THEORY OF ALGEBRAIC INTEGERS

Other books available in the Cambridge Mathematical Library:

A. Baker	*Transcendental number theory*
H.F. Baker	*Abelian functions*
N. Biggs	*Algebraic graph theory, 2nd edition*
S. Chapman & T.G. Cowling	*The mathematical theory of non-uniform gases*
G.H. Hardy	*A course of pure mathematics, 10th edition*
G.H. Hardy, J.E. Littlewood & G. Pólya	*Inequalities, 2nd edition*
D. Hilbert	*Theory of algebraic invariants*
W.V.D. Hodge & D. Pedoe	*Methods of algebraic geometry, volumes I, II & III*
R.W.H.T. Hudson	*Kummer's quartic surface*
A.E. Ingham	*The distribution of prime numbers*
H. Lamb	*Hydrodynamics*
F.S. Macaulay	*The algebraic theory of modular systems*
G.N. Watson	*A treatise on the theory of Bessel functions, 2nd edition*
E.T. Whittaker	*A treatise on the analytical dynamics of particles and rigid bodies*
A. Zygmund	*Trigonometric series*

Theory of Algebraic Integers

Richard Dedekind

Translated and introduced by John Stillwell

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published in French 1877

First published in English 1996

Library of Congress cataloging in publication data
Dedekind, Richard, 1831-1916.
Theory of algebraic integers / Richard Dedekind;
translated and with an introduction by John Stillwell
p. cm.
Includes bibliographical references and index.
ISBN 0-521-56518-9 (pbk.)
1. Algebraic number theory. 2. Integral representations.
I. Title
QA247.D43 1996
512′.74–dc20 96-1601 CIP

British Library cataloguing in publication data available

ISBN 0 521 56518 9 paperback

Transferred to digital printing 2004

Contents

Part one: Translator's introduction *page* 1
Translator's introduction 3
0.1 General remarks 3
0.2 Squares 6
0.2.1 Pythagorean triples 6
0.2.2 Divisors and prime factorisation 7
0.2.3 Irrational numbers 8
0.2.4 Diophantus 8
0.3 Quadratic forms 10
0.3.1 Fermat 10
0.3.2 The grit in the oyster 12
0.3.3 Reduction of forms 13
0.3.4 Lagrange's proof of the two squares theorem 15
0.3.5 Primitive roots and quadratic residues 16
0.3.6 Composition of forms 17
0.3.7 The class group 19
0.4 Quadratic integers 21
0.4.1 The need for generalised "integers" 21
0.4.2 Gaussian integers 22
0.4.3 Gaussian primes 24
0.4.4 Imaginary quadratic integers 25
0.4.5 The failure of unique prime factorisation 27
0.5 Roots of unity 29
0.5.1 Fermat's last theorem 29
0.5.2 The cyclotomic integers 30
0.5.3 Cyclotomic integers and quadratic integers 32
0.5.4 Quadratic reciprocity 36
0.5.5 Other reciprocity laws 38

0.6 Algebraic integers 39
0.6.1 Definition 39
0.6.2 Basic properties 40
0.6.3 Class numbers 41
0.6.4 Ideal numbers and ideals 42
0.7 The reception of ideal theory 44
0.7.1 How the memoir came to be written 44
0.7.2 Later development of ideal theory 45
Acknowledgements 47
Bibliography 48
Part two: Theory of algebraic integers 51
Introduction 53
1 Auxiliary theorems from the theory of modules 62
§1. Modules and their divisibility 62
§2. Congruences and classes of numbers 64
§3. Finitely generated modules 67
§4. Irreducible systems 71
2 Germ of the theory of ideals 83
§5. The rational integers 83
§6. The complex integers of Gauss 84
§7. The domain $\mathfrak{o}$ of numbers $x + y\sqrt{-5}$ 86
§8. Role of the number 2 in the domain $\mathfrak{o}$ 89
§9. Role of the numbers 3 and 7 in the domain $\mathfrak{o}$ 91
§10. Laws of divisibility in the domain $\mathfrak{o}$ 93
§11. Ideals in the domain $\mathfrak{o}$ 95
§12. Divisibility and multiplication of ideals in $\mathfrak{o}$ 98
3 General properties of algebraic integers 103
§13. The domain of all algebraic integers 103
§14. Divisibility of integers 105
§15. Fields of finite degree 106
§16. Conjugate fields 108
§17. Norms and discriminants 111
§18. The integers in a field Ω of finite degree 113
4 Elements of the theory of ideals 119
§19. Ideals and their divisibility 119
§20. Norms 121
§21. Prime ideals 123
§22. Multiplication of ideals 125
§23. The difficulty in the theory 126
§24. Auxiliary propositions 128

§25. Laws of divisibility 129
§26. Congruences 134
§27. Examples borrowed from circle division 138
§28. Classes of ideals 146
§29. The number of classes of ideals 147
§30. Conclusion 149
Index 153