

# Index

- abelian closure, 48
- absolute coordinate ring, 223
- absolute function field, 223, 225
- absolutely irreducible
  - affine algebraic set, 223
  - projective algebraic set, 225
- adèle, 45
  - principal, 45
- adèle ring, 45
- affine algebraic set, 222
  - absolutely irreducible, 223
  - irreducible, 222
  - reducible, 222
- affine  $n$ -space, 219
- affine variety, 223
  - dimension of, 224
  - smooth, 224
- AG code, 143
- algebraic curve, 225
- algebraic function field, 1, 219
- algebraic-geometry code, 143
- almost perfect sequence, 177
- approximation theorem, 6
- Artin reciprocity, 48
- Artin reciprocity map
  - global, 48
  - local, 47
- Artin-Schreier degenerate, 63
- Artin-Schreier extension, 63
- Artin-Schreier nondegenerate, 63
- Artin symbol, 20
- asymptotically bad tower, 124
- asymptotically good tower, 124
- asymptotic Gilbert-Varshamov bound, 152
- authentication scheme, 189
- basis, 12
  - $P$ -integral, 12
- canonical generator matrix, 142
- Carlitz module, 73
- Cauchy sequence, 37
- ciphertext, 170
- class field theory
  - global, 48
  - local, 47
- closed point, 220–222, 225
  - degree of, 220, 221
- complementary set, 12
- complete splitting, 11
- complete system of representatives, 38
- complete valued field, 37
- completion, 37
  - $P$ -adic, 37
- conductor, 42
- conductor exponent, 41
- conductor theorem, 49
- conjugate place, 14
- constant field extension, 20
- continued fraction expansion, 172
- convergent sequence, 36
- coordinate, 220
  - homogeneous, 220
- coordinate ring, 223
  - absolute, 223
- curve
  - projective, 225
  - projective algebraic, 225

## INDEX

241

- cyclotomic function field, 66
- deception probability, 189
- decomposition field, 16
- decomposition group, 16
- defined over  $\mathbf{F}_q$ , 222, 224
- degree
  - of closed point, 220, 221
  - of divisor, 3
  - of place, 2
- different, 12
- different exponent, 12
- digital method, 197
- digital strict  $(t, m, s)$ -net, 197
- digital strict  $(t, s)$ -sequence, 200
- digital  $(t, m, s)$ -net, 197
- digital  $(t, s)$ -sequence, 200
- dimension
  - of affine variety, 224
  - of code, 141
  - of projective variety, 225
- discrete valuation, 36
- discriminant, 12
- divisor, 3
  - degree of, 3
  - equivalent, 7
  - $\mathbf{F}_q$ -rational, 23
  - global different, 13
  - nonspecial, 4
  - pole, 3
  - positive, 3
  - principal, 3
  - support of, 3
  - zero, 3
- divisor class, 7
- divisor class group, 6
  - of degree zero, 7
- divisor group, 6
  - of degree zero, 6
- $d$ -perfect sequence, 177
- Drinfeld  $A$ -module, 72
- Eisenstein criterion, 11
- Eisenstein polynomial, 11
- elementary interval, 193
- elliptic function field, 4
- entropy function, 152
- equivalent code, 145
- equivalent divisor, 7
- explicit Weil formulas, 33
- $\varepsilon$ -almost strongly universal, 187
- $\varepsilon$ -almost universal, 187
- finite place, 3
- $\mathbf{F}_q$ -closed point, 220, 221
- $\mathbf{F}_q$ -conjugate point, 220, 221
- $\mathbf{F}_q$ -isomorphic curves, 226
- $\mathbf{F}_q$ -isomorphism, 226
- $\mathbf{F}_q$ -morphism, 225
- $\mathbf{F}_q$ -rational divisor, 23
- $\mathbf{F}_q^m$ -rational point, 220, 221
- $\mathbf{F}_q^m$ -rational point set, 219
- $\mathbf{F}_q^n$ -rational place, 26
- fractional ideal class group, 7
- fractional ideal class number, 7
- fractional ideal group, 7
- fractional  $\mathcal{S}$ -ideal, 7
- fractional  $\mathcal{S}$ -ideal class group, 7
- fractional  $\mathcal{S}$ -ideal group, 7
- Frobenius automorphism, 19
- Frobenius symbol, 19
- full constant field, 1, 219
- function field, 219, 223, 225
  - absolute, 223, 225
  - algebraic, 1, 219
  - cyclotomic, 66
  - elliptic, 4
  - global, 6, 44
  - global maximal, 64
  - global optimal, 32
  - Hermitian, 65
  - rational, 2
- function-field code, 144

- gap number, 5
- Garcia-Stichtenoth tower, 136, 137
- generalized Rueppel sequence, 179
- generating function, 171
  - irrational, 171
  - rational, 171
- generating matrices, 197, 200
- generator matrix, 141
  - canonical, 142
- genus, 4, 226
- Gilbert-Varshamov bound, 151
  - asymptotic, 152
- global Artin reciprocity map, 48
- global class field theory, 48
- global different divisor, 13
- global field, 44
- global function field, 6, 44
  - maximal, 64
  - optimal, 32
  - with many rational places, 76
- $G$ -module, 55
- Golod-Shafarevich condition, 61
- Golod-Shafarevich theorem, 57
- Goppa's construction, 143, 156
- group of divisor classes of degree zero, 7
  
- Hamming weight, 141
- hash family, 186
- Hasse-Arf theorem, 41
- Hasse-Weil bound, 30
- Hermitian function field, 65
- Hilbert class field, 50, 58
- Hilbert class field tower, 57, 58
- Hilbert different formula, 19
- homogeneous coordinate, 220
- homogeneous ideal, 224
- homogeneous polynomial, 224
- Hurwitz genus formula, 13
  
- idèle, 45
- idèle class group, 45
- idèle group, 45
  
- impersonation attack, 189
- inertia field, 16
- inertia group, 16, 39
- infinite place, 3
- information rate, 150
- integral basis, 12
- integral  $\mathcal{S}$ -ideal, 7
- irrational generating function, 171
- irreducible affine algebraic set, 222
- irreducible projective algebraic set, 225
- isomorphic curves, 226
  - $\mathbb{F}_q$ , 226
- isomorphism of curves, 226
  - $\mathbb{F}_q$ , 226
  
- key, 170
- keystream, 170
- Kummer degenerate, 62
- Kummer extension, 62
- Kummer nondegenerate, 62
  
- length of code, 141
- linear code, 141
  - optimal, 163
- linear complexity, 171
- linear complexity profile, 175
- linear recurrence relation, 171
- linear recurring sequence, 171
- local Artin reciprocity map, 47
- local class field theory, 47
- local expansion, 6, 38
- local parameter, 5
- local ring, 223, 224
- low-discrepancy point set, 193
- low-discrepancy sequence, 193
- $L$ -polynomial, 29
  - $n$ th, 29
- $\ell$ -rank, 58, 127
- $(\ell, \mathcal{S})$ -Hilbert class field, 58
- $(\ell, \mathcal{S})$ -Hilbert class field tower, 58
  
- maximal global function field, 64

## INDEX

243

- maximal ideal, 2, 37
- minimum distance, 141
- minimum weight, 141
- morphism, 225
  - $\mathbb{F}_q$ -, 225
- morphism over  $\mathbb{F}_q$ , 225
- M-torsion element, 73
- M-torsion module, 73
  
- narrow ray class extension, 52
- narrow ray class field, 52
- narrow ray class group, 52
- net
  - digital strict  $(t, m, s)$ -, 197
  - digital  $(t, m, s)$ -, 197
  - strict  $(t, m, s)$ -, 193
  - $(t, m, s)$ -, 193
- Newton polygon, 38
- nonspecial divisor, 4
- nonspecial prime power, 98
- norm, 11
- normalized discrete valuation, 1, 36
- norm residue symbol, 48
- $n$ th  $L$ -polynomial, 29
- $n$ th zeta function, 28
- NXL code, 156
  
- optimal global function field, 32
- optimal linear code, 163
- optimal tower, 124
- over-set, 11
  
- $P$ -adic completion, 37
- parity-check matrix, 142
- perfect hash family, 184
- perfect sequence, 177
- $P$ -integral basis, 12
- place, 1
  - complete splitting of, 11
  - conjugate, 14
  - degree of, 2
  - finite, 3
  - $\mathbb{F}_{q^n}$ -rational, 26
  - infinite, 3
  - ramified, 10, 16
  - rational, 2
  - relative degree of, 10
  - tamely ramified, 14, 16
  - totally ramified, 10, 11
  - unramified, 10, 16
  - wildly ramified, 14, 16
- plaintext, 170
- Plotkin bound, 151
- point, 220
  - closed, 220–222, 225
  - $\mathbb{F}_q$ -closed, 220, 221
  - $\mathbb{F}_q$ -conjugate, 220, 221
  - $\mathbb{F}_{q^m}$ -rational, 220, 221
  - rational, 220
- pole divisor, 3
- pole number, 5
- pole of element, 3
- pole of function, 223
- positive divisor, 3
- prime element, 5
- prime ideal, 8
- principal adèle, 45
- principal divisor, 3
- principal divisor group, 6
- principal  $\mathcal{S}$ -ideal, 7
- projective algebraic curve, 225
- projective algebraic set, 224
  - absolutely irreducible, 225
  - irreducible, 225
  - reducible, 225
- projective curve, 225
- projective  $n$ -space, 220
- projective variety, 225
  - dimension of, 225
  - smooth, 225
- propagation rule, 164
  
- quality parameter, 193, 195

- quasi-Monte Carlo method, 192
- ramification field, 16
- ramification group, 16, 39
  - upper, 41
- ramification index, 10, 37
- ramified place, 10, 16
- rational function field, 2
- rational generating function, 171
- rational place, 2
- rational point, 220
- ray class extension, 52
  - narrow, 52
- ray class field, 49
  - narrow, 52
- ray class group, 10, 46
  - narrow, 52
- reducible affine algebraic set, 222
- reducible projective algebraic set, 225
- relative degree, 10
- relative minimum distance, 150
- residue class field, 2, 37
- Riemann-Roch space, 4
- Riemann-Roch theorem, 4, 226
- Rueppel sequence, 179
  - generalized, 179
- $\mathcal{S}$ -congruence subgroup, 46
- sequence
  - digital strict  $(t, s)$ -, 200
  - digital  $(t, s)$ -, 200
  - generalized van der Corput, 201
  - strict  $(t, s)$ -, 195
  - $(t, s)$ -, 195
- Serre bound, 31
- sgn-normalized, 73
- $\mathcal{S}$ -Hilbert class field, 50
- $\mathcal{S}$ -Hilbert class field tower, 57
- $\mathcal{S}$ -ideal, 7
  - fractional, 7
  - integral, 7
  - principal, 7
- $\mathcal{S}$ -idèle class group, 46
- $\mathcal{S}$ -idèle group, 45
- sign function, 51
- Singleton bound, 142
- $\mathcal{S}$ -integral ring, 7, 45
- smooth affine variety, 224
- smooth projective variety, 225
- splits completely, 11
- $\mathcal{S}$ -ray class group, 10, 46
- star discrepancy, 192
- stream cipher, 170
- substitution attack, 189
- subtower of function fields, 122
- support of divisor, 3
- system, 198
  - $(d, m, s)$ -, 198
- tamely ramified place, 14, 16
- Tate cohomology, 55, 127
- Tate cohomology group, 55
- totally ramified place, 10, 11
- tower formulas, 10, 12, 13
- tower of function fields, 122
- trace, 11
- transcendence degree, 219
- unramified extension, 13
- unramified place, 10, 16
- upper ramification group, 41
- valid message, 189
- valuation, 1, 36
- valuation ring, 2, 37
- valued field, 36
  - complete, 37
- variety
  - affine, 223
  - projective, 225
  - smooth affine, 224
  - smooth projective, 225
- Vlăduț-Drinfeld bound, 34

Cambridge University Press

978-0-521-66543-8 - Rational Points on Curves over Finite Fields: Theory and Applications

Harald Niederreiter and Chaoping Xing

Index

[More information](#)*INDEX*

245

Weierstrass gap theorem, 5

weight, 141

wildly ramified place, 14, 16

XNL code, 161

zero divisor, 3

zero(s)

of element, 3

of function, 223

set of, 222

zero set, 222

zeta function, 26

 $n$ th, 28