Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

785

Wolfgang M. Schmidt

Diophantine Approximation

Springer-Verlag
Berlin Heidelberg New York

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

785

Wolfgang M. Schmidt

Diophantine Approximation

Springer-Verlag
Berlin Heidelberg New York 1980

Author

Wolfgang M. Schmidt
Department of Mathematics
University of Colorado
Boulder, CO 80309
USA

AMS Subject Classifications (1980): 10B16, 10E05, 10E15, 10E40, 10F05, 10F10, 10F20, 10F25, 10F30, 10K15

ISBN 3-540-09762-7 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-09762-7 Springer-Verlag New York Heidelberg Berlin

Library of Congress Cataloging in Publication Data. Schmidt, Wolfgang M., Diophantine approximation. (Lecture notes in mathematics ; 785) Bibliography: p. Includes index. 1. Algebraic number theory. 2. Approximation, Diophantine. I. Title. II. Series: Lecture notes in mathematics (Berlin) ; 785. QA3.L28 no.785 [QA247] 510s [512'.74] 80-11695
ISBN 0-387-09762-7

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2141/3140-543210

Preface

In spring 1970 I gave a course in Diophantine Approximation at the University of Colorado, which culminated in simultaneous approximation to algebraic numbers. A limited supply of mimeographed Lecture Notes was soon gone. The completion of these new Notes was greatly delayed by my decision to add further material.

The present chapter on simultaneous approximations to algebraic numbers is much more general than the one in the original Notes. This generality is necessary to supply a basis for the subsequent chapter on norm form equations. There is a new last chapter on approximation by algebraic numbers. I wish to thank all those, in particular Professor C.L. Siegel, who have pointed out a number of mistakes in the original Notes. I hope that not too many new mistakes have crept into these new Notes.

The present Notes contain only a small part of the theory of Diophantine Approximation. The main emphasis is on approximation to algebraic numbers. But even here not everything is included. I follow the approach which was initiated by Thue in 1908, and further developed by Siegel and by Roth, but I do not include the effective results due to Baker. Not included is approximation in p-adic fields, for which see e.g. Schlickewei [1976, 1977], or approximation in power series fields, for which see e.g., Osgood [1977] and Ratliff [1978]. Totally missing are Pisot-Vijayaraghavan Numbers, inhomogeneous approximation and uniform distribution. For these see e.g. Cassels [1957] and Kuipers and Niederreiter [1974]. Also excluded are Weyl Sums, nonlinear approxi-

mation and diophantine inequalities involving forms in many variables.

My pace is in general very leisurely and slow. This will be especially apparent when comparing Baker's [1975] chapter on approximation to algebraic numbers with my two separate chapters, one dealing with Roth's Theorem on approximation to a single algebraic number, the other with simultaneous approximation to algebraic numbers.

Possible sequences are chapters

I, II, III, for a reader who is interested in game and measure theoretic results, or

I, II, V, for a reader who wants to study Roth's Theorem , or

I, II, IV, V, VI, VII (§ 11, 12), VIII (§ 7-10), for a general theory of simultaneous approximation to algebraic numbers, or

I, II, IV, V, VI, VII, if the goal is norm form equations, or

I, II, VIII (§ 1-6, §11), if the emphasis is on approximation by algebraic numbers.

December 1979 W.M. Schmidt

Notation

A real number ξ may uniquely be written as

$$\xi = [\xi] + \{\xi\} \quad ,$$

where $[\xi]$, the integer part of ξ , is an integer, and where $\{\xi\}$, the fractional part of ξ , satisfies $0 \leqq \{\xi\} < 1$.

$\|\xi\| = \min(\{\xi\}, 1 - \{\xi\})$ is the distance from ξ to the nearest integer,

U denotes the unit interval $0 \leqq \xi < 1$.

$\mathbb{R}^n$ denotes the n-dimensional real space,

E^n denotes Euclidean n-space.

$\underline{x}, \underline{y}, \ldots$ will denote vectors; so $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, or

$\underline{x} = (x_1, \ldots, x_m) \in \mathbb{R}^m$, etc.

Addition and multiplication of vectors by scalars is obvious.

$\underline{e}_1, \ldots, \underline{e}_n$ will denote basis vectors.

λK , where $\lambda > 0$ and where K is in $\mathbb{R}^n$, is the set of elements $\lambda \underline{x}$ with $\underline{x} \in K$.

δ_{ij} is the Kronecker Symbol.

$X, Y, \ldots$, in general will be variables, while $x, y, \ldots$ will be real, usually rational integers. But this rule is sometimes hard to follow: In chapter IV, the symbols $X, Y, \ldots$ will also be used to denote coordinates in compound spaces.

$\left|\underline{x}\right| = \max(|x_1|, \ldots, |x_n|)$ if $\underline{x} = (x_1, \ldots, x_n)$. However $\left|\underline{\beta}\right|$, where $\underline{\beta} = (\beta_1, \ldots, \beta_n)$ has coordinates in an algebraic number field K , is given by $\left|\underline{\beta}\right| = \max(|\beta_1^{(1)}|, \ldots, |\beta_n^{(1)}|, \ldots, |\beta_1^{(k)}|, \ldots, |\beta_n^{(k)}|)$, if $\beta^{(1)} = \beta$, $\beta^{(2)}, \ldots, \beta^{(k)}$ are the conjugates of an elements β (But, on p. 173 , $|\gamma|$ for a single element γ has a different meaning.)

$\lceil P \rceil$ is the maximum absolute value of the coefficients of a polynomial P,

$\mathbb{Q}$ is the field of rationals,

$\mathbb{R}$ is the field of reals,

$\mathbb{C}$ is the field of complex numbers.

$[L : K]$ is the degree of a field extension L over K.

$\{a,b,\ldots,w\}$ denotes the set consisting of $a,b,\ldots,w$, and

$\sim$ denotes a set theoretic difference.

$\ll$ is the Vinogradov symbol. Thus e.g. $f(\underline{x}) \ll g(\underline{x})$ means that $|f(\underline{x})| \leqq c|g(\underline{x})|$ with a constant c. Often this "implied" constant c may depend on extra parameters, such as the dimension, etc.

$\gg \ll$, in the context $f \ll g$, means that both $f \ll g$ and $g \ll f$.

o, the "little o", in the context $f(n) = o(g(n))$, means that $f(n)/g(n)$ tends to 0 as $n \to \infty$.

g.c.d. denotes the greatest common divisor of integers.

Starred Theorems, such as Theorem 6A*, are not proved in these Notes.

Table of Contents

I. Approximation to Irrational Numbers by Rationals.

References: Dirichlet (1842), Hurwitz (1891), Perron (1954), Cassels (1957).

§1. Dirichlet's Theorem.

Given a real number α, let $[\alpha]$, the integer part of α, denote the greatest integer $\leq \alpha$, and let $\{\alpha\} = \alpha - [\alpha]$. Then $\{\alpha\}$ is the fractional part of α, and satisfies $0 \leq \{\alpha\} < 1$. Also, let $\|\alpha\|$ denote the distance from α to the nearest integer. Then always $0 \leq \|\alpha\| \leq \frac{1}{2}$.

THEOREM 1A. (Dirichlet (1842)). Let α and Q be real numbers with $Q > 1$. Then there exist integers p,q such that $1 \leq q < Q$ and $|\alpha q - p| \leq \frac{1}{Q}$.

Proof. First assume that Q is an integer. Consider the following $Q + 1$ numbers:

$$0,1,\{\alpha\},\{2\alpha\},\ldots,\{(q-1)\alpha\} .$$

They all lie in the unit interval $0 \leq x \leq 1$. We divide the unit interval into Q subintervals

$$\frac{u}{Q} \leq x < \frac{u+1}{Q} \quad (u = 0,1,\ldots,Q-1) ,$$

but with $<$ replaced by $\leq$ if $u = Q-1$. At least one such subinterval contains two (or more) of the $Q+1$ numbers above. Hence there are integers r_1,r_2,s_1,s_2 with $0 \leq r_i < Q$ $(i = 1,2)$ and $r_1 \neq r_2$ such that

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q} .$$

If, say, $r_1 > r_2$, put $q = r_1 - r_2$, $p = s_1 - s_2$. Then $1 \le q < Q$ and $|q\alpha - p| \le \frac{1}{Q}$, proving the theorem when Q is an integer.

Next, suppose Q is not an integer. Apply what has already been proved to $Q' = [Q] + 1$. Then $1 \le q < Q'$ implies $1 \le q \le [Q]$, whence $1 \le q < Q$, and the theorem is true for Q.

Remark. The two inequalities in Dirichlet's Theorem yield

$$|\alpha - \frac{p}{q}| \le \frac{1}{Qq} < \frac{1}{q^2} .$$

COROLLARY 1B. Suppose that α is irrational. Then there exist infinitely many pairs p,q of relatively prime integers with

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2} . \tag{1.1}$$

Proof. Dirichlet's Theorem obviously remains true if we ask for relatively prime integers p,q satisfying $1 \le q < Q$ and $|\alpha q - p| \le \frac{1}{Q}$. Since α is irrational, $\alpha q - p$ is never zero, and hence for any given p,q, the inequality $|\alpha q - p| \le \frac{1}{Q}$ can only be satisfied for $Q \le Q_0(p,q)$. Hence as $Q \to \infty$, there will be infinitely many distinct pairs p,q of relatively prime integers occuring in Dirichlet's Theorem.

Remark. This corollary is not true if α is rational. For suppose that $\alpha = \frac{u}{v}$. If $\alpha \ne \frac{p}{q}$, then $|\alpha - \frac{p}{q}| = |\frac{u}{v} - \frac{p}{q}| = |\frac{qu - pv}{vq}| \ge \frac{1}{vq}$, and therefore (1.1) can be satisfied by only finitely many pairs p,q of relatively prime integers.

§2. Farey Series.

Definition. The Farey series $\mathcal{F}_n$ of order $n (\ge 1)$ is the sequence of rationals in their lowest terms between 0 and 1 with

denominators $\leq n$, written in ascending order. For example,

$$\mathcal{F}_5\colon\ 0,\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},1\ .$$

THEOREM 2A. *If* $\frac{h}{k}$, $\frac{h'}{k'}$ *are successive terms in* $\mathcal{F}_n$, *then* $h'k - hk' = 1$.

We need

LEMMA 2B. *Suppose that* $\underline{x} = (x_1,x_2)$ *and* $\underline{y} = (y_1,y_2)$ *are integer points in the plane, with* $\underline{0} = (0,0),\underline{x},\underline{y}$ *not on a line. Suppose further that the closed triangle with vertices* $\underline{0}$, $\underline{x}$, $\underline{y}$ *contains no integer points but its vertices. Then*

$$x_1y_2 - x_2y_1 = \pm 1\ .$$

Proof of the Lemma. Let $\mathcal{T}$ be the triangle mentioned above, and let $\mathcal{P}$ be the closed parallelogram with vertices $\underline{0}$, $\underline{x}$, $\underline{y}$ and $\underline{x}+\underline{y}$. Then $\mathcal{P}$ contains no integer points but its vertices: for suppose that $\underline{z}$ is an integer point in $\mathcal{P}$, $\underline{z} \notin \mathcal{T}$. Then $\underline{x} + \underline{y} - \underline{z} \in \mathcal{T}$, hence $\underline{x} + \underline{y} - \underline{z} = \underline{0}, \underline{x}$ or $\underline{y}$, and therefore $\underline{z} = \underline{x} + \underline{y},\underline{y}$ or $\underline{x}$.

If $\underline{p}$ is any integer point, we may write $\underline{p} = \lambda\underline{x} + \mu\underline{y}$ with *real* coefficients λ , μ since $\underline{0}$, $\underline{x}$, $\underline{y}$ are not collinear. Then $\underline{p} = \underline{p}' + \underline{p}''$, where

$$\underline{p}' = [\lambda]\underline{x} + [\mu]\underline{y} \text{ and } \underline{p}'' = \{\lambda\}\underline{x}+\{\mu\}\underline{y}\ .$$

Both $\underline{p}$ and $\underline{p}'$ are integer points, hence so is $\underline{p}''$. Also $\underline{p}'' \in \mathcal{P}$. Since $\underline{p}'' \neq \underline{x},\underline{y}$ and $\underline{x} + \underline{y}$, we have $\underline{p}'' = \underline{0}$. Therefore $\underline{p} = \lambda\underline{x} + \mu\underline{y}$ with *integer* coefficients λ,μ .

In particular,

$$(1,0) = \lambda\underline{x} + \mu\underline{y} = (\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2) \quad ,$$

$$(0,1) = \lambda'\underline{x} + \mu'\underline{y} = (\lambda' x_1 + \mu' y_1, \lambda' x_2 + \mu' y_2)$$

for certain integers $\lambda, \mu, \lambda', \mu'$. It follows that

$$1 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = \begin{vmatrix} \lambda & \mu \\ \lambda' & \mu' \end{vmatrix} \cdot \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \quad ,$$

whence

$$\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} = \pm 1$$

as claimed.

Proof of the Theorem. Put $\underline{x} = (h,k)$, $\underline{y} = (h', k')$. Then $\underline{0}, \underline{x}, \underline{y}$ are not collinear since $\gcd(h,k) = \gcd(h',k') = 1$ and $\underline{x} \neq \underline{y}$. Let $\mathcal{T}$ denote the closed triangle with vertices $\underline{0}, \underline{x}, \underline{y}$. Then there is no integer point in $\mathcal{T}$ besides $\underline{0}, \underline{x}, \underline{y}$. For if there were such a point (h'', k''), then there also would be a point with $\gcd(h'', k'') = 1$. Then $(h'', k'') = \lambda(h,k) + \mu(h', k')$ with $\lambda \geq 0$, $\mu \geq 0$, $0 < \lambda + \mu \leq 1$ and (λ, μ) not equal to $(1,0)$ or to $(0,1)$. This implies that $k'' \leq \lambda n + \mu n \leq n$. We have $\lambda > 0$, $\mu > 0$ (since $\gcd(h,k) = \gcd(h',k') = 1$), whence $\frac{h}{k} < \frac{h''}{k''} < \frac{h'}{k'}$. Thus $\frac{h''}{k''}$ would belong to $\mathcal{F}_n$, contradicting the supposition that $\frac{h}{k}$ and $\frac{h'}{k'}$ are consecutive elements of $\mathcal{F}_n$. The hypotheses of Lemma 2B are now satisfied, and we conclude that $h'k - hk' = \pm 1$. Since $\frac{h}{k} < \frac{h'}{k'}$, we have $h'k - hk' = 1$.

COROLLARY 2C. If $\frac{h}{k}, \frac{h''}{k''}, \frac{h'}{k'}$ are consecutive elements of $\mathcal{F}_n$, then

$$\frac{h''}{k''} = \frac{h+h'}{k+k'} \quad .$$

Proof. By the theorem, $h''k - hk'' = 1$ and $h'k'' - h''k' = 1$, so that $h''(k+k') - k''(h+h') = 0$.

LEMMA 2D. Suppose that $\frac{h}{k}$, $\frac{h'}{k'}$ are successive terms in the Farey series $\mathcal{F}_n$, and put $h'' = h + h'$, $k'' = k + k'$. (Note that $\frac{h''}{k''}$ does NOT belong to $\mathcal{F}_n$). Then for every α in $\frac{h}{k} \leqq \alpha \leqq \frac{h'}{k'}$, at least one of the following three inequalities holds:

$$(2.1) \qquad \left|\alpha - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2} \quad , \quad \left|\alpha - \frac{h''}{k''}\right| < \frac{1}{\sqrt{5}k''^2} \quad , \quad \left|\alpha - \frac{h'}{k'}\right| < \frac{1}{\sqrt{5}k'^2} \quad .$$

Proof. We may assume that $\alpha > \frac{h''}{k''}$. Namely, otherwise replace α by $1 - \alpha'$, $\frac{h}{k}$ by $1 - \frac{h'}{k'}$, etc. If none of the inequalities above hold, then

$$\alpha - \frac{h}{k} \geq \frac{1}{\sqrt{5}k^2} \quad , \quad \alpha - \frac{h''}{k''} \geq \frac{1}{\sqrt{5}k''^2} \quad , \quad \frac{h'}{k'} - \alpha \geq \frac{1}{\sqrt{5}k'^2} \quad .$$

Adding the first and third inequalities, we obtain

$$\frac{h'}{k'} - \frac{h}{k} = \frac{1}{kk'} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k^2} + \frac{1}{k'^2}\right) ;$$

adding the second and third inequalities, we obtain

$$\frac{h'}{k'} - \frac{h''}{k''} = \frac{1}{k'k''} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k'^2} + \frac{1}{k''^2}\right) \quad .$$

Then $\sqrt{5}kk' \geq k^2 + k'^2$ and $\sqrt{5}k'k'' \geq k'^2 + k''^2$, so that $\sqrt{5}\,k'(k+k'') \geq k^2 + 2k'^2 + k''^2$, and therefore $\sqrt{5}\,k'(2k+k') \geq 2k^2 + 3k'^2 + 2kk'$. It follows that

$$0 \geq \frac{1}{2}((\sqrt{5} - 1)k' - 2k)^2 \quad .$$

But this is impossible, since k and k' are nonzero integers.

LEMMA 2E. *Suppose α is a real quadratic irrational which is a root of a non-zero polynomial*

$$P(X) = aX^2 + bX + c$$

with rational integer coefficients and discriminant $D = b^2 - 4ac$. Then for $A > \sqrt{D}$, the inequality

$$|\alpha - \frac{p}{q}| < \frac{1}{Aq^2} \tag{2.2}$$

has only finitely many solutions.

Proof. Write $P(X) = a(X-\alpha)(X-\alpha')$, so that $D = a^2(\alpha-\alpha')^2$. Given p/q with (2.2) we have

$$\frac{1}{q^2} \leqq |P(\frac{p}{q})| = |\alpha - \frac{p}{q}||a(\alpha' - \frac{p}{q})| < \frac{1}{Aq^2}|a(\alpha' - \alpha + \alpha - \frac{p}{q})| < \frac{\sqrt{D}}{Aq^2} + \frac{|a|}{A^2q^4},$$

which clearly is impossible if $A > \sqrt{D}$ and if q is large.

THEOREM 2F. (Hurwitz (1891)).

(i) *For every irrational number α there are infinitely many distinct rationals $\frac{p}{q}$ with*

$$|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}\,q^2}. \tag{2.3}$$

(ii) *This would be wrong if $\sqrt{5}$ were replaced by a constant $A > \sqrt{5}$.*

Proof. We may suppose that $0 < \alpha < 1$. If $\frac{h}{k}$ and $\frac{h'}{k'}$ are the successive terms in the Farey series $\mathcal{F}_n$ with $\frac{h}{k} < \alpha < \frac{h'}{k'}$, then