MATHEMATICAL SURVEYS

Number 17

MATHEMATICAL SURVEYS · *Number 17*

APPROXIMATION BY POLYNOMIALS WITH INTEGRAL COEFFICIENTS

BY

LE BARON O. FERGUSON

1980
AMERICAN MATHEMATICAL SOCIETY
PROVIDENCE, RHODE ISLAND

Library of Congress Cataloging in Publication Data

Ferguson, Le Baron O 1939–

Approximation by polynomials with integral coefficients.

(Mathematical surveys; no. 17)

1. Approximation theory. 2. Polynomials. I. Title. II. Series: American Mathematical Society. Mathematical surveys; no. 17.

QA221.F46 511'.4 79-20331

ISBN 0-8218-1517-2

1980 Mathematics Subject Classifications. Primary 41A10, 41A29, 41A30, 41A25.

PREFACE

Results in the approximation of functions by polynomials with coefficients which are integers have been appearing since that of Pál in 1914. The body of results has grown to an extent which seems to justify the present book. The intention here is to make these results as accessible as possible.

Aside from the intrinsic interest to the pure mathematician, there is the likelihood of important applications to other areas of mathematics; for example, in the simulation of transcendental functions on computers. In most computers, fixed point arithmetic is faster than floating point arithmetic and it may be possible to take advantage of this fact in the evaluation of integral polynomials to create more efficient simulations. Another promising area for applications of this research is in the design of digital filters. A central step in the design procedure is the approximation of a desired system function by a polynomial or rational function. Since only finitely many binary digits of accuracy actually can be realized for the coefficients of these functions in any real filter the problem amounts (to within a scale factor) to approximation by polynomials or rational functions with integral coefficients. For more details one may consult this author's listing in the Bibliography. It would be gratifying to the author if this book stimulates research in this direction.

Most of the results here have already appeared in the literature. However, for the expert, we mention the following exceptions: Corollaries 7.17, 7.20, Propositions 7.16, 9.8, and Theorems 9.7, 9.9, 9.10, 9.11, A.4, A.5.

It is a pleasure to acknowledge the help of many people in the writing of this book. It was my advisor, Edwin Hewitt, who initially brought the problem to my attention. G. G. Lorentz suggested the book itself. In learning the subject, especially as it relates to number theory, I am indebted to a number of valuable conversations with David Cantor. I would also like to express my gratitude for the support of the institutions listed at the end of the Bibliography and to the Air Force Office of Scientific Research for partial support from grants numbered AFOSR 71-2030 and AFOSR 78-3599. Finally, I thank Mrs. Joyce Kepler for her excellent services as typist.

Riverside
February, 1976

La vie est brève:
Un peu d'espoir,
Un peu de rêve
Et puis–bonsoir! Leon Montenaeken

TABLE OF CONTENTS

INTRODUCTION

As an introduction to our subject we consider some elementary results and their simple proofs. Besides giving an indication of the kind of results to expect, they may be useful in themselves. Also, the techniques of proof will occur again in establishing the stronger results.

For the present an integral polynomial is a polynomial whose coefficients all lie in the set of rational integers $\{0, \pm 1, \pm 2, \ldots\}$. In references to the bibliography, we give the author's name, followed by the last two digits of the year of publication in square brackets. For references which appeared in the nineteenth century, all four digits are given.

The results in the theory of approximation by integral polynomials can be summarized very roughly as follows. In contrast with the classical case of arbitrary coefficients for the polynomials, approximation on a set X by integral polynomials is only possible if certain conditions are satisfied by the function to be approximated and the set X. The set X must not be too large in the sense that its transfinite diameter must be less than unity. If S has transfinite diameter less than unity, then there is a finite subset $J(X)$ of X such that uniform approximation to a continuous f is possible by integral polynomials if and only if f can be interpolated on $J(X)$ by such polynomials. Apparently the first result concerning the approximation of functions by integral polynomials is the following by Pál [**14**]. Let f be a continuous real valued function on an interval $[-\alpha, \alpha]$ with $0 < \alpha < 1$. Then f can be uniformly approximated by integral polynomials if and only if $f(0)$ is an integer. This is easily proved as follows (Ferguson [**70b**]). The condition that $f(0)$ be an integer is obviously necessary. Indeed, if k is an integer and $\{g_n\}$ a sequence of polynomials with integral coefficients tending uniformly to f on a set containing k, then $g_n(k) \to f(k)$ as $n \to \infty$. But each $g_n(k)$ is an integer; hence $f(k)$ is a limit point of the set of integers, hence an integer itself. Conversely, suppose $f(0)$ is an integer. Since it suffices to approximate $f - f(0)$ we can assume $f(0) = 0$. Let $\varepsilon > 0$. Since $0 < \alpha < 1$, $\sum_{n=1}^{\infty} \alpha^n < \infty$ and there is an odd integer k such that

$$\sum_{n>k} \alpha^n < \varepsilon/3. \tag{1}$$

Since k is odd, the function x^k separates the points of $[-\alpha, \alpha]$ and by the Stone-Weierstrass theorem there is a polynomial p_0 with real coefficients such that if $p(x) = p_0(x^k)$, $-\alpha \leqslant x \leqslant \alpha$, then

$$\|f - p\| < \varepsilon/3 \tag{2}$$

where $\|\cdot\|$ is the norm defined by $\|h\| = \sup_{|x| \leqslant \alpha} |h(x)|$. If we let p_1 be the polynomial p without its constant term, we see from the assumption $f(0) = 0$ and (2) that

$$\|p - p_1\| < \varepsilon/3. \tag{3}$$

Finally, if we define $[p_1]$ to be the polynomial p_1, with each coefficient replaced by its integral part, then $p_1 - [p_1]$ is a polynomial without constant term which involves only powers $\geqslant k$ and with coefficients between 0 and 1; hence by (1)

$$\|p_1 - [p_1]\| < \varepsilon/3. \tag{4}$$

From (2), (3), and (4) and the triangle inequality we have

$$\|f - [p_1]\| < \varepsilon$$

which establishes Pál's result.

It is natural to ask next what happens in case $\alpha = 1$. As we have noted, a continuous function which is approximable in the above sense must take on integral values at -1, 0, and 1. This is not a sufficient condition, however. Indeed, later that same year Kakeya [**14**] published the following generalization of Pál's result: a continuous real valued function f on $[-1, 1]$ is uniformly approximable by integral polynomials if and only if $f(-1)$, $f(0)$, and $f(1)$ are integers and $f(-1) + f(1)$ is even. The necessity of the latter condition is easily seen when one notes that if p is an integral polynomial, then $p(-1) + p(1)$ is twice the sum of the coefficients of the even powered monomials in p. As α tends upward to 2 we will see that, in order to be approximable, a continuous function needs to satisfy more and more conditions of an arithmetic nature. The number of conditions tends to infinity as α tends to 2.

When the polynomials are allowed to have arbitrary real coefficients then we know from Weierstrass' theorem that any continuous function can be uniformly approximated on any closed bounded interval. In the case of approximation by integral polynomials there are two major differences. First, as we have seen, only those functions which satisfy certain arithmetic conditions are approximable. The second difference is that in approximation by integral polynomials the set on which the approximation is to take place may be so "large" that the problem is trivial. Indeed, Kakeya [**14**] showed that on any interval of length $\geqslant 4$ no function can be uniformly approximated by integral polynomials unless it is identically equal to such a polynomial. This is easily proved as follows.

Suppose $\{p_n\}$ is a sequence of integral polynomials tending uniformly to a function f on $[a, b]$ which is not identically equal to an integral polynomial there. Then there exist n and m such that $\|p_n - f\| < \frac{1}{2}$, $\|p_m - f\| < \frac{1}{2}$ ($\|\cdot\|$ is the uniform norm on $[-1, 1]$), and $p_n \not\equiv p_m$. It follows that $\|p_n - p_m\| < 1$ and

since $p_n - p_m$ is not zero it has a leading coefficient c, say, which is a nonzero integer; hence $|c| \geqslant 1$ and

$$\|(p_n - p_m)/c\| < 1. \tag{5}$$

However, $(p_n - p_m)/c$ is a monic polynomial (i.e., has leading coefficient unity); hence (5) is impossible. Indeed, it is a well-known result of Čebyšev (Lorentz [**66**, Chapter 2, Theorem 11]) that the monic polynomial of degree n ($n \geqslant 1$) which has least supremum norm on $[-1, 1]$ has the form $2^{1-n}\cos(n \times \cos^{-1} x)$, $-1 \leqslant x \leqslant 1$. It follows that the polynomial with the same attributes on $[-2, 2]$ has the form $2\cos(n \cos^{-1}(x/2))$, $-2 \leqslant x \leqslant 2$. For any positive integer n these polynomials all have norm 2. Since translation does not change the norm or the monicity of a polynomial, it follows that every nonconstant monic polynomial on an interval of length greater than or equal to 4 has norm at least 2.

In 1925 the following result by Chlodovsky [**25**] appeared: if $[a, b]$ is an interval not containing an integer, then any continuous function f on $[a, b]$ can be uniformly approximated by integral polynomials. This is an immediate consequence of Pál's result but the proof is different. We first note that after translating by an integer we can make $0 < a < b < 1$; hence we assume this without loss of generality. Next notice that from Weierstrass' theorem it suffices to show that any constant can be uniformly approximated on $[a, b]$ by integral polynomials. (First approximate f by a polynomial with real coefficients and then replace each coefficient by an approximating integral polynomial.) Since every real number can be approximated by one of the form $n2^{-m}$ where n and m are integers, it suffices to approximate the constant $\frac{1}{2}$. But for large k the constant $\frac{1}{2}$ is uniformly approximated on $[a, b]$ by a function of the form $1/(2 - x^k)$. Finally

$$\frac{1}{2 - x^k} = \frac{1}{1 - (x^k - 1)} = \sum_{n=0}^{\infty} (x^k - 1)^n$$

where the series converges uniformly on $[a, b]$. Since any truncation of the series is a polynomial with integral coefficients we have Chlodovsky's result.

A final indication of some of the techniques of proof in this subject is the following which appeared in a paper by Kantorovič [**31**]: a continuous real valued function f on $[0, 1]$ is uniformly approximable by integral polynomials if and only if $f(0)$ and $f(1)$ are integers. We have already seen the necessity of this condition. Conversely, suppose the condition holds. Since it suffices to approximate $f(x) - (f(1)x + f(0)(1 - x))$, we can assume that $f(0) = f(1) = 0$. It is well known that the sequence of Bernšteĭn polynomials for f converges uniformly to f on $[0, 1]$ (Lorentz [**66**, Chapter 1, Theorem 4]) hence it suffices to approximate

$$p_n(x) = \sum_{\nu=1}^{n-1} f\left(\frac{\nu}{n}\right)\binom{n}{\nu} x^{\nu}(1 - x)^{n-\nu}$$

for all sufficiently large n. The $\nu = 0$ and $\nu = n$ terms are not present here since we have assumed that $f(0) = f(1) = 0$. Let

$$q_n(x) = \sum_{\nu=1}^{n-1} \left[f\left(\frac{\nu}{n}\right)\binom{n}{\nu} \right] x^\nu (1-x)^{n-\nu},$$

where $[\cdot]$ represents the greatest integer function, i.e., $[x]$ is the greatest integer $\leqslant x$. Since $\binom{n}{\nu} \geqslant n$ $(1 \leqslant \nu \leqslant n-1)$ we have

$$\begin{aligned} \sum_{\nu=1}^{n-1} x^\nu (1-x)^{n-\nu} &\leqslant \frac{1}{n} \sum_{\nu=1}^{n-1} \binom{n}{\nu} x^\nu (1-x)^{n-\nu} \\ &\leqslant \frac{1}{n} \sum_{\nu=0}^{n} \binom{n}{\nu} x^\nu (1-x)^{n-\nu} = \frac{1}{n}, \end{aligned}$$

by the binomial theorem. Thus, with $\| \cdot \|$ denoting the uniform norm on $[0, 1]$, we have $\| p_n - q_n \| \leqslant 1/n$ and since q_n is an integral polynomial, we are done.

In what follows we will establish generalizations of the above results as well as some related results. In order to be able to describe them economically we will first introduce some notation. The results fall into two main categories. On the one hand they characterize those functions that can be approximated uniformly or in the L_p norms by integral polynomials. These we call qualitative results. Some examples are those results already mentioned. On the other hand there are the quantitative results which give estimates of the rates of convergence of integral polynomials of best approximation. An example is the result of Kantorovič which appears later in the introduction.

Throughout, X will denote a compact Hausdorff space and for any subset $S \subset X$ we will use $\| \cdot \|_S$ to denote the uniform (Čebyšev, sup) norm on S. Thus for any bounded, real or complex valued function f on S, we have

$$\|f\|_S = \sup_{x \in S} |f(x)|.$$

The interior of X will be denoted X°.

The algebra of all complex continuous functions in this norm is denoted by $C(X)$, and the subalgebra of real valued elements by $C(X, R)$. We often write $\| \cdot \|$ in place of $\| \cdot \|_X$. The symbols **N**, **Z**, **Q**, **R**, and **C** are used to denote, respectively, the natural numbers $\{0, 1, 2, \ldots\}$, the rational integers $\{0, \pm 1, \pm 2, \ldots\}$, the rational numbers, the real numbers, and the complex numbers. A *monic polynomial* is one whose leading coefficient is unity. If A and B are two sets, the relative complement of B in A is denoted by $A \setminus B$. The empty set is denoted by $\varnothing$. By *integral polynomials* we mean polynomials with integral coefficients, where "integral" is the adjectival form of "integer." By *integers* we mean the elements of some discrete subring R of the complex numbers **C**. If $R = \mathbf{Z}$ we speak of *rational integers*. If $R = \mathbf{Z} + i\mathbf{Z}$ we have the so-called *Gaussian integers*. For a real number x, $[x]$ will denote the greatest integer which is $\leqslant x$, and (x) will denote the fractional part, $x - [x]$, of x.

If X is an interval of the real line **R** and f is a real or complex valued function

defined on X, then we define

$$E_n(f) = \inf_{\deg p < n} \|f - p\|_X$$

where the polynomials p have real coefficients and

$$E_n^e(f) = \inf_{\deg q < n} \|f - q\|_X$$

where the polynomials q have rational integral coefficients. As a rule we reserve the symbol q for polynomials having integral coefficients.

As an example of a quantitative result we mention the following (Kantorovič [31]): if f is a continuous function on $X = [0, 1]$ with $f(0) = f(1) = 0$, then

$$E_n^e(f) \leqslant 2E_n(f) + O(1/n). \tag{6}$$

This can be proved as follows. Let n be any positive integer. Then there exists a (unique) polynomial p_n with degree $\leqslant n$ and real coefficients such that ($\|\cdot\| = \|\cdot\|_{[0,1]}$)

$$\|f - p_n\| = E_n(f). \tag{7}$$

Since $f(0) = 0 = f(1)$ we see from this that $|p_n(0)| \leqslant E_n(f) \geqslant |p_n(1)|$; hence

$$|p_n(1)x + p_n(0)(1 - x)| \leqslant E_n(f), \qquad 0 \leqslant x \leqslant 1.$$

Setting $\tilde{p}_n(x) = p_n(x) - (p_n(1)x + p_n(0)(1 - x))$ we have

$$\tilde{p}_n(0) = 0 = \tilde{p}_n(1) \tag{8}$$

and

$$\|p_n - \tilde{p}_n\| \leqslant E_n(f). \tag{9}$$

Thus by (7) and (9)

$$\|f - \tilde{p}_n\| \leqslant 2E_n(f). \tag{10}$$

It is easy to see that any polynomial of degree at most n can be written as a linear combination of the terms $\{x^\nu(1 - x)^{n-\nu}\}_{\nu=0}^n$; hence for some choice of real numbers a_ν ($0 \leqslant \nu \leqslant n$) we have

$$\tilde{p}_n(x) = \sum_{\nu=0}^{n} a_\nu x^\nu (1 - x)^{n-\nu}$$

and by (8)

$$\tilde{p}_n(x) = \sum_{\nu=1}^{n-1} a_\nu x^\nu (1 - x)^{n-\nu}.$$

As above, if we set $[\tilde{p}_n](x) = \sum_{\nu=1}^{n-1}[a_\nu]x^\nu(1 - x)^{n-\nu}$ then we have $\|\tilde{p}_n - [\tilde{p}_n]\| \leqslant 1/n$. This together with (10) gives

$$\|f - [\tilde{p}_n]\| \leqslant 2E_n(f) + 1/n.$$

This establishes (6). We note in passing that much stronger results are known. See Chapter 12.

The qualitative results are divided into four cases, as follows. If X is a compact subset of $\mathbf{R}$ and $R = \mathbf{Z}$ we say that we are in the *real case*. If R is an

arbitrary but fixed discrete subring of $\mathbf{C}$ with rank 2 and X a compact subset of $\mathbf{C}^n$ we say that we are in the *complex case*. The most complete results in this case hold for $n = 1$. A more general case is the following. For lack of a better word we call it the *adelic case*. Let T be a finite set of equivalence classes of valuations on an algebraic number field K which contains all the Archimedean classes. For each v in T let K_v be the corresponding completion of K, X_v a compact subset of K_v, and f_v a K_v-valued continuous function on X_v. The question is whether or not there exists p in $K[x]$ with T-integers for coefficients and such that $p - f_v$ is uniformly small on X_v for each v in T. The final case is that in which X is any compact Hausdorff space and $\mathfrak{F}$ is a point separating family of continuous functions on X. The integral polynomials in this case are $\mathbf{Z}[\mathfrak{F}]$, the polynomials in elements of $\mathfrak{F}$ with rational integral coefficients. We call this the *general case*. See Chapter 9.

We give criteria in all the above cases which characterize the functions which can be uniformly approximated by polynomials with integral coefficients. Proofs are given in all but the adelic case where, however, the results are stated completely and the connections with the previous cases are indicated. Although the adelic case could have been established first and the results of the real and complex cases derived from it, we have not done so because this would have limited the usefulness of the qualitative part of the book to those readers conversant with algebraic number theory.

PART I: PRELIMINARIES

CHAPTER 1

DISCRETE RINGS

In the real case we will take the rational integers for the coefficients of our integral polynomials. In the complex case, however, a larger ring is needed in order to include some nonreal numbers among the coefficients. It happens that we can establish our results for a whole class of rings: those which are discrete and have rank 2. We proceed to define these terms and to establish the properties of these rings which we will need later. We will also do the same for the adelic case.

DEFINITION 1.1. Throughout the following, A will denote a fixed but arbitrary discrete subring of $\mathbf{C}$ with rank 2. A subring of $\mathbf{C}$ which is discrete but not necessarily of rank 2 will usually be denoted by R. By *discrete* we mean that A is discrete as a subset of the topological space $\mathbf{C}$. By *rank* 2 we mean that the real linear space spanned by A has dimension 2.

A reader not interested in maximum generality may think of A as the ring of Gaussian integers $\mathbf{Z} + i\mathbf{Z}$.

The requirement that A have rank 2 is actually equivalent to A not being a subring of $\mathbf{R}$, as follows. Suppose A has rank less than 2 and $A \not\subseteq \mathbf{R}$. Then there exists $z \in A \setminus \mathbf{R}$. Thus z and z^2 are linearly dependent over $\mathbf{R}$; hence there exist $a, b \in \mathbf{R}$, not both zero, such that $az + bz^2 = 0$. Since $z \neq 0$ we have $a + bz = 0$. Since a and b are not both zero, this equation shows that neither is zero. Solving for z shows that $z \in \mathbf{R}$, a contradiction. Thus, if A has rank less than 2, then $A \subset \mathbf{R}$. The converse is obvious.

The requirement that a subring A of $\mathbf{C}$ be discrete is equivalent to the condition that $0 \neq z \in A$ implies $|z| \geqslant 1$. Indeed, if $0 < |z| < 1$ and $z \in A$, then $z^n \to 0$; hence 0 is a limit point of A and A is not discrete. Conversely the condition implies that $|z_1 - z_2| \geqslant 1$ for every distinct $z_1, z_2 \in A$. Hence the open unit disk centered at $z \in A$ meets A only in z which shows that z is an isolated point of A. Since z is any point of A, this shows that A is discrete.

The following result will be of use to us as we will often have occasion to replace the complex coefficients of an approximating polynomial by "nearest" elements of A.

PROPOSITION 1.2. *There is a $\delta > 0$ such that if z is any complex number, there exists $a \in A$ with $|z - a| < \delta$.*

PROOF. By Bourbaki [**63**, Theorem 1, p. 77], there exist b_1 and b_2 in $\mathbf{C}$ which are linearly independent over the reals and which generate A as an additive group. Since $\mathbf{C}$ has dimension 2 as a real vector space, there exist real numbers r_1 and r_2 such that $z = r_1 b_1 + r_2 b_2$. For $i = 1$ or 2 there exist integers n_i and real numbers r_i' such that $r_i = n_i + r_i'$ and $|r_i'| \leqslant \frac{1}{2}$. Then $n_1 b_1 + n_2 b_2$ is in A and $|z - (n_1 b_1 + n_2 b_2)| = |r_1' b_1 + r_2' b_2| \leqslant \frac{1}{2}(|b_1| + |b_2|)$. It suffices to set $\delta = \frac{1}{2}(|b_1| + |b_2|) + 1$. □

A *quadratic field* is a field F containing the rationals $\mathbf{Q}$ such that the degree of F over $\mathbf{Q}$, denoted by $[F : \mathbf{Q}]$, is equal to two. It is well known (Weiss [**63**]) that every quadratic field F is of the form $\mathbf{Q}(\sqrt{d})$ for a unique square-free rational integer d different from 0 and 1. If d is negative (positive) the field $\mathbf{Q}(\sqrt{d})$ is said to be *imaginary* (*real*). Throughout this survey the symbol L will always denote an imaginary quadratic field. There is a connection between discrete rings of rank 2 and imaginary quadratic fields which we proceed to establish.

DEFINITION 1.3. If R is any subring with identity of the complex numbers $\mathbf{C}$, then we say that an element z of $\mathbf{C}$ is *integral over* R if z is a root of a monic polynomial with coefficients in R.

PROPOSITION 1.4. *If F is a quadratic field, the elements of F which are integral over $\mathbf{Z}$ form a ring containing $\mathbf{Z}$.*

PROOF. Jacobson [**51**, Theorem 8, p. 182]. □

DEFINITION 1.5. The ring of elements of a quadratic field F which are integral over $\mathbf{Z}$ is denoted by I_F. When we have some definite quadratic field F in mind, we often use the term *integer* to mean an element of I_F. Throughout the following, elements of the ring $\mathbf{Z}$ will be referred to as *rational integers*.

PROPOSITION 1.6. *Let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic field. Then a basis for I_F as a $\mathbf{Z}$-module is given by*

(i) $\{1, \sqrt{d}\}$ *if* $d \not\equiv 1 \pmod 4$, *and*

(ii) $\{1, (1 + \sqrt{d})/2\}$ *if* $d \equiv 1 \pmod 4$.

PROOF. By Jacobson [**51**, Theorem 2, p. 186], if $d \not\equiv 1 \pmod 4$, then $I_L = \{m + n\sqrt{d} : m, n \in \mathbf{Z}\}$ and it is easily seen that 1 and $\sqrt{d}$ are linearly independent over the rational integers $\mathbf{Z}$. Likewise, if $d \equiv 1 \pmod 4$, the same theorem in Jacobson shows that

$$I_L = \{m + n\sqrt{d} : m, n \in \mathbf{Z}\} \cup \left\{\tfrac{1}{2}((2m + 1) + (2n + 1)\sqrt{d}) : m, n \in \mathbf{Z}\right\}.$$

Plainly this set is just $\{m + n(1 + \sqrt{d})/2 : m, n \in \mathbf{Z}\}$. To see that (ii) is actually linearly independent over $\mathbf{Z}$, suppose that $m, n \in \mathbf{Z}$ and that

$$m + n(1 + \sqrt{d})/2 = 0. \qquad (*)$$

We must show that both m and n are zero. This is clear if $n = 0$. But if $n \neq 0$,

(*) shows that $\sqrt{d}$ is rational, which we know to be false since $[F : \mathbf{Q}] = 2$. □

PROPOSITION 1.7. *If L is an imaginary quadratic field, then the ring I_L is discrete and has rank 2; that is, I_L satisfies the conditions on A in Definition 1.1.*

PROOF. Write $L = \mathbf{Q}(\sqrt{d})$, as usual. Then $d < 0$, which implies that $\sqrt{d}$ is purely imaginary. This shows that the bases in Proposition 1.6 are linearly independent over $\mathbf{R}$, so I_L has rank 2. From this linear independence we also see that I_L is discrete (Bourbaki [**63**, pp. 74–75]). □

We note in passing that if F is a real quadratic field, then I_F does not satisfy the conditions on A in Definition 1.1 as follows. Since F is real, $F \subset \mathbf{R}$ and then $I_F \subset \mathbf{R}$, by definition. Thus F does not have rank 2 by the comment following Definition 1.1. Also, I_F is not discrete. Indeed, it is dense in $\mathbf{R}$ as follows. Let $F = \mathbf{Q}(\sqrt{d})$. Then a basis for I_F as a $\mathbf{Z}$-module is given by Proposition 1.6. The first element of each of these bases is unity and the second element is irrational; otherwise, $\sqrt{d}$ would be rational and $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}$, a contradiction. Thus, by the well-known theorem of Kronecker, linear combinations with rational integer coefficients of these base elements are dense in $\mathbf{R}$.

PROPOSITION 1.8. *For quadratic fields $\mathbf{Q}(\sqrt{d_1})$ and $\mathbf{Q}(\sqrt{d_2})$, the nonequality $I_{\mathbf{Q}(\sqrt{d_1})} \neq I_{\mathbf{Q}(\sqrt{d_2})}$ implies $I_{\mathbf{Q}(\sqrt{d_1})} \cap I_{\mathbf{Q}(\sqrt{d_2})} = \mathbf{Z}$.*

PROOF. It is clear from Proposition 1.6 that $I_{\mathbf{Q}(\sqrt{d_1})} \cap I_{\mathbf{Q}(\sqrt{d_2})} \supset \mathbf{Z}$. Suppose that $z \in (I_{\mathbf{Q}(\sqrt{d_1})} \cap I_{\mathbf{Q}(\sqrt{d_2})}) \setminus \mathbf{Z}$. The proof now splits into cases. Suppose first that $d_1 \equiv d_2 \equiv 1 \pmod 4$. Then we have

$$z = m + n\left(1 + \sqrt{d_1}\right)/2 = m' + n'\left(1 + \sqrt{d_2}\right)/2$$

where m, n, m', n' are in $\mathbf{Z}$ and $n \neq 0 \neq n'$. Thus since $n \neq 0$,

$$r\sqrt{d_1} = r_1 + r_2\sqrt{d_2}, \qquad r_1, r_2 \in \mathbf{Q}.$$

This gives $\mathbf{Q}(\sqrt{d_1}) = \mathbf{Q}(r_1 + r_2\sqrt{d_2}) = \mathbf{Q}(r_2\sqrt{d_2}) = \mathbf{Q}(\sqrt{d_2})$ which implies $I_{\mathbf{Q}(\sqrt{d_1})} = I_{\mathbf{Q}(\sqrt{d_2})}$, a contradiction. The cases $d_1 \not\equiv 1 \equiv d_2 \pmod 4$ and $d_1 \equiv 1 \not\equiv d_2 \pmod 4$ (which are the same, by symmetry) and $d_1 \not\equiv 1 \not\equiv d_2 \pmod 4$ follow by the same argument. □

PROPOSITION 1.9. *If R is a discrete subring of $\mathbf{C}$, then $R \subset I_L$ for some imaginary quadratic field.*

PROOF [ADAPTED FROM PÓLYA [**23**, FOOTNOTE, p. 27]]. By Bourbaki [**63**, Theorem 1, p. 77] we have $R = \alpha\mathbf{Z}$ or $R = \alpha\mathbf{Z} + \beta\mathbf{Z}$ where $\alpha, \beta \in \mathbf{C}$ and in the second case α and β are linearly independent over $\mathbf{R}$. If $R = \alpha\mathbf{Z}$ we have $\alpha^2 = n\alpha$; so, $\alpha = n \in \mathbf{Z}$ unless $\alpha = 0$, in which case the conclusion is obvious. Then we have $R = n\mathbf{Z} \subset \mathbf{Z} \subset I_L$ for all L. If $R = \alpha Z + \beta Z$, we first show that $R \cap Z \neq \{0\}$. Since R is a ring we have

$$\alpha\beta = k\alpha + k'\beta, \tag{1}$$

$$\beta^2 = m\alpha + m'\beta, \tag{2}$$