THE AMERICAN MATHEMATICAL
MONTHLY
MAA
VOLUME 118, NO. 1 JANUARY 2011

An Official Publication of the **Mathematical Association of America**

THE AMERICAN MATHEMATICAL
MONTHLY
MAA
VOLUME 118, NO. 1 JANUARY 2011

NOTICE TO AUTHORS

The MONTHLY publishes articles, as well as notes and other features, about mathematics and the profession. Its readers span a broad spectrum of mathematical interests, and include professional mathematicians as well as students of mathematics at all collegiate levels. Authors are invited to submit articles and notes that bring interesting mathematical ideas to a wide audience of MONTHLY readers.

The MONTHLY's readers expect a high standard of exposition; they expect articles to inform, stimulate, challenge, enlighten, and even entertain. MONTHLY articles are meant to be read, enjoyed, and discussed, rather than just archived. Articles may be expositions of old or new results, historical or biographical essays, speculations or definitive treatments, broad developments, or explorations of a single application. Novelty and generality are far less important than clarity of exposition and broad appeal. Appropriate figures, diagrams, and photographs are encouraged.

Notes are short, sharply focused, and possibly informal. They are often gems that provide a new proof of an old theorem, a novel presentation of a familiar theme, or a lively discussion of a single issue.

Beginning January 1, 2011, submission of articles and notes is required via the MONTHLY's Editorial Manager System. Initial submissions in pdf or LaTeX form can be sent to the Editor-Elect Scott Chapman at

http://www.editorialmanager.com/monthly

The Editorial Manager System will cue the author for all required information concerning the paper. Questions concerning submission of papers can be addressed to the Editor-Elect at monthly@shsu.edu. Authors who use LaTeX are urged to use article.sty, or a similar generic style, and its standard environments with no custom formatting. The style of citations for journal articles and books should match that used on MathSciNet (see http://www.ams.org/mathscinet). Follow the link to Electronic Publications Information for authors at http://www.maa.org/pubs/monthly.html for information about figures and files, as well as general editorial guidelines.

Letters to the Editor on any topic are invited. Comments, criticisms, and suggestions for making the MONTHLY more lively, entertaining, and informative can be forwarded to the Editor-Elect at monthly@shsu.edu.

The online MONTHLY archive at *www.jstor.org* is a valuable resource for both authors and readers; it may be searched online in a variety of ways for any specified keyword(s). MAA members whose institutions do not provide JSTOR access may obtain individual access for a modest annual fee; call 800-331-1622.

See the MONTHLY section of MAA Online for current information such as contents of issues and descriptive summaries of forthcoming articles:

http://www.maa.org/

Proposed problems or solutions should be sent to:

DOUG HENSLEY, MONTHLY Problems
Department of Mathematics
Texas A&M University
3368 TAMU
College Station, TX 77843-3368

In lieu of duplicate hardcopy, authors may submit pdfs to monthlyproblems@math.tamu.edu.

Advertising Correspondence:
MAA Advertising
1529 Eighteenth St. NW
Washington DC 20036

Phone: (866) 821-1221
Fax: (866) 387-1208
E-mail: advertising@maa.org

Further advertising information can be found online at www.maa.org

Change of address, missing issue inquiries, and other subscription correspondence:
MAA Service Center, *maahq@maa.org*

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036

Recent copies of the MONTHLY are available for purchase through the MAA Service Center.
maahq@maa.org, 1-800-331-1622

Microfilm Editions: University Microfilms International, Serial Bid coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

The AMERICAN MATHEMATICAL MONTHLY (ISSN 0002-9890) is published monthly except bimonthly June-July and August-September by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, DC 20036 and Lancaster, PA, and copyrighted by the Mathematical Association of America (Incorporated), 2011, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution. Periodicals postage paid at Washington, DC, and additional mailing offices. ***Postmaster***: Send address changes to the American Mathematical Monthly, Membership/Subscription Department, MAA, 1529 Eighteenth Street, N.W., Washington, DC, 20036-1385.

Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*

David A. Cox

Abstract. This article explores the history of the Eisenstein irreducibility criterion and explains how Theodor Schönemann discovered this criterion before Eisenstein. Both were inspired by Gauss's *Disquisitiones Arithmeticae*, though they took very different routes to their discoveries. The article will discuss a variety of topics from 19th-century number theory, including Gauss's lemma, finite fields, the lemniscate, elliptic integrals, abelian groups, the Gaussian integers, and Hensel's lemma.

The Eisenstein irreducibility critierion is part of the training of every mathematician. I first learned the criterion as an undergraduate and, like many before me, was struck by its power and simplicity. This article will describe the unexpectedly rich history of the discovery of the Eisenstein criterion and in particular the role played by Theodor Schönemann.

For a statement of the criterion, we turn to Dorwart's 1935 article "Irreducibility of polynomials" in this MONTHLY [**9**]. As you might expect, he begins with Eisenstein:

> The earliest and probably best known irreducibility criterion is the Schoenemann-Eisenstein theorem:
>
> *If, in the integral polynomial*
>
> $$a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
>
> *all of the coefficients except a_0 are divisible by a prime p, but a_n is not divisible by p^2, then the polynomial is irreducible.*

Here's our first surprise—Dorwart adds Schönemann's name in front of Eisenstein's. He then gives a classic application:

> An important application of this theorem is the proof of the irreducibility of the so-called "cyclotomic polynomial"
>
> $$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1,$$
>
> where p is prime.

doi:10.4169/amer.math.monthly.118.01.003

*This paper originally appeared in the journal *Normat*, published by the Swedish National Center for Mathematics Education and the Mittag-Leffler Institute in cooperation with the Mathematical Societies of Denmark, Finland, Iceland, Norway, and Sweden. The author thanks the Editor of Normat for permission to reprint the article in this MONTHLY with minor changes from the original.

If, instead of $f(x)$, we consider $f(x+1)$, where

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p,$$

the theorem is seen to apply directly, and the irreducibility of $f(x+1)$ implies the irreducibility of $f(x)$.

The combination "Schönemann-Eisenstein" (often "Schoenemann-Eisenstein") was common in the early 20th century. An exception is Dorrie's delightful book *Triumph der Mathematik*, published in 1933 [**8**], where he states the "Satz von Schoenemann." Another exception is van der Waerden's *Moderne Algebra* from 1930 [**29**], where we find the "Eisensteinscher Satz."[1]

Given the influence of van der Waerden's book on succeeding generations of textbook writers, we can see how Schönemann's name got dropped. But how did it get added in the first place? Equally important, how did Eisenstein's get added? And why both names? To answer these questions, we need to explore some 19th-century number theory. This is a rich subject, so by necessity my treatment will be far from complete. I will instead focus on specific highlights to trace the development of these ideas. There will be numerous quotes (translated into English when necessary[2]) to illustrate how mathematics was done at the time and what it looked like. We begin with Gauss.

GAUSS. *Disquisitiones Arithmeticae* [**13**], published in 1801, contains an amazing amount of mathematics. In particular, Gauss proves that when p is prime, the cyclotomic polynomial $x^{p-1} + \cdots + x + 1$ is irreducible. His proof uses an explicit representation of the roots and is not easy. However, he also uses the following general result that relates irreducibility over $\mathbb{Z}$ to irreducibility over $\mathbb{Q}$:

42.

If the coefficients $A, B, C \ldots N; a, b, c \ldots n$ of two functions of the form

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots\ldots + N \ldots\ldots\ldots\ldots (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \ldots\ldots + n \ldots\ldots\ldots\ldots (Q)$$

are all rational and not all integers, and if the product of (P) and (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$$

then not all the coefficients $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{Z}$ can be integers.

This is what we now call *Gauss's lemma*. His proof is essentially the same one that appears in abstract algebra texts, though he states the result in the contrapositive form and never uses the term "polynomial." Gauss also doesn't use the three dots $\cdots$ that are standard today.

Another major result of *Disquisitiones* is Gauss's proof that $x^n - 1 = 0$ is solvable by radicals. The modern approach to solvability by radicals allows the introduction of arbitrary roots of unity, which implies that $x^n - 1 = 0$ is trivially solvable. Gauss instead followed the inductive strategy pioneered by Lagrange, where one constructs

[1] The 1930 edition included a reference to Schönemann that was dropped in the 1937 second edition.

[2] See `http://www.cs.amherst.edu/~dac/normat.pdf` for a version of the article that gives the quotes in their original languages.

the roots recursively using polynomials of strictly smaller degree that are solvable by radicals. In modern terms, this gives an explicit description of the intermediate fields of the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/p})$$

when p is prime. This has degree $p-1$ by the irreducibility of $x^{p-1}+\cdots+x+1$. From here, Gauss obtains his wonderful result about dividing the circle into n equal arcs by straightedge and compass.

The second paragraph of Section VII of *Disquisitiones* begins with a famous passage:

> The principles of the theory we are going to explain actually extend much farther than we will indicate. For they can be applied not only to circular functions but just as well to other transcendental functions, e.g. to those which depend on the integral $\int \frac{dx}{\sqrt{(1-x^4)}}$ and also to various types of congruences. Since, however, we are preparing a large work on those transcendental functions and since we will treat congruences at length in the continuation of these *Disquisitiones*, we have decided to consider only circular functions here.

In this quote, the reference to circular functions is clear. But what about transcendental functions that depend on the integral $\int \frac{dx}{\sqrt{1-x^4}}$? Here, any 19th-century mathematician would immediately think of the lemniscate $r^2 = \cos 2\theta$, whose arc length is $4\int_0^1 \frac{dx}{\sqrt{1-x^4}}$. This integral and its relation to the lemniscate were discovered by the Bernoulli brothers in the late 17th century and played a key role in the development of elliptic integrals by Fagnano, Euler, and Legendre in the 18th century. Gauss's "large work" on these functions never appeared, though fragments found after Gauss's death contain some astonishing mathematics (see [**3**]).

The quote also mentions "various types of congruences" that will be discussed "in the continuation of these *Disquisitiones*." The published version of *Disquisitiones* had seven sections, but Gauss drafted an eighth section, *Disquisitiones generales de congruentiis*, that studied polynomial congruences $f(x) \equiv 0 \bmod p$, where $f \in \mathbb{Z}[x]$ and p is prime (see pp. 212–242 of [**14**, vol. II] or pp. 602–629 of the German version of [**13**]). In modern terms, Gauss is studying the polynomial ring $\mathbb{F}_p[x]$. Here are some of his results:

- The existence and uniqueness of factorizations of polynomials modulo p.
- A formula for the number of monic irreducible degree-n polynomials modulo p. His result is

$$\frac{1}{n}\left(p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \sum p^{\frac{n}{abc}} \text{ etc.}\right)$$

  where the sum $\sum p^{\frac{n}{a}}$ is over all distinct prime factors of n, $\sum p^{\frac{n}{ab}}$ is over all pairs of distinct prime factors of n, and similarly for the remaining terms in the formula.

Gauss also had a theory of finite fields, though his approach is not easy for the modern reader because of his reluctance to introduce roots of polynomial congruences. Here is what Gauss says about the congruence $\xi \equiv 0 \bmod p$, where ξ is a polynomial with integer coefficients:

> ... but nothing prevents us from decomposing ξ, nevertheless, into factors of two, three or more dimensions [degrees], whereupon, in some sense, *imaginary* roots could be attributed to them. Indeed, we could have shortened incomparably all our following investigations, had we wanted to introduce such imaginary quantities by taking the same liberty some more recent mathematicians have taken; ...

Over the complex numbers, Gauss was the first to prove the existence of roots of polynomials. He was critical of those who simply assumed that roots exist, so he clearly wasn't going to assume that congruences of higher degree have solutions.

We refer the reader to [**11**] for a fuller account of Gauss's work on finite fields. Unfortunately, none of this was available until after Gauss's death in 1855. In particular, Schönemann was unaware of these developments when he rediscovered many of Gauss's results in the 1840s.

ABEL. Gauss's cryptic comments about the integral $\int \frac{dx}{\sqrt{1-x^4}}$ in *Disquisitiones* had a profound influence on Abel. He developed the theory of elliptic functions (as did Jacobi), based on the equation

$$y^2 = (1 - c^2x^2)(1 + e^2x^2), \tag{1}$$

and his elliptic functions were inverse functions to the elliptic integrals

$$\int \frac{dx}{y} = \int \frac{dx}{\sqrt{(1 - c^2x^2)(1 + e^2x^2)}}. \tag{2}$$

Setting $e = c = 1$ gives $\int \frac{dx}{\sqrt{1-x^4}}$. In Abel's time, it was well known that this integral is intimately related to arc length on the lemniscate shown in Figure 1 (see [**3**] for the history of this relation).

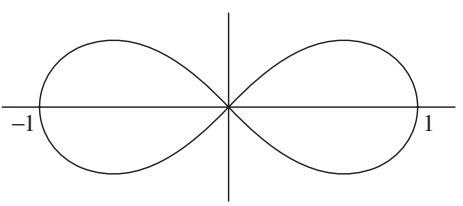

Figure 1. The lemniscate $r^2 = \cos 2\theta$.

It follows that dividing an arc of the lemniscate starting at the origin into m pieces of equal arc length can be interpreted as a relation between integrals, which Abel and Eisenstein would write as

$$\int_0 dy/\sqrt{1 - y^4} = m \int_0 dx/\sqrt{1 - x^4}. \tag{3}$$

This is the *m-division problem* for the lemniscate. When the entire lemniscate is divided into m pieces of equal length, equation (3) led Abel and Eisenstein (and Gauss before them, though unpublished) to a polynomial $P_m(x)$ of degree m^2 satisfied by the polar coordinates of the m-division points of the lemniscate. We will explain how this works when we discuss Eisenstein later in the article.

The mathematics involved here is surprisingly rich. The study of elliptic integrals such as (2) eventually become the study of *elliptic curves* such as (1). The book [**22**] gives a nice introduction to elliptic curves and their relation to elliptic integrals. These days, the m-division problem for elliptic integrals is described in terms of the m-division points on elliptic curves. See [**22**] and [**28**] for more on this important topic in modern number theory.

For Abel and his contemporaries, a central question was whether polynomial equations such as $P_m(x) = 0$ were "solvable algebraically," which these days means solvable by radicals. Abel was uniquely qualified to pose this question, since just four years earlier he had proved that the general quintic was not solvable by radicals.

In his great paper *Recherches sur les functions elliptiques* [**1**, pp. 263–388], published in volumes 2 and 3 of Crelle's journal[3] in 1827 and 1828, Abel considers the equation $P_{2n+1}(x) = 0$ coming from the $(2n + 1)$-division problem for the elliptic integral (2). Here is what he has to say about this equation:

> Thus finally the solution of the equation $P_{2n+1} = 0$ is reduced to a single equation of degree $2n + 2$; but *in general* this equation does not appear to be solvable algebraically. Nevertheless one can solve it completely in many particular cases, for example, when $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$ etc. In the course of this memoir I will concern myself with these cases, of which the first is especially remarkable, both for the simplicity of its solution, as well as by its beautiful application to geometry.
>
> Indeed among other theorems I arrived at this one:
>
> "One can divide the entire circumference of the lemniscate into m parts *by ruler and compass only*, if m is of the form 2^n or $2^n + 1$, the last number being at the same time prime, or if m is a product of several numbers of these two forms."
>
> This theorem is, as one sees, precisely the same as that of M. *Gauss*, relative to the circle.

The reduction to an equation of degree $2n + 2$ was done by classical methods of Lagrange. The mind-blowing result about ruler and compass constructions on the lemniscate ($e = c$) can be stated more formally as follows.

Abel's Theorem on the Lemniscate. *The lemniscate can be divided into m pieces of equal arc length by ruler and compass if and only if m is a power of* 2 *times a product of distinct Fermat primes.*

We will say more about Abel's theorem later in the article. Other aspects of Abel's quote are equally mind-blowing when considered from the modern perspective of elliptic curves:

- The cases $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$, etc. that Abel can solve by radicals correspond to elliptic curves with complex multiplication (see [**4**] for an introduction). Abel was the first to identify this important class of elliptic curves.
- By class field theory, division points of elliptic curves with complex multiplication generate abelian extensions and hence have abelian Galois groups. Since abelian groups are solvable, Galois theory implies that the division equations $P_{2n+1}(x) = 0$ are solvable by radicals.
- When the curve doesn't have complex multiplication, Abel was more cautious: they do "not appear to be solvable algebraically." By deep work of Serre on Galois

[3] The *Journal für die reine und angewandte Mathematik*, founded by August Leopold Crelle in 1826.

representations of elliptic curves [**27**], we now know that with at most finitely many exceptions, these equations aren't solvable by radicals.

Again we are in the presence of remarkably rich mathematics.

Abel thought deeply about why his equations $P_{2n+1}(x) = 0$ were solvable by radicals when the curve has complex multiplication. He realized that the underlying reason was the structure of the roots and how they relate to each other. His general result appears in his *Mémoire sur une classe particulière d'équations résolubles algébriquement* [**1**, pp. 478–507], which was published in Crelle's journal in 1829. The article begins:

> Although the algebraic solution of equations is not possible in general, there are nevertheless particular equations of all degrees which admit such a solution. Examples are the equations of the form $x^n - 1 = 0$. The solution of these equations is based on certain relations that exist among the roots.

The first sentence refers to Abel's result on the unsolvability of the general quintic and the solution of $x^n - 1 = 0$ described by Gauss in *Disquisitiones*. To give the reader a sense of what he means by "relations that exist among the roots," Abel takes a prime n and considers the cyclotomic equation $x^{n-1} + \cdots + x + 1 = 0$. Let $\theta(x) = x^\alpha$, where α is a primitive root modulo n. Then the roots are given by

$$x,\ \theta(x) = x^\alpha,\ \theta^2(x) = x^{\alpha^2},\ \theta^3(x) = x^{\alpha^3}, \ldots,\ \theta^{n-2}(x) = x^{\alpha^{n-2}},\ \text{where } \theta^{n-1}(x) = x.$$

Abel goes on to say that the same property appears in a certain class of equations that he found in the theory of elliptic functions. He then states the main theorem of the paper:

> In general I have proved the following theorem:
>
> „If the roots of an equation of arbitrary degree are related among themselves in such a way, that *all* of the roots can be rationally expressed in terms of one of them, which we designate by x; if in addition, designating by θx, $\theta_1 x$ two other arbitrary roots, one has
>
> $$\theta\theta_1 x = \theta_1\theta x,$$
>
> the equation in question is always solvable algebraically. . . ."

Abel's "classe particulière" consists of all polynomials that satisfy the hypothesis of his theorem. To see what this means in modern terms, let $K \subseteq L$ be a Galois extension with primitive element α. For each element σ_i of the Galois group $\mathrm{Gal}(L/K)$, there is a polynomial $\theta_i(x) \in K[x]$ such that $\sigma_i(\alpha) = \theta_i(\alpha)$. Then one easily computes that

$$\sigma_i\sigma_j(\alpha) = \theta_j(\theta_i(\alpha)).$$

The switch of indices is correct—you should check why. Since σ_i is determined by its value on α,

$$\sigma_i\sigma_j = \sigma_j\sigma_i \iff \theta_j(\theta_i(\alpha)) = \theta_i(\theta_j(\alpha)).$$

Since the $\theta_i(\alpha)$ are the roots of the minimal polynomial $f(x)$ of α over K, we see that $f(x)$ is in the "classe particulière" if and only if $\mathrm{Gal}(L/K)$ is commutative. Abel's

theorem now follows easily from Galois theory since commutative Galois groups are solvable.

Besides proving his general theorem, Abel intended to give two applications:

> After having developed this theory in general, I will apply it to circular and elliptic functions.

The version published in Crelle's journal has a section on circular functions, but ends with the following footnote by Crelle:

> *) The author of this memoir will give applications to elliptic functions on another occasion.

Alas, Abel died shortly after this article appeared.

AFTER ABEL. Abel's "classe particulière" had an important influence on Kronecker, Jordan, and Weber. Specifically:

- In 1853, Kronecker [**18**, vol. IV, p. 11] defined $f(x) = 0$ to be "abelian" provided it has roots $x, \theta(x), \ldots, \theta^{n-1}(x)$, $x = \theta^n(x)$. Here, as for Abel, θ is a rational function. This special case of Abel's "classe particulière" corresponds to polynomials with cyclic Galois groups.
- In 1870, Jordan [**17**, p. 287] defined $f(x) = 0$ to be "abelian" in terms of its Galois group:

  > We thus call *abelian equations* all of those whose group only contains substitutions that are exchangeable among each other.

  Here, "exchangeable" is Jordan's way of saying "commutative." He then proves [**17**, p. 288] that for irreducible equations, his definition is equivalent to Abel's "classe particulière."
- The first two volumes of Weber's monumental *Lehrbuch der Algebra* were published in 1894 and 1896. He gives the name "abelian" to Abel's "classe particulière" [**30**, vol. I, p. 576] and later defines a commutative group to be "abelian" [**30**, vol. II, p. 6]. As far as I know, this is the first appearence of the term "abelian group" in the modern sense.[4]

The definition of "abelian group" given in introductory algebra courses seems so simple. But in the background is a rich history involving Gauss, Abel, the leminiscate, elliptic functions, complex multiplication, and solvability by radicals.

SCHÖNEMANN. Unlike the other people mentioned so far, Theodor Schönemann is not a familiar name. He has no biography at the MacTutor History of Mathematics archive [**21**]. According to the *Allgemeine Deustsche Biographie* [**2**, vol. 32, pp. 293–294], Schönemann lived from 1812 to 1868 and was educated in Königsberg and Berlin under the guidance of Jacobi and Steiner. He got his doctorate in 1842 and became Oberlehrer and eventually Professor at a gymnasium in Brandenburg an der Havel. Lemmermeyer's book [**19**] includes several references to Schönemann's work in number theory, and some of his results are mentioned in Dickson's classic *History*

[4] In 1870, Jordan used the term "groupe abélien" to refer to a group closely related to a symplectic group over a finite field [**17**, Livre II, §VIII].

of the Theory of Numbers [**7**], especially in the chapter on higher congruences in the first volume.

For us, Schönemann's most important work is a long paper printed in two parts in Crelle's journal in 1845 and 1846. The first part [**24**], consisting of §§1–50, appeared as *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist* (*Foundations of a general theory of higher congruences, whose modulus is a real prime number*). In the preface, Schönemann refers to Gauss:

> The famous author of *Disquisitiones Arithmeticae* had intended a general theory of higher congruences for Section Eight of his work. Since, however, this Section Eight did not appear, and also, as far as I know, the author did not publish anything on this subject, nor indicate anything precisely ...

Schönemann suspects that he may have been scooped by Gauss, but is not worried:

> ... the loss of first discovery would be compensated by my knowing of having met in my own and independent way such a spirit.

Indeed, Schönemann had been scooped by Gauss, and as we will see later in the article, also by Galois. Hence we should change "a spirit" to "spirits" in the quote, in which case the sentiment is even more apt.

Similar to what Gauss did, Schönemann gave a careful treatement of polynomials modulo p, including unique factorization. But then, in §14, he did something different. Let $f(x) \in \mathbb{Z}[x]$ be monic of degree n and irreducible modulo p, and let $\alpha \in \mathbb{C}$ be a root of $f(x)$ (proved to exist by Gauss). Given polynomials $\varphi, \psi \in \mathbb{Z}[x]$, Schönemann defined $\varphi(\alpha)$ and $\psi(\alpha)$ to be *congruent modulo* (p, α), written $\varphi(\alpha) \equiv \psi(\alpha) \pmod{p, \alpha}$, if $\varphi(\alpha) = \psi(\alpha) + pR(\alpha)$ for some $R \in \mathbb{Z}[x]$. He then proves that the "allgemeine Form eines kleines Restes" ("general form of a smallest remainder") is $a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}$, where $a_i \in \{0, \ldots, p-1\}$. This gives a field with p^n elements.

We can recast Schönemann's construction as follows. The root α is an algebraic integer and $\mathbb{Z}[\alpha]$ is a ring under multiplication. The equivalence relation $\varphi(\alpha) \equiv \psi(\alpha) \pmod{p, \alpha}$ means that $\varphi(\alpha)$ and $\psi(\alpha)$ give the same coset in the quotient ring $\mathbb{Z}[\alpha]/\langle p\rangle$, where $\langle p\rangle = p\mathbb{Z}[\alpha]$ is the ideal generated by p. We will see later that $\mathbb{Z}[\alpha]/\langle p\rangle$ is a field since $f(x)$ is irreducible modulo p. Thus $\mathbb{Z}[\alpha]/\langle p\rangle$ is the modern version of Schönemann's finite field. In what follows, we will write $\mathbb{F}_{p^n}$ instead of $\mathbb{Z}[\alpha]/\langle p\rangle$ since this field has p^n elements.

Here are some other results proved by Schönemann:

- The elements of $\mathbb{F}_{p^n}$ are the roots of $x^{p^n} - x$. He wrote this as $x^{p^n} - x \equiv 0 \pmod{p, \alpha}$.
- $f(x) \equiv (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{n-1}}) \pmod{p, \alpha}$. Thus $\mathbb{F}_{p^n}$ is the splitting field of $f(x)$ modulo p. The Galois group (generated by Frobenius) is implicit in this factorization of f.

The first part of Schönemann's paper culminates in §50 with a lovely proof of the irreducibility of $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. We will give the proof in modern notation. Pick a prime $\ell \neq p$ and consider the prime factorization

$$\Phi_p(x) \equiv f_1(x) \cdots f_r(x) \bmod \ell.$$

where the f_i are irreducible modulo ℓ. Standard properties of finite fields imply that for $i = 1, \ldots, r$,

$$\begin{aligned}\deg(f_i) &= \text{the minimum } n \text{ such that } \mathbb{F}_{\ell^n}^* \text{ has an element of order } p \\ &= \text{the minimum } n \text{ such that } \ell^n \equiv 1 \bmod p \\ &= \text{the order of the congruence class of } \ell \text{ in } (\mathbb{Z}/p\mathbb{Z})^*.\end{aligned} \tag{4}$$

We leave this as a fun exercise for the reader. By Dirichlet's theorem on primes in arithmetic progressions (proved just a few years before Schönemann's paper), every congruence class modulo p contains a prime. In particular, the congruence class of a primitive root contains a prime ℓ. A primitive root modulo p gives a congruence class of order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^*$, so that $n = p-1$ in (4) for this choice of ℓ. This implies that $\Phi_p(x)$ is irreducible modulo ℓ and hence irreducible over $\mathbb{Z}$. Then $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ by Gauss's lemma.

This proof is simpler than Gauss's, though it does require knowledge of finite fields and uses Dirichlet's classic result. The use of the auxiliary prime ℓ is especially elegant. When I studied Grothendieck-style algebraic geometry as a graduate student in the 1970s, I was always happy when a proof picked a prime different from the residue characteristic. This seemed so modern and cutting-edge. Little did I realize that Schönemann had used the same idea 120 years earlier.

The second part of Schönemann's paper [**25**], titled *Von denjenigen Moduln, welche Potenzen von Primzahlen sind* (*On those moduli, which are powers of prime numbers*), consists of §§51–66. In this paper, Schönemann considered the factorization of polynomials modulo p^m, and in particular, how the factorization changes as m varies. One of his major results, in §59, is what we now call *Hensel's lemma*:

> Lemma. If any monic polynomial[5] of x can be factored modulo p into two monic factors, which for this modulus have no common divisor: then this polynomial can be factored modulo p^m, ***in a unique manner***, into two factors, which are congruent to those first two factors modulo p.[6]

As a consequence, when an irreducible polynomial modulo p^m is reduced modulo p, the result must be a power of an irreducible polynomial modulo p. In §61, Schönemann asks about the converse:

> Problem. To investigate, whether the power of an irreducible polynomial modulo p is or is not irreducible modulo p^m.

An especially simple example is $(x-a)^n$, and for a polynomial congruent to $(x-a)^n$ modulo p, the first place to check for irreducibility is modulo p^2. Here is Schönemann's answer:

> ... hence one may state the theorem: ***that $(x-a)^n + pFx$ is irreducible modulo p^2, when the factor $x-a$ is not contained in Fx modulo p***....

[5] Schönemann used "Ausdruck" ("expression") for polynomial and "einfach" ("simple") for monic.

[6] The uniqueness assertion enables us to take the limit as $m \to \infty$, giving a factorization over the p-adic integers $\mathbb{Z}_p$ that reduces to the given factorization modulo p. This version of Hensel's lemma is stated in [**16**, Thm. 3.4.6], and the discussion on [**16**, p. 72] relates this to the more common version of Hensel's lemma, which asserts that for $f(x) \in \mathbb{Z}_p[x]$, a solution of $f(x) \equiv 0 \bmod p$ of multiplicity one lifts to a solution of $f(x) = 0$ in $\mathbb{Z}_p$.

As stated, this is not quite correct—one needs to assume that $\deg(F) \le n$.[7] Since $x - a$ divides $F(x)$ modulo p if and only if $F(a) \equiv 0 \bmod p$, we can state Schönemann's result as follows.

Schönemann's Irreducibility Criterion. *Let $f(x) \in \mathbb{Z}[x]$ have degree $n > 0$ and assume that there is a prime p and an integer a such that*

$$f(x) = (x - a)^n + pF(x), \quad F(x) \in \mathbb{Z}[x].$$

If $F(a) \not\equiv 0 \bmod p$, then $f(x)$ is irreducible modulo p^2.

We sketch a proof for the convenience of the reader.

Proof. Suppose $(x - a)^n + pF(x)$ has a nontrivial factorization modulo p^2, say

$$(x - a)^n + pF(x) \equiv G(x)H(x) \bmod p^2. \tag{5}$$

One can easily reduce to the case where $G(x)$ and $H(x)$ are monic. Then $(x - a)^n \equiv G(x)H(x) \bmod p$ and unique factorization imply $G(x) \equiv (x - a)^i \bmod p$ and $H(x) \equiv (x - a)^j \bmod p$, where $i, j > 0$ and $i + j = n$. Setting $x = a$ in these congruences, we see that p divides both $G(a)$ and $H(a)$ since $i, j > 0$. Then setting $x = a$ in (5) implies $pF(a) \equiv 0 \bmod p^2$, a contradiction. ∎

The pleasant surprise is that this result implies the Eisenstein criterion. To see why, suppose that $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ satisfies the hypothesis of the Eisentstein criterion. Multiplying by a suitable integer, we may assume $a_0 \equiv 1 \bmod p$. This allows us to write $f(x) = x^n + pF(x)$. Note also that $F(0) \not\equiv 0 \bmod p$ since p^2 does not divide a_n. Then $f(x)$ is irreducible modulo p^2 by Schönemann's criterion. This implies irreducibility over $\mathbb{Z}$ and hence over $\mathbb{Q}$ by Gauss's lemma.

As you might expect, Schönemann immediately applies his irreducibility criterion to a familiar polynomial:

> Let us apply the result just obtained to the expression $\dfrac{x^n - 1}{x - 1}$, where n denotes a prime number. In this case $x^n - 1 \equiv (x - 1)^n$ (mod. n), and one thus obtains
>
> $$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = (x - 1)^{n-1} + nFx.$$
>
> For $x = 1$ one obtains $n = nF(1)$ and thus $F(1) = 1$, and not $\equiv 0$ (mod. n). ***From this, it follows that $\dfrac{x^n - 1}{x - 1}$ is always irreducible modulo n^2, if n is a prime number; hence, this expression is certainly irreducible in the algebraic sense.***
>
> The ease of proof of this theorem is striking, because the proof in „Disquisitiones" requires much greater cleverness, and is much more elaborate. (See §. 50. Rem. 2.)

This proves the irreducibility of $x^{n-1} + \cdots + x + 1$ without the change of variable $x \leftrightarrow x + 1$ needed when one uses the Eisenstein criterion. Schönemann is clearly

[7] For example, let $F(x) = x^3 - p^2x + 1$. Then $x^2 + pF(x) = (px + 1)(x^2 - p^2x + p)$ even though $F(0) \not\equiv 0 \bmod p$.

pleased that his proof is so much simpler than Gauss's. (The parenthetical comment at the end of the quote refers to Schönemann's earlier proof of irreducibility from §50 of his article.)

Schönemann's criterion is lovely but is unknown to most mathematicians. So how did I learn about it? My book on Galois theory [**5**] gives Eisenstein's proof of Abel's theorem on the lemniscate. In trying to understand Eisenstein, I looked at Lemmermeyer's wonderful book *Reciprocity Laws* [**19**], where I found a reference to Schönemann. When I tried to read Schönemann's paper, I couldn't find the Eisenstein criterion, in part because the paper is long and my German isn't very good, and in part because I was looking for Eisenstein's version, not Schönemann's. I looked back at Lemmermeyer's book and noticed that Lemmermeyer thanked Michael Filaseta for the Schönemann reference. I wrote to Filaseta, who replied that Schönemann proved a criterion for a polynomial to be irreducible modulo p^2. This quickly led me to §61 of the article, which is where Schönemann states his result.

BACK TO GAUSS. Besides discovering the Eisenstein criterion before Eisenstein, Schönemann also discovered Hensel's lemma before Hensel. Unfortunately, Schönemann and Hensel were both scooped by Gauss. In his draft of the unpublished eighth section of *Disquisitiones* (p. 627 of the German version of [**13**] or p. 238 of [**14**, vol. II]), Gauss takes a polynomial X with integer coefficients and studies its behavior modulo p and p^2:

> PROBLEM. *If the function X decomposes modulo p into mutually prime factors ξ, ξ', ξ'' etc., then similarly X decomposes modulo p^2 into factors Ξ, Ξ', Ξ'' etc. such that*
>
> $$\xi \equiv \Xi,\ \xi' \equiv \Xi',\ \xi'' \equiv \Xi'',\ \text{etc. (mod. } p)$$

Gauss proves this and then explains how the same principle applies modulo p^k for any k. His "PROBLEM" is weaker than Schönemann's "Lemma" because it doesn't say that the lifted factorization is unique. So what Gauss really proved was a "proto-Hensel's lemma." Nevertheless, Gauss was sufficiently pleased with this result that he recorded it in his famous mathematicial diary [**15**]. Here is entry 79, dated September 9, 1797:

> Beginning to uncover principles, by which the resolution of congruences according to multiple moduli is reduced to congruences according to linear moduli.

Here, "resolution of congruences according to multiple moduli" means factoring polynomials modulo p^k, and similarly "congruences according to linear moduli" means working modulo p. This reading of Gauss's diary entry is carefully justified in [**11**].

Besides this elementary version of Hensel's lemma, Gauss also considered the case when the factors modulo p are not distinct. For example, the congruence $X \equiv X'(x-a)^m$ (mod. p) appears near the end of Gauss's draft of the eighth section. Had he pursued this, it is quite possible that he would have followed the same path as Schönemann and discovered the Eisenstein criterion. But instead, the draft ends abruptly in the middle of a congruence: the last thing Gauss wrote was

$$0 \equiv$$

As with many other projects, Gauss never returned to finish *Disquisitiones generales de congruentiis*. It came to light only after being published in 1863 in the second volume of his collected works, and today is still overshadowed by its more famous sibling, *Disquisitiones Arithmeticae*.

MORE ON FINITE FIELDS. Besides Gauss and Schönemann, Galois also developed the theory of finite fields. In his paper *Sur la théorie des nombres*, appearing in 1830 in the *Bulletin des sciences mathématiques de Ferussac* [**12**, pp. 113–127], Galois begins with a congruence $F(x) \equiv 0 \bmod p$, or as he writes it, $Fx = 0$, where $F(x)$ is irreducible modulo p. Then he considers the roots:

> One must regard the roots of this congruence as a kind of imaginary symbol . . .

He then goes on to prove the results about finite fields discovered later by Schönemann. It appears that Schönemann was unaware of Galois's work.

Gauss would have been critical of the roots so blithely assumed to exist by Galois. Schönemann's construction via $\mathbb{Z}[\alpha]/\langle p\rangle$, on the other hand, is rigorous since it uses a root $\alpha \in \mathbb{C}$ of $f(x)$. However, the fundamental theorem of algebra is really a theorem in analysis since it ultimately depends on the completeness of the real numbers. For an algebraic version of Schönemann's construction, note that since $f(x) \in \mathbb{Z}[x]$ is monic and irreducible, $x \mapsto \alpha$ induces a ring isomorphism

$$\mathbb{Z}[x]/\langle f(x)\rangle \simeq \mathbb{Z}[\alpha].$$

Reducing $f(x)$ modulo p gives a polynomial $\bar{f} \in \mathbb{F}_p[x]$, which Schönemann assumed to be irreducible. It follows that the quotient ring $\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle$ is a field. Then the isomorphisms

$$\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle \simeq \mathbb{Z}[x]/\langle p,\, f(x)\rangle \simeq \mathbb{Z}[\alpha]/\langle p\rangle$$

show that Schönemann's ring $\mathbb{Z}[\alpha]/\langle p\rangle$ is in fact a finite field with p^n elements.

This algebraic version of finite fields was made explicit by Dedekind in his 1857 paper *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus* (*Outline of a theory of higher congruences for a real prime modulus*) [**6**]. Dedekind begins the paper by noting that the subject was initiated by Gauss and had been studied by Galois and Schönemann. Dedekind was unaware of the full power of what Gauss had done, though later he became the editior in charge of publishing *Disquisitiones generales de congruentiis* in volume II of Gauss's collected works in 1863.

Dedekind's construction is essentially what we did above with the quotient ring $\mathbb{Z}[x]/\langle p,\, f(x)\rangle$, $f(x)$ irreducible modulo p, though Dedekind was writing before the concept of quotient ring was fully established. Nevertheless, he shows that this is a finite field with p^n elements, $n = \deg(f)$. For much of the 19th century, "finite field" meant this object. It has the advantage of being easy to compute with (even today, computers represent finite fields this way), but mathematically, it depends on the choice of $f(x)$ and hence is intrinsically noncanonical.

One of the first fully abstract definitions of finite field was given by E. H. Moore, whose paper [**20**] appeared in the proceedings of the 1893 international congress of mathematicians. Here is his definition:

> Suppose that we have a system of s distinct symbols or *marks**, $\mu_1, \ldots, \mu_s$ (s being some finite positive integer), and suppose that these marks may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, and division—these operations being subject to the ordinary abstract *operational identities* of algebra
>
> $$\mu_i + \mu_j = \mu_j + \mu_i;\ \mu_i\mu_j = \mu_j\mu_i;\ (\mu_i + \mu_j)\mu_k = \mu_i\mu_k + \mu_j\mu_k;\ \text{etc.}$$

and that when the marks are so combined the results of these operations are in every case uniquely determined and belong to the system of marks. Such a system we shall call a *field of order s*, using the notation $F[s]$.

We are led at once to seek *To determine all such fields of order s*, $F[s]$.

The words "system" and "marks" indicate that Moore was writing before the language of set theory was standardized. Moore went on to show that his definition was equivalent to the Dedekind-style representation of a finite field. So in 1893 we finally have a modern theory of finite fields.

The word "marks" in Moore's quote has an the asterisk that leads to the following footnote:

* It is necessary that all *quantitative* ideas should be excluded from the concept *marks*. Note that the signs $>$, $<$ do not occur in the theory.

Moore was writing for a mathematically sophisticated audience, but he didn't assume that they had the apparatus of set theory in their heads—his footnote was intended to help them understand the abstract nature of what he was saying. This is something we should keep in mind when we teach abstract algebra to undergraduates.

EISENSTEIN. We finally get to Eisenstein, whose work on Abel's theorem on the lemniscate culminated in a long two-part paper in Crelle's journal in 1850 [**10**, pp. 536–619]. To set the stage, we use the polar equation $r^2 = \cos 2\theta$ of the lemniscate and regard r as a function of arc length s. Thus

$$r = \varphi(s)$$

means that if we start at the origin and follow the branch of the lemniscate in the first quadrant for distance s, then we end at a point with polar coordinates (r, θ). Figure 2 shows what happens when we follow the curve into the fourth quadrant.

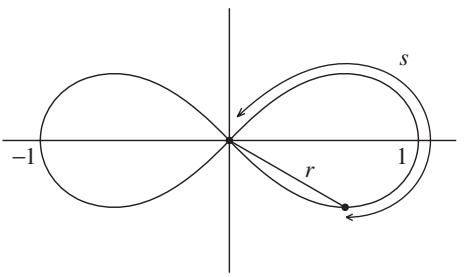

Figure 2. $r = \varphi(s)$ on the lemniscate.

An arc length calculation (see [**5**, §15.2]) shows that s is related to r via the equation

$$s = \int_0^r \frac{dr}{\sqrt{1 - r^4}}.$$

(We follow the 19th-century practice of using the same letter for the variable and limit of integration.) Combining this with $r = \varphi(s)$, we obtain

$$r = \varphi(s) \iff s = \int_0^r \frac{dr}{\sqrt{1 - r^4}}. \tag{6}$$

In other words, the lemniscatic function $r = \varphi(s)$ is the inverse function of the elliptic integral $\int_0^r \frac{dr}{\sqrt{1-r^4}}$ we first met in Section VII of *Disquisitiones*.

In the equation (6), $0 \le r \le 1$ corresponds to $0 \le s \le \varpi = \int_0^1 \frac{dr}{\sqrt{1-r^4}}$, so that ϖ is one-fourth of the total arc length of the lemniscate. In particular, $\varphi(\varpi) = 1$ and $\varphi(2\varpi) = 0$, and for any positive integer m, the radii $r = \varphi(k \cdot 2\varpi/m)$, $k = 1, \ldots, m$, give the points that divide the right half of the lemniscate into m equal pieces.

The change of variables $r = iu$ in (6) led Abel to define $\varphi(is) = i\varphi(s)$, and then Euler's addition law makes $\varphi(z) = \varphi(s + it)$ into a function of a complex variable $z \in \mathbb{C}$.[8] Further application of the addition law shows that for any Gaussian integer $m \in \mathbb{Z}[i]$, $\varphi(mz)$ is a rational function of $\varphi(z)$ and its derivative $\varphi'(z)$. This is what *complex multiplication* means for the lemniscatic function φ.

If $m = a + ib$ is an *odd* Gaussian integer, meaning that $a + b$ is odd, then $\varphi(mz)$ is a rational function of $\varphi(z)$ of a very special form. More precisely, given such an m, there are polynomials $U(x)$ and $V(x)$ with coefficients in $\mathbb{Z}[i]$ such that $y = \varphi(mz)$ is related to $x = \varphi(z)$ via

$$y = \frac{U(x)}{V(x)} = \frac{A_0 x + A_1 x^5 + \cdots + A_{(N(m)-1)/4} x^{N(m)}}{1 + B_1 x^4 + \cdots + B_{(N(m)-1)/4} x^{N(m)-1}}, \tag{7}$$

where $N(m) = a^2 + b^2$ is the norm (in the sense of algebraic number theory) of $m = a + ib$. A modern proof can be found in [**5**, Thm. 15.4.4]. Using (6), we obtain

$$\int_0^y \frac{dy}{\sqrt{1-y^4}} = m \int_0^x \frac{dx}{\sqrt{1-x^4}} \iff y = \frac{U(x)}{V(x)}.$$

In 19th-century parlance, the relation $y = U(x)/V(x)$ is an *algebraic integral* of this equality of integrals. This explains equation (3) from earlier in the article.

When m is an ordinary odd integer, we know that $r = \varphi(k \cdot 2\varpi/m)$ gives m-division points on the lemniscate. Substituting

$$y = \varphi(m \cdot (k \cdot 2\varpi/m)) = \varphi(k \cdot 2\varpi) = 0 \text{ and } x = \varphi(k \cdot 2\varpi/m) = r$$

into (7), we see that

$$0 = \frac{U(r)}{V(r)}, \text{ hence } U(r) = 0.$$

This proves that the division radii r are roots of the polynomial equation $U(x) = 0$. When $m = 2n + 1$, this is *precisely* the equation $P_{2n+1}(x) = 0$ considered by Abel.

Eisenstein used the same setup as Abel. To prove Abel's theorem on the lemniscate, he reduced to the case when $m = a + ib$ is an odd Gaussian prime. Since $U(x)$ has x as a factor, Eisenstein wrote $U(x) = xW(x)$, and the strategy of his proof was to show that $W(x)$ is irreducible. Once this is proved, Abel's theorem follows—see [**5**, §15.5].[9]

But how did Eisenstein prove that the polynomial $W(x)$ is irreducible? This is not easy. A key step for Eisenstein was when he noticed something about the coefficients of $W(x)$. He shared his thoughts with Gauss in a letter dated 18 August 1847 [**10**, p. 845]:

[8] Gauss followed the same path in 1797, though he never published his findings. See [**3**] for more details.

[9] For a complete proof of Abel's theorem on the lemniscate, the reader should consult [**5**], [**22**], or [**23**]. The last reference gives a modern proof via class field theory.

When $m = a + bi$ is an odd complex integer of norm p and $y = \dfrac{U}{V} = \dfrac{A_0x + A_1x^5 + \cdots + A_{(p-1)/4}x^p}{1 + B_1x^4 + \cdots + B_{(p-1)/4}x^{p-1}}$ is the algebraic integral of the equation

$$\int_0 dy/\sqrt{1-y^4} = m \int_0 dx/\sqrt{1-x^4},$$

I had earlier shown that for a *two-term* complex prime number m the coefficients of the numerator up to the last, which is a complex unit, and the coefficients of the denominator except the first, which $= 1$, are all divisible by m. I conjectured that this proposition is also correct when m is a *one-term* prime number ($\equiv 3 \pmod 4$ apart from sign or a complex unit as factor);

In the first part of the quote, Eisenstein sets up the situation, and after the displayed equation, describes the structure of the coefficients of the numerator and denominator. Recall that odd Gaussian primes come in two flavors:

- *Two-term* primes of the form $m = a + ib$, where $p = a^2 + b^2$ is prime and $p \equiv 1 \bmod 4$.
- *One-term* primes of the form $m = \varepsilon q$, where ε is a unit in $\mathbb{Z}[i]$ and $q \equiv 3 \bmod 4$.

Now consider the polynomial

$$W(x) = \frac{1}{x}U(x) = A_0 + A_1x^4 + \cdots + A_{(p-1)/4}x^{p-1}.$$

For a two-term prime m, Eisenstein says that he earlier had shown that the last coefficient $A_{(p-1)/4}$ is a complex unit and the other coefficients $A_0, \ldots, A_{(p-1)/4-1}$ are divisible by m. He conjectures that the same is true for one-term primes.

This smells like the Eisenstein criterion, especially since Eisenstein notes in the letter that the constant term A_0 is m, which is not divisible by m^2. The difference is that m and the coefficients of W are Gaussian integers. A bit later in the letter, Eisenstein considers what happens if W is not irreducible over $\mathbb{Q}(i)$ [**10**, pp. 848–849]:

> ... if it is possible that W is the product of two polynomials[10] of x with Gaussian integer coefficients, and their degrees are $< p - 1$. Let $W = PQ$; since the constant term of W is $= m$, so if m is a complex prime, the constant term in one of the two polynomials P, Q is $= 1$ and the other $= m$; then the coefficients of P and Q if rational, must necessarily be integral, as one can show by the same considerations which your Eminence[11] used in the real number theory (Disq. Section I).

Here, "real number theory" means over $\mathbb{Z}$ rather than $\mathbb{Z}[i]$, and the reference to *Disquisitiones* is the first Gauss quote of this article. Thus Eisenstein is telling Gauss that

[10] Eisenstein used the term "rationalen ganzen Funktionen" ("rational entire functions").

[11] The German original says "Ew. Hochwohlgeboren," which translates literally as "your High Well Born." The word "Hochwohlgeboren" originally applied to lesser German nobility and gentry. This flowery language is reflected in the letter's salutation, "Sr. Hochwohlgeboren, dem Geheimrath pp. Prof. Dr. Gauss," which translates "To his Eminence, the Distinguished, and so on, Professor Doctor Gauss." The word "Geheimrath," now spelled "Geheimrat," originated as the German equivalent of a "Privy councillor" in the middle ages and was an honorific for distinguished professors in German universities in the 19th century.

Gauss's lemma applies to the Gaussian integers. Mind-blowing. Then Eisenstein proceeds to prove that W is irreducible using one of the standard proofs of the Eisenstein criterion.[12] In other words, Eisenstein's first proof of his criterion

- was over the Gaussian integers;
- applied to a polynomial associated with the division problem on the lemniscate; and
- appeared in a letter to Gauss.

When Eisenstein wrote up his results for publication, he realized that his criterion was much more general. The first part of his 1850 paper had the title *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt* (*On the irreducibility and some other properties of equations that depend on the division of the lemniscate*) [**10**, pp. 536–555]. This paper contains Eisenstein's version of the Eisenstein criterion:

> „If in a polynomial $F(x)$ of x of arbitrary degree the coefficient of the highest „term is $= 1$, and all following coefficients are integers (real or complex), in „which a certain (real resp. complex) prime number m appears, if further the last „coefficient is $= \varepsilon m$, where ε represents a number not divisible by m: then it is „impossible to bring $F(x)$ into the form
>
> $$(x^{\mu} + a_1 x^{\mu-1} + \ldots . + a_{\mu})(x^{\nu} + b_1 x^{\nu-1} + \ldots . + b_{\nu})$$
>
> „where μ and $\nu \geq 1$, $\mu + \nu =$ the degree of $F(x)$, and all a and b are (real resp. „complex) ***integers***; and the equation $F(x) = 0$ is accordingly irreducible."[13]

(This quote uses the same format that Eisenstein used in his paper.)

After giving the proof, Eisenstein applies his criterion to the equation $W = 0$ that arises from division of the lemniscate and also to our friend $x^{p-1} + \cdots + 1$. Eisenstein's proof that the latter is irreducible is essentially identical to the one sketched on the first page of this article.

Eisenstein's paper is the first appearance of this classic proof of the irreducibility of $x^{p-1} + \cdots + 1$. Eisenstein is clearly pleased to have found such a splendid argument:

> ... This thus gives, if you will, a new and most highly simple proof of the irreducibility of the equation $x^{p-1} + x^{p-2} + \ldots . + x + 1 = 0$; and in contrast with earlier ones **), this proof does not presuppose knowledge of the roots and the relations among them.
>
> **) Besides the proof of ***Gauss***, only that of ***Kronecker*** in volume 29 of this journal, page 280, is known to me.

We know about Gauss's proof, and Kronecker's proof [**18**, vol. I, pp. 1–4] from 1845 is simpler than Gauss's but still uses the explicit relations among the roots. But notice what the footnote does *not* mention: Schönemann's two proofs of the irreducibility of $x^{p-1} + \cdots + 1$ given in his papers of 1845 and 1846. Yet Eisenstein's paper appears in the same journal in 1850!

[12] There are two standard proofs of the Eisenstein criterion. One proof (due to Eisenstein) works by studying which coefficients of the factors are divisible by the prime. The other proof (due to Schönemann) was given earlier in this article and uses reduction modulo p together with unique factorization in $\mathbb{F}_p[x]$.

[13] The Eisenstein criterion is true over any unique factorization domain—see van der Waerden [**29**]—and hence applies over $\mathbb{Z}$ and $\mathbb{Z}[i]$.

SCHÖNEMANN COMPLAINS. Eisenstein's paper, with the offending footnote, appeared in volume 39 of Crelle's journal. In volume 40, Schönemann published a *Notiz* [**26**], which began by describing two theorems from Eisenstein's paper:

- The Eisenstein criterion for real primes (in $\mathbb{Z}$) and complex primes (in $\mathbb{Z}[i]$).
- The irreducibility of the cyclotomic polynomial $x^{p-1} + \cdots + 1$, proved using the Eisenstein criterion.

Then Schönemann goes on to say:

> ... Since ***Eisenstein*** expressly noted, that for the last theorem he only knew the proofs of ***Gauss*** and ***Kronecker***, I am led to recall that in §. 6 of my paper „Foundations of a general theory of higher congruences etc." in volume 31 of this journal, I proved the first theorem [the Eisentein criterion] for real primes and deduced the last [the irreducibility of $x^{p-1} + \cdots + 1$] from the first, and also the method used by ***Eisenstein*** is not significantly different from mine. For the last theorem, I in addition even gave an entirely different proof in §. 50 of the first part of the paper.

It seems clear that Eisenstein messed up by not citing Schönemann. However, there are some complications and confusions. First, Schönemann refers to §6 of his *Grundzüge* paper in volume 31 of Crelle's journal, yet his irreducibility criterion and its application to $x^{p-1} + \cdots + 1$ are in §61 of the second part of his paper, which appeared in volume 32. The "§. 6" in his *Notiz* should have been "§. 61." This explains part of the reason I had trouble finding Schönemann's criterion—I was looking in the wrong section!

But there was also confusion on Eisenstein's side as well. As already noted, Eisenstein's study of the division equations of the lemniscate was published in a two-part paper in Crelle's journal. The footnote quoted above appeared in the first part, in issue II of volume 39. The second part of the paper, *Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie* (*On some general properties of equations that depend on the division of the lemniscate, together with applications to number theory*) [**10**, pp. 555–619], appeared in issue III of the same volume. This paper included an *explicit reference* to Schönemann's first proof of the irreducibility of $x^{p-1} + \cdots + 1$ (the one from §50 of Schönemann's paper in volume 31). Yet somehow this proof was unknown to Eisenstein when he wrote the first part of his paper. One can speculate on why this happened, but we will never know for sure.

CONCLUSION. We are now at the end of the amazing story of how Schönemann and Eisenstein independently discovered their criteria. Since Schönemann discovered it first, the name "Schönemann-Eisenstein criterion" used by Dorwart is the most historically accurate. However, most people use Eisenstein's version, so the name "Eisenstein-Schönemann criterion" is also reasonable.

In the quote from Section VII of *Disquisitiones*, Gauss acknowledged two items of unfinished business: the extension from circular to transcendental functions such as Abel's lemniscatic function φ, and the study of higher congruences. Both led to major areas of modern mathematics (elliptic curves and complex multiplication in the first case, p-adic numbers and local methods in number theory in the second), and both led to the Schönemann-Eisenstein criterion. Schönemann followed higher congruences to Hensel's lemma to a question about irreducibility modulo p^2: his criterion appears in a completely natural way. Eisenstein followed Abel's work on the

lemniscate and considered the coefficients of the resulting division polynomials: his criterion appears in a completely natural way, completely different from the context considered by Schönemann. Yet both have their origin in the same paragraph in *Disquisitiones*. As I said, it is an amazing story.

ACKNOWLEDGMENTS. The English translations of the first two Gauss quotes are from the English version of [**13**]. For the third Gauss quote and the first two Schönemann quotes, I used [**11**]. I would also like to thank Annemarie and Günter Frei for help in understanding the salutation in Eisenstein's letter to Gauss. Thanks also to Michael Filaseta for his help in pointing me to the right place in Schönemann's papers and to David Leep for bringing Dorrie's book [**8**] to my attention. I am also grateful to the referees (for both *Normat* and the MONTHLY) for several useful suggestions.

I should also mention that the papers from Crelle's journal quoted in this article are available electronically through the Göttinger Digitalisierungzentrum at the web site `http://gdz.sub.uni-goettingen.de/dms/load/toc/?IDDOC=238618`.

REFERENCES

1. N. H. Abel, *Oeuvres complètes de Niels Henrik Abel*, vol. I, L. Sylow and S. Lie, eds., Grøndahl & Søn, Christiana, 1881.
2. *Allgemeine Deutsche Biographie*, Duncker & Humblot, Leipzig, 1875–1912; also available at `http://www.deutsche-biographie.de/~ndb/adb_index.html` and `http://de.wikisource.org/wiki/Allgemeine_Deutsche_Biographie`.
3. D. A. Cox, The arithmetic-geometric mean of Gauss, *Enseign. Math.* **30** (1984) 275–330; reprinted in *Pi: A Source Book*, L. Berggren, J. Borwein, and P. Borwein, eds., 3rd ed., Springer, New York, 2003, 481–536.
4. ———, *Primes of the Form* $x^2 + ny^2$, Wiley, Hoboken, NJ, 1989.
5. ———, *Galois Theory*, Wiley, Hoboken, NJ, 2004.
6. R. Dedekind, Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus, *J. Reine Angew. Math.* **54** (1857) 269–325; reprinted in *Gesammelte mathematische Werke*, vol. I, E. Noether and O. Ore, eds., Vieweg, Braunschweig, 1930, 40–67.
7. L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institute, Washington, DC, 1919–1923; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1969.
8. H. Dorrie, *Triumph der Mathematik: Hundert berühmte Probleme aus zwei Jahrtausenden mathematischer Kultur*, Fredrich Hirt, Breslau, 1933; English trans. of 5th ed. by D. Antin, *100 Great Problems of Elementary Mathematics: Their History and Solution*, Dover, Mineola, NY, 1965.
9. H. L. Dorwart, Irreducibility of polynomials, *Amer. Math. Monthly* **42** (1935) 369–381. `doi:10.2307/2301357`
10. F. G. Eisenstein, *Mathematische Werke*, vol. II; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1989.
11. G. Frei, The unpublished section eight: On the way to function fields over a finite field, in *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones arithmeticae*, C. Goldstein, N. Schappacher, and J. Schwermer, eds., Springer, Berlin, 2007, 159–198.
12. E. Galois, *Écrits et Mémoires Mathématiques D'Évariste Galois*, R. Bourgne and J.-P. Azra, eds., Gauthier-Villars, Paris, 1962.
13. C. F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801; reprinted in 1863 as vol. I of [**14**]; German trans. by H. Maser, *Untersuchungen über Höhere Arithmetik*, Springer, Berlin, 1889; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1965; English trans. by A. A. Clarke, Yale University Press, New Haven, 1966; reprinted by Springer, New York, 1986.
14. ———, *Werke*, König. Gesell. Wissen., Göttingen, 1863–1927; vols. I–IX available at `http://www.wilbourall.org` (search for "Carl").
15. ———, Mathematical Diary, Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliotek Göttingen, Cod. Ms. Gauß Math. 48 Cim. Ed. (Latin with German annotations); reproduced as Abrdruck des Tagebuchs (Notizenjournals), [**14**, vol. X.1, pp. 483–575]; French trans. by P. Eymard and J.-P. Lafon, Le journal mathématique de Gauss, *Rev. Hist. Sci. Appl.* **9** (1956) 21–51; English trans. by J. Gray, A commentary on Gauss's mathematical diary, 1796–1814, *Expo. Math.* **2** (1984) 97–130; German trans. by E. Schumann, with historical introduction by K.-R. Biermann, and annotations by H. Wußing and O. Neumann, *Mathematisches Tagebuch 1796–1814*, 4th ed., Ostwalds Klassiker der exakten Wissenschaften **256**, Akademische Verlagsgesellschaft Geest & Portig, Leipzig, 1985.

16. F. Gouvêa, *p-adic Numbers: An Introduction*, Springer, New York, 1993.
17. C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870; 2nd ed., 1957.
18. L. Kronecker, *Werke*, B. G. Teubner, Leipzig, 1895–1931; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1968.
19. F. Lemmermeyer, *Reciprocity Laws*, Springer, New York, 2000.
20. E. H. Moore, A doubly-infinite system of simple groups, in *Mathematical Papers Read at the International Mathematical Congress, 1893*, Cambridge University Press, Cambridge, 1896.
21. J. J. O'Connor and E. F. Robertson, Mactutor History of Mathematics archive, available at `http://www-history.mcs.st-andrews.ac.uk/history/index.html`.
22. V. Prasolov and Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, American Mathematical Society, Providence, RI, 1997.
23. M. Rosen, Abel's theorem on the lemniscate, *Amer. Math. Monthly* **88** (1981) 387–395. `doi:10.2307/2321821`
24. T. Schönemann, Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, *J. Reine Angew. Math.* **31** (1845) 269–325.
25. ———, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. Reine Angew. Math.* **32** (1846) 93–105.
26. ———, Notiz, *J. Reine Angew. Math.* **40** (1850) 188.
27. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331. `doi:10.1007/BF01405086`
28. J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.
29. B. L. van der Waerden, *Moderne algebra*, Springer, Berlin, 1930.
30. H. Weber, *Lehrbuch der Algebra*, 2nd ed., Vieweg, Braunschwieg, 1898–1908; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1961.

DAVID A. COX went to Rice University and received his Ph.D. from Princeton University in 1975. After teaching at Haverford and Rutgers, he has been at Amherst College since 1979, except for a sabbatical at Oklahoma State University. His current areas of research include toric varieties and the commutative algebra of curve parametrizations, though he also has interests in number theory and the history of mathematics. He is the author of texts on number theory, computational algebraic geometry, mirror symmetry, Galois theory, and most recently toric varieties.
Department of Mathematics, Amherst College, Amherst, MA 01002-5000
dac@math.amherst.edu

Mathematics Is . . .

"Mathematics is, of all the arts and sciences, the most austere and the most remote."

G. H. Hardy, *A Mathematician's Apology*,
Cambridge University Press, Cambridge, 1967, p. 143.

—Submitted by Carl C. Gaither, Killeen, TX

How Small Can a Polynomial Be Near Infinity?

Jennifer M. Johnson and János Kollár

Abstract. We give bounds for real polynomials in two variables near infinity and near a zero. The bounds depend only on the degree of the polynomial and are simple to state.

1. INTRODUCTION. This paper investigates two parallel questions about polynomials. First, we ask how small a polynomial can be near infinity, and secondly we consider how quickly a polynomial can vanish near one of its zeros.

If we think only of polynomials of a single variable these questions are easy to answer, but as soon as we have two or more variables they acquire a surprising depth. Starting in the familiar one-variable case we reformulate the definition of the degree n of a polynomial and the multiplicity d of a polynomial root at the origin with these two questions in mind.

Lemma 1. *The polynomial $f(x)$ has degree n if there are constants $C_1, C_2 > 0$ so that*

$$C_1|x|^n \le |f(x)| \le C_2|x|^n \quad \textit{whenever} \quad |x| \gg 1. \tag{1.1}$$

The polynomial $f(x)$ has a d-fold root at $x = 0$ if there are constants $C_1, C_2 > 0$ so that

$$C_1|x|^d \le |f(x)| \le C_2|x|^d \quad \textit{whenever} \quad |x| \ll 1. \tag{1.2}$$

Here the notation $|x| \gg 1$ means that $|x|$ is sufficiently large; similarly, $|x| \ll 1$ means that $|x|$ is sufficiently small.

Consider now

$$f(x, y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + \cdots = \sum_{i,j} a_{ij}x^i y^j,$$

a polynomial in two variables. The standard definitions of the degree and the multiplicity of a root generalize in the obvious way. The degree of f is simply the largest value of $i + j$ for which $x^i y^j$ appears in the sum with nonzero coefficient a_{ij}, and f has a zero of multiplicity d at the origin if d is the smallest value of $i + j$ for which $x^i y^j$ appears with nonzero coefficient.

We would like to understand what this says about the size of f near infinity and about the rate of vanishing of f at the origin. That is, we would like to generalize the inequalities in Lemma 1 to the two-variable case, but this turns out to be quite difficult.

First we observe that we easily get the desired upper bounds. Indeed,

$$\left|\sum_{i,j} a_{ij}x^i y^j\right| \le \sum_{i,j} |a_{ij}|\left(\sqrt{x^2 + y^2}\right)^{i+j}.$$

doi:10.4169/amer.math.monthly.118.01.022

Hence

$$|f(x,y)| \le \left(\sum_{i,j} |a_{ij}|\right)\left(\sqrt{x^2+y^2}\right)^n \quad \text{if} \quad x^2+y^2 \ge 1$$

and

$$|f(x,y)| \le \left(\sum_{i,j} |a_{ij}|\right)\left(\sqrt{x^2+y^2}\right)^d \quad \text{if} \quad x^2+y^2 \le 1.$$

That is, $|f(x,y)|$ will grow no faster than $\left(\sqrt{x^2+y^2}\right)^n$ near infinity if f has degree n and will die out near the origin at least as quickly as $\left(\sqrt{x^2+y^2}\right)^d$ if the lowest degree terms in $f(x,y)$ have degree d.

Next we look for a lower bound for $f(x,y)$ when (x,y) is near infinity or near the origin. A simple example shows that there can be no lower bound in general.

Example 2. If $f(x,y) = x^2 + y^3$ then f vanishes on the curve defined by $x = t^3$ and $y = -t^2$. Since this curve passes through the origin and it also gives a path to infinity, neither of the lower bounds we want for f can exist.

One can still ask what happens with polynomials that do not vanish on such a curve. To this end, we make the following restriction. From now on when we work near infinity we consider only polynomials f that are positive there (outside some compact set in the plane, say) and when we work near the origin we assume that f has an isolated local minimum of 0 there.

Our next example shows that even with such restrictions the most obvious generalization of Lemma 1 cannot hold. We see that we may get *different* upper and lower bounds.

Example 3. The degree-4 polynomial $f(x,y) = x^2 + y^4$ is positive except at $(0,0)$, where it has an isolated local minimum of 0; this zero has multiplicity $d = 2$, the degree of the lowest order term in f. To understand the bounds on f near the origin we can restrict to a small circle $x^2 + y^2 = \epsilon^2$ centered at the origin. Using the method of Lagrange multipliers we see that for ϵ sufficiently small (in this case, $< 1/\sqrt{2}$) there will be exactly four critical points $(\pm\epsilon, 0)$ and $(0, \pm\epsilon)$ on the circle, and so

$$\epsilon^4 = f(0, \pm\epsilon) \le f(x,y) \le f(\pm\epsilon, 0) = \epsilon^2$$

when $\sqrt{x^2+y^2} = \epsilon$. Since the same argument holds on any smaller circle, we have

$$\left(\sqrt{x^2+y^2}\right)^4 \le f(x,y) \le \left(\sqrt{x^2+y^2}\right)^2 \quad \text{whenever} \quad \sqrt{x^2+y^2} \ll 1.$$

Our analysis so far might lead to the following:

Naive Guess 4. *For a polynomial f in two variables with an isolated local minimum of 0 at $(0,0)$ there is a constant $C_1 > 0$ so that*

$$f(x,y) \ge C_1\left(\sqrt{x^2+y^2}\right)^{\deg f} \quad \textit{whenever} \quad \sqrt{x^2+y^2} \ll 1.$$

In the other direction, working near infinity with a polynomial f that is positive outside a compact set, we can again get different upper and lower bounds, and the lower bound can even be a constant. For example, $f(x, y) = 1 + x^2y^2$ satisfies an inequality of the form

$$1 = \left(\sqrt{x^2 + y^2}\right)^0 \leq f(x, y) \leq (1 + \epsilon)\left(\sqrt{x^2 + y^2}\right)^4$$

when $\sqrt{x^2 + y^2} \gg 1$. This observation might suggest the following:

Naive Guess 5. *For a polynomial f in two variables for which $f(x, y) > 0$ whenever $\sqrt{x^2 + y^2} \gg 1$ there is a constant $C_1 > 0$ so that*

$$f(x, y) \geq C_1 \quad \textit{whenever} \quad \sqrt{x^2 + y^2} \gg 1.$$

Two closely related examples show that these guesses are not true in general.

Example 6 (Counterexample to Naive Guess 5). The degree-4 polynomial

$$f(x, y) = (xy - 1)^2 + y^4$$

is everywhere positive. Approaching infinity along the hyperbolic path defined by $y = 1/x$ with $x \geq 1$ we see that

$$f\left(x, \frac{1}{x}\right) = \frac{1}{x^4} \to 0 \quad \text{as} \quad x \to \infty.$$

Note that $\sqrt{x^2 + x^{-2}} \sim |x|$ as $x \to \infty$, so on this particular hyperbolic path $f(x, y)$ vanishes at the same rate as $\left(\sqrt{x^2 + y^2}\right)^{-4}$.

We see that even a polynomial that is everywhere positive on the xy-plane can vanish at infinity and our naive conjecture about polynomial behavior is certainly false.

It is somewhat easier to work at the origin than at infinity and we will see that in fact understanding rates of vanishing at a zero is equivalent to understanding rates of vanishing at infinity. Therefore we now focus on understanding the vanishing behavior near a zero as precisely as possible in the following example.

Example 7 (Counterexample to Naive Guess 4). The degree-4 polynomial

$$f(x, y) = (y - x^2)^2 + y^4$$

has a zero of multiplicity 2 at $(0, 0)$. Note that on most paths through the origin, for example, on any straight line path through $(0, 0)$, the multiplicity of the root, which is certainly less than the degree of f, tells us the rate of vanishing. For example, substituting $y = mx$ gives a one-variable polynomial, and the bounds of Lemma 1 hold. Approaching $(0, 0)$ along the line $x = 0$ again gives order-2 vanishing.

However, restricting f to the parabola $y = x^2$ we see that f vanishes much more rapidly than indicated by the multiplicity 2 or even the degree 4 as we approach the origin:

$$f(x, x^2) = x^8 \quad \text{and} \quad \sqrt{x^2 + x^4} \sim |x| \quad \text{as} \quad x \to 0.$$

On this parabolic path f vanishes to order 8, twice the degree of f. So our naive guess about polynomial behaviour near a zero is also wrong.

To complete our analysis we need to be sure that there is no other path through the origin where f vanishes even more rapidly than it does on the parabola $y = x^2$. We could proceed as in Example 3 and try to calculate the extrema of f on an arbitrary small circle centered at the origin. However, it is equally good and computationally simpler to calculate the extrema on a small square S_ϵ centered at the origin with corners $(\pm\epsilon, \pm\epsilon)$.

Assume that $\epsilon < 1$ and let $||(x, y)||_{\sup} = \max\{|x|, |y|\}$ denote the sup norm. Our square S_ϵ is defined by $||(x, y)||_{\sup} = \epsilon$ and it contains the two points $(\pm\epsilon, \epsilon^2)$ where f takes the value ϵ^8.

At the four corners f takes the values $\epsilon^2 \pm 2\epsilon^3 + 2\epsilon^4$, much larger than ϵ^8 when ϵ is small. Thus the minimum of f on S_ϵ must occur at an interior critical point on one of the four edges. We easily check that the only critical points on the top and bottom edges occur at the center, and again these cannot be the minimum since $f(0, \pm\epsilon) = \epsilon^2 + \epsilon^4$ will be much larger than ϵ^8. Since f is an even function of x we are guaranteed that the minimum value can be found at a critical point on the right edge.

Calculating $\frac{\partial f}{\partial y}(\epsilon, y)$ and setting it to zero we find that the minimum of f on the square must occur at a point (ϵ, y_1) where

$$2y_1^3 + y_1 = \epsilon^2.$$

Immediately we see that the minimum value of f does not in fact occur on the parabola $y = x^2$, so we need to see how much smaller f can be. We have just enough information to get a lower bound for f on the square. Note that y_1 will lie between 0 and ϵ and write the minimum value of f on S_ϵ in terms of y_1:

$$f(\epsilon, y_1) = y_1^2 - 2y_1\epsilon^2 + \epsilon^4 + y_1^4 = 4y_1^6 + y_1^4.$$

Thus for $||(x, y)||_{\sup} = \epsilon$ we have

$$\frac{f(x, y)}{||(x, y)||_{\sup}^8} \geq \frac{4y_1^6 + y_1^4}{(2y_1^3 + y_1)^4} \to 1$$

as ϵ, and hence y_1, goes to zero. Given any $\delta > 0$ we can choose ϵ sufficiently small to ensure that

$$f(x, y) \geq (1 - \delta)||(x, y)||_{\sup}^8$$

on the square S_ϵ, and thus

$$f(x, y) \geq (1 - \delta)\|(x, y)\|_{\sup}^8 \quad \text{whenever} \quad \|(x, y)\|_{\sup} \ll 1.$$

2. FINDING A LOWER BOUND FOR A GENERAL POLYNOMIAL. In general, given any polynomial f with an isolated local minimum of 0 at $(0, 0)$, we expect that on most paths through the origin the vanishing will be no faster than suggested by the degree, but Example 7 shows that the order of vanishing on some special curves can be much larger. Moreover, Example 7 suggests a whole series of polynomials

$$f_q(x, y) = (y - x^q)^2 + y^{2q} \quad \text{for} \quad q = 2, 3, \ldots$$

where the order of vanishing is even more extreme compared to the degree. On the curve $(x, y) = (t, t^q)$ we see that $f_q(x, y) = t^{2q^2}$ and $||(t, t^q)||_{\sup} = |t|$ if $|t| < 1$. Thus

$$f_q(t, t^q) \leq C||(t, t^q)||_{\sup}^{2q^2} = C||(t, t^q)||_{\sup}^{\frac{1}{2}(\text{degree } f_q)^2}.$$

The general analysis given in the discussion of Example 7 extends to these polynomials as well to show that for any $\delta > 0$, if we choose $\epsilon > 0$ sufficiently small we can ensure that

$$f_q(x, y) = (y - x^q)^2 + y^{2q} \geq (1 - \delta)||(x, y)||_{\sup}^{\frac{1}{2}(\text{degree } f_q)^2}$$

for $||(x, y)||_{\sup} \ll 1$. This suggests the following:

Question 8. *Given a polynomial f with an isolated local minimum of* 0 *at* $(0, 0)$*, does there always exist a positive exponent $N = N(f)$ and a constant $C > 0$ so that*

$$f(x, y) \geq C||(x, y)||_{\sup}^N \quad \textit{whenever} \quad ||(x, y)||_{\sup} \ll 1?$$

Returning to the parallel issue of polynomial behavior near infinity, we expect that along most paths to infinity the polynomial f will grow at a rate determined by its degree. However, we saw in Example 6 that f can actually vanish rapidly on certain special paths to infinity. Again we can construct a whole series of similar examples of more and more extreme behavior. Consider

$$\tilde{f}_q(x, y) = (x^{q-1}y - 1)^2 + y^{2q} \quad \text{for} \quad q = 2, 3, \ldots$$

of degree $2q$ on the path defined by $x = t$ and $y = 1/t^{q-1}$ when $t \gg 1$; we see that

$$\tilde{f}_q\left(t, 1/t^{q-1}\right) = \frac{1}{t^{2q(q-1)}} = \frac{1}{\left\|\left(t, 1/t^{q-1}\right)\right\|_{\sup}^{2q(q-1)}}.$$

This suggests a parallel question about bounds on the rate of vanishing at infinity:

Question 9. *Given a polynomial f that is positive everywhere outside some compact set in the plane, does there always exist a positive exponent $M = M(f)$ and a constant $C > 0$ so that*

$$f(x, y) \geq \frac{C}{||(x, y)||_{\sup}^M} \quad \textit{whenever} \quad ||(x, y)||_{\sup} \gg 1?$$

If it turns out that there are always such exponents $N(f)$ and $M(f)$, we might naturally ask how these exponents depend on f. Is it enough simply to know the degree of f?

We will see that the answer to all these questions is yes and we will prove this using only elementary methods found in standard undergraduate mathematics courses. The precise statement is given in our two main theorems, which are equivalent:

Theorem 10 (Vanishing at a Zero). *If $f(x, y)$ is a polynomial of degree n in two variables with an isolated local minimum of* 0 *at* $(0, 0)$*, then there is a constant $C > 0$*

so that

$$f(x, y) \geq C||(x, y)||_{\sup}^{n(n-1)} \quad \textit{whenever} \quad ||(x, y)||_{\sup} \ll 1.$$

Theorem 11 (Vanishing at Infinity). *If $f(x, y)$ is a polynomial of degree n in two variables that is positive outside a compact set, then there is a constant $C > 0$ so that*

$$f(x, y) \geq \frac{C}{||(x, y)||_{\sup}^{n(n-2)}} \quad \textit{whenever} \quad ||(x, y)||_{\sup} \gg 1.$$

We will first prove Theorem 10 and then we will explain how it is equivalent to Theorem 11.

3. THE KEY LEMMA. In this section we state the key lemma that we will use to establish Theorem 10. First we rotate coordinates if necessary to ensure that both x^n and y^n appear in $f(x, y)$. The leading terms of $f(x, y)$ form a degree-n homogeneous polynomial which has n complex linear factors. These determine at most n real lines through the origin. We want to avoid the case where either of the coordinate axes is among these n lines, and all but finitely many rotations will achieve this.

As in Example 7 we will investigate the minimum value of f on a small square centered at the origin. The minimum occurs either at a corner (where the analysis is very easy) or it occurs at an interior critical point on one of the edges of the square.

It suffices to find a lower bound for f on the right edge of S_ϵ, for all sufficiently small ϵ. Then simply replacing x by $-x$ or replacing y by $\pm x$ will show that a similar bound holds along the other edges as well.

Thus most of our effort will go toward understanding the behavior of f at its critical points along a vertical line segment. Our rotation of coordinates having ensured that y^n occurs in $f(x, y)$, we know that for any fixed choice of x the derivative $\partial f/\partial y$ will have degree precisely $n - 1$ when viewed as a polynomial in y. We let $\beta_j(x)$ for j from 1 to $n - 1$ denote the critical points of f, or equivalently, the roots of $\partial f/\partial y$.

We cannot know in general what the roots β_j are. For different choices of f or x the $n - 1$ roots might be all real or all complex; all or none of them might fall on the edge of our small square.

One of the lessons of the study of polynomials, a central insight of Galois theory, is that we must deal with *all* the roots *simultaneously* to get general statements. It is counterproductive to focus too soon on the particular root we want. To work with all the roots simultaneously we need a well-chosen expression that depends on the roots *symmetrically*, that is, an expression where the order in which we list the roots β_j does not matter.

Given our ultimate goal of finding the minimum of f, the two most obvious symmetric expressions we might consider are the sum $\sum_{j=1}^{n-1} f(x, \beta_j)$ and the product $\prod_{j=1}^{n-1} f(x, \beta_j)$. For our purposes the product seems more promising because we are ultimately interested in a choice of β where $f(x, \beta)$ is small. A particularly small $f(x, \beta)$ will have little effect on the sum, but it will have a large effect on the product. The heart of the proof of Theorem 10 is to show that this product is a polynomial function of x.

Lemma 12 (Key Lemma). *Consider f and g, polynomials of degree n and m, respectively, in two variables x and y. Further, assume that y^n appears in f and y^m appears in g with nonzero coefficients. For any choice of x let $\beta_j(x)$ for j from 1 to m*

denote the roots of g viewed as a polynomial in y. Then

$$P(x) = \prod_{j=1}^{m} f(x, \beta_j(x))$$

is a polynomial in x of degree at most nm. Furthermore, $P(x)$ is not identically 0 if f and g have no common factors.

Note. In the statement of Lemma 12 we pretend that the equation $g(x, y) = 0$ implicitly defines m functions $\beta_1, \ldots, \beta_m$ of x. Choosing a particular value for x and solving $g(x, y) = 0$ always gives a list of m roots, but it will not give us an *ordered* list. For us this does not matter because $P(x)$ depends on the roots of g symmetrically. We get the same value for $P(x)$ no matter how we happen to list the m roots.

Later we will give three proofs of Lemma 12, after we use it to prove Theorem 10 and after we establish the equivalence between Theorems 10 and 11. The first proof of our key lemma is somewhat longer but quite elementary, using only basic facts about polynomials and determinants. Moreover it gives an explicit formula for computing $P(x)$ from the coefficients of f and g. The second proof is much shorter than the first and also algebraic; it relies on the theory of elementary symmetric functions. The third proof uses standard consequences of the Cauchy integral formula from complex analysis, including the fact that any analytic function on $\mathbb{C}$ that grows like a polynomial near infinity must actually be a polynomial.

4. VANISHING NEAR (0, 0)—THE PROOF OF THEOREM 10. Observe that it suffices to prove the theorem for f an irreducible polynomial. Otherwise, write f as a product $\Pi_{i=1}^{k} f_i(x, y)$ of irreducible polynomials, where f_i has degree n_i. Each f_i is nonzero in a punctured neighborhood of the origin, and therefore it cannot change sign on that neighborhood. Thus, we can assume that each irreducible factor is larger than or equal to zero near the origin.

Once we have proved the theorem for irreducible polynomials, we will have a lower bound for f where the exponent is $\sum_{i=1}^{k} n_i(n_i - 1)$. Since

$$n(n-1) = \sum_{i=1}^{k} n_i(n-1) \geq \sum_{i=1}^{k} n_i(n_i - 1),$$

we obtain the desired lower bound for f.

Now we assume that f is irreducible and we bound its minimum on the right edge of the small square S_ϵ defined by $\|(x, y)\|_{\sup} = \epsilon$. In Lemma 12 set $g = \partial f/\partial y$ (so $m = n - 1$) to conclude that $P(x)$ is a polynomial of degree at most $n(n-1)$ in x. Since $f(x, y)$ is irreducible, f itself is the only possible common factor of f and $g = \partial f/\partial y$. However, g has degree $n - 1$, so f cannot divide g. Therefore, $P(x)$ is not identically zero.

It follows that P has a zero of multiplicity $d \leq n(n-1)$ at $x = 0$, and thus by Lemma 1 we know that there is a constant $C_1 > 0$ so that

$$|P(x)| \geq C_1|x|^d \geq C_1|x|^{n(n-1)} \quad \text{whenever} \quad |x| \ll 1.$$

We choose ϵ sufficiently small to ensure that this inequality holds on the right edge of S_ϵ.

It is straightforward to find an upper bound for the critical points β_j when x is small, and hence for the individual factors $f(x, \beta_j(x))$ that appear in the product $P(x)$ as well. We need the following:

Lemma 13. *For $h(y) = y^m + c_1\, y^{m-1} + \cdots + c_{m-1}\, y + c_m$ and for γ any root of h we have*

$$|\gamma| \le \max\{1, \textstyle\sum_{j=1}^{m} |c_j|\}.$$

Proof. The proof is very simple. Any root γ satisfies

$$\gamma^m = -c_1\, \gamma^{m-1} - \cdots - c_{m-1}\, \gamma - c_m,$$

and so

$$|\gamma| \le |c_1| + \left|\frac{c_2}{\gamma}\right| + \cdots + \left|\frac{c_{m-1}}{\gamma^{m-2}}\right| + \left|\frac{c_m}{\gamma^{m-1}}\right|.$$

If $|\gamma| \ge 1$ then $|\gamma| \le \displaystyle\sum_{j=1}^{m} |c_j|$. ∎

As a consequence of Lemma 13 we have:

Corollary 14. *There are positive constants C_2 and M so that if $|x| \le 1$ and if $\beta(x)$ denotes any root of $g(x, y) = 0$, then*

$$|\beta(x)| \le C_2 \quad \textit{and} \quad |f(x, \beta(x))| \le M.$$

Proof. Our definition of g guarantees that we can write

$$g(x, y) = b_m(x) y^m + b_{m-1}(x) y^{m-1} + \cdots + b_1(x) y + b_0(x),$$

where $\deg b_{m-j}(x) \le j$ for every j. In particular, $b_m(x)$ is a constant.

Divide g by its leading coefficient b_m to get h as in Lemma 13. The coefficient c_j of y^{m-j} will be $b_{m-j}(x)/b_m$, a polynomial in x of degree at most j. We conclude that

$$|\beta(x)| \le \max\{1, \textstyle\sum_{j=1}^{m} |c_j(x)|\}$$

for any x. Let A_j denote the maximum absolute value of the coefficient $c_j = c_j(x)$ on the compact set defined by $|x| \le 1$. Then

$$|\beta(x)| \le \max\{1, \textstyle\sum_{j=1}^{m} A_j\} = C_2 \quad \text{whenever} \quad |x| \le 1.$$

Similarly, let M be the maximum of $|f|$ restricted to the compact set defined by $|x| \le 1$ and $|y| \le C_2$. ∎

Now we can finish the proof of Theorem 10, assuming Lemma 12. The minimum value of f on the right edge of S_ϵ occurs either at one of the corners or at an interior critical point $(\epsilon, \beta_1(\epsilon))$. Setting $y = \pm x$ gives the corner points and reduces f to a polynomial of degree n in x which vanishes with multiplicity $d \le n$ at 0. By Lemma 1

there is a positive constant C_3 so that

$$f(x, \pm x) \geq C_3|x|^d \geq C_3|x|^n \geq C_3|x|^{n(n-1)}$$

whenever $|x| \ll 1$.

Similarly, by Lemma 12 and Lemma 1, there is a positive constant C_1 so that

$$|P(x)| \geq C_1|x|^{n(n-1)} \quad \text{whenever} \quad |x| \ll 1.$$

Thus, by Corollary 14, for any critical point $\beta_1(x)$ we have

$$|f(x, \beta_1(x))| = \frac{|P(x)|}{|f(x, \beta_2(x)) \cdots f(x, \beta_{n-1}(x))|} \geq \frac{C_1|x|^{n(n-1)}}{M^{n-2}},$$

when $|x| \ll 1$.

If we assume that ϵ is sufficiently small (to ensure in addition that $f(x, y) > 0$ on S_ϵ) then on the right edge of our small square we will have

$$f(x, y) \geq C|x|^{n(n-1)} = C||(x, y)||_{\sup}^{n(n-1)},$$

where $C = \min\{C_3, C_1/M^{n-2}\}$. This completes the proof of Theorem 10.

5. VANISHING NEAR INFINITY—THE PROOF OF THEOREM 11. Suppose that $f(x, y) = \sum_{i+j \leq n} a_{ij} x^i y^j$ is a polynomial of degree n, positive outside a compact set in the plane as in Theorem 11. Having established Theorem 10, we now use it to show that the desired lower bound holds for f near infinity.

We define a new polynomial $g(u, v) = u^n f(1/u, v/u)$, and show that a lower bound for g on a narrow vertical strip centered on the v-axis will produce the desired lower bound for f when $|x|$ is large and $|x| \geq |y|$.

For any positive constant a, the transformation $x = 1/u$, $y = v/u$ maps the rectangle R_a^+ in the uv-plane defined by $0 < u \leq a$ and $-1 \leq v \leq 1$ to the region H_a^+ in the xy-plane defined by $x \geq 1/a$ and $-x \leq y \leq x$. Let R_a denote the rectangle where $-a \leq u \leq a$ and $-1 \leq v \leq 1$. Similarly, let H_a denote the region in the xy-plane obtained as the union of H_a^+ with its reflection across the y-axis H_a^-.

Since $f(x, y)$ is positive outside a compact set, it follows that n must be even and $f(x, y)$ must be positive whenever $|x|$ is sufficiently large. We conclude that $g(u, v) > 0$ whenever $0 < |u| \ll 1$. Of course, g may vanish along the line $u = 0$, but it cannot vanish there identically since the degree-n terms of f, being of the form $a_{ij}x^i y^j$ with $i + j = n$, will produce terms of the form $a_{ij}v^j$ in $g(u, v)$.

Thus, in any sufficiently narrow strip R_a where $0 < a \ll 1$, we see that $g(u, v) > 0$ except possibly at finitely many points of the form $(0, v_k)$ where g vanishes. Since g has an isolated local minimum of 0 at each $(0, v_k)$, it follows that $g(u, v - v_k)$ will satisfy the hypotheses of Theorem 10. Thus, there is a positive constant C_k so that

$$g(u, v - v_k) \geq C_k||(u, v - v_k)||_{\sup}^{n(n-1)} \geq C_k|u|^{n(n-1)}$$

holds in an open neighborhood N_k of $(0, v_k)$.

Note that g has a positive minimum value on the compact set obtained by deleting the finitely many N_k's from our narrow strip R_a. Taking $C > 0$ to be the minimum of the C_k's, we have

$$g(u, v) \geq C|u|^{n(n-1)}$$

on the entire strip R_a, provided a is sufficiently small. Translating back to the xy-plane we have the desired lower bound for f on H_a:

$$f(x, y) = x^n\, g(1/x, y/x) \geq x^n \cdot \frac{C}{|x|^{n(n-1)}} = \frac{C}{|x|^{n(n-2)}}.$$

To complete the proof of Theorem 11, we observe that interchanging x and y converts H_a to a similar region $\tilde{H}_a$ lying along the y-axis, and every point (x, y) with $\|(x, y)\|_{\sup} > 1/a$ lies in at least one of these two regions.

6. RESULTANTS AND THE SYLVESTER MATRIX. In our first, elementary, proof that the product $P(x)$ is a polynomial of degree at most nm we make heavy use of an old-fashioned tool from the study of polynomials of a single variable, namely the resultant, and the closely related notion of the discriminant. Regarded as fundamental notions in the nineteenth century, they had moved to the periphery by the mid-twentieth century; for example, resultants were removed from the fourth edition of van der Waerden's classic *Algebra* in 1959, and have not reappeared in subsequent editions. However, they are making a comeback in modern computational algebraic geometry, appearing as an important tool in recent books such as [**4**] and [**12**]. We review the basic definitions and facts below.

Definition 15. For $f(y) = a_n y^n + \cdots + a_1 y + a_0$ a polynomial of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ and for $g(y) = b_m y^m + \cdots + b_1 y + b_0$ a polynomial of degree m with roots $\beta_1, \ldots, \beta_m$ we form the *resultant* of f and g as follows:

$$R(f, g) = a_n^m \cdot b_m^n \cdot \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (\alpha_i - \beta_j).$$

We see that $R(f, g) = 0$ if and only if f and g have a common root. The special case $R(f, f')$ where $g = f'$ is the derivative polynomial of f is called the *discriminant* $D(f)$ and this will be zero if and only if f and f' have a common root, that is, if f has a root of multiplicity larger than 1.

The resultant $R(f, g)$ is a polynomial in the $n + m$ variables $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ of degree nm with leading coefficient $a_n^m \cdot b_m^n$. Thus it makes sense to write $R(\vec{\alpha}, \vec{\beta})$ instead of $R(f, g)$.

Lemma 16. *For polynomials f and g as in Definition 15, evaluate f at each of the roots of g and take the product:*

$$P(f, g) = \prod_{j=1}^{m} f(\beta_j).$$

Then

$$R(f, g) = (-1)^{nm} \cdot b_m^n \cdot P(f, g).$$

In the special case when g is the derivative of f,

$$D(f) = (na_n)^n \cdot P(f, f').$$

Proof. To prove Lemma 16 we simply write $f(y) = a_n \prod_{i=1}^{n}(y - \alpha_i)$ to get

$$P(f, g) = \prod_{j=1}^{m} a_n \prod_{i=1}^{n}(\beta_j - \alpha_i) = a_n^m (-1)^{nm} \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\alpha_i - \beta_j)$$

and compare to Definition 15. ∎

Historical Remark. Sylvester showed that the resultant of two polynomials can be calculated as the determinant of a matrix formed from their coefficients. In [**21**] he explained the process in detail, starting with how to write down $m + n$ rows of $m + n$ numbers from the coefficients of two polynomials, one of degree n and the other of degree m. Nowadays this array is called the Sylvester matrix of course. It is interesting to see that in 1840 he never used the word "determinant." Rather he described the calculation in terms of even and odd permutations. He went on to illustrate his method of computing resultants for two general quadratic polynomials by writing down all permutations on the set $\{1, 2, 3, 4\}$, sorted into twelve positive (even) ones and twelve negative ones, to calculate what we would call the determinant of his 4×4 array. The "derivatives" in the title of [**21**] refer to the resultant, not to any differentiation.

Definition 17 (The Sylvester Matrix). Let $\mathcal{P}_{n+m-1}$ denote the $(n + m)$-dimensional vector space of polynomials in the single variable y of degree at most $n + m - 1$. Let $\mathcal{B}_{n+m-1}$ denote the standard basis $\{y^{n+m-1}, \ldots, y^2, y, 1\}$. From the given polynomials f and g we form a collection $\mathcal{C}(f, g)$ of $n + m$ vectors in $\mathcal{P}_{n+m-1}$:

$$\mathcal{C}(f, g) = \{y^{m-1} f, y^{m-2} f, \ldots, yf, f, y^{n-1} g, y^{n-2} g, \ldots, yg, g\}.$$

For i from 1 to m the ith row of the Sylvester matrix $\mathcal{S}(f, g)$ is the coordinate vector of $y^{m-i} f$ taken with respect to the basis $\mathcal{B}_{n+m-1}$. For k from 1 to n the $(m + k)$th row of $\mathcal{S}(f, g)$ is the coordinate vector of $y^{n-k} g$ with respect to $\mathcal{B}_{n+m-1}$.

Example 18. For $m = 2$ and $n = 3$ let $f(y) = a_3 y^3 + a_2 y^2 + a_1 y + a_0$ and $g(y) = b_2 y^2 + b_1 y + b_0$. The first two rows are formed from yf and f. The last three rows are formed from $y^2 g$, yg, and g. Thus $\mathcal{S}(f, g)$ will be

$$\begin{bmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{bmatrix}.$$

Lemma 19 (Sylvester). *For polynomials f and g as in Definition 15 we have*

$$R(f, g) = \det \mathcal{S}(f, g).$$

We prove the lemma first for monic polynomials f and g. Since

$$\det \mathcal{S}(f, g) = a_n^m b_m^n \det \mathcal{S}\left(\frac{1}{a_n} f, \frac{1}{b_m} g\right),$$

and a similar statement clearly holds for $R(f, g)$ as well, the general case will immediately follow. We start with two straightforward observations.

Observation 20. *$R(f, g) = 0$ if and only if $\det \mathcal{S}(f, g) = 0$ if and only if f and g have a common factor.*

The vectors in $\mathcal{C}(f, g)$ will be linearly independent and hence a basis for $\mathcal{P}_{n+m-1}$ if and only if the determinant of the Sylvester matrix $\mathcal{S}(f, g)$ is nonzero. In that case, every polynomial in $\mathcal{P}_{n+m-1}$, in particular the polynomial 1, can be written as a linear combination of the vectors in $\mathcal{C}(f, g)$. Regrouping terms we see that there are polynomials u of degree at most $m - 1$ and v of degree at most $n - 1$ so that

$$f(y)u(y) + g(y)v(y) \equiv 1.$$

Consequently, $\det(\mathcal{S}(f, g)) \neq 0$ implies that f and g can have no common root.

Conversely, if $\det(\mathcal{S}(f, g)) = 0$ then there are nonzero polynomials u and v as above so that

$$f(y)u(y) + g(y)v(y) \equiv 0.$$

Thus the polynomial g divides the product of f and u but the degree of g is larger than the degree of u. We conclude that f and g have a common factor and hence a common root.

Observation 21. *For monic polynomials f and g, the determinant of $\mathcal{S}(f, g)$ is also a polynomial in the $n + m$ variables $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ and $R(f, g)$ divides this polynomial.*

The nonzero entries of the first m rows of $\mathcal{S}(f, g)$ are the coefficients of f, which can be expressed in terms of the roots of f as

$$a_{n-i} = (-1)^i \sigma_i(\alpha_1, \ldots, \alpha_n) \quad \text{for} \quad i = 1, \ldots, n.$$

Here, as usual, σ_i denotes the elementary symmetric function of degree i on $\alpha_1, \ldots, \alpha_n$. That is, $\sigma_0 = 1$ and, for $i > 0$, σ_i is the sum of all products of i elements chosen from the α's. For example,

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n, \\
\sigma_2 &= \alpha_1\alpha_2 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_2\alpha_n + \cdots + \alpha_{n-1}\alpha_n, \\
&\vdots \\
\sigma_n &= \alpha_1\alpha_2 \cdots \alpha_n.
\end{aligned}$$

Similarly, the nonzero entries of the last n rows of the Sylvester matrix are

$$b_{m-j} = (-1)^j \sigma_j(\beta_1, \ldots, \beta_m) \quad \text{for} \quad j = 1, \ldots, m.$$

Expanding the determinant thus gives a polynomial in the $n + m$ roots.

Since $\det \mathcal{S}(f, g) = \det \mathcal{S}(\vec{\alpha}, \vec{\beta})$ vanishes whenever f and g have a common root, that is whenever $\alpha_i = \beta_j$ for some i and j, it follows that $\alpha_i - \beta_j$ must divide $\det \mathcal{S}(\vec{\alpha}, \vec{\beta})$ for every i and j. Thus the resultant $R(\vec{\alpha}, \vec{\beta})$ divides $\det \mathcal{S}(\vec{\alpha}, \vec{\beta})$.

Claim 22. *The polynomial $\det \mathcal{S}(\vec{\alpha}, \vec{\beta})$ has degree nm and therefore*

$$\det \mathcal{S}(f, g) = C_{m,n} \cdot R(f, g),$$

where $C_{m,n}$ could in principle depend on the degrees m and n.

Proof. Since the first row of $\mathcal{S}(\vec{\alpha}, \vec{\beta})$ will be

$$\begin{bmatrix} \sigma_0(\vec{\alpha}) & -\sigma_1(\vec{\alpha}) & \sigma_2(\vec{\alpha}) & \cdots & (-1)^n\sigma_n(\vec{\alpha}) & 0 & \cdots & 0 & 0 \end{bmatrix},$$

we observe that the degree of a nonzero term in column j will be $j-1$. To get the next row of $\mathcal{S}$ we just shift the nonzero entries one column to the right and wrap the leftover zero around to the start of the row. Thus the degree of any nonzero entry in column j of row 2 will be $j-2$. We continue in this way, shifting the nonzero entries one column to the right as we move to the next row to construct the first m rows of the $\mathcal{S}$ where

$$\mathcal{S}_{ij} = 0 \quad \text{or} \quad \deg \mathcal{S}_{ij} = j - i.$$

The last n rows of $\mathcal{S}$ are obtained in a similar way from the polynomial g and its roots $\vec{\beta}$. For $m+1 \le i \le m+n$ we have

$$\mathcal{S}_{ij} = 0 \quad \text{or} \quad \deg \mathcal{S}_{ij} = j - (i-m).$$

Finally, the bound on the degree of $\det \mathcal{S}$ follows from Lemma 23 below. ∎

Lemma 23. *Let $S = (s_{ij})$ be an $(n+m) \times (n+m)$ matrix whose entries are polynomials. Assume that, in the first m rows, $s_{ij} = 0$ or $\deg s_{ij} \le j - i$, and in the last n rows, $s_{ij} = 0$ or $\deg s_{ij} \le j - (i-m)$. Then $\det S$ is a polynomial of degree $\le nm$.*

Proof. By definition we sum up all possible terms which are, up to sign, of the form $\prod_{i=1}^{n+m} s_{i,\gamma(i)}$, where γ is a permutation of $\{1, \ldots, n+m\}$. If $s_{i,\gamma(i)} = 0$ for some i then the product is zero and contributes nothing to the determinant. Otherwise we calculate that

$$\begin{aligned} \deg \prod_{i=1}^{n+m} s_{i,\gamma(i)} &= \sum_{i=1}^{m} \deg s_{i,\gamma(i)} + \sum_{i=m+1}^{m+n} \deg s_{i,\gamma(i)} \\ &\le \sum_{i=1}^{m} (\gamma(i) - i) + \sum_{i=m+1}^{m+n} (\gamma(i) - i + m) \\ &= \sum_{i=1}^{m+n} \gamma(i) - \sum_{i=1}^{m+n} i + \sum_{i=m+1}^{m+n} m = nm. \end{aligned}$$

Adding up all these terms gives a polynomial of degree $\le nm$. ∎

To complete the proof of Lemma 19 and show that the resultant is actually the same as the determinant of the Sylvester matrix it remains only to show that $C_{m,n} = 1$. It suffices to compute both R and $\det \mathcal{S}$ for one choice of the α's and β's.

Choose $f(y) = y^n$, so that $\alpha_i = 0$ for all i, and let $g(y) = (y+1)^m$, so that $\beta_j = -1$ for all j. Then every factor $\alpha_i - \beta_j$ is equal to 1. On the other hand, the Sylvester matrix in this case will be lower triangular, with 1's along the main diagonal. Thus for this particular choice of α's and β's we have

$$R(\vec{\alpha}, \vec{\beta}) = \det \mathcal{S}(\vec{\alpha}, \vec{\beta}) = 1,$$

and so $C_{m,n} = 1$.

First Proof of Lemma 12. With these preliminaries established we are now ready to prove our key lemma. We consider $f(x, y)$ and $g(x, y)$ as in Lemma 12 and, as before, view them as polynomials in y whose coefficients are in $\mathbb{R}[x]$, the ring of polynomials in x with real coefficients.

Lemma 12 follows from Lemmas 16, 19, and 23, but we need to think this through carefully.

First we note that the coefficient $a_{n-i}(x)$ of y^{n-i} in $f(x, y)$ will have degree at most i and, similarly, the coefficient $b_{m-j}(x)$ of y^{m-j} in $g(x, y)$ will have degree at most j. It follows that the Sylvester matrix $\mathcal{S}(f, g)$ will be of the type described in Lemma 23, and thus $\det \mathcal{S}(f, g)$ will be a polynomial in x of degree at most nm. We will write $\det \mathcal{S}(x)$ to emphasize this.

For any particular choice of $x = x_0$, both $f(x_0, y)$ and $g(x_0, y)$ are polynomials in y with real coefficients. We can apply Lemmas 16 and 19 to conclude that $(na_n)^n P(x_0) = \det \mathcal{S}(x_0)$. Since this holds for every choice of x_0, we conclude that $P(x)$ is also a polynomial of degree at most nm in x. Furthermore, $P(x)$ is identically zero if and only if $f(x_0, y)$ and $g(x_0, y)$ have a common root for every x_0. We need to show that unless $f(x, y)$ and $g(x, y)$ have a common factor, there must be at least one choice of x_0 where $f(x_0, y)$ and $g(x_0, y)$ have no common root.

View f and g as elements of $\mathbb{R}(x)[y]$, the ring of polynomials in y whose coefficients are rational functions of x. Since f and g have no common factor in $\mathbb{R}[x, y]$, polynomials in two variables with real coefficients, they can have no nontrivial common factor in $\mathbb{R}(x)[y]$ either (since clearing denominators in $\mathbb{R}(x)[y]$ brings us back to $\mathbb{R}[x][y] = \mathbb{R}[x, y]$).

Since $\mathbb{R}(x)[y]$ is a ring of polynomials in a single variable over a field, we can use the Euclidean algorithm there [**5**]. We know that f and g are relatively prime, so we can find $\tilde{u}$ and $\tilde{v}$ in $\mathbb{R}(x)[y]$ so that

$$f(x, y)\tilde{u}(x, y) + g(x, y)\tilde{v}(x, y) = 1.$$

Multiply through by a nonzero polynomial $w(x)$ in $\mathbb{R}[x]$ to clear denominators in $\tilde{u}$ and $\tilde{v}$ to obtain

$$f(x, y)u(x, y) + g(x, y)v(x, y) = w(x),$$

where now u and v are in $\mathbb{R}[x, y]$.

Choose x_0 so that $w(x_0) \neq 0$. It follows that $f(x_0, y)$ and $g(x_0, y)$ can never be zero for the same value of y. Therefore none of the factors $f(x_0, \beta(x_0))$ that appear in $P(x_0)$ can vanish. We conclude that $P(x_0) \neq 0$; hence $P(x)$ cannot be identically zero. ∎

7. TWO ALTERNATE PROOFS OF LEMMA 12. A key step of both our second and third proofs of Lemma 12 consists of showing that the product $P(x)$ grows no faster than a polynomial of degree nm near infinity. A small variation on the simple argument given in Lemma 13 produces the desired result.

Lemma 24. *Consider any polynomial*

$$h(y) = y^m + c_1(x)\, y^{m-1} + \cdots + c_{m-1}(x)\, y + c_m(x)$$

where the coefficient $c_j(x)$ has degree at most j in x. Let $\beta(x)$ denote any root of h. Then there is a positive constant C_1 such that for all x with $|x| > 1$,

$$|\beta(x)| \leq C_1\, |x|.$$

Proof. We can choose positive constants B_j for which $|c_j(x)| \le B_j|x|^j$ holds whenever $|x| > 1$. Fix x with $|x| = r > 1$ and consider

$$\frac{h(ry)}{r^m} = y^m + \frac{c_1(x)}{r}\, y^{m-1} + \cdots + \frac{c_{m-1}(x)}{r^{m-1}}\, y + \frac{c_m(x)}{r^m}.$$

Since $\beta(x)/r$ is a root of $h(ry)$, Lemma 13 gives

$$\left|\frac{\beta(x)}{r}\right| \le \max\left\{1, \sum_{j=1}^{m}\left|\frac{c_j(x)}{r^j}\right|\right\} \le \max\left\{1, \textstyle\sum_{j=1}^{m} B_j\right\}.$$

Take $C_1 = \max\{1, \sum_{j=1}^{m} B_j\}$ and we have $|\beta(x)| \le C_1 r$. ∎

This immediately gives us a bound on the growth of P.

Corollary 25. *There is a positive constant C_2 so that*

$$|P(x)| \le C_2|x|^{nm} \text{ whenever } |x| > 1.$$

Proof. Since $f(x, y) = \sum_{i+j\le n} a_{ij}x^i y^j$ and $|x| > 1$, Lemma 24 gives

$$\begin{aligned} |f(x, \beta(x))| &\le \sum_{i+j\le n} |a_{ij}||x|^i|\beta(x)|^j \\ &\le \sum_{i+j\le n} C_1^j|a_{ij}||x|^{i+j} \\ &\le \sum_{i+j\le n} C_1^j|a_{ij}||x|^n. \end{aligned}$$

Thus $f(x, \beta(x)) \le C_3|x|^n$ for a positive constant C_3 if $|x| > 1$, and

$$|P(x)| = \prod_{j=1}^{m}|f(x, \beta_j(x))| \le \prod_{j=1}^{m} C_3|x|^n = C_3^m|x|^{nm} = C_2|x|^{nm}.$$ ∎

Second Proof of Lemma 12. We recall the fundamental theorem of symmetric functions:

Theorem 26. *Let R be any commutative ring with identity and let P be any symmetric polynomial in the indeterminates $\gamma_1, \gamma_2, \ldots, \gamma_m$ with coefficients in R. Then P is a polynomial in the elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_m$ in the γ's with coefficients in R.*

This theorem is often proved as a straightforward application of basic Galois theory and such a proof can be found in [**5**]. A simpler, purely combinatorial proof is in [**18**, Sec. I.2].

In the expression $P(x) = \prod_{j=1}^{m} f(x, \beta_j)$ we view x and the β's as independent variables. Then $P(x)$ is a symmetric polynomial in the β's with coefficients in $R =$

$\mathbb{R}[x]$. The fundamental theorem then gives

$$\prod_{j=1}^{m} f(x, \beta_j) = \sum a_{i_1 i_2 \ldots i_m}(x)\, \sigma_1^{i_1}(\vec{\beta}) \sigma_2^{i_2}(\vec{\beta}) \cdots \sigma_m^{i_m}(\vec{\beta}),$$

where the coefficients $a_{i_1 i_2 \ldots i_m}(x)$ are in $\mathbb{R}[x]$.

That established, now we fix $x = x_0$ and set $\beta_j = \beta_j(x_0)$ to match the roots of the polynomial $g(x_0, y)$. With these substitutions, the left-hand side becomes $P(x_0)$ and the right-hand side becomes

$$\sum A_{i_1 i_2 \ldots i_m}(x_0) b_{m-1}(x_0)^{i_1} b_{m-2}(x_0)^{i_2} \cdots b_0(x_0)^{i_m},$$

where $A_{i_1 i_2 \ldots i_m}(x_0)$ differs from $a_{i_1 i_2 \ldots i_m}(x_0)$ by a multiplicative constant since

$$\sigma_j(\beta_1(x_0), \ldots, \beta_m(x_0)) = \frac{(-1)^j}{b_m} \cdot b_{m-j}(x_0).$$

Since $b_{m-j}(x)$ is a polynomial in x, we obtain that $P(x)$ is also.

Now we know that $P(x)$ is a polynomial in x, and Corollary 25 tells us that it grows at worst like $|x|^{nm}$ when x is large. In other words the degree of the polynomial $P(x)$ is at most nm.

Now refer to the end of the first proof of Lemma 12 to see that $P(x)$ cannot be identically zero if $f(x, y)$ and $g(x, y)$ have no common factor. ∎

Third Proof of Lemma 12 (Using Complex Analysis). A standard theorem in complex analysis tells us (as a consequence of the Cauchy integral formula) that an entire function that grows like a polynomial near infinity must actually be a polynomial. Thus, in view of Corollary 25 another way to prove Lemma 12 is to show that the function $P(x)$ is an everywhere defined, analytic function of the complex variable x.

To this end, we first introduce a new collection of symmetric functions and we use the Cauchy integral formula to prove that they are analytic.

Lemma 27. *For f and g as in Lemma 12 and for any positive integer k, the function*

$$\psi_k(x) = \sum_{j=1}^{m} f^k(x, \beta_j(x))$$

is an analytic function of x.

Note that $\psi_k(x)$ is well-defined because it depends on the roots $\beta_1(x), \ldots, \beta_m(x)$ symmetrically. Later we will state and sketch a proof of the Newton identities to show that the product $P(x)$ can be written as a polynomial in the functions $\psi_1(x), \ldots, \psi_m(x)$. It follows then that $P(x)$ is also an analytic function of x.

To see why Lemma 27 is true we recall briefly some elementary facts from complex analysis. Suppose that u and v are functions of a complex variable y, holomorphic on and inside the circle C_r defined by $|y| = r$. Note that y_0 is a pole of the function v'/v if and only if $v(y_0) = 0$. Moreover, all the poles of v'/v are simple and the residue of the pole at y_0 is the multiplicity $m(y_0)$ of y_0 as a zero of v. For any such y_0 and any positive integer k, we can similarly observe that the function $u^k \cdot v'/v$ is either analytic

at y_0 or it has a pole there whose residue is $m(y_0) \cdot u^k(y_0)$. Thus by the Cauchy integral formula we have

$$\frac{1}{2\pi i} \int_{C_r} u^k(y) \frac{v'(y)}{v(y)}\, dy = \sum_{\substack{y_0 \text{ a zero of} \\ v \text{ inside } C_r}} u^k(y_0) \cdot m(y_0).$$

Fix some $N > 0$. For any choice of x we take $u(y) = f(x, y)$ and $v(y) = g(x, y)$ and observe that our root estimates in Corollary 14 and Lemma 24 guarantee that, as long as $|x| < N$, we can enclose all m roots $\beta(x)$ of v in a sufficiently large circle C_r, with r depending only on N. We see that

$$\psi_k(x) = \sum_{j=1}^{m} f^k(x, \beta_j(x)) = \frac{1}{2\pi i} \int_{C_r} f^k(x, y) \frac{\partial g(x, y)/\partial y}{g(x, y)}\, dy.$$

The functions $\psi_k(x)$ are analytic since differentiating by an independent variable can be interchanged with integration; see [**19**, Example 4, pp. 131–132] for details.

The Newton Identities. Given any set $\Gamma_m = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$, the Newton identities relate the elementary symmetric functions $\sigma_1, \ldots, \sigma_m$ on Γ_m to another collection of m symmetric functions on Γ_m. These are called the symmetric power functions and are defined by

$$\psi_k(\gamma_1, \gamma_2, \ldots, \gamma_m) = \gamma_1^k + \gamma_2^k + \cdots + \gamma_m^k \quad \text{for} \quad k = 1, 2, \ldots.$$

Note that the analytic functions $\psi_k(x)$ in Lemma 27 are examples of symmetric power functions on $\Gamma_m(x) = \{f(x, \beta_1(x)), f(x, \beta_2(x)), \ldots, f(x, \beta_m(x))\}$.

The Newton identities say that on any Γ_k,

$$\begin{aligned}
\sigma_1 &= \psi_1, \\
2\sigma_2 &= \psi_1\sigma_1 - \psi_2, \\
3\sigma_3 &= \psi_1\sigma_2 - \psi_2\sigma_1 + \psi_3, \\
&\vdots \\
k\sigma_k &= \sum_{j=1}^{k} (-1)^{j-1} \psi_j \sigma_{k-j}.
\end{aligned}$$

(As before, we set $\sigma_0 = 1$.) By our earlier definition of the elementary symmetric functions, $\sigma_i(\Gamma_k)$ makes sense only when $k \geq i$. If $k < i$ it is convenient to define $\sigma_i(\Gamma_k)$ to be the zero function.

We do not give a complete proof, but the key step is to show that the kth Newton identity holds on Γ_k. In order to bring the elementary symmetric functions into the picture we construct a monic polynomial $h(t)$ by viewing Γ_k as a list of roots:

$$h(t) = \prod_{i=1}^{k} (t - \gamma_i) = t^k - \sigma_1(\Gamma_k) t^{k-1} + \cdots \pm \sigma_{k-1}(\Gamma_k)\, t \mp \sigma_k(\Gamma_k).$$

Evaluating h at any root γ_i we obtain

$$0 = h(\gamma_i) = \gamma_i^k - \sigma_1 \gamma_i^{k-1} + \cdots \pm \sigma_{k-1}\gamma_i \mp \sigma_k,$$

where all the σ's are evaluated on Γ_k. Adding these up for i from 1 to k gives the kth Newton identity in k variables:

$$0 = \psi_k - \sigma_1\psi_{k-1} + \cdots \pm \psi_1\sigma_{k-1} \mp k\sigma_k.$$

Once we know that an identity among symmetric functions holds in k variables, it immediately follows that it holds in fewer variables simply by setting the extra variables to zero. Moreover, it is easy to see that the kth Newton identity holds in more than k variables as well.

A different proof of the Newton identities can be found in [**20**].

To complete our third proof of Lemma 12, we observe that

$$P(x) = \prod_{j=1}^{m} f(x, \beta_j) = \sigma_m(f(x, \beta_1), \ldots, f(x, \beta_m))$$

and note that the Newton identities allow us to solve recursively for $P(x) = \sigma_m(x)$ as a polynomial (with rational coefficients) in the symmetric power functions $\psi_1(x)$, $\psi_2(x), \ldots, \psi_m(x)$. Since we already know that these functions are analytic by Lemma 27, we can conclude that $P(x)$ is analytic, hence entire. ∎

8. A SURVEY OF RELATED RESULTS. Theorems 10 and 11 are equivalent formulations of a special case of a series of results that estimate not just one polynomial but the maximum of a collection of polynomials or analytic functions on $\mathbb{R}^n$ or $\mathbb{C}^n$, or on various subsets of them. For a given f, the value of the optimal exponent is called the *Łojasiewicz exponent* of f.

The classical works in this area, [**13, 17, 1**], answer Questions 8 and 9 for a given collection of polynomials or analytic functions, but do not provide actual estimates.

Bounds depending on the degrees appeared in [**3, 15, 14, 10, 11, 16**]. Theorems 10 and 11 are closest to the results of Gwoździewic while the proof is nearer to [**16**].

The bounds on the order of vanishing given in Theorems 10 and 11 are not the best possible—for example our method guarantees only that a degree-4 polynomial cannot vanish more quickly than $||(x, y)||_{\sup}^{12}$. It can be shown that a degree-4 polynomial cannot vanish more quickly than $||(x, y))||_{\sup}^{8}$. For $n = 5$ the optimal power is 14, whereas Theorem 10 gives 20, and for $n = 6$ the optimal power is 20 and Theorem 10 gives 30; see [**23**]. These proofs are more difficult and require various techniques of algebraic geometry.

For larger values of $n = \deg f$ the optimal bounds are not known. There is a factor of 2 between the exponent $\frac{1}{2}n^2$ in the series of polynomials $(y - x^q)^2 + y^{2q}$ of degree $n = 2q$ inspired by Example 7 and the upper bound, with exponent roughly n^2, of Theorem 10. Both of these are improved in [**9**]. Asymptotically, for large values of n, their example gives $\frac{15}{28}n^2$ and their upper bound is $\frac{3}{4}n^2$.

Readers who know algebraic geometry will surely have recognized the theory of algebraic curves behind the proofs. In the proof of Theorem 10 we use the local intersection multiplicity of the curves $(f = 0)$ and $(\partial f/\partial y = 0)$ at the origin to bound the order of vanishing and then use Bézout's theorem to estimate the local intersection multiplicity. For more information behind these ideas see the introductory textbooks [**2, 6, 7, 8, 12**].

ACKNOWLEDGMENT. Partial financial support for JK was provided by the NSF under grant number DMS-0758275. This paper was written while the authors enjoyed the lively mathematical atmosphere at MSRI.

1. M. F. Atiyah, Resolution of singularities and division of distributions, *Comm. Pure Appl. Math.* **23** (1970) 145–150. doi:10.1002/cpa.3160230202
2. R. Bix, *Conics and Cubics. A Concrete Introduction to Algebraic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1998.
3. W. D. Brownawell, Local diophantine Nullstellen inequalities, *Jour. Amer. Math. Soc.* **1** (1988) 311–322.
4. D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics, vol. 185. Springer-Verlag, New York, 1998.
5. D. Dummit and R. Foote, *Abstract Algebra*, Prentice Hall, Englewood Cliffs, NJ, 1991.
6. G. Fischer, *Plane Algebraic Curves* (trans. from 1994 German original by L. Kay), Student Mathematical Library, vol. 15, American Mathematical Society, Providence, RI, 2001.
7. W. Fulton, *Algebraic Curves, An Introduction to Algebraic Geometry*, Mathematics Lecture Note Series, W. A. Benjamin, New York, 1969.
8. C. G. Gibson, *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction*, Cambridge University Press, Cambridge, 1998.
9. S. M. Gusein-Zade and N. N. Nekhoroshev, On singularities of type A_k on simple curves of fixed degree, *Funktsional. Anal. i Prilozhen.* **3** (2000) 69–70.
10. J. Gwoździewicz, Growth at infinity of a polynomial with a compact zero set, *Singularities Symposium—Łojasiewicz 70*, Banach Center, Warszawa, 1998.
11. ———, The Łojasiewicz exponent of an analytic function at an isolated zero, *Comment. Math. Helv.* **74** (1999) 364–375. doi:10.1007/s000140050094
12. B. Hassett, *Introduction to Algebraic Geometry*, Cambridge University Press, Cambridge, 2007.
13. L. Hörmander, On the division of distributions by polynomials, *Ark. Mat.* **3** (1958) 555–568. doi:10.1007/BF02589517
14. S. Ji, J. Kollár, and B. Shiffman, A global Łojasiewicz inequality for algebraic varieties, *Trans. Amer. Math. Soc.* **329** (1992) 813–818. doi:10.2307/2153965
15. J. Kollár, Sharp effective Nullstellensatz, *Jour. Amer. Math. Soc.* **1** (1988) 963–975. doi:10.2307/1990996
16. ———, An effective Łojasiewicz inequality for real polynomials, *Period. Math. Hungar.* **38** (1999) 213–221. doi:10.1023/A:1004806609074
17. S. Łojasiewicz, Sur le problème de la division, *Studia Math.* **18** (1959) 87–136.
18. I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford, 1979.
19. J. E. Marsden, *Basic Complex Analysis*, W. H. Freeman, San Francisco, 1973.
20. D. G. Mead, Newton's identities, *Amer. Math. Monthly* **99** (1992) 749–751. doi:10.2307/2324242
21. J. J. Sylvester, A method of determining by mere inspection the derivatives from two equations of any degree, *Philosophical Magazine* **XVI** (1840) 132–135; reprinted in J. J. Sylvester, *The Collected Mathematical Papers of James Joseph Sylvester*, Vol. I (1837–1853) Cambridge University Press, 1904, and Chelsea Publishing, New York, NY, 1973.
22. B. L. van der Waerden, *Algebra*, Vols. I–II (trans. from 5th and 7th German editions by F. Blum and J. R. Schulenberger), Springer-Verlag, New York, 1991.
23. H. Yoshihara, On plane rational curves, *Proc. Japan Acad. Ser. A Math. Sci.* **55** (1979) 152–155. doi:10.3792/pjaa.55.152

JENNIFER M. JOHNSON received her Ph.D. at Brandeis University in 1987. For 12 years she taught at the University of Utah and currently she is a Senior Lecturer at Princeton University. She is the author (with J. Carlson) of the book *Multivariable Mathematics with Maple*, Prentice-Hall, Inc., 1997.
Department of Mathematics, Fine Hall, Washington Road, Princeton University, Princeton NJ 08544-1000
jmjohnso@math.princeton.edu

JÁNOS KOLLÁR received his Ph.D. at Brandeis University in 1984. He was a Junior Fellow at Harvard University and then for 12 years he taught at the University of Utah. Currently he is the Donner Professor of Science at Princeton University. He is the author of about 100 research papers and 6 books on algebraic geometry.
Department of Mathematics, Fine Hall, Washington Road, Princeton University, Princeton NJ 08544-1000
kollar@math.princeton.edu

Arnol'd, the Jacobi Identity, and Orthocenters

Nikolai V. Ivanov

Abstract. The three altitudes of a plane triangle pass through a single point, called the orthocenter of the triangle. This property holds literally in Euclidean geometry, and, properly interpreted, also in hyperbolic and spherical geometries. Recently, V. I. Arnol'd offered a fresh look at this circle of ideas and connected it with the well-known Jacobi identity. The main goal of this article is to present an elementary version of Arnol'd's approach. In addition, several related ideas, including ones of M. Chasles, W. Fenchel and T. Jørgensen, and A. A. Kirillov, are discussed.

To the memory of Vladimir Igorevich Arnol'd

1. INTRODUCTION. The three altitudes of a Euclidean triangle are concurrent, i.e., pass through a single point, called the *orthocenter* of the triangle. This theorem was known to Euclid and did not escape the attention of Euler and Gauss. For Euler's proof of this theorem, see [**7**, Chapter 1, Section 7], and for Gauss's proof see [**4**, Exercise II.18], for example.

The corresponding theorem is not true in hyperbolic geometry, if interpreted in the most direct way. Sometimes no two altitudes of a hyperbolic triangle intersect. But if two altitudes do intersect at a point, then the third one also passes through this point, which is then called the *orthocenter* of the triangle. Moreover, if two altitudes are asymptotically parallel (i.e., have a common point at infinity), the third one is asymptotically parallel to both of them, and if two altitudes have a common perpendicular, the third altitude is also orthogonal to it. (Recall that any two lines in a hyperbolic plane either intersect, or are asymptotically parallel, or have a unique common perpendicular.) One may consider these three statements together as the theorem about the altitudes in hyperbolic geometry. A synthetic proof of this result is outlined in [**10**, Exercise 40.14].

In fact, one can make sense of the orthocenter even in the case when the altitudes do not intersect. In this case the orthocenter lies outside the hyperbolic plane, sometimes on the circle at infinity (when the altitudes are asymptotically parallel), but usually beyond it (see Remark 1 at the end of Section 6).

Recently, V. I. Arnol'd [**3**] offered a fresh look at this circle of issues. Namely, he showed that the Jacobi identity

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$$

lies at the heart of the theory of altitudes in hyperbolic geometry. In his approach, Arnol'd used the Jacobi identity for the Poisson bracket of quadratic forms on $\mathbf{R}^2$ endowed with its canonical symplectic structure. Unfortunately, the use of these advanced notions renders Arnol'd's approach nonelementary.

The main goal of this article is to present an elementary version of Arnol'd's ideas. We use the most simple form of the Jacobi identity, namely, the Jacobi identity for the commutator $[A, B] = AB - BA$ of 2-by-2 matrices. This allows us to improve upon

doi:10.4169/amer.math.monthly.118.01.041

Arnol'd's exposition in another respect: while Arnol'd needs to bring his quadratic forms to diagonal form in order to do his computations, we do not need to bring our matrices (which play a role similar to the role of quadratic forms in Arnol'd's approach) to any normal form. In addition, we prove a sufficient condition for the altitudes to intersect, and show that the altitudes sometimes do not intersect if this condition is violated (see Section 7). The latter results are merely stated by Arnol'd (probably, because they are comparatively simple). In Section 8 we prove the theorem about the altitudes in spherical geometry by using the Jacobi identity for the usual vector product in 3-space. Sections 9 and 10 are devoted to the Euclidean case. While the theorem is simpler in the Euclidean case, its connection with the Jacobi identity is not so direct as in the hyperbolic and spherical cases (see the discussion at the end of Section 10). Sections 11 and 12 are devoted to an alternative approach to the hyperbolic altitudes theorem, still based on the Jacobi identity. This approach, based on Fenchel's theory of lines [**9**], is less elementary, but is very elegant nonetheless. In Section 12 we compare this approach with the approach of Sections 2–6.

The reader familiar with Arnol'd's paper may notice that our approach bypasses a point made by Arnol'd, namely, that these geometric theorems are intimately connected to mathematical physics. Instead, in this note these theorems are related to a little piece of algebra (the algebra of 2-by-2 matrices). Here I would like to quote A. Weil (see [**19**, Preface]).

> We are dealing here with mathematics, not with theology. . . . I have tried to show that, from the point of view which I have adopted, one could give a coherent treatment, logically and aesthetically satisfying, of the topics I was dealing with.

The prerequisites for reading this article are rather modest. We expect that the reader has had no more than a fleeting encounter with hyperbolic geometry and the projective plane. Since the Poincaré unit disc model is the most ubiquitous version of hyperbolic geometry, we choose it as our starting point. We will review the basic facts about these topics along the way. On the algebraic side we expect that the reader is familiar with symmetric bilinear forms (pairings) and matrices. Only in the last two Sections, 11 and 12, will we assume more from the reader (namely, familiarity with the upper half-space model of hyperbolic 3-space).

Most of our arguments are carried out in the less well-known projective Klein model, and we explain its definition, basic properties, and relation to the Poincaré model in Section 2. In order to relate the Poincaré and Klein models we will use the basic properties of inversions, which can be found in [**7**, Chapter 6]. A crucial tool in our arguments will be the notion of polarity, discussed from the geometric and algebraic points of view in Sections 3 and 4 respectively.

We use polarity in a manner similar to that of Arnol'd. In fact, the use of polarity in order to prove the hyperbolic altitudes theorem goes back more than one hundred years. J. L. Coolidge (see [**5**, Theorem 2, p. 103]) included such a proof in his classical treatise [**5**]. Another classical proof based on polarity is presented by Coxeter [**6**, Section 11.6]. The approach of Coolidge is closer in spirit to that of Arnol'd and of the present paper, but neither he nor Coxeter relate the theorem to the Jacobi identity.

The heart of the paper is Section 6, where we use the Jacobi identity to prove the altitudes theorem in hyperbolic geometry, after an important preliminary observation is made in Section 5.

Sections 7–12 complement this result in several ways, as described above. These sections are independent from each other, with the exception of Section 12, which depends on Section 11.

2. PRELIMINARIES. The Poincaré unit disc model of (plane) hyperbolic geometry is the open unit disc $\mathbf{U} = \{(x, y) : x^2 + y^2 < 1\} \subset \mathbf{R}^2$. The points of the model are the points of this unit disc, and its lines are the intersections of the unit disc with the circles orthogonal (in the usual Euclidean sense) to its boundary (the unit circle), and the diameters of the disc without their endpoints. These diameters are usually regarded as the intersections of the unit disc with the circles of infinite radius (i.e., the Euclidean lines) orthogonal to the unit circle.

The angles between these hyperbolic lines are by definition equal to the angles between them in the Euclidean sense. One can define hyperbolic distances and areas, but we will be concerned only with angles, and, except in Section 7, with right angles. For this reason we do not discuss the metric aspects of the Poincaré model.

Now let us introduce the projective Klein model of hyperbolic geometry. We will use the upper hemisphere $S^2_+ = \{(x, y, z) : x^2 + y^2 + z^2 = 1, z > 0\} \subset \mathbf{R}^3$ as an intermediary to pass from the Poincaré model to the Klein one. Let V be the orthogonal projection of the upper hemisphere S^2_+ to the equatorial disc $\{(x, y, z) : x^2 + y^2 + z^2 < 1, z = 0\}$, which we will identify with $\mathbf{U}$. In other words, $V(x, y, z) = (x, y)$. Let S be the stereographic projection of the upper hemisphere S^2_+ to the equatorial disc from the south pole $s = (0, 0, -1)$. The map S is the restriction of the stereographic projection $\widehat{S} : S^2 \setminus \{s\} \to \mathbf{R}^2$. By definition, $\widehat{S}(p)$ is equal to the point of intersection of the line connecting s with p and the plane $\{(x, y, z) \in \mathbf{R}^3 : z = 0\}$, which we identify with $\mathbf{R}^2$.

Proposition. *$\widehat{S}$ preserves angles and takes circles on S^2 (which are the intersections of S^2 with Euclidean planes) to circles in the plane $\mathbf{R}^2$.*

Proof. A convenient way to prove this is to use the inversion I of $\mathbf{R}^3$ with respect to the sphere with center s and radius $\sqrt{2}$. Recall that for any point $p \in \mathbf{R}^3 \setminus \{s\}$, the image $I(p)$ is defined to be the point q on the ray from s through p such that the product of the distances from p and q to s is equal to $(\sqrt{2})^2$.

Let us prove first that I takes S^2 into $\mathbf{R}^2$. Since S^2 contains s, the inversion I takes $S^2 \setminus \{s\}$ into a plane P. Note that the distance from s to the points on the equator of S^2 (i.e., the intersection of S^2 with the plane $z = 0$) is equal to $\sqrt{2}$, and therefore these points are fixed by I. So P must contain the equator of S^2, and therefore it must be the plane $z = 0$.

Now it is easy to see that I restricted to $S^2 \setminus \{s\}$ is equal to the stereographic projection $\widehat{S}$. Let l be any line intersecting S^2 at s and some other point p. Let q be the point of intersection of l with $P = \mathbf{R}^2$. Since I preserves l (because l contains s) and takes S^2 to $\mathbf{R}^2$, we see that $I(p) = q$. Therefore, I restricted to S^2 is equal to the stereographic projection $\widehat{S}$.

Now we can deduce the properties of $\widehat{S}$ from the standard properties of I. Namely, it is well known that inversions take circles to circles (lines are considered as circles passing through infinity) and preserve angles. (In three dimensions one may establish the first fact by using the facts that circles are intersections of spheres and planes, and inversions take spheres and planes into spheres and planes.) ∎

Corollary. *The map S^{-1} takes lines in the Poincaré model into vertical (i.e., orthogonal to $\mathbf{R}^2$) semicircles.*

Proof. Note that $\widehat{S}$ fixes (pointwise) the equator $S^1 = \{(x, y, 0) : x^2 + y^2 = 1\}$ of S^2. By the proposition, $\widehat{S}$ takes arcs of circles orthogonal to S^1 and having endpoints on S^1 into arcs of circles on S^2 orthogonal to S^1 (and having endpoints on S^1). The corollary follows. ∎

Corollary. *The map $V \circ S^{-1}$ takes lines in the Poincaré model to chords of the unit circle.*

Proof. The vertical projections of vertical semicircles are chords. ∎

Now we can define the Klein model of hyperbolic geometry. It is the image of the Poincaré model under the map $V \circ S^{-1}$. So, the points of the Klein model are the points of the unit disc, as before, but the lines are the chords of the unit circle. The angle between two lines is defined as the angle between the corresponding lines (arcs of circles) in the Poincaré model. In contrast with the Poincaré model, this angle usually does not agree with the Euclidean angle between these lines. In the next section we will introduce the notion of polarity, which will allow us to recognize the orthogonality of lines in the Klein model, i.e., right angles.

Note that (since both V and $\widehat{S}^{-1}$ fix S^1), the line in the Klein model corresponding to a line in the Poincaré model is the chord with the same endpoints as the Poincaré line (an arc of a circle).

3. POLARITY FROM THE GEOMETRIC POINT OF VIEW. For every chord C of the unit circle S^1 we will define a point p outside of S^1, which we will call the point *(geometrically) polar* to C. If C is not a diameter of S^1, we define p as the point of intersection of the two lines tangent to S^1 at the endpoints of C.

In order to make this definition work for diameters also, we embed the Euclidean plane $\mathbf{R}^2$ in the projective plane $\mathbf{P}^2$ by adding points at infinity in the usual way. Namely, for every line k in $\mathbf{R}^2$ let us denote by $[k]$ the set of all lines parallel to k. For every such set $[k]$ we add to $\mathbf{R}^2$ a new point, which we may denote also by $[k]$. The result is the projective plane $\mathbf{P}^2$. The collection of added points $[k]$ forms a new line, called the line at infinity. We extend every line k by adding to it the point $[k]$ at infinity. Then any two parallel lines intersect at a well-defined point at infinity (and the line at infinity intersects any other line at a single point).

Since the lines tangent to S^1 at the endpoints of a diameter are parallel, they intersect at one point at infinity. In other words, the polar point p of a diameter d is a well-defined point of $\mathbf{P}^2$ and lies on the line at infinity. It is equal to $[k]$, where k is any line in $\mathbf{R}^2$ orthogonal (in the Euclidean sense) to d. Clearly, any point outside of the unit circle S^1 (including points at infinity) is polar to a unique chord of S^1.

Now we can give a criterion for two lines in the Klein model to be orthogonal (in the sense of the Klein model). For a line l in the Klein model we will denote by $\overline{l}$ the projective line extending l.

Theorem 1. *Two lines l and m in the Klein model are orthogonal if and only if $\overline{m}$ contains the point polar to l (or, equivalently, $\overline{l}$ contains the point polar to m).*

Proof. See Figure 1. Let p and q be the points polar to l and m, respectively. Let L and M be the Poincaré lines corresponding to l and m, respectively. So, L is the arc of a circle $\overline{L}$ having the same endpoints as l and orthogonal to S^1. It follows that the center of $\overline{L}$ is the polar point p. Similarly, M is an arc of a circle $\overline{M}$ with center q.

By definition, l is orthogonal to m in the sense of the Klein model if and only if L is orthogonal to M in the sense of the Poincaré model, i.e., in the usual Euclidean sense.

Let us consider the inversion I in the circle $\overline{L}$. It preserves all lines passing through p, in particular, the two such lines tangent to S^1. Since any inversion takes circles to circles, I takes S^1 into another circle tangent to these two lines. Since I fixes the circle $\overline{L}$ (pointwise), and, in particular, its intersection with S^1 (which consists of the two

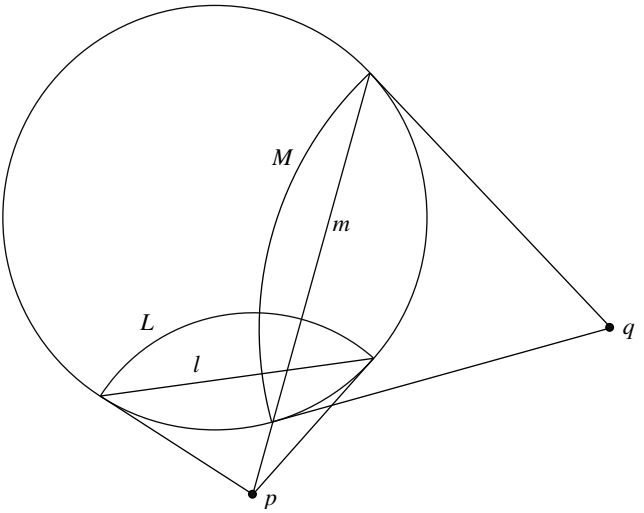

Figure 1.

endpoints of L), it follows that I takes S^1 to S^1 (but does not fix it pointwise). Also, I fixes the two points of intersection of $\overline{L}$ and $\overline{M}$.

Now, suppose that l is orthogonal to m in the sense of the Klein model. This means that L is orthogonal to M. Then $\overline{M}$ is orthogonal to $\overline{L}$ (at one point of intersection, and, therefore, at the other), and $I(\overline{M})$ is a circle orthogonal to $\overline{L}$ at these two points of intersection. It follows that I preserves $\overline{M}$.

Since the inversion I also preserves S^1, it interchanges the two points of intersection of $\overline{M}$ and S^1, i.e., the endpoints of m. This may happen only if $\overline{m}$ contains p, as claimed.

Conversely, suppose that $\overline{m}$ contains p. Then I interchanges the two intersection points of $\overline{m}$ and S^1. Since the circle $\overline{M}$ is orthogonal to S^1, it follows that its image is equal to $\overline{M}$ (there is only one circle orthogonal to S^1 at two given points). It follows that $\overline{M}$ is orthogonal to $\overline{L}$ (because at a point of intersection of $\overline{M}$ and $\overline{L}$ the inversion I reflects the tangent line to $\overline{M}$ with respect to the tangent line of $\overline{L}$).

If l is a diameter of S^1, the point p lies at infinity. In this case we should take as I the reflection in the line $\overline{L}$, and then the rest of the proof is similar. Also, if m is a diameter, then the circle $\overline{M}$ is actually a line (equal to $\overline{m}$). The reader can either consider these special cases separately, or just treat the lines as circles with center at infinity. ■

The above proof closely follows the proof of this theorem in [**18**, Section 4.8].

4. POLARITY FROM THE ALGEBRAIC POINT OF VIEW. Let us recall the standard description of the projective plane $\mathbf{P}^2$ in terms of homogeneous coordinates. Call two nonzero triples of real numbers (x, y, z) and (x', y', z') equivalent if $(x', y', z') = (\lambda x, \lambda y, \lambda z)$ for some nonzero real number λ. We will denote by $[x : y : z]$ the equivalence class of the triple (x, y, z). One may consider $\mathbf{P}^2$ to be the set of such equivalence classes. Indeed, if $z \neq 0$, then the equivalence class $[x : y : z]$ contains a unique representative of the form $(x, y, 1)$, and we identify it with the point $(x, y) \in \mathbf{R}^2$. The points of the form $[x : y : 0]$ form the line at infinity. Every line in $\mathbf{R}^2$ is given by an equation of the form $ax + by + c = 0$, where at least one of a and b is nonzero. In order to form the corresponding line in $\mathbf{P}^2$ we add to it the point $[b : -a : 0]$; the resulting line is given by the homogeneous equation

$ax + by + cz = 0$ (i.e., it consists of classes $[x : y : z]$ such that (x, y, z) satisfies this equation). The line at infinity is given by any equation of the form $cz = 0$ with $c \neq 0$. So, all homogeneous equations of the form $ax + by + cz = 0$, where at least one of a, b, and c is nonzero, define lines in $\mathbf{P}^2$, and every line has this form. The triple (a, b, c) is determined by the line up to multiplication by a nonzero $\lambda \in \mathbf{R}$.

Recall that a *pairing* on a real vector space V (over $\mathbf{R}$) is a *bilinear map* $V \times V \to \mathbf{R}$. The key role in the algebraic approach to polarity is played by the pairing on $\mathbf{R}^3$ defined by the formula

$$\langle (x, y, z), (x', y', z') \rangle = xx' + yy' - zz'.$$

This pairing is obviously *symmetric*, i.e., $\langle p, q \rangle = \langle q, p \rangle$ for all $p, q \in \mathbf{R}^3$. Let $Q(a) = \langle a, a \rangle$, where $a \in \mathbf{R}^3$. We call Q *the quadratic form associated to* the pairing $\langle \cdot , \cdot \rangle$.

In homogeneous coordinates the unit circle S^1 is given by the equation $x^2 + y^2 - z^2 = 0$. Indeed, this equation has no nonzero solutions with $z = 0$, so its set of solutions is actually contained in $\mathbf{R}^2$. Written as an equation for the points $[x : y : 1] \in \mathbf{R}^2$, it turns into the familiar equation $x^2 + y^2 - 1 = 0$ of the unit circle. In terms of the above quadratic form we can write this equation as $Q(x, y, z) = 0$.

In order to avoid cluttered notation, we will often abuse notation by not distinguishing between a point $p \in \mathbf{P}^2$ and its representatives in $\mathbf{R}^3$, i.e., between $[x : y : z]$ and (x, y, z). Since we will do this only when our equations are homogeneous, this can cause no harm.

Let us define the line *(algebraically) polar* to a point $a \in \mathbf{P}^2$ as the projective line defined by the homogeneous equation $\langle p, a \rangle = 0$ for the point $p \in \mathbf{P}^2$. We will denote this line by $a^\perp$. This is an example of abuse of notation alluded to in the previous paragraph; strictly speaking, we should write here representatives of a and p in $\mathbf{R}^3$ instead of a and p. Note that if $a^\perp = b^\perp$, then $a = b$. Indeed, if equations $\langle p, a \rangle = 0$ and $\langle p, b \rangle = 0$ have the same solutions p, then a and b are proportional as points of $\mathbf{R}^3$ and equal as points of $\mathbf{P}^2$ (this is another example of our abuse of notations).

Our next goal is to relate this notion of polarity to the one discussed in the previous section.

Lemma. *Suppose that $a \in S^1$, i.e., $Q(a) = 0$. Then $a^\perp$ is the tangent to S^1 at a. In particular, a is the only point of intersection of $a^\perp$ and S^1.*

Proof. Since $Q(a) = 0$, we have $\langle a, a \rangle = 0$, and therefore $a \in a^\perp$. Since $a \in S^1$, the point a is not contained in the line at infinity, and hence has the form $a = [u : v : 1]$ with $u^2 + v^2 = 1$. A point $[x : y : 1]$ is contained in $a^\perp$ if and only if $\langle (x, y, 1), (u, v, 1) \rangle = 0$, i.e., $xu + yv - 1 = 0$, or $xu + yv = 1$. But the last equation is exactly the equation of the Euclidean tangent to the unit circle S^1 at the point (u, v). In addition to such points $[x : y : 1]$ the line $a^\perp$ contains a point at infinity. ∎

Proposition. *Suppose a is a point in $\mathbf{P}^1$. Then a lies outside of the unit circle if and only if $a^\perp$ intersects the unit disc. If a is outside of the unit circle (so $a^\perp$ intersects the unit disc), then a is geometrically polar to the intersection of $a^\perp$ with the unit disc.*

Proof. Suppose first that a lies outside of the unit circle. Let t and t' be the two tangents to S^1 passing through the point a. Let b and b' be the corresponding points of tangency. By the lemma, t is algebraically polar to b and t' is algebraically polar to b'. Therefore, $\langle a, b \rangle = 0$ and $\langle a, b' \rangle = 0$. By the symmetry of the form $\langle \cdot , \cdot \rangle$, we have $\langle b, a \rangle = 0$ and

$\langle b', a\rangle = 0$. In other words, $b, b' \in a^\perp$. We see that $a^\perp$ is the line passing through the two points b and b', and hence the point a of intersection of the two tangents t and t' to S^1 at these points is geometrically polar to the intersection of $a^\perp$ with the unit disc.

Now, suppose a lies inside of the unit circle (i.e. in the unit disc). If $a^\perp$ intersects the unit disc, then we can consider the point p geometrically polar to the intersection of $a^\perp$ with the unit disc. The point p lies outside of the unit circle, and therefore p is geometrically polar to the intersection of $p^\perp$ with the unit disc by the previous paragraph. It follows that p is geometrically polar to the intersections of both $a^\perp$ and $p^\perp$ with the unit disc. Hence, these intersections are equal, and $a^\perp = p^\perp$. As we noticed above, this implies that $a = p$. This contradicts to the fact that a lies inside of the unit circle, and p lies outside. The contraction shows that if a lies inside of the unit circle, then $a^\perp$ does not intersect the unit disc. This completes the proof. ∎

Theorem 2. *Let l and m be two lines in the Klein model, and let a and b be the points geometrically polar to them. The following four conditions are equivalent:*

(i) *l is orthogonal to m;*
(ii) $\langle a, b\rangle = 0$;
(iii) $b^\perp \ni a$;
(iv) $a^\perp \ni b$.

Proof. By the proposition, l and m are the intersections of $a^\perp$ and $b^\perp$, respectively, with the unit disc. By Theorem 1, l is orthogonal to m if and only if $b^\perp$ contains a, i.e., if and only if $\langle a, b\rangle = 0$. Finally, $\langle a, b\rangle = 0$ is equivalent to $\langle b, a\rangle = 0$, and therefore to $a^\perp \ni b$. ∎

Note the usefulness of the symmetry of the form $\langle \cdot\,, \cdot\rangle$ in the above arguments.

For a more systematic treatment of polarity and its use in hyperbolic geometry, we recommend E. Rees's book [**16**].

5. THE KLEIN MODEL IN A VECTOR SPACE WITH A PAIRING. It is now clear that the notions of points and lines in the Klein model and of the orthogonality of such lines can be formulated entirely in terms of the pairing $\langle \cdot\,, \cdot\rangle$ and the associated quadratic form Q. Namely, the circle $Q(p) = 0$ in $\mathbf{P}^2$ divides $\mathbf{P}^2$ into two parts; one of them is the unit disc, and the other is a Möbius band. A point p is contained in the unit disc if and only if $Q(p) < 0$. The lines are the intersections of the projective lines with the disc part, and Theorem 2 allows us to define orthogonality in terms of the pairing $\langle \cdot\,, \cdot\rangle$.

Let V be some 3-dimensional vector space endowed with a pairing $D_V(\cdot\,, \cdot)$. Suppose that D_V is symmetric, i.e., $D_V(p, q) = D_V(q, p)$ for all p, q. As in the previous section, the quadratic form Q_V associated to the pairing D_V is defined by the formula $Q_V(a) = D_V(a, a)$. Let W be some other 3-dimensional vector space endowed with a symmetric pairing $D_W(\cdot\,, \cdot)$, and let Q_W be the associated quadratic form. We call a vector space isomorphism $f : V \to W$ an *isometry* between (V, D_V) and (W, D_W) if $D_W(f(p), f(q)) = D_V(p, q)$ for all $p, q \in V$. Usually the pairings are not mentioned explicitly and we speak just about an isometry $f : V \to W$.

Suppose that there is an isometry $f : \mathbf{R}^3 \to V$, where $\mathbf{R}^3$ is endowed with our pairing $\langle \cdot\,, \cdot\rangle$. In this case we can define a Klein model using V and $D_V(\cdot\,, \cdot)$ instead of $\mathbf{R}^3$ and $\langle \cdot\,, \cdot\rangle$. Namely, the role of the circle S^1 will be played by the *conic* given by the equation $Q_V(p) = 0$, the role of the unit disc will be played the interior of this conic given by the inequality $Q_V(p) < 0$, etc. Any theorem about lines and orthogonality

proved for this new model will automatically be true for the old one (one can use f to go from one model to the other). This trivial observation allows us to replace $\mathbf{R}^3$ by a vector space with a richer structure. This freedom of choosing V and D_V turns out to be a key tool in our proof of the theorem about the altitudes in hyperbolic geometry.

Lemma. *If an isomorphism of vector spaces $f : V \to W$ takes Q_V into Q_W, i.e., $Q_W(f(p)) = Q_V(p)$ for all $p \in V$, then f is an isometry.*

Proof. Let $D = D_V$. Recall the polarization identity

$$D(p, q) = \frac{1}{2}(D(p + q, p + q) - D(p, p) - D(q, q))$$

(to check this identity, expand $D(p + q, p + q)$ by bilinearity and use the symmetry $D(p, q) = D(q, p)$). We can rewrite it as follows:

$$D(p, q) = \frac{1}{2}(Q_V(p + q) - Q_V(p) - Q_V(q)). \tag{1}$$

Therefore, $D = D_V$ can be reconstructed from Q_V (and the vector space structure of V). Of course, the same applies to D_W and Q_W. It follows that if an isomorphism f takes Q_V into Q_W, then it is an isometry. ∎

Given any function Q_V on V that is a homogeneous polynomial of degree 2 when written in some (and therefore in any) coordinates on V, one can use formula (1) in order to define a symmetric pairing. Although we do not need this general fact for our proofs, knowing that this is true allows us to start the search for an appropriate pairing from a quadratic form.

6. ORTHOCENTERS IN THE KLEIN MODEL. The main theorem about the altitudes of triangles in the Klein model is the following.

Theorem 3. *The three altitudes of a triangle in the Klein model intersect in a point of the projective plane, which is called the* orthocenter *of the triangle.*

Notice that the orthocenter may lie outside of the Klein model itself (i.e., outside of the unit disc). But if two altitudes do intersect in a point in the Klein model, then the theorem implies that the third altitude also passes through this point, and in this case the orthocenter is a point of the Klein model. In a more classical spirit one may say that the triangle has an orthocenter in this case. In the next section we will discuss when this happens.

Using our freedom of choice of a 3-dimensional vector space V and a pairing on it, in the proof of the theorem we will use the space $sl(2)$ of real 2-by-2 matrices with trace 0. Every such matrix has the form

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix},$$

and we will use (x, y, z) as standard coordinates on $sl(2)$.

We will choose the pairing $D = D_V$ in such a way that the associated quadratic form is equal to $-\det$:

$$-\det \begin{pmatrix} x & y \\ z & -x \end{pmatrix} = -(-x^2 - yz) = x^2 + yz.$$

By the remark at the end of the previous section such a pairing must exist. Anyhow, we will give a simple and explicit formula for it in the next lemma. Note that $\operatorname{tr}(XY) = \operatorname{tr}(YX)$, and hence the bilinear form $\frac{1}{2}\operatorname{tr}(XY)$ is symmetric.

Lemma. *The quadratic form associated to* $D(X, Y) = \frac{1}{2}\operatorname{tr}(XY)$ *is equal to* $-\det$. *Here* tr *denotes the trace of a matrix.*

Proof. We need to check that

$$-\det(X) = \frac{1}{2}\operatorname{tr}(X^2)$$

for any matrix

$$X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}.$$

Clearly,

$$X^2 = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}\begin{pmatrix} x & y \\ z & -x \end{pmatrix} = \begin{pmatrix} x^2+yz & \cdot \\ \cdot & zy+x^2 \end{pmatrix},$$

where dots denote the terms we are not interested in. It follows that $\operatorname{tr}(X^2) = 2(y^2 + xz) = -2\det(X)$. ∎

Let $f : \mathbf{R}^3 \to sl(2)$ be the map

$$f(x, y, z) = \begin{pmatrix} x & y-z \\ y+z & -x \end{pmatrix}.$$

Clearly, f is a vector space isomorphism, and

$$-\det(f(x, y, z)) = x^2 + y^2 - z^2 = Q(x, y, z).$$

So, f takes the quadratic form Q associated to $\langle \cdot\,, \cdot \rangle$ into the quadratic form $-\det$ associated to $D(\cdot\,, \cdot)$. By the lemma from Section 5, f is an isometry. So by the discussion in Section 5, we can use $sl(2)$ and $D(\cdot\,, \cdot)$ instead of $\mathbf{R}^3$ and $\langle \cdot\,, \cdot \rangle$ in our proofs.

The minus sign in front of det, which may look strange at first sight, is needed for the existence of f taking Q to our quadratic form on $sl(2)$. This immediately follows from Silvester's law of inertia of quadratic forms. Of course, we need the existence of f only for our choice of sign.

The next lemma will allow us to relate commutators and polarity. As usual, for any 2-by-2 matrices A and B, we write $[A, B]$ to denote the commutator $AB - BA$ of A and B. Using the fact that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, we see that $\operatorname{tr}([A, B]) = \operatorname{tr}(AB - BA) = \operatorname{tr}(AB) - \operatorname{tr}(BA) = 0$, so $[A, B] \in sl(2)$.

Lemma about Traces. *For any* 2*-by-*2 *matrices* A *and* B, *we have* $\operatorname{tr}(A[A, B]) = 0$.

Proof. We will apply the basic property of the trace $\operatorname{tr}(XY) = \operatorname{tr}(YX)$ with $X = A$, $Y = AB$. Namely,

$$\begin{aligned} \operatorname{tr}(A[A, B]) &= \operatorname{tr}(AAB - ABA) = \operatorname{tr}(AAB) - \operatorname{tr}(ABA) \\ &= \operatorname{tr}(ABA) - \operatorname{tr}(ABA) = 0. \end{aligned}$$

This completes the proof. ∎

In order to use this lemma, we need to know when this trace is not equal to zero for trivial reasons, i.e., when $[A, B] \neq 0$. It turns out that this is essentially always the case.

Lemma. *If $A, B \in sl(2)$ and $[A, B] = 0$, then the matrices A and B are proportional.*

Proof. Let

$$A = \begin{pmatrix} X & Y \\ Z & -X \end{pmatrix}, B = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} Xx + Yz & Xy - Yx \\ Zx - Xz & Zy + Xx \end{pmatrix}, BA = \begin{pmatrix} xX + yZ & xY - yX \\ zX - xZ & zY + xX \end{pmatrix}.$$

Therefore, if $AB = BA$, then

$$\begin{aligned} Yz = yZ, \quad & 2Xy = 2Yx, \\ 2Zx = 2Xz, \quad & Zy = zY. \end{aligned}$$

So, in this case we have

$$Y/y = Z/z, \quad X/x = Y/y, \quad X/x = Z/z.$$

It follows that the matrices A and B are proportional. ∎

Following the conventions of Section 4, we will not distinguish between a nonzero matrix $X \in sl(2)$ and the point defined by X in the projective plane corresponding to $sl(2)$.

Corollary. *Suppose that A and B represent two different points of $\mathbf{P}^2$. Then $[A, B] \neq 0$ and the line $[A, B]^\perp$ passes through A and B.*

Proof. Since A and B represent different points, the matrices A and B are not proportional. Therefore, $[A, B] \neq 0$. By the definition of D and the lemma about traces, $D(A, [A, B]) = 0$. Similarly,

$$D(B, [A, B]) = -D(B, [B, A]) = 0.$$

The corollary follows. ∎

A useful special case of this situation occurs if the line $[A, B]^\perp$ intersects the unit disc. By the proposition from Section 4, in this case $[A, B]$ is the point outside the unit circle that is polar to the intersection of $[A, B]^\perp$ with the unit disc. In particular, this is true if either A or B is inside of the unit disc. Indeed, the line $[A, B]^\perp$ contains A and B by the corollary.

Now we can describe the altitudes in terms of commutators and polarity.

Main Lemma. *Let A, B, C be three points in $sl(2)$ representing three vertices of a triangle in the Klein model. Then $[C, [A, B]]$ is nonzero, and therefore defines a point in $\mathbf{P}^2$. The line polar to this point contains the point defined by C and the intersection of*

this line with the unit disc is orthogonal to the line in the Klein model passing through A and B. In other words, the line polar to $[C, [A, B]]$ *is the projective extension of the altitude of the triangle ABC passing through C and orthogonal to AB.*

Proof. First, let us show that $[C, [A, B]]$ is nonzero. Since A and B are inside of the unit disc, $[A, B]$ is a point outside the unit circle by the remarks following the last corollary. Since C is assumed to be inside of the unit disc, $C \neq [A, B]$, and $[C, [A, B]] \neq 0$ by the last corollary.

Let $\gamma = [C, [A, B]]$. By the last corollary, $C \in \gamma^{\perp}$, and, hence, C is contained in the line polar to γ. Also, by the last corollary, $[A, B] \in \gamma^{\perp}$. This means that $D([A, B], \gamma) = 0$, and (using the symmetry of our form again!) that $\gamma \in [A, B]^{\perp}$. Note that $[A, B]$ is a point outside of the unit circle (as we noted in the previous paragraph), and therefore $[A, B]$ is a point geometrically polar to the intersection of $[A, B]^{\perp}$ with the unit disc. Also, C is a point inside of the unit circle, and therefore γ is polar to the intersection of $\gamma^{\perp} = [C, [A, B]]^{\perp}$ with the unit disc (by remarks following the last corollary, with C and $[A, B]$ in the role of A and B, respectively).

Now we can apply Theorem 2 to $\gamma^{\perp}$ and $[A, B]^{\perp}$ (more precisely, their intersections with the unit disc) in the role of l and m and γ and $[A, B]$ in the role of a and b, respectively.

By Theorem 2 $\gamma \in [A, B]^{\perp}$ implies that the lines polar to γ and $[A, B]$ are orthogonal. Using the last corollary once more, we see that the line polar to $[A, B]$ passes through A and B.

Collecting all these facts together, we see that the line polar to γ contains C and is orthogonal to the line passing through A and B, as claimed. ∎

The next lemma provides us with a tool for establishing that three lines have a common point. It corresponds to a key theorem in Arnol'd's approach; see [**3**, Theorem 4].

Lemma about Common Points. *If three nonzero matrices* α, β, γ *satisfy the relation* $\alpha + \beta + \gamma = 0$*, then the three projective lines* $\alpha^{\perp}$, $\beta^{\perp}$, $\gamma^{\perp}$ *have a common point.*

Proof. The linear dependence among α, β, and γ implies that the equations $D(X, \alpha) = D(X, \beta) = D(X, \gamma) = 0$ have a nonzero solution X. Such a solution represents a common point of these lines. ∎

Now we are ready to prove Theorem 3 by using the Jacobi identity

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0.$$

This identity is well known and can be verified by simply substituting for all commutators their definition and canceling the terms pairwise.

Proof of Theorem 3. Let $\alpha = [A, [B, C]]$, $\beta = [B, [C, A]]$, $\gamma = [C, [A, B]]$. By the main lemma, the lines $\alpha^{\perp}$, $\beta^{\perp}$, $\gamma^{\perp}$ contain the three altitudes of the triangle ABC. By the Jacobi identity, $\alpha + \beta + \gamma = 0$. Now the lemma about common points implies that these three lines have a common point. ∎

Remark 1. There are three possibilities for the orthocenter of a triangle in the Klein model. First, the orthocenter may be contained in the Klein model itself. In this case we have the classical situation, namely, the three altitudes have a common point in the

hyperbolic plane. Second, the orthocenter may be contained in the unit circle (or in the conic given by $Q_V(p) = 0$ in general). In this case the three altitudes have a common point at infinity. In other words, the altitudes are asymptotically parallel. Third, the orthocenter may lie outside of the closed unit disc. In the last case, let us consider the line l polar to the orthocenter O. Since every altitude contains O, Theorem 2 implies that every altitude is orthogonal to l. Therefore, in this case the altitudes have a common perpendicular.

By summing up these observations, we see that the altitudes of a hyperbolic triangle either have a common point, or are asymptotically parallel, or have a common perpendicular.

Remark 2. The above arguments are largely independent of the assumption that the points A, B, and C are contained in the Klein model (based on $sl(2)$). This makes it possible to base a proof of a classical theorem of Chasles on these arguments. In order to state this theorem, we need a definition. Let us say that a point a is *polar to a line l* in the projective plane if l is polar to a in the sense of Section 4, i.e., if $l = a^{\perp}$. As we noted right after the definition of algebraically polar lines (see Section 4), a is uniquely defined by l.

Chasles's theorem. *Let A, B, and C be three different points in the projective plane, and let a, b, c be the points polar to the lines BC, CA, AB, respectively. Suppose that $a \neq A$, $b \neq B$, $c \neq C$. Then the three projective lines aA, bB, cC are (obviously well defined and) concurrent, i.e., have a common point.*

Proof. By the corollary, $[A, B]^{\perp}$ is the line AB, i.e., $[A, B]$ is polar to AB. This means that $c = [A, B]$. Similarly, $b = [C, A]$ and $a = [B, C]$. Using the corollary again, we see that $[c, C]^{\perp}$ is the line cC. This means that the line cC is polar to $[c, C] = [[A, B], C]$. Similarly, bB is polar to $[[C, A], B]$, and aA is polar to to $[[B, C], A]$. Now the lemma about common points implies, in view of the Jacobi identity, that the lines aA, bB, cC have a common point. ∎

In the context of the theorem about the altitudes the assumption $a \neq A$, $b \neq B$, $c \neq C$ holds automatically, because A, B, C are contained in the Klein model, and the points a, b, c polar to the sides of the triangle ABC are outside of the Klein model. In this case Theorem 1 implies that aA, bB, cC are the altitudes of the triangle ABC. By combining this fact with Chasles's theorem, we can deduce the theorem about the altitudes.

For a classical approach to Chasles's theorem, we recommend [**6**] or [**8**]; see [**6**, Theorem 3.22] and [**8**, Theorem 7.31].

7. WHEN DO ALTITUDES INTERSECT? In this section, we will give a partial answer to the question of when the altitudes of a hyperbolic triangle intersect (inside of the hyperbolic plane itself). Namely, we will prove the following.

Theorem 4. *If all angles in a hyperbolic triangle are $\leq 2\pi/3 = 120°$, then its altitudes have a common point. For every $\gamma > 2\pi/3$ there exists a triangle with an angle equal to γ, whose altitudes do not intersect and are not asymptotically parallel.*

We will deal with acute triangles first. To this end, we need the following simple lemma.

Lemma. *Consider a hyperbolic triangle ABC. If the altitude from A intersects the line BC outside of the segment BC, say, on the side of C, then the angle $\angle ACB$ is obtuse. If this altitude intersects the segment BC, then the angles $\angle ABC$ and $\angle ACB$ are acute.*

Proof. Let H be the point of intersection of the altitude from A with the line containing BC. See Figure 2. Suppose that H lies outside the segment BC on the side of C. If the angle $\angle ACB$ is not obtuse, then the sum of the angles of the triangle ACH is more than $\angle ACH + \angle AHC = \angle ACH + \pi/2 > \pi$, a contradiction. Therefore $\angle ACB$ is obtuse. The case when H lies in the segment BC is similar. ∎

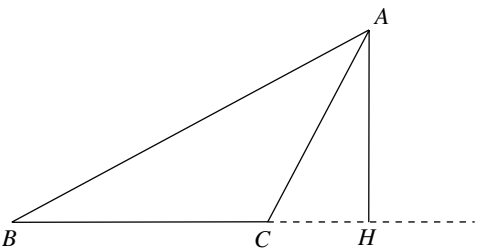

Figure 2.

Corollary. *The altitudes of an acute triangle have a common point inside of the triangle.*

Proof. The first part of the lemma implies that any two altitudes intersect inside of the triangle, exactly as in Euclidean geometry. It remains to apply Theorem 3. ∎

So, in order to prove the theorem, it remains to consider obtuse triangles.

Proof of Theorem 4 for obtuse triangles. We will use the Klein model from Section 2. We may assume that the angle $\angle BAC$ is obtuse. It follows from the last lemma that the altitudes from B and C intersect the lines AB and AC in some points of the rays starting at A and not containing C and B, respectively.

At this point, our main difficulty is that angles in the Klein model are, in general, different from Euclidean angles. We could switch to the Poincaré model, but then we would have to deal with arcs of circles instead of segments. Fortunately, we are interested in a single angle, namely $\angle BAC$. Using the correspondence between the Klein and Poincaré models from Section 2, we see that angles in the Klein model agree with Euclidean angles at the origin (since $V \circ S^{-1}$ takes diameters into themselves). We now invoke a basic property of the hyperbolic plane: for any two points there is a hyperbolic motion taking one point into the other. So, we can move our triangle ABC into such a position that A coincides with the origin, and therefore the hyperbolic angle $\angle BAC$ is equal to the Euclidean angle.

In this case the sides AB and AC are contained in diameters of the unit circle. The point polar to a diameter lies at infinity. Any projective line passing through this point is parallel (in the Euclidean sense) to the tangents to the circle at the endpoints of the diameter, and, therefore, is orthogonal to the diameter. Hence, Theorem 1 implies that hyperbolic orthogonality of a line to the line AB or the line AC is the same as Euclidean orthogonality. In other words, the hyperbolic altitudes of the triangle ABC from B and C are the same as the Euclidean altitudes. We would like to know when these two altitudes intersect inside of the unit disc.

Now, if for a triangle ABC as above (with the vertex A situated at the origin) these two altitudes intersect inside of the unit disc, then for any triangle $AB'C'$ such that B' and C' are contained in the sides AB and AC, respectively, the altitudes from B' and C' also intersect inside of unit disc. See Figure 3. This suggests moving the vertices B and C as far as possible along two rays starting at A and looking at what happens. So, we will move them to infinity and consider an ideal triangle ABC with A at the origin and B and C lying on the unit circle. Clearly, if for such an ideal triangle the altitudes from B and C intersect inside of the unit circle, then for any triangle $AB'C'$ with B' and C' contained in the rays AB and AC, respectively, the altitudes from B' and C' also intersect inside of the unit circle. Moreover, if the altitudes from B and C intersect on the unit circle, then altitudes from B' and C' still intersect inside of the unit circle, if at least one of the points B' and C' is inside of the unit circle. On the contrary, if the altitudes from B and C intersect outside of the unit circle, then for some points B' and C' on the rays AB and AC which are sufficiently close in the Euclidean sense to B and C respectively, the altitudes from B' and C' also intersect outside of the unit circle.

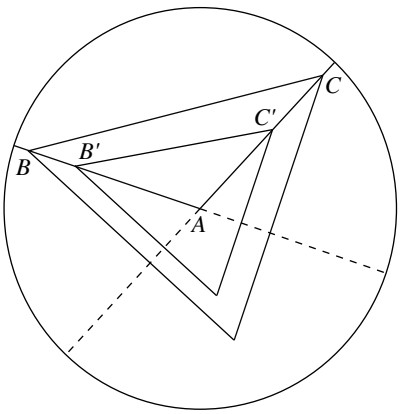

Figure 3.

Therefore, it is sufficient to prove that for ideal triangles ABC as above the point of intersection of the altitudes from B and C is contained in the (closed) unit disc if the angle $\angle BAC$ is $\leq 2\pi/3$, and is outside of it if this angle is $> 2\pi/3$.

So, let us consider such an ideal triangle ABC. See Figure 4. The whole configuration is symmetric with respect to the line bisecting the angle $\angle BAC$. Let XY be the intersection of this line with the (closed) unit disc; we may assume that the ray AY is directed inside the triangle BAC. Let O be the intersection of the altitudes from B and C. By symmetry, O is contained in the bisecting line, and, in addition, O and X are on the same side of A (since the angle $\angle BAC$ is obtuse). By definition, CO is orthogonal to AB; let D be the point of intersection of these two lines. Let α be the angle $\angle CAY$, equal to the angle $\angle YAB$. Clearly, the angle $\angle DAO$ is equal to the angle $\angle YAB$, which is equal to α by symmetry. Let β be the Euclidean angle $\angle DOA$.

Suppose that O is contained inside of the unit circle or on the unit circle itself. Then $\beta \geq \angle CXY$, and $\angle CXY$ is equal to half the angle $\angle CAY$. It follows that $\beta \geq \alpha/2$. Now, consider the right Euclidean triangle ODA. We see that $\beta + \alpha = \pi/2$. Together with the inequality $\beta \leq \alpha/2$ this implies $\alpha/2 + \alpha \leq \pi/2$, so $3\alpha \leq \pi$ and $2\alpha \leq 2\pi/3$. It remains to notice that $\angle BAC = 2\alpha$.

Suppose now that the orthocenter is outside the unit circle. In this case $\beta < \angle CXY$, and, arguing as in the previous paragraph, we conclude that $\angle BAC = 2\alpha > 2\pi/3$. ■

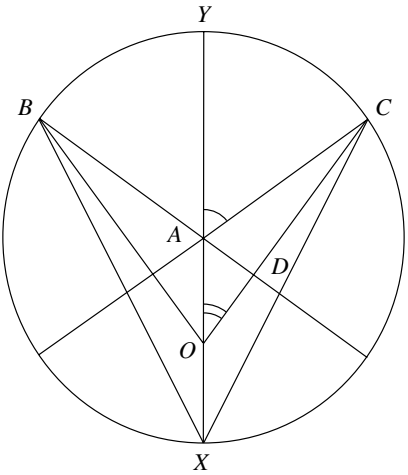

Figure 4.

8. ORTHOCENTERS IN SPHERICAL GEOMETRY. In order to relate the theorem about the altitudes in spherical geometry with the Jacobi identity, we will use the usual vector product of vectors in $\mathbf{R}^3$. The Jacobi identity for the vector product has the well-known form

$$(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0.$$

Let S^2 be the unit sphere in $\mathbf{R}^3$. The points in spherical geometry are the points of S^2, i.e., the unit vectors in $\mathbf{R}^3$. The lines in spherical geometry are the intersections of planes (here we use the term *planes* in the sense of linear algebra, i.e., planes are 2-dimensional vector subspaces of $\mathbf{R}^3$) with S^2, and the angle between two spherical lines is equal to the angle between the corresponding planes, which is, in turn, equal to the angle between the lines orthogonal to these planes.

Let abc be a spherical triangle. As usual, the vertices a, b, c are assumed to be distinct. In addition, we will assume that these vertices are different from the points $-a$, $-b$, $-c$. In this case the sides ab, bc, and ca are well defined. Notice that in this case the vector products $a \times b$, $b \times c$, and $c \times a$ are nonzero.

If c is orthogonal to the plane spanned by a and b, then every spherical line passing through c is orthogonal to ab. Otherwise, only one spherical line passing through c is orthogonal to ab. So, we will assume that none of the vectors a, b, c is orthogonal to the plane spanned by the other two. In this case the three altitudes of abc are well defined, and the vector products $(a \times b) \times c$, $(b \times c) \times a$, and $(c \times a) \times b$ are nonzero.

By definition, the vector product $a \times b$ is orthogonal to the plane (i.e., vector subspace) P spanned by a and b. The vector product $(a \times b) \times c$ is orthogonal to $a \times b$, and therefore is contained in P. Now, consider the plane γ orthogonal to $(a \times b) \times c$. Since $(a \times b) \times c$ is contained in P, the plane γ is orthogonal to P.

It follows that the intersection of γ with the unit sphere is the spherical line passing through c and orthogonal to the spherical line ab (which is equal to the intersection of P with S^2). In other words, this intersection is the altitude from c of the spherical triangle abc. Similarly, the intersections of the planes α and β orthogonal to $(b \times c) \times a$ and $(c \times a) \times b$ respectively are the altitudes from a and b.

Since the vectors $(a \times b) \times c$, $(b \times c) \times a$, $(c \times a) \times b$ are linearly dependent by the Jacobi identity, either the intersection of the three planes γ, α, β is a line, or

these three planes coincide. In the first case all three altitudes of the triangle abc pass through the two points in S^2 corresponding to the intersection line. (The altitudes have two common points, since two different lines in spherical geometry always intersect at two points.) In the second case all three vertices a, b, c are contained in the plane $\alpha = \beta = \gamma$. Clearly, in this case the altitudes intersect in two unit vectors orthogonal to this plane.

The argument in the previous paragraph is similar to the use of the lemma about common points in Section 6.

This completes our discussion of the altitudes in spherical geometry. Further applications of the Jacobi identity to spherical geometry in the spirit of Arnol'd's ideas are discussed in [**17**].

9. ORTHOCENTERS IN EUCLIDEAN GEOMETRY: KIRILLOV'S PROOF. In this section we present the proof of the Euclidean altitudes theorem outlined by A. A. Kirillov in [**12**, Appendix III, §1, Exercise 1]. This proof is very close in spirit and in outline to our proofs of the altitudes theorems in hyperbolic and spherical geometry.

We will denote by (u, v) the usual scalar product of two vectors u and v in $\mathbf{R}^3$.

Let $P \subset \mathbf{R}^3$ be the plane consisting of all points $(1, x_1, x_2)$, where $x_1, x_2 \in \mathbf{R}$. Our triangles will be contained in P, but the ambient space $\mathbf{R}^3$ will play a crucial role in the proof.

Let $e_0 = (1, 0, 0)$. If a vector $u \in \mathbf{R}^3$ is not proportional to e_0, then the intersection of the plane orthogonal to u with P is a line in P, which we will denote by $u^\perp$.

For a vector u, let $\overline{u} = (u, e_0)\, e_0$, and $\widetilde{u} = u - \overline{u}$. If $u = (u_0, u_1, u_2)$, then $\overline{u} = (u_0, 0, 0)$ and $\widetilde{u} = (0, u_1, u_2)$.

Proposition.

(i) *If $u = (u_0, u_1, u_2)$, then the line $u^\perp$ is given by the equation $u_0 + u_1 x_1 + u_2 x_2 = 0$.*

(ii) *If a and b are two different points in P, then the line $(a \times b)^\perp$ contains a and b.*

(iii) *Two lines $u^\perp$ and $v^\perp$ are orthogonal if and only if the vectors $\widetilde{u}$ and $\widetilde{v}$ are orthogonal.*

(iv) *If $a \in P$, and $u^\perp$ is a line in P, then the line $(a \times \widetilde{u})^\perp$ contains a and is orthogonal to $u^\perp$.*

Proof. (i) is clear. (ii) follows from the fact that the vectors a and b are orthogonal to $a \times b$. (iii) follows from (i) and the fact that $\widetilde{u} = (0, u_1, u_2)$, if $u = (u_0, u_1, u_2)$.

Let us prove (iv). Since a is orthogonal to $(a \times \widetilde{u})$, it is contained in $(a \times \widetilde{u})^\perp$. By (iii), $(a \times \widetilde{u})^\perp$ is orthogonal to $u^\perp$ if and only if $(a \times \widetilde{u}) - \overline{(a \times \widetilde{u})}$ is orthogonal to $\widetilde{u}$. It remains to notice that both vectors $(a \times \widetilde{u})$ and $\overline{(a \times \widetilde{u})}$ are orthogonal to $\widetilde{u}$: the first one by the main property of the vector product (which we have already used many times), and the second one because $\overline{v}$ is orthogonal to $\widetilde{w}$ for any two vectors v and w. This completes the proof. ∎

Lemma about Common Points. *Suppose that none of the three vectors u, v, w is proportional to e_0. If $u + v + w = 0$, then the lines $u^\perp$, $v^\perp$, $w^\perp$ either have a common point or are parallel.*

Proof. Since the vectors u, v, w are linearly dependent, the planes orthogonal to them are either equal or intersect along a line l. If these planes are equal, then our lines

are also equal (and so are parallel). If l intersects P, then the intersection point is a common point of the lines $u^\perp$, $v^\perp$, $w^\perp$. If l is parallel to P, then these lines are parallel (by elementary geometry). ■

Let x, y, z be the vertices of a triangle in P. By statement (ii) of the last proposition, the line $(y \times z)^\perp$ passes through vertices y and z. By statement (iv), the line $(x \times \widetilde{(y \times z)})^\perp$ contains x and is orthogonal to the line through y and z. In other words, this line is the altitude from x in our triangle xyz. The other two altitudes can be described in a similar way. By the lemma about common points, in order to prove the theorem about the altitudes it is sufficient to prove that (notice that altitudes cannot be parallel)

$$x \times \widetilde{(y \times z)} + y \times \widetilde{(z \times x)} + z \times \widetilde{(x \times y)} = 0.$$

By the Jacobi identity,

$$x \times (y \times z) + y \times (z \times x) + z \times (x \times y) = 0.$$

Since $\widetilde{u} = u - \overline{u}$, we see that it is sufficient to prove that

$$x \times \overline{(y \times z)} + y \times \overline{(z \times x)} + z \times \overline{(x \times y)} = 0.$$

Recalling that $\overline{u} = (u, e_0)\, e_0$, we see that the last identity is equivalent to

$$(y \times z, e_0)\, x \times e_0 + (z \times x, e_0)\, y \times e_0 + (x \times y, e_0)\, z \times e_0 = 0.$$

This immediately follows from the lemma below (take $a = b = e_0$, and recall that $a \times a = 0$ for any a). So, the theorem about the altitudes is proved modulo the following Lemma.

Lemma. *Let x, y, z, a, b be vectors in $\mathbf{R}^3$. Then*

$$(y \times z, a)\, x \times b + (z \times x, a)\, y \times b + (x \times y, a)\, z \times b = (x \times y, z)\, a \times b.$$

Proof. It is sufficient to prove that for any $c \in \mathbf{R}^3$ the scalar products of both sides with c are equal, i.e., that

$$\begin{aligned}(y \times z, a)\,(x \times b, c) + (z \times x, a)\,(y \times b, c) + (x \times y, a)\,(z \times b, c)\\ = (x \times y, z)\,(a \times b, c).\end{aligned}$$

Consider the left-hand side as a function $D(x, y, z)$ of the triple (x, y, z). Clearly, $D(x, y, z)$ is multilinear in x, y, z. The first term is skew-symmetric in y and z (i.e., changes sign if y and z are interchanged), as is the sum of other two terms. Therefore D is skew-symmetric in y and z. Similarly, D is skew-symmetric in the two other pairs of our variables. By the well-known characterization of the determinant, D is proportional to the determinant of the matrix with rows x, y, z. The latter is equal to $(x \times y, z)$, as is also well known. In order to find the coefficient of proportionality, it is sufficient to compute the left-hand side for a particular choice of linearly independent x, y, z. Let us take $x = (1, 0, 0)$, $y = (0, 1, 0)$, $z = (0, 0, 1)$. Then $(x \times y, z) = 1$. Let $a = (a_0, a_1, a_2)$, $b = (b_0, b_1, b_2)$, $c = (c_0, c_1, c_2)$. Then $x \times b = (0, -b_2, b_1)$ and

$$(x \times b, c) = -b_2c_1 + b_1c_2 = \det \begin{pmatrix} b_1 & b_2 \\ c_1 & c_2 \end{pmatrix}.$$

Also, $y \times z = (1, 0, 0)$ and $(y \times z, a) = a_0$. So, the first term on the left-hand side is equal to

$$a_0 \det \begin{pmatrix} b_1 & b_2 \\ c_1 & c_2 \end{pmatrix}.$$

The two other terms can be computed in the same way. We see that the left-hand side is equal to the expansion of the determinant

$$\det \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{pmatrix}$$

along the first row. So, for $x = (1, 0, 0)$, $y = (0, 1, 0)$, $z = (0, 0, 1)$ the left-hand side is equal to this determinant, i.e., to $(a \times b, c)$. Therefore, the coefficient of proportionality is equal to $(a \times b, c)$, and in general the left-hand side is equal to $(x \times y, z)\,(a \times b, c)$. This proves the lemma. ∎

10. ORTHOCENTERS IN EUCLIDEAN GEOMETRY: OTHER PROOFS. It turns out that the Euclidean altitudes theorem can be deduced from the hyperbolic one.

Another proof of the Euclidean altitudes theorem. There is a situation in which orthogonality in the Klein model is the same as Euclidean orthogonality. Namely, this is the case when one of the lines passes through the center **0** of the unit disc. In fact, we already encountered this phenomenon in the proof of Theorem 4. We will recall the argument for the convenience of the reader. Let l be a line in the Klein model (the classical one, see Sections 2 and 3) passing through **0**. Then the point geometrically polar to l is equal to the point at infinity $[k]$ of k, where k is any (Euclidean) perpendicular to l. By Theorem 1 (see Section 3) a line m is hyperbolically orthogonal to l if and only if its extension $\overline{m}$ to a projective line contains $[k]$, i.e., if it is orthogonal to l in Euclidean sense. So, two notions of orthogonality agree for such an l.

Let us consider a triangle ABC in the Klein model having **0** as one of its vertices, say $A = \mathbf{0}$. Then the sides AB and AC pass through **0**. By the previous paragraph, the hyperbolic altitudes from B and C are also the Euclidean altitudes from B and C. By the same token, the hyperbolic altitude from $A = \mathbf{0}$ is also the Euclidean altitude from A. It follows that the hyperbolic and Euclidean altitudes theorems for such a triangle are equivalent.

Since every Euclidean triangle is similar to a triangle contained in the unit disc and having **0** as one of its vertices, we see that the hyperbolic altitudes theorem implies the Euclidean one. ∎

One can also deduce the Euclidean altitudes theorem from the spherical one in a similar way. Given a Euclidean triangle, one may put it on a plane tangent to the unit sphere in S^2 in such a way that one of its vertices is equal to the tangency point. For such a triangle ABC, the Euclidean theorem is equivalent to the spherical theorem for the spherical triangle obtained by radial projection of ABC. We leave the details to the interested readers.

One more proof of the Euclidean altitudes theorem. Let us denote by (u, v) the usual scalar product of two vectors u and v in $\mathbf{R}^2$. Let abc, where a, b, and c are three vectors

in $\mathbf{R}^2$, be our triangle. We assume that the triangle is nondegenerate. This is equivalent to linear independence of the vectors $b - c$ and $c - a$, say. The linear subspace orthogonal to $b - c$ is given by the equation $(b - c, x) = 0$. The line orthogonal to $b - c$ and passing through a is given by the equation $(b - c, x) = (b - c, a)$. It is the altitude of the triangle abc from the vertex a. For the three altitudes we get the following three equations.

$$(b - c, x) = (b - c, a)$$
$$(c - a, x) = (c - a, b)$$
$$(a - b, x) = (a - b, c)$$

The linear map assigning to $x \in \mathbf{R}^2$ the vector whose components are the left-hand sides of these equations has rank 2 (because our triangle is nondegenerate) and its image consists of all vectors (A, B, C) such that $A + B + C = 0$. The vector whose components are the right-hand sides satisfies this condition, and, therefore, our system of linear equations has a solution x. This solution is the point of intersection of the three altitudes. This proves the theorem. ■

Notice that a key point of this proof is based on an argument similar to the lemma about common points from Section 6.

In [**1**] Arnol'd claimed that the Jacobi identity "forces the heights of a triangle to cross at one point". In [**2**], he claimed more specifically that the Jacobi identity for the ordinary vector product *"expresses the altitude theorem"* in Euclidean geometry.

As we just saw, the altitude theorem in Euclidean geometry can be deduced from either the hyperbolic or the spherical theorem, which in their turn can be deduced from the Jacobi identity. But both of these proofs require moving the triangle into a special position and singling out one of its vertices. So, these proofs proceed by destroying the intrinsic symmetry of the problem, and then by transferring the problem either to hyperbolic or to spherical geometry.

Kirillov's proof, presented in Section 9, comes much closer to a justification of the above claims by Arnol'd. Still, it is relatively complicated, and is based on a fairly complicated identity, the last lemma of Section 9, in addition to the Jacobi identity.

In contrast with these proof, our last proof keeps the symmetry of the problem, is carried out entirely in Euclidean geometry (as is Kirillov's proof), is much simpler, and is somewhat parallel to our proof of the hyperbolic theorem (which also keeps the symmetry of the problem). But it does not use the Jacobi identity. Another proof, similar in spirit, but less elementary and more complicated, can be found in [**15**, Section 10.3]. Similarly, the classical proofs of this theorem, such as the proofs of Euler and Gauss mentioned in the Introduction, do not use the Jacobi identity.

Given this, it seems that the claim that the Jacobi identity "forces the heights of a triangle to cross at one point" is well justified, but the claim that the Jacobi identity "expresses" the Euclidean theorem is somewhat exaggerated. Rather, the Jacobi identity for the ordinary vector product "expresses" the spherical altitudes theorem, as Section 8 shows. Since Arnol'd claimed in [**2**] (see p. 30 of the English translation) that the altitudes theorem fails in both hyperbolic and spherical geometries, one may think that he mistook a version of the arguments in Section 8 for a proof of the altitudes theorem in Euclidean geometry. One may guess that this mistake eventually led to his proof of the altitudes theorem in hyperbolic geometry.

Of course, the reader may form a different opinion on these matters.

11. FENCHEL'S THEORY OF LINES AND ORTHOCENTERS. In this section we present another approach to the hyperbolic altitudes theorem. This approach is based on Fenchel's theory of lines (see [**9**, Chapter V]). It is algebraically strikingly similar to our proof from Section 6 (and is also based ultimately on the Jacobi identity), but the two proofs are very different in what geometric tools they use. In the next section we will compare the two approaches. Recall that in this section and in the next one we expect much more than before from the reader; namely, the reader should be familiar with the upper half-space model of hyperbolic 3-space and with its group of motions.

Following Fenchel [**9**], we will work with the upper half-space model $\mathbf{H} = \mathbf{R}^2 \times \mathbf{R}_{>0}$ (where $\mathbf{R}_{>0}$ is the set of positive real numbers) of 3-dimensional hyperbolic space. It is convenient to identify $\mathbf{H}$ with $\mathbf{C} \times \mathbf{R}_{>0}$. As is well known, this identification leads to the identification of the group of orientation-preserving motions of $\mathbf{H}$ with the group of Möbius transformations of $\mathbf{C}$, i.e., with the group of maps $F : \mathbf{C} \cup \{\infty\} \to \mathbf{C} \cup \{\infty\}$ of the form

$$F(z) = \frac{az + b}{cz + d}$$

such that $ad - bc \neq 0$. In turn, this leads to the identification of the group of motions of $\mathbf{H}$ with the group $PGL_2(\mathbf{C})$.

The lines in the upper half-space model are the intersections of the open half-space $\mathbf{C} \times \mathbf{R}_{>0}$ with the circles orthogonal to $\mathbf{C} \times \{0\}$ (note that such circles always have center in $\mathbf{C} \times \{0\}$) and with the lines orthogonal to $\mathbf{C} \times \{0\}$. The lines of the first type are (open) Euclidean semicircles having two endpoints in $\mathbf{C} \times \{0\}$. The lines of the second type are (open) Euclidean half-lines having an endpoint in $\mathbf{C} \times \{0\}$. We think of such a half-line as a semicircle of infinite radius whose other endpoint is ∞. In particular, every line can be thought as having two endpoints in $(\mathbf{C} \times \{0\}) \cup \{\infty\}$. In the future, we will identify $\mathbf{C} \times \{0\}$ with $\mathbf{C}$ and $(\mathbf{C} \times \{0\}) \cup \{\infty\}$ with $\mathbf{C} \cup \{\infty\}$.

In [**9**, Chapter V], Fenchel suggested representing the lines in $\mathbf{H}$ by motions of $\mathbf{H}$, namely representing a line l by the rotation by the angle π around l. Since the group of motions is isomorphic to $PGL_2(\mathbf{C})$, this also allows us to represent lines by complex 2-by-2 matrices. Fenchel proved that a matrix $A \in GL_2(\mathbf{C})$ represents a rotation by the angle π around a line if and only if $\operatorname{tr} A = 0$.

Following Fenchel, we call nonzero matrices with trace zero *line matrices*. If a line matrix A is nondegenerate (i.e., $\det A \neq 0$), then it represents a line. Its endpoints in $\widehat{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$ are the fixed points of the corresponding Möbius transformation. If a line matrix A is degenerate, then the corresponding Möbius transformation has exactly one fixed point. In this case we say that A represents a *degenerate line* having z as both of its endpoints, where $z \in \widehat{\mathbf{C}}$ is the unique fixed point of the corresponding Möbius transformation. An ordinary line has two different endpoints in $\widehat{\mathbf{C}}$. We will denote the line corresponding to a line matrix A by l_A, including the degenerate case.

We will say that a degenerate line l is orthogonal to the ordinary line l' if the only endpoint of l is equal to one of the endpoints of l'. As is well known, two ordinary lines in $\mathbf{H}$ either have a nondegenerate common perpendicular or are asymptotically parallel (i.e., have a common endpoint). So, with our definitions, two different lines (ordinary or degenerate) always have a unique common perpendicular.

The basic fact relating line matrices with orthogonality is the following.

Proposition. *Let A and B be two line matrices. If they are both nondegenerate, then* $\operatorname{tr}(AB) = 0$ *if and only if the lines l_A and l_B intersect and are orthogonal at the inter-*

section point. If A is nondegenerate and B is degenerate, then $\operatorname{tr}(AB) = 0$ *if and only if the (only) endpoint of l_B is also an endpoint of l_A. In particular, in both cases l_A is orthogonal to l_B.*

See [**9**, Section V.1] for a proof of a more general result. The following corollary and lemma are also special cases of some propositions from that section. The corollary (more precisely, its more general version from [**9**]) apparently appeared for the first time in the famous paper by Jørgensen [**11**]; see [**11**, Section 4]. An exposition of this theory, closer in spirit to Jørgensen [**11**] than to the more elementary approach of Fenchel [**9**], is given in a recent book by Marden; see [**13**, Chapter 7].

Corollary. *If A and B are line matrices representing two different nondegenerate lines, then $l_{[A,B]}$ is a common perpendicular to l_A and l_B.*

Proof. Since the matrices A and B represent different lines, they are not proportional. By the lemma about zero commutators (see Section 6), this implies that $[A, B] \neq 0$ and, therefore, $l_{[A,B]}$ is well defined. By the lemma about traces (see Section 6) $\operatorname{tr}(A[A, B]) = 0$ and $\operatorname{tr}(B[A, B]) = -\operatorname{tr}(B[B, A]) = 0$. By the proposition, this implies that both l_A and l_B are orthogonal to $l_{[A,B]}$. ∎

In the case when $[A, B]$ is degenerate, the corollary implies that l_A and l_B have a common endpoint, namely, the unique endpoint of the degenerate line $l_{[A,B]}$.

Lemma about Common Perpendiculars. *If three line matrices α, β, γ satisfy the relation $\alpha + \beta + \gamma = 0$, then the three projective lines l_α, l_β, l_γ have a common perpendicular.*

Proof. The linear dependence among α, β, and γ implies that the equations $\operatorname{tr}(X\alpha) = \operatorname{tr}(X\beta) = \operatorname{tr}(X\gamma) = 0$ have a nonzero solution X such that $\operatorname{tr}(X) = 0$. By the proposition, for such a solution X the line l_X is a common perpendicular to our lines. ∎

Theorem. *Let abc be a triangle in* **H**. *Its three altitudes are either concurrent (i.e., have a common point in* **H***), or have a common (nondegenerate) perpendicular contained in the plane of the triangle abc, or are asymptotically parallel (i.e., have a common endpoint).*

Proof. Let P be the plane of the triangle abc (as usual, we assume that our triangle is nondegenerate, i.e., the points a, b, c are not contained in a line and, therefore, determine a plane). Let A, B, C be the line matrices representing the lines orthogonal to P at the points a, b, c, respectively. Then $l_{[A,B]}$ is a common perpendicular to l_A and l_B. On the other hand, the line ab is a common perpendicular to l_A and l_B by the choice of A and B. Since two lines may have no more than one common perpendicular, this implies that $l_{[A,B]} = ab$. Similarly, $l_{[B,C]} = bc$ and $l_{[C,A]} = ca$.

Next, $l_{[[A,B],C]}$ is a common perpendicular to $l_{[A,B]} = ab$ and l_C. But the altitude of the triangle abc passing through c and orthogonal to ab is also a common perpendicular to ab and l_C. It follows that $l_{[[A,B],C]}$ is equal to this altitude. Similarly, $l_{[[B,C],A]}$ and $l_{[[C,A],B]}$ are the other two altitudes of the triangle abc.

Now, the Jacobi identity

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$$

together with the lemma about common perpendiculars implies that the three altitudes of abc have a common perpendicular.

Let us consider two of the altitudes of abc. Suppose that they intersect at a point x. Clearly, $x \in P$. In this case the only common perpendicular to these two altitudes is the line orthogonal to the plane P and passing through x. Since all three altitudes have a common perpendicular, this line is also orthogonal to the third altitude. In particular, the third altitude intersects it. But this line has only one common point with P, namely, x, and the third altitude is contained in P. It follows that x is a common point of all three altitudes. This proves the theorem in this case.

Suppose that the two altitudes have a common (nondegenerate) perpendicular in P. Since two lines may have no more than one common perpendicular, and we know that the three altitudes have a common perpendicular, this common perpendicular is actually a common perpendicular of all three altitudes. This proves the theorem in this case.

Suppose now that the two altitudes are asymptotically parallel. Let x be their common endpoint. In this case the common perpendicular is the degenerate line connecting x to itself. This degenerate line has to be a perpendicular to the third altitude also. This means that the three altitudes share a common endpoint, namely, x. This proves the theorem in this case, and completes the proof of the theorem. ∎

12. TWO WAYS TO ASSIGN LINES TO MATRICES. Let A be a real line matrix such that $-\det(A) > 0$. There are two ways to assign a line in a hyperbolic plane to A: assign the line l_A as in Section 11, or assign the line $A^{\perp}$ in the Klein model based on $sl(2)$ as described in the proposition in Section 4. It turns out that these two ways are essentially the same.

In order to make sense out of this claim, we need a way to compare our two models of hyperbolic geometry. Our strategy will be to compare lines by comparing their endpoints, so we have to pay special attention to what happens at infinity.

First, let us consider the hyperbolic plane $\mathbf{R} \times \mathbf{R}_{>0} \subset \mathbf{C} \times \mathbf{R}_{>0}$ in the upper half-space model. This plane is nothing else than the upper half-plane model of the hyperbolic plane. Its circle at infinity is $(\mathbf{R} \times \{0\}) \cup \{\infty\}$, which we will identify with $\widehat{\mathbf{R}} = \mathbf{R} \cup \{\infty\}$. The standard way to identify the upper half-plane model with the Poincaré unit disc model in $\mathbf{R}^2$ is to apply to it the inversion with center $(0, -1)$ and radius $\sqrt{2}$. See, for example, [**14**, Appendix, p. 364]. This inversion takes $\widehat{\mathbf{R}}$ to the unit circle; the restriction of this inversion to $\widehat{\mathbf{R}}$ is the stereographic projection from $\widehat{\mathbf{R}}$ to the unit circle. As is well known (and easily checked), it takes $t \in \widehat{\mathbf{R}}$ to

$$\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right) \tag{2}$$

(it takes ∞ to $(0, -1)$). The standard identification of the Poincaré unit disc model with the Klein model (see Section 2) is equal to the identity on the circle at infinity. So, the point at infinity in the Klein model corresponding to $t \in \widehat{\mathbf{R}}$ is still the same point (2). Considered as a point of the projective plane, it is equal to

$$[2t : 1 - t^2 : 1 + t^2],$$

if $t \neq \infty$, and to $[0, -1, 1]$ if $t = \infty$. In order to pass to the Klein model based on $sl(2)$, we have to use the map $f : \mathbf{R}^3 \to sl(2)$ from Section 6. Recall that

$$f(x, y, z) = \begin{pmatrix} x & y - z \\ y + z & -x \end{pmatrix}.$$

In particular,

$$f(2t, 1 - t^2, 1 + t^2) = \begin{pmatrix} 2t & -2t^2 \\ 2 & -2t \end{pmatrix},$$

and

$$f(0, -1, 1) = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}.$$

Now, consider a real line matrix

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

such that $-\det(A) = a^2 + bc > 0$. The endpoints of the line l_A are the fixed points of the corresponding Möbius transformations of $\widehat{\mathbf{C}}$, i.e., they are solutions t of the equation

$$\frac{at + b}{ct - a} = t. \tag{3}$$

Equation (3) is equivalent* to

$$ct^2 - 2at - b = 0 \tag{4}$$

for $t \neq \infty$. Clearly, $t = \infty$ is a solution of (3) if and only if $c = 0$. In this case (4) has only one solution in $\mathbf{R}$, and we will consider $t = \infty$ as the second solution in $\widehat{\mathbf{R}}$. (Since $a^2 + bc > 0$, it cannot happen that $c = a = 0$.) If A is a real line matrix and $-\det(A) = a^2 + bc > 0$, then both solutions of (4) belong to $\widehat{\mathbf{R}}$. This implies that both endpoints of l_A are contained in $\widehat{\mathbf{R}}$, and therefore l_A is contained in the plane $\mathbf{R} \times \mathbf{R}_{>0}$.

The line $A^\perp$ corresponding to A in the Klein model based on $sl(2)$ is given by the equation $\operatorname{tr}(PA) = 0$. The point $t \in \mathbf{R}$ corresponds to an endpoint of this line if and only if

$$\operatorname{tr}(f(2t, 1 - t^2, 1 + t^2)A) = \operatorname{tr}\left(\begin{pmatrix} 2t & -2t^2 \\ 2 & -2t \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\right) = 0,$$

i.e., if and only if

$$2at - 2ct^2 + 2b + 2at = 0.$$

The last equation is equivalent to

$$ct^2 - 2at - b = 0. \tag{5}$$

*Notice that if we have $ct - a = 0$ for a solution of (4), then $at + b = ct^2 - at = t(ct - a) = 0$. But if $ct - a = at + b = 0$, then either $c = a = 0$, or $a = b = 0$, or $t = a/c = -b/a$, and in all these cases $a^2 + bc = 0$, contradicting our assumption that $a^2 + bc > 0$.

The point $t = \infty$ corresponds to an endpoint of $A^\perp$ if and only if

$$\operatorname{tr}(f(0,-1,1)A) = \operatorname{tr}\left(\begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\right) = -2c = 0,$$

i.e., if and only if $c = 0$.

The equation (4) describes the endpoints of l_A (with our convention that $t = \infty$ is a solution for $c = 0$). The equation (5) desribes the points $t \in \mathbf{R}$ corresponding to the endpoints of $A^\perp$ under our identification of the two models. If we treat the equation (5) in the same way as (4), i.e., if we consider $t = \infty$ as a solution of (5) if $c = 0$, then (5) covers the case $t = \infty$ too. Since the two equations (4) and (5) are the same, we see l_A has exactly the same endpoints as $A^\perp$, and therefore $l_A = A^\perp$.

We see that the two ways to assign a line to a matrix agree. This agreement can be extended to an "isomorphism" between the two proofs of the theorem about altitudes, the proof from Section 11 and the proof from Section 6. We leave this task to the interested readers. The two proofs are exactly the same on the algebraic level, but are noticeably different in their geometric form.

ACKNOWLEDGMENTS. Clearly, this article owes its existence to the ideas of V. I. Arnol'd. I would like to use this occasion to express my gratitude to V. I. Arnol'd for his support during the eighties, and for his general influence on my mathematical tastes. I would like to thank Yu. Baryshnikov for email correspondence about questions discussed in Sections 8 and 10, and M. F. Prokhorova for informing me about Kirillov's proof of the altitudes theorem. Two referees helped to improve the paper significantly. The first referee suggested bringing in Chasles's theorem (see Remark 2 in Section 6), and suggested the first proof of the Euclidean altitudes theorem from Section 10. The second referee directed me to the beautiful ideas of Fenchel and Jørgensen (see Sections 11 and 12). Both referees corrected a lot of English mistakes. This research was supported in part by NSF Grant DMS-0406946.

REFERENCES

1. V. I. Arnol'd, On teaching mathematics (in Russian) *Uspekhi Mat. Nauk* **53** (1998) 229–234; English translation: *Russian Math. Surveys* **53** (1998) 229–236.
2. ———, A. N. Kolmogorov and the natural science (in Russian), *Uspekhi Mat. Nauk* **59** (2004) 25–44; English translation: *Russian Math. Surveys* **59** (2004) 27–46.
3. ———, Lobachevsky triangle altitude theorem as the Jacobi identity in the Lie algebra of quadratic forms on symplectic plane, *J. of Geometry and Physics*, **53** (2005) 421–427; Russian version: *Matematicheskoe prosvestchenie, Ser. 3*, **9** (2005) 93–99.
4. M. Audin, *Geometry*, Springer, Berlin, 2002.
5. J. L. Coolidge, *The Elements of Non-Euclidean Geometry*, Clarendon Press, Oxford, 1909.
6. H. S. M. Coxeter, *Non-Euclidean Geometry*, 6th ed., Mathematical Association of America, Washington, DC, 1998; University of Toronto Press, Toronto, 1942.
7. ———, *Introduction to Geometry*, John Wiley, New York, 1989; reprint of 2nd ed., John Wiley, New York, 1969; John Wiley, New York, 1961.
8. ———, *Projective Geometry*, Springer, Berlin, 2003; Blaisdell, New York, 1964.
9. W. Fenchel, *Elementary Geometry in Hyperbolic Space*, Walter de Gruyter, Berlin, 1989.
10. R. Hartshorne, *Geometry: Euclid and Beyond*, Springer, Berlin, 2005; corrected 4th printing of 1st ed., 2000.
11. T. Jørgensen, Compact 3-manifolds of constant negative curvature fibering over the circle, *Ann. of Math.* **106** (1977) 61–72. doi:10.2307/1971158
12. A. A. Kirillov, *Lectures on the Orbit Method*, Graduate Studies in Mathematics, vol. 64, American Mathematical Society, Providence, RI, 2004.
13. A. Marden, *Outer Circles*, Cambridge University Press, Cambridge, 2007.
14. J. Milnor, On the Geometry of the Kepler Problem, *Amer. Math. Monthly* **90** (1983) 353–365. doi:10.2307/2975570
15. D. Pedoe, *Geometry: A Comprehensive Course*, Dover, Mineola, NY, 1988; Cambridge University Press, London, 1970.
16. E. G. Rees, *Notes on Geometry*, Springer, Berlin, 2005; 6th printing of 1st ed., 1983.

17. M. B. Skopenkov, Theorem about the altitudes of a triangle and the Jacobi identity (in Russian), *Matematicheskoe Prosvestchenie, Ser. 3* **11** (2007) 79–89.
18. J. Stillwell, *Geometry of Surfaces*, Springer, Berlin, 1995; corrected 2nd reprint of 1st ed., 1992.
19. A. Weil, *Basic Number Theory*, Springer, Berlin, 1995; Die Grundlehren der mathematischen Wissenschaften, vol. 144, Springer, Berlin, 1967.

NIKOLAI V. IVANOV graduated from the Leningrad State University in 1976 and got his Ph.D. from the Steklov Mathematical Institute in 1980, under the direction of V. A. Rokhlin. In 1988 he received the Doctor of Sciences degree (something similar to the habilitation in western Europe), again from the Steklov Mathematical Institute. From 1979 until 1998 he was a researcher at the Leningrad branch of the Steklov Mathematical Institute and since 1991 he has been at Michigan State University, first as a visitor, then, after a half-year break spent at Duke University, as a permanent faculty member. His research interests include low-dimensional topology, quasiconformal maps, Teichmüller spaces, and Teichmüller modular groups. He has a strong preference for topics where different branches of mathematics interact, as in this paper.
Michigan State University, Department of Mathematics, Wells Hall, East Lansing, MI 48824-1027
ivanov@math.msu.edu

A Special Continued Fraction for the Golden Mean

$$3+\frac{-4}{3}=\frac{5}{3},\quad 3+\frac{-4+\frac{5}{3}}{3+\frac{-4}{3}}=\frac{8}{5},\quad 3+\frac{-4+\frac{5+\frac{-6}{3}}{3+\frac{-4}{3}}}{3+\frac{-4+\frac{5}{3}}{3+\frac{-4}{3}}}=\frac{13}{8},\ldots,$$

and therefore

$$3+\cfrac{-4+\cfrac{5+\cfrac{-6+\cfrac{7+\cdots}{3+\cdots}}{3+\cfrac{-4+\cdots}{3+\cdots}}}{3+\cfrac{-4+\cfrac{5+\cdots}{3+\cdots}}{3+\cfrac{-4+\cdots}{3+\cdots}}}}{3+\cfrac{-4+\cfrac{5+\cfrac{-6+\cdots}{3+\cdots}}{3+\cfrac{-4+\cdots}{3+\cdots}}}{3+\cfrac{-4+\cfrac{5+\cdots}{3+\cdots}}{3+\cfrac{-4+\cdots}{3+\cdots}}}}=\phi=\frac{1+\sqrt{5}}{2}.$$

—Submitted by Domingo Gomez Morin,
Universidad Santa Maria, Caracas, Venezuela

NOTES

Edited by **Ed Scheinerman**

Two Extensions of Results of Archimedes

Nicholas Pippenger

Abstract. We review the two results in the *Method* of Archimedes, show how they follow from Cavalieri's principle, and show how two extensions of them can also be proved using Cavalieri's principle.

1. INTRODUCTION. In 1906, J. L. Heiberg discovered in Constantinople (now Istanbul) a partial copy of a work by Archimedes that had long been thought to have been lost. It takes the form of a letter from Archimedes to Eratosthenes, and is entitled *The Method of Deriving Geometrical Conclusions from Mechanical Propositions*, which is today usually abbreviated as the *Method*. The copy is part of a palimpsest, and is incomplete, with some parts being missing or indecipherable. Heiberg published a transcription of the Greek [**5**], and a translation into German [**6**], with commentary by H. G. Zeuthen. L. G. Robinson published a translation into English [**8**] (from Heiberg's German), with a commentary by D. E. Smith. And T. L. Heath published a translation into English (from the original Greek), with commentary, as a supplement to his edition [**4**] of Archimedes' works. The copy was lost again in the 1920s, but rediscovered in the 1990s. After a dispute over its ownership, it now resides at the Walters Art Museum in Baltimore, where efforts to recover previously indecipherable material are underway. A preliminary report on these efforts has been given by Netz, Saito, and Tchernetska [**7**].

The *Method* offers proofs of two results, which may be stated in modern language as follows. Let X be a filled right circular cylinder of radius 1 about the x-axis (so that its intersection with any plane perpendicular to the x-axis is a filled circle (disk) of radius 1 centered at the axis), and let Y be a similar cylinder about the y-axis. Archimedes showed that the volume of the intersection $R = X \cap Y$ of these two cylinders is $\mathrm{vol}(R) = 16/3 = 5.3333\ldots$. (The surface ∂R of R consists of four curved parts, two from each cylinder. See Figure 1.) We shall show that if Z is a similar cylinder about the z-axis, then the volume of the intersection $S = X \cap Y \cap Z$ of these three cylinders is $\mathrm{vol}(S) = 16 - 8\sqrt{2} = 4.6862\ldots$. (The surface ∂S of S consists of twelve curved parts, four from each cylinder. See Figure 2.) The other problem treated

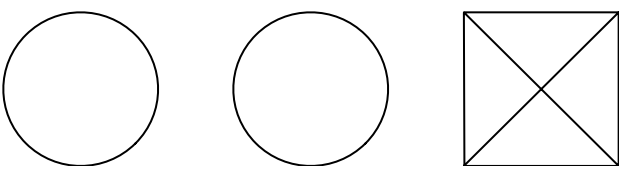

Figure 1. The intersection $R = X \cap Y$ of two cylinders, viewed (left to right) from the positive x-, y-, and z-axes.

doi:10.4169/amer.math.monthly.118.01.066

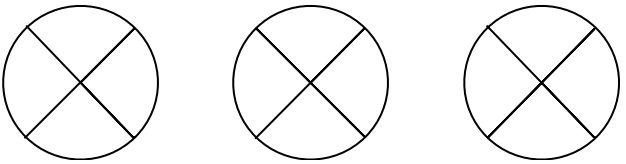

Figure 2. The intersection $S = X \cap Y \cap Z$ of three cylinders, viewed (left to right) from the positive x-, y-, and z-axes.

by Archimedes in the *Method* concerns a solid known as the "hoof." Let U be a filled right isosceles triangular cylinder with side 1, defined by the inequalities $z \geq 0$, $z \leq y$, and $y \leq 1$. The hoof is the intersection $H = U \cap Z$ of two cylinders, one triangular and one circular. (The surface ∂H of H comprises a filled semi-circle in the plane $z = 0$ and a filled semi-ellipse in the plane $z = y$, in addition to a curved part coming from the cylinder ∂Z. See Figure 3.)

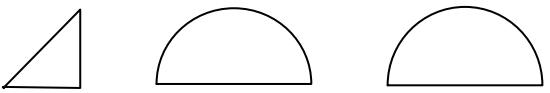

Figure 3. The hoof $H = U \cap Z$, viewed (left to right) from the positive x-, y-, and z-axes.

The volume of this solid was determined by Archimedes to be $\text{vol}(H) = 2/3 = 0.6666\ldots$. Let V be a filled right isosceles triangular cylinder with side 1, defined by the inequalities $z \geq 0$, $z \leq x$, and $x \leq 1$. Let $J = U \cap V \cap Z$, the intersection of these three cylinders, two triangular and one circular. The solid J is the intersection of H with its reflection in the plane $x = y$. (The surface ∂J of J comprises a filled quarter-circle in the plane $z = 0$ and filled eighth-ellipses in the planes $z = y$ and $z = x$, in addition to a curved part coming from the cylinder ∂Z.) We shall show that the volume of the intersection of these two hooves is $\text{vol}(J) = (2 - \sqrt{2})/3 = 0.1952\ldots$. (Note that for each of these extensions, the volume is a quadratic irrational, whereas the volume for Archimedes' original is rational.)

Apart from the results described above, the *Method* provides unique insight into the question as to which arguments Archimedes considered rigorous, and which he considered merely heuristic. He makes it clear that the method of "balancing" used in the surviving parts of the *Method* was only used for a preliminary investigation of the problems, and the solutions that it disclosed were to be proved rigorously by the method of "exhaustion." The rigorous proofs are missing from the extant copy of the *Method*, but another of his works, the *Quadrature of the Parabola* (see Heath [**4**, pp. 233–252]), provides examples of both balancing and exhaustion.

The method of balancing bears a strong resemblance to Cavalieri's principle, which was introduced by Bonaventura Cavalieri in the 1600s, before the development of the calculus (see Eves [**2**]). Cavalieri's principle (for volumes) states: if the nonzero areas of the sections of solids F and G by planes parallel to a given plane are in constant ratio, then the volumes of F and G are in the same ratio. Cavalieri's principle is not a theorem if "solids" is given its modern set-theoretic meaning and "volume" is interpreted as Lebesgue measure. For if G is a copy of F in which the sections in planes parallel to the xy-plane are displaced by a small amount for a nonmeasurable set of z values, then Cavalieri's principle claims the volumes of F and G are equal, when in fact the set G is not even measurable (and the inner and outer measures of G are both different from that of F). When restricted to solids bounded by algebraic surfaces,

however, Cavalieri's principle is perfectly reliable. This is most easily seen by using Jordan content, rather than Lebesgue measure, for areas and volumes. Jordan content is based on coverings by finite sets of rectangular parallelopipeds, whereas Lebesgue measure is based on coverings by countably infinite sets. A key theorem says that a d-dimensional region Q has a Jordan content if its boundary ∂Q has d-dimensional Jordan content zero. This easily implies that all surfaces and solids bounded by algebraic curves and surfaces have Jordan areas and volumes. Cavalieri's principle then says that if solids F and G have Jordan volumes, and if the sections of F and G by planes parallel to a given plane have Jordan areas in a given ratio, then the volumes of F and G are in the same ratio. (See Spivak [**9**, Chap. 3, Ex. 3-36], where the justification of Cavalieri's principle is given as an exercise.) The method of exhaustion, on the other hand, is rigorous even by modern standards; by expressing a solid as a countable union of disjoint sets whose volumes are known, it establishes measurability at the same time as it determines the volume.

This note uses Cavalieri's principle, not only for the extensions described above, but also to rederive the results of Archimedes and some of his predecessors. The other properties of area and volume we rely on are invariance under congruence, scaling with coordinate axes, and finite additivity for disjoint regions.

2. TWO CYLINDERS AND THREE CYLINDERS. We begin with a derivation of Archimedes' result $\mathrm{vol}(R) = 16/3$. Let B denote the filled sphere (ball) with radius 1 centered at the origin, so that $\mathrm{vol}(B) = 4\pi/3 = 4.1887\ldots$. Planes parallel to the xy-plane cut B in a filled circle and R in a filled square. Furthermore, the circle is inscribed in the square: the points of tangency are the points of the two circles at which the sphere ∂B bounding B touches the unfilled cylinders ∂X and ∂Y bounding X and Y. (See Figure 4.) Since the ratio of the area of a filled square to that of a filled inscribed circle is $4/\pi$, Cavalieri's principle says that the ratio of the volume of R to that of B is also $4/\pi$, so we have $\mathrm{vol}(R) = (4/\pi)(4\pi/3) = 16/3$. (The author first learned of this result from the *Mathematical Games* column [**3**] of Martin Gardner in *Scientific American*, where it was attributed to Archimedes. It is also sometimes attributed to Charles Proteus Steinmetz, an engineer who lived at the time that the copy of the *Method* was discovered. Indeed, Eves [**2**] attributes it to Steinmetz in an article in a book dedicated to Martin Gardner! Both Gardner and Eves give derivations using Cavalieri's principle.)

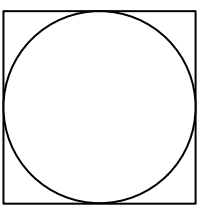

Figure 4. A plane parallel to the xy-plane intersects the body R in a filled square and intersects the ball B in an inscribed disk.

This derivation of $\mathrm{vol}(R) = 16/3$ uses Archimedes' result $\mathrm{vol}(B) = 4\pi/3$, from *On the Sphere and the Cylinder, I* (see Heath [**4**, pp. 1–55]), where it is proved by the method of exhaustion. This latter result can also be derived using Cavalieri's principle. Consider the solid K comprising all points (x, y, z) lying inside cylinder Z (that is, satisfying $x^2 + y^2 \le 1$), but lying outside the conic $x^2 + y^2 = z^2$ (that is, satisfying $x^2 + y^2 \ge z^2$). Any plane parallel to the xy-plane with $-1 \le z \le 1$ cuts B in a disk

of radius $\sqrt{1-z^2}$, and thus having area $\pi(1-z^2)$, while it cuts the solid K in an annulus with outer radius 1 and inner radius z, and thus also having area $\pi(1-z^2)$. (See Figure 5.) It follows from Cavalieri's principle that $\mathrm{vol}(B) = \mathrm{vol}(K)$, so it remains only to determine $\mathrm{vol}(K)$. The body K is the difference between a segment of a filled cylinder, with altitude 2 and base area π, and two cones, each having altitude 1 and base area π. Thus $\mathrm{vol}(K) = 2\pi - 2(\pi/3) = 4\pi/3$.

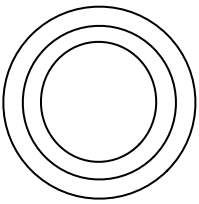

Figure 5. A plane parallel to the xy-plane intersects the body K in an annulus and intersects the ball B in a disk. Circles of radius 1, 4/5, and 3/5 are shown. For $z = 4/5$, the annulus is the region between the outer two circles and the disk is bounded by the inner circle. For $z = 3/5$, both regions have expanded to include the area between the two inner circles.

This derivation of $\mathrm{vol}(B) = 4\pi/3$ uses the result that the volume of a cone is one-third the altitude times the area of the base. (In the *Method*, Archimedes attributes the statement of this result to Democritus, and the proof to Eudoxus, but neither of these sources has survived.) This result too can be derived using Cavalieri's principle. By rescaling the base and altitude if necessary, it suffices to verify that the volume of a cone with altitude 1 and base of area 1/2 is 1/6. By Cavalieri's principle, it suffices to verify this fact for any one particular cone with altitude 1 and base 1/2. But this fact is clear for the filled tetrahedron with vertices (0, 0, 0), (0, 0, 1), (0, 1, 1), and (1, 1, 1), since six tetrahedra congruent to this one can be assembled to form a filled cube with side 1. (Consider the six possible orders in which the three coordinates can be changed from 0 to 1 when defining the four vertices of a tetrahedron.)

Having seen three applications of Cavalieri's principle, we are ready to use it again to determine $\mathrm{vol}(S)$. The three unfilled cylinders ∂X, ∂Y, and ∂Z intersect at eight points $(x, y, z) = (\pm 1, \pm 1 \pm 1)/\sqrt{2}$, which form the vertices of a filled cube C with volume $\mathrm{vol}(C) = (2/\sqrt{2})^3 = 2\sqrt{2}$. This filled cube lies entirely within S. (The solid S is the intersection of three convex cylinders, and is thus itself convex. Since it contains the eight points $(\pm 1, \pm 1 \pm 1)/\sqrt{2}$, it also contains their convex hull C.) The remainder of S consists of six "caps," one affixed to each face of the cube. (The caps are disjoint, since at most one of x, y, and z can exceed $1/\sqrt{2}$ in absolute value at any point in S.) These six caps are congruent, so it will suffice to determine the volume of one of them, say the one affixed to the face at $z = 1/\sqrt{2}$. This cap is simply that part, call it R^+, of R that lies in the half-space $z \geq 1/\sqrt{2}$, since this half-space constraint, together with the constraints $x^2 + z^2 \leq 1$ and $y^2 + z^2 \leq 1$ that define R, imply the constraint $x^2 + y^2 \leq 1$ that distinguishes S from R. Thus, using Cavalieri's principle as in the derivation of $\mathrm{vol}(R)$, we see that $\mathrm{vol}(R^+)$ is $4/\pi$ times the volume of that part, call it B^+, of B that lies in the half-space $z \geq 1/\sqrt{2}$. Reasoning as in the derivation of $\mathrm{vol}(B)$, we see that $\mathrm{vol}(B^+)$ is equal to the volume of that part, call it K^+, of K that lies in the half-space $z \geq 1/\sqrt{2}$. The body K^+ is the difference between a segment of Z, having altitude $1 - 1/\sqrt{2}$ and base area π, and a frustum of a cone. This frustum is in turn the difference between a cone of altitude 1 and base area π and a cone of altitude $1/\sqrt{2}$ and base area $\pi(1/\sqrt{2})^2 = \pi/2$. Thus we have $\mathrm{vol}(B^+) = \pi(1 - 1/\sqrt{2}) - (\pi/3 - \pi/6\sqrt{2}) =$

$\pi(2/3 - 5\sqrt{2}/12)$. Multiplying by $4/\pi$, we obtain $\text{vol}(R^+) = (8 - 5\sqrt{2})/3$. Finally, we have $\text{vol}(S) = \text{vol}(C) + 6\ \text{vol}(R^+) = 2\sqrt{2} + 6(8 - 5\sqrt{2})/3 = 16 - 8\sqrt{2}$. (This result was obtained by Angell and Moore [**1**] as a byproduct of their determination of the area of ∂S.)

3. ONE HOOF AND TWO HOOVES. We next consider the volume of the hoof: $\text{vol}(H) = 2/3$. This result can also be found by Cavalieri's principle, as suggested by Eves [**2**]. Let L be the body obtained by removing from the prism comprising those points of U satisfying $-1 \le x \le 1$ two pyramids, each having as base one of the bases of the prism just defined and each having as apex the origin $(0, 0, 0)$. Since the prism has base area $1/2$ and altitude 2, it has volume 1. From it we remove two pyramids, each having base area $1/2$ and altitude 1, which together have volume $1/3$. Thus we have $\text{vol}(L) = 2/3$. Any plane parallel to the yz-plane with $0 \le x \le 1$ cuts H in a filled right isosceles triangle with legs $\sqrt{1 - x^2}$ and thus having area $(1 - x^2)/2$, while it cuts L in an isosceles trapezoid obtained by removing from a right isosceles triangle with legs 1 a right isosceles triangle with legs x, which therefore also has area $(1 - x^2)/2$. (See Figure 6.) By symmetry, the areas are also equal for planes parallel to the yz-plane with $-1 \le x \le 0$. Thus we have $\text{vol}(H) = \text{vol}(L) = 2/3$.

Finally, we show that $\text{vol}(J) = (2 - \sqrt{2})/3$. This time we decompose J into three parts: a pyramid P with base a filled square with vertices $(0, 0, 0)$, $(1, 0, 0)/\sqrt{2}$, $(0, 1, 0)/\sqrt{2}$, and $(1, 1, 0)/\sqrt{2}$ and apex $(1, 1, 1)/\sqrt{2}$, so that $\text{vol}(P) = 1/6\sqrt{2}$, and two "caps," one affixed to each of the two faces of the pyramid that does not meet the origin. The two caps are congruent, so it will suffice to consider the one affixed to the face at $x = 1/\sqrt{2}$. This cap is simply that part, call it H^+, of H that lies in the half-space $x \ge 1/\sqrt{2}$, which has the same volume as that part, call it L^+, of L that lies in that half-space. The body L^+ is the difference between a prism, having altitude $1 - 1/\sqrt{2}$ and base area $1/2$, and a frustum of a pyramid. This frustum is in turn the difference between a pyramid having altitude 1 and base area $1/2$ and a pyramid of altitude $1/\sqrt{2}$ and base area $1/4$. Thus we have $\text{vol}(L^+) = (1 - 1/\sqrt{2})/2 - (1/6 - 1/12\sqrt{2}) = 1/3 - 5/12\sqrt{2}$. Finally, we have $\text{vol}(J) = \text{vol}(P) + 2\ \text{vol}(L^+) = 1/6\sqrt{2} + 2(1/3 - 5/12\sqrt{2}) = (2 - \sqrt{2})/3$.

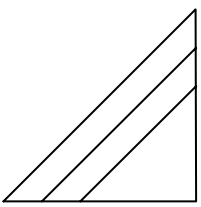

Figure 6. A plane parallel to the yz-plane intersects the hoof H in a filled isosceles right triangle and intersects the body L in an isosceles trapezoid. Isosceles right triangles with side 1, $4/5$, and $3/5$ are shown. For $z = 4/5$, the trapezoid is the region between the outer two triangles and the filled isosceles right triangle is bounded by the inner triangle. For $z = 3/5$, both regions have expanded to include the area between the two inner triangles.

ACKNOWLEDGMENTS. This research was partially supported by NSF Grant CCF 0430656.

REFERENCES

1. I. O. Angell and M. Moore, Symmetrical intersections of cylinders, *Acta Crystallogr. Sect. A* **43** (1987) 244–250.

2. H. Eves, Slicing it thin, pp. 100–111 in *The Mathematical Gardner*, D. A. Klarner, ed., Prindle, Weber, and Schmidt, Boston, 1981.
3. M. Gardner, Mathematical games, *Scientific American* **207**(4) (1962) 138; **207**(5) (1962) 164. doi:10.1038/scientificamerican0362-138;
4. T. L. Heath, *The Works of Archimedes*, Cambridge University Press, Cambridge, 1897; reprinted with the *Method* as supplement in 1912; reprinted with the supplement by Dover, Mineola, NY, 1953.
5. J. L. Heiberg, Eine neue Archimedeshandschrift, *Hermes* **42** (1907) 234–303.
6. J. L. Heiberg and H. G. Zeuthen, Eine neue Schrift des Archimedes, *Bibliotheca Mathematica* (3rd Series) **7** (1907) 321–363.
7. R. Netz, K. Saito, and N. Tchernetska, A new reading of *Method* proposition 14: Preliminary evidence from the Archimedes palimpsest (Part 1), *SCIAMVS: Sources and Commentaries in Exact Sciences* **2** (2001) 9–29; also available at http://www.sciamvs.org/v2p9.pdf.
8. L. G. Robinson and D. E. Smith, A newly discovered treatise of Archimedes, *Monist* **19** (1909) 202–230.
9. M. Spivak, *Calculus on Manifolds*, W. A. Benjamin, Menlo Park, CA, 1965.

Department of Mathematics, Harvey Mudd College, Claremont, CA 91711
njp@math.hmc.edu

On Polynomial Rings with a Goldbach Property

Paul Pollack

Abstract. David Hayes observed in 1965 that when $R = \mathbf{Z}$, every element of $R[T]$ of degree $n \geq 1$ is a sum of two irreducibles in $R[T]$ of degree n. We show that this result continues to hold for any Noetherian domain R with infinitely many maximal ideals.

It appears that David Hayes [**5**] was the first to observe the following polynomial analogue of the celebrated Goldbach conjecture: If $R = \mathbf{Z}$, then

> every element of $R[T]$ of degree $n \geq 1$ can be written as the sum of two irreducibles of degree n. $(\star)$

His proof is a clever application of Eisenstein's irreducibility criterion. Hayes's theorem and its proof were rediscovered by Rattan and Stewart [**10**] (see also [**1**] for some cognate results). Recently Saidak [**11**] and Kozek [**7**] have considered quantitative variants of Hayes's theorem. The latter shows that in a precise sense, for a given monic polynomial $A(T) \in \mathbf{Z}[T]$ of degree $n \geq 2$, almost all (asymptotically 100%) of its representations as a sum of two monic polynomials are such that both summands are irreducible.

In this note we consider a generalization in a different direction. Namely, we investigate which integral domains R have the property $(\star)$. In [**5**], Hayes points out that his proof shows that $(\star)$ holds whenever R is a principal ideal domain with infinitely many maximal ideals, and so in particular when R is the polynomial ring $F[x]$ with F an arbitrary field. Here we show how to relax the requirement that R be a PID to the much weaker condition that the ideals of R are finitely generated.

doi:10.4169/amer.math.monthly.118.01.071

2. H. Eves, Slicing it thin, pp. 100–111 in *The Mathematical Gardner*, D. A. Klarner, ed., Prindle, Weber, and Schmidt, Boston, 1981.
3. M. Gardner, Mathematical games, *Scientific American* **207**(4) (1962) 138; **207**(5) (1962) 164. doi:10.1038/scientificamerican0362-138;
4. T. L. Heath, *The Works of Archimedes*, Cambridge University Press, Cambridge, 1897; reprinted with the *Method* as supplement in 1912; reprinted with the supplement by Dover, Mineola, NY, 1953.
5. J. L. Heiberg, Eine neue Archimedeshandschrift, *Hermes* **42** (1907) 234–303.
6. J. L. Heiberg and H. G. Zeuthen, Eine neue Schrift des Archimedes, *Bibliotheca Mathematica* (3rd Series) **7** (1907) 321–363.
7. R. Netz, K. Saito, and N. Tchernetska, A new reading of *Method* proposition 14: Preliminary evidence from the Archimedes palimpsest (Part 1), *SCIAMVS: Sources and Commentaries in Exact Sciences* **2** (2001) 9–29; also available at http://www.sciamvs.org/v2p9.pdf.
8. L. G. Robinson and D. E. Smith, A newly discovered treatise of Archimedes, *Monist* **19** (1909) 202–230.
9. M. Spivak, *Calculus on Manifolds*, W. A. Benjamin, Menlo Park, CA, 1965.

Department of Mathematics, Harvey Mudd College, Claremont, CA 91711
njp@math.hmc.edu

On Polynomial Rings with a Goldbach Property

Paul Pollack

Abstract. David Hayes observed in 1965 that when $R = \mathbf{Z}$, every element of $R[T]$ of degree $n \geq 1$ is a sum of two irreducibles in $R[T]$ of degree n. We show that this result continues to hold for any Noetherian domain R with infinitely many maximal ideals.

It appears that David Hayes [**5**] was the first to observe the following polynomial analogue of the celebrated Goldbach conjecture: If $R = \mathbf{Z}$, then

> every element of $R[T]$ of degree $n \geq 1$ can be written as the sum of two irreducibles of degree n. ($\star$)

His proof is a clever application of Eisenstein's irreducibility criterion. Hayes's theorem and its proof were rediscovered by Rattan and Stewart [**10**] (see also [**1**] for some cognate results). Recently Saidak [**11**] and Kozek [**7**] have considered quantitative variants of Hayes's theorem. The latter shows that in a precise sense, for a given monic polynomial $A(T) \in \mathbf{Z}[T]$ of degree $n \geq 2$, almost all (asymptotically 100%) of its representations as a sum of two monic polynomials are such that both summands are irreducible.

In this note we consider a generalization in a different direction. Namely, we investigate which integral domains R have the property ($\star$). In [**5**], Hayes points out that his proof shows that ($\star$) holds whenever R is a principal ideal domain with infinitely many maximal ideals, and so in particular when R is the polynomial ring $F[x]$ with F an arbitrary field. Here we show how to relax the requirement that R be a PID to the much weaker condition that the ideals of R are finitely generated.

doi:10.4169/amer.math.monthly.118.01.071

Theorem 1. *Suppose that R is an integral domain which is Noetherian and has infinitely many maximal ideals. Then R has property* ($\star$).

The condition that R be Noetherian cannot be removed. To illustrate, let R be the ring of all algebraic integers, i.e., the collection of all complex numbers which are roots of some monic polynomial with integer coefficients. It is known that over R, there are no irreducible polynomials of degree $n > 1$; in fact, as is nicely explained in (e.g.) [**8**], every nonconstant polynomial in $R[x]$ can be written as a product of linear factors. However, there are certainly infinitely many maximal ideals of R: indeed, for every (positive) prime p of $\mathbf{Z}$, Zorn's lemma implies the existence of a maximal ideal of R containing (p) (see [**2**, p. 254]), and distinct primes p correspond to distinct maximal ideals. The condition that R contain infinitely many maximal ideals also cannot be dispensed with (e.g., take R to be your favorite algebraically closed field), but can perhaps be relaxed beyond what is obvious from the proof below; it would be interesting to investigate this further.

The proof of Theorem 1 is a nice application of the commutative ring theory seen in an introductory graduate algebra course. As a corollary of the proof (but not Theorem 1 as stated), we have the following:

Theorem 2. *If S is any integral domain, then $R = S[x]$ has property* ($\star$).

In their proof of ($\star$) for $R = \mathbf{Z}$, Hayes as well as Rattan and Stewart appear to use "irreducible" to mean "irreducible over $\mathbf{Q}$"; so, e.g., $2T$ is considered irreducible. Throughout this paper, we use "irreducible" in its usual ring-theoretic sense: an element of $R[T]$ is *irreducible* if it is not a unit and cannot be factored as a product of two nonunits. So (strictly speaking) even in the case $R = \mathbf{Z}$, our result is stronger than that asserted by previous authors.

In what follows, all rings are assumed commutative and with an identity.

1. THE BASIC ARGUMENT. We begin by stating our version of Eisenstein's criterion.

Lemma 3 (Eisenstein's criterion). *Let P be a prime ideal of the integral domain R. Suppose $A(T) = a_nT^n + \cdots + a_1T + a_0 \in R[T]$ is a nonconstant polynomial whose coefficients satisfy the following three conditions:*

(i) *$a_0, a_1, \ldots, a_{n-1}$ are all contained in P,*

(ii) *a_0 is not contained in P^2,*

(iii) *a_n is not contained in P.*

Moreover, suppose that A is a primitive *polynomial, in the sense that*

(iv) *the coefficients a_i generate the unit ideal, i.e., $(a_0, \ldots, a_n) = R$.*

Then A is irreducible over R.

Proof (sketch). The proof follows the familiar argument for Eisenstein's criterion where one passes to the domain R/P; see, e.g., [**2**, p. 611]. Conditions (i)–(iii) guarantee that A has no decomposition of the form $G(T)H(T)$ where $G(T)$ and $H(T)$ are nonconstant. Finally, condition (iv) implies that every constant polynomial dividing A is a unit in R (and so in $R[T]$). ∎

Hayes's argument in [**5**] utilizes a familiar result from the foundations of number theory: If m and n are relatively prime integers, then there is a solution in integers x

and y to the equation $mx + ny = 1$. One can view this as a result about the solvability of simultaneous linear congruences: Given x and y with $mx + ny = 1$, the integer $a = mx$ solves the simultaneous congruences $a \equiv 0 \pmod{m}$ and $a \equiv 1 \pmod{n}$. Conversely, given a solution a to these congruences, we obtain an integral solution of $mx + ny = 1$ by setting $a = mx$ and solving for x and y.

When are we guaranteed the existence of a solution to a system of simultaneous congruences? One answer is given by the Chinese remainder theorem, a ring-theoretic version of which we quote here (for a proof, see, e.g., [**2**, p. 265]). Recall that two ideals I and J of a ring R are said to be *comaximal* if $I + J = R$.

Chinese Remainder Theorem for Rings. *Let R be a ring containing ideals $I_1, \ldots, I_k$. Suppose that for every pair of i and j with $i \neq j$, the ideals I_i and I_j are comaximal. Then the map*

$$R \to R/I_1 \times \cdots \times R/I_k$$
$$r \mapsto (r \bmod I_1, \ldots, r \bmod I_k)$$

is a surjective homomorphism with kernel $I_1 \cap \cdots \cap I_k$. Moreover, $I_1 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$, so that

$$R/(I_1 \cdots I_k) = R/(I_1 \cap \cdots \cap I_k) \cong R/I_1 \times \cdots \times R/I_k.$$

To apply this result, one needs to know that certain pairs of ideals are comaximal. An easy observation is that if I is a maximal ideal and J is an ideal not contained in I, then I and J are comaximal. (Otherwise $I \subsetneq I + J \subsetneq R$, contradicting the maximality of I.) Apart from this, the only property of comaximality we need is its preservation upon taking powers:

Lemma 4. *Suppose that I and J are comaximal ideals. Then for any positive integers m and n, the ideals I^m and J^n are comaximal.*

Proof. Since I and J are comaximal, one can pick $a \in I$ and $b \in J$ with $a + b = 1$. By the binomial theorem,

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$

If $k \geq m$, the kth term of the sum is divisible by a^m, and so belongs to I^m. If $k < m$, then $m + n - k > n$, and so the kth term is divisible by b^n and therefore belongs to J^n. Hence $1 = (a+b)^{m+n}$ belongs to $I^m + J^n$. Consequently, I^m and J^n are comaximal. ∎

We now prove, by Hayes's method, a somewhat technical general result from which we will deduce both Theorems 1 and 2.

Theorem 5. *Suppose that R is an integral domain possessing distinct maximal ideals P and Q for which the following hold:*

(i) $P^2 \neq P$ *and* $Q^2 \neq Q$,

(ii) $\#R/P > 2$ *and* $\#R/Q > 2$.

Then R has property ($\star$).

Proof. Let $A(T) = \sum_{j=0}^{n} a_j T^j \in R[T]$ be given, where A has degree $n \geq 1$.

Suppose first that $n = 1$, so that $A(T) = a_1 T + a_0$. If $a_1 \neq 1$, then $A(T) = ((a_1 - 1)T + 1) + (T + a_0 - 1)$ is a decomposition of the desired form. If $n = 1$ and $a_1 = 1$, then by a change of variables, we can assume $A(T) = T$. Then picking $r \in R$ with $r \notin \{0, 1\}$, we have the decomposition $T = (rT + 1) + ((1 - r)T - 1)$.

Suppose now that $n \geq 2$. We will find degree-n polynomials $B = \sum_{i=0}^{n} b_i T^i$ and $C = \sum_{i=0}^{n} c_i T^i$ satisfying $A = B + C$, where B and C satisfy the conditions of Eisenstein's criterion (Lemma 3). It is enough to describe how to choose the b_i, since clearly $c_i = a_i - b_i$. Using hypothesis (i), fix $p \in P \setminus P^2$ and $q \in Q \setminus Q^2$. Using the Chinese remainder theorem and Lemma 4, pick the coefficients b_i to satisfy the congruences

$$b_i \equiv 0 \pmod{P}, \quad c_i \equiv 0 \pmod{Q} \quad \text{for } i = 1, 2, \ldots, n-1,$$
$$b_0 \equiv p \pmod{P^2}, \quad c_0 \equiv q \pmod{Q^2},$$
$$b_n \not\equiv 0 \pmod{P}, \quad c_n \not\equiv 0 \pmod{Q}.$$

(Here a congruence on c_i is to be interpreted as a congruence on b_i, via the relation $b_i + c_i = a_i$.) Then B satisfies conditions (i)–(iii) of Lemma 3 with respect to P, and C satisfies these conditions with respect to Q.

To ensure that (iv) is satisfied, we amend the construction somewhat. In addition to the constraints imposed on the b_i above, we add that

$$c_n \not\equiv 0 \pmod{P} \quad \text{and} \quad b_n \not\equiv 0 \pmod{Q};$$

since $\#R/P > 2$ and $\#R/Q > 2$, this is permissible. Fix $b_2, \ldots, b_n$ satisfying all of the congruence conditions specified above. Now choose b_0 to satisfy all the above and the additional congruence

$$b_0 \equiv 1 \pmod{b_n}. \tag{1}$$

To see that this is possible, notice that we now have congruence conditions on b_0 with respect to the moduli P^2, Q^2, and (b_n); since we have specified above that b_n is in neither P nor Q, these three moduli are pairwise comaximal (again, we appeal to Lemma 4). Similarly, we can choose b_1 satisfying all the congruences given above as well as

$$c_1 \equiv 1 \pmod{c_n}. \tag{2}$$

From (1) we have that b_0 and b_n generate the unit ideal, and from (2) we get the same for c_1 and c_n. In particular, we have secured condition (iv) of Lemma 3. ∎

2. PROOF OF THEOREM 1. In this section we show that any Noetherian domain with infinitely many maximal ideals satisfies the hypotheses of Theorem 5 and thus has property ($\star$). The first lemma shows that if R is a Noetherian domain, then condition (i) of Theorem 5 is satisfied for all nonzero P and Q.

Lemma 6. *If R is a Noetherian domain and M is a nonzero maximal ideal, then $M^2 \neq M$.*

Proof. Since R is Noetherian and $M \neq 0$, we can choose nonzero generators $g_1, \ldots, g_k$ for M, where k is a positive integer. Suppose that $M^2 = M$. Since each

$g_i \in M = M^2$, we can write

$$g_i = \sum_{j=1}^{k} m_{ij} g_j \quad \text{for} \quad 1 \le i \le k, \quad \text{where each} \quad m_{ij} \in M.$$

The matrix $(m_{ij}) - \mathrm{Id}$ kills the column vector $[g_1, \ldots, g_k]^T$. But the determinant of this matrix is congruent to $\pm 1 \pmod{M}$; in particular, it is nonvanishing, so that the matrix is invertible over the quotient field of R. So we have an invertible matrix killing a nonzero vector, an absurdity. ∎

The next lemma shows that if R is a Noetherian domain with infinitely many maximal ideals M, then infinitely many of these M have $\#R/M > 2$.

Lemma 7. *Let R be a Noetherian ring. Then R has only finitely many maximal ideals M with $\#R/M = 2$.*

Clearly Theorem 1 follows from Theorem 5 and Lemmas 6 and 7.

Proof. Let J be the intersection of all maximal ideals M of R for which $\#R/M = 2$. We will show that $S := R/J$ is finite. Hence there are only finitely many ideals of S, and so by the lattice isomorphism theorem, also only finitely many ideals of R containing J. Since each M contains J, we obtain the lemma.

Let us show that S has the property that each of its prime ideals is maximal, with corresponding residue field $\mathbf{Z}/2\mathbf{Z}$. Suppose $x \in R$. Since $R/M \cong \mathbf{Z}/2\mathbf{Z}$, we have that $x^2 - x \in M$ for all M, and hence $x^2 - x \in \cap M = J$. So in $S = R/J$, every element is idempotent (i.e., S is a *Boolean ring*). It follows that the same is true for every quotient of S. In particular, if P is a prime ideal of S, then S/P is a domain where every element satisfies $x^2 - x = 0$; the field $\mathbf{Z}/2\mathbf{Z}$ is the only such domain.

Since S is Noetherian, every ideal of S contains a product of prime ideals [**2**, p. 685]. Applying this to the zero ideal, we find that $(0) = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$ for distinct prime ideals $P_1, \ldots, P_k$ of S. Since each P_i is maximal, the Chinese remainder theorem and Lemma 4 give that $S \cong S/(0) \cong \prod_{i=1}^{k} S/P_i^{e_i}$. Since each element of S is idempotent, none of the rings $S/P_i^{e_i}$ can have nonzero nilpotent elements. This forces $P_i^{e_i} = P_i$ for each i, yielding that $S \cong \prod_{i=1}^{k} S/P_i \cong (\mathbf{Z}/2\mathbf{Z})^k$. ∎

With a bit of effort, one can tweak the proof of Lemma 7 to show that for any Noetherian ring R and any constant B, there are only finitely many ideals I of R with $\#R/I \le B$. This argument is due to Samuel [**12**, p. 292].

3. PROOF OF THEOREM 2. It suffices to verify that $R = S[x]$ satisfies the two conditions of Theorem 5. Fix a maximal ideal M of S and let K denote the field S/M. The ring $K[x]$ contains infinitely many monic irreducibles; one can see this by mimicking the usual Euclidean proof that there are infinitely many primes. Each such irreducible has the form $\overline{I}$, where $I \in S[x]$ is monic, and $\overline{I}$ signifies that the coefficients are reduced modulo M. We have an isomorphism

$$S[x]/(M, I(x)) \cong K[x]/(\overline{I}),$$

which shows that $(M, I(x))$ is a maximal ideal of $S[x]$. Moreover, any two distinct monic irreducibles $\overline{I}$ generate the unit ideal of $K[x]$, and so correspond to distinct maximal ideals $(M, I(x))$ of $S[x]$. Note that the above isomorphism shows that the

quotient of $S[x]$ by $(M, I(x))$ has size > 2 provided either that K is infinite or that $\overline{I}$ has degree at least two; in particular, regardless of the size of K, there are always infinitely many choices of I for which the quotient has size > 2.

Now let monic polynomials I_1 and I_2 in $S[x]$ be chosen so that $\overline{I}_1, \overline{I}_2$ are distinct irreducibles over K, and so that $P := (M, I_1(x))$ and $Q := (M, I_2(x))$ have residue fields with more than two elements. To see that $P^2 \neq P$, note that the elements of P are exactly those elements of $S[x]$ whose reductions modulo M are divisible by $\overline{I}_1$ over K. So every element of P^2, after reduction modulo M, is congruent to a multiple of $\overline{I}_1^2$. Since $\overline{I}_1^2$ does not divide $\overline{I}_1$ in $K[x]$, we see that $I_1 \notin P^2$, so that $P^2 \neq P$. Similarly, $Q^2 \neq Q$.

4. CONCLUDING REMARKS. Theorem 1 does not directly comment on the case when $R = F$ is a field, since in that case (0) is the only maximal ideal. However, if F is the quotient field of a unique factorization domain R satisfying the conditions of Theorem 1, then Gauss's lemma [**2**, p. 303] shows that ($\star$) holds. At a much deeper level, we have the investigations into the Hilbert irreducibility theorem (see [**13**, §4.4]), from which we may deduce that ($\star$) holds if $R = F$ and F is any infinite finitely generated field.

If we ask what happens when $R = F$ is a finite field, then we are quickly led to interesting open problems. Suppose first that $\#F > 2$. Here one expects that every element of $F[T]$ can be written as a sum of two irreducibles, and that for elements of sufficiently large degree (larger than an absolute constant), the summands can be taken to be of the same degree as F. However, for all anyone knows, proving this may be as difficult as resolving the classical Goldbach conjecture. Just as in the classical situation, the expected results *are* known for sums of three irreducibles; see [**6**], [**3**], and the survey [**4**]. The situation is similar for $F = \mathbf{Z}/2\mathbf{Z}$, but now congruence obstructions modulo the primes T and $T + 1$ of $F[T]$ must be taken into account. For a precise discussion of these issues, see [**9**].

ACKNOWLEDGMENTS. The author is supported by an NSF postdoctoral research fellowship. He would also like to thank Carl Pomerance and the referees for suggestions that helped make this note more readable.

REFERENCES

1. C. Betts, Additive and subtractive irreducible monic decompositions in $\mathbf{Z}[x]$, *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998) 86–90.
2. D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley, Hoboken, NJ, 2004.
3. G. Effinger and D. R. Hayes, A complete solution to the polynomial 3-primes problem, *Bull. Amer. Math. Soc. (N.S.)* **24** (1991) 363–369. doi:10.1090/S0273-0979-1991-16035-0
4. G. Effinger, K. Hicks, and G. L. Mullen, Integers and polynomials: Comparing the close cousins $\mathbf{Z}$ and $\mathbf{F}_q[x]$, *Math. Intelligencer* **27**(2) (2005) 26–34. doi:10.1007/BF02985791
5. D. R. Hayes, A Goldbach theorem for polynomials with integral coefficients, *Amer. Math. Monthly* **72** (1965) 45–46. doi:10.2307/2312999
6. ———, The expression of a polynomial as a sum of three irreducibles, *Acta Arith.* **11** (1966) 461–488.
7. M. Kozek, An asymptotic formula for Goldbach's conjecture with monic polynomials in $\mathbf{Z}[x]$, *Amer. Math. Monthly* **117** (2010) 365–369. doi:10.4169/000298910X480856
8. A. Magidin and D. McKinnon, Gauss's lemma for number fields, *Amer. Math. Monthly* **112** (2005) 385–416. doi:10.2307/30037491
9. P. Pollack, The exceptional set in the polynomial Goldbach problem (to appear); also available at http://www.math.illinois.edu/~pppollac/.
10. A. Rattan and C. Stewart, Goldbach's conjecture for $\mathbf{Z}[x]$, *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998) 83–85.
11. F. Saidak, On Goldbach's conjecture for integer polynomials, *Amer. Math. Monthly* **113** (2006) 541–545. doi:10.2307/27641978

12. P. Samuel, About Euclidean rings, *J. Algebra* **19** (1971) 282–301. doi:10.1016/0021-8693(71)90110-4
13. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

Department of Mathematics, University of Illinois at Urbana-Champaign,
1409 West Green Street, Urbana, Illinois 61801
pppollac@illinois.edu

Measurable Functions with a Given Set of Integrability Exponents

Alfonso Villani

Abstract. Given a measure space $(\Omega, \mathcal{A}, \mu)$, it is well known that for every $\mathcal{A}$-measurable function $f : \Omega \to \mathbb{R}$ the set $\mathcal{E}(f) = \{p \in (0, +\infty) : f \in \mathcal{L}^p(\mu)\}$ is always an interval, possibly degenerate, but, in general, it cannot be any given interval $I \subseteq (0, +\infty)$. Thus we consider the problem of characterizing those measure spaces for which $\mathcal{E}(f)$ can be an arbitrary subinterval of $(0, +\infty)$. We show that they are precisely the measure spaces such that there is no inclusion between different $\mathcal{L}^p$ spaces.

1. INTRODUCTION. Let $(\Omega, \mathcal{A}, \mu)$ be a positive measure space and, for each exponent $p \in (0, +\infty)$, let $\mathcal{L}^p(\mu)$ denote, as usual, the vector space of all $\mathcal{A}$-measurable real functions f on Ω for which the integral $\int_\Omega |f|^p \, d\mu$ is finite. Also, for every fixed $\mathcal{A}$-measurable real function f on Ω, let $\mathcal{E}(f)$ denote the set of all *integrability exponents* of f, i.e., the set of all $p \in (0, +\infty)$ such that f lies in $\mathcal{L}^p(\mu)$.

It is well known, as a consequence of Hölder's inequality, that the set $\mathcal{E}(f)$ is always an interval, possibly degenerate (i.e., a singleton or the empty set). This fact suggests, in a natural way, the question of whether $\mathcal{E}(f)$ actually may be equal to any subinterval of $(0, +\infty)$ (see, for instance, [**1**, Exercise 4, p. 71]).

It is promptly realized that for a general measure space this question admits a negative response. Indeed, there are measure spaces $(\Omega, \mathcal{A}, \mu)$—like spaces in which $\mu(\Omega)$ is finite—for which the set-theoretic inclusion $\mathcal{L}^q(\mu) \subseteq \mathcal{L}^p(\mu)$ holds for every $p, q \in (0, +\infty)$, $p < q$, and spaces—like counting measure spaces—for which the reverse inclusion $\mathcal{L}^p(\mu) \subseteq \mathcal{L}^q(\mu)$ is true. In these two cases it is obvious that the interval $\mathcal{E}(f)$ cannot be arbitrary, but must satisfy, if nonempty, the condition $\inf \mathcal{E}(f) = 0$ or $\sup \mathcal{E}(f) = +\infty$, respectively.

On the other hand, there exist measure spaces for which it is true that every real interval $I \subseteq (0, +\infty)$ is the set of the integrability exponents $\mathcal{E}(f)$ of some measurable real function f. The real line $\mathbb{R}$, equipped with the Lebesgue measure, provides an example of such a measure space. This is easily realized, for instance, by considering functions of the form $\alpha \, \mathbf{1}_U \, \varphi + \beta \, \mathbf{1}_{\mathbb{R}\setminus U} \, \psi$ ($\mathbf{1}_E$ denotes the indicator of a set E), where: α and β are nonnegative numbers, U is a measurable bounded neighbourhood of 0, and φ and ψ belong to the class of all functions which are almost-everywhere equal to some negative power either of $|x|$ or of $|x|\big(1 + \big|\log |x|\big|\big)^\gamma$ ($\gamma > 1$).

doi:10.4169/amer.math.monthly.118.01.077

12. P. Samuel, About Euclidean rings, *J. Algebra* **19** (1971) 282–301. doi:10.1016/0021-8693(71)90110-4
13. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

Department of Mathematics, University of Illinois at Urbana-Champaign,
1409 West Green Street, Urbana, Illinois 61801
pppollac@illinois.edu

Measurable Functions with a Given Set of Integrability Exponents

Alfonso Villani

Abstract. Given a measure space $(\Omega, \mathcal{A}, \mu)$, it is well known that for every $\mathcal{A}$-measurable function $f : \Omega \to \mathbb{R}$ the set $\mathcal{E}(f) = \{p \in (0, +\infty) : f \in \mathcal{L}^p(\mu)\}$ is always an interval, possibly degenerate, but, in general, it cannot be any given interval $I \subseteq (0, +\infty)$. Thus we consider the problem of characterizing those measure spaces for which $\mathcal{E}(f)$ can be an arbitrary subinterval of $(0, +\infty)$. We show that they are precisely the measure spaces such that there is no inclusion between different $\mathcal{L}^p$ spaces.

1. INTRODUCTION. Let $(\Omega, \mathcal{A}, \mu)$ be a positive measure space and, for each exponent $p \in (0, +\infty)$, let $\mathcal{L}^p(\mu)$ denote, as usual, the vector space of all $\mathcal{A}$-measurable real functions f on Ω for which the integral $\int_\Omega |f|^p \, d\mu$ is finite. Also, for every fixed $\mathcal{A}$-measurable real function f on Ω, let $\mathcal{E}(f)$ denote the set of all *integrability exponents* of f, i.e., the set of all $p \in (0, +\infty)$ such that f lies in $\mathcal{L}^p(\mu)$.

It is well known, as a consequence of Hölder's inequality, that the set $\mathcal{E}(f)$ is always an interval, possibly degenerate (i.e., a singleton or the empty set). This fact suggests, in a natural way, the question of whether $\mathcal{E}(f)$ actually may be equal to any subinterval of $(0, +\infty)$ (see, for instance, [**1**, Exercise 4, p. 71]).

It is promptly realized that for a general measure space this question admits a negative response. Indeed, there are measure spaces $(\Omega, \mathcal{A}, \mu)$—like spaces in which $\mu(\Omega)$ is finite—for which the set-theoretic inclusion $\mathcal{L}^q(\mu) \subseteq \mathcal{L}^p(\mu)$ holds for every $p, q \in (0, +\infty)$, $p < q$, and spaces—like counting measure spaces—for which the reverse inclusion $\mathcal{L}^p(\mu) \subseteq \mathcal{L}^q(\mu)$ is true. In these two cases it is obvious that the interval $\mathcal{E}(f)$ cannot be arbitrary, but must satisfy, if nonempty, the condition $\inf \mathcal{E}(f) = 0$ or $\sup \mathcal{E}(f) = +\infty$, respectively.

On the other hand, there exist measure spaces for which it is true that every real interval $I \subseteq (0, +\infty)$ is the set of the integrability exponents $\mathcal{E}(f)$ of some measurable real function f. The real line $\mathbb{R}$, equipped with the Lebesgue measure, provides an example of such a measure space. This is easily realized, for instance, by considering functions of the form $\alpha \, \mathbf{1}_U \, \varphi + \beta \, \mathbf{1}_{\mathbb{R}\setminus U} \, \psi$ ($\mathbf{1}_E$ denotes the indicator of a set E), where: α and β are nonnegative numbers, U is a measurable bounded neighbourhood of 0, and φ and ψ belong to the class of all functions which are almost-everywhere equal to some negative power either of $|x|$ or of $|x|\big(1 + \big|\log |x|\big|\big)^\gamma$ ($\gamma > 1$).

doi:10.4169/amer.math.monthly.118.01.077

The aim of this note is to point out that every measure space with the property that there is no inclusion between different $\mathcal{L}^p$ spaces actually behaves just like $\mathbb{R}$ with the Lebesgue measure. More explicitly, we have the following theorem, from which the previous assertion readily follows.

Theorem. *Let a measure space $(\Omega, \mathcal{A}, \mu)$ have the property that the family $\mathcal{A}'$ of all sets $E \in \mathcal{A}$ such that $0 < \mu(E) < +\infty$ is nonempty and satisfies both the following conditions:*

$$\inf_{E \in \mathcal{A}'} \mu(E) = 0, \tag{1}$$

$$\sup_{E \in \mathcal{A}'} \mu(E) = +\infty. \tag{2}$$

Then for every interval $I \subseteq (0, +\infty)$ (possibly degenerate), there exist $\mathcal{A}$-measurable real functions f on Ω such that $\mathcal{E}(f) = I$.

Indeed, by the characterizations of the inclusion $\mathcal{L}^p(\mu) \subseteq \mathcal{L}^q(\mu)$ given in [**2**], we know that the occurrence of both conditions (1) and (2) is actually equivalent to the assumption $\mathcal{L}^p(\mu) \nsubseteq \mathcal{L}^q(\mu)$ for every $p, q \in (0, +\infty)$, $p \neq q$. Thus, we have the following corollary.

Corollary. *Let $(\Omega, \mathcal{A}, \mu)$ be a measure space such that no inclusion $\mathcal{L}^p(\mu) \subseteq \mathcal{L}^q(\mu)$ holds for different exponents $p, q \in (0, +\infty)$. Then for every interval $I \subseteq (0, +\infty)$ (possibly degenerate), there exist $\mathcal{A}$-measurable real functions f on Ω such that $\mathcal{E}(f) = I$.*

As a matter of fact, we will see in the final remark that the same argument used to prove the above theorem shows that in every measure space the interval $\mathcal{E}(f)$ can be arbitrary, apart from the constraints $\inf \mathcal{E}(f) = 0$ or $\sup \mathcal{E}(f) = +\infty$ deriving from the possible inclusions between different $\mathcal{L}^p$ spaces.

2. TECHNICAL LEMMATA AND THE PROOF OF THE THEOREM. To prove the theorem stated above we need two simple lemmas on numerical series.

Lemma 1. *Let $\{x_n\}$ be a decreasing sequence of positive numbers, with $\lim_{n\to\infty} x_n = 0$. Then the series*

$$\sum_{n=1}^{\infty} \frac{1}{x_n}(x_n - x_{n+1}) \tag{3}$$

diverges.

Proof. We distinguish two possibilities.

First, suppose that we have $x_{n+1}/x_n \leq 1/2$ for infinitely many n. Then, owing to the equivalence

$$\frac{x_{n+1}}{x_n} \leq \frac{1}{2} \Longleftrightarrow \frac{1}{x_n}(x_n - x_{n+1}) = 1 - \frac{x_{n+1}}{x_n} \geq \frac{1}{2},$$

it is apparent that the series (3) diverges.

Now suppose that $x_{n+1}/x_n > 1/2$ for all sufficiently large n. Then, having in mind the implication

$$\frac{x_{n+1}}{x_n} > \frac{1}{2} \Longrightarrow \frac{1}{x_n}(x_n - x_{n+1}) \geq \frac{1}{2x_{n+1}}(x_n - x_{n+1}),$$

and observing that, since $1/x$ is a decreasing function, we have

$$\sum_{n=1}^{\infty} \frac{1}{x_{n+1}}(x_n - x_{n+1}) \geq \sum_{n=1}^{\infty} \int_{x_{n+1}}^{x_n} \frac{1}{x}\,dx = \int_0^{x_1} \frac{1}{x}\,dx = +\infty,$$

we conclude, by the comparison test, that also in this case the series (3) diverges. ■

Lemma 2 below can be proved in a completely analogous way or, alternatively, can be inferred from Lemma 1 by means of the substitution $x_n = 1/y_n$.

Lemma 2. *Let $\{y_n\}$ be an increasing sequence of positive numbers, with $\lim_{n\to\infty} y_n = +\infty$. Then the series*

$$\sum_{n=1}^{\infty} \frac{1}{y_{n+1}}(y_{n+1} - y_n)$$

diverges.

Now we turn to the theorem.

Proof of the Theorem. We first notice that in order to prove the theorem it is sufficient to show the existence of four nonnegative $\mathcal{A}$-measurable real functions g_0, h_0, g_∞, and h_∞ on Ω such that:

$$\mathcal{E}(g_0) = (0, 1), \qquad \mathcal{E}(h_0) = (0, 1], \qquad \mathcal{E}(g_\infty) = (1, +\infty), \qquad \mathcal{E}(h_\infty) = [1, +\infty).$$

Indeed, once we have got such functions, then, using them and having in mind the obvious remark that for every two nonnegative $\mathcal{A}$-measurable real functions g and h on Ω we have $\mathcal{E}(g + h) = \mathcal{E}(g) \cap \mathcal{E}(h)$, for every interval $I \subseteq (0, +\infty)$ it is easy to construct a function f such that $\mathcal{E}(f) = I$. For instance, to obtain $\mathcal{E}(f) = (0, b)$, or $\mathcal{E}(f) = (a, b]$ $(a, b \in (0, +\infty)$, $a < b)$, or $\mathcal{E}(f) = \emptyset$, it is enough to take $f = g_0^{1/b}$, or $f = g_\infty^{1/a} + h_0^{1/b}$, or $f = g_0 + g_\infty$, respectively. All other cases for the interval I are covered in a similar way.

Now we show that condition (1) allows us to construct the functions g_0 and h_0.

From (1) we get the existence of a sequence $\{E_n\} \subseteq \mathcal{A}'$ satisfying:

$$\mu(E_{n+1}) < \frac{1}{2}\mu(E_n)$$

for $n = 1, 2, \ldots$ and hence:

$$\mu(E_{n+r}) < \left(\frac{1}{2}\right)^r \mu(E_n)$$

for $n, r = 1, 2, \ldots$. Of course, by the ratio test, we also have:

$$\sum_{n=1}^{\infty} \mu(E_n) < +\infty.$$

Letting

$$A_n = E_n \setminus \left(\bigcup_{k=n+1}^{\infty} E_k \right)$$

for $n = 1, 2, \dots$, we obtain another sequence $\{A_n\}$ of measurable sets with the following features: the A_n's are pairwise disjoint, are contained in the corresponding E_n's, so that $\sum_{n=1}^{\infty} \mu(A_n) < +\infty$, and are of positive measure; indeed we have:

$$\begin{aligned} \mu(A_n) &= \mu(E_n) - \mu\left(E_n \cap \left(\bigcup_{k=n+1}^{\infty} E_k \right) \right) \\ &\geq \mu(E_n) - \sum_{k=n+1}^{\infty} \mu(E_k) > \mu(E_n) - \sum_{r=1}^{\infty} \left(\frac{1}{2} \right)^r \mu(E_n) = 0. \end{aligned}$$

Then, we introduce the real sequence $\{x_n\}$, defined by putting

$$x_n = \sum_{k=n}^{\infty} \mu(A_k)$$

for $n = 1, 2, \dots$, so that $\mu(A_n) = x_n - x_{n+1}$ for $n = 1, 2, \dots$, and notice that this sequence is decreasing to zero.

Let us now consider the nonnegative $\mathcal{A}$-measurable real functions g_0, h_0 on Ω defined as follows:

$$g_0 = \sum_{n=1}^{\infty} \frac{1}{x_n} \mathbf{1}_{A_n}, \qquad h_0 = \sum_{n=1}^{\infty} \frac{1}{x_n (1 + \log^2 x_n)} \mathbf{1}_{A_n},$$

and check that for these two functions we have

$$\mathcal{E}(g_0) = (0, 1), \qquad \mathcal{E}(h_0) = (0, 1].$$

In fact, from Lemma 1 it follows that

$$\int_{\Omega} g_0 \, d\mu = \sum_{n=1}^{\infty} \frac{1}{x_n} \mu(A_n) = \sum_{n=1}^{\infty} \frac{1}{x_n} (x_n - x_{n+1}) = +\infty,$$

and hence $1 \notin \mathcal{E}(g_0)$. On the other hand, for every $p \in (0, 1)$, we have

$$\begin{aligned} \int_{\Omega} g_0^p \, d\mu &= \sum_{n=1}^{\infty} \frac{1}{x_n^p} (x_n - x_{n+1}) \leq \sum_{n=1}^{\infty} \int_{x_{n+1}}^{x_n} \frac{1}{x^p} \, dx \\ &= \int_0^{x_1} \frac{1}{x^p} \, dx < +\infty \end{aligned}$$

and thus p lies in $\mathcal{E}(g_0)$. This shows that $\mathcal{E}(g_0) = (0, 1)$.

Turning to h_0, we first observe that, owing to the inequality $0 \leq h_0 \leq g_0$, we have $(0, 1) \subseteq \mathcal{E}(h_0)$. Next we show that $1 \in \mathcal{E}(h_0)$; indeed, using the fact that

$1/(x(1+\log^2 x))$ is a decreasing function, we have:

$$\begin{aligned}\int_\Omega h_0\,d\mu &= \sum_{n=1}^{\infty} \frac{1}{x_n(1+\log^2 x_n)}(x_n - x_{n+1}) \\ &\le \sum_{n=1}^{\infty} \int_{x_{n+1}}^{x_n} \frac{1}{x(1+\log^2 x)}\,dx = \int_0^{x_1} \frac{1}{x(1+\log^2 x)}\,dx \\ &= \arctan(\log x_1) + \frac{\pi}{2} < +\infty.\end{aligned}$$

Finally, we prove that no exponent $p > 1$ belongs to $\mathcal{E}(h_0)$. To see this, remember that

$$\sum_{n=1}^{\infty} \frac{1}{x_n}(x_n - x_{n+1}) = +\infty$$

and observe that

$$\lim_{n\to\infty} \frac{\frac{1}{x_n^p(1+\log^2 x_n)^p}(x_n - x_{n+1})}{\frac{1}{x_n}(x_n - x_{n+1})} = \lim_{n\to\infty} \frac{x_n^{1-p}}{(1+\log^2 x_n)^p} = +\infty;$$

thus, by the comparison test, we also have

$$\int_\Omega h_0^p\,d\mu = \sum_{n=1}^{\infty} \frac{1}{x_n^p(1+\log^2 x_n)^p}(x_n - x_{n+1}) = +\infty.$$

To complete the proof of the Theorem, we show that, using condition (2), we can construct the functions g_∞ and h_∞.

Using (2) we can construct a sequence $\{B_n\}$ of pairwise disjoint measurable sets such that:

$$1 \le \mu(B_n) < +\infty$$

for $n = 1, 2, \dots$ (select, by (2), a sequence $\{F_n\} \subseteq \mathcal{A}'$ such that $\mu(F_1) \ge 1$ and $\mu(F_{n+1}) \ge \mu(F_1) + \cdots + \mu(F_n) + 1$ for $n = 1, 2, \dots$, and put $B_1 = F_1$ and $B_{n+1} = F_{n+1} \setminus (F_1 \cup \cdots \cup F_n)$). Then, letting

$$y_n = \mu(B_1) + \cdots + \mu(B_n)$$

for $n = 1, 2, \dots$, so that $y_{n+1} - y_n = \mu(B_{n+1})$ for $n = 1, 2, \dots$, we get an increasing sequence of positive numbers such that $\lim_{n\to\infty} y_n = +\infty$. At this point we define

$$g_\infty = \sum_{n=1}^{\infty} \frac{1}{y_{n+1}}\,\mathbf{1}_{B_{n+1}}, \qquad h_\infty = \sum_{n=1}^{\infty} \frac{1}{y_{n+1}(1+\log^2 y_{n+1})}\,\mathbf{1}_{B_{n+1}}$$

and, with the aid of Lemma 2, are able to show that these two nonnegative $\mathcal{A}$-measurable functions satisfy:

$$\mathcal{E}(g_\infty) = (1, +\infty), \qquad \mathcal{E}(h_\infty) = [1, +\infty).$$

The details of this check are very similar to those of the previous argument, regarding g_0 and h_0, and so they are left to the reader. ∎

Remark. Notice that we have been able to construct the functions g_0 and h_0 only on the basis of condition (1). Thus, having in mind the results of [**2**], we can conclude that, if the measure space $(\Omega, \mathcal{A}, \mu)$ has the property that the strict inclusion $\mathcal{L}^q(\mu) \subsetneq \mathcal{L}^p(\mu)$ holds for $p, q \in (0, +\infty)$, $p < q$, then, for every nonempty interval $I \subseteq (0, +\infty)$ such that $\inf I = 0$, there are $\mathcal{A}$-measurable functions $f : \Omega \to \mathbb{R}$ such that $\mathcal{E}(f) = I$. Moreover, if we want to get $\mathcal{E}(f) = \emptyset$ in this case, we can still do so by defining f only by means of the sets A_n's, namely: $f = \sum_{n=1}^{\infty} c_n \mathbf{1}_{A_n}$, where $\{c_n\}$ is a suitable sequence of real numbers (e.g., $c_n = \exp\left(1/\mu(A_n)\right)$).

Likewise, since the existence of g_∞ and h_∞ is proved using only condition (2), we have that, if the space $(\Omega, \mathcal{A}, \mu)$ is such that $\mathcal{L}^p(\mu) \subsetneq \mathcal{L}^q(\mu)$ for every $p, q \in (0, +\infty)$, $p < q$, then every interval $I \subseteq (0, +\infty)$ satisfying $\sup I = +\infty$ is the set of the integrability exponents of some $\mathcal{A}$-measurable real function f.

REFERENCES

1. W. Rudin, *Real and Complex Analysis*, 3rd ed., McGraw Hill, New York, 1987.
2. A. Villani, Another note on the inclusion $L^p(\mu) \subset L^q(\mu)$, *Amer. Math. Monthly* **92** (1985) 485–487. doi:10.2307/2322503

Dipartimento di Matematica e Informatica, V.le A. Doria 6, 95125, Catania, Italy
villani@dmi.unict.it
http://www.dmi.unict.it/~villani

Operator Reverse Monotonicity of the Inverse

Alexis Akira Toda

Abstract. In statistics and econometrics, the equivalence between matrix inequalities $A \geq B \iff B^{-1} \geq A^{-1}$ is used to obtain a lower bound on the variance matrix, where A, B are symmetric and positive definite. The same property holds for linear operators on Hilbert spaces that are bijective, self-adjoint, and positive definite. I give a short and elementary proof of this fact.

Let H be a Hilbert space. In this note every operator $A : H \to H$ is self-adjoint, that is, $\langle Ax, y\rangle = \langle x, Ay\rangle$ for all $x, y \in H$. An operator A is positive definite if $\langle x, Ax\rangle > 0$ for all $x \neq 0$, and it is positive semidefinite if $\langle x, Ax\rangle \geq 0$ for all $x \in H$. We write $A \succ O$ to indicate that A is positive definite, and $A \succeq O$ to indicate that it is positive semidefinite. We define a partial order by $A \succeq B \iff A - B \succeq O$.

Theorem. *Let $A, B : H \to H$ be bijective, self-adjoint, and positive definite. Then $A \succeq B \iff B^{-1} \succeq A^{-1}$.*

Proof. By symmetry, we only need to show $A \succeq B \Longrightarrow B^{-1} \succeq A^{-1}$.

doi:10.4169/amer.math.monthly.118.01.082

Remark. Notice that we have been able to construct the functions g_0 and h_0 only on the basis of condition (1). Thus, having in mind the results of [**2**], we can conclude that, if the measure space $(\Omega, \mathcal{A}, \mu)$ has the property that the strict inclusion $\mathcal{L}^q(\mu) \subsetneq \mathcal{L}^p(\mu)$ holds for $p, q \in (0, +\infty)$, $p < q$, then, for every nonempty interval $I \subseteq (0, +\infty)$ such that $\inf I = 0$, there are $\mathcal{A}$-measurable functions $f : \Omega \to \mathbb{R}$ such that $\mathcal{E}(f) = I$. Moreover, if we want to get $\mathcal{E}(f) = \emptyset$ in this case, we can still do so by defining f only by means of the sets A_n's, namely: $f = \sum_{n=1}^{\infty} c_n \mathbf{1}_{A_n}$, where $\{c_n\}$ is a suitable sequence of real numbers (e.g., $c_n = \exp\left(1/\mu(A_n)\right)$).

Likewise, since the existence of g_∞ and h_∞ is proved using only condition (2), we have that, if the space $(\Omega, \mathcal{A}, \mu)$ is such that $\mathcal{L}^p(\mu) \subsetneq \mathcal{L}^q(\mu)$ for every $p, q \in (0, +\infty)$, $p < q$, then every interval $I \subseteq (0, +\infty)$ satisfying $\sup I = +\infty$ is the set of the integrability exponents of some $\mathcal{A}$-measurable real function f.

REFERENCES

1. W. Rudin, *Real and Complex Analysis*, 3rd ed., McGraw Hill, New York, 1987.
2. A. Villani, Another note on the inclusion $L^p(\mu) \subset L^q(\mu)$, *Amer. Math. Monthly* **92** (1985) 485–487. doi: 10.2307/2322503

Dipartimento di Matematica e Informatica, V.le A. Doria 6, 95125, Catania, Italy
villani@dmi.unict.it
http://www.dmi.unict.it/~villani

Operator Reverse Monotonicity of the Inverse

Alexis Akira Toda

Abstract. In statistics and econometrics, the equivalence between matrix inequalities $A \geq B \iff B^{-1} \geq A^{-1}$ is used to obtain a lower bound on the variance matrix, where A, B are symmetric and positive definite. The same property holds for linear operators on Hilbert spaces that are bijective, self-adjoint, and positive definite. I give a short and elementary proof of this fact.

Let H be a Hilbert space. In this note every operator $A : H \to H$ is self-adjoint, that is, $\langle Ax, y\rangle = \langle x, Ay\rangle$ for all $x, y \in H$. An operator A is positive definite if $\langle x, Ax\rangle > 0$ for all $x \neq 0$, and it is positive semidefinite if $\langle x, Ax\rangle \geq 0$ for all $x \in H$. We write $A \succ O$ to indicate that A is positive definite, and $A \succeq O$ to indicate that it is positive semidefinite. We define a partial order by $A \succeq B \iff A - B \succeq O$.

Theorem. *Let $A, B : H \to H$ be bijective, self-adjoint, and positive definite. Then $A \succeq B \iff B^{-1} \succeq A^{-1}$.*

Proof. By symmetry, we only need to show $A \succeq B \Longrightarrow B^{-1} \succeq A^{-1}$.

doi:10.4169/amer.math.monthly.118.01.082

Since $B \succ O$, for any $x, y \in H$ we obtain

$$\begin{aligned} 0 &\le \langle y - B^{-1}x, B(y - B^{-1}x)\rangle \\ &= \langle y, By\rangle - \langle y, x\rangle - \langle B^{-1}x, By\rangle + \langle x, B^{-1}x\rangle \\ &= \langle y, By\rangle - 2\,\mathrm{Re}\langle x, y\rangle + \langle x, B^{-1}x\rangle, \end{aligned}$$

so

$$2\,\mathrm{Re}\langle x, y\rangle - \langle y, By\rangle \le \langle x, B^{-1}x\rangle. \tag{1}$$

Since $A \succeq B$, it follows from (1) that

$$2\,\mathrm{Re}\langle x, y\rangle - \langle y, Ay\rangle \le 2\,\mathrm{Re}\langle x, y\rangle - \langle y, By\rangle \le \langle x, B^{-1}x\rangle. \tag{2}$$

Letting $y = A^{-1}x$ in the leftmost expression of (2), we obtain

$$\langle x, A^{-1}x\rangle \le \langle x, B^{-1}x\rangle$$

because A^{-1} is self-adjoint. Since $x \in H$ is arbitrary, we get $B^{-1} \succeq A^{-1}$. ■

The theorem (with $H = \mathbb{R}^n$ and A, B symmetric positive definite matrices) is often applied in statistics and econometrics to establish a lower bound on the variance-covariance matrix.

ACKNOWLEDGMENTS. I would like to thank two anonymous referees for suggestions for improvement and clarification. I am grateful to the Nakajima Foundation, the Cowles Foundation, and Yale University for financial support.

Department of Economics, Yale University, New Haven, CT 06511
alexisakira.toda@yale.edu

PROBLEMS AND SOLUTIONS

Edited by **Gerald A. Edgar, Doug Hensley, Douglas B. West**
with the collaboration of Mike Bennett, Itshak Borosh, Paul Bracken, Ezra A. Brown, Randall Dougherty, Tamás Erdélyi, Zachary Franco, Christian Friesen, Ira M. Gessel, László Lipták, Frederick W. Luttmann, Vania Mascioni, Frank B. Miles, Bogdan Petrenko, Richard Pfiefer, Cecil C. Rousseau, Leonard Smiley, Kenneth Stolarsky, Richard Stong, Walter Stromquist, Daniel Ullman, Charles Vanden Eynden, Sam Vandervelde, and Fuzhen Zhang.

Proposed problems and solutions should be sent in duplicate to the MONTHLY *problems address on the back of the title page. Submitted solutions should arrive at that address before May 31, 2011. Additional information, such as generalizations and references, is welcome. The problem number and the solver's name and address should appear on each solution. An asterisk (*) after the number of a problem or a part of a problem indicates that no solution is currently available.*

PROBLEMS

11544. *Proposed by Max A. Alekseyev, University of South Carolina, Columbia, SC, and Frank Ruskey, University of Victoria, Victoria, BC, Canada.* Prove that if m is a positive integer, then

$$\sum_{k=0}^{m-1} \varphi(2k+1) \left\lfloor \frac{m+k}{2k+1} \right\rfloor = m^2.$$

Here φ denotes the Euler totient function.

11545. *Proposed by Manuel Kauers, Research Institute for Symbolic Computation, Linz, Austria, and Sheng-Lan Ko, National Taiwan University, Taipei, Taiwan.* Find a closed-form expression for

$$\sum_{k=0}^{n} (-1)^k \binom{2n}{n+k} s(n+k,k),$$

where s refers to the (signed) Stirling numbers of the first kind.

11546. *Proposed by Kieren MacMillan, Toronto, Canada, and Jonathan Sondow, New York, NY.* Let d, k, and q be positive integers, with k odd. Find the highest power of 2 that divides $\sum_{n=1}^{2^d k} n^q$.

11547. *Proposed by Francisco Javier García Capitán, I.E.S Álvarez Cubero, Priego de Córdoba, Spain, and Juan Bosco Romero Márquez, University of Valladolid, Spain.* Let the altitude AD of triangle ABC be produced to meet the circumcircle again at E. Let K, L, M, and N be the projections of D onto the lines BA, AC, CE, and EB, and let P, Q, R, and S be the intersections of the diagonals of $DKAL$, $DLCM$, $DMEN$, and $DNBK$, respectively. Let $|XY|$ denote the distance from X to Y, and let α, β, γ be the

doi:10.4169/amer.math.monthly.118.01.084

radian measure of angles BAC, CBA, ACB, respectively. Show that $PQRS$ is a rhombus and that $|QS|^2/|PR|^2 = 1 + \cos(2\beta)\cos(2\gamma)/\sin^2\alpha$.

11548. *Proposed by Cezar Lupu (student), University of Bucharest, Bucharest, Romania, and Tudorel Lupu, Decebal High School, Constanta, Romania.* Let f be a twice-differentiable real-valued function with continuous second derivative, and suppose that $f(0) = 0$. Show that

$$\int_{-1}^{1} (f''(x))^2\,dx \geq 10\left(\int_{-1}^{1} f(x)\,dx\right)^2.$$

11549. *Proposed by Marian Tetiva, National College "Gheorghe Roşca Codreanu," Bîrlad, Romania.* Determine all continuous functions f on $\mathbb{R}$ such that for all x,

$$f(f(f(x))) - 3f(x) + 2x = 0.$$

11550. *Proposed by Stefano Siboni, University of Trento, Trento, Italy.* Let G be a point inside triangle ABC. Let α, β, γ be the radian measures of angles BGC, CGA, AGB, respectively. Let O, R, S be the triangle's circumcenter, circumradius, and area, respectively. Let $|XY|$ be the distance from X to Y. Prove that

$$|GA|\cdot|GB|\cdot|GC|(|GA|\sin\alpha + |GB|\sin\beta + |GC|\sin\gamma) = 2S(R^2 - |GO|^2).$$

SOLUTIONS

A Consequence of Wolstenholme's Theorem

11382 [2008, 665]. *Proposed by Roberto Tauraso, Università di Roma "Tor Vergata," Rome, Italy.* For $k \geq 1$, let H_k be the kth harmonic number, defined by $H_k = \sum_{j=1}^{k} 1/j$. Show that if p is prime and $p > 5$, then

$$\sum_{k=1}^{p-1} \frac{H_k^2}{k} \equiv \sum_{k=1}^{p-1} \frac{H_k}{k^2} \pmod{p^2}.$$

(Two rationals are congruent modulo d if their difference can be expressed as a reduced fraction of the form da/b with b relatively prime to a and d.)

Solution by Douglas B. Tyler, Raytheon, Torrance, CA. Let $S = \{1, 2, \ldots, p-1\}$. All summations are over $k \in S$. Note that

$$3\left(\sum \frac{H_k}{k^2} - \sum \frac{H_k^2}{k}\right) = \sum \left(H_k - \frac{1}{k}\right)^3 - \sum H_k^3 + \sum \frac{1}{k^3}.$$

Since $H_k - \frac{1}{k} = H_{k-1}$, the right side telescopes to $-H_{p-1}^3 + \sum \frac{1}{k^3}$. Since $p > 3$, it suffices to show that H_{p-1}^3 and $\sum \frac{1}{k^3}$ are both congruent to 0 modulo p^2.

Modulo p, the reciprocals of the elements of S form a permutation of S, so $H_{p-1} = \sum k^{-1} \equiv \sum k = \frac{1}{2}p(p-1) \equiv 0 \pmod{p}$. Thus $H_{p-1}^3 \equiv 0 \bmod p^3$.

By reversing the index in one copy of the sum, modulo p^2 we have

$$2\sum \frac{1}{k^3} = \sum \frac{p^3 - 3p^2k + 3pk^2}{k^3(p-k)^3} \equiv \sum \frac{3pk^2}{k^3(p-k)^3} = 3p\sum \frac{1}{k(p-k)^3}.$$

It remains to show $\sum \frac{1}{k(p-k)^3} \equiv 0 \bmod p$. This sum is congruent to $\sum \frac{1}{-k^4}$. Modulo p, the reciprocals of the fourth powers of S form a permutation of the fourth powers of S, so $\sum \frac{1}{k^4} = \sum k^4 \bmod p$. It is well known that the sum over S of the rth powers is a polynomial of degree $r+1$ in p. In fact, $\sum k^4 = \frac{p^5}{5} - \frac{p^4}{2} + \frac{p^3}{3} - \frac{p}{30}$, easily proved by induction. With no constant term, the polynomial has value $0 \bmod p$ when $p > 5$.

Editorial comment. That $H_{p-1} \equiv 0 \bmod p$, and that $\sum_{k=1}^{p-1} k^{-3} \equiv 0 \bmod p^2$, could have been established by an appeal to Wolstenholme's theorem.

Also solved by R. Chapman (U. K.), P. Corn, P. P. Dályay (Hungary), Y. Dumont (France), O. Kouba (Syria), J. H. Lindsey II, O. P. Lossers (Netherlands), M. A. Prasad (India), N. C. Singer, A. Stadler (Switzerland), R. Stong, M. Tetiva (Romania), GCHQ Problem Solving Group (U. K.), and the proposer.

Groups with Arbitrarily Sparse Squares

11388 [2008, 758]. *Proposed by M. Farrokhi D.G., University of Tsukuba, Tsukuba Ibakari, Japan.* Given a group G, let G^2 denote the set of all squares in G. Show that for each natural number n there exists a finite group G such that the cardinality of G is n times the cardinality of G^2.

Solution by Richard Stong, San Diego, CA. When G has odd order, every element is a square, so $|G|/|G^2| = 1$. For order 2, only the identity is a square, so $|G|/|G^2| = 2$.

Let p be an odd prime, and let s be the largest integer such that $p \equiv 1 \bmod 2^s$. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of nonzero congruence classes modulo p is cyclic of order $p-1$ and has an element a of order 2^s. Hence $a^{2^{s-1}} \equiv -1 \bmod p$, and no smaller power of a satisfies this congruence. Now consider the group H_p with presentation

$$H_p = \langle x, y : x^p = y^{2^{s+1}} = 1,\ yxy^{-1} = x^a \rangle.$$

Every element of this group can be written uniquely as $x^b y^c$ for $b \in \mathbb{Z}/p\mathbb{Z}$ and $c \in \mathbb{Z}/2^{s+1}\mathbb{Z}$, and the multiplication law is

$$x^{b_1} y^{c_1} x^{b_2} y^{c_2} = x^{b_1 + a^{c_1} b_2} y^{c_1 + c_2}$$

with operations in the exponents of x and y taken mod p and mod 2^{s+1}, respectively. Setting $b = b_1 = b_2$ and $c = c_1 = c_2$, we see that the squares in H_p are precisely the elements of the form $x^{b(1+a^c)} y^{2c}$. Hence, if $x^\beta y^\gamma = (x^b y^c)^2$, then γ is even and either $c = \gamma/2$ or $c = \gamma/2 + 2^s$. Since $a^{2^s} = 1$, both possibilities give the same value of $1 + a^c$. If $\gamma \neq 2^s$ (that is, if $c \neq 2^{s-1}$), then $1 + a^c$ is nonzero and all choices of β give squares. If $\gamma = 2^s$, then $c = \pm 2^{s-1}$ and $1 + a^{c_2} = 0$, so only $\beta = 0$ gives a square. Thus $|H_p^2| = (2^s - 1)p + 1$. Note that $p \equiv 1 + 2^s \bmod 2^{s+1}$, so $(2^s - 1)p + 1$ is indeed a multiple of 2^{s+1}. Hence

$$\frac{|H_p|}{|H_p^2|} = \frac{2^{s+1} p}{(2^s - 1)p + 1} = \frac{p}{r_p},$$

where r_p is the integer $((2^s - 1)p + 1)/(2^{s+1})$ and $r_p < p$.

If G and H are finite, then the set of squares in $G \times H$ is $G^2 \times H^2$, so

$$\frac{|G \times H|}{|(G \times H)^2|} = \frac{|G|}{|G^2|} \cdot \frac{|H|}{|H^2|}.$$

The result now follows by induction on n. We have given examples for $n = 1$ and $n = 2$, so consider $n \geq 3$. When n is even, let $G_{n/2}$ be an example with $|G_{n/2}|/|G_{n/2}^2| =$

$n/2$; now $G_{n/2} \times \mathbb{Z}/2\mathbb{Z}$ is the desired example for G_n. When n is odd, let p be an odd prime divisor of n, let $m = nr_n/p < n$ (with r_n as above), and let G_m be an example with $|G_m|/|G_m^2| = m$. Now $G_m \times H_p$ is the desired example for G_n.

Also solved by A. J. Bevelacqua, R. Martin (Germany), L. Reid, D. B. Tyler, NSA Problems Group, and the proposer.

A Nonexistent Ring

11407 [2009, 82]. *Proposed by Erwin Just (emeritus), Bronx Community College of the City University of New York, New York, NY.* Let p be a prime greater than 3. Does there exists a ring with more than one element (not necessarily having a multiplicative identity) such that for all x in the ring, $\sum_{i=1}^{p} x^{2i-1} = 0$?

Solution by O.P. Lossers, Eindhoven University of Technology, Eindhoven, The Netherlands. We prove that no such ring R exists by showing that the assumption $\sum_{i=1}^{p} x^{2i-1} = 0$ for all x yields $R = \{0\}$, contradicting the hypothesis that $|R| \geq 2$. Multiplying by x^2 yields $\sum_{i=1}^{p} x^{2i+1} = 0$, and then $x^{2p+1} = x$ by subtraction. Now $x^{4p} = x^{2p-1}x^{2p+1} = x^{2p-1}x = x^{2p}$. We conclude that all positive even powers of x^p are equal. Next compute

$$0 = \sum_{i=1}^{p} \left(x^{2p}\right)^{2i-1} = \sum_{i=1}^{p} x^{2(2i-1)p} = px^{2p}.$$

Since $x^{2p+1} = x$, we have $px = px^{2p+1} = \left(px^{2p}\right)x = 0x = 0$. Thus $(x+x)^p = x^p + x^p$. Now

$$2x = (2x)^{2p+1} = 2x[(x+x)^p]^2 = 2x(x^p + x^p)^2 = 2x4x^{2p} = 8x^{2p+1} = 8x.$$

Therefore, $6x = 8x - 2x = 0$, and we already know that $px = 0$. Therefore, $0 = \gcd(6, p)x = x$. Since x is an arbitrary element of R, it follows that $R = \{0\}$.

Also solved by E. P. Amendariz, N. Caro (Colombia), R. Chapman (U. K.), Y. Ge (Austria), D. Grinberg, J. H. Lindsey II, A. Sh. Shabani (Kosova), R. Stong, C. T. Stretch (Ireland), N. Vonessen, FAU Problem Solving Group, NSA Problem Group, and the proposer.

Summing to kth Powers

11408 [2009, 83]. *Proposed by Marius Cavachi, "Ovidius" University of Constanţa, Constanţa, Romania.* Let k be a fixed integer greater than 1. Prove that there exists an integer n greater than 1, and distinct integers $a_1, \ldots, a_n$ all greater than 1, such that both $\sum_{j=1}^{n} a_j$ and $\sum_{j=1}^{n} \varphi(a_j)$ are kth powers of a positive integer. Here φ denotes Euler's totient function.

Solution by C. R. Pranesachar, Indian Institute of Science, Bangalore, India. We first choose a and b such that $2a + 6b = (2k+2)^k$ and $a + 2b = (2k)^k$, both kth powers of integers. Solving the linear system yields $a = 3(2k)^k - (2k+2)^k = 2^k(3k^k - (k+1)^k)$ and $b = \frac{1}{2}((2k+2)^k - 2(2k)^k) = 2^{k-1}((k+1)^k - 2k^k)$. Since $2 < (1 + \frac{1}{k})^k < 3$ for $k > 1$, it follows that a and b are positive integers. Express the even integers $2a$ and $2b$ as sums of distinct positive powers of 2:

$$2a = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_l}, \qquad 1 \leq r_1 < r_2 < \cdots < r_l;$$
$$2b = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_m}, \qquad 1 \leq s_1 < s_2 < \cdots < s_m.$$

Let $a_i = 2^{r_i}$ for $1 \le i \le l$ and $a_{l+j} = 3 \cdot 2^{s_j}$ for $1 \le j \le m$. Let $n = l + m$, and consider $a_1, \ldots, a_n$, which are clearly distinct. Note that $\sum_{j=1}^{n} a_j = 2a + 6b = (2k+2)^k$. Since $\varphi(2^r) = 2^{r-1}$ and $\varphi(3 \cdot 2^r) = 2^r$,

$$\sum_{h=1}^{n} \varphi(a_h) = \sum_{i=1}^{l} 2^{r_i - 1} + \sum_{j=1}^{m} 2^{s_i} = a + 2b = (2k)^k.$$

Editorial comment. The GCHQ Problem Solving Group used distinct powers of 3, distinct numbers of the form $3 \cdot 2^r$, and distinct powers of 2 to show that there are distinct numbers $a_1, \ldots, a_n$, all greater than 1, such that $\sum_{j=1}^{n} a_j = s$ and $\sum_{j=1}^{n} \phi(a_j) = t$, provided that $s/2 < t < 8s/15$.

Also solved by P. P. Dályay (Hungary), A. Stadler (Switzerland), R. Stong, M. Tetiva (Romania), GCHQ Problem Solving Group (U. K.), and the proposer.

An Inequality

11430 [2009, 366]. *Proposed by He Yi, Macao University of Science and Technology, Macao, China.* For real $x_1, \ldots, x_n$, show that

$$\frac{x_1}{1 + x_1^2} + \frac{x_2}{1 + x_1^2 + x_2^2} + \cdots + \frac{x_n}{1 + x_1^2 + \cdots + x_n^2} < \sqrt{n}.$$

Solution by Kenneth F. Andersen, University of Alberta, Edmonton, AB, Canada. Letting $x_0 = 1$, we have

$$\sum_{j=1}^{n} \frac{x_j^2}{(1 + x_1^2 + \cdots + x_j^2)^2} \le \sum_{j=1}^{n} \left[\frac{1}{x_0^2 + x_1^2 + \cdots + x_{j-1}^2} - \frac{1}{x_0^2 + x_1^2 + \cdots + x_j^2} \right]$$

$$= 1 - \frac{1}{1 + x_1^2 + \cdots + x_n^2} < 1.$$

The Cauchy–Schwarz inequality shows that, as required,

$$\sum_{j=1}^{n} \frac{x_j}{1 + x_1^2 + \cdots + x_j^2} \le \left[\sum_{j=1}^{n} 1 \right]^{1/2} \left[\sum_{j=1}^{n} \frac{x_j^2}{(1 + x_1^2 + \cdots + x_j^2)^2} \right]^{1/2} < \sqrt{n}.$$

Editorial comment. This problem is known. (1) It was a Romanian proposal for the IMO 2001; two solutions are on page 676 of *The IMO Compendium* (Springer, 2006). (2) It was part of the Indian Team Selection Test for the 2002 IMO; a solution was published in *Crux Mathematicorum with Mathematical Mayhem* **35** (2009) 98. (3) It was Problem 1242 in *Elementa der Mathematik* **63** (2008) 103.

Also solved by A. Alt, M. S. Ashbaugh & S. G. Saenz (U.S.A. & Chile), R. Bagby, M. Bataille (France), D. Borwein (Canada), P. Bracken, M. Can, R. Chapman (U. K.), H. Chen, L. Csete (Hungary), P. P. Dályay (Hungary), J. Fabrykowski & T. Smotzer, O. Geupel (Germany), J. Grivaux (France), E. Hysnelaj & E. Bojaxhiu (Australia & Albania), Y. H. Kim (Korea), O. Kouba (Syria), J. H. Lindsey II, O. P. Lossers (Netherlands), J. Moreira (Portugal), P. Perfetti (Italy), C. Pohoata (Romania), M. A. Prasad (India), A. Pytel (Poland), H. Ricardo, C. R. & S. Selvaraj, J. Simons (U. K.), A. Stadler (Switzerland), R. Stong, M. Tetiva (Romania), D. Vacaru (Romania), E. I. Verriest, M. Vowe (Switzerland), A. P. Yogananda (India), GCHQ Problem Solving Group (U. K.), Microsoft Research Problems Group, and the proposer.

Shur and Definite

11431 [2009, 336]. *Proposed by Finbarr Holland and Stephen Wills, University College Cork, Cork, Ireland.* A matrix is *Schur invertible* if all its entries are nonzero, and the *Schur inverse* is the matrix obtained by taking the reciprocal of each entry. Show that an $n \times n$ complex matrix A with all entries nonzero has the property that it and its Schur inverse are both nonnegative definite if and only if there are nonzero complex numbers $a_1, \ldots, a_n$ such that for $1 \le j, k \le n$, the (j, k)-entry of A is $a_j\overline{a_k}$.

Solution by Éric Pité, Paris, France. Let A be an $n \times n$ complex matrix with all entries nonzero such that it and its Schur inverse are both nonnegative definite. Such an A is a Gramian matrix, i.e., there exist $v_1, \ldots, v_n \in \mathbb{C}^n$ such that $a_{j,k} = \langle v_j, v_k \rangle$ for all (j, k).

Using the Cauchy-Schwarz inequality, for $1 \le j, k \le n$ we have

$$|a_{j,k}|^2 \le \|v_j\|^2 \|v_k\|^2 = a_{j,j}a_{k,k}.$$

The Schur inverse is also Gramian, so $1/|a_{j,k}|^2 \le 1/(a_{j,j}a_{k,k})$ as well. Hence in all these applications of the Cauchy-Schwarz inequality we have equality. It follows that the vectors $v_1, \ldots, v_n$ are all proportional. Hence we can write $v_j = \overline{a_j}u$ for some common unit vector u and complex numbers $a_1, \ldots, a_n$ and the (j, k)-entry of A is $a_j\overline{a_k}$.

The converse is clear: if y is the vector $(a_1, \ldots, a_n)$, then $A = y\overline{y}^T$ and $v^T Av = |\langle y, v \rangle|^2 \ge 0$, so A is nonnegative definite, and similarly for its Schur inverse.

Also solved by P. Budney, R. Chapman (U. K.), P. P. Dályay (Hungary), N. Grivaux (France), E. A. Herman, O. Kouba (Syria), J. H. Lindsey II, O. P. Lossers (Netherlands), A. Muchlis (Indonesia), R. Stong, M. Tetiva (Romania), Con Amore Problem Group (Denmark), and the proposer.

Interior Evaluation and Boundary Evaluation

11432 [2009, 463]. *Proposed by Marian Tetiva, National College "Gheorghe Roşca Codreanu," Bîrlad, Romania.* Let P be a polynomial of degree n with complex coefficients and with $P(0) = 0$. Show that for any complex α with $|\alpha| < 1$ there exist complex numbers $z_1, \ldots, z_{n+2}$, all of norm 1, such that $P(\alpha) = P(z_1) + \cdots + P(z_{n+2})$.

Solution I by O. P. Lossers, Technical University of Eindhoven, Eindhoven, The Netherlands. We prove something stronger. Given α we prove the existence of $z_1, \ldots, z_{n+2}$ such that $|z_j| = 1$ and $z_1^k + \cdots + z_{n+2}^k = \alpha^k$ for $1 \le k \le n$. Thus, for every polynomial P of degree n with $P(0) = 0$, we have $P(\alpha) = \sum_{j=1}^{n+2} P(z_j)$.

To any list of numbers $(z_1, \ldots, z_{n+2})$ we associate the polynomial Q given by $Q(z) = \prod_{k=1}^{n+2}(z - z_j)$, and numbers π_k given by $\pi_k = \sum_{j=1}^{n+2} z_j^k$. The numbers π_k and the coefficients c_j in the expansion $Q(z) = \sum_{j=0}^{n+2}(-1)^j c_j z^{n+2-j}$ are related by the Newton identities: $c_0 = 1$, and

$$k(-1)^k c_k + \pi_k c_0 - \pi_{k-1}c_1 + \cdots + (-1)^{k-1}\pi_1 c_{k-1} = 0 \quad \text{for } 1 \le k \le n+2.$$

We want $\pi_k = \alpha^k$ for $1 \le k \le n$. This can only happen if $c_1 = \alpha$ and $c_j = 0$ for $2 \le j \le n$. We must therefore choose $Q(z)$ of the form $z^{n+2} - \alpha z^{n+1} + Az + B$. We take $Q(z) = z^{n+2} - \alpha z^{n+1} - \overline{\alpha}z + 1$. With this choice of Q, each z_j satisfies $z^{n+1} = (\overline{\alpha}z - 1)/(z - \alpha)$. The expression on the right side of this equation is the value at z of a Möbius transformation that maps the inside of the unit disk to the outside and vice versa, so $|z_j| = 1$ for $1 \le j \le n + 2$.

Solution II by Richard Stong. We prove something stronger. If k is any integer ≥ 2, then there exist $z_1, \ldots, z_k$ of norm 1 with $P(\alpha) = P(z_1) + \cdots + P(z_k)$. Let $B =$

$\{P(z)\colon |z| = 1\}$ and $F = \{P(z)\colon |z| \le 1\}$. Both sets are closed and bounded, and since P is an open map (L. Ahlfors, *Complex Analysis*, Corollary 1, p. 132), the boundary ∂F of F is a subset of B. Also, F and B are both path connected, since both are the continuous image of a path connected set.

Lemma. *For any $p, q \in F$ there exist $w, z \in B$ such that $p + q = w + z$.*

Proof. Let $m = \frac{1}{2}(p + q)$. It will suffice to show that $B \cap (2m - B) \neq \emptyset$, because given $w \in B \cap (2m - B)$, we make take $z = 2m - w$ and have $w, z \in B$ with $w + z = 2m = p + q$. Observe next that $\partial(2m - F) \subseteq (2m - B)$. Now $\partial(F \cup (2m - F)) \neq \emptyset$. If $\partial F \cap \partial(2m - F) \neq \emptyset$, we are done. Otherwise, after replacing u by $2m - u$ if necessary, we may assume the existence of u such that $u \in \partial F$, $u \notin 2m - F$. Thus $u \in B$, $u \notin 2m - F$, $2m - u \in \partial(2m - F)$, and $2m - u \notin F$. On the other hand, $p \in F \cap (2m - F)$ because $2m - p = q$. Since $2m - F$ is path connected, there is a path in $2m - F$ from $2m - u$ to p. Since $2m - u \notin F$ and $p \in F$, there is a v along the path such that $v \in \partial F$, whence $v \in (2m - F) \cap B$. Finally, since B too is path connected, there is a path in B from $u \notin 2m - F$ to v, and it contains a w in $\partial(2m - F)$. This puts $w \in (2m - B) \cap B$. ∎

Now taking $p = P(\alpha)$ and $q = P(0) = 0$ in the lemma, we get $P(\alpha) = P(z_1) + P(w)$, where z_1 and w have norm 1. Next, taking $p = P(w)$ and $q = 0$, we get $P(w) = P(z_2) + P(w')$, where again z_2 and w' have norm 1. Continuing in this way, we see that for any $k \ge 2$ we can write $P(\alpha) = P(z_1) + \cdots + P(z_k)$ with all z_j of norm 1.

Also solved by R. Chapman (U. K.), O. Kouba (Syria), J. Schaer (Canada), J. Simons (U. K.), GCHQ Problem Solving Group (U. K.), and the proposer.

A Triangle Inequality

11435 [2009, 463]. *Proposed by Panagiote Ligouras, Leonardo da Vinci High School, Noci, Italy.* In a triangle T, let a, b, and c be the lengths of the sides, r the inradius, and R the circumradius. Show that

$$\frac{a^2bc}{(a+b)(a+c)} + \frac{b^2ca}{(b+c)(b+a)} + \frac{c^2ab}{(c+a)(c+b)} \le \frac{9}{2}rR.$$

Solution by Chip Curtis, Missouri State Southern University, Joplin, MO. Write K for the area of T and s for the semiperimeter. Then $r = K/s$ and $R = abc/(4K)$, so $rR = abc/(4s) = abc/(2(a + b + c))$. The claimed inequality is equivalent to

$$abc\left[\frac{a}{(a+b)(a+c)} + \frac{b}{(b+c)(b+a)} + \frac{c}{(c+a)(c+b)}\right] \le \frac{9abc}{4(a+b+c)}$$

which simplifies to $(a^2b + a^2c + b^2a + b^2c + c^2a + c^2b) \ge 6abc$. In this last form, it follows from the AM–GM inequality.

Editorial comment. The problem was published with a misprint: 9/4 in place of 9/2. We regret the oversight.

Also solved by A. Alt, R. Bagby, M. Bataille (France), E. Braune (Austria), M. Can, R. Chapman (U. K.), L. Csete (Hungary), P. P. Dályay (Hungary), S. Dangc, V. V. García (Spain), M. Goldenberg & M. Kaplan, M. R. Gopal, D. Grinberg, J.-P. Grivaux (France), S. Hitotumatu (Japan), E. Hysnelaj & E. Bojaxhiu (Australia & Albania), B.-T. Iordache (Romania), O. Kouba (Syria), K.-W. Lau (China), J. H. Lindsey II, O. P. Lossers (Netherlands), M. Mabuchi (Japan), J. Minkus, D. J. Moore, R. Nandan, M. D. Nguyen (Vietnam), P. E. Nuesch

(Switzerland), J. Oelschlager, G. T. Prăjitură, C. R. Pranesachar (India), J. Rooin & A. Asadbeygi (Iran), S. G. Saenz (Chile), I. A. Sakmar, C. R. & S. Selvaraj, J. Simons (U. K.), E. A. Smith, S. Song (Korea), A. Stadler (Switzerland), R. Stong, W. Szpunar-Łojasiewicz, R. Tauraso (Italy), M. Tetiva (Romania), B. Tomper, E. I. Verriest, Z. Vörös (Hungary), M. Vowe (Switzerland), J. B. Zacharias, Con Amore Problem Group (Denmark), GCHQ Problem Solving Group (U. K.), Microsoft Research Problems Group, and the proposer.

Partition by a Function

11439 [2009, 547]. *Proposed by Stephen Herschkorn, Rutgers University, New Brunswick, NJ.* Let f be a continuous function from $[0, 1]$ into $[0, 1]$ such that $f(0) = f(1) = 0$. Let G be the set of all (x, y) in the square $[0, 1] \times [0, 1]$ so that $f(x) = f(y)$.

(**a**) Show that G need not be connected.

(**b**)* Must $(0, 1)$ and $(0, 0)$ be in the same connected component of G?

Composite solution by Armenak Petrosyan (student), Yerevan State University, Yerevan, Armenia, and Richard Stong, San Diego, CA.

(**a**) Let f be the piecewise linear function whose graph joins the points $(0, 0)$, $(1/6, 1)$, $(1/3, 1/2)$, $(1/2, 1)$, $(2/3, 0)$, $(5/6, 1/2)$, and $(1, 0)$. This f has a strict local minimum at $x = 1/3$ and a strict local maximum at $x = 5/6$ with $f(1/3) = f(5/6) = 1/2$. Thus $(1/3, 5/6)$ is an isolated point of G, so G is not connected.

(**b**) We claim that $(0, 1)$ and $(0, 0)$ are in the same component of G. Let $D = \{(x, x)\colon\ 0 \le x \le 1\}$. If $(0, 1)$ and D are in different components of G, then there are disjoint open sets U, V in the square $S = [0, 1] \times [0, 1]$ such that $(0, 1) \in U$, $D \subset V$, and $G \subset U \cup V$. Let $C_1 = G \cap U$ and $C_2 = G \cap V$. Since C_1 and C_2 are both open in G, they are also both closed, hence compact. We may further assume that C_1 lies entirely above the line $y = x$. For each point $p \in C_1$, choose an open square centered at p with sides parallel to the axes, not lying along any edge of S, and with closure disjoint from C_2. These squares form an open cover of C_1, so there is a finite subcover. Let F be the union of the closed squares corresponding to this subcover. Let F' be the intersection of S with the boundary of F. Now F is closed, lies above $y = x$, and contains C_1 in its interior and C_2 in its complement. Also, F' consists of line segments. From F' we define a graph H whose vertices are the intersections of these line segments with each other or with the boundary of S; vertices of H are adjacent when connected by a segment contained in F'. Vertices have degree 1, 2, or 4, with degree 1 only on the boundary of S.

Since $(0, 1) \in F$ and $D \cap F = \emptyset$, toggling membership in F at vertices of H along the left edge of S implies that the number of vertices of degree 1 on the left edge of S is odd, and similarly along the top edge. Since each component of a graph has an even number of vertices of odd degree, some component contains vertices of degree 1 on both of these edges, and hence H must contain at least one path joining these edges. However, the function ϕ on S given by $\phi(x, y) = f(x) - f(y)$ is continuous, nonnegative on the top edge and nonpositive on the left edge. Thus some point (x, y) on this path must have $\phi(x, y) = 0$. Such a point lies in G, contrary to our construction. Thus $(0, 1)$ and D lie in the same component of G.

Editorial comment. A second approach to solving part (**b**) builds from the case where f is piecewise linear (essentially the "Two Men of Tibet" problem; see P. Zeitz, *The Art and Craft of Problem Solving*, John Wiley & Sons, 1999).

Also solved by D. Ray, V. Rutherfoord, Szeged Problem Solving Group "Fejéntaláltuka" (Hungary). Part (**a**) solved by R. Chapman (U. K.), W. J. Cowieson, M. D. Meyerson, J. H. Nieto (Venezuela), A. Pytel (Poland), Fisher Problem Solving Group, GCHQ Problem Solving Group (U. K.), and Microsoft Research Problems Group.

REVIEWS

Edited by **Jeffrey Nunemacher**
Mathematics and Computer Science, Ohio Wesleyan University, Delaware, OH 43015

What's Math Got To Do With It? by Jo Boaler. Viking Press, London, England, 2008, xii + 273 pp., ISBN 978-0-670-01952-6, $24.95

Reviewed by **Virginia McShane Warfield**

Three years in the middle of a major battleground of the Math Wars provide a fair amount of involuntary education, much of it applicable well beyond the maelstrom. Most notably, they provide a five-credit course on the subject of communication: communication as a weapon of mass destruction; communication as a political art; communication as a war victim; and especially communication as an absolute necessity.

Interest in communication is not a novelty for me. As a born and bred member of the mathematics community who followed conventional grooves up through a degree in stochastic control theory before being drawn more and more into issues of mathematics education, I have thoroughly enjoyed being in a position to build bridges between mathematics and mathematics education. Most mathematics educators are aware of the value to their field of deeper knowledge of mathematics, and most mathematicians are aware (or can be made so) that more than mathematical knowledge alone is involved in producing the kind of confidence and reasoning ability that we look for in addition to basic knowledge in our students. Providing connections among such folks has been a joy.

This idyllic state ended with the arrival on the scene of people whose agendas preclude listening. This is profoundly jarring for an innocent denizen of academia, not only because it is disturbing to know that any attempt at communication with them will be twisted into a weapon, but, worse, because their success in polarization has seriously disrupted all other communication. Currently the attack, which has reached lawsuit level, is an attempt to prevent a school district in Washington from adopting a textbook series whose major virtue in the eyes of a hard-working selection committee is that it supports both traditional and nontraditional teaching. Exploring the issue led me into a conversation with a colleague whom I both like and trust, and thence to the discovery that what each of us saw while reading the same words in the same textbook was wildly dissimilar to what the other saw. Earlier this might have led to an interesting and lively debate; now it is just too loaded. It did lead to a long discussion with another friend, whose response was to wonder why he was only hearing me talk about teachers and mathematicians—how do students feel about all this? Since student response and engagement are the heart and center of our efforts, I was nonplussed.

Fortunately even when rendered speechless by the amount that I want to convey and can't, I now have a recourse, and until I run out of copies of Jo Boaler's *What's Math Got to Do with It?* I won't be completely helpless. For a solidly grounded and highly readable account of the point of the attempted changes in K-12 teaching, and the necessity of them, and what they have to offer, the book is an absolute treasure.

doi:10.4169/amer.math.monthly.118.01.092

An instantly visible component of that treasure status is Boaler's ability to paint pictures in well under a thousand words that take us into a classroom and set us down in the midst of the students, to be part of the mathematical action. She opens the book with one such classroom visit, letting us listen in on a group of high school students completely and successfully engaged in working out a problem unlike any they have previously encountered. The teacher, having expertly gauged the level of the problem so that the students are thoroughly challenged but able to succeed, is watching closely, and unquestionably learning ever more about her students' abilities and knowledge. She could step in if the discussion goes awry or bogs down, but she has no need to do so. The students are autonomous, energetic, and determined. They also are working together, respecting each other's contributions not only by listening but also by questioning. They are using a wide swath of mathematical concepts—tools developed in quite different courses and contexts. And in the end they are deeply satisfied with their joint success.

This is a beautiful picture, but it's a lot more than that. Boaler, in the interests of brevity and accessibility, refrains from going into the historical and philosophical background that it represents. That background is worth bringing up. For centuries—perhaps millennia—occasional voices have popped up with comments that boil down to "You can't learn unless your mind is actively engaged." The first of these voices to be widely heard, recognized, and discussed was Dewey, who early in the 20th century advocated what came to be called experiential learning. His ideas never disappeared, but also never swept the system, so the model of teaching that features students in straight and preferably silent rows remained the norm. Several decades later a theory with the same basic philosophy entered the scene and eventually became more or less an academic household word: constructivism. Like most household words, it wound up with a good many interpretations and misinterpretations, and like most academic words it wound up discussed, refined, philosophically re-examined, and occasionally beaten to death. One core element, however, survives in all of the variations of the theory and all of its applications: knowledge is not simply absorbed, it is constructed. Unless the mind is actively engaged, neither the mind nor the knowledge will grow. The impact of accepting this theory is to shift the focus of teaching mathematics from organizing material in the way that may be the most mathematically pleasing to organizing it in a way that enables students to engage with and internalize concepts so as to build further concepts from them. That's a nontrivial shift, and appropriately has been the subject of a lot of research.

Some of the most accessible research is Boaler's own. First in England, then later in California, she conducted longitudinal studies in pairs of schools. In each case, the schools were matched in demographics and socio-economic status, and in each case one of the schools was a respected model of traditional teaching. In the English study the second school had adopted project-based learning, leaving students with a wide variety of choices of mathematical challenges and ways to address them. In California the nontraditional school based its math teaching on the idea of "complex instruction"—a particularly rich format of group work with a strong emphasis on addressing issues of social and academic status among the students. Boaler and her colleagues studied students at each pair of schools over a period of several years and in some cases managed follow-up interviews. The outcome in each case was that the nontraditionally taught students came out on average somewhat better on standardized tests and enormously better on their ability to recognize and use mathematics outside of the classroom—not to mention to enjoy it.

A more formal study occurred in France starting in the 1970s, spearheaded by Guy Brousseau. He and his colleagues in the field of *Didactique* committed themselves to

carrying out scientific research to establish the validity of their educational ideas. In particular, Brousseau created an observation school at which over the course of several decades he and dozens of research colleagues collaborated. One notable study resulted from Brousseau's setting himself the challenge of validating his constructivist-based Theory of Situations by creating and experimenting with a sequence of Situations leading fifth graders to construct a deep and functional understanding of fractions and decimal numbers. That study has recently appeared in English in a series of articles in the *Journal of Mathematical Behavior*.[1]

In *What's Math Got to Do with It?* Boaler avoids discussing the theory and takes us straight to the classroom implications. One, as illustrated above, is the possibility and the impact of having students really tussle with genuine mathematical challenges. She also illustrates the flip side: "One day when I was visiting a class that the students knew as 'traditional math,' I stopped and knelt by the side of one boy and asked him how he was getting on. He replied enthusiastically, 'Great. I love traditional math. The teacher tells it to you and you get it.' Pleased that he was so positive, I was about to go to another desk when the teacher came around handing tests back. The boy's face fell when he saw a large F circled in red on the front of his test. He stared at the F, looked through his test, and turned back to me, saying, 'Of course, that's what I hate about traditional math—you think you've got it when you haven't.'" (p. 48)

In between those two extreme cases are a number of other vignettes underscoring Boaler's most central message: mathematics is about reasoning and problem-solving and communicating. That is why we in mathematics love it, and that is why it is something that all students need, whatever direction their studies and lives may take them. If we want students to love mathematics and learn it in a deep way, then they need to be actively doing mathematics, not receiving it passively. Note that her message does not include any recipes for how all classrooms should run, or what materials everyone should use. It's not about the format, and it's not about the curriculum—what matters is that students be doing mathematics. I recently ran into a one-sentence version of this theory: "You can capture any student with five words: Can you figure this out?" Boaler's version includes many essential nuances, but it shares a lot with that capsule.

As I said, for me the most exciting aspect of the book is Boaler's capacity to bring readers into classrooms that illustrate the kind of learning that many of us have as our goal and to make it clear why that is our goal. Along the way, not too surprisingly, she also brings up some other topics upon which I am in hearty agreement, a few stories that I am delighted to have made public, and one topic that leaves me a little uneasy. I'll start with the last: Chapter 6, "Paying the Price for Sugar and Spice," deals with the unambiguously thorny issue of gender imbalances and the underrepresented female population. She starts on solid ground with her own observations and some research by Israeli colleagues. There she has some very interesting results from classrooms and interviews and questionnaires. Then she starts explaining why—and that is where a knowledgeable colleague of mine raised several alarm flags. Currently there are all sorts of entrancing studies on the functioning of the brain itself, and they provide highly attractive explanations for many of the differences. The problem is that it is, as Boaler herself reports, emerging research, and a fair number of the early confident assertions have been called into question. Myself, I'm inclined to feel that Boaler succumbed to the inevitable temptation to accept results that she liked from a field that is not her own without delving quite deeply enough. Like any other explanation of the gender issue in mathematics that I have ever run into, it worries me.

[1] G. Brousseau, N. Brousseau, and V. Warfield, "Rationals and decimals as required in the school curriculum." Part 1 appeared in vol. 23 (2004), part 2 in vol. 26 (2007), part 3 in vol. 27 (2008), and part 4 in vol. 28 (2009).

On the other hand, an area where I have no issue with her at all, partly because what she writes is in total agreement with everything else I have learned, is what she calls The Monster: standardized testing. No topic is more current, and few are scarier. No Child Left Behind is much reviled by those observing and dealing with its impact on schools, and its replacement is in progress, but for all the focus on NCLB's evils one central fact doesn't seem to be registering in any of the places where it needs to register: scores on existing widely administered multiple choice tests correlate little if at all with later success in mathematics, and making such tests carry high stakes in terms of the futures of students and their teachers puts very heavy pressure on teachers to spend their effort and the students' time working on disconnected factoids and procedures of the kind that can be recognized by a machine. If you question the hazards of such tests, take some piece of mathematics that is particularly dear to your heart and try to devise a multiple choice question that will tell you whether a student has a deep understanding of the concepts involved. To me, this represents a current nightmare.

Boaler also addresses another thorny issue: tracking. She cites very convincing research from a number of sources indicating that both the high- and the low-achieving students can benefit from working together. Here, though, the thorns are so numerous that a fair number escape her attention. One thicket of them is that it takes the right kind of teaching to make that true—in a traditionally taught classroom it's not so clear. A denser thicket is the politics of school administration: the parents who make noise and put pressure on administrators are the parents of the high achievers, and by and large in order to pacify them administrators tend to assign the more experienced teachers to their children. So in fact their children probably often do benefit from tracking. A fair number of parents probably even convince themselves that "those other kids" are better off in classes with lower expectations—a conviction which to preserve my blood pressure I will refrain from discussing.

As a final gem—more or less the icing on the cake for me—Boaler recounts some personal observations and experiences about the Math Wars themselves. It is hard for anyone without direct experience to believe the nature and impact of the Math Wars—in fact many still question their existence. Unfortunately, they really do exist, and some of their manifestations are extraordinarily repellent, and that information needs to be out there.

For the readers of the MONTHLY, the chapters I have described so far are the ones that seem likely to be of interest and to answer questions that may have arisen. They are the basis of my hearty recommendation that you all go out and snap up a copy and cruise through it. I might add, though, a bonus for those of you with nonmathematical neighbors who have children. After spending the first six chapters on what is happening and what should be happening—in fact, desperately needs to be happening—Boaler turns in her last three chapters to what a parent can do about it, from games to play with children of various ages to conversational gambits for trying to work with a teacher or administrator. These could well be a treasure—and think what having them to offer might do for your neighborhood relations!

University of Washington, Seattle, WA 98195
warfield@math.washington.edu