(\Phi_{11}(x)) = \frac{1}{11}\big(20d_3 + 14d_4 - 10\ \mathrm{Re}(d_5) - 6\ \mathrm{Im}(d_5)\big).$$

Here $\chi_{-5}$ is the complex odd character with $\chi_{-5}(2) = i$. In this formula we have written $=$ rather than $\stackrel{?}{=}$ since the roots on the unit circle are all roots of unity and so the formula becomes a finite Fourier transform which can be evaluated explicitly in terms of the $L(\chi, 2)$.

## 2. Formulas involving $L$-functions of elliptic curves

The formulas to be described in this section were motivated by a recent result of Deninger [D]. A more complete account may be found in [Bo2].

Deninger, realizing that formulas involving $L'(\chi, -1)$ were likely to be connected with the Beilinson conjectures [Be] was motivated to find a cohomological framework for such formulas. In [D], he showed that if $P(x_1, \ldots, x_n)$ does not vanish on the torus, then $m(P)$ is a Deligne period of a certain mixed motive connected with the cohomology of the set $\{P(x_1, \ldots, x_n) \neq 0\}$. Since Deligne periods and mixed motives seem somewhat abstract, I asked if he could provide a more concrete formula for one of the measures that occurs in [Bo1] as the second smallest limit point so far determined of the set $\mathbb{L}$ of Mahler measures. He quickly produced the conjectural formula:

$$m(y^2 + (x^2 + x + 1)y + x^2) \stackrel{?}{=} rL'(E_{15}, 0) \tag{9}$$

Here $E_{15}$ is the elliptic curve of conductor 15 which is the projective closure of the curve $y^2 + (x^2 + x + 1)y + x^2 = 0$ , $L(E_{15}, s)$ is the $L$-function of that curve and $r$ is conjectured to be rational. In fact, numerically $r$ is exactly 1 to at least 50 decimal places. Note that this polynomial *does* vanish on the torus so this is not a special case of his general result but requires a more subtle consideration.

It is convenient to adopt the following notation

$$b_N = L'(E, 0) = \epsilon \frac{N}{(2\pi)^2} L(E, 2),$$

for a modular elliptic curve of conductor $N$, where $\epsilon$ is the sign in the functional equation. Since $L(E, s)$ is an isogeny invariant this notation is unambiguous provided there is only one isogeny class of such curves, as will be the case for the

examples we mention here. (Since the equations could be formulated in terms of $L(E,2)$, there is really no need to assume $E$ is modular. However the results take on a more pleasant appearance if we make this assumption.)

Experimenting with other numerical values of $m(P)$ which had been computed in connection with [Bo1], we discovered that.

$$m((x+1)y^2+(x^2+x+1)y+x(x+1)) \stackrel{?}{=} b_{14}, \tag{10}$$

where this polynomial gives the smallest known measure of two variable polynomials.

The three smallest possible conductors of elliptic curves are 11, 14 and 15 [Cr] and the values 14 and 15 give the two smallest known limit points of $\mathbb{L}$. What about the conductor 11? Numerically,

$$b_{11} = .152147\cdots < \log(1.176280\ldots) = .162357\ldots,$$

so the existence of a polynomial with $m(P) = b_{11}$ (or even $m(P) \stackrel{?}{=} b_{11}$) would be very surprising for Lehmer's question since it would give an infinite number of improvements to Lehmer's polynomial (1)! But, of course, there is no particular reason to suppose such a polynomial exists. However, we do have a few examples in which $b_{11}$ appears, e.g.

$$m(y^2+(x^2+2x-1)y+x^3) \stackrel{?}{=} 5b_{11}. \tag{11}$$

It should be pointed out that formulas such as (9), (10) and (11) have a somewhat different nature than (2)–(6), since the latter arise because of the way the curve $P(x,y)=0$ intersects the torus $\mathbb{T}^2 = \{|x|=1\}\times\{|y|=1\}$, while the former are seemingly only sensitive to the curve $P(x,y)=0$ itself. This is one of many reasons to find these formulas fascinating.

A recently discovered formula illustrates a mixture of the two types:

$$m(y^2+2xy+(x^2+1)^2) \stackrel{?}{=} d_3 + b_{24}. \tag{12}$$

The term $b_{24}$ comes from the fact that the Jacobian of the curve $P(x,y)=0$ is an elliptic curve of conductor 24, while the term $d_3$ comes from the particular way $P(x,y)=0$ intersects $\mathbb{T}^2$. Of course, it would be easy to construct formulas such as (12) with reducible polynomials $P(x,y)$, but here $P(x,y)$ is irreducible.

Among the examples we discovered in our early experiments is the following example:

$$m((x^2+x+1)y^2+(x^2+x)y+(x^3+x^2+x)) \stackrel{?}{=} (1/3)b_{34}. \tag{13}$$

This is at first no more or less surprising than (9), (10) or (11), until one realizes that the curve $P(x,y)=0$ has genus 2. The Jacobian of this curve happens to split into the product of two elliptic curves, of conductors 34 and 17 and $m(P)$ picks out one of these two factors.

# 3. What is known?

The paper [Bo2] describes an attempt to understand and generalize such formulas by means of numerical experiment. The idea is to study certain one-parameter families of polynomials which define curves of genus 1 and 2 in order to determine conditions on the polynomials $P(x,y)$ so that formulas such as (9)–(11), and (13) should hold. The example

$$m(y^2 - x^3 - k) = m(x + y + k) = \log|k|, \quad \text{if } |k| \geq 2,$$

shows that it is not sufficient that $P(x,y) = 0$ define an elliptic curve nor is it necessary, as example (13) shows.

For example, generalizing (10), we found that

$$m((x+1)y^2 + (x^2 + kx + 1)y + x(x+1)) \stackrel{?}{=} r_k L'(E_k, 0),$$

for all integer $|k| \leq 100$ for which the polynomial defines an elliptic curve $E_k$, and where $r_k$ is a rational number which seems usually to be the reciprocal of an integer. In degenerate cases, i.e. for values of $k$ for which the curve $P(x,y) = 0$ is rational, the measure seems to be a multiple of an appropriate $L'(\chi, -1)$.

Similarly, generalizing (11), we find that

$$m(y^2 + (x^2 + kx - 1)y + x^3) \stackrel{?}{=} r_k L'(E_k, 0),$$

for integers $k$ with $2 \leq |k| \leq 20$. The reason for the omission of the integers $-1, 0, 1$ is explained in [Bo2]. For these values of $k$ the condition (B), mentioned below, is not satisfied.

One condition (A) that appears to be necessary, is that the "faces" $P_F$ of the polynomial $P(x,y)$ must have Mahler measure 0. Here the faces are defined in terms of the Newton polygon $N(P)$ of $P$ which is the convex hull in $\mathbb{R}^2$ of the set of lattice points $(i,j)$ for which the monomial $x^i y^j$ appears as a term in $P(x,y)$. A *face* $F$ of $N(P)$ is the intersection of $N(P)$ with a support line to $N(P)$, and a *face* $P_F$ of $P$ is the sum of the monomials making up $P$ over all lattice points in $F$. Each $P_F(x,y)$ is essentially a polynomial in one variable and the condition $m(P_F) = 0$ means that this polynomial is cyclotomic.

A second condition (B) has to do with the way in which the complex curve $P(x,y) = 0$ links the torus $\mathbb{T}^2$. This is described precisely in [Bo2]. We conjectured in [Bo2], for polynomials of the form $P(x,y) = A(x)y^2 + B(x)y + C(x)$, with $\deg(AC - 4B^2) \leq 4$, that if $P(x,y) = 0$ has genus 1, and satisfies (A) and (B), then $m(P)$ is a rational multiple of $L'(E,0)$ where $E$ is the Jacobian of $P(x,y) = 0$.

Recently, Rodriguez Villegas [RV] and independently, Hubert Bornhorn (private communication), have shown how this conjecture is related to Beilinson's conjectures. The condition (B) can be used to show that $m(P)$ is a rational multiple of the Beilinson regulator applied to the symbol $\{x,y\}$ and the condition (A) shows that some power of $\{x,y\}$ is in the kernel of the tame symbol (if one accepts a conjecture concerning the rank of a certain $K$-group). Putting these together shows that the above conjecture is a special case of the Beilinson conjectures.

If $E$ has complex multiplication, then in many cases the conjectured formulas can actually be proved due to the more explicit knowledge about $L(E,s)$. Rodriguez Villegas [RV] has also given a very interesting interpretation of many of the formulas in terms of certain non-holomorphic modular forms.

Nothing of this nature has yet been proved about the genus 2 examples constructed in [Bo2]. For the two classes of examples considered there, the polynomials $P$ all vanish on the torus so Deninger's result does not apply directly. However, it does appear that conditions (A) and (B) correctly predict the existence of formulas of the type $m(P) = rL'(E,0)$, so presumably there is some connection with the Beilinson conjectures. Then there are also the examples of the type (12) for which there should be a cohomological explanation.

Finally, since the formulas described here are of a very explicit and concrete nature, it would be interesting to have analytic proofs. For example, the curve $E_{15}$ of (9) is modular and the normalized cusp form is easily seen to be

$$f(z) = \sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} (1-q^n)(1-q^{3n})(1-q^{5n})(1-q^{15n}), \tag{14}$$

So (9) is a completely explicit identity:

$$\int_0^{2\pi} \int_0^{2\pi} \log|1 + 2\cos(s) + 2\cos(t)|\, ds\, dt \stackrel{?}{=} 15 \sum_{n=1}^{\infty} \frac{a_n}{n^2}, \tag{15}$$

with the $a_n$ given by (14). Surely this begs for a direct proof.

Since Deninger's result [D] applies to polynomials in any number of variables that do not vanish on the torus, it raises the possibility of finding explicit formulas for measures of such polynomials in terms of special values of $L$-functions. In general, for $n$-variable polynomials we would expect that these would be expressible in terms of suitable $L$-functions evaluated at $s = n$. However, very little in this direction has been done. Villegas' modular forms methods [RV] seem to apply to certain 3-variable polynomials, but for the moment the only explicit formula known is the remarkable formula of Smyth:

$$m(1 + x + y + z) = 7\zeta(3)/(2\pi^2) = 14\zeta'(-2).$$

It is a challenge, both experimentally and theoretically, to find such formulas for even the simplest polynomials in 3 or more variables. For example, even a conjectural formula for $m(1 + x + y + z + w)$ would be welcome.

## References

[Be] Beilinson, A.A., Higher regulators and values of $L$-functions. J. Soviet Math. 30 (1985), 2036–2070.

[Bo1] Boyd, D.W., Speculations concerning the range of Mahler's measure. Canad. Math. Bull. 24 (1981), 453–469.

[Bo2] — Mahler's measure and special values of $L$-functions. Experiment. Math. 7 (1998), 37–82.

[Br] Browkin, J., Conjectures on the dilogarithm. $K$-Theory 3 (1989), 29–56.

[Ch] Chinburg, T., Salem numbers and $L$-functions. J. Number Theory 18 (1984), 213–214.

[Cr] Cremona, J.E., Algorithms for modular elliptic curves. Cambridge University Press, Cambridge 1992.

[D] Deninger, C., Deligne periods of mixed motives, $K$-theory and the entropy of certain $\mathbb{Z}^n$-actions. J. Amer. Math. Soc. 10 (1997), 259–281.

[La] Lawton, W., On a problem of Boyd concerning geometric means of polynomials. J. Number Theory 16 (1983), 356–362.

[Le] Lehmer, D.H., Factorization of certain cyclotomic functions. Ann. of Math. (2) 34 (1933), 461–479.

[Ma] Mahler, K., On some inequalities for polynomials in several variables. J. London Math. Soc. 37 (1962), 341–344.

[Ra] Ray, G.A., Relations between Mahler's measure and values of $L$-series. Canad. J. Math. 39 (1987), 694–732.

[RV] Rodriguez Villegas, F., Modular Mahler measures I. In: Proceedings of the conference "Special topics in number theory", Pennsylvania State Univ., July 1997. To appear.

[Sm] Smyth, C.J., On measures of polynomials in several variables. Bull. Austral. Math. Soc. 23 (1981), 49–63.

[St] Stark, H., $L$-functions at $s = 1$, II. Adv. Math. 17 (1975), 60–92.

[Z] Zagier, D., Special values and functional equations of polylogarithms. In: Structural properties of polylogarithms (ed. by L. Lewin), 377–400. Amer. Math. Soc., Providence 1991.

# On the distribution of solutions of Thue's equation

*Béla Brindza, Ákos Pintér,*
*Alfred J. van der Poorten and Michel Waldschmidt*

*To Andrzej Schinzel on his 60th birthday*

## 1. Introduction

We consider solutions in relatively prime integers $x$ and $y$ of an equation

$$|F(x,y)| = m. \tag{1}$$

Here $F \in \mathbb{Z}[X,Y]$ is an irreducible binary form of degree $n \geq 3$ and $m$ denotes a positive integer with $s$ distinct prime factors. Solutions $(x,y)$ and $(-x,-y)$ will be deemed the same.

Bombieri and Schmidt [1] generalised and improved several earlier results in showing that there is an effectively computable absolute positive constant $c$ so that (1) has at most $cn^{s+1}$ solutions in coprime integers $x$ and $y$. Brindza [2] obtained a bound linear in the degree $n$, provided that $m$ is large enough; however, this bound remains exponential in $s$.

It seems likely that almost all the solutions of the equation (1) are small, and around $m^{1/n}$ provided that $m$ is large compared to the height of $F$.

Our principal result, which is based on Baker's method and a gap principle, illustrates that tendency. For brevity, we set $M$ to denote the Mahler height of the binary form $F$ (compare [1]).

**Theorem.** *Let* $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. *There are at most* $2n^2(s+1) + 13n$ *solutions of equation* (1) *with*

$$\max(|x|,|y|) \geq 21n^2M^5m^{\mu(n)}. \tag{2}$$

**Remark.** The binary form is not necessarily reduced. Further, one sees readily that all solutions of (1) satisfy

$$\max(|x|,|y|) \geq \tfrac{1}{2}M^{-1/n}m^{1/n}.$$

# 2. Preliminaries

Our proof requires several auxiliary results. The first is a gap principle. The crucial step in applying it will be provided by a different gap principle of Bombieri and Schmidt [1].

It will be convenient occasionally to use a compact notation

$$\eta^{\mathbf{k}_j} = \eta_0^{k_{0,j}} \cdots \eta_{t-1}^{k_{t-1,j}} \quad \text{and} \quad \psi^{\mathbf{k}_j} = \psi_0^{k_{0,j}} \cdots \psi_{t-1}^{k_{t-1,j}}.$$

to denote certain monomials that arise in our enunciation and argument.

**Lemma 1.** *Take $t$ at least 1, and let $\lambda$, $\eta_0, \ldots, \eta_{t-1}$, $\mu$, $\psi_0, \ldots, \psi_{t-1}$ be nonzero complex numbers. Suppose that the equation*

$$\lambda\eta_0^{\mathbf{k}_0} \cdots \eta_{t-1}^{\mathbf{k}_{t-1}} + \mu\psi_0^{\mathbf{k}_0} \cdots \psi_{t-1}^{\mathbf{k}_{t-1}} = 1$$

*has at least $t+2$ solutions in $t$-tuples $\mathbf{k}_j = (k_{0,j}, \ldots, k_{t-1,j})$ of integers. Denote by $K$ the maximum 'gap' between 'consecutive' such solutions; specifically*

$$K = \max_{0 \le i \le t-1, 1 \le j \le t+1} \{2, |k_{i,j+1} - k_{i,j}|\}.$$

*Then*

$$\tfrac{1}{4}(t+1)^{t/2} K^t \ge |\lambda\eta^{\mathbf{k}_1}|,$$

*provided that for $j = 1, \ldots, t+1$,*

$$|\lambda\eta^{\mathbf{k}_1}| \ge 6 \quad \textit{and} \quad |\eta^{\mathbf{k}_{j+1}}/\eta^{\mathbf{k}_j}| \ge 9(t+1)^{t/2} K^t.$$

**Remark.** Here is the scheme of the proof: We note that each solution $\mathbf{k}_j$ gives rise to a linear combination, $\Lambda_j$ say, with rational coefficients in the $t+1$ logarithms $2\pi i$, $\log(\eta_0/\psi_0)$, $\ldots$, $\log(\eta_{t-1}/\psi_{t-1})$. It follows that the $t+2$ complex numbers $\Lambda_1, \ldots, \Lambda_{t+2}$ must be linearly dependent over $\mathbb{Q}$. We recall that the $\Lambda_j$ 'are small' and apply 'Siegel's Lemma', in this case just a trivial estimate of the determinants arising from solving by Cramer's rule, to complete the argument.

*Proof.* The conditions detailed for Lemma 1 immediately entail

$$\tfrac{1}{6} \ge |\lambda\eta^{\mathbf{k}_1}|^{-1} > |\lambda\eta^{\mathbf{k}_2}|^{-1} > \ldots > |\lambda\eta^{\mathbf{k}_{t+2}}|^{-1},$$

and, for $j = 1, \ldots, t+1$,

$$\left|\eta^{\mathbf{k}_{j+1}}/\eta^{\mathbf{k}_j}\right| \ge 9K^t \ge 18,$$

$$\left|\psi^{\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}}\right| = \left|(1-(\lambda\eta^{\mathbf{k}_j})^{-1})/(\eta^{\mathbf{k}_{j+1}-\mathbf{k}_j} - (\lambda\eta^{\mathbf{k}_j})^{-1})\right| \le \tfrac{1+1/6}{18-1/6} < \tfrac{1}{15},$$

$$1 - \tfrac{1}{15} < \left|1 - \psi^{\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}}\right| < 1 + \tfrac{1}{15}.$$

Furthermore, for $z \in \mathbb{C}$ with $|z| \le \frac{1}{4}$, and with $\log(\ \ )$ denoting the principal branch, the simple inequality

$$\tfrac{5}{6}|z| \le |\log(1 \pm z)| \le \tfrac{7}{6}|z|,$$

and the relation $1-\eta^{\mathbf{k}_{j+1}-\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}-\mathbf{k}_j}=\lambda^{-1}\eta^{-\mathbf{k}_j}(1-\psi^{\mathbf{k}_j-\mathbf{k}_{j+1}})$, imply

$$\tfrac{5}{6}(1-\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}\le|\log(1-(1-\eta^{\mathbf{k}_{j+1}-\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}-\mathbf{k}_j}))|\le\tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}.$$

So there are rational integers $h_1,\ldots,h_{t+1}$ for which

$$\tfrac{5}{6}(1-\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}\le|2\pi ih_j+\sum_{i=0}^{t-1}(k_{i,j+1}-k_{i,j})\log(\eta_i/\psi_i)|\le\tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}.$$

From Siegel's Lemma we deduce that there exist rational integers $z_1,\ldots,z_{t+1}$, not all zero, so that for $i=0,\ldots,t-1$

$$\sum_{j=1}^{t+1}z_j(k_{i,j+1}-k_{i,j})=0\quad\text{and}\quad\max_{1\le j\le t+1}|z_j|\le(t+1)^{t/2}K^t.$$

Now for $j=1,\ldots,t+1$ set

$$\Lambda_j=2\pi ih_j+\sum_{i=0}^{t-1}(k_{i,j+1}-k_{i,j})\log(\eta_i/\psi_i),$$

and write $Z=\max_{1\le j\le t+1}|z_j|$, and $K_1=\frac{45}{8}(t+1)^{t/2}K^t$. Then $\Lambda_j\neq0$ and

$$\sum_{j=1}^{t+1}z_j\Lambda_j=2\pi i\sum_{j=1}^{t+1}z_jh_j.$$

Furthermore,

$$\frac{|\Lambda_j|}{|\Lambda_{j+1}|}>\frac{\frac{5}{6}(1-\frac{1}{15})}{\frac{7}{6}(1+\frac{1}{15})}\left|\frac{\eta^{\mathbf{k}_{j+1}}}{\eta^{\mathbf{k}_j}}\right|=\tfrac{5}{8}\left|\frac{\eta^{\mathbf{k}_{j+1}}}{\eta^{\mathbf{k}_j}}\right|\ge K_1>15,$$

for $j=1,\ldots,t+1$.

Now let $l$ be the smallest positive integer for which $z_l\neq0$. Then

$$\begin{aligned}|\sum_{j=1}^{t+1}z_j\Lambda_j|=|\sum_{j=l}^{t+1}z_j\Lambda_j|&\ge|z_l||\Lambda_l|-Z(|\Lambda_{l+1}|+\ldots+|\Lambda_{t+1}|)\\&\ge|\Lambda_l|-(t+1)^{t/2}K^t|\Lambda_l|\left(\frac{1}{K_1}+\frac{1}{K_1^2}+\ldots\right)\\&=|\Lambda_l|(1-(t+1)^{t/2}K^t(K_1-1)^{-1})>0.\end{aligned}$$

Therefore,

$$\begin{aligned}2\pi\le|\sum_{j=l}^{t+1}z_j\Lambda_j|&\le Z(|\Lambda_{l+1}|+\ldots+|\Lambda_{t+1}|)\\&\le Z|\Lambda_1|\left(1+\frac{1}{K_1}+\frac{1}{K_1^2}+\ldots\right)\le|\Lambda_1|Z/(1-\tfrac{1}{15})\\&\le\tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_1}|^{-1}(t+1)^{t/2}K^t\times\tfrac{15}{14},\end{aligned}$$

which proves Lemma 1.

Of course, the absolute constants given here can certainly be improved a little, but doing that would not change the proof of the Theorem.

In the sequel $m^+$ denotes $\max\{|m|, 3\}$.

**Lemma 2.** *All solutions $x, y$ to the equation* (1) *satisfy*

$$\log(\max\{|x|, |y|\}) < 3^{3(n+9)} n^{18(n+1)} 2^{2(n-1)^2} M^{2n-2} ((n-1)\log 2 + \log M)^{2n-1} \log m^+.$$

*Proof.* See [4], Theorem 3, §3.3, noting that $H \leq 2^{n-1}M$.

Let $\mathbb{K}$ be an algebraic number field of degree $n$ and discriminant $D_{\mathbb{K}}$. Denote by $S$ a finite set of absolute values of $\mathbb{K}$, including the set $S_\infty$ of all the archimedean values. Set $t = \operatorname{Card} S$. Let $P$ be the maximum of the norms of the prime ideals corresponding to nonarchimedean values of $S$ (if $S = S_\infty$ we set $P = 2$). As usual, a nonzero element $\gamma \in \mathbb{K}$ is said to be an $S$-unit if $|\gamma|_v = 1$ for all $v \notin S$. The $S$-units of $\mathbb{K}$ form a finitely generated multiplicative subgroup $U_S$ of $\mathbb{K}^*$.

The symbol $h(\ )$ denotes the absolute logarithmic height.

**Lemma 3.** *There are $S$-units $\pi_1, \ldots, \pi_{t-1}$ in $\mathbb{K}$ so that each $\gamma \in U_S$ can be written as a product*

$$\gamma = \rho \pi_1^{k_1} \cdots \pi_{t-1}^{k_{t-1}},$$

*with $\rho$ a root of unity and*

$$\max_{1 \leq i \leq t-1} |k_i| \leq (t!)^2 \big(\log(3n)\big)^3 h(\gamma).$$

*Proof.* This follows from relation (26) in [3].

**Lemma 4.** *Let $\alpha$ be a zero of the polynomial $F(X, 1)$ and let $D_{\mathbb{K}}$, $R_{\mathbb{K}}$, $h_{\mathbb{K}}$ denote the discriminant, regulator and class number of the field $\mathbb{K} = \mathbb{Q}(\alpha)$, respectively. Then*

$$|D_{\mathbb{K}}| \leq n^n M^{2n-2}, \qquad h_{\mathbb{K}} R_{\mathbb{K}} < n^{4n} M^{2(n-1)}, \quad \text{and} \quad 0.056 < R_{\mathbb{K}}.$$

*Proof.* We note that $D_{\mathbb{K}}$ divides the discriminant of $F(X, 1)$, so the upper bound for the discriminant follows from an estimate of Mahler [6], Theorem 1, p. 261. The upper bound for the product of the class number by the regulator may be deduced from a result of Siegel's [7], Satz 1, p. 72. Finally the lower bound for the regulator is due to Zimmert [8], Korollar, p. 375.

We denote the maximum of the absolute values of the conjugates of an algebraic number $\alpha$ by $\lceil \alpha \rceil$ (Kurt Mahler called this 'house' of $\alpha$).

**Lemma 5.** *Let $\alpha$ be a non-zero element in $\mathbb{K}$ with $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N$. There exists a unit $\epsilon$ such that*

$$\overline{|\alpha\epsilon|} \leq N^{1/n} \exp\left\{ (6rn^2/\log n)^r \, \tfrac{1}{2} r R_{\mathbb{K}} \right\},$$

*where $r$ is the unit rank of $\mathbb{K}$.*

*Proof.* See [5], Lemma 3.

**Lemma 6.** *Set $C = 2m(2\sqrt{n}M)^n$ and assume $y \neq 0$. Then*

$$\min_{\alpha, F(\alpha,1)=0} \min(1, |\alpha - x/y|) \leq \frac{C}{2(\max(|x|,|y|))^n}$$

*Proof.* See [1], Lemma 1.

**Remark.** If $y^n > C/2$ then obviously

$$\min_{\alpha, F(\alpha,1)=0} |\alpha - x/y| \leq C/2y^n.$$

Consider two distinct solutions $(x, y)$, $(x', y')$ with $y' \geq y > (C/2)^{1/n}$ such that

$$|\alpha_1 - x/y| = \min_i |\alpha_i - x/y| \quad \text{and} \quad |\alpha_1 - x'/y'| = \min_i |\alpha_i - x'/y'|.$$

Then we have

$$\frac{1}{yy'} \leq \left| \frac{x}{y} - \frac{x'}{y'} \right| \leq \left| \frac{x}{y} - \alpha_1 \right| + \left| \alpha_1 - \frac{x'}{y'} \right| \leq \frac{C}{2y^n} + \frac{C}{2y'^n} \leq \frac{C}{y^n}.$$

Hence

$$\frac{y^{n-1}}{C} \leq y'.$$

From now on we denote the zeros of the polynomial $F(X, 1)$ by $\alpha_1, \ldots, \alpha_n$. If $(x_1, y_1), \ldots, (x_j, y_j)$ are solutions to (1) satisfying $(C/2)^{1/n} < y_1 \leq \ldots \leq y_j$, and for $k = 1, \ldots, j$,

$$\min_{1 \leq i \leq n} |\alpha_i - x_k/y_k| = |\alpha_1 - x_k/y_k|,$$

then by induction we obtain, compare the *strong gap principle* at [1], p. 73,

$$\left( y_1 \,/\, C^{1/(n-2)} \right)^{(n-1)^{j-1}} \leq y_j.$$

**Lemma 7.** *Suppose $y_1 \geq 20n^2(M^n m)^{\mu(n)}$, where $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. Set $c_1 = n(n-1)^{j-3} - (n^2+3n)$, $c_2 = \frac{1}{2}n(n-1)^{j-3} - \frac{1}{2}n^2$, $c_3 = n^2(n-1)^{j-3} - n^2$, and $c_4 = n(n-1)^{j-3} - n$; and write*

$$R_j = \left| \frac{x_{j+1} - \alpha_2 y_{j+1}}{x_{j+1} - \alpha_1 y_{j+1}} \right| \Big/ \left| \frac{x_j - \alpha_2 y_j}{x_j - \alpha_1 y_j} \right|.$$

*Then for $j > 4$ we have*

(a) $y_j > (2\sqrt{n} m M^n)^{(n-1)^{j-3}}$;

(b) $\frac{1}{2}y_j|\alpha_i-\alpha_1| \le |x_j-\alpha_i y_j| \le \frac{3}{2}y_j|\alpha_i-\alpha_1|$ *for* $i=2, 3. \ldots, n$;

(c) $R_j \ge 2^{c_1}n^{c_2}M^{c_3}m^{c_4}$; *and*

(d) $|\alpha_1-\alpha_3|/|\alpha_2-\alpha_3|\cdot|x_j-\alpha_2 y_j|/|x_j-\alpha_1 y_j| \ge \frac{1}{2}\cdot y_j^n/(2nM^3)^{n-1} \ge 6.$

*Proof.* a) On noting that, for $n \ge 3$,

$$2^{\frac{n+1}{n-2}+\frac{1}{(n-1)^2}} < 20 \quad \text{and} \quad (\sqrt{n})^{\frac{n}{n-2}+\frac{1}{(n-1)^2}} < n^2,$$

and since

$$y_1 > C^{1/(n-2)}(2\sqrt{n}mM^n)^{\frac{1}{(n-1)^2}} = 2^{\frac{n+1}{n-2}+\frac{1}{(n-1)^2}}(\sqrt{n})^{\frac{n}{n-2}+\frac{1}{(n-1)^2}}(M^n m)^{\frac{1}{n-2}+\frac{1}{(n-1)^2}},$$

we deduce that

$$\left(y_1\cdot C^{-1/(n-2)}\right)^{(n-1)^2} > 2\sqrt{n}mM^n,$$

which proves inequality (a).

b) Let $a$ denote the leading coefficient of the polynomial $F(X,1)$. From a result of Bombieri and Schmidt [1] (p. 72, proof of Lemma 1), we deduce that

$$\prod_{i=2}^{n}|\alpha_i-\alpha_1| = |F'(\alpha_1,1)|/|a| \ge |F'(\alpha_1,1)|/M \ge n^{-(n-1)/2}M^{-(n-1)}.$$

But, for $2 \le k \le n$, we have $\prod_{i=2,i\ne k}^{n}|\alpha_i-\alpha_1| \le (2M)^{n-2}$, whence

$$|\alpha_k-\alpha_1| \ge n^{-(n-1)/2}2^{-(n-2)}M^{-2n+3}.$$

Moreover

$$y_j|\alpha_k-\alpha_1| \ge (2\sqrt{n}M^n m)^{(n-1)^{j-3}}n^{-(n-1)/2}2^{-(n-2)}M^{-2n+3} > 1.$$

Now Lemma 6 yields

$$|x_j-\alpha_1 y_j| \le \frac{C}{2(2\sqrt{n}M^n m)^{(n-1)^{j-3}(n-1)}} \le \frac{1}{2},$$

and, finally, the inequalities

$$|x_j-\alpha_i y_j| \le |x_j-\alpha_1 y_j|+|\alpha_i-\alpha_1|y_j \quad \text{and} \quad |x_j-\alpha_i y_j| \ge |\alpha_i-\alpha_1|y_j-|x_j-\alpha_1 y_j|$$

complete the proof of inequality (b).

c) Using the inequalities (b) we have, for $2 \le i \le n$,

$$\left|\frac{x_{j+1}-\alpha_i y_{j+1}}{x_j-\alpha_i y_j}\right| \ge \frac{\frac{1}{2}|\alpha_i-\alpha_1|y_{j+1}}{\frac{3}{2}|\alpha_i-\alpha_1|y_j} = \frac{y_{j+1}}{3y_j}.$$

Hence

$$\left|\frac{x_j-\alpha_1 y_j}{x_{j+1}-\alpha_1 y_{j+1}}\right| = \frac{\frac{m}{|a|}\prod_{i=2}^{n}|x_{j+1}-\alpha_i y_{j+1}|}{\frac{m}{|a|}\prod_{i=2}^{n}|x_j-\alpha_i y_j|} \ge \left(\frac{y_{j+1}}{3y_j}\right)^{n-1}.$$

Thus we obtain

$$R_j \ge \left(\frac{y_{j+1}}{3y_j}\right)^n \ge \left(\frac{y_j^{n-2}}{3C}\right)^n \ge \left(\frac{y_j}{3C}\right)^n > \left(\frac{(2\sqrt{n}M^n m)^{(n-1)^{j-3}}}{8(2\sqrt{n}M)^n m}\right)^n,$$

and this gives the announced values for the exponents $c_1$, $c_2$, $c_3$, and $c_4$.

d) Define

$$S_j = \frac{|\alpha_1 - \alpha_3|}{|\alpha_2 - \alpha_3|} \cdot \frac{|x_j - \alpha_2 y_j|}{|x_j - \alpha_1 y_j|}.$$

We bound $S_j$ from below as follows. Using (b) twice, we first obtain

$$S_j \geq \frac{|\alpha_1 - \alpha_3|}{|\alpha_1 - \alpha_2| + |\alpha_1 - \alpha_3|} \cdot \frac{\frac{1}{2} y_j |\alpha_2 - \alpha_1|}{|x_j - \alpha_1 y_j|},$$

and next we find that

$$\frac{m}{|a|} = |x_j - \alpha_1 y_j| \cdot |x_j - \alpha_2 y_j| \cdots |x_j - \alpha_n y_j| \geq |x_j - \alpha_1 y_j| \cdot \frac{y_j^{n-1}}{2^{n-1}} \cdot |\alpha_2 - \alpha_1| \cdots |\alpha_n - \alpha_1|.$$

Hence we have

$$\frac{1}{|x_j - \alpha_1 y_j|} \geq \frac{y_j^{n-1}}{2^{n-1}} \cdot \frac{|a|}{m} \cdot |\alpha_2 - \alpha_1| \cdots |\alpha_n - \alpha_1| \geq \frac{y_j^{n-1}}{2^{n-1}} \cdot |F'(\alpha_1, 1)|,$$

and therefore

$$S_j \geq \frac{y_j^n}{2^n} \cdot \frac{|F'(\alpha_1, 1)|}{\frac{1}{|\alpha_2 - \alpha_1|} + \frac{1}{|\alpha_3 - \alpha_1|}}.$$

Combining this lower bound with

$$|F'(\alpha_1, 1)| \geq n^{-(n-1)/2} M^{-(n-2)}$$

and

$$\frac{1}{|\alpha_2 - \alpha_1|} + \frac{1}{|\alpha_3 - \alpha_1|} \leq 2n^{(n-1)/2} 2^{n-2} M^{2n-3},$$

we deduce that

$$S_j \geq \frac{y_j^n}{2^{2n-1} n^{n-1} M^{3n-5}}.$$

This proves the first part of the bound (d). The second part then follows from (a).

# 3. Proof of the Theorem

We fix an arbitrary solution $(x, y)$ to (1) satisfying (2) and with $y > 0$. Recall that $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. We first show that

$$y \geq 20n^2 M^4 m^{\mu(n)}. \tag{3}$$

Indeed, if $|x| \leq |y|$, then (3) is a consequence of (2), while if $\max\{|x|, |y|\} = |x|$, then there is a zero $\alpha$ of $F(X, 1)$ such that

$$m^{1/n} \geq (m/|a|)^{1/n} \geq |x - \alpha y| \geq |x| - |\alpha| y \geq 21n^2 M^5 m^{\mu(n)} - My.$$

Therefore, $y \geq M^{-1}(21n^2 M^5 m^{\mu(n)} - m^{1/n})$, which implies (3).

For $k = 1, \ldots, n$, let $(x_1, y_1), \ldots, (x_{N_k}, y_{N_k})$ be the sequence of solutions to (1) satisfying

$$20n^2 M^4 m^{\mu(n)} \leq y_1 \leq y_2 \leq \ldots \leq y_{N_k},$$

with

$$|\alpha_k - x_j/y_j| = \min_i |\alpha_i - x_j/y_j|, \qquad (1 \le j \le N_k).$$

There are at most $n$ solutions $(x, y)$ of (1) with $y = 0$. Therefore the number of solutions of (1) is bounded by $N_1 + \cdots + N_n + n$. It now suffices to prove $N_k \le 2n(s+1) + 12$, for each $k$, and by symmetry, for some $k$. Thus we produce the desired upper bound only for $N_1$. Therefore, from now on, we consider only solutions $(x, y)$ of (1) for which

$$\min_{1 \le i \le n} |\alpha_i - x/y| = |\alpha_1 - x/y|.$$

For clarity we divide the argument into four steps.

*Step* 1 (On the ideal factors of $x - \alpha_1 y$). Set $\mathbb{K} = \mathbb{Q}(\alpha_1)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s_1}$ be the distinct (finite) prime divisors of $m$ in $\mathbb{K}$. Then the integer $s_1$ satisfies

$$0 \le s_1 \le ns \le n \log_2 m,$$

where $\log_2$ denotes the logarithm to base 2.

Let $\mathfrak{A}$ denote the denominator of the principal ideal $\langle \alpha_1 \rangle_{\mathbb{K}}$. Then $\mathfrak{A}$ can uniquely be written in the form

$$\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2,$$

where $\mathfrak{A}_1$ and $m$ are relatively prime and where every prime divisor of $\mathfrak{A}_2$ divides $m$ (that is, $\mathfrak{A}_1$ is the $m$-free part of $\mathfrak{A}$). For a prime $\mathfrak{P}$ of $\mathbb{K}$, denote by $v_{\mathfrak{P}}$ the corresponding valuation (both of an element of $\mathbb{K}$, and of an ideal of $\mathbb{K}$). Since $\mathfrak{A}(x - \alpha_1 y)$ is an integral ideal of $\mathbb{K}$, we have $v_{\mathfrak{P}}(x - \alpha_1 y) \ge -v_{\mathfrak{P}}(\mathfrak{A})$ for any $\mathfrak{P}$. Further, since $\mathfrak{A} | a$, we also have $v_{\mathfrak{P}}(\mathfrak{A}) \le v_{\mathfrak{P}}(a)$. Moreover, since $F(X, Y)$ is the product of $X - \alpha_1 Y$ by a form whose coefficients are algebraic integers of $\mathbb{K}$, we must have $v_{\mathfrak{P}}(x - \alpha_1 y) \le v_{\mathfrak{P}}(m)$. Therefore we may write

$$\langle x - \alpha_1 y \rangle_{\mathbb{K}} = \mathfrak{A}_1^{-1} \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_{s_1}^{l_{s_1}}, \tag{4}$$

where the exponents $l_i = v_{\mathfrak{p}_{s_i}}(x - \alpha_1 y)$ are rational integers which satisfy

$$\mathfrak{p}_i^{-l_i} | a \quad \text{if} \quad l_i < 0, \quad \text{or} \quad \mathfrak{p}_i^{l_i} | m \quad \text{if} \quad l_i > 0.$$

Thus we get the bound

$$\max_{1 \le i \le s_1} |l_i| \le \log_2 |am|^n \le n \log_2 (Mm).$$

*Step* 2 (On the application of Lemmas 2, 3, 4, and 5). Let $h_{\mathbb{K}}$ be the ideal class number of $\mathbb{K}$. From Lemma 5 we see that there is a generator $\tau$ of the ideal $\left(\mathfrak{A}_1^{-1}\right)^{h_{\mathbb{K}}}$ satisfying

$$|\overline{\tau}| \le \left(N(\mathfrak{A}_1^{-1})\right)^{h_{\mathbb{K}}/n} \cdot \exp\left\{ \left(6rn^2/\log n\right)^r \tfrac{1}{2} r R_{\mathbb{K}} \right\},$$

and that for $i = 1, \ldots, s_1$ there are generators $\pi_i$ of the ideals $\mathfrak{p}_i^{h_{\mathbb{K}}}$, respectively, so that

$$|\overline{\pi_i}| \le (N(\mathfrak{p}_i))^{h_{\mathbb{K}}/n} \cdot \exp\left\{ \left(6rn^2/\log n\right)^r \tfrac{1}{2} r R_{\mathbb{K}} \right\}.$$

But the inequalities

$$r < n, \quad N(\mathfrak{A}_1^{-1}) \le |a| \le M, \quad N(\mathfrak{p}_i) \le m, \quad R_{\mathbb{K}} \le h_{\mathbb{K}} R_{\mathbb{K}} \le n^{4n} M^{2(n-1)},$$
$$\text{and} \quad h_{\mathbb{K}} \le (0.056)^{-1} n^{4n} M^{2(n-1)} < 20 n^{4n} M^{2(n-1)}$$

imply

$$\max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \le (mM)^{h_{\mathbb{K}}/n} \exp\left\{ \left(6n^3/\log n\right)^n \tfrac{1}{2} n \cdot n^{4n} M^{2(n-1)} \right\}.$$

Hence

$$\log \max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \le 20 n^{4n-1} M^{2(n-1)} \log(mM) + 6^n n^{7n+1} M^{2(n-1)}$$
$$\le n^{9n} M^{2n-2} \log(m^+ M).$$

By taking the $h_{\mathbb{K}}$-th power of (4) we get

$$(x - \alpha_1 y)^{h_{\mathbb{K}}} = \epsilon \tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}, \tag{5}$$

where $\epsilon$ is an ordinary unit in $\mathbb{K}$. We need an upper bound for the height of $\epsilon$. First, we estimate the height of $x - \alpha_1 y$. We claim that

$$h(x - \alpha_1 y) \le 3^{2n^2 - n + 21} n^{20(n+1)} M^{4n} \log m^+. \tag{6}$$

The proof of (6) rests on Lemma 2. Indeed, according to this Lemma, we have

$$h(x - \alpha_1 y) \le h(\alpha_1) + \log(|x| + |y|)$$
$$\le 2 \cdot 3^{3(n+9)} n^{18(n+1)} 2^{2(n-1)^2} M^{2n-2} ((n-1)\log 2 + \log M)^{2n-1} \log m^+.$$

The claim (6) then follows from

$$3^{3n+27} 2^{2(n-1)^2+1} ((n-1)\log 2 + \log M)^{2n-1} \le 3^{2n^2-n+21} n^{2(n+1)} M^{2(n+1)}.$$

Next we notice that

$$h(\tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}) \le n^{9n+5} M^{2n-1} (\log m^+)(\log(m^+ M))^2.$$

But this is a consequence of the inequalities $s_1 \le n \log_2 m$, $\max |l_i| \le n \log_2(mM)$,

$$\max\{h(\tau), h(\pi_i)\} \le n \log \max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \le n^{9n+1} M^{2n-1} \log m^+$$

and

$$1 + n^2 (\log_2 m) \log_2(mM) \le n^4 (\log m^+) \log(m^+ M).$$

From these two upper bounds we deduce the desired estimate for the height of $\epsilon$, namely

$$h(\epsilon) \le h_{\mathbb{K}} h(x - \alpha_1 y) + h(\tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}) \le n^{2n^2+23n+44} M^{6n-2} (\log m^+)^3.$$

Let $\rho_0$ be a generator of the group of roots of unity in $\mathbb{K}$. For later purposes we denote the order of $\rho_0$ by $w_{\mathbb{K}}$. Applying Lemma 3, we produce a fundamental system of units for $\mathbb{K}$, say $\epsilon_1, \ldots, \epsilon_r$, such that $\epsilon$ can be written in the form

$$\epsilon = \rho_0^{q_0} \epsilon_1^{q_1} \cdots \epsilon_r^{q_r},$$

with

$$\max_{0\le i\le r}(|q_i|) \le ((r+1)!)^2\,(\log(3n))^3\,h(\epsilon)$$
$$\le n^{4n}\cdot n^{2n^2+23n+44}M^{6n-2}(\log m^+)^3$$
$$\le n^{2n^2+27n+44}M^{6n-2}(\log m^+)^3.$$

We choose an automorphism $\sigma_i$ of $\mathbb{C}$ for each $i=1,\dots,n$, such that $\sigma_i(\alpha_1)=\alpha_i$. Then we obtain

$$\left(\frac{x-\alpha_i y}{x-\alpha_1 y}\right)^{h_{\mathbb{K}}} = \frac{\sigma_i(\epsilon\tau\pi_1^{l_1}\cdots\pi_{s_1}^{l_{s_1}})}{\epsilon\tau\pi_1^{l_1}\cdots\pi_{s_1}^{l_{s_1}}}.$$

*Step* 3 (On the way to the application of Lemma 1). Set $t=r+s_1+2$. Then we have

$$t\le n(s+1)+1\le n(1+\log_2 m^+)+1\le 3n\log m^+.$$

Now define

$$\lambda=\frac{\alpha_3-\alpha_1}{\alpha_3-\alpha_2},\qquad \mu=\frac{\alpha_1-\alpha_2}{\alpha_3-\alpha_2}$$

and write $\eta_1=(\sigma_2(\tau)/\tau)^{1/h_{\mathbb{K}}}$, $\eta_2=(\sigma_2(\epsilon_1)/\epsilon_1)^{1/h_{\mathbb{K}}}$, $\dots$, $\eta_{r+1}=(\sigma_2(\epsilon_r)/\epsilon_r)^{1/h_{\mathbb{K}}}$; $\eta_{r+2}=(\sigma_2(\pi_1)/\pi_1)^{1/h_{\mathbb{K}}},\dots,\eta_{r+s_1+1}=(\sigma_2(\pi_{s_1})/\pi_{s_1})^{1/h_{\mathbb{K}}}$ and $\psi_1=(\sigma_3(\tau)/\tau)^{1/h_{\mathbb{K}}}$, $\psi_2=(\sigma_3(\epsilon_1)/\epsilon_1)^{1/h_{\mathbb{K}}}$, $\dots$, $\psi_{r+1}=(\sigma_3(\epsilon_r)/\epsilon_r)^{1/h_{\mathbb{K}}}$, $\psi_{r+2}=(\sigma_3(\pi_1)/\pi_1)^{1/h_{\mathbb{K}}}$, $\dots$, $\psi_{r+s_1+1}=(\sigma_3(\pi_{s_1})/\pi_{s_1})^{1/h_{\mathbb{K}}}$, where the $h_{\mathbb{K}}$-th roots are fixed. Further, set $k_1=q_0$, $k_2=q_1,\dots,k_{r+1}=q_r$, $k_{r+2}=l_1,\dots,k_{r+s_1+1}=l_{s_1}$.

Eliminating $x$ and $y$ between the three linear forms $x-\alpha_1 y$, $x-\alpha_2 y$, and $x-\alpha_3 y$ yields (the so-called) *Siegel's identity*

$$(\alpha_1-\alpha_2)(x-\alpha_3 y)+(\alpha_2-\alpha_3)(x-\alpha_1 y)+(\alpha_3-\alpha_1)(x-\alpha_2 y)=0,$$

or

$$\frac{\alpha_3-\alpha_1}{\alpha_3-\alpha_2}\frac{x-\alpha_2 y}{x-\alpha_1 y}+\frac{\alpha_1-\alpha_2}{\alpha_3-\alpha_2}\frac{x-\alpha_3 y}{x-\alpha_1 y}=1.$$

That is,

$$\lambda\,(\sigma_2(\rho)/\rho)^{k_0}\,\eta_1^{k_1}\cdots\eta_{t-1}^{k_{t-1}}+\mu\,(\sigma_3(\rho)/\rho)^{k_0}\,\psi_1^{k_1}\cdots\psi_{t-1}^{k_{t-1}}=1, \tag{7}$$

where $\rho$ is a $w_{\mathbb{K}}h_{\mathbb{K}}$-th primitive root of unity, and $k_0\le\omega_{\mathbb{K}}h_{\mathbb{K}}$.

Notice that none of $\lambda$, $\mu$, $\rho$, $\eta_1,\dots,\eta_{t-1}$, $\psi_1,\dots,\psi_{t-1}$, nor $\sigma_2$, $\sigma_3$ depend on the selected solution of (1). Moreover, the mapping $(x,y)\to(k_0,k_1,\dots,k_{t-1})$ is injective. Indeed, $(x-\alpha_1 y)^{h_{\mathbb{K}}}=(x'-\alpha_1 y')^{h_{\mathbb{K}}}$, with $x$, $y$, $x'$, $y$ in $\mathbb{Z}$, implies $x=x'$ and $y=y'$; notice that $\alpha_1$ is real and that $y$, $y'$ are positive. Therefore we obtain at least $N_1$ distinct solutions $(k_0,\dots,k_{t-1})$ to (7).

*Step* 4 (Final step). We define the integer $K$ as in Lemma 1. Hence

$$K\le 2\max_{0\le i\le t-1}\max\{2,|k_i|\}\le 2n^{2n^2+27n+44}M^{6n-2}(\log m^+)^3$$
$$\le n^{2n^2+27n+45}M^{6n-2}(\log m^+)^3.$$

With the notation of Lemma 1 and Lemma 7, we have

$$\eta^{k_j} = \frac{x_j - \alpha_2 y_j}{x_j - \alpha_1 y_j} \qquad \text{and} \qquad R_j = |\eta_{k_{j+1}}/\eta_{k_j}|.$$

However, in order to apply Lemma 1 we need to check the lower bounds

$$R_j \geq 9(t+1)^{t/2}K^t \qquad \text{and} \qquad |\lambda\eta^{k_1}| \geq 6.$$

The latter one follows from part (d) in Lemma 7. To prove the first, it is shown by part (c) of Lemma 7 that it suffices to notice that, for $j \geq t+10$, we have

$$2^{c_1} n^{c_2} M^{c_3} m^{c_4} \geq 9(3n \log m^+)^{t/2} (n^{2n^2+27n+45} M^{6n-2} (\log m^+)^3)^t,$$

where $c_1$, $c_2$, $c_3$ and $c_4$ (which depend on $n$ and $j$) are defined in Lemma 7.

We assume $N_1 \geq 2t+11$, and apply Lemma 1 using the solutions $(x_{t+10}, y_{t+10})$, $\ldots$, $(x_{2t+11}, y_{2t+11})$. We obtain

$$|\lambda\eta^{k_{t+10}}| = \left|\frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} \cdot \frac{x_{t+10} - \alpha_2 y_{t+10}}{x_{t+10} - \alpha_1 y_{t+10}}\right| \leq \frac{1}{4}(t+1)^{t/2}K^t$$
$$\leq \frac{1}{4}(3n \log m^+)^{t/2} (n^{2n^2+27n+45} M^{6n-2} (\log m^+)^3)^t.$$

Finally, using part d) of Lemma 7 we get

$$\left|\frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} \cdot \frac{x_{t+10} - \alpha_2 y_{t+10}}{x_{t+10} - \alpha_1 y_{t+10}}\right| > \tfrac{1}{2}\left((2\sqrt{n} M^n m)^{(n-1)^{t+6}n}/4nM^3\right)^{n-1}$$
$$= 2^{(n-1)^{t+7}n-2n+1} n^{\frac{1}{2}(n-1)^{t+7}n-(n-1)} M^{n^2(n-1)^{t+7}-3(n-1)} m^{n(n-1)^{t+7}},$$

which we see to be a contradiction on recalling that $t \geq 3$ and comparing the exponents of the absolute constant, and of $n$, $M$ and $m$.

That means that $N_1$ is at most $2t+10$ and, as we saw at the beginning of the proof, this shows that the number of solutions of (1) satisfying (2) is at most $n(2t+11)$. This completes the proof of the Theorem.

**Acknowledgements.** The work of Béla Brindza was supported by grant D23992 from the Hungarian National Foundation for Scientific Research, and that of Ákos Pinter by grants 16975 and 19479 from the Hungarian National Foundation for Scientific Research and the Hungarian Academy of Sciences. Alf van der Poorten's research was supported in part by a grant from the Australian Research Council.

**Added in proof.** As kindly pointed out to us by Yann Bugeaud, one deduces from the proof of the first author's paper *On large values of binary forms*, Rocky Mountain J. Math. 26 (1996), 839–845, that the equation $|F(x,y)| = m$ has at most $6n$ solutions satisfying

$$H(x,y) \geq m^{1/(n-2)+1/(n-1)}.$$

## References

[1] Bombieri, E., Schmidt, W.M., On Thue's equation. Invent. Math. 88 (1987), 69–81.

[2] Brindza, B., On large values of binary forms. Rocky Mountain J. Math. 26 (1996), 839–845.

[3] Bugeaud, Y., Győry, K., Bounds for the solutions of unit equations. Acta Arith. 74 (1996), 67–80.

[4] — Bounds for the solutions of Thue-Mahler equations and norm form equations. Acta Arith. 74 (1996), 273–292.

[5] Győry, K., On the solutions of linear diophantine equations in algebraic integers in bounded norm. Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 22/23 (1979–1980), 225–233.

[6] Mahler, K., An inequality for the discriminant of a polynomial. Michigan Math. J. 11 (1964), 257–262.

[7] Siegel, C.L., Abschätzung von Einheiten. Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1969), 71–86.

[8] Zimmert, R., Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung. Invent. Math. 62 (1981), 367–380.

# Linear independence and divided derivatives of a Drinfeld module. I

*W. Dale Brownawell**

*Dedicated to Andrzej Schinzel*

**Abstract.** In this note we extend work of L. Denis on the linear independence of values of the derivatives of the exponential function of a Drinfeld module. Our results generalize Denis's statements in three main ways: We use divided derivatives (and thus higher order ones), we remove a technical hypothesis on the nature of the Drinfeld module, and we introduce related quasi-periodic functions as well. Continuity of divided derivatives allows us to restate our results in the style of Denis.

1991 Mathematics Subject Classification: 11J72, 11G09.

## 1. Introduction

For a finite field $\mathbb{F}_q$ of characteristic $p$, set $A := \mathbb{F}_q[T]$. Let $\phi$ denote an $A$-Drinfeld module of rank $d > 0$ defined over $\bar{k}^{\text{sep}}$, a separable closure of $\mathbb{F}_q(T)$:

$$\phi(T) = TF^0 + a_1F^1 + \ldots + a_dF^d, \quad a_i \in \bar{k}^{\text{sep}}, a_d \neq 0.$$

Here $F$ denotes the $q$-power Frobenius $F : x \mapsto x^q$. The exponential function corresponding to $\phi$,

$$e(z) = z + \sum_{h>0} c_h z^{q^h},$$

is determined by the functional equation

$$e(Tz) = \phi(T)e(z), \tag{1}$$

and so all $c_h \in \bar{k}^{\text{sep}}$. Moreover $e(z)$ is an entire function; that is, $e(z)$ converges on all of $\mathbf{C}_p$, a completion of an algebraic closure of $k_\infty := \mathbb{F}_q((1/T))$.

By $D_i, i \geq 0$, denote the $i$th divided derivative with respect to $T$:

$$D_iT^n = \binom{n}{i} T^{n-i}, \quad n \geq 0.$$

* Research supported in part by an NSF grant

$D_i$ extends uniquely to all of $\bar{k}_\infty^{\text{sep}}$, the separable closure of $k_\infty$ [8]. The main properties that we need about the family of hyperderivatives $\{D_i\}$ are developed in the Appendix below. When $a \in \bar{k}_\infty^{\text{sep}}$, we also write $a^{[i]}$ for $D_i a$.

Elements of the non-commutative ring $\mathbf{C}_p\{F\}$ are called *twisted polynomials*. For a twisted polynomial with no scalar term $\delta(T) \in F\mathbf{C}_p\{F\}$, the functional equation

$$\begin{aligned} Q(Tz) &= TQ(z) + \delta(T)e(z) \\ Q(z) &\equiv 0 \mod z^q \end{aligned} \tag{2}$$

determines an entire function $Q(z)$ uniquely. $Q(z)$ is called the *quasi-periodic function related to the bi-derivation determined by* $\delta(T)$. The bi-derivation is called *inner* if there is a twisted polynomial $S \in \mathbf{C}_p\{F\}$ such that $\delta(T) = S\phi(T) - TS$. See [2] for a more complete explanation and further references.

Our main result is the following:

**Theorem 1.** *Let $u \neq 0$ with $e(u) \in \bar{k}^{\text{sep}}$. If $d > 1$, let $\delta(T) \in \bar{k}^{\text{sep}}\{F\}F$ determine a non-inner bi-derivation and let $Q(z)$ be the associated quasi-periodic function. Then the numbers*

$$1, u, e^{[1]}(u), \ldots, e^{[q-1]}(u), Q(u), \ldots, Q^{[q-1]}(u)$$

*are $\bar{k}$-linearly independent. If $d = 1$, then*

$$1, u, e^{[1]}(u), \ldots, e^{[q-1]}(u)$$

*are $\bar{k}$-linearly independent.*

When $d = 1$, all derivations are inner, and all quasi-periodic $Q(z)$ arise algebraically from $e(z)$. Whether $d = 1$ or not, we always have the following result:

**Corollary 1.** *If $u \neq 0$ with $e(u) \in \bar{k}^{\text{sep}}$, then*

$$1, u, e^{[1]}(u), \ldots, e^{[q-1]}(u)$$

*are $\bar{k}$-linearly independent.*

Corollary 1 is equivalent to the following statement:

**Corollary 2.** *If $u \neq 0$ with $e(u) \in \bar{k}^{\text{sep}}$, then*

$$1, u, u^{[1]}, \ldots, u^{[q-1]}$$

*are $\bar{k}$-linearly independent.*

This corollary extends the main statement of L. Denis [5], which amounts to the linear independence of $1, u, u^{[1]}, \ldots, u^{[p-1]}$ when the non-$p$th power coefficients $a_1, \ldots, a_d$ of $\phi(T)$ are polynomials over the $p$th powers of strictly decreasing degree modulo $p$.

**Corollary 3.** *If $\omega$ is a non-zero period of $e(z)$, then the values $1, \omega, \omega^{[1]}, \ldots, \omega^{[q-1]}$ are linearly independent over $\bar{k}$.*

In [5], Denis showed the analogue of the previous result when $\omega$ is Carlitz's analogue of $\pi$. We can rephrase the first two corollaries in the following way:

**Corollary 4.** *If a non-zero $u \in \bar{k}^{\mathrm{sep}}$ is the solution of a non-trivial (possibly inhomogeneous) linear differential equation of order $< q$ over $\bar{k}$, then $e(u)$ is transcendental over $k$.*

I am indebted to William Waterhouse for helpful discussions on the continuity of divided derivatives. I hope to return to the general case of divided derivatives of arbitrary order in a future paper with L. Denis.

## 2. $t$-modules

The setting for the proofs of our main results is that of natural $t$-modules associated to a given Drinfeld module. For in a series of influential papers culminating in [10], [11], J. Yu developed transcendence theory for Drinfeld modules and more generally for $t$-modules as a satisfying analogue of the established characteristic zero theory for commutative algebraic groups.

By a *$t$-module of dimension $N$* we mean a pair $E = ((\mathbb{G}_a)^N, \Phi)$, where

$$\Phi : A \longrightarrow \mathrm{Mat}_{N\times N}(\mathbf{C}_p\{F\})$$

is an injective homomorphism, which we think of as a monomorphism $\Phi : A \longrightarrow \mathrm{End}\,\mathbb{G}_a^N(\mathbf{C}_p)$, such that the difference

$$\mathfrak{N} := d\Phi(T) - TI_N$$

is nilpotent, where $I_N$ denotes the $N \times N$ identity matrix and $d\Phi(T)$ denotes the matrix obtained from $\Phi(T)$ on replacing each entry by its coefficient of $F^0$. According to a theorem of G. Anderson [1] there is a unique $\mathbb{F}_q$-linear entire non-zero map $\mathrm{Exp} = \mathrm{Exp}_\Phi : \mathbb{G}_a^N \longrightarrow \mathbb{G}_a^N$ such that

$$\mathrm{Exp}(d\Phi(T)\mathbf{z}) = \Phi(T)\,\mathrm{Exp}(\mathbf{z}). \tag{3}$$

A *morphism* from the $t$-module $\Phi$ to the $t$-module $\Phi'$ is a matrix $\Psi$ with coefficients from $\mathbf{C}_p\{F\}$ such that

$$\Psi\Phi = \Phi'\Psi.$$

In this case,

$$\mathrm{Exp}_{\Phi'} \circ d\Psi = \Psi \circ \mathrm{Exp}_\Phi\,. \tag{4}$$

By a *sub-$t$-module* of $E$ we mean a connected algebraic subgroup of $E$ which is closed under the action of $\Phi(T)$. As indicated above, a $t$-module in dimension one is a Drinfeld module.

# 3. Derivatives and $T$-action

In a series of papers culminating in [4], [5], L. Denis developed the insight that, by differentiating the functional equation (1) with respect to $T$, one obtains functional equations for the derivatives. When we follow that lead for divided derivatives, using the results of our Appendix, we find

$$\begin{aligned} e^{[1]}(Tz) + z &= \phi^{[1]}(T)e(z) + Te^{[1]}(z) \\ e^{[n]}(Tz) &= \phi^{[n]}(T)e(z) + Te^{[n]}(z) + e^{[n-1]}(z),\ 1 < n < q, \end{aligned} \tag{5}$$

where $\phi^{[n]}(T) := \sum_{i=0}^{d} a_i^{[n]} F^i$ and $e^{[n]}(z) := \sum_{h \geq 0} c_h^{[n]} z^{q^h}$, $c_0 = 1$. Since, as remarked above, all $a_i \in \bar{k}^{\text{sep}} \Longrightarrow$ all $c_h \in \bar{k}^{\text{sep}}$, these definitions make sense. Thus equation (5) provides a natural $q+1$-dimensional $t$-module $\Phi^*(T)$:

$$\Phi^*(T) := \begin{pmatrix} T & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \phi(T) & 0 & 0 & 0 & \dots & 0 \\ -1 & \phi^{[1]}(T) & T & 0 & 0 & \dots & 0 \\ 0 & \phi^{[2]}(T) & 1 & T & 0 & \dots & 0 \\ & & \dots & & & & 0 \\ 0 & \phi^{[q-1]}(T) & & \dots & 0 & 1 & T \end{pmatrix}$$

with exponential function

$$\text{Exp}^* \begin{pmatrix} x \\ y \\ z_1 \\ \vdots \\ z_m \end{pmatrix} = \begin{pmatrix} x \\ e(y) \\ z_1 + e^{[1]}(y) \\ \vdots \\ z_{q-1} + e^{[q-1]}(y) \end{pmatrix}$$

to which transcendence techniques apply just as in [5].

In this paper, we also want to apply our divided derivatives $D_i$ to the defining equations for our quasi-periodic function. Since $\delta(T) \in \bar{k}^{\text{sep}}\{F\}F$, we find from the functional equation (2) that $Q(z) \in \bar{k}^{\text{sep}}[[z]]$ and, since $Q(z) \equiv 0 \mod z^q$,

$$Q^{[j]}(Tz) = \delta^{[j]}(T)e(z) + TQ^{[j]}(z) + Q^{[j-1]}(z),\ 1 \leq j < q, \tag{6}$$

where $\delta^{[j]}(T)$ is obtained from $\delta(T)$ by taking the $j$th divided derivative of each coefficient.

We can put all of these relations together to obtain a single $t$-module $\Phi(T)$:

$$\Phi(T) := \begin{pmatrix} T & 0 & 0 & 0 & \dots & 0 & 0 \\ 0^* & B_{0,0} & 0 & 0 & \dots & 0 & 0 \\ -1^* & B_{0,1} & TI_2 & 0 & \dots & 0 & 0 \\ 0^* & B_{0,2} & I_2 & TI_2 & \dots & 0 & 0 \\ 0^* & \dots & & & \dots & 0 & 0 \\ 0^* & B_{0,q-2} & 0 & 0 & \dots & TI_2 & 0 \\ 0^* & B_{0,q-1} & 0 & 0 & \dots & I_2 & TI_2 \end{pmatrix},$$

where, in the first column, $0^*$ (resp. $-1^*$) denote column vectors $(0,0)^{\mathrm{tr}}$ (resp. $(-1,0)^{\mathrm{tr}}$), and otherwise 0 denotes the $2 \times 2$ zero matrix,

$$B_{0,0} := \begin{pmatrix} \phi(T) & 0 \\ \delta(T) & T \end{pmatrix},$$

and

$$B_{0,j} := \begin{pmatrix} \phi^{[j]}(T) & 0 \\ \delta^{[j]}(T) & 0 \end{pmatrix}, \quad 1 \le j < q.$$

# 4. Independence of divided derivatives

We use a slightly extended version of this $T$-action to prove the following claim, which also holds even if $d = 1$, since the list of $Q^{[i]}(z)$ is empty:

**Theorem 2.** *The functions*

$$\begin{gathered} z; \\ e(z), e^{[1]}(z), \ldots, e^{[i]}(z), \ldots; \\ Q(z), Q^{[1]}(z), \ldots, Q^{[i]}(z), \ldots; \end{gathered}$$

*are algebraically independent over $\mathbf{C}_p$, where $Q(z)$ is any quasi-periodic function related to a non-inner $\phi$-biderivation.*

Our proof makes use of the formal rules of substitution following from differentiating the functional equations (1), (2) for $e(z)$ and $Q(z)$. We introduce variables corresponding to the various functions:

$$\begin{aligned} z &\longleftrightarrow x_{-1} \\ e^{[j]}(z) &\longleftrightarrow x_{j,0}, \quad j = 0, 1, 2, \ldots \\ Q^{[j]}(z) &\longleftrightarrow x_{j,1}, \quad j = 0, 1, 2, \ldots \end{aligned}$$

and order them according to the lexicographical order of the subscripts ($-1$ counts as, say, $(-1,0)$) on the variables.

By taking the divided derivatives of the functional equations (1), (2) for $e(z)$ and $Q(z)$ we obtain expressions

$$\begin{aligned} Q^{[j]}(Tz) &= TQ^{[j]}(z) + Q^{[j-1]}(z) + Q_j(z, e(z), \ldots, e^{[j]}(z)) \\ e^{[j]}(Tz) &= Te^{[j]}(z) + e^{[j-1]}(z) + E_j(z, e(z), \ldots, e^{[\lfloor j/q \rfloor]}), \end{aligned}$$

for *arbitrary* $j$, not just for $j < q$. Note from the generalized product rule and Part (a) of Lemma 1 of the Appendix that these expressions are $\mathbb{F}_q$-linear functions. We use these expressions to define a $T$-action

$$x_{j,0} \longmapsto Tx_{j,0} + x_{j-1,0} + E_j(x_{-1}, x_{0,0}, \ldots, x_{[\lfloor j/q \rfloor],0}) \tag{7}$$

$$x_{j,1} \longmapsto Tx_{j,1} + x_{j-1,1} + Q_j(x_{-1}, x_{0,0}, \ldots, x_{j,0}). \tag{8}$$

on $\mathbf{C}_p[x_{-1}, \ldots, x_{i,j}, \ldots]$.

Note that $E_j$ (and $Q_j$) are $\mathbb{F}_q$-linear expressions involving functions which are smaller than $e^{[j]}(z)$ (and $Q^{[j]}(z)$) with respect to our ordering. This action takes polynomials which are sums of twisted polynomials acting on distinct variables to sums of twisted polynomials acting on distinct variables. If $R$ is a polynomial in the above variables, let us denote by $R_T$ the effect of the $T$-action.

*Proof.* The proof goes by induction on lexicographical ordering of the functions in which the order of derivative counts most and then the ordering $z < e(z) < Q(z)$. This corresponds to ordinary lexicographical ordering according to the subscripts on the variables $x_{-1}, x_{ij}$.

If no derivatives are involved, then the independence of the functions is established implicitly in [9] and explicitly in [2]. There and in the proof below, we repeatedly use Artin's theorem, see Section VI, §12 of [7], that minimal relations on additive functions consist of a sum of twisted polynomials, each involving only one function. Artin's theorem applies because each of the functions is $\mathbb{F}_q$-linear.

In order to start our induction for the general situation, the case that $e^{[1]}(z)$ is the largest function involved in a dependence relation must be treated separately, since its functional equation (5) is atypical, in that it involves $z$. Since we are dealing with additive functions, we know that a minimal relation is given by minimal degree (i.e. no common left factor) twisted polynomials $P_{-1}, P_0, P_1, P_{1,0}$ such that for

$$\boldsymbol{\lambda}_{1,0}(z) := (z, e(z), Q(z), e^{[1]}(z))$$

and

$$R(x_{-1}, x_0, x_1, x_{1,0}) := P_{-1}x_{-1} + P_0x_0 + P_1x_1 + P_{1,0}x_{1,0},$$

$$R(\boldsymbol{\lambda}_{1,0}(z)) = 0. \tag{9}$$

But then also

$$R(\boldsymbol{\lambda}_{1,0}(Tz)) = 0.$$

Moreover from the functional equations (5), we obtain a twisted polynomial $R_T$ such that

$$R(\boldsymbol{\lambda}_{1,0}(Tz)) = R_T(\boldsymbol{\lambda}_{1,0}(z)).$$

We thus see that, if $q^j$ is the highest power of $e^{[1]}(z)$ actually appearing in $R(\boldsymbol{\lambda}_{1,0}(z))$, then the same is true, with its non-zero coefficient multiplied by $T^{q^j}$, in $R_T(\boldsymbol{\lambda}_{1,0}(z))$.

Then however

$$T^{q^j}R(\boldsymbol{\lambda}_{1,0}(z)) - R_T(\boldsymbol{\lambda}_{1,0}(z)) = 0.$$

also gives a polynomial relation on our functions, but which is of lower degree in $e^{[1]}(z)$. Thus by the minimality of the degree of $R$, this new relation is the trivial

identity. That is,

$$R_T(x_{-1}, x_0, x_1, x_{1,0}) = T^{q^j} R(x_{-1}, x_0, x_1, x_{1,0}); \tag{10}$$

so, by looking at the resulting identity in $x_{1,0}$, we see that

$$P_{1,0} = \alpha F^j$$

for some non-zero $\alpha \in \mathbf{C}_p$ and for some $j \geq 0$. Therefore setting $R_T(\boldsymbol{\lambda}_{1,0}(z)) = 0$ shows that

$$\begin{aligned} &R_T(\boldsymbol{\lambda}_{1,0}(z)) = \\ &R(\boldsymbol{\lambda}_{1,0}(Tz)) = P_{-1}(Tz) + \alpha(-z)^{q^j} \\ &\qquad + P_0(\phi(T)e(z)) + P_1(\delta(T)e(z)) + \alpha(\phi^{[1]}(T)e(z))^{q^j} \\ &\qquad + P_1(TQ(z)) + \alpha(Te^{[1]}(z))^{q^j} = 0. \end{aligned}$$

Comparing the coefficients of $x_{-1}^{q^j}$ in (10), we now see that, if $\beta$ is the coefficient of $F^j$ in $P_{-1}$, then

$$\beta T^{q^j} + \alpha(-1)^{q^j} = T^{q^j}\beta.$$

However this equality implies that $\alpha = 0$, contrary to our assumption that the relation (9) actually involves $e^{[1]}(z)$. This contradiction establishes the algebraic independence of $z, e(z), Q(z), e^{[1]}(z)$.

Now we can carry out our induction by mimicking the above proof with the principal difference being that, when we apply the $T$ action to our minimal relation, we do not get a contribution involving $z$ from our largest function, say involving $Q^{[j]}(z)$, but rather a contribution involving only $Q^{[j-1]}(z)$. (Of course, if the largest function involved is of the form $e^{[j]}(z)$ instead, then the contribution involves $e^{[j-1]}(z)$.)

Assume that we have proved that an initial string of our functions, say, the components of

$$\boldsymbol{\lambda}_{j,0}(z) := (z, e(z), Q(z), e^{[1]}(z), Q^{[1]}(z), \ldots, e^{[j]}(z))$$

are algebraically independent, $j \geq 1$. We want to prove the same is true when we adjoin the next largest function, $Q^{[j]}(z)$, i.e. for the components of

$$\boldsymbol{\lambda}_{j,1}(z) := (z, e(z), Q(z), e^{[1]}(z), Q^{[1]}(z), \ldots, e^{[j]}(z), Q^{[j]}(z)).$$

If that were not true, then there would be minimal degree twisted polynomials

$$P_{-1}, P_{0,0}, P_{1,0}, \ldots, P_{j-1,0}, P_{j-1,1}, P_{j,0}, P_{j,1}$$

such that $P_{j,1} \neq 0$, and, for

$$R(x_{-1}, x_{0,0}, \ldots, x_{j,0}, x_{j,1}) := P_{-1}x_{-1} + \sum_{0 \leq r \leq j} \{P_{r,j}x_{r,j} + P_{r,1}x_{r,j}\},$$

$$R(\boldsymbol{\lambda}_{j1}(z)) = 0.$$

Since this relation holds for all values of $z$, it holds when we replace $z$ by $Tz$. That is to say, $R(\boldsymbol{\lambda}_{j1}(Tz)) = 0$. Thus by the $T$-action (7), (8),

$$\begin{aligned} R(\boldsymbol{\lambda}_{j,1}(Tz)) &= R_T(\boldsymbol{\lambda}_{j,1}(z)) \\ &= P^*_{-1}(z) + \sum_{0\le r<j-1} \left\{ P^*_{r,0} e^{[r]}(z) + P^*_{r,1} Q^{[r]}(z) \right\} \\ &\quad + P^*_{j-1,0} e^{[j-1]}(z) + P_{j-1,1}(TQ^{[j-1]}(z)) + P_{j,1} Q^{[j-1]}(z) \\ &\quad + P_{j,0}(Te^{[j]}(z)) + P_{j,1}(TQ^{[j]}(z)) \\ &= 0. \end{aligned}$$

If $P_{j,1} = \alpha F^s +$ lower terms, $\alpha \neq 0$, then we see by the minimality of the degree of $R$ that

$$R_T(\boldsymbol{\lambda}_{j,1}(z)) - T^{q^s} R(\boldsymbol{\lambda}_{j,1}(z)) = 0 \tag{11}$$

is the trivial relation on the coordinates of $\boldsymbol{\lambda}_{j,1}(z)$.

Then on writing $P_{j-1,1} = \beta F^s +$ terms of different degree (may be higher or lower), we see that the coefficient of $Q^{[j-1]}(z)^{q^s}$ in (11) is

$$\beta T^{q^s} - T^{q^s}\alpha - T^{q^s}\beta = 0.$$

Thus we can conclude once again that $\alpha = 0$, contrary to our assumption. The induction step where the next function is $e^{[j]}(z)$, $j > 1$ is very similar, so we omit it. In this way, we arrive at a contradiction as above to find that the functions are algebraically independent.

Note that the proof works even when $d = 1$, by suppressing all mention of $Q$ and its divided derivatives. □

## 5. The derived $t$-modules

Using the functions introduced above, we have an $\mathbb{F}_q$-linear analytic map

$$\boldsymbol{\lambda}(z) : \mathbf{C}_p \longrightarrow \mathbf{C}_p{}^{2q+1}$$

defined by:

$$\boldsymbol{\lambda}(z) := (z; e(z), Q(z); e^{[1]}(z), Q^{[1]}(z); \ldots; e^{[q-1]}(z), Q^{[q-1]}(z))$$

with entries which are algebraically independent. We already have the matrix $\Phi(T)$ which defines an $A$-action on $\mathbb{G}_a^{2q+1}$.

**Theorem 3.** *$\Phi(T)$ determines the unique $t$-module $\Phi$ such that*

- $\Phi(T)(\boldsymbol{\lambda}(z)) = \boldsymbol{\lambda}(Tz)$,
- $(d\Phi(T) - TI_{2q+1})^q = 0$.

*The action on the tangent space is*

$$d\Phi(T) = \begin{pmatrix} T & 0 & 0 & 0 & \dots & 0 & 0 \\ 0^* & TI_2 & 0 & 0 & \dots & 0 & 0 \\ -1^* & I_2 & TI_2 & 0 & \dots & 0 & 0 \\ 0^* & 0 & I_2 & TI_2 & \dots & 0 & 0 \\ 0^* & \dots & & & \dots & 0 & 0 \\ 0^* & \dots & 0 & 0 & \dots & TI_2 & 0 \\ 0^* & \dots & 0 & 0 & \dots & I_2 & TI_2 \end{pmatrix},$$

*where, as before,* $0^* = (0,0)^{\mathrm{tr}}$, $-1^* = (-1,0)^{\mathrm{tr}}$, $0$ *is the* $2\times 2$ *zero matrix, and* $I_2$ *the* $2 \times 2$ *identity matrix. Moreover, for non-zero* $a \in A$, $\mathrm{Card}(\mathrm{Ker}\,\Phi(a)) = q^{d(\deg a)}$.

*Proof.* The matrix for $\Phi$ was defined to reflect the functional equations (5), (6), so the first two claims hold for $\Phi$. Conversely, if $\Psi(T)\boldsymbol{\lambda}(z)) = \boldsymbol{\lambda}(Tz)$, then the algebraic independence of the functions $z, e(z), \dots, Q^{[q-1]}(z)$ shows that $\Psi(T) = \Phi(T)$.

The matrix $\Phi(T)$ is lower triangular with diagonal terms all equal to $a$, except for the $\phi(a)$ in the second position. If $\Phi(a)(z_{-1}, z_{0,0}, z_{0,1}, \dots, z_{q-1,1}) = 0$, then $z_{-1} = 0$ and $z_{0,0}$ is an $a$-torsion point of $\phi$ which determines $z_{0,1}, \dots, z_{q-1,1}$ uniquely. Since $\phi(a)$ is a separable twisted polynomial of degree $d(\deg a)$ in $F$, there are $q^{d(\deg a)}$ $a$-torsion points. The result follows. □

Because of the refinements of [3] and [6], the last item of the theorem is no longer necessary for the applications. We now move on to consider the exponential map Exp of this $T$-module.

**Theorem 4.** *The exponential map* Exp *of* $\Phi$ *is the following:*

$$\mathrm{Exp}(\mathbf{z}) = \mathrm{Exp}\begin{pmatrix} z \\ z_{0,0} \\ z_{0,1} \\ z_{1,0} \\ z_{1,1} \\ \vdots \\ z_{q-1,0} \\ z_{q-1,1} \end{pmatrix} := \begin{pmatrix} z \\ e(z_{0,0}) \\ z_{0,1} + Q(z_{0,0}) \\ z_{1,0} + e^{[1]}(z_{0,0}) \\ z_{1,1} + Q^{[1]}(z_{0,0}) \\ \vdots \\ z_{q-1,0} + e^{[q-1]}(z_{0,0}) \\ z_{q-1,1} + Q^{[q-1]}(z_{0,0}) \end{pmatrix}$$

*The kernel* Ker Exp *is the group*

$$\mathrm{Ker}\,\mathrm{Exp} = \begin{pmatrix} 0 \\ u \\ -Q(u) \\ u^{[1]} \\ -Q^{[1]}(u) \\ \vdots \\ u^{[q-1]} \\ -Q^{[q-1]}(u) \end{pmatrix},$$

*where $e(u) = 0$, i.e. $u$ is a period of the exponential function of the Drinfeld module.* $\operatorname{Ker}\operatorname{Exp}$ *is closed under the $A$-action.*

*Proof.* For the first part, we need only establish that $\Phi(T)\operatorname{Exp}(\mathbf{z}) = \operatorname{Exp}(d\Phi(T)\mathbf{z})$. We consider the entries according to the ordering we have been using:

Top entry: Here the entries are $Tz_{-1}$ and $Tz_{-1}$.

Second entry: Here the entries are $\phi(T)e(z_{0,0})$ and $e(Tz_{0,0})$, whose equality amounts to the Drinfeld functional equation (1).

Third entry: Here the entries are $\delta(T)e(z_{0,0}) + T(z_{0,1} + Q(z_{0,0}))$ and $Tz_{0,1} + Q(Tz_{0,0})$, whose equality is the defining functional equation (2) for $Q(z)$.

Fourth entry: Here the entries are $-z_{-1} + \phi^{[1]}(T)(e(z_{0,0})) + T(z_{1,0} + e^{[1]}(z_{0,0}))$ and $-z_{-1} + Tz_{0,0} + Tz_{1,0} + e^{[1]}(Tz_{0,0})$. The equality amounts to the first case of (5).

$(2j+3)$rd entry, $1 \le j \le q-1$: Here the entries are $\delta^{[j]}(T)e(z_{0,0}) + (z_{j-1,1} + Q^{[j-1]}(z_{0,0})) + T(z_{j,1} + Q^{[j]}(z_{0,0}))$ and $(z_{j-1,1} + Tz_{j,1}) + Q^{[j]}(Tz_{0,0})$, whose equality is the general case of equation (6).

$(2j+2)$nd entry, $2 \le j \le q-1$: Here the entries are $\phi^{[j]}(T)e(z_{0,0}) + (z_{j-1,0} + e^{[j-1]}(z_{0,0})) + T(z_{j,0} + e^{[j]}(z_{0,0}))$ and $(z_{j-1,0} + Tz_{j,0}) + e^{[j]}(Tz_{0,0})$, whose equality is equation (5).

We deduce the first claim of the theorem by the unicity (3) of the exponential function.

Now let $\operatorname{Exp}(\mathbf{u}) = 0$. Then $u_{-1} = 0$ and $e(u_0) = 0$, so $u_0$ is a period of $e$.

Now by the lemmas of the Appendix, since $e(u_0) = 0$, we have also that

$$0 = D_j(e(u_0)) = e^{[j]}(u_0) + D_j(u_0),\ 0 \le j < q.$$

Therefore since also $u_{0,j} + e^{[j]}(u_0) = 0$, we see that $u_{0,j} = u_0^{[j]}$, as claimed. □

Having defined our $t$-module and established its basic properties, we need to refine the arguments of [5] to apply here.

# 6. Proof of Theorem 1

Our proof is based on the following fundamental result [10], [3], [6], due essentially to J. Yu.

**Theorem 5** (Sub-$t$-Module Theorem). *Let the $t$-module $G = (\mathbb{G}_a^n, \Psi)$ be defined over $\bar{k}$. Let $\mathbf{v} \in \operatorname{Lie} G(\mathbf{C}_p)$ with $\operatorname{Exp}_\Psi(\mathbf{v}) \in G(\bar{k})$. Let $V$ be the smallest vector space in $\operatorname{Lie} G(\mathbf{C}_p)$ which contains $\mathbf{v}$, is defined over $\bar{k}$, and is closed under the action of the differential $d\Psi(T)$. Then $V = \operatorname{Lie} H(\mathbf{C}_p)$ for some $t$-submodule $H$ of $G$.*

When $d\Psi(T)$ is badly behaved with respect to the question of $\bar{k}$-linear dependence, we would like to be able to simplify our $t$-module. By the nilpotency of $d\Psi(T) - TI_n$, we are led to consider an appropriate $q$th power of $\Psi$ instead as

a plausible candidate. This is especially appealing because the uniqueness of the exponential function of a $t$-module guarantees that the exponential function of a power of $t$-module is the same as that of the original $t$-module. Therefore $\mathrm{Exp}_\Psi(\mathbf{v})$ is also an algebraic point of the new $t$-module.

Now $\Psi^{q^\nu}$ is, strictly speaking, no longer a $t$-module with respect to $A = \mathbb{F}_q[T]$, but rather with respect to $\widetilde{A} = \mathbb{F}_q[T^{q^\nu}]$. However since $\bar{k} = \overline{\mathbb{F}_q(T^{q^\nu})}$ as well, we can still apply the Sub-$t$-Module Theorem to $(\mathbb{G}_a^n, \Psi^{q^\nu})$, as $\Psi$ (and thus $\Psi^{q^\nu}$) is defined over $\bar{k}$ and the value of their common exponential function at $\mathbf{v}$ has coordinates in $\bar{k}$. Thus we find the following commutative diagram:

$$\begin{array}{ccc} (\mathbb{G}_a^m, \Psi_0) & \xrightarrow{\Xi} & (\mathbb{G}_a^n, \Psi^{q^\nu}) \\ {\scriptstyle \mathrm{Exp}_{\Psi_0}}\uparrow & & \uparrow{\scriptstyle \mathrm{Exp}_{\Psi^{q^\nu}} = \mathrm{Exp}_\Psi} \\ V & \xrightarrow{d\Xi} & \mathbb{G}_a^n \end{array}$$

in which $H = (\mathbb{G}_a^m, \Psi_0)$ and $d\Xi : V \longrightarrow \mathbb{G}_a^n$ is simply inclusion.

However when $q^\nu \geq n$, the action of $d\Psi(T^{q^\nu})$ is scalar multiplication by $T^{q^\nu}$. Therefore the minimal vector space $V$ containing $\mathbf{v}$ which is closed under the action of $d\Psi(T^{q^\nu})$ is simply $V = \mathbf{C}_p\mathbf{v}$, i.e. $H(V) = \mathrm{Exp}_\Psi(\mathbf{C}_p\mathbf{v})$. In particular, we have the following conclusion, which does not involve any conditions on the action of the original differential and which therefore allows us to remove the technical hypothesis occurring in [5].

**Theorem 6** (Linear Independence Criterion). *Let the $t$-module $G = (\mathbb{G}_a^n, \Psi)$ be defined over $\bar{k}$. Let $\mathbf{v} \in \mathrm{Lie}\, G(\mathbf{C}_p)$ with $\mathrm{Exp}_\Psi(\mathbf{v}) \in G(\bar{k})$. If the coordinates of $\mathbf{v}$ are $\bar{k}$-linearly dependent, then the coordinate functions of the one-parameter analytic subgroup $z \longmapsto \mathrm{Exp}_\Psi(z\mathbf{v})$ are algebraically dependent.*

We give a proof of Theorem 1 in the case $d > 1$. When $d = 1$, it suffices to suppress the $Q^{[i]}$ and to work with $(\mathbb{G}_a^{q+1}, \Phi^*)$. We apply the preceding result to $(\mathbb{G}_a^{2q+1}, \Phi)$ with regard to the point $\mathbf{v} = (1, u, -Q(u), -e^{[1]}(u), \ldots, -Q^{[q-1]}(u))$.

Thus we find

$$\mathrm{Exp}(z\mathbf{u}) = \begin{pmatrix} z \\ e(uz) \\ -Q(u)z + Q(uz) \\ -e^{[1]}(u)z + e^{[1]}(uz) \\ -Q^{[1]}(u)z + Q^{[1]}(uz) \\ \vdots \\ -e^{[q-1]}(u)z + e^{[q-1]}(uz) \\ -Q^{[q-1]}(u)z + Q^{[q-1]}(uz) \end{pmatrix}$$

satisfy the non-trivial polynomial relations defining the image of $H$ in $\mathbb{G}_a^{2q+1}$. However, the above coordinates satisfy no non-trivial relation, since $u$ is non-zero and the functions $z, e(z), Q(z), \ldots, e^{[q-1]}(z), Q^{[q-1]}(z)$ are algebraically independent. This contradiction establishes the linear independence of the coordinates of $\mathbf{u}$.

*Proof of Corollary* 2. If $L$ is a finite separable extension of $k$ containing the coefficients $a_i$ of $\phi(T)$, then $L$ contains the coefficients $c_h$ of $e(z)$. Since Denis showed on page 6 of [5] that $u \in \bar{k}_\infty^{\text{sep}}$, we know that the composite $Lk_\infty(u)$ is a finite separable extension of the complete field $k_\infty$ and that $Lk_\infty(u)$ is complete. In particular, by Lemma 2 of the Appendix below, we see that each $D_i$ is continuous on $Lk_\infty(u)$ and hence $D_i(e(u)) = u^{[i]} + \sum_{h>0} D_i(c_h u^{q^h})$. Thus by Lemma 1 of the Appendix we see that, for $i < q$,

$$(e(u))^{[i]} = u^{[i]} + \sum_{h>0} c_h^{[i]} u^{q^h} = u^{[i]} + e^{[i]}(u),$$

and the numbers $e^{[i]}(u)$ differ from $-u^{[i]}$ by algebraic quantities, viz. $(e(u))^{[i]}$. □

This reasoning also complements the arguments given for Theorems 2 and 3 in [5].

# 7. Appendix: Hyperderivatives

Hyperderivatives are useful for power series in positive characteristic as a replacement for ordinary derivatives, which necessarily vanish when taken to an order exceeding the characteristic. Hyperderivatives are families $\{D_i\}_{i=0}^{\infty}$ of linear mappings on an algebra $B$ ($D_0 = id_B$) satisfying the generalized product rule:

$$D_i(ab) = \sum_{j=0}^{i} D_j(a) D_{i-j}(b).$$

The canonical family of hyperderivatives $\{\Delta_i\}$ on $k_\infty$ is given in the following two parts

$$\Delta_i \left(\frac{1}{T}\right)^{-n} = \binom{i}{k} \left(\frac{1}{T}\right)^{i-n}, \quad n > 0,$$

$$\Delta_i \left(\frac{1}{T}\right)^{n} = \binom{n+i-1}{n-1} \left(\frac{1}{T}\right)^{n+i}, \quad n > 0,$$

and by setting $\Delta_i a = 0$ if $a \in \mathbb{F}_q$ and $i > 0$. Here we have used the convention that $\binom{i}{k} = 0$ if $i < k$.

These definitions come from the coefficients of powers of $z$ in the identities

$$(x+z)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} z^k, \quad n > 0,$$

$$\frac{1}{(x+z)^n} = \frac{1}{x^n} \sum_{k=0}^{\infty} \binom{n+k-1}{n-1} \left(\frac{-z}{x}\right)^k, \quad n > 0.$$

A moment's reflection shows that the definition of $\Delta_i$ above gives a family of hyperderivatives on the Laurent polynomials $\mathbb{F}_q[T, 1/T]$, which extends uniquely by continuity to a family of hyperderivatives on $k_\infty$.

It is a general fact that a family of hyperderivatives on any field extends uniquely to the separable closure of the field [8]. We denote the extension of $\{\Delta_i\}_{i=0}^{\infty}$ to $\bar{k}_\infty^{\text{sep}}$ by $\{D_i\}_{i=0}^{\infty}$.

If $f(z) = \sum f_h z^h$, then for simplicity of notation, for each $i$, we define $f^{[i]}(z) := \sum D_i(f_h) z^h$.

We collect here a few useful properties of our family of hyperderivatives:

**Lemma 1.**

(a) *For any* $a \in \bar{k}^{\text{sep}}$,

$$D_k(a^{p^\ell}) = \begin{cases} (D_j(a))^{p^\ell}, & \text{for } k = jp^\ell, \\ 0, & \text{otherwise.} \end{cases}$$

(b) *If* $f(z) = \sum f_h z^{q^h}$, *then for each* $i$,

$$D_i(f(Tz)) = f^{[i]}(Tz) + \sum_h \sum_{j+q^h=i} D_j(f_h) z^{q^h}.$$

(c) *Using* $\phi^{[i]}(T) := D_i(a_1)F^1 + \ldots + D_i(a_d)F^d$ *as above, we find that, when* $i < q$,

$$D_i(\phi(T)e(z)) = e^{[i-1]}(z) + Te^{[i]}(z) + \phi^{[i]}(T)e(z).$$

(d) *If* $a \in \bar{k}^{\text{sep}}$ *and* $D_i(e(a)) = 0$, $\forall j \le i$, *then*

$$0 = e^{[i]}(a) + \sum_h \sum_{\substack{j+\ell q^h=i \\ l>0}} D_j(a_h)(D_\ell(a))^{q^h}.$$

*Proof.* (a): Now

$$D_k(a^{p^\ell}) = \sum_{k_1+\ldots+k_{p^\ell}=k} D_{k_1}(a) \cdots D_{k_{p^\ell}}(a).$$

Let us say the distinct indices occur in the vector $(k_1, \ldots, k_{p^\ell})$ with multiplicities $n_1, \ldots, n_r$. Then the same product occurs in the preceding sum exactly

$$\binom{p^\ell}{n_1, \ldots, n_r}$$

times with the factors in various orders. However $p$ divides this number except when $n_1 = p^\ell, r = 1$, i.e.

$$D_k(a^{p^\ell}) = \begin{cases} (D_j(a))^{p^\ell}, & \text{for } k = jp^\ell, \\ 0, & \text{otherwise,} \end{cases}$$

as claimed.

(b): Writing $f(z) = \sum f_h z^{q^h}$, we see from the product rule for the hyperderivatives $D_i$ that

$$\begin{aligned} D_i(f(Tz)) &= \sum_h D_i(f_h(Tz)^{q^h}) = \sum_h \sum_{j+k=i} D_j(f_h) D_k((Tz)^{q^h}) \\ &= \sum_h D_i(f_h)(Tz)^{q^h} + \sum_{\substack{j+k=i \\ k>0}} D_j(f_h) D_k((Tz)^{q^h}) \\ &= f^{[i]}(Tz) + \sum_h \sum_{\substack{j+k=i \\ k>0}} D_j(f_h) D_k((Tz)^{q^h}). \end{aligned}$$

But $D_k(T^{q^h}) = \binom{q^h}{k} T^{q^h-k}$, and $p \mid \binom{q^h}{k} T^{q^h-k}$, unless $k = q^h$. Therefore we see that

$$D_i(f(Tz)) = \sum_h D_i(f_h(Tz)^{q^h}) = f^{[i]}(Tz) + \sum_h \sum_{j+q^h=i} D_j(f_h)(z)^{q^h},$$

and the latter is an $\mathbb{F}_q$-linear polynomial, say $-R_i(z)$.

(c): In this terminology, recall that

$$\phi(T)e(z) = Te(z) + \phi^{[0]}(T)e(z),$$

$\phi^{[0]}(T) := \phi(T) - TF^0$. Then applying $D_i$ to (7) and recalling part (a) of the Lemma gives the result, since

$$D_i(Te(z)) = e^{[i-1]}(z) + Te^{[i]}(z).$$

(d): This works very nearly as in part (b):

$$0 = D_i(e(a)) = e^{[i]}(a) + \sum_h \sum_{\substack{j+k=i \\ k>0}} D_j(c_h) D_k((a)^{q^h}),$$

and we conclude as before by part (a). □

**Lemma 2.** *The divided derivatives $D_i$ are continuous maps on every finite separable extension $L$ of $k_\infty$.*

*Proof.* Say $L = k_\infty(\alpha)$, $n = [L : k_\infty]$. Since all norms on $L$ extending that on $k_\infty$ are equivalent, it is enough to show that $D_i$ is continuous on $L$ in the "sup" norm:

$$v_L(\lambda) := \min_j \{v(\kappa_j)\}$$

when $\lambda = \sum_{j=0}^{n-1} \kappa_j \alpha^j$ with $\kappa_j \in k_\infty$ and $v(1/T) = 1$. By the product rule,

$$D_i(\lambda) = \sum_j \sum_{r+s=i} D_r(\kappa_j) D_s(\alpha^j).$$

By the strong triangle inequality,

$$v_L\Big(D_i\Big(\sum_j \kappa_j \alpha^j\Big)\Big) \geq \min_{r,j} \{v(D_r(\kappa_j)) v_L(D_{i-r}(\alpha^j))\}.$$

For given $i$, the finitely many $D_s(\alpha^j) = \sum_l \lambda_{jl}^{(s)} \alpha^l, s \leq i$ are fixed. So there is *a priori* a constant $C_i > 0$ such that

$$v_L(D_s(\alpha^j)) \geq -C_i.$$

In addition the $\kappa_j \in k_\infty$, so

$$v(D_r(\kappa_j)) \geq r + v(D_r(\kappa_j)) \geq r + v_L(\lambda).$$

Therefore

$$v_L(D_i(\lambda)) \geq v_L(\lambda) - C_i.$$

This shows that each $D_i$ is continuous on $L$, as claimed. □

## References


[1] Anderson, G., $t$-motives. Duke Math. J. 53 (1986), 457–502.

[2] Brownawell, W.D., Drinfeld exponential and quasi-periodic functions. In: Advances in number theory (ed. by F.Q. Gouvêa and N. Yui), 341–365. Oxford University Press, Oxford 1993.

[3] Brownawell, W.D., Tubbs, R., Zero estimates for $t$-modules. Available by anonymous ftp from `ftp.math.psu.edu/pub/wdb/papers/zero.estimates.ps`.

[4] Denis, L., Transcendance et dérivées de l'exponentielle de Carlitz. In: Séminaire de Théorie de Nombres, Paris 1991–92 (ed. S. David; Progr. Math. 116), 1–21. Birkhäuser, Boston 1993.

[5] — Dérivées d'un module de Drinfeld et transcendance. Duke Math. J. 80 (1995), 1–13.

[6] — Lemmes de multiplicité et $T$-modules. Michigan Math. J. 43 (1996), 67–79.

[7] Lang, S., Algebra, 3rd edn. Addison Wesley, Reading 1993.

[8] Waterhouse, W.C., Notes toward higher differential algebra. J. Pure Appl. Algebra 7 (1976), 121–132.

[9] Yu, J., On periods and quasi-periods of Drinfeld modules. Compositio Math. 74 (1990), 235–245.

[10] — Analytic homomorphisms into Drinfeld modules. Ann. of Math. (2) 145 (1997), 215–233.

[11] — Transcendence in finite characteristic. In: The arithmetic of function fields (ed. by D. Goss, D.R. Hayes, and M.I. Rosen), 253–264. Walter de Gruyter, Berlin 1992.

# Cubic threefolds with six double points

*D.F. Coray, D.J. Lewis,*
*N.I. Shepherd-Barron and Sir Peter Swinnerton-Dyer*

**Abstract.** This note is concerned primarily with cubic threefolds having precisely six singular points in general position in $\mathbb{P}^4_K$, where $K$ is a number field. We prove that the Hasse Principle holds for all varieties $T$ in this class. The result is obtained in a fairly elementary way by studying the family of rational quartic curves lying on $T$ that pass through all the double points. We show that this family is parametrized by a hyperplane section of Segre's ten-nodal cubic threefold.

## 1. Rational normal quartics

We begin by recalling some facts about rational quartic curves in $\mathbb{P}^4$. Here we may assume that the ground field is algebraically closed. More general ground fields will not appear until §3.

Our main tool is the standard Cremona pentahedral transformation $T_4^{\text{pent}}$, which is defined as follows. Given five (distinct) points, say $P_0, \ldots, P_4$, not contained in a common hyperplane, we are free to assume that their expression in coordinates is $(1,0,0,0,0)$, $(0,1,0,0,0)$, $\ldots$, and $(0,0,0,0,1)$. Then the Cremona transformation of $\mathbb{P}^4$ that we are considering is the very obvious involution

$$\Phi\colon (x_0,x_1,x_2,x_3,x_4) \mapsto \Big(\frac{1}{x_0},\frac{1}{x_1},\frac{1}{x_2},\frac{1}{x_3},\frac{1}{x_4}\Big). \tag{1.1}$$

Here $\frac{1}{x_i}$ is an abbreviation for $x_0x_1x_2x_3x_4/x_i$. From this we see that the transformation has degree 4 and is undefined only on the 2-planes where two of the $x_i$ vanish.

Broadly speaking, the hyperplane $\{x_i = 0\}$ is blown down into the opposite vertex of the fundamental pentahedron, which is blown up. The situation can be examined more precisely by renaming the coordinates in the image as $X_0, \ldots, X_4$. Then the birational transformation is identical with the correspondence in $\mathbb{P}^4 \times \mathbb{P}^4$ defined by the equations:

$$x_0X_0 = x_1X_1 = x_2X_2 = x_3X_3 = x_4X_4\,. \tag{1.2}$$

**Lemma 1.1.** *The homaloidal hypersurfaces in $\mathbb{P}^4$, i.e., the elements of the associated linear system $\mathcal{M}$, are all the quartic hypersurfaces on which $P_0, \ldots, P_4$ are (at least) triple.*

*Proof.* Indeed, a quartic hypersurface has a triple point at $P_0$ if and only if each monomial in its equation contains $x_0$ at most to the first power. Repeating this argument at the other vertices $P_i$, we see that the equation is a sum of monomials in $x_0x_1x_2x_3x_4/x_i$, as expected. □

The homaloidal curves of the system, i.e., the inverse images ${}^0\Gamma_4$ of generic straight lines in the second projective space $\mathbb{P}^4$, are rational irreducible curves of degree 4. In fact, their degree can be computed in the first projective space by intersecting with a generic hyperplane. Now, this corresponds in the second projective space to intersecting a straight line with a generic quartic threefold in the inverse linear system, which coincides with $\mathcal{M}$ since $\Phi$ is an involution.

These curves ${}^0\Gamma_4$ span $\mathbb{P}^4$, since they pass through all five points $P_0, \ldots, P_4$. Indeed, a generic straight line in the second space $\mathbb{P}^4$ meets each hyperplane $\{X_i = 0\}$ in a general point, which is blown down by $\Phi^{-1}$ into $P_i$. Such quartics are of course irreducible and smooth.

For future reference it is important to remark that this computation of the degree fails only when the corresponding line meets the fundamental pentahedron on the base locus of $\mathcal{M}$. In fact, the proper transform of a line that meets any of the 2-planes defined by three of the $P_i$ is a curve of degree less than 4, but this is the only case.

**Remark 1.2.** One can also work quite explicitly with parametric representations. Up to the action of $\mathbb{P}\mathrm{GL}_5$, we can assume that $\Gamma$, which is not included in any of the hyperplanes $\{x_i = 0\}$, passes through $P_5 = (1,1,1,1,1)$ and one further point $P_6 = (\bar{x}_0, \ldots, \bar{x}_4)$, general in the sense that the $\bar{x}_i$ are distinct and non-zero. Therefore $\Gamma$ corresponds to the straight line through $\Phi(P_5) = (1,1,1,1,1)$ and $\Phi(P_6) = (1/\bar{x}_0, \ldots, 1/\bar{x}_4)$. This is the image of $\mathbb{P}^1$ under the map:

$$t \mapsto (1 + t/\bar{x}_0, \ldots, 1 + t/\bar{x}_4). \tag{1.3}$$

Hence $\Gamma$ is parametrized by

$$\rho\colon t \mapsto \left(\frac{\bar{x}_0}{\bar{x}_0 + t}, \ldots, \frac{\bar{x}_4}{\bar{x}_4 + t}\right). \tag{1.4}$$

One can also check directly that $\rho(-\bar{x}_i) = P_i$ for $i \leq 4$ and, moreover, $\rho(0) = P_5$ and $\rho(\infty) = P_6$.

Conversely, we are guaranteed to obtain all twisted quartics in this way:

**Lemma 1.3.** *Every smooth irreducible quartic curve $\Gamma_4$ through $P_0, \ldots, P_4$ is a homaloid.*

*Proof.* This means simply that the image of $\Gamma$ under $\Phi$ is a line. Now the degree of the image is equal to its intersection number with a generic hyperplane. This

corresponds to the number of free intersections of $\Gamma$ with a generic quartic threefold $W \in \mathcal{M}$. Our assumption is that $\Gamma$ passes through the vertices, which are triple on $W$. Hence the number of free intersections is at most equal to $4 \cdot 4 - 5 \cdot 3 = 1$. And it cannot be 0, since $\Phi$ is locally an isomorphism off the base locus of $\mathcal{M}$. □

For our purposes a finite set of points in $\mathbb{P}^n$ will be said to be *in general position* if every subset consisting of $m \leq n+1$ points spans a copy of $\mathbb{P}^{m-1}$. For a set of five or more points in $\mathbb{P}^4$, this means simply: '*no five in a common hyperplane*'.

**Corollary 1.4.** *Given seven points in general position in $\mathbb{P}^4$, there is a unique rational, smooth quartic curve ${}^0\Gamma_4$ passing through them.*

*Proof.* After fixing the first five points $P_0, \ldots, P_4$, with coordinates as above, we see that the curve we are looking for corresponds to the unique straight line through the images under $\Phi$ of the remaining two points, $P_5$ and $P_6$. Again we are free to assume that $P_5 = (1,1,1,1,1)$, so that $\Phi(P_5) = P_5$. The discussion leading to Remark 1.2 has shown that the only case where we do not obtain a smooth quartic is when the line meets the base locus of $\mathcal{M}$. However, in this case $\Phi(P_5)$, $\Phi(P_6)$, and three points from among $P_0, \ldots, P_4$ (say, $P_2$, $P_3$ and $P_4$) would lie in a common 3-space, namely $\{X_0 = X_1\}$. But, from the definition of $\Phi$, this would imply: $P_6 \in \{x_0 = x_1\}$, and the five points $P_2, \ldots, P_6$ would lie in a common hyperplane; a contradiction. □

**Remark 1.5.** It follows from the same considerations that the family of rational quartics through six general points in $\mathbb{P}^4$ is birationally parametrized by the family of all straight lines through a fixed point (namely, through the image of $P_5$). Hence it is birationally equivalent to $\mathbb{P}^3$.

This observation is useful, but insufficient for our purpose. Indeed, over a non-algebraically closed ground field it gives rise to a twisted representation: we cannot fix the first five points without introducing an algebraic extension of degree 6 (in general). That is why we shall need to look for some other descriptions of this family.

**Remark 1.6.** This theory extends with virtually no change to rational normal curves of degree $n$ in $\mathbb{P}^n$ for arbitrary $n \geq 2$. The best known case is when $n = 3$ (twisted cubics). We shall refer to it in the proof of Lemma 2.5 below.

## 2. Six and seven points in general position

We now turn to cubic threefolds and analyse the independence of the conditions which express that several points are singular on them.

**Lemma 2.1.** *Given six points in general position in $\mathbb{P}^4$, the linear system $\mathcal{L}$ of cubic threefolds $T$ that are singular at these points has dimension 4.*

*Proof.* Up to the action of $\mathbb{P}\mathrm{GL}_5$, we are free to assume, as before, that the points are expressed in coordinates as $P_0 = (1,0,0,0,0)$, $P_1 = (0,1,0,0,0)$, ..., $P_4 = (0,0,0,0,1)$, and $P_5 = (1,1,1,1,1)$. (This will be a standing assumption in most of what follows.)

Let $f(x_0,\ldots,x_4) = 0$ be the equation of a cubic threefold $T \subset \mathbb{P}^4$. We see that $T$ is singular at $P_0$ if and only if the initial form at $P_0$ contains no linear term, which means that the polynomial $f$ has no terms of the form $x_0^3$ or $x_0^2 x_j$ for any $j \geq 1$. Thus $T$ is singular at $P_0,\ldots,P_4$ if and only if $f$ is of the form

$$f(x_0,\ldots,x_4) = \sum_{i<j<k} a_{ijk}\, x_i x_j x_k\,. \tag{2.1}$$

Hence these polynomials depend on 10 coefficients. Moreover the condition that $T$ is also singular at $P_5$ is expressed by five relations, which come from computing derivatives:

$$\sum_{0<j<k} a_{0jk} = 0 \qquad \text{and circular permutations.} \tag{2.2}$$

(By this we mean that we write only the first of five equations derived by the cyclic permutation (01234) of the subscripts.)

In characteristic 3 we also need the relation

$$\sum_{i<j<k} a_{ijk} = 0, \tag{2.3}$$

which merely states that $T$ contains $P_5$. Except in characteristic 2 these conditions can be expressed in the slightly simpler form

$$\sum_{0<i<j<k} a_{ijk} = 0 \qquad \&\ \text{circ. perm.} \tag{2.4}$$

Now it is a straightforward verification that the rank of these relations is equal to 5. An explicit (and very useful) set of independent generators for the family of solutions is as follows:

$$f_0 = x_0(x_1 - x_2)(x_3 - x_4) \qquad \&\ \text{circ. perm.} \tag{2.5}$$

□

On the other hand, seven points do not impose independent conditions. In fact, the following result holds (cf. [A], Prop. 5.2):

**Lemma 2.2.** *Let $P_0,\ldots,P_6$ be points in general position in $\mathbb{P}^4$. Then there is a unique cubic hypersurface which has singularities at $P_0,\ldots,P_6$.*

*Proof.* I. Consider the 4-dimensional linear system of cubic threefolds $T$ singular at $P_0,\ldots,P_5$ (Lemma 2.1). One linear condition is enough to ensure that $T$ contains $P_6$. Let now ${}^0\Gamma_4$ be the curve through $P_0,\ldots,P_6$ whose existence was established in Corollary 1.4. The Bézout theorem implies that $\Gamma$ is contained in $T$. Therefore $T$ contains also the tangent direction at $P_6$ along $\Gamma$.

It follows that we need to impose only three more linear conditions (three more tangent vectors) for $P_6$ to be singular on $T$. This shows the existence of a cubic threefold having singularities at $P_0, \ldots, P_6$.

II. We give an alternative, more computational argument for existence. What we need to find is a set of coefficients $b_i$ such that the threefold given by

$$\sum_{i=0}^{4} b_i f_i = 0 \tag{2.6}$$

is singular at $P_6$, where the $f_i$ are given explicitly in (2.5). Let $M$ be the associated Jacobian matrix evaluated at $P_6 = (x_0, \ldots, x_4)$, i.e.,

$$M = \left[ \frac{\partial f_i}{\partial x_j}(x_0, \ldots, x_4) \right] \qquad (i, j \geq 0). \tag{2.7}$$

It is enough to prove that $\det M = 0$.

Now, this is a homogeneous polynomial in the $x_i$ of degree 10. To begin with we show that it is divisible by $x_0$. Indeed, if we specialize $P_6$ so that $x_0 = 0$ we see that $\frac{\partial f_0}{\partial x_j}$ vanishes for $j \geq 1$. Hence it is enough to look at the principal minor

$$M' = \left[ \frac{\partial f_i}{\partial x_j}(x_0, \ldots, x_4) \right] \qquad (i, j \geq 1). \tag{2.8}$$

But an immediate verification shows that $f_1 = -f_4$ when restricted to $\{x_0 = 0\}$. Since

$$\frac{\partial f_i}{\partial x_j}(x_0, \ldots, x_4)\Big|_{x_0=0} = \frac{\partial f_i|_{x_0=0}}{\partial x_j}(0, x_1, \ldots, x_4)$$

for $j \geq 1$, it follows that $M'$ has two identical columns (up to sign) when $x_0 = 0$. Hence $\det M'|_{x_0=0} = 0$, and $\det M$ is divisible by $x_0$.

Further we note that the condition $x_0 = 0$ is just the statement that $P_6$ specializes to a point in the hyperplane $P_1P_2P_3P_4$. By symmetry we get a similar factor of $\det M$ from any hyperplane through four of the six points $P_0, \ldots, P_5$. There are 15 such hyperplanes, and it follows that $\det M$ is divisible by $x_0 \ldots x_4 \prod_{i<j}(x_i - x_j)$. Since this has higher degree than $\det M$, we have $\det M = 0$, which completes the existence part of the proof.

III. Uniqueness derives from the fact that there is only one solution even under the assumption that $x_0 = 0$. In this case, since $\frac{\partial f_0}{\partial x_j} = 0$ if (and only if) $j \geq 1$, it is enough to prove that

$$M'' = \left[ \frac{\partial f_i}{\partial x_j}(0, x_1, \ldots, x_4) \right] \qquad (i, j \geq 2) \tag{2.9}$$

has maximal rank for general $x_i$. Now it is very easy to check that this is true even if we specialize the $x_i$ so that $x_j = 1$ for all $j \geq 1$. □

**Lemma 2.3.** *Let $P_0, \ldots, P_6$ be points in general position in $\mathbb{P}^4$. Let $T$ be any cubic threefold which contains $P_6$ and is singular at $P_0, \ldots, P_5$. Then the unique rational, smooth quartic curve ${}^0\Gamma_4$ through $P_0, \ldots, P_6$ lies on $T$.*

*If, moreover, $P_6$ is a double point of $T$ then the whole curve ${}^0\Gamma_4$ is double on $T$, and $T$ is the variety spanned by the chords of ${}^0\Gamma_4$.*

*Proof.* The first assertion is an obvious consequence of the Bézout theorem and has already been used in the preceding argument.

For the second statement, consider the image of a threefold $T$ as in Lemma 2.1 under the Cremona transformation $\Phi$. Clearly, it is the quadric hypersurface $Q$ with equation

$$g(X_0, \ldots, X_4) = X_0 \ldots X_4 \sum_{i<j<k} a_{ijk} \frac{1}{X_i X_j X_k} = 0. \tag{2.10}$$

As $\Phi(P_5) = (1, \ldots, 1)$ is singular on $Q$, we see that $Q$ is a cone.

The unique quartic curve $\Gamma$ passing through $P_0, \ldots, P_6$ corresponds to the generating line of this cone through $\Phi(P_6)$. If $P_6$ is also double on $T$ (and in general position) then $\Phi(P_6)$ is a further double point of $Q$. But it is well-known that a quadric has a linear space of vertices. Hence the whole line joining $\Phi(P_5)$ and $\Phi(P_6)$ consists of double points. The proper transform of this line, i.e., the quartic curve $\Gamma$ through $P_0, \ldots, P_6$, is therefore double on $T$.

Finally, if $T$ is double along $\Gamma$ then $T$ contains every chord (or *bisecant*) of $\Gamma$. So it is enough to show that the chord-locus $\mathrm{Bisec}(\Gamma)$ is a threefold. Now this can be seen in various ways. For instance, if we project $\Gamma$ from one of its points into $\mathbb{P}^3$, we are reduced to the same question for a twisted cubic. And we know that the chord-locus of a twisted cubic is the whole of $\mathbb{P}^3$, since projecting from a general point in $\mathbb{P}^3$ yields a plane cubic with a node. □

**Corollary 2.4** (cf. [S2], no. 16). *A cubic threefold cannot contain seven double points in general position in $\mathbb{P}^4$ without containing infinitely many.*

**Lemma 2.5.** *Let $T \subset \mathbb{P}^4$ be a cubic threefold with only isolated singularities, which are not in general position. Then no three singular points are on a line, but there is a 2-plane in $T$ containing at least four of them.*

*Proof.* If $T$ has 3 singularities on a line $\ell$, then every 2-plane through $\ell$ intersects $T$ in the union of $\ell$ counted twice and some other line. This is possible only if $\ell$ is double on $T$, contrary to the assumption that the singularities are isolated.

Thus, if $T$ has 4 singularities in a 2-plane $\pi$, we see that $\pi \cap T$ contains 6 lines joining the multiple points in pairs. Clearly, this is possible only if $\pi \subset T$.

Hence we are reduced to the case where $T$ has 5 singularities which are in general position in a hyperplane $H \simeq \mathbb{P}^3$. Let $S = H \cap T$. By a result which is the exact analogue of Corollary 1.4 and which one can prove in the same way (cf. Remark 1.6), using the Cremona transformation $T_3^{\mathrm{tet}}$ (cf. [SR], p. 179 and p. 186),

we can find an irreducible twisted cubic ${}^0\Gamma_3$ through the five singularities and one further general point in $\mathbb{P}^3$ not on the surface $S$. Now, the Bézout theorem implies that this curve is entirely contained in a component of $S$, which is absurd. □

**Lemma 2.6.** *A general threefold $T \subset \mathbb{P}^4$ as in Lemma 2.1 contains six double points and no other singularities.*

*Proof.* Suppose first that we are in characteristic 0. Then, by one of the Bertini theorems, the linear system $\mathcal{L}$ cannot have any movable singularities. But there is no fixed singularity apart from the six assigned double points. Indeed, the unions of three hyperplanes in (2.5), each through four of the $P_i$, have no other common singularity.

For arbitrary characteristic, we can argue as follows: it is enough to show that if $P_0, \ldots, P_5$ are in general position, the cubic threefolds $T$ which have singularities at $P_0, \ldots, P_5$ and at some further (unassigned) point $P$ form a finite union of families of dimension at most 3. By Lemma 2.3, those $T$ which have a further singularity in general position with respect to $P_0, \ldots, P_5$ are in one-one correspondence with the smooth rational quartics through $P_0, \ldots, P_5$; and by Remark 1.5 these form a family of dimension 3. (This includes most cases where $T$ has non-isolated singularities. The remaining cases of this sort can be handled by looking, as in Lemma 2.5, at the intersection $S = H \cap T$ with a hyperplane through four of the $P_i$.)

Suppose instead that $T$ has a further singularity $P$ not in general position (and only isolated singularities). Then, by Lemma 2.5, we can after renumbering assume that $P$ lies in the plane spanned by $P_2, P_3, P_4$. This implies that in (2.1) we have $a_{234} = 0$. Now this last condition does not hold for the general $T$ with singularities at $P_0, \ldots, P_5$. Indeed it is equivalent to the statement that in the notation of (2.5) the equation of $T$ does not involve $f_3$. □

We now state a partial converse to Lemma 2.5, which will be needed in §3.

**Lemma 2.7.** *If a threefold $T \subset \mathbb{P}^4$ contains a 2-plane $\pi$ then it has some singularities in it.*

*It may have four nodes in $\pi$ or singularities of a more complicated type. But if $T$ has six multiple points in general position and no other singularities, then it does not contain any of the 2-planes spanned by three of them.*

*Proof.* We may assume that $\pi$ is given by $x_0 = x_1 = 0$ and write the equation of $T$ as $x_0 q_0 + x_1 q_1 = 0$, where $q_0$ and $q_1$ are quadratic forms. The intersection $\{x_0 = x_1 = q_0 = q_1 = 0\}$ defines four ordinary singular points in general. We refrain from analysing the degenerate cases here (cf. [K] and references therein).

However, the case where $T$ has six multiple points in general position and no other singularities is of interest for what follows. We may assume that the multiple points $P_0, \ldots, P_5$ have coordinates as above, and that $T$ contains the

plane $\pi = \{x_0 = x_1 = 0\}$ through $P_2, P_3$ and $P_4$. Then we see that $T$ is the set of zeros of a polynomial $f$ as in (2.1) with $a_{234} = 0$.

Thus, if we look at the point $P = (0, 0, 1, 1, 1)$, which is the intersection of $\pi$ with the plane spanned by $P_0, P_1$ and $P_5$, we see that it is singular on $T$, contrary to our assumptions. Indeed it follows from (2.1) that $P$ is singular on $T$ if and only if

$$a_{023} + a_{024} + a_{034} = 0 \quad \text{and} \quad a_{123} + a_{124} + a_{134} = 0.$$

Now, these relations are consequences of (2.4) since $a_{234} = 0$. This completes the proof of the lemma. □

# 3. Segre's cubic threefold as a variety of moduli

For most of the discussion, the ground field will be any perfect field $K$ with sufficiently many elements. We denote by $\overline{K}$ an algebraic closure of $K$. If we consider a given cubic threefold $T$ with six double points $P_0, \ldots, P_5$ in general position in $\mathbb{P}^4_K$, we can look at the family of quartic curves lying on $T$ and passing through the double points. We know from Corollary 1.4 and Lemma 2.3 that each (general) point of $T$ belongs to one and only one of them. Hence the variety $T$ can be viewed as a bundle of rational quartics over some variety which parametrizes these curves.

It is possible to give local arguments to describe a parametrizing variety inside the Chow variety of curves of degree 4 in $\mathbb{P}^4$. As mentioned briefly at the end of §1, the trouble with these arguments is that they fail to describe the situation symmetrically with respect to the six double points, and it is not easy to get rid of the twisting they introduce.

Fortunately, we can give an explicit $K$-invariant description of this family, thanks to the rather unexpected fact that there is a nice, faithful description of the family of all rational quartic curves through $P_0, \ldots, P_5$ in $\mathbb{P}^4$ (i.e., not only of those lying on $T$). Then the parametrizing variety we are looking for will simply be obtained as a smooth hyperplane section of this more general variety of moduli.

**Theorem 3.1.** *Given six points $P_0, \ldots, P_5$ in general position in $\mathbb{P}^4_K$, the family of all quartic curves passing through them is parametrized by a cubic threefold $\Sigma \subset \mathbb{P}^4_K$ with ten double points.*

*More precisely, let $\mathcal{L}$ be the linear system of all cubic hypersurfaces on which $P_0, \ldots, P_5$ are double. Then $\mathcal{L}$ maps the whole of $\mathbb{P}^4_K$ into a cubic hypersurface $\Sigma$, which is a form of the Segre variety with equation:*

$$y_0y_1y_2 + y_1y_2y_3 + y_2y_3y_4 + y_3y_4y_0 + y_4y_0y_1 = 0. \tag{3.1}$$

*A general fibre of this map $\Psi\colon \mathbb{P}^4_K \dashrightarrow \Sigma$ is a smooth, geometrically rational quartic curve ${}^0\Gamma_4$ through $P_0, \ldots, P_5$. Those curves which lie on a given irreducible threefold $T$ correspond to the points in some hyperplane section $S$ of $\Sigma$.*

*Proof.* The family of all cubics with six double points at $P_0, \ldots, P_5$ is 4-dimensional (Lemma 2.1). This linear system $\mathcal{L}$ therefore defines a rational map $\Psi\colon \mathbb{P}^4_K \dashrightarrow \mathbb{P}^4_K$. Over $\overline{K}$ a set of generators was given explicitly in (2.5). Hence in this case we can write:

$$(x_0, \ldots, x_4) \mapsto (y_0 = f_0, \ldots, y_4 = f_4).$$

We note that the image of $\Psi$ is not the whole of $\mathbb{P}^4_K$. For suppose a cubic threefold in the linear system contains a point of some quartic $\Gamma$, other than $P_0, \ldots, P_5$. Then by the Bézout theorem, it contains $\Gamma$ entirely. In other words, the quartic curves through $P_0, \ldots, P_5$ are blown down each into one point.

Thus the image of $\Psi$ has dimension $\leq 3$ (cf. Remark 1.5), and a simple verification shows that there is indeed the relation

$$f_0 f_1 f_2 + f_1 f_2 f_3 + f_2 f_3 f_4 + f_3 f_4 f_0 + f_4 f_0 f_1 = 0.$$

(For instance, this expression is a multiple of $x_0$, because both $f_0$ and, as already used before, $f_1 + f_4$ have this property; etc.)

Moreover, a hyperplane section $S$ in the image corresponds to the points of some element $T$ in $\mathcal{L}$. So, cutting out $\Sigma$ by a straight line $\ell$ amounts to intersecting three general elements of $\mathcal{L}$. This yields a curve in $\mathbb{P}^4$ of degree 27, which contains the 15 lines joining the $P_i$. The residual part is a union of quartic curves. Hence there are three of them, mapping into the 3 intersection points of $\ell$ with $\Sigma$. In this way we have checked that the image of $\Psi$ is 3-dimensional and that the fibre above a general point of $\Sigma$ is indeed reduced to one quartic curve.

Much the same argument shows that a smooth point in general position on an element $T$ of $\mathcal{L}$ (by Lemma 2.3 this is equivalent to saying that the corresponding quartic is not double on $T$) is mapped to a smooth point of the corresponding hyperplane section $S$ of $\Sigma$.

Note that the whole construction is defined over the ground field $K$. The only purpose of the generators in (2.5) is for checking that the image is indeed a cubic threefold with 10 double points. □

The ten-nodal cubic $\Sigma \subset \mathbb{P}^4$ was studied in great detail by Corrado Segre [S1]. Some of its basic geometry is described in [SR, p. 169]. We recall that (over $\overline{K}$) $\Sigma$ is the unique cubic threefold with ten nodes. It contains fifteen 2-planes, which cut out 15 lines on any smooth hyperplane section $S$ of $\Sigma$. As $S$ has altogether 27 lines, an important property is:

**Lemma 3.2.** *The residual twelve lines on $S$ form a double-six.*

*Proof.* This is stated in [S1], no. 3. One can also view this through another description of $\Sigma$. Indeed (cf. [SR], pp. 182–183 and Remark 3.3 below), $\Sigma$ is also the image of $\mathbb{P}^3$ under the rational map $\psi$ defined by the system $\mathcal{N}$ of quadrics passing through five points $Q_0, \ldots, Q_4$ in general position. Five of the 15 planes on $\Sigma$ correspond to the $Q_i$ and the other ten to the planes spanned by any three of them.

Hence we may regard $S$ as the blow-up of an element $\mathbb{P}^1 \times \mathbb{P}^1$ of $\mathcal{N}$ in $Q_0, \ldots, Q_4$. Ten of the residual 12 lines are the strict transforms $L_0, \ldots, L_4$ of lines of bidegree $(1,0)$, resp. $M_0, \ldots, M_4$ of lines of bidegree $(0,1)$, passing through the $Q_i$; and the other two are the strict transforms $L_5, M_5$ of twisted cubics of bidegree $(2,1)$, resp. $(1,2)$, passing through the $Q_i$. That these lines form a double-six is immediate. □

**Remark 3.3.** To make the situation more precise, we observe that $\Psi$ is a morphism off the base locus $E = \bigcup e_{ij}$, where $e_{ij}$ denotes the line through $P_i$ and $P_j$. Moreover, $\Psi$ blows down each 2-plane $\pi_{ij5}$ through $P_i, P_j$ and $P_5$ and its complementary plane into a double point $P_{ij}$ of $\Sigma$. For instance, $\pi_{015} = \{x_2 = x_3 = x_4\}$ and $\pi_{234} = \{x_0 = x_1 = 0\}$ are blown down into $(0,0,0,1,0)$. In addition, the hyperplanes spanned by four of the $P_i$ (like $\{x_0 = 0\}$) are blown down into the fifteen 2-planes on $\Sigma$ (in our example, $\{y_0 = y_1 + y_4 = 0\}$).

Thus the whole situation can be studied quite explicitly if we wish. For instance, the rational map defined by $\mathcal{N}$ in Lemma 3.2 can be written down as follows: suppose $Q_0 = (1,0,0,0), \ldots, Q_3 = (0,0,0,1)$, and $Q_4 = (1,1,1,1)$; then $\Sigma$ is obtained in the form (3.1) as the image of the map

$$\psi\colon (Y_0, \ldots, Y_3) \mapsto (y_0 = g_0, \ldots, y_4 = g_4),$$

where

$$g_0 = (Y_1 - Y_2)Y_3, \quad g_1 = (Y_3 - Y_2)Y_0, \quad g_2 = (Y_0 - Y_1)Y_3,$$
$$g_3 = (Y_2 - Y_1)Y_0, \quad g_4 = (Y_0 - Y_1)(Y_2 - Y_3).$$

As a matter of fact, $\Psi$ has a very interesting decomposition as:

$$\Psi = \psi \circ \pi \circ \Phi,$$

where $\Phi$ is given by (1.1) and where $\pi$ is just the projection from $P_5$ into the hyperplane spanned by $P_0, \ldots, P_3$. This can be seen quite simply by writing:

$$Y_0 = X_0 - X_4, \quad Y_1 = X_1 - X_4, \quad Y_2 = X_2 - X_4, \quad Y_3 = X_3 - X_4\,.$$

**Lemma 3.4.** *Suppose $S$ is a smooth hyperplane section of a 10-nodal cubic threefold $\Sigma \subset \mathbb{P}^4_K$. Then $S$ is a cubic surface with a double-six defined over $K$. In particular, if $K$ is a number field then $S$ satisfies the Hasse principle.*

*Proof.* Going over to some quadratic extension $K'/K$, we find, by Lemma 3.2, a smooth cubic surface $S' = S \times_K K'$ with a sextuplet of lines, for which the Hasse principle is known to hold (cf. [SD], Theorem 7 or [CM], Cor. 2.6). Finally, we can go down to $K$ by a standard argument which consists of connecting a $K'$-point to its conjugate by a straight line and looking at the third residual intersection, which is defined over $K$. □

**Corollary 3.5.** *Suppose $T \subset \mathbb{P}^4_K$ is a cubic threefold, defined over any field $K$, with six singular points in general position and no other singularities. Then*
(i) *$T$ is $K$-birationally equivalent to a conic bundle over a smooth hyperplane section $S$ of a 10-nodal cubic threefold;*
(ii) *$T$ has a $K$-point if and only if $S$ does.*

*Proof.* (i) By Theorem 3.1, $T$ is fibred above a hyperplane section of $\Sigma$ which is a smooth cubic surface. Otherwise, as we know from Remark 3.3, either $T$ would have some further singularity or it would contain the 2-plane $\pi_{ij5}$ spanned by three of its nodes, which is impossible, by Lemma 2.7. Furthermore a general fibre is a smooth geometrically rational quartic curve, hence isomorphic to a conic over its field of definition.

(ii) If $S$ has a $K$-point then $T$ contains a twisted quartic curve defined over $K$. Hence $T$ has a point over some quadratic extension $K'$ of $K$, and so over $K$. □

From this we derive an interesting corollary (cf. [C], §4):

**Corollary 3.6.** *Let $T \subset \mathbb{P}^4_K$ be a cubic threefold, defined over any field $K$, with six nodes in general position. Suppose $T$ contains a $K$-rational 0-cycle of degree $\delta$ prime to 3. Then $T(K) \neq \varnothing$.*

*Proof.* This is an easy consequence of Corollary 3.5(ii), since the result holds for $S$. Indeed, for smooth cubic surfaces this statement is classical (cf. [CM], Cor. 2.3 and Prop. 1.6) because (with the notation of Lemma 3.4) $S' = S \times_K K'$ is birationally equivalent to a Severi-Brauer variety. And quadratic extensions are harmless. □

**Corollary 3.7.** *Suppose $T \subset \mathbb{P}^4_K$ is a cubic threefold, defined over a number field $K$, with six nodes in general position. Then $T$ satisfies the Hasse principle.*

*Proof.* This is immediate from Lemma 3.4 and Corollary 3.5. □

We may add that the smoothness of $S$, which has been achieved by some rather delicate considerations, does not play a major role in the proofs of these corollaries. Indeed in each case the result is also known for singular cubic surfaces. In fact, our assertions can be somewhat generalized (to cubic threefolds with a closed set of 6 double points —for the Galois action— but maybe some further singularities) by applying this remark. To wind up the discussion, we note that one also has:

**Lemma 3.8.** *If $T \subset \mathbb{P}^4_K$ is a cubic threefold with exactly six singular points that are not in general position then $T$ has a $K$-point.*

*Proof.* First, suppose that the singularities span $\mathbb{P}^4$. By Lemma 2.5, there is a 2-plane in $T$ containing at least four of them. But the assumption implies that there is only one set of four singularities which are coplanar. Hence the plane is defined over $K$, and it is contained in $T$.

Second, suppose the singularities all lie in a hyperplane $H$. Then $S = H \cap T$ is a cubic surface in $H \simeq \mathbb{P}^3_K$ with at least six singularities, so that it must be reducible (as in Lemma 2.5, $S$ cannot be ruled). In fact, by Lemma 2.5, $S$ contains a 2-plane containing at least 4 singular points of $T$. Hence either this 2-plane is defined over $K$ or $S$ is the union of three conjugate planes, whose intersection (in $\mathbb{P}^3_K$) contains a $K$-point. □

## References

[A] Alexander, J., Singularités imposables en position générale à une hypersurface projective. Compositio Math. 68 (1988), 305–354.

[C] Coray, D.F., Cubic hypersurfaces and a result of Hermite. Duke Math. J. 54 (1987), 657–670.

[CM] Coray, D.F., Manoil, C., On large Picard groups and the Hasse Principle for curves and K3 surfaces. Acta Arith. 76 (1996), 165–189.

[K] Koelblen, L., Surfaces de $\mathbb{P}_4$ tracées sur une hypersurface cubique. J. Reine Angew. Math. 433 (1992), 113–141.

[S1] Segre, C., Sulla varietà cubica con dieci punti doppi dello spazio a quattro dimensioni. Atti Reale Accad. Sci. Torino 22 (1887), 547–557.

[S2] — Sulle varietà cubiche dello spazio a quattro dimensioni e su certi sistemi di rette e certe superficie dello spazio ordinario. Memorie Reale Accad. Sci. Torino 39 (1887), 3–48.

[Se] Semple, J.G., On certain loci of three dimensions representable on ordinary space by means of cubic surfaces, and the Cremona transformations for ordinary space obtained by projection of such loci. Proc. Cambridge Philos. Soc. 25 (1929), 145–167.

[SR] Semple, J.G., Roth, L., Introduction to algebraic geometry. Clarendon Press, Oxford 1949.

[SD] Swinnerton-Dyer, H.P.F., Applications of algebraic geometry to number theory. In: 1969 Number Theory Institute (ed. by D.J. Lewis; Proc. Symp. Pure Math. 20), 1–52. Amer. Math. Soc., Providence 1971.

# Arithmétique et espaces de modules de revêtements

*Pierre Dèbes*

**Résumé.** Les espaces de modules de revêtements constituent un cadre approprié pour l'étude de certains problèmes arithmétiques mettant en jeu courbes algébriques et fonctions rationnelles. Dans un premier temps, nous revenons sur la construction de ces espaces ainsi que sur leurs propriétés géométriques. Puis nous nous intéressons à leur utilisation à des fins arithmétiques, par exemple pour le problème inverse de Galois, le problème de Hilbert-Siegel, etc. Enfin nous considérons quelques développements récents comme la construction de tours modulaires.

1991 Mathematics Subject Classification: Primary 11Gxx, 14H10; Secondary 14H30, 12-xx.

## 1. Introduction

Dans un article de 1891 [Hu], A. Hurwitz explique comment on peut mettre une structure de variété complexe sur l'ensemble des revêtements simples de degré fixé $d$ de $\mathbb{P}^1$ ("simple" signifiant ici que les fibres comportent au moins $d-1$ points). Par espaces de Hurwitz on entend aujourd'hui espaces de modules de revêtements de groupe d'automorphismes fixé et pour lesquels on impose certaines contraintes à la ramification. La construction générale et le développement de ces espaces sont essentiellement dûs à M. Fried. Il faut y associer aussi les noms de Fulton et Mumford pour leurs travaux sur les espaces de modules de courbes. Ce texte reprend, en insistant sur les implications arithmétiques, les différentes étapes de la théorie. Les sources principales sont [Fr2], [DeFr1-4], [FrVö], [Fr6].

Les espaces de Hurwitz constituent un outil de choix pour certains problèmes diophantiens mettant en jeu courbes algébriques et fonctions rationnelles; plus généralement, pour l'étude de l'arithmétique des revêtements de la droite. Par exemple le Problème Inverse de Galois (dans sa forme régulière sur $\mathbb{Q}(T)$) revient à trouver des points $\mathbb{Q}$-rationnels sur ces espaces. De façon générale, l'idée est de regarder les contraintes que le problème étudié impose aux données intrinsèques des revêtements en question, comme le groupe d'automorphismes et la ramification, et de voir ensuite s'il existe sur l'espace de modules associé d'éventuelles solutions, sur $\mathbb{C}$ d'abord, puis sur le corps de base. Le problème conserve sa nature diophantienne mais cette approche permet d'une certaine façon, de classifier les équations en en abstrayant les propriétés structurelles.

Cette approche repose sur l'idée que la théorie des groupes, à travers la description des revêtements par leur monodromie, régit également l'arithmétique des revêtements. Le problème de Hilbert-Siegel en est une illustration (§4.1), où l'on voit la solution d'un problème arithmétique concret — l'étude de l'irréductibilité des polynômes du type $f(Y) - t$ ($f \in \mathbb{Q}[Y]$, $t \notin f(\mathbb{Q})$) — provenir de la classification des groupes simples. Plus généralement, on vise à développer des outils de pure théorie des groupes, permettant d'apprécier les propriétés arithmétiques des revêtements de monodromie fixée.

Pour les applications, le problème majeur est de trouver des points rationnels sur les espaces de Hurwitz. On a des réponses sur $\mathbb{Q}$ pour les "petites" valeurs des paramètres ou bien sur de "gros" corps $K$. Ces questions arithmétiques nécessitent une étude géométrique préalable (§2): il faut commencer par déterminer les composantes irréductibles de ces espaces, leurs corps de définition, leur structure géométrique, par exemple, si elles sont (uni-)rationnelles, etc.

Les succès les plus marquants de la théorie des espaces de Hurwitz concernent le problème inverse de Galois. Nous y revenons au §3. Il y a d'autres applications (§4): au problème de Hilbert-Siegel, au problème de Davenport, au théorème de Mason-Stothers, à un critère d'existence de points rationnels, etc. Afin d'illustrer la méthode, nous détaillerons un peu plus l'une d'elles, la première (§4.1 & §4.2).

On peut espérer que de nouveaux développements viendront de la considération de *tours modulaires* (§5). Ces objets ont été introduits par M. Fried [Fr6]. Une tour modulaire est une tour d'espaces de Hurwitz associés de façon naturelle à un espace de Hurwitz donné $\mathcal{H}$; chaque niveau de la tour se projette sur $\mathcal{H}$ par un revêtement de Frattini. L'exemple fondateur est celui de la tour des courbes modulaires. Ce cas particulier est riche en résultats arithmétiques (théorèmes de Serre, de Mazur-Merel, etc.). On peut se demander si des résultats de même nature subsistent dans le cas général des tours modulaires.

La plupart des questions développées dans cet article ont pour origine des problèmes diophantiens sur lesquels A. Schinzel a eu une grande influence. Ainsi, l'approche modulaire des problèmes de Hilbert-Siegel et de Davenport (§4) a été motivée par ses travaux sur les équations à variables séparées $h(x) = g(y)$. C'est aussi un résultat de Schinzel avec Lewis [LeSc] qui est à l'origine de notre travail [DeFr1], présenté en §4.4, sur l'existence de points rationnels dans les familles de courbes. Avec cet article, écrit à l'occasion du 60ème anniversaire d'A. Schinzel, l'auteur souhaite lui témoigner son estime et sa reconnaissance.

## 2. Espaces de modules de revêtements

Dans cette section, on introduit les espaces de Hurwitz (§2.1), on revient brièvement sur leur construction (§2.2), ainsi que leurs propriétés géométriques (§2.5); la plupart proviennent de la présentation des espaces de Hurwitz comme revêtement de l'espace $\mathcal{U}_r$ (§2.3). De premiers exemples sont donnés en §2.4.

## 2.1. Présentation

Les objets qui sont au centre de cet exposé sont les revêtements finis $f : X \to \mathbb{P}^1$ de la droite projective $\mathbb{P}^1$, définis sur la clôture algébrique $\overline{K}$ d'un corps $K$ de caractéristique 0. Plus simplement, on peut les voir comme la donnée d'une courbe irréductible $X$ définie sur $\overline{K}$ et d'une fonction rationnelle non constante $f \in \overline{K}(X)$. Il y a une notion classique d'isomorphisme (l'équivalence des revêtements). Les classes d'équivalence ont les invariants suivants.

### Invariants

- Le groupe de monodromie $G$ du revêtement $f$, qui est isomorphe au groupe de Galois de la clôture galoisienne de l'extension $\overline{K}(X)/\overline{K}(T)$ et anti-isomorphe au groupe d'automorphismes de la clôture galoisienne du revêtement $f$.
- Le degré $d = \deg(f)$ et l'action de monodromie $G \hookrightarrow S_d$, correspondant à l'action de $G$ sur une fibre non ramifiée du revêtement.
- L'ensemble $\mathbf{t} = \{t_1, \ldots, t_r\} \subset \mathbb{P}^1(\mathbb{C})$ des points de ramification. On notera $\mathcal{U}_r$ l'espace paramétrant cette donnée, *i.e.*, la variété des ensembles de $r$ points distincts de $\mathbb{P}^1$. En associant à chaque $\mathbf{t}$ les coefficients du polynôme dont les racines sont $t_1, \ldots, t_r$, on voit $\mathcal{U}_r$ comme l'espace projectif $\mathbb{P}^r$ privé du lieu discriminant. On notera aussi $\mathcal{U}^r$ l'espace $(\mathbb{P}^1)^r$ privé des $r$-uplets dont deux coordonnées sont égales. La variété $\mathcal{U}_r$ correspond au quotient de $\mathcal{U}^r$ par l'action de $S_r$.
- L'inertie $\mathbf{C} = \{C_1, \ldots, C_r\}$ [1], *i.e.*, la donnée des classes de conjugaison des cycles de ramification, ou, de façon équivalente, des générateurs des groupes d'inertie, au-dessus des points de ramification.

**Théorème 2.1** (Fried [Fr2]). *On suppose donnés une représentation transitive $G \hookrightarrow S_d$ et un entier $r \geq 3$.*

(a) *Il existe un espace de modules grossier $\mathcal{H}_G$ pour la catégorie $\mathcal{C}_{r,G}$ des revêtements de $\mathbb{P}^1$ définis sur $\mathbb{C}$, avec $r$ points de ramification et de groupe $G \subset S_d$.*

(b) *L'espace $\mathcal{H}_G$ est une variété algébrique lisse définie sur $\mathbb{C}$ dont les points complexes correspondent bijectivement aux classes d'isomorphisme d'objets de la catégorie $\mathcal{C}_{r,G}$. On notera $[f]$ le point sur $\mathcal{H}_G(\mathbb{C})$ correspondant à un revêtement $f$. De plus l'espace $\mathcal{H}_G$ a la propriété suivante. Si $\mathcal{P}$ est une variété algébrique paramétrant une famille $\mathcal{F}$ de revêtements dans $\mathcal{C}_{r,G}$, alors l'application $\mathcal{P} \to \mathcal{H}_G$ envoyant tout point $\mathrm{p} \in \mathcal{P}$ sur le point $[\mathcal{F}_\mathrm{p}] \in \mathcal{H}_G$ est un morphisme algébrique.*

(c) *$\mathcal{H}_G$ a un modèle défini sur $\mathbb{Q}$. Ce modèle a les propriétés suivantes. Soit $K$ un corps de caractéristique 0. Dans toute classe $[f] \in \mathcal{H}_G(\overline{K})$, il existe un revêtement $f$ défini sur $\overline{K}$. De plus, l'action de $G_K = G(\overline{K}/K)$ sur $\mathcal{H}_G(\overline{K})$ coincide avec l'action sur les revêtements correspondants. C'est-à-dire, $[f]^\tau = [f^\tau]$ pour tout $[f] \in \mathcal{H}_G(\overline{K})$ et tout $\tau \in G_K$.*

---

1) Certaines des classes $C_i$ peuvent être répétées. Plutôt qu'un ensemble, il faut voir $\mathbf{C}$ comme un $r$-uplet modulo l'action de $S_r$.

(d) *On appelle corps des modules du revêtement $f$ le corps $\mathbb{Q}([f])$; sous des hypothèses convenables* [DeDo1], *c'est le plus petit corps de définition de $f$.*
(e) *L'application $\psi : \mathcal{H}_G \to \mathcal{U}_r$ associant à $[f] \in \mathcal{H}_G(\mathbb{C})$ l'ensemble $\mathbf{t}$ des points de ramification de $f$ est un morphisme étale et défini sur $\mathbb{Q}$.*

**Variante**: Il y a un énoncé similaire pour les G-*revêtements* de $\mathbb{P}^1$ de groupe $G$ (au lieu de revêtements). Un G-revêtement est la donnée d'un revêtement galoisien $f : X \to \mathbb{P}^1$ et d'un isomorphisme $G(K(X)/K(T)) \simeq G$. On distingue généralement les deux situations en mettant en exposant de $\mathcal{H}_G$ l'indication *ab* (pour les revêtements *purs*) ou *in* (pour les G-revêtements). Pour simplifier, nous ne le ferons que quand nous l'estimerons nécessaire à la compréhension.

## 2.2. Construction

**2.2.1. 1ère approche** (Fried [Fr2], Coombes-Harbater [CoHa], Fried-Völklein [FrVo], Emsalem [Em]). Les différentes étapes de la construction sont les suivantes.

• On pose $\mathcal{H}_G(\mathbb{C}) \stackrel{\text{déf}}{=} \coprod(\mathbf{t}, \varphi_\mathbf{t})$ où $\mathbf{t}$ parcourt $\mathcal{U}_r(\mathbb{C})$ et $\varphi_\mathbf{t}$ l'ensemble des homomorphismes $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G \subset S_d$ (à équivalence près).

• On munit $\mathcal{H}_G(\mathbb{C})$ d'une topologie. On utilise pour cela les isomorphismes

$$\pi_1(\mathbb{P}^1 - \mathbf{t}) \stackrel{\chi}{\simeq} \pi_1(\mathbb{P}^1 - \mathbf{D})$$

(obtenus par rétraction) où $\mathbf{D} = \{D_1, \ldots, D_r\}$ est une famille de petits disques $D_i$ autour de $t_i$. Essentiellement, deux points $(\mathbf{t}, \varphi_\mathbf{t})$ et $(\mathbf{t}', \varphi_{\mathbf{t}'})$ sont considérés comme proches si $\mathbf{t}$ et $\mathbf{t}'$ sont proches dans $\mathcal{U}_r(\mathbb{C})$ (dans un même polydisque $\mathbf{D}$) et si $\varphi_\mathbf{t}$ et $\varphi_{\mathbf{t}'}$ sont égaux *via* l'isomorphisme $\chi$. Pour cette topologie, la projection $\psi : \mathcal{H}_G(\mathbb{C}) \to \mathcal{U}_r(\mathbb{C})$ est un revêtement topologique.

• D'après le théorème de Grauert-Remmert [GrRe1-3], le revêtement $\psi$, dont la base $\mathcal{U}_r(\mathbb{C})$ est une variété algébrique, est prolongeable en un revêtement analytique compact $\overline{\psi} : \overline{\mathcal{H}_G(\mathbb{C})} \to \mathbb{P}_r(\mathbb{C})$.

• Ce revêtement analytique compact provient d'un morphisme algébrique $\overline{\psi} : \overline{\mathcal{H}_G} \to \mathbb{P}_r$ défini sur $\mathbb{C}$: cela résulte des théorèmes GAGA [Se1].

• On montre ensuite que $\overline{\psi}$ peut être défini sur $\overline{\mathbb{Q}}$. On utilise pour cela un résultat général de descente des revêtements d'une base définie sur un corps algébriquement clos [Se2; Ch. 6].

• *Descente de Weil* [We]. On montre enfin que $\overline{\psi}$ peut être défini sur $\mathbb{Q}$. Pour cela, on considère, pour tout $\tau \in G_\mathbb{Q}$, l'application

$$\varepsilon_\tau : \begin{cases} \mathcal{H}_G^\tau(\overline{\mathbb{Q}}) & \to & \mathcal{H}_G(\overline{\mathbb{Q}}) \\ [f]^\tau & \to & [f^\tau] \end{cases}$$

Une première étape est de montrer que les $\varepsilon_\tau$ sont continus (voir ci-dessous). Ensuite, de $\psi\varepsilon_\tau = \psi^\tau$, on déduit que les $\varepsilon_\tau$ sont des isomorphismes analytiques; alors ce doivent être des isomorphismes algébriques à cause de l'unicité de la structure

algébrique sur $\mathcal{H}_G$ (induisant la structure analytique). Enfin on vérifie la condition de cocycle de Weil: $\varepsilon_u \varepsilon_v^u = \varepsilon_{uv}$ $(u, v \in G_{\mathbb{Q}})$. Le critère de descente de Weil donne alors les deux parties de la conclusion (c) du Th. 2.1.

*Continuité des $\varepsilon_\tau$.* On peut se placer sur un revêtement $\widetilde{\mathcal{H}}$ de $\mathcal{H}_G$ (plutôt que $\mathcal{H}_G$ lui-même): la continuité des $\varepsilon_\tau$ résulte de celle des $\widetilde{\varepsilon}_\tau : \widetilde{\mathcal{H}}^\tau \to \widetilde{\mathcal{H}}$. Il y a plusieurs revêtements $\widetilde{\mathcal{H}}$ de $\mathcal{H}_G$ possibles:

— (Fried-Völklein): $\widetilde{\mathcal{H}} = \mathcal{H}_{\widetilde{G}}$ où $\widetilde{G}$ est une extension de $G$ de centralisateur dans $S_{\tilde{d}}$ trivial (ou de centre trivial pour la situation "G-revêtements"). Les revêtements paramétrés par $\widetilde{\mathcal{H}}$ n'ont alors pas d'automorphismes. Cela nécessite un lemme préalable de théorie des groupes disant que tout groupe $G$ a une extension $\widetilde{G}$ ayant les propriétés requises.

— (Emsalem): $\widetilde{\mathcal{H}}$ est l'espace des modules des revêtements $f \in \mathcal{H}_G$ "pointés" par un point sur $X$ (au-dessus d'un point-base $t_0$). Ces revêtements pointés n'ont pas d'automorphismes.

Dans les deux cas, l'absence d'automorphismes entraîne l'existence d'une *famille* $\widetilde{\mathcal{F}}$ de revêtements (éventuellement pointés) au-dessus de $\widetilde{\mathcal{H}}$ (voir §2.5.3). La continuité des $\widetilde{\varepsilon}_\tau$ s'ensuit. Voici essentiellement pourquoi.

Supposons que $([f_n]^\tau)_n$ tend vers $[f]^\tau$ dans $\widetilde{\mathcal{H}}^\tau$. Il existe une famille au-dessus de $\widetilde{\mathcal{H}}^\tau$, à savoir la famille $\widetilde{\mathcal{F}}^\tau$. Il en résulte ceci: *les* représentants des $([f_n]^\tau)_n$ dans la famille $\widetilde{\mathcal{F}}^\tau$ tendent vers *le* représentant de $[f]^\tau$ dans la famille $\widetilde{\mathcal{F}}^\tau$. Convenons que $f_n$ $(n > 0)$ et $f$ sont *les* revêtements de la famille $\widetilde{\mathcal{F}}$ représentant les points $[f_n]$ $(n > 0)$ et $[f]$. Alors $f_n^\tau$ $(n > 0)$ et $f^\tau$ sont *les* revêtements de la famille $\widetilde{\mathcal{F}}^\tau$ représentant les points $([f_n]^\tau)$ $(n > 0)$ et $[f]^\tau$. Conclusion: $f_n^\tau$ tend vers $f^\tau$; *a fortiori*, $[f_n^\tau]$ tend vers $[f^\tau]$ sur $\widetilde{\mathcal{H}}$.

**2.2.2. 2ème approche** (Bertin [Be]). J. Bertin reprend des techniques purement algébriques mises en place par Mumford et Gieseker dans le contexte de la construction de l'espace $\mathcal{M}_g$ de modules des courbes. Il les utilise pour construire l'espace des modules $H_{g,G}$ des courbes lisses de genre $g \geq 2$ données avec une action d'un groupe $G$. L'espace $\mathcal{M}_g$ s'obtient à partir du schéma de Hilbert des courbes de genre $g$ et de degré $m(2g-2)$ dans $\mathbb{P}_n$ $(n = card(G))$. Ici il faut ne s'intéresser qu'aux courbes qui sont laissées invariantes par l'action de $G$. L'espace $H_{g,G}$ s'obtient comme sous-variété de $\mathcal{M}_g$ fixée par l'action de $G$ (étendue au schéma de Hilbert). Cette construction a l'avantage d'être valable en toute caractéristique. Cette approche conduit également à une construction d'une compactification $\overline{H}_{g,G}$ de $H_{g,G}$; elle fournit une description intéressante des points du bord de $\overline{H}_{g,G}$ comme courbes stables de genre $g$ munie d'une action *stable* (voir [Be] pour une définition précise) de $G$. Cette étude du "bord" éclaire d'autre part un peu plus le phénomène de "collision des points de ramification".

Il y a une autre différence avec la construction précédente. Si les objets correspondant aux points de $H_{g,G}$ peuvent être vus comme des revêtements $X \to X/G$, la base n'est pas fixée comme pour les revêtements paramétrés par les points de $\mathcal{H}_G$. Cela rend l'espace $\mathcal{H}_G$ peut-être plus approprié pour des considérations

diophantiennes, puisque ce choix de la base correspond au choix d'une coordonnée et donc d'une équation pour la courbe du haut. Chez Bertin, la base n'est fixée qu'à isomorphisme près. Le schéma $H_{g,G}$ est en fait un quotient de l'espace $\mathcal{H}_G$ (pour $g = 0$, le quotient par $\mathrm{PGL}(2,\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^1)$). En conséquence, l'interprétation du corps de définition des points sur $H_{g,G}$ diffère quelque peu. Ainsi, les points $k$-rationnels sur l'espace $H_{0,G}$ correspondent, non pas à des revêtements de $\mathbb{P}^1$ définis sur $k$, mais à des revêtements d'une $k$-courbe de genre 0 (et donc éventuellement d'une conique sans $k$-points).

Pour les questions liées à la construction, la compactification et la réduction des espaces de modules de courbes ou de revêtements, on pourra aussi consulter les articles [Fu], [DelMu], [HarMu] et les plus récents [Ek], [Mo] et [Wew].

## 2.3. Le revêtement $\mathcal{H}_G \to \mathcal{U}_r$

Pour tout $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$, la fibre $\psi^{-1}(\mathbf{t})$ est en bijection avec

- l'ensemble des classes d'équivalence de revêtements de monodromie $G \subset S_d$ et de points de ramification donnés, ou, de façon équivalente,
- l'ensemble des homomorphismes surjectifs $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G$, à équivalence près dans $S_d$, du groupe fondamental $\pi_1(\mathbb{P}^1 - \mathbf{t})$ (qui est isomorphe au groupe libre $F(x_1,\dots,x_r)/x_1\cdots x_r$) dans $G$, ou, de façon équivalente,
- l'ensemble $\mathrm{ni}_G^{\mathrm{ab}} = \left\{ (g_1,\dots,g_r) \in G^r \;\middle|\; \begin{array}{l} g_1\cdots g_r = 1 \\ \langle g_1,\dots,g_r\rangle = G \end{array} \right\} \;/\; \mathrm{Nor}_{S_d}(G)$.

Le groupe fondamental de $\mathcal{U}_r(\mathbb{C})$ est un groupe de tresses, le groupe $H_r$ des tresses d'Hurwitz. Il peut être décrit par générateurs et relations. Plus précisément, le groupe des tresses d'Artin $B_r$ est le groupe engendré par $r-1$ générateurs $Q_1,\dots,Q_{r-1}$ modulo les relations

$$\begin{cases} Q_iQ_j = Q_jQ_i \text{ pour } |i-j| > 1 \\ Q_{i+1}Q_iQ_{i+1} = Q_iQ_{i+1}Q_i \text{ pour } 1 \le i \le r-2 \end{cases}$$

Si on ajoute la relation $Q_1\cdots Q_{r-1}Q_{r-1}\cdots Q_1 = 1$, on obtient le groupe des tresses d'Hurwitz. Pour un certain choix (standard) d'un isomorphisme entre $\pi_1(\mathbb{P}^1-\mathbf{t})$ et le groupe libre $F(x_1,\dots,x_r)/x_1\cdots x_r$, l'action de monodromie associée au revêtement $\mathcal{H}_G \to \mathcal{U}_r$ est l'action de $H_r$ sur $\mathrm{ni}_G^{\mathrm{ab}}$ donnée par la formule suivante (qu'on trouve déjà dans [Hu]; voir aussi [Fr2] et [FrVo]): pour $\mathbf{g} = (g_1,\dots,g_r) \in \mathrm{ni}_G^{\mathrm{ab}}$,

$$(\mathbf{g})Q_i = (g_1,\dots,g_{i-1},g_ig_{i+1}g_i^{-1},g_i,g_{i+2},\dots,g_r), \quad i = 1,\dots,r-1.$$

**Proposition 2.2.** *Les composantes connexes (et donc irréductibles*[2]*) de $\mathcal{H}_G$ correspondent aux orbites de l'action de $H_r$ sur $\mathrm{ni}_G^{\mathrm{ab}}$.*

2) car le revêtement $\psi : \mathcal{H}_G \to \mathcal{U}_r$ est étale.

Localement sur $\mathcal{H}_G(\mathbb{C})$, l'inertie $\mathbf{C} = \{C_1, \ldots, C_r\}$ ne change pas (*e.g.* [DeFr1; Lemma 1.5]); l'inertie est donc constante dans toute composante irréductible de $\mathcal{H}_G(\mathbb{C})$. Etant donné $\mathbf{C}$, on note $\mathcal{H}_G(\mathbf{C})(\mathbb{C})$ le sous-ensemble de $\mathcal{H}_G(\mathbb{C})$ constitué des points représentant des revêtements d'inertie $\mathbf{C}$; c'est une réunion de composantes connexes de $\mathcal{H}_G(\mathbb{C})$, qui est connexe (et irréductible) si et seulement si $H_r$ agit transitivement sur l'ensemble

$$\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}} = \left\{ (g_1, \ldots, g_r) \in G^r \;\middle|\; \begin{array}{l} g_1 \cdots g_r = 1 \\ \langle g_1, \ldots, g_r \rangle = G \\ g_i \in C_i \text{ (à l'ordre près)} \end{array} \right\} / \mathrm{Nor}_{S_d}(G)$$ [3)]

Sans l'indication "à l'ordre près", l'ensemble obtenu est un sous-ensemble de $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ noté $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$.

## 2.4. Premiers exemples

**2.4.1. Une famille de polynômes de degré 5** [DeFr1]. On prend $G = S_5$ (plongé dans lui-même), $r = 4$; $C_2 = C_3$ est la classe des 2-cycles, $C_1$ est la classe des produits de deux 2-cycles disjoints et $C_4$ celle des 5-cycles. Un premier calcul conduit à la liste des éléments $(g_1, \ldots, g_4)$ de $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Ceux pour lesquels $g_i \in C_i$, $i = 1, \ldots, 4$ et $g_4 = (54321)$ sont les suivants (on donne $g_1, g_2, g_3$):

(a) $((23)(45), (12), (14))$ (b) $((23)(45), (14), (24))$
(c) $((23)(45), (24), (12))$ (d) $((25)(34), (12), (35))$
(e) $((25)(34), (35), (12))$.

L'espace de Hurwitz $\mathcal{H}_G(\mathbf{C})$ paramètre des revêtements $f : X \to \mathbb{P}^1$ de genre $g = 0$ $(2(5 + g - 1) = 2 + 1 + 1 + 4 = 8)$. Si on impose que le point de ramification d'inertie dans $C_4$ est $\infty$, le revêtement $f : \mathbb{P}^1 \to \mathbb{P}^1$ est donné par un polynôme.

On vérifie que $Q_1^2$ et $Q_2^2$ agissent sur la liste ci-dessus de la façon suivante:

$$\begin{cases} Q_1^2 : (a\ e\ c)(b\ d) \\ Q_2^2 : (a\ c\ b)(d\ e) \end{cases}$$

L'action de $H_r$ sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est donc transitive. L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible.

**2.4.2. Irréductibilité de $\mathcal{M}_g$.** Etant donné un entier $g \geq 0$, on prend $G = S_d$ où $d \geq g + 1$, $r = 2g + 2d - 2$, $C_i = C$ est la classe des 2-cycles, $i = 1, \ldots, r$. Toute courbe de genre $g$ peut être présentée comme revêtement simple de $\mathbb{P}^1$, *i.e.*, avec seulement des points de ramification d'inertie associée dans $C$. Cela donne une surjection $\mathcal{H}_G(\mathbf{C}) \to \mathcal{M}_g$. Des calculs de Lurôth et Clebsch [Cl] montrent que l'action de $H_r$ sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est transitive. L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible; son image $\mathcal{M}_g$ l'est donc aussi. Historiquement, l'espace $\mathcal{H}_G(\mathbf{C})$, considéré par

3) *Stricto sensu* ce n'est pas le normalisateur $\mathrm{Nor}_{S_d}(G)$ qui agit mais le sous-groupe des éléments qui laissent globalement invariant l'ensemble $\{C_1, \ldots, C_r\}$.

Hurwitz, est le premier espace de modules de revêtements qui apparait dans la littérature [Hu]. L'argument ci-dessus pour prouver l'irréductibilité de $\mathcal{M}_g$ en caractéristique 0 est donné dans un article de Severi [Sev]. Le cas de caractéristique $p > 0$ sera traité par la suite par Fulton [Fu] et Deligne-Mumford [DelMu].

**2.4.3. Irréductibilité des courbes modulaires** (Fried). Les courbes modulaires peuvent être présentées comme quotients d'espaces de Hurwitz paramétrant des revêtements galoisiens de $\mathbb{P}^1$ de groupe diédral avec 4 points de ramification (voir §3.1.4). Comme précédemment, on montre que cet espace de Hurwitz est irréductible en vérifiant la transitivité de l'action de $H_4$ associée.

## 2.5. Préalable géométrique

L'utilisation des espaces de Hurwitz pour des questions arithmétiques dépend de la possibilité d'y trouver des points rationnels. La recherche de points $K$-rationnels commence par celle de composantes irréductibles définies sur $K$. Pour cela, on dispose des résultats suivants.

### 2.5.1. Critères d'irréductibilité

• *Critère général.* L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible si et seulement si $H_r$ agit transitivement sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. De plus, $\mathcal{H}_G$ est défini sur $\mathbb{Q}$, donc $G_{\mathbb{Q}}$ permute les espaces $\mathcal{H}_G(\mathbf{C})$. Précisément, on a, pour tout $\tau \in G_{\mathbb{Q}}$,

$$\mathcal{H}_G(\mathbf{C})^{\tau} = \mathcal{H}_G(\mathbf{C}^{\chi(\tau)})$$

où $\chi : G_{\mathbb{Q}} \to \mathbb{Z}/n\mathbb{Z}$ ($n = card(G)$) est le caractère cyclotomique. Le corps de définition de $\mathcal{H}_G(\mathbf{C})$ est un corps cyclotomique, qu'on peut explicitement déterminer, et qui est égal à $\mathbb{Q}$ sous des hypothèses supplémentaires assez simples, par exemple, si les classes $C_1, \ldots, C_r$ sont *rationnelles* (*i.e.*, invariantes par toute élévation à une puissance première à l'ordre de leurs éléments).

*Observations*: l'application de ce critère demande des calculs compliqués, faisables en pratique uniquement pour des petites valeurs de $r$.

• *Critère de Conway-Parker* [FrVo; appendix]. Supposons le groupe $G$ de centre trivial et de multiplicateur de Schur engendré par les commutateurs. Si chaque classe $C \neq \{1\}$ est répétée suffisamment souvent dans $\mathbf{C}$, alors $H_r$ agit transitivement sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. En conséquence, $\mathcal{H}_G(\mathbf{C})$ est irréductible et défini sur $\mathbb{Q}$.

*Observations*: ce critère n'est utilisable que pour des grandes valeurs de $r$; de plus la borne pour $r$ n'est pas effective.

• *Inertie de type Harbater-Mumford* (Fried) [Fr6]. Un élément $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ est dit de type HM s'il est de la forme $\mathbf{g} = (g_1, g_1^{-1}, \ldots, g_s, g_s^{-1})$. Fried a montré que, sous quelques hypothèses techniques (dont $Z(G) = \{1\}$), les éléments $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ de type HM sont dans une même orbite de $H_r$ et que la composante connexe correspondante est définie sur $\mathbb{Q}$.

**2.5.2. Critères d'(uni-)rationalité.** Rappelons qu'une $K$-variété $V$ est dite *rationnelle* si son corps de fonctions $K(V)$ est une extension transcendante pure de $K$, ou, de façon équivalente, si $V$ est birationnelle sur $K$ à un ouvert d'un espace projectif $\mathbb{P}^r$; $V$ est dite *unirationnelle* si $K(V)$ est contenu dans une extension transcendante pure de $K$. On dispose de critères de rationalité pour la variété $\mathcal{H}'_G(\mathbf{C})$. Le $'$ indique qu'on a adjoint les points de ramification: $\mathcal{H}'_G(\mathbf{C})$ est une composante connexe (quelconque) du produit fibré de $\mathcal{H}_G(\mathbf{C})$ avec $\mathcal{U}^r$ (défini en §2.1) au-dessus de $\mathcal{U}_r$; le corps des fonctions de $\mathcal{H}'_G(\mathbf{C})$ est celui de $\mathcal{H}_G(\mathbf{C})$ avec les indéterminées $t_1, \ldots, t_r$ adjointes.

• *Rigidité* (Belyi, Fried, Matzat, Shih, Thompson; voir [Se2]). Le cardinal des ensembles $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$ [resp. $\mathrm{sni}_G(\mathbf{C})^{\mathrm{in}}$] peut être calculé explicitement, à la main ou par ordinateur pour des petites valeurs de $r$; il existe aussi une formule faisant intervenir les caractères de $G$. La rigidité est un ensemble d'hypothèses qui garantit que ce nombre vaut 1. Dans ce cas, le revêtement $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{ab}} \to \mathcal{U}^r$ [resp. $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}^r$] est un isomorphisme; le corps de définition d'un revêtement [resp. d'un G-revêtement] d'inertie $\mathbf{C}$ est celui de ses points de ramification.

• *Un autre cas de rationalité* [FrBi], [Fr4], [Fr5]. Supposons $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$ irréductible. On peut en privilégiant une des variables $t_1, \ldots, t_r$, par exemple $t_1$, voir la flèche $\mathcal{H}' \to \mathcal{U}^r$ comme une famille $\mathcal{H}'_{t_2,\ldots,t_r}$ de revêtements de $\mathbb{P}^1$ paramétrée par les $r-1$ autres variables. La ramification de ces revêtements est connue: ils sont ramifiés aux points $t_2, \ldots, t_r$ et les cycles de ramification associés sont donnés par des formules explicites dans un groupe de tresses approprié. Le genre de la courbe $\mathcal{H}'_{t_2,\ldots,t_r}$ s'obtient grâce à la formule de Riemann-Hurwitz. Dans certaines situations, l'examen de la ramification permet également de conclure à l'existence générique d'un point rationnel au-dessus d'un des points de ramification $t_2, \ldots, t_r$. Si c'est le cas et si le genre est nul, la variété $\mathcal{H}'$ est une variété rationnelle.

• *Critères d'unirationalité* (Fried [DeFr4]). Fried a établi un critère d'unirationalité de l'espace $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$. Il conjecture d'autre part que, sous certaines hypothèses sur $G$ et si $r$ assez grand, l'espace $\mathcal{H}'_G(\mathbf{C})$ est unirationnel.

**2.5.3. Existence de familles de Hurwitz.** Les espaces de Hurwitz ont été introduits *a priori* comme des espaces de modules grossiers. Se pose naturellement la question de l'existence d'une famille au-dessus d'un espace de Hurwitz $\mathcal{H}$, *i.e.*, d'un revêtement $\mathcal{T} \to \mathcal{H} \times \mathbb{P}^1$ tel que, pour tout $[f] \in \mathcal{H}$, le revêtement-fibre $\mathcal{T}_{[f]} \to [f] \times \mathbb{P}^1$ au-dessus de $\{[f]\}$ soit un revêtement équivalent à $f$. Et dans le cas où il existe une famille, est-elle universelle?

Dans son article [Fr2], Fried montre que la réponse à ces deux questions est positive dans le cas où les revêtements paramétrés par $\mathcal{H}$ n'ont pas d'automorphismes (non triviaux), ou, de façon équivalente, si $\mathrm{Cen}_{S_d}(G) = \{1\}$; $\mathcal{H}$ est dans ce cas un espaces de modules *fin*. Le point est que les familles de Hurwitz existent au moins localement; l'absence d'automorphismes permet ensuite de construire une famille au-dessus de $\mathcal{H}$ entier par recollement. Ce résultat, démontré pour les revêtements purs, s'étend au cas des G-revêtements ([CoHa], [FrVo]); l'absence d'automorphismes s'exprime dans ce cas par la condition $Z(G) = \{1\}$. Les es-

paces de Hurwitz sont également des espaces de modules fins dans la situation de revêtements *pointés* ([CoHa], [Em]); là aussi, le point est qu'un revêtement pointé n'a pas d'automorphismes.

Le problème est plus difficile dans le cas où les objets ont des automorphismes non triviaux. Il y a alors une obstruction à l'existence d'une famille au-dessus de $\mathcal{H}$, qui est de nature cohomologique. Dans la situation de G-revêtements, l'obstruction peut être mesurée par une classe dans $H^2(\pi_1(\mathcal{H}), Z(G))$. Le problème est plus complexe dans la situation de revêtements purs puisqu'il se pose en termes de cohomologie non abélienne: l'obstruction "vit" dans le groupe $H^2(\pi_1(\mathcal{H}), \mathrm{Cen}_{S_d}(G))$. On peut, en procédant comme dans [DeDo1], ramener la question dans $H^2(\pi_1(\mathcal{H}), Z(G))$. D'un point de vue théorique, l'outil le mieux adapté est la notion de *gerbe*, introduite par Grothendieck et Giraud (voir [DeDoEm]).

# 3. Le problème inverse de Galois

Cette section revient sur les résultats sur le problème inverse de Galois obtenus par le biais des espaces de Hurwitz. On s'intéresse en fait à la forme *régulière* du problème inverse de Galois.

**Problème.** *Etant donné un corps $K$, tout groupe fini $G$ est-il le groupe de Galois d'une extension galoisienne $E/K(T)$ régulière*[4] *sur $K$? ou, de façon équivalente, le groupe d'automorphismes d'un revêtement galoisien $f : X \to \mathbb{P}^1$, défini sur $K$ comme G-revêtement?*

Dans sa forme originale, le problème est posé avec $\mathbb{Q}$ à la place de $K(T)$. Cette forme se déduit de la forme régulière sur $\mathbb{Q}(T)$ grâce au théorème d'irréductibilité de Hilbert. Etant donné un groupe fini $G$, réaliser $G$ sur $\mathbb{Q}(T)$ régulièrement revient à trouver au moins un point $\mathbb{Q}$-rationnel sur un espace de Hurwitz $\mathcal{H}_G^{\mathrm{in}}$ de G-revêtements. Dans la suite de cette section, on distingue deux types de résultats suivant que l'on travaille avec un groupe donné (§3.1) ou sur un corps fixé (§3.2). Nous renvoyons à [De1] et [DeDes] respectivement pour plus de détails et une bibliographie plus complète.

## 3.1. Le problème avec $G$ fixé sur $\mathbb{Q}$

**3.1.1. Le cas rigide** (Thompson, et al.). C'est le cas le plus simple (voir §2.5.2): $\mathcal{H}'_G(\mathbf{C})^{\mathrm{in}}$ est isomorphe sur $\mathbb{Q}$ à $\mathcal{U}^r$ (*via* $\psi'$). Les hypothèses rigides, qui entraînent que les revêtements en question sont déterminés par leurs points de ramification, sont assez contraignantes. Certains groupes les satisfont cependant, le groupe symétrique $S_d$, le Monstre [Th], par exemple. Ce cas ne nécessite pas strictement

4) c'est-à-dire, $G = G(E/K(T)) = G(E\overline{K}/\overline{K}(T))$.

l'introduction des espaces de Hurwitz, mais il est le point de départ de la méthode modulaire et en a assuré la promotion.

**3.1.2. Autres cas de rationalité** (Matzat). En utilisant le second critère de rationalité expliqué plus haut (§2.5.2), Matzat a réussi à réaliser sur $\mathbb{Q}(T)$ (régulièrement) un certain nombre de groupes simples, en particulier des groupes sporadiques (seul $M_{23}$ résiste encore, tous les autres ont été réalisés). La méthode a été développée par l'école d'Heidelberg (Matzat, Malle, et al.), ce qui a donné lieu à de nombreux travaux, à de nombreuses variantes du critère original et de nombreuses autres réalisations de groupes (voir [MaMa] pour un point des résultats). Cette approche est un des grands succès de la théorie des espaces de Hurwitz. Elle est cependant vraisemblablement insuffisante pour traiter la totalité du problème. Elle s'applique groupe par groupe et demande des calculs assez compliqués. Sa systématisation est improbable: le genre de $\mathcal{H}'_{t_2,\ldots,t_r}$ (cf. §2.5.2), qui doit être nul dans la méthode, n'est pas borné en général [DeFr3; §4].

**3.1.3. Un raffinement de Völklein-Strambach** [StrVo]. La méthode précédente consiste à trouver une composante rationnelle de $\mathcal{H}_G(\mathbf{C})$ qui soit définie sur $\mathbb{Q}$; on utilise pour cela la présentation de $\mathcal{H}_G(\mathbf{C})$ comme revêtement de $\mathcal{U}_r$. Völklein et Strambach fixent une sous-variété fermée $\mathcal{P}$ de $\mathcal{U}_r$ et regardent à quelles conditions on peut trouver une variété rationnelle définie sur $\mathbb{Q}$ au-dessus de $\mathcal{P}$. La variété $\mathcal{P}$ avec laquelle ils travaillent est celle des ensembles de $r$ points symétriques par rapport à l'origine. Son groupe fondamental a une description concrète: ils l'appellent le groupe de tresses de type symplectique. La méthode précédente peut être mise en place dans ce contexte; ils obtiennent des critères de rationalité de même nature. Comme application, ils parviennent à réaliser certains groupes $\mathrm{Sp}_n(4^s)$.

**3.1.4. Groupes diédraux et courbes modulaires** [Fr3], [DeFr3]. Décider si un espace de Hurwitz a ou non des points rationnels est un problème difficile. Par exemple, dans la situation suivante, cela est équivalent à trouver à trouver des points rationnels sur une courbe modulaire.

On prend $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ et toutes les classes $C_i$, $i = 1, \ldots, 4$ égales à la classe $C$ des involutions de $G$. On montre qu'il existe un morphisme surjectif, défini sur $\mathbb{Q}$

$$\chi : \mathcal{H} = \mathcal{H}_G^{\mathrm{in}}(\mathbf{C}) \to X_1(p) - \{\text{pointes}\}$$

En conséquence, d'après le théorème de Mazur, si $p > 7$, $\mathcal{H}(\mathbb{Q}) = \emptyset$; le groupe diédral $D_p$ ne peut donc être réalisé sur $\mathbb{Q}(T)$ régulièrement avec ces contraintes sur la ramification. En fait, quelques observations supplémentaires montrent que le groupe diédral $D_p$ ne peut être réalisé avec moins de 6 points de ramification (alors qu'il en suffit de 3 pour le Monstre). Nous conjecturons que pour $r_0$ fixé, on ne peut réaliser régulièrement sur $\mathbb{Q}(T)$ qu'un nombre fini de groupes diédraux $D_p$ avec moins de $r_0$ points de ramification. Cela résulterait de conjectures de Mazur-

Kamienny [MaKa] sur la finitude des nombres premiers qui sont ordre d'un point rationnel sur une variété abélienne de dimension donnée sur $\mathbb{Q}$.

*Indications sur la construction de* $\chi$. Supposons donné un revêtement $f : E \to \mathbb{P}^1$ défini et galoisien sur $\mathbb{Q}$, de groupe $D_p$, ramifié en 4 points et d'inertie dans $\mathbf{C}$. La formule de Riemann-Hurwitz donne le genre $g$ de $E$: $2g-2 = 2p(-2)+4p$ soit $g = 1$. Quitte à remplacer $E$ par $Pic^o(E)$, on peut supposer que $E$ a un point $\mathbb{Q}$-rationnel et donc est une courbe elliptique sur $\mathbb{Q}$. Les éléments d'ordre $p$ de $D_p$ sont des automorphismes de $E$ d'ordre $p$ définis sur $\mathbb{Q}$. Ce sont des translations par un point p de $p$-torsion définis sur $\mathbb{Q}$. On sait que la donnée $(E, \mathrm{p})$ correspond à un point de la courbe modulaire $X_1(p)$ qui n'est pas une pointe.

Inversement, soit $(E, \mathrm{p})$ une courbe elliptique munie d'un point de $p$-torsion, tous deux définis sur $\mathbb{Q}$. Le revêtement $E \to E/\langle \mathrm{p} \rangle$ est cyclique d'ordre $p$. La courbe $E_0 = E/\langle \mathrm{p} \rangle$ est une courbe elliptique définie sur $\mathbb{Q}$. Si on compose le revêtement précédent avec le revêtement $E_0 \to E_0/\langle -1 \rangle = \mathbb{P}^1$ (où $-1$ est l'involution canonique de $E$), on obtient un revêtement $E \to \mathbb{P}^1$ défini et galoisien sur $\mathbb{Q}$, de groupe $D_p$, ramifié en 4 points et d'inertie dans $\mathbf{C}$. □

## 3.2. Le problème avec $K$ fixé pour tout $G$

Plutôt que de chercher à réaliser un groupe donné sur $\mathbb{Q}(T)$, on peut fixer un corps $K$ et chercher à réaliser le plus grand nombre possible de groupes sur $K(T)$.

**3.2.1. Réduction du problème** [FrVo]. Fried et Völklein ont montré qu'à chaque groupe fini $G$, on peut associer une infinité d'espaces de Hurwitz $\mathcal{H}_G^{\mathrm{in}}(\mathbf{C})$, irréductibles et définis sur $\mathbb{Q}$ tels que l'existence d'un point $K$-rationnel sur l'un d'eux suffit pour conclure que $G$ est groupe de Galois sur $K(T)$ régulièrement.

Le point ici est que les espaces $\mathcal{H}_G^{\mathrm{in}}(\mathbf{C})$ sont irréductibles. Fried et Völklein utilisent le critère de Conway-Parker (§2.5.1). Plus précisément, ils commencent par se placer sur une extension $\widetilde{G}$ de $G$ vérifiant les hypothèses du critère de Conway-Parker ($Z(G) = \{1\}$, etc.); il faut donc démontrer un lemme préalable de théorie des groupes qui assure l'existence d'une telle extension. Puis ils considèrent un uplet $\widetilde{\mathbf{C}}$ où chaque classe de conjugaison de $\widetilde{G}$ non triviale est répétée aussi souvent que le requiert le critère de Conway-Parker. L'espace $\mathcal{H}_{\widetilde{G}}^{\mathrm{in}}(\widetilde{\mathbf{C}})$ est alors irréductible, défini sur $\mathbb{Q}$ et tout point $K$-rationnel dessus fournit une réalisation régulière sur $K$ de $\widetilde{G}$ et donc de $G$.

*Observations.* Conway et Parker ne donnent pas une borne effective du nombre de répétitions nécessaires de chaque classe de conjugaison. Mais il y a maintenant une alternative à l'utilisation de Conway-Parker, et qui elle est effective. Il s'agit du critère d'irréductibilité des espaces de Hurwitz $\mathcal{H}_G(\mathbf{C})$ pour une inertie $\mathbf{C}$ de type Harbater-Mumford (voir §2.5.1).

**3.2.2. Les résultats.** Cette approche a permis la résolution du problème inverse de Galois (forme régulière) sur les corps $K$ suivants:

• $K$ Pseudo Algébriquement Clos de caractéristique 0 (Fried-Völklein [FrVo]). Les ultra-produits de corps finis constituent les exemples type de corps PAC. Le résultat de Fried-Völklein fournit cette conséquence: tout groupe $G$ est réalisable régulièrement sur $\mathbb{F}_p(T)$, pour tout $p$ sauf un nombre fini.

• $K = \mathbb{Q}^{tr} = \{\text{nombres algébriques totalement réels}\}$ (Dèbes-Fried [DeFr3]).

• $K = \mathbb{Q}^{tp} = \{\text{nombres algébriques totalement } p\text{-adiques}\}$ (Dèbes [De2]).

Pour ces deux derniers cas, on utilise un résultat de Pop [Po; appendix] selon lequel une variété lisse définie sur $\mathbb{Q}$ a des points totalement $p$-adiques si elle a des points $p$-adiques (y compris pour $p = \infty$). Les points réels d'un espace de Hurwitz peuvent être déterminés de façon très explicite car l'action de la conjugaison complexe sur les revêtements de $\mathbb{P}^1$ est parfaitement connue ([Hu], [KrNe], [DeFr2]). Pour construire des espaces de Hurwitz $\mathcal{H}_G^{\text{in}}$ avec des points $p$-adiques (*i.e.*, des revêtements définis sur $\mathbb{Q}_p$), on utilise des techniques de recollements d'espaces analytiques formels ou rigides, dues à Harbater [Ha].

• B. Deschamps [Des] a repris la construction précédente et montré que l'espace de Hurwitz $\mathcal{H}_G^{\text{in}}(\mathbf{C})$ contenant des points $p$-adiques pouvait être construit indépendant de $p$. Précisément, il démontre qu'à chaque groupe fini $G$, on peut associer une infinité d'espaces de Hurwitz $\mathcal{H}_G^{\text{in}}(\mathbf{C})$, irréductibles et définis sur $\mathbb{Q}$ et possédant des points $p$-adiques pour tout nombre premier, y compris $p = \infty$.

• Les résultats précédents ont été généralisés par Pop [Po]. Le problème inverse de Galois (forme régulière sur $K(T)$) est maintenant résolu pour tout corps $K$ *ample*. Un corps $K$ est dit ample si toute courbe lisse définie sur $K$ a une infinité de points $K$-rationnels si elle en a au moins un. Les corps PAC, les corps valués complets, les corps $\mathbb{Q}^{tp}$, etc. sont amples.

# 4. Autres applications arithmétiques

Cette section en donne quatre. Nous développons plus particulièrement la première, qui concerne le problème de Hilbert-Siegel (§4.1 et §4.2). D'autres applications au problème de Davenport et au théorème de Mason-Stothers (§4.3) sont mentionnées plus rapidement. On termine par un critère d'existence de points rationnels sur des revêtements utilisant la monodromie sous-jacente des espaces de Hurwitz (§4.4).

## 4.1. Le problème de Hilbert-Siegel [Fr5]

Fried appelle ainsi le problème suivant (en référence à une observation de Siegel dans [Si]). Il s'agit de déterminer les polynômes $h(Y) \in \mathbb{Q}[Y]$ tels que $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} - h(\mathbb{Q})$. On supposera $h$ indécomposable (dans le cas contraire $h(Y) = h_1(h_2(Y))$ et $h(Y) - t$ est réductible pour tout $t$ de la forme $t = h_1(z)$, $z \in \mathbb{Q}$). On a le résultat suivant.

**Théorème 4.1** (Fried). *Les seuls polynômes indécomposables $h(Y) \in \mathbb{Q}[Y]$ pour lesquels $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z}-h(\mathbb{Q})$ sont de degré 5.*

*Schéma de preuve.* Considérons une factorisation non triviale $h(Y) - T = Q(Y)R(Y)$ dans $\overline{\mathbb{Q}}(T)$. Soit $F \subset \overline{\mathbb{Q}}(T)$ le corps engendré par les coefficients de $Q$ et $R$. Le corps $F$ est une extension stricte de $\overline{\mathbb{Q}}(T)$, laquelle correspond à un revêtement $f : C \to \mathbb{P}^1$. Les nombres rationnels $t \in \mathbb{Q}$ tels que $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ correspondent (sauf éventuellement pour un nombre fini d'entre eux) aux spécialisations $\mathbb{Q}$-rationnelles d'un des corps $F$ associés aux diverses factorisations possibles de $h(Y) - T$ dans $\overline{\mathbb{Q}}(T)$ [5], ou, de façon équivalente, aux valeurs $f(\mathrm{m})$ prises par $f$ en un point $\mathbb{Q}$-rationnel m sur une des courbes $C$ correspondantes.

Supposons que $h(Y) - t$ soit réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z}-h(\mathbb{Q})$. D'après le théorème de Siegel sur les points entiers des courbes algébriques, il existe au moins une des courbes $C$ (en dehors de la courbe $h(y) = t$) qui est $\mathbb{Q}$-birationnelle à $\mathbb{P}^1$ et telle que la fonction $g$ a ou bien un pôle $\mathbb{Q}$-rationnel ou bien deux pôles quadratiques réels. Autrement dit, il existe des fractions rationnelles non-constantes $g_1(Z), \ldots, g_s(Z) \in \mathbb{Q}(Z)$ avec $s \geq 1$ vérifiant:

- $h(Y) - g_i(Z)$ réductible dans $\overline{\mathbb{Q}}(Z)[Y]$, $i = 1, \ldots, s$.
- Le dénominateur de chaque $g_i(Z)$ est de la forme $(Z - a)^\ell$ avec $a \in \mathbb{Q}$ ou $(z^2 + pZ + q)^\mu$ avec $p^2 - 4q > 0$.
- $g_i(Z)$ ne se déduit pas de $h(Z)$ par changement de variable $(z \leftrightarrow (az+b)/(cz+d))$, $i = 1, \ldots, s$.
- Pour tout $t \in \mathbb{Z}-h(\mathbb{Q})$ (sauf un nombre fini), $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ si et seulement si il existe $i \in \{1, \ldots, s\}$ tel que $t = g_i(z)$ avec $z \in \mathbb{P}^1(\mathbb{Q})$.

Fixons un indice $i$ et posons $g_i = g$. La première condition signifie que le produit fibré des deux revêtements de $\mathbb{P}^1$ induits par $h(Y)$ et $g(Y)$ est réductible. Le point suivant de la preuve de Fried est de montrer que les clôtures galoisiennes sur $\overline{\mathbb{Q}}(T)$ des deux polynômes $h(Y) - T$ et $g(Y) - T$ sont nécessairement égales [Fr1]. Notons $G$ le groupe de Galois de cette extension galoisienne. Les deux revêtements correspondent à deux représentations transitives $T_h : G \to S_n$ et $T_g : G \to S_m$. Les deux revêtements sont de genre 0; cela fournit, *via* la formule de Riemann-Hurwitz, une première condition sur les représentations $T_h$ et $T_g$. Les quatre points ci-dessus se traduisent de la façon suivante. On note $T_g(1)$ [resp. $T_h(1)$] le fixateur de 1 dans la représentation $T_g$ [resp. $T_h$].

- La restriction de $T_g$ à $T_h(1)$ n'est pas transitive.
- Il existe $\sigma \in G$ tel que $T_h(\sigma)$ est un $n$-cycle et $T_g(\sigma)$ est, soit un $m$-cycle, soit le produit de deux $\mu$-cycles.
- $T_h(1)$ ne contient aucun conjugué de $T_g(1)$.

5) L'existence de telles spécialisations de $F$ entraîne que $F$ est une extension régulière de $\mathbb{Q}$.

Enfin, il est classique que l'hypothèse "$h(Y)$ indécomposable" est équivalente à la condition

- La représentation $T_h : G \to S_n$ est primitive.

Le reste de la preuve est un travail de théorie des groupes. En utilisant la classification des groupes simples, on montre que l'existence de telles représentations n'est possible que si $n = 5$, $m = 10$ et $G = S_5$ ou $G = A_5$. □

**Remarque 4.2.** Cette approche du problème a été développée par P. Mueller [Mu]. Soit $f(T, Y) \in \mathbb{Q}[T, Y]$ absolument irréductible. Supposons que, pour une infinité de $t \in \mathbb{Z}$, $f(t, Y)$ est réductible mais n'a pas de facteur linéaire. Peut-on conclure que nécessairement $\deg_Y(f) = 5$? Mueller a montré que oui si le groupe de Galois de $f(T, Y)$ sur $\overline{\mathbb{Q}}(T)$ est le groupe symétrique ou si $\deg_Y(f)$ est premier.

## 4.2. Etude d'un cas exceptionnel où $\deg(h) = 5$ ([DeFr1], [DeFr4])

La résolution du problème de Hilbert-Siegel conduit à une description précise des cas exceptionnels de degré 5. L'un d'eux est le suivant. Les deux revêtements $h$ et $g$ sont de groupe $S_5$, sont ramifiés en $r = 4$ points de $\mathbb{P}^1$. Les cycles de ramification sont du type suivant (dans $S_5$):

- pour $h$: (2)(2) ; (2) ; (2) ; (5)

On notera $\mathbf{C}$ l'ensemble des 4 classes de conjugaison de $S_5$ correspondantes. On retrouve l'exemple vu en §2.4.1. La représentation $T_h : S_5 \to S_5$ est donnée par l'action standard de $S_5$ sur $\{1, \ldots, 5\}$. La représentation $T_g : S_5 \to S_{10}$ est donnée par l'action de $S_5$ sur les 10 paires $\{i, j\}$ d'éléments distincts de $\{1, \ldots, 5\}$. (Ce cas exceptionnel correspond à la situation où l'on part d'une décomposition *a priori* $h(Y) - T = Q(Y)R(Y)$ dans $\overline{\mathbb{Q}(T)}$ avec un des facteurs de degré 2). On en déduit le type des cycles de ramification (dans $S_{10}$):

- pour $g$: (2)(2)(2)(2) ; (2)(2)(2) ; (2)(2)(2) ; (5)(5)

On s'intéresse ici à la question suivante: existe-t-il un polynôme $h(Y) \in \mathbb{Q}[Y]$ satisfaisant les hypothèses de ce cas et qui est réellement exceptionnel, *i.e.*, pour lequel $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z}$–$h(\mathbb{Q})$? Introduisons l'espace de Hurwitz $\mathcal{H} = \mathcal{H}_{S_5}(\mathbf{C})$ [6]. L'espace $\mathcal{H}$ est irréductible (§2.4.1). De plus, comme $\mathrm{Cen}_{S_5}(S_5) = \{1\}$ et $\mathrm{Cen}_{S_{10}}(S_5) = \{1\}$, $\mathcal{H}$ est un espace de modules fin (§2.5.3): il existe au-dessus de $\mathcal{H}$ une famille universelle $\mathcal{F}_5$ [resp. $\mathcal{F}_{10}$] de revêtements de degré 5 [resp. de degré 10] ayant les caractéristiques ci-dessus. La question se reformule ainsi:

6) A priori, $S_5$ est plongé, d'une part dans lui-même et d'autre part dans $S_{10}$, et il faudrait distinguer les deux situations. Mais on vérifie que le nombre d'éléments dans $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est le même dans les deux situations, si bien que les deux espaces de Hurwitz sont isomorphes.

**Question 4.3.** *Existe-t-il un point* $[h] \in \mathcal{H}(\mathbb{Q})$ *tel que*

(*) *le revêtement correspondant* $h : \mathbb{P}^1 \to \mathbb{P}^1$ *de la famille* $\mathcal{F}_5$ *est un revêtement polynomial et le revêtement correspondant* $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ *de la famille* $\mathcal{F}_{10}$ *a la propriété que* $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap \mathbb{Z}$ *est infini et que* $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap h(\mathbb{Q}) \cap \mathbb{Z}$ *est fini?*

On peut décrire plus concrètement le revêtement $\gamma_{[h]}$: en termes de corps de fonctions, le revêtement $h : \mathbb{P}^1 \to \mathbb{P}^1$ correspond à l'extension $\overline{\mathbb{Q}}(y_1)/\overline{\mathbb{Q}}(T)$, où $y_1$ est l'une des 5 racines dans $\overline{\mathbb{Q}(T)}$ de $h(Y) - T$. Le revêtement $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ correspond alors à l'extension $\overline{\mathbb{Q}}(y_1 + y_2, y_1 y_2)/\overline{\mathbb{Q}}(T)$.

**Théorème 4.4** (Dèbes-Fried [DeFr4]). *L'ensemble des points* $[h] \in \mathcal{H}(\mathbb{Q})$ *tels que* (*) *a lieu est Zariski-dense. En conséquence, il existe* $h(Y) \in \mathbb{Q}[Y]$ *indécomposable et tel que* $h(Y) - t$ *est réductible dans* $\mathbb{Q}[Y]$ *pour une infinité de* $t \in \mathbb{Z} - h(\mathbb{Q})$.

*Schéma de preuve.* La preuve comporte les points suivants.

• $\mathcal{F}_{10}$ est une famille de revêtements de genre 0. De plus, l'ensemble des points de $\mathcal{H}(\mathbb{C})$ pour lesquels le revêtement correspondant dans la famille $\mathcal{F}_{10}$ a les trois propriétés suivantes, est Zariski-dense:
— le revêtement est défini sur $\mathbb{R}$,
— $\infty$ est le point de ramification d'inertie dans $C_4$,
— les deux points dans la fibre au-dessus de $\infty$ sont réels.

Ce premier point est une condition nécessaire pour que la conclusion du Th. 4.4 soit vraie. Pour étudier les conditions ci-dessus, qui sont de nature "réelle", on dispose de critères de pure théorie des groupes portant sur l'ensemble $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Nous renvoyons à [DeFr4] pour plus de détails.

• $\mathcal{H}$ est unirationnel: Soit $\mathcal{M} = (\mathbb{A}^1)^2 \times (\mathbb{A}^1 - \{0\})^2$. Pour tout $\mathbf{x} = (\beta, s, t, \alpha)$ dans $\mathcal{M}$, le polynôme

$$h_{\mathbf{x}}(y) = \alpha\left(\frac{y^5}{5} - s\frac{y^4}{4} + 2ty^3 - 5st\frac{y^2}{2} + 5t^2 y\right) + \beta$$

induit un revêtement de la famille $\mathcal{F}_5$ (à équivalence près). Inversement, tout point $[h] \in \mathcal{H}$ correspondant à un revêtement polynômial représente la classe d'équivalence d'un revêtement associé à un polynôme comme ci-dessus. D'où une flèche $\mathcal{M} \dashrightarrow \mathcal{H}$.

• $\mathcal{H}$ est défini sur $\mathbb{Q}$: car les classes de conjugaison dans $\mathbf{C}$ sont rationnelles (§2.5.1).

• Calcul du revêtement $\gamma_{[h_{\mathbf{x}}]}$ noté plus simplement $\gamma_{\mathbf{x}}$. Le diviseur constitué des deux points au-dessus de $\infty$ (correspondant aux deux 5-cycles du 4ème cycle de ramification) est de degré 2 et rationnel sur $\mathbb{Q}(\mathbf{x})$. Le calcul d'une base du système linéaire associé fournit un plongement de $Y_{[h_{\mathbf{x}}]} = Y_{\mathbf{x}}$ dans $\mathbb{P}^2$. L'image de ce plongement est la conique $C_{\mathbf{x}}$:

$$U^2 + V^2 - 3UV - 5s\frac{U}{4} + 5s\frac{V}{2} - 5t = 0.$$

On obtient la flèche du revêtement $\gamma_{\mathbf{x}}$ en exprimant $T$ en fonction de $U$ et $V$

$$T = \frac{\alpha}{2}\Big[\Big(\frac{U^5}{5} - U^4V + U^3V^2\Big) - \frac{s}{4}(U^4 - 4U^3V + 2U^2V^2) + t(-3U^3 + 4U^2V) + \frac{5}{2}stU^2 + \frac{25}{2}st^2\Big] + \beta.$$

• On trouve un sous-ensemble Zariski-dense $\mathcal{O}$ de points $\mathbf{x} \in \mathcal{M}(\mathbb{Q})$ tels que la conique $C_{\mathbf{x}}$ ait un point $\mathbb{Q}$-rationnel. L'ensemble des points $(\beta, c+d, cd, \alpha)$ avec $c, d \in \mathbb{Q}$ convient: le point $(2c, \frac{c-5d}{2})$ est sur $C_{\mathbf{x}}$ (cf. [DeFr1; Lemma 3.18]).

• En utilisant la paramétrisation d'Euler, on identifie, pour $\mathbf{x} \in \mathcal{O}$ la conique $C_{\mathbf{x}}$ à $\mathbb{P}^1$. Précisément, on obtient

$$\begin{cases} U(w) = \dfrac{8cw^2 + (-14c + 10d)w + 3c - 25d}{4(w^2 - 3w + 1)}, \\ V(w) = \dfrac{12cw^2 + (-11c + 5d)w + 2(c - 5d)}{4(w^2 - 3w + 1)} \quad \text{où } w = \dfrac{V - \frac{c-5d}{2}}{U - 2c}. \end{cases}$$

En reportant $U$ et $V$ dans l'expression de $T$ ci-dessus, on obtient une fraction rationnelle $g_{\mathbf{x}}(w)$ de degré 10, de dénominateur une puissance d'un trinôme.

• Pour terminer la preuve, il reste à étudier les valeurs de cette fraction rationnelle, et, plus précisément, à vérifier que

— $g_{\mathbf{x}}(\mathbb{Q}) \cap \mathbb{Z}$ est infini pour tout $\mathbf{x}$ dans un sous-ensemble Zariski-dense de $\mathcal{O}$: cela se fait en utilisant la forme explicite de $g_{\mathbf{x}}$.

— $g_{\mathbf{x}}(\mathbb{Q}) \cap h_{\mathbf{x}}(\mathbb{Q}) \cap \mathbb{Z}$ est fini: cela est équivalent à montrer que le produit fibré $\mathbb{P}^1 \times_{\mathbb{P}^1} Y_{\mathbf{x}}$ des revêtements $h_{\mathbf{x}}$ et $\gamma_{\mathbf{x}}$ n'a qu'un nombre fini de points $\mathbb{Q}$-rationnels au-dessus d'entiers $z \in \mathbb{Z}$. Cela résulte du théorème de Siegel si ce produit fibré n'a que des composantes irréductibles de genre $> 0$. Un calcul basé sur la formule de Riemann-Hurwitz et le lemme d'Abhyankar [DeFr4] montre qu'il y a deux composantes irréductibles: l'une est de genre 1 et l'autre de genre 2. □

**Remarque 4.5** (Familles de Siegel). On peut voir le paragraphe §4.2 comme un cas particulier d'un problème général, qui est l'étude d'une réciproque du théorème de Siegel. Etant donnés une courbe algébrique $C$, une fonction rationnelle $f : C \to \mathbb{P}^1$, définis sur $\mathbb{Q}$ et un idéal fractionnaire $\mathcal{A}$ de $\mathbb{Q}$, le théorème de Siegel donne une condition nécessaire pour que $C(\mathbb{Q}) \cap f^{-1}(\mathcal{A})$ soit infini: $C$ est de genre 0 et $f$ a soit un unique pôle rationnel soit deux pôles quadratiques réels conjugués. La réciproque que nous considérons est la suivante. Soit $\mathcal{P}$ l'espace des paramètres d'une famille lisse $\Phi : \mathcal{P} \times \mathbb{P}^1 \to \mathcal{P} \times \mathbb{P}^1$, définie sur $\mathbb{Q}$, de fractions rationnelles (de degré $n$). Supposons que pour un ensemble Zariski-dense de points $\mathbf{p} \in \mathcal{P}(\mathbb{Q})$, la fonction $\Phi_{\mathbf{p}}$ a deux pôles quadratiques réels conjugués. La famille $\Phi$ est alors appelée une *famille de Siegel*. On demande si la condition du théorème de Siegel — $\Phi_{\mathbf{p}}(\mathbb{Q}) \cap \mathcal{A}$ infini — est vraie pour tout point $\mathbf{p}$ dans un sous-ensemble Zariski-dense de $\mathcal{P}$. Ci-dessus, nous avons montré que la famille de fractions rationnelles (de degré 10) paramétrée par le pull-back de $\mathcal{O}$ par l'application $(\beta, c, d, \alpha) \to (\beta, c+d, cd, \alpha)$ vérifiait cette réciproque du théorème de Siegel.

## 4.3. Davenport, Mason et al.

**4.3.1. Le problème de Davenport.** Le problème de Hilbert-Siegel est un cas particulier du problème général de la classification des paires de revêtements de $\mathbb{P}^1$ de produit fibré réductible. La méthode a consisté à traduire le problème en termes de bi-représentations du groupe de Galois associé. Les contraintes plus spécifiques données par le théorème de Siegel ont permis de conclure. En utilisant la même démarche, on peut apporter une réponse au problème, posé par Davenport, qui est de classer les polynômes $h(y), g(y) \in \mathbb{Z}[Y]$ qui prennent les mêmes valeurs modulo $p$, pour tout premier $p$, sauf un nombre fini. L'énoncé suivant a été démontré par Fried [Fr5]; d'importantes contributions sont dues à Schinzel (dans le cadre de ses travaux sur les équations à variables séparées $h(x) = g(y)$ [DaLeSc], [Sc]) et à Feit (pour la partie de théorie des groupes [Fe1-3]).

**Théorème 4.6.** *Soient $K$ un corps de nombres et $O_K$ son anneau d'entiers. Soient $h(Y), g(Y) \in O_K[Y]$ tels que $h$ est indécomposable et "linéairement indépendant" de $g$ (i.e., $h(y) \neq g(ay+b)$, $a, b \in \mathbb{C}$). Supposons que, pour tout premier* p *de $O_K$ sauf un nombre fini, les ensembles de valeurs $h(O_K/\mathrm{p})$ et $g(O_K/\mathrm{p})$ prises par $h$ et $g$ sur $O_K/\mathrm{p}$ coincident. Alors on a*

$$\begin{cases} \deg(h) = \deg(g) = n \in \{7, 11, 13, 15, 21, 31\} \\ [\mathbb{Q}(\zeta_n) \cap K : \mathbb{Q}] > 1. \end{cases}$$

*En particulier, si $K = \mathbb{Q}$, il n'existe pas de polynômes $h(Y)$, $g(Y)$ vérifiant de telles hypothèses.*

Chacun des degrés $n$ ci-dessus est réellement une exception sur $\mathbb{Q}(\zeta_n)$: on peut trouver des paires $h(Y), g(Y) \in O_{\mathbb{Q}(\zeta_n)}[Y]$ vérifiant les hypothèses du théorème et $\deg(h) = n$; les paires exceptionnelles $(h, g)$ ont récemment été classifiées par P. Cassou-Noguès et J-M. Couveignes [CaCou]. En revanche, pour $K = \mathbb{Q}$, on ne connait même pas d'exemples avec $h$ décomposable.

**4.3.2. Sur le théorème de Mason-Stothers** [Za1]. Les espaces de Hurwitz apparaissent aussi dans un travail de U. Zannier. Il s'intéresse au cas d'égalité dans le théorème de Mason-Stothers[7] (analogue polynomial de la conjecture *abc* — si $a, b, c \in \mathbb{C}[Y]$ sont trois polynômes premiers entre eux tels que $a - b = c$, alors le nombre de racines distinctes dans $\mathbb{C}$ de $abc$ est strictement plus grand que le maximum des degrés de $a$, $b$ et $c$ —). A un triplet $(a, b, c)$, il associe le revêtement $f : \mathbb{P}^1 \to \mathbb{P}^1$ induit par la fraction rationnelle $a/b$. Puis traduit les conditions d'égalité dans le théorème de Mason-Stothers en termes de la ramification de ce revêtement: le revêtement est ramifié en 0, 1 et $\infty$ avec certaines conditions sur les indices de ramification. Si bien qu'il arrive à entièrement poser le problème en termes d'existence de sous-groupes de $S_n$ engendrés par des éléments $\sigma_1, \ldots, \sigma_{r-1}$

7) Zannier signale dans [Za2] que ce résultat qu'on attribue généralement à Mason est en fait apparu precédemment dans un article de Stothers [St].

vérifiant certaines conditions. Il donne ensuite une construction combinatoire de sous-groupes du type requis.

Les espaces de Hurwitz apparaissent explicitement quand on se pose des questions de rationalité. C'est le théorème d'existence de Riemann qui permet en dernier lieu d'associer aux sous-groupes de $S_n$ construits un revêtement $f : X \to \mathbb{P}^1$, de genre 0, et donc une fraction rationnelle $a/b$. Mais les polynômes $a$ et $b$ sont *a priori* à coefficients dans $\mathbb{C}$. L'existence de polynômes à coefficients dans $\mathbb{Q}$ revient à montrer que le revêtement $f$ peut être défini sur $\mathbb{Q}$, et donc à trouver des points $\mathbb{Q}$-rationnels sur des espaces de Hurwitz. Zannier explique que c'est possible quand on fait certaines hypothèses qui garantissent l'unicité du revêtement $f$: c'est le cas "rigide". Il suggère que plus généralement, on pourrait utiliser les résultats connus sur l'arithmétique des espaces de Hurwitz. L'intérêt d'obtenir des solutions sur $\mathbb{Q}$ est que, par spécialisation, on peut espérer obtenir un triplet d'entiers pour lequel on serait proche du cas d'égalité dans la conjecture *abc* numérique.

## 4.4. Critère d'existence de points rationnels [DeFr1]

Nous terminons ces applications par la description d'un critère qui utilise la structure modulaire même des espaces de Hurwitz — de façon précise, la monodromie du revêtement $\mathcal{H}_G(\mathbf{C}) \to \mathcal{U}_r$ — pour détecter des points rationnels sur les revêtements paramétrés par les points de $\mathcal{H}_G(\mathbf{C})$.

Soit $f : X \to \mathbb{P}^1$ un revêtement défini sur un corps $K$. *Via* le choix d'un isomorphisme $\pi_1(\mathbb{P}^1 - \mathbf{t}) \simeq F(x_1, \ldots, x_r)/x_1 \cdots x_r$, $f$ peut être vu (à isomorphisme près) comme la donnée de l'ensemble $\mathbf{t} = \{t_1, \ldots, t_r\}$ de ses points de ramification et d'un $r$-uplet $\mathbf{g} = (g_1, \ldots, g_r) \in \mathrm{ni}_G(\mathbf{C})$, où $G$ est le groupe et $\mathbf{C}$ l'inertie du revêtement $f$. Pour $i = 1, \ldots, r$, considérons la décomposition de $g_i$ en cycles à supports disjoints dans $S_d$: $g_i = \beta_{i1} \cdots \beta_{i\ell_i}$. On sait que, pour $i = 1, \ldots, r$, les points dans la fibre $f^{-1}(t_i)$ correspondent aux cycles $\beta_{ij}$ de la décomposition de $g_i$, la longueur de chaque cycle étant égale à l'indice de ramification correspondant. On sait aussi (*e.g.* [Fr2; p. 62]) que l'action de $G_K$ sur l'ensemble des points de ramification a la propriété suivante. Pour $\tau \in G_K$ et $i = 1, \ldots, r$, si $t_i^\tau = t_j$, alors il existe $\gamma \in S_d$ et un entier $a$ premier à l'ordre des éléments de $C_i$ tels que $C_j = \gamma C_i^a \gamma^{-1}$. Il en résulte que, pour tout $i \in \{1, \ldots, r\}$, le diviseur $\sum_j (t_j)$, où $j$ parcourt l'ensemble $I$ des indices tels que $C_j = \gamma C_i^a \gamma^{-1}$ avec $\gamma$ et $a$ comme ci-dessus, est un diviseur $K$-rationnel de $\mathbb{P}^1$.

Fixons un indice $i \in \{1, \ldots, r\}$ et la longueur $\lambda$ d'un des cycles $g_{ik}$. Notons $g(i, \lambda)$ l'ensemble des cycles de longueur $\lambda$ intervenant dans la décomposition des $g_{jk}$ où $j$ décrit $I$ et $P_f(i, \lambda)$ l'ensemble des points de $X$ correspondant aux cycles dans $g(i, \lambda)$. Considérons le sous-groupe

$$H_{\mathbf{g}} = \{Q \in H(r) \mid \exists \gamma \in S_d, Q(\mathbf{g}) = (\gamma g_1 \gamma^{-1}, \ldots, \gamma g_r \gamma^{-1})\}.$$

Supposons que le groupe $G$ du revêtement est de centralisateur $\mathrm{Cen}_{S_d}(G)$ trivial. Alors l'élément $\gamma$ associé dans la définition à tout élément $Q \in H_{\mathbf{g}}$ est unique.

L'action de $Q$ combinée à celle de la conjugaison par $\gamma^{-1}$ fixe le $r$-uplet $\mathbf{g}$ et donc permute les cycles dans $g(i,\lambda)$; on obtient ainsi une action de $H_{\mathbf{g}}$ sur $g(i,\lambda)$.

En plus de la condition $\mathrm{Cen}_{S_d}(G) = \{1\}$, nous supposerons que $H(r)$ agit transitivement sur $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$. Alors l'action de $H_{\mathbf{g}}$ sur $g(i,\lambda)$ ne dépend pas (à équivalence près) du $r$-uplet $\mathbf{g}$ choisi dans $\mathrm{sni}_G(\mathbf{C})$ (voir [DeFr1; Remark 3.13]). Notons $\mathcal{H}$ l'espace de Hurwitz $\mathcal{H} = \mathcal{H}_G(\mathbf{C})$. La condition de transitivité ci-dessus entraîne que $\mathcal{H}$ est irréductible. D'après l'hypothèse $\mathrm{Cen}_{S_d}(G) = \{1\}$, les revêtements paramétrés par $\mathcal{H}$ n'ont pas d'automorphismes; en conséquence, il existe une famille universelle de Hurwitz $\mathcal{F}$ au-dessus de $\mathcal{H}$. Notons $f_{\mathrm{gen}} : X_{\mathrm{gen}} \to \mathbb{P}^1$ le revêtement générique de $\mathcal{F}$ et $F = \overline{\mathbb{Q}}(\mathcal{H})$ le corps des fonctions de $\mathcal{H}$, lequel est un corps de définition de $f_{\mathrm{gen}}$.

**Théorème 4.7** (Dèbes-Fried) [DeFr1; Th. 3.14]. *Les orbites de $H_{\mathbf{g}}$ sur $g(i,\lambda)$ correspondent exactement aux orbites de $G_F$ sur $P_{f_{\mathrm{gen}}}(\mathbf{g},\lambda)$.*

Il s'agit d'un énoncé sur le revêtement générique de $\mathcal{F}$. L'intérêt des familles de Hurwitz est que, ce type de propriété, une fois établi sur le revêtement générique, s'étend à tous les revêtements de la famille. Une application pratique du Th. 4.7 est la suivante. Supposons que le groupe $H_{\mathbf{g}}$ possède une unique[8)] orbite d'une longueur donnée $\ell$. Le Th. 4.7 permet d'en déduire que, pour tout revêtement $f : X \to \mathbb{P}^1$ de la famille de Hurwitz $\mathcal{F}$, il existe sur $X$ un diviseur de longueur $\ell$, rationnel sur le corps de définition de $f$.

Dans le cas où $X$ est de genre 0 ou 1, le Th. 4.7 conduit à un critère pratique d'existence de points rationnels sur $X$, en le combinant au fait suivant [DeFr1; Cor. 3.15 et Cor. 3.17]. Pour trouver un point rationnel sur une courbe de genre 0, il suffit de trouver un diviseur rationnel de degré impair, et sur une courbe de genre 1, il suffit de trouver des diviseurs rationnels de degrés premiers entre eux. Plus généralement, cela conduit à la notion de points rationnels produits par la ramification [DeFr1; §3.2]: ce sont les points rationnels, qui comme diviseurs, sont dans le groupe engendré, par les diviseurs rationnels à support dans l'ensemble des points ramifiés de $f$, et les diviseurs de fonctions rationnelles. Des questions se posent naturellement [DeFr1; §3 & §4]. Ainsi, pour les genres 0 et 1, dans quelle mesure l'existence générique de points rationnels sur $X$ est-elle équivalente à l'existence générique de points rationnels produits par la ramification (auquel cas le Th. 4.7 devient un critère décisif quant à l'existence de points rationnels sur le revêtement générique de la famille de Hurwitz)? On peut également se demander si, pour ce qui est des points rationnels produits par la ramification, leur existence générique équivaut à leur existence sur toutes les courbes $X$ de la famille considérée? On montre en fait, grâce au théorème d'irréductibilité de Hilbert, que cette seconde question a une réponse positive pour les genres 0 et 1 [DeFr1; Th. 3.11]. Cette seconde question est évidemment à relier à la question

8) Soit $k$ le corps de définition minimal de $\mathcal{H}$. L'unicité assure ici que l'orbite en question sera une orbite, non seulement du groupe de Galois $G_{\overline{\mathbb{Q}}(\mathcal{H})}$ mais aussi du groupe de Galois $G_{k(\mathcal{H})}$.

similaire où l'on s'intéresse aux points rationnels quelconques (et pas seulement à ceux produits par la ramification). D'après un travail de Lewis et Schinzel [LeSc] (à l'origine de [DeFr1]), le résultat subsiste pour des familles de courbes de genre 0; mais on pense que le résultat devient faux dès le genre 1.

# 5. Tours modulaires

Les tours modulaires constituent un développement récent de la théorie des espaces de Hurwitz. Cette section présente leur construction (§5.1). L'exemple fondateur est celui de la tour des courbes modulaires (§5.2). En suivant cet exemple, on est conduit naturellement à certaines questions de nature arithmétique sur les tours modulaires en général (§5.3). La notion de tour modulaire est due à Fried; cette section est une présentation succinte de son article [Fr6].

## 5.1. Construction

On se donne un groupe fini $G$, plongé dans $S_d$, un nombre premier $p$ divisant $|G|$, un entier $r \geq 3$ et un ensemble $\mathbf{C} = \{C_1, \ldots, C_r\}$ de classes de conjugaison de $G$ dont les éléments ont un ordre premier à $p$.

On note ${}_p\tilde{G}$ le $p$-revêtement universel de Frattini de $G$. Rappelons (voir [FrJa] pour plus de détails) qu'un homomorphisme surjectif de groupes (un revêtement) $\psi : H \to G$ est dit *de Frattini* si, pour tout sous-groupe $H'$ de $H$, $\psi(H') = G \Rightarrow H' = H$, ou, de façon équivalente, si son noyau est contenu dans l'intersection des sous-groupes maximaux de $G$. Par exemple, l'homomorphisme $\mathbb{Z}/(p_1^{\alpha_1} \cdots p_r^{\alpha_r})\mathbb{Z} \to \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$ est de Frattini ($\alpha_1, \ldots, \alpha_r > 0$). Le produit fibré de deux revêtements de Frattini a la propriété de Frattini. Il y a un objet universel pour les revêtements de Frattini d'un groupe $G$ donné. On le note $\tilde{G}$ et on peut montrer que $\tilde{G}$ est un revêtement profini projectif de $G$. Par exemple, pour $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, on a $\tilde{G} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$. Il existe aussi un objet universel pour les revêtements de Frattini $\psi : H \to G$ de $G$ de noyau $\ker(\psi)$ un $p$-groupe. C'est cet objet qu'on appelle le $p$-revêtement universel de Frattini de $G$ et qu'on note ${}_p\tilde{G}$. Par exemple, pour $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, on a ${}_{p_1}\tilde{G} = \mathbb{Z}_{p_1} \times \mathbb{Z}/p_2\mathbb{Z} \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.

On définit ensuite, à partir du noyau ker de l'homomorphisme ${}_p\tilde{G} \to G$, une suite de quotients caractéristiques de ${}_p\tilde{G}$:

$$\ker_0 = \ker,\ \ker_1 = \ker_0^p[\ker_0, \ker_0], \ldots,\ \ker_n = \ker_{n-1}^p[\ker_{n-1}, \ker_{n-1}], \ldots$$

et on note ${}_p^n\tilde{G}$ le quotient ${}_p\tilde{G}/\ker_n$ ($n \geq 0$). Par exemple, pour $G = \mathbb{Z}/p\mathbb{Z}$, on a $\ker_n = p^{n+1}\mathbb{Z}_p$ et ${}_p^n\tilde{G} = \mathbb{Z}/p^{n+1}\mathbb{Z}$.

**Lemme 5.1.** *Si $C$ est une classe de conjugaison d'éléments de ${}_p^n\tilde{G}$ d'ordre $\rho$ premier à $p$, alors il existe une unique classe de conjugaison de ${}_p^{n+1}\tilde{G}$ relevant $C$ et dont les éléments sont d'ordre $\rho$.*

*Preuve.* Notons $\phi : {}^{n+1}_{p}\tilde{G} \to {}^{n}_{p}\tilde{G}$ la surjection naturelle. Soient $g \in C$ et $H = \phi^{-1}(\langle g \rangle)$. On a une suite exacte $1 \to \ker_n / \ker_{n+1} \to H \to \langle g \rangle \to 1$. D'après le lemme de Schur-Zassenhaus, comme $g$ est d'ordre premier à $p$, cette suite est scindée; de plus, il y a unicité de la section $\langle g \rangle \to H$, à conjugaison près. □

Grâce à ce lemme, on peut définir , pour tout $n \geq 0$, un $r$-uplet, noté $\mathbf{C}^n = (C_1^n, \ldots, C_r^n)$ de classes de conjugaisons de ${}^{n}_{p}\tilde{G}$, de telle façon que $C_i^{n+1}$ relève $C_i^n$ et soit de même ordre, $i = 1, \ldots, r$ (par ordre, on entend ici l'ordre des éléments dans la classe). Cette définition fournit naturellement, pour tout $n \geq 0$, une flèche

$$\mathrm{ni}_{{}^{n+1}_{p}\tilde{G}}(\mathbf{C}^{n+1}) \to \mathrm{ni}_{{}^{n}_{p}\tilde{G}}(\mathbf{C}^n).$$

Dans le cas de revêtements purs, il faut encore définir, de façon compatible, une représentation $T_n$ de ${}^{n}_{p}\tilde{G}$ dans un groupe symétrique ($n \geq 0$). Notons $G(1)$ le fixateur de 1 dans la représentation $G \subset S_d$ et choisissons le premier $p$ ne divisant pas l'ordre de $G(1)$. En appliquant comme ci-dessus le lemme de Schur-Zassenhaus, on obtient qu'il existe une copie de $G(1)$ dans l'image inverse de $G(1)$ par le morphisme ${}^{n}_{p}\tilde{G} \to G$, unique à conjugaison près ($n \geq 0$). On définit $T_n$ comme l'action par translation à gauche de ${}^{n}_{p}\tilde{G}$ sur les classes à gauche modulo cette copie de $G(1)$ ($n \geq 0$).

A tout entier $n \geq 0$, on peut maintenant associer un espace de Hurwitz

$$\mathcal{H}_n = \mathcal{H}_{{}^{n}_{p}\tilde{G}}(\mathbf{C}_n).$$

Pour tout $n \geq 0$, il y a un morphisme naturel $\psi_n : \mathcal{H}_{n+1} \to \mathcal{H}_n$. La collection des espaces $\mathcal{H}_n$ et des morphismes $\psi_n$ ($n \geq 0$) est appelée *tour modulaire* associée au triplet $(G \subset S_d, p, \mathbf{C})$.

## 5.2. Le cas du groupe diédral

Comme en §3.1.4, on prend ici $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ et les quatre classes $C_1, \ldots, C_4$ égales à la classe $C$ des involutions de $G$. On a alors ${}_{p}\tilde{D}_p = \mathbb{Z}_p \times^s \mathbb{Z}_2 := D_{p^\infty}$ et pour tout $n \geq 0$, ${}^{n}_{p}\tilde{D}_p = D_{p^n}$. On sait (§3.1.4) qu'il existe un morphisme surjectif et défini sur $\mathbb{Q}$

$$\chi_n : \mathcal{H}_n = \mathcal{H}^{\mathrm{in}}_{D_{p^n}}(\mathbf{C}^n) \to X_1(p^n) - \{\text{pointes}\}.$$

D'autre part, on a pour tout $n > 0$, un diagramme commutatif

$$\begin{array}{ccc} \mathcal{H}_n & \xrightarrow{\chi_n} & X_1(p^n) \\ {\scriptstyle \psi_{n-1}}\downarrow & & \downarrow{\scriptstyle \times p} \\ \mathcal{H}_{n-1} & \xrightarrow{\chi_{n-1}} & X_1(p^{n-1}) \end{array}$$

où la flèche verticale de droite $\times p$ est la multiplication par $p$. En d'autres termes, il existe un morphisme de la tour modulaire associée au triplet $(G \subset S_d, p, \mathbf{C})$ vers la tour des courbes modulaires $(X_1(p^n))_{n>0}$.

## 5.3. Questions arithmétiques sur les tours modulaires

Comme précédemment, on s'intéresse aux corps de définition des composantes irréductibles et, éventuellement, à l'existence de points rationnels sur ces composantes. Ci-dessous, nous précisons ces questions en poursuivant le parallèle avec la tour des courbes modulaires.

**5.3.1. Composantes irréductibles.** Soit $\mathcal{T}$ une composante irréductible de $\mathcal{H}_1$ (correspondant à une orbite $\mathcal{O}$ de $H_r$ sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ (ou $\mathrm{ni}_G(\mathbf{C})^{\mathrm{in}}$ dans la situation de G-revêtements comme en §5.2 par exemple). On cherche à quelle condition cette composante se relève au niveau $n$.

**Proposition 5.2** [Fr6]. *Pour $\mathbf{g} \in \mathcal{O}$, on définit le sous-ensemble $\nu_n(\mathbf{g}) \subset {}^n_p\tilde{G}$ par*

$$\nu_n(\mathbf{g}) = \left\{ \tilde{g}_1 \cdots \tilde{g}_r \;\middle|\; \begin{array}{l} \tilde{g}_i \in {}^n_p\tilde{C}_i, i = 1, \ldots, r \text{ (à l'ordre près)} \\ \text{et } \tilde{\mathbf{g}} \text{ relève } \mathbf{g} \end{array} \right\}$$

(a) *L'ensemble $\nu_n(\mathbf{g})$ ne dépend que de $\mathcal{O}$ et définit donc un invariant $\nu_n(\mathcal{O})$.*
(b) *Il existe une composante irréductible de $\mathcal{H}_n$ au-dessus de $\mathcal{T}$ ssi $1 \in \nu_n(\mathcal{O})$.*
(c) *Si $1 \in \nu_n(\mathcal{O})$, alors tout élément $\mathbf{g} \in \mathcal{O}$ se relève dans $\mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$. En conséquence les composantes irréductibles de $\mathcal{H}_n$ s'envoient surjectivement sur celles de $\mathcal{H}_1$.*

*Preuve.* (b) Le sens ($\Rightarrow$) est trivial. Inversement, supposons $1 \in \nu_n(\mathcal{O})$. Il existe donc un $r$-uplet $\tilde{\mathbf{g}}$ tel que $\tilde{g}_1 \cdots \tilde{g}_r = 1$ et $\tilde{g}_i \in {}^n_p\tilde{C}_i$, $i = 1, \ldots, r$ (à l'ordre près). Pour conclure que $\tilde{\mathbf{g}} \in \mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$, et donc que la composante $\mathcal{T}$ se relève dans $\mathcal{H}_n$, il reste à voir que $\tilde{g}_1, \ldots, \tilde{g}_r$ engendrent le groupe ${}^n_p\tilde{G}$. Cela provient de la propriété de Frattini du revêtement ${}^n_p\tilde{G} \to G$.

Soient $\mathbf{g}^o, \mathbf{g} \in \mathcal{O}$; $\mathbf{g}$ est de la forme $(\mathbf{g}^o)Q$ avec $Q \in H_r$. Si $\tilde{\mathbf{g}}^o_n$ relève $\mathbf{g}^o$, alors $\tilde{\mathbf{g}}_n = (\mathbf{g}^o_n)Q$ relève $\mathbf{g}$ et $\tilde{g}_1 \cdots \tilde{g}_r = \tilde{g}^o_1 \cdots \tilde{g}^o_r$. On en déduit (a) et (c). □

**Remarque 5.3.** La preuve de (b) montre l'utilité de la propriété de Frattini. Les revêtements de Frattini ont cette autre propriété notable: ils ne peuvent pas être scindés (sauf à être des isomorphismes). D'une certaine façon, être scindé et être de Frattini sont deux propriétés à l'opposé l'une de l'autre dans le paysage des extensions de groupes. Rappelons aussi ce fait utile: le revêtement universel de Frattini est un revêtement projectif [FrJa].

Une composante $\mathcal{T}$ de $\mathcal{H}_1$ est dite *obstruée* au niveau $n$ s'il n'existe pas de composante irréductible $\mathcal{T}_n$ de $\mathcal{H}_n$ se projetant sur $\mathcal{T}$. Une condition nécessaire et

suffisante est que $1 \notin \nu_n(\mathcal{O})$. Ce phénomène n'arrive pas avec la tour des courbes modulaires puisque chaque niveau de la tour est irréductible. En général, les composantes d'une tour modulaire au-dessus d'une composante donnée de $\mathcal{H}_1$ forment un arbre, avec des chaines finies ou infinies.

On définit ensuite $\nu(\mathcal{O})$ comme la limite projective des $\nu_n(\mathcal{O})$ $(n \geq 1)$. Le résultat ci-dessous dit essentiellement que $\nu(\mathcal{O})$ est un invariant qui peut permettre de distinguer arithmétiquement deux composantes irréductibles de $\mathcal{H}_1$, et donc de trouver éventuellement des composantes irréductibles définies sur $\mathbb{Q}$.

**Théorème 5.4** [Fr6; Th. 3.16]. *Supposons $G$ de centre trivial. Soit $\mathcal{H}_1 = \bigcup_{i=1}^{t} \mathcal{H}_{1i}$ la décomposition de $\mathcal{H}_1$ en composantes irréductibles. Supposons que $\mathcal{H}_1$ est défini sur $\mathbb{Q}$ (e.g. $C_1, \ldots, C_r$ sont rationnelles). Alors $G_{\mathbb{Q}}$ permute les composantes $\mathcal{H}_{1i}$. Plus précisément, pour tout $\tau \in G_{\mathbb{Q}}$, on a*

$$\big(\nu(\mathcal{H}_{1i}^{\tau})\big)^{\chi(\tau)} = \nu(\mathcal{H}_{1i}),\ i = 1, \ldots, t$$

*où $\chi : G_{\mathbb{Q}} \to (\mathbb{Z}_p)^{\times}$ est le caractère cyclotomique modulo $(p^n)_{n\geq 1}$.* [9]

En particulier, si $\nu(\mathcal{H}_{1i})^t = \nu(\mathcal{H}_{1i})$ pour tout $t \in (\mathbb{Z}_p)^{\times}$ et $\nu(\mathcal{H}_{1i}) \neq \nu(\mathcal{H}_{1j})$ pour $j \neq i$, alors $\mathcal{H}_{1i}$ est défini sur $\mathbb{Q}$. En effet, la première condition entraîne que, pour tout $\tau \in G_{\mathbb{Q}}$, $\mathcal{H}_{1i}$ et $\mathcal{H}_{1i}^{\tau}$ on même invariant $\nu$. Comme, d'après la seconde condition, cet invariant distingue $\mathcal{H}_{1i}$ des autres composantes, $\mathcal{H}_{1i} = \mathcal{H}_{1i}^{\tau}$, pour tout $\tau \in G_{\mathbb{Q}}$.

**5.3.2. Système projectif de points rationnels.** Considérons un système projectif de points $(\mathbf{p}_n)_{n>0}$ sur la tour des courbes modulaires. Chaque point $\mathbf{p}_n$ correspond à la donnée d'un point de $p^n$-torsion sur une courbe elliptique $E$ (la même pour tout $n$). Supposons que $E$ est définie sur un corps $K$. Le groupe $G_K$ opère sur l'ensemble des points de $p$-torsion de $E$: il s'agit de l'action de $G_K$ sur le $\mathbb{Z}_p$-module de Tate $V_p$ associé à $E$. Notons $j : X_1(p) \to \mathbb{P}^1$ l'application qui a un point $(E, \mathbf{p}) \in X_1(p)$ associe l'invariant canonique de la courbe elliptique $E$. L'action précédente est une action sur l'ensemble des systèmes projectifs de points $(\mathbf{p}_n)_{n>0}$ au-dessus de l'invariant $j(E)$ de $E$.

On obtient de la même façon une représentation de $G_K$ dans la situation plus générale d'une tour modulaire:

(*) Le groupe $G_K$ opère sur l'ensemble des systèmes projectifs de points $(\mathbf{p}_n)_{n>0}$ au-dessus d'un élément fixé $\mathbf{t} \in \mathcal{U}_r(K)$.

Dans le cas des courbes modulaires, un théorème célèbre de Serre permet d'affirmer que, si $K$ est un corps de nombres,

(**) étant donnés un système projectif de points $(\mathbf{p}_n)_{n>0}$ au-dessus de $j \in \mathbb{P}^1(K)$ et une extension finie $F/K$, $\mathbf{p}_n \notin \mathcal{H}_n(F)$, sauf pour un nombre fini d'entiers $n$.

9) Pour tout $n \geq 1$, l'élément $\nu_n(\mathcal{O}) \in {}^n_p\tilde{G}$ appartient à $\ker_0 / \ker_n$ qui est par construction un $p$-groupe, disons d'ordre $p^N$. En conséquence, toute puissance $\nu_n(\mathcal{O})^t$ avec $t \in \mathbb{Z}/p^N\mathbb{Z}$ a un sens.

En effet, il n'y a qu'un nombre fini de points de $p$-torsion $F$-rationnels sur une courbe elliptique définie sur $K$ donnée. On peut penser que cet énoncé subsiste en général, avec $\mathbf{t} \in \mathcal{U}_r(K)$ au lieu de $j \in \mathbb{P}^1(K)$ et avec éventuellement quelques hypothèses supplémentaires. En particulier, il semble naturel de fixer un système projectif $(\mathcal{T}_n)_{n>0}$ de composantes irréductibles définies sur $K$ telles que pour tout $n > 0$, $\mathbf{p}_n \in \mathcal{T}_n(K)$.

## Références


[Be] Bertin, J., Compactification des schémas de Hurwitz. C. R. Acad. Sci. Paris Sér. I Math. 322 (1996), 1063–1066 [+preprint, même titre, 49 pages, 1996].

[CaCou] Cassou-Noguès, P., Couveignes, J.-M., Factorisation explicite de $g(y) - h(z)$. Preprint, 1997.

[Cl] Clebsch, A., Zur Theorie der Riemann'schen Fläche. Math. Ann. 6 (1872), 216–230.

[CoHa] Coombes, K., Harbater, D., Hurwitz families and arithmetic Galois groups. Duke Math. J. 52 (1985), 821–839.

[DaLeSc] Davenport, H., Lewis, D.J., Schinzel, A., Equations of the form $f(x) = g(y)$. Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[De1] Dèbes, P., Groupes de Galois sur $K(T)$. Sém. Théor. Nombres Bordeaux (2) 2 (1990), 229–243.

[De2] — Covers of $\mathbb{P}^1$ over the $p$-adics. In: Recent developments in the inverse Galois problem (éd. par M.D. Fried et al.; Contemp. Math. 186), 217–238. Amer. Math. Soc., Providence 1995.

[DeDes] Dèbes, P., Deschamps, B., The regular inverse Galois problem over large fields. In: Geometric Galois action vol. 2 (éd. par L. Schneps et P. Lochak; London Math. Soc. Lecture Note Ser. 243), 119–138. Cambridge University Press, Cambridge 1997.

[DeDo1] Dèbes, P., Douai, J.-C., Algebraic covers: field of moduli versus field of definition. Ann. Sci. École Norm. Sup. (4) 30 (1997), 303–338.

[DeDo2] — Gerbes and covers. Comm. Algebra, à paraître.

[DeDoEm] Dèbes, P., Douai, J.-C., Emsalem, M., Familles de Hurwitz et cohomologie non abélienne. Preprint, 1998.

[DeFr1] Dèbes, P., Fried, M., Arithmetic variation of fibers in algebraic families of curves. Part 1: Criteria for existence of rational points. J. Reine Angew. Math. 409 (1990), 106–137.

[DeFr2] — Rigidity and real residue class fields. Acta Arith. 56 (1990), 13–45.

[DeFr3] — Non rigid situations in constructive Galois Theory. Pacific J. Math. 163 (1994), 81–122.

[DeFr4] — Integral specialization of families of rational functions. Pacific J. Math., à paraître.

[DelMu] Deligne, P., Mumford, D., The irreducibility of the space of curves of given genus. Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–109.

[Des] Deschamps, B., Existence de points $p$-adiques pour tout $p$ sur un espace de Hurwitz. In: Recent developments in the inverse Galois problem (éd. par M.D. Fried et al.; Contemp. Math. 186), 239–247. Amer. Math. Soc., Providence 1995.

[Ek] Ekedahl, T., Boundary behaviour of Hurwitz schemes. In: The moduli space of curves (éd. par R. Dijkgraaf, C. Faber et G. van der Geers; Progr. Math. 129), 173–198. Birkhäuser, Boston 1995.

[Em] Emsalem, M., Familles de revêtements de la droite projective. Bull. Soc. Math. France 123 (1995), 47–85.

[Fe1] Feit, W., Automorphisms of symmetric balanced incomplete block designs. Math. Z. 118 (1970), 40–49.

[Fe2] — On symmetric balanced incomplete block designs with doubly transitive automorphism groups. J. Combin. Theory Ser. A 14 (1973), 221–247.

[Fe3] — Some consequences of the classification of finite simple groups. Proc. Sympos. Pure Math. 37 (1980), 175–181.

[Fr1] Fried, M., The fields of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J. Math. 17 (1973), 128–146.

[Fr2] — Fields of definition of function fields and Hurwitz families—groups as Galois groups. Comm. Algebra 5 (1977), 17–82.

[Fr3] — Exposition of an arithmetic-group theoretic connection via Riemann's existence theorem. Proc. Sympos. Pure Math. 37 (1980), 571–602.

[Fr4] — On reduction of the inverse Galois group problem to simple groups. In: Proceedings of the Rutgers group theory year (1983/84) (éd. par M. Aschbacher et al.), 289–301. Cambridge Univ. Press, Cambridge-New York 1985.

[Fr5] — Rigidity and applications of the classification of simple groups to monodromy. Preprint, 1987.

[Fr6] — Introduction to modular towers. In: Recent developments in the inverse Galois problem (éd. par M.D. Fried et al.; Contemp. Math. 186), 111–171. Amer. Math. Soc., Providence 1995.

[FrBi] Fried, M., Biggers, R., Moduli spaces of covers and the Hurwitz monodromy group. J. Reine Angew. Math. 335 (1982), 87–121.

[FrJa] Fried, M., Jarden, M., Field arithmetic (Ergeb. Math. Grenzgeb. (3) 11). Springer, Berlin 1986.

[FrVö] Fried, M., Völklein, H., The inverse Galois problem and rational points on moduli spaces. Math. Ann. 290 (1991), 771–800.

[Fu] Fulton, W., Hurwitz schemes and irreducibility of moduli of algebraic curves. Ann. of Math. (2) 90 (1969), 543–573.

[GrRe1] Grauert, H., Remmert, R., Faisceaux analytiques cohérents sur le produit d'un espace analytique et d'un espace projectif. C. R. Acad. Sci. Paris 245 (1957), 819–822.

[GrRe2] — Espaces analytiquement complets. Ibid., 822–825.

[GrRe3] Grauert, H., Remmert, R., Sur les revêtements analytiques des variétés analytiques. Ibid., 918–921.

[Ha] Harbater, D., Galois covering of the arithmetic line. In: Number theory (New York, 1984/85) (éd. par D.V. Chudnovsky et al.; Lecture Notes in Math. 1240), 165–195. Springer, Berlin 1987.

[HarMu] Harris, J., Mumford, D., On the Kodaira dimension of the moduli space of curves. Invent. Math. 67 (1982), 23–86.

[Hu] Hurwitz, A., Über Riemann'sche Flächen mit gegebenen Veizweigungspunkten. Math. Ann. 39 (1891), 1–61 [= Mathematische Werke, I, 321–383].

[KrNe] Krull, A., Neukirch, J., Die Struktur der absoluten Galois Gruppe über dem Körper $\mathbb{R}(T)$. Math. Ann. 193 (1971), 197–209.

[LeSc] Lewis, D.J., Schinzel, A., Quadratic diophantine equations with parameters. Acta Arith. 37 (1980), 133–141.

[MaKa] Mazur, B., Kamienny, S., Rational torsion of prime order in elliptic curves over number fields. Preprint, 1992.

[MaMa] Matzat, B. H., Malle, G., Inverse Galois theory. Preprint, Univ. Heidelberg, 1996.

[Me] Merel, L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. 124 (1996), 437–449.

[Mo] Mochizuki, S., The geometry of the compactification of the Hurwitz scheme. Publ. Res. Inst. Math. Sci. 31 (1995), 355–441.

[Mu] Müller, P., Hilbert's irreducibility theorem for polynomials of prime degree and for generic polynomials. Preprint, 1996.

[Po] Pop, F., Embedding problems over large fields. Ann. of Math. (2) 144 (1996), 1–35.

[Sc] Schinzel, A., Reducibility of polynomials of the form $f(x) - g(y)$. Colloq. Math. 18 (1967), 213–218.

[Se1] Serre, J.-P., Géométrie algébrique et géométrie analytique. Ann. Inst. Fourier (Grenoble) 6 (1956), 1–42.

[Se2] — Topics in Galois Theory. Jones and Bartlett Publ., Boston 1992.

[Sev] Severi, F., Vorlesungen über algebraische Geometrie (traduit par E. Löffler). Teubner, Leipzig 1921.

[Si] Siegel, C.L., Über einige Anwendungen Diophantischer Approximationen. Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. 1929, Nr. 1. Gesammelte Abhandlungen, vol. I, 209–266. Springer, Berlin 1966.

[St] Stothers, W.W., Polynomial identitites and Hauptmoduln. Quart. J. Math. Oxford Ser. (2) 32 (1981), 349–370.

[StrVo] Strambach, K., Völklein, H., The symplectic braid group and Galois realizations. In: Geometric Galois action vol. 2 (éd. par L. Schneps et P. Lochak; London Math. Soc. Lecture Note Ser. 243), 139–150. Cambridge University Press, Cambridge 1997.

[Th] Thompson, J.G., Some finite groups which occur as $\mathrm{Gal}(L/K)$ where $K \leq \mathbb{Q}(\mu_n)$. J. Algebra 89 (1984), 437–499.

[We] Weil, A., The field of definition of a variety. In: Oeuvres complètes (Collected papers) II, 291–306. Springer, New York 1979.

[Wew] Wewers, S., Construction of Hurwitz spaces. Thesis, Inst. Exp. Math., Essen 1998.

[Za1] Zannier, U., On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's existence theorem. Acta Arith. 72 (1995), 107–137.

[Za2] — Acknowledgement of priority. Acta Arith. 74 (1996), 387.

# On a polynomial with large number of irreducible factors

*A. Dubickas*

**Abstract.** We give an example of a polynomial which has large number of cyclotomic factors. We thus obtain an inequality between the number of all irreducible factors of a polynomial counted with multiplicities and its degree and norm which is not far from being the best possible. It is also shown that this polynomial is vanishing at 1 with high multiplicity.

## 1. Introduction

Let $P$ be a polynomial of degree $n$ with integer coefficients such that $P(0) \neq 0$:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad a_n, a_0 \neq 0.$$

In the sequel we use the following notations:

$$H(P) = \max_{0 \leqslant i \leqslant n} |a_i|,$$

$$\nu(P) = \max_{|z| \leqslant 1} |P(z)|,$$

$$s(P) = \frac{\log \nu(P)}{n}.$$

Put also $\Omega_c(P)$ for the number of cyclotomic factors of $P$ counted with multiplicities, and put $\Omega(P)$ for the number of all irreducible factors of $P$ counted with multiplicities. Finally, suppose that the polynomial $P$ is vanishing at 1 with multiplicity $r = r(P)$.

In the course of improving the lower bound for the difference between an algebraic number and 1 due to M. Mignotte and M. Waldschmidt [9] (see also [3]), the author [5] introduced the following polynomial:

$$F(x) = F_k(x) = \prod_{1 \leqslant v < u \leqslant k} (x^{u-v} - 1)^{J_u J_v}, \tag{1}$$

where $k \geqslant 3$ is an integer and $J_u = [k \sin(\pi u/k)]$ for $u = 1, 2, \ldots, k$. In the present paper we show that the polynomial $F$ has large number of cyclotomic factors and is vanishing at 1 with high multiplicity.

In Section 2 we state Theorem 1 concerning the number of cyclotomic factors of the polynomial $F(x^2)$. Since the number of noncyclotomic factors of a polynomial is small (Theorem 2), we conjecture that the number of all irreducible factors of a polynomial is bounded above by the quantity with a slightly better constant than the one obtained in [9] (see Section 2). In Section 3 we state Theorem 3 which shows that the polynomial $F(x)$ has high multiplicity of 1. Finally, in Section 4 we prove our theorems in the reverse order and the corollary.

## 2. The number of irreducible factors of a polynomial

The problem of estimating $\Omega(P)$ has been studied by A. Schinzel [11] and E. Dobrowolski [4]. As it follows from their work it is natural to give separate estimates for $\Omega_c(P)$ and for the number of noncyclotomic factors $\Omega(P) - \Omega_c(P)$.

In 1993, C. Pinner and J. Vaaler [9] strengthened and generalized the results of A. Schinzel and E. Dobrowolski. In particular, they proved that

$$\frac{1}{n}\big(\Omega(P) - \Omega_c(P)\big) \leqslant c_1 s(P)\left(\frac{\log\big(1/s(P)\big)}{\log\log\big(1/s(P)\big)}\right)^3, \tag{2}$$

$$\frac{1}{n}\Omega_c(P) \leqslant \left(\sqrt{\frac{\zeta(2)\zeta(3)}{\zeta(6)}} + o(1)\right)\sqrt{s(P)\log\big(1/s(P)\big)}. \tag{3}$$

Here $c_1$ is an absolute and computable constant and $o(1) \to 0$ as $s(P) \to 0$. They also showed that the bound (3) is essentially sharp: the constant $\sqrt{\zeta(2)\zeta(3)/\zeta(6)} = 1.39\ldots$ which occurs in (3) cannot by replaced by a constant smaller than $3\sqrt{3}/4 = 1.29\ldots$. In this paper we prove the following inequality:

**Theorem 1.** *Suppose that $Q_k(x) = F_k(x^2)$, where the polynomial $F_k$ is given in* (1). *Then*

$$\frac{\Omega_c(Q_k)}{\deg Q_k} \geqslant \left(\frac{3\sqrt{2}}{\pi} + o(1)\right)\sqrt{s(Q_k)\log\big(1/s(Q_k)\big)}, \tag{4}$$

*where $o(1) \to 0$ as $k \to \infty$. Numerically one has $3\sqrt{2}/\pi = 1.35\ldots$.*

**Corollary.** *For every integer $n$ there exists a polynomial $P$ of degree $n$ such that*

$$\frac{1}{n}\Omega(P) \geqslant \frac{1}{n}\Omega_c(P) \geqslant \left(\frac{3\sqrt{2}}{\pi} + o(1)\right)\sqrt{s(P)\log\big(1/s(P)\big)}, \tag{5}$$

*where $o(1) \to 0$ as $n \to \infty$, $s(P) \to 0$.*

Put now $M(P)$ for the Mahler measure of $P$ and let

$$h(P) = \frac{\log M(P)}{n}.$$

Note that the inequalities

$$M(P) \leqslant \sqrt{\sum_{i=0}^{n} |a_i|^2} \leqslant \nu(P)$$

imply that $h(P) \leqslant s(P)$. The following theorem follows from [4], [6], [9]:

**Theorem 2.** *We have*

$$\frac{1}{n}\big(\Omega(P) - \Omega_c(P)\big) \leqslant \left(\frac{4}{9} + o(1)\right) h(P) \left(\frac{\log\big(1/h(P)\big)}{\log\log\big(1/h(P)\big)}\right)^3, \tag{6}$$

*where* $o(1) \to 0$ *as* $h(P) \to 0$.

The inequalities of the type (2), (6) are closely related with Lehmer's problem. If there exists a positive absolute constant $\delta$ such that $\log M(T) \geqslant \delta$ for all irreducible noncyclotomic polynomials $T$, then

$$\frac{1}{n}\big(\Omega(P) - \Omega_c(P)\big) \leqslant \frac{h(P)}{\delta}. \tag{7}$$

We will show below that inequality (7) is sharp (see also [10], Theorem 3, which is a more general result).

Notice that the right-hand side of (2) is small compared to the right-hand side of (3) whenever $s(P) \to 0$. Therefore both quantities $n^{-1}\Omega_c(P)$ and $n^{-1}\Omega(P)$ are bounded above by

$$\left(\sqrt{\frac{\zeta(2)\zeta(3)}{\zeta(6)}} + o(1)\right) \sqrt{s(P)\log\big(1/s(P)\big)},$$

where $o(1) \to 0$ as $s(P) \to 0$. Bearing in mind (5), it is tempting to conjecture that they are bounded above by

$$\left(\frac{3\sqrt{2}}{\pi} + o(1)\right) \sqrt{s(P)\log\big(1/s(P)\big)},$$

where $o(1) \to 0$ as $s(P) \to 0$. Then this bound would be the best possible.

It is interesting to note that the inequality

$$\frac{1}{n}\log|\alpha - 1| \geqslant \left(\frac{\pi}{4} + o(1)\right) \sqrt{h(P)\log\big(1/h(P)\big)},$$

obtained using the polynomial (1) in [5] is of the form similar to (5). Here $o(1) \to 0$ as $h(P) \to 0$ and not $n \to \infty$ as it is stated in [5]. The author wishes to express his thanks to Professor D. Masser for pointing out this misstatement in [5].

## 3. Polynomials with zeros of high multiplicity at 1

In 1933, I. Schur [12] showed that the number of real roots of a polynomial with complex coefficients is bounded from above by $2\sqrt{n\log\left(L(P)/\sqrt{|a_0a_n|}\right)}$, where $L(P)$ is the length of $P$. G. Szegő [13] proved that this bound is the best possible. In particular, for the multiplicity of 1 of an integer polynomial we have

$$r = r(P) \leqslant 2\sqrt{n\log\big(nH(P)\big)}. \tag{8}$$

On the other hand, applying Siegel's lemma M. Mignotte [7] proved that there exists a polynomial $P$ such that

$$r^2 \geqslant \big(2+o(1)\big)\frac{n\log H(P)}{\log n}, \tag{9}$$

where $o(1)\to 0$ as $r/n\to 0$.

Recently F. Amoroso [1] improved (8) and (9) showing that

$$r \leqslant 1.21\sqrt{n\log H(P)},$$

whenever $r,n,\to\infty$, $r/n\to 0$, $\sqrt{n\log n}/r\to 0$, and

$$r^2\log(n/r) \geqslant \big(4+o(1)\big)n\log H(P), \tag{10}$$

where $o(1)\to 0$ as $r,n\to\infty$, $r/n\to\infty$, $\sqrt{n/\log n}/r\to 0$. Earlier E. Bombieri and J. Vaaler [2] obtained inequality (10) with the constant 2 instead of 4 under the conditions $r,n\to\infty$, $r/n\to 0$. The proofs of both (9) and (10) are the proofs of existence. In fact, M. Mignotte's proof is based on pigeon-hole principle. The proof of E. Bombieri and J. Vaaler uses the geometry of numbers. The proof of F. Amoroso is also based on their result. We will show below that the polynomial given by (1) is vanishing at 1 with high multiplicity:

**Theorem 3.** *Suppose that the polynomial $F_k(x)$ of degree $n_k$ is given in* (1). *Then*

$$r(F_k)^2\log\big(n_k/r(F_k)\big) \geqslant \left(\frac{32}{\pi^2}+o(1)\right)n_k\log\nu(F_k), \tag{11}$$

$$r(F_k) \geqslant \left(\frac{8}{\pi}+o(1)\right)n_k\sqrt{s(F_k)/\log\big(1/s(F_k)\big)}, \tag{12}$$

*where both $o(1)\to 0$ as $k\to\infty$.*

Since $H(P)\leqslant\nu(P)\leqslant(n+1)H(P)$ and $32/\pi^2 = 3.24\ldots$ is less than 4, inequality (11) gives a bound which is slightly worse than (10).