

---

## INDEX

---

- algebraic geometry 91
- algebraic integers 44
- associate elements 36
- associative law 9
  
- Bézout domain 47
- binary operation 5
- binomial coefficient 55
- Boole, George 12
- Boolean ring 12
  
- cancellation law 20
- Carmichael number 95
- cartesian product 5
- circulant 86
- Classical Ideal
  - Theory 90
- common divisor 47
- common factor 47
- commutative law 9
- commutative ring 11
- congruence 28
- content of a
  - polynomial 68
- coprime 51
- cyclotomic
  - polynomial 77
  
- Dedekind 3, 90
- Dedekind ring 90, 91
- degree 43
- degree function 43
- degree of a
  - polynomial 21
  
- determinantal
  - identity 82
- Devlin, Keith 4, 34
- Dirichlet 3
- distributive law 9
- division algorithm 43
  - for integers 40
  - for polynomials 40
- divisor 36
- Dörrie, Heinrich 46
  
- Eisenstein 75
- Eisenstein's Irreducibility
  - Criterion 75
- embedding 18
- Euclidean domain 43
- Euclid's algorithm 48
- Euclid's Elements 39
- evaluation 14
  
- factor 36
- Factor Theorem 63
- Fermat, Pierre 31
- Fermat's Last
  - 'Theorem' 2, 46
- Fermat's Little
  - Theorem 31
- field 24
- field of fractions 26
- formal power series 7
- Fraenkel, A. A. 5
- Fundamental Theorem of
  - Algebra 1, 64
- Fundamental Theorem of
  - Arithmetic 1

110 *Index*

- Galois, Evariste 31
- Galois field 31
- Gauss 2, 31
- Gaussian integer 18, 43
- Gauss's Lemma 68
- greatest common divisor (GCD) 47
- greatest common divisor (GCD) domain 47
- group of units 23
  
- Hamilton, Sir William 27
- Hardy, G. H. 45
- highest common factor (HCF) 47
- Hilbert, David 90
- homogeneous polynomial 83
- homological algebra 91
- homomorphism 13
  
- ideal 3, 90
- identity element 9
- image of a mapping 17
- indeterminate 7, 11
- integral domain 20
- irreducible element 37
- isomorphism 18
  
- Kaplansky, Irving 91
- Kronecker 78, 90
- Kronecker's method 78, 80
- Kummer 3, 90
  
- Lagrange's Interpolation Formula 78
- Lagrange's Theorem 32
- Leibniz 33
- Lenstra, A. K. 81
- Lenstra, H. W. 4, 81
- linear factor 65
- Lovász, L. 81
  
- monic polynomial 35
- Multiplicative Ideal Theory 90
  
- negative 9
- Noether, Emmy 90
- Noetherian ring 91
- norm 38, 43
- Northcott, D. G. 91
  
- order of a power series 22
  
- polynomial 7
- polynomial ring 11
- power series 7
- prime element 53
- prime ideal 90
- prime number 37, 53
- primitive polynomial 68
- principal ideal domain 91
- proper divisors of zero 20
- proper factor 36
- Public-Key Cryptography 3
  
- quadratic polynomial 66
- quaternion 27
- quotient 40
  
- regular local ring 91
- relatively prime 51
- remainder 40
- Remainder Theorem 63
- residue class 29
- ring 9
  
- Samuel, Pierre 91
- Stewart, Ian 65
- subring 15
- Subring Criterion 16
- symmetric difference 12

*Index*

111

- |                        |    |                   |    |
|------------------------|----|-------------------|----|
| Tall, David            | 65 | Waring            | 33 |
| trisection of an angle | 67 | Well-Ordering     |    |
| trivial ring           | 10 | Principle         | 40 |
| two-squares theorem    | 56 | Wilson, Sir John  | 33 |
| unique factorization   |    | Wilson's Theorem  | 32 |
| domain (UFD)           | 37 | Yellow Brick Road | 62 |
| unit                   | 23 | zero element      | 9  |
| Vandermonde's          |    |                   |    |
| determinant            | 84 |                   |    |