Introduction to My Book “Essays in Constructive Mathematics”

Harold M. Edwards

Courant Institute of Mathematical Science hme1@scires.acf.nyu.edu

The point of view of the book derives from Leopold Kronecker (1823-1891), whose views were quite consonant with those of MAP. Kronecker resisted the overthrow of the Aristotelian (and Gaussian) prohibition of completed infinites on the ground that the overthrow was *unnecessary.* In other words, he committed himself to doing mathematics without completed infinites, basing his work on *algorithmic* proofs and constructions.

The book is divided into five parts, each being an algorithmic treatment of a different mathematical topic.

Part 1. The construction of a splitting field of a polynomial. The essential difficulty in this construction is the factorization of polynomials with coefficients in an algebraic number field. Kronecker sketched an algorithm that accomplishes this, but at the time I wrote my book on Galois theory I was unable to give a satisfactory exposition of either the algorithm or the proof that it was correct. Part 1 contains a detailed statement and proof of an algorithm that, in retrospect, is the one Kronecker sketched. It also applies the algorithm to the construction of splitting fields.

Part 2. Galois theory. The construction of Part 2 is a convenient basis for an algorithmic presentation of Galois theory. (In fact, Galois’s own presentation is quite algorithmic except that he took for granted that the roots of an equation were quantities with which one could compute according to the usual rules of arithmetic.) Part 2 also covers a few other topics in algebra, including the explicit construction of the splitting field of a general nth degree equation.

Part 3. Some quadratic problems. The primary problem solved in this part is $A\Box + B = \Box$, by which I mean the problem, “Given two positive integers A and B, find all integer solutions x and y of $Ax^2 + B = y^2$.” The algorithm developed for the complete solution is very similar to the continued fractions algorithm, but it is derived from ideas that have nothing to do with continued fractions and that lead not only to a proof of the law of quadratic reciprocity but also to a simplification of Gauss’s composition of binary quadratic forms. (It is important to notice that Gauss composed *forms,* which is what is done in the book, but that the modern development of the theory does not compose forms but only *equivalence classes* of forms.)

Part 4. The genus of an algebraic curve. This will be the topic of my second lecture, so I will not say more about it now.

Dagstuhl Seminar Proceedings 05021
Mathematics, Algorithms, Proofs
http://drops.dagstuhl.de/opus/volltexte/2006/280

Part 5. Miscellany. The first topic in this part is a proof of the so-called Fundamental Theorem of Algebra by means of an*algorithm* that embeds the splitting field of any given polynomial with integer coefficients in the field of complex numbers. The real *substance* of the theorem lies in the theorem of part 1 which implies that the splitting field can be described as the field obtained by adjoining one root of one irreducible, monic polynomial with integer coefficients to the field of rational numbers. The “Fundamental Theorem” then becomes the fairly simple exercise of proving that an irreducible, monic polynomial with integer coefficients has one complex root. Other topics in this part are a proof by infinite descent of the Sylow theorems in the theory of finite groups, and a constructive proof of the spectral theorem for symmetric matrices of integers.