BIBLIOGRAPHY

General

Cohn, P.M., *Algebra, Volumes 1 and 2*, John Wiley and Sons, New York, 1989 Dummit, D.S. and Foote, R.M., *Abstract Algebra*, Prentice-Hall, Upper Saddle River, NJ, 1999

Hungerford, T.M., Algebra, Springer-Verlag, New York, 1974

Isaacs, I.M., Algebra, a Graduate Course, Brooks-Cole, a division of Wadsworth, Inc., Pacific Grove, CA, 1994

Jacobson, N., Basic Algebra I and II, W.H. Freeman and Company, San Francisco, 1980 Lang, S., Algebra, Addison-Wesley, Reading, MA, 1993

Modules

Adkins, W.A., and Weintraub, S.H., Algebra, An Approach via Module Theory, Springer-Verlag, New York, 1992

Blyth, T.S., Module Theory, Oxford University Press, Oxford, 1990

Basic Group Theory

Alperin, J.L., and Bell, R.B., *Groups and Representations*, Springer-Verlag, New York, 1995 Humphreys, J.F., *A Course in Group Theory*, Oxford University Press, Oxford 1996 Robinson, D.S., *A Course in the Theory of Groups*, Springer-Verlag, New York, 1993 Rose, J.S., *A Course on Group Theory*, Dover, New York, 1994 Rotman, J.J., *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1998

Fields and Galois Theory

Adamson, I.T., Introduction to Field Theory, Cambridge University Press, Cambridge, 1982 Garling, D.J.H., A Course in Galois Theory, Cambridge University Press, Cambridge, 1986 Morandi, P., Fields and Galois Theory, Springer-Verlag, New York, 1996 Roman, S., Field Theory, Springer-Verlag, New York, 1995 Rotman, J.J., Galois Theory, Springer-Verlag, New York, 1998

Algebraic Number Theory

Borevich, Z.I., and Shafarevich, I.R., *Number Theory*, Academic Press, San Diego, 1966 Fröhlich, A., and Taylor, M.J., *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991

Gouvea, F.Q., p-adic Numbers, Springer-Verlag, New York, 1997

Janusz, G.J., Algebraic Number Fields, American Mathematical Society, Providence, 1996 Lang, S., Algebraic Number Theory, Springer-Verlag, New York, 1994

Marcus, D.A., Number Fields, Springer-Verlag, New York, 1977

Samuel, P., Algebraic Theory of Numbers, Hermann, Paris, 1970

Algebraic Geometry and Commutative Algebra

Atiyah, M.F., and Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969

Bump, D., Algebraic Geometry, World Scientific, Singapore, 1998

Cox, D., Little, J., and O'Shea, D., *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York, 1992

Eisenbud, D., Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995

Fulton, W., Algebraic Curves, W.A. Benjamin, New York, 1969

Hartshorne, R., Algebraic Geometry, Springer-Verlag, New York, 1977

Kunz, E., Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, 1985

Matsumura, H., Commutative Ring Theory, Cambridge University Press, Cambridge, 1986 Reid, M., Undergraduate Algebraic Geometry, Cambridge University Press, Cambridge, 1988 Reid, M., Undergraduate Commutative Algebra, Cambridge University Press, Cambridge, 1995

Shafarevich, I.R., Basic Algebraic Geometry, Volumes 1 and 2, Springer-Verlag, New York 1988

Ueno, K., Algebraic Geometry 1, American Mathematical Society, Providence 1999

Noncommutative Rings

Anderson, F.W., and Fuller, K.R., Rings and Categories of Modules, Springer-Verlag, New York, 1992

Beachy, J.A., Introductory Lectures on Rings and Modules, Cambridge University Press, Cambridge, 1999

Farb, B., and Dennis, R.K., *Noncommutative Algebra*, Springer-Verlag, New York, 1993 Herstein, I.N., *Noncommutative Rings*, Mathematical Association of America, Washington, D.C., 1968

Lam, T.Y., A First Course in Noncommutative Rings, Springer-Verlag, New York, 1991

Group Representation Theory

Curtis, C.W., and Reiner, I., Methods of Representation Theory, John Wiley and Sons, New York, 1981

Curtis, C.M., and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, John Wiley and Sons, New York, 1966

Dornhoff, L., Group Representation Theory, Marcel Dekker, New YOrk, 1971

James, G., and Liebeck, M., Representations and Characters of Groups, Cambridge University Press, Cambridge, 1993

Homological Algebra

Hilton, P.J., and Stammbach, U., A Course in Homological Algebra, Springer-Verlag, New York, 1970

Hilton, P., and Wu, Y-C., A Course in Modern Algebra, John Wiley and Sons, New York, 1974

Mac Lane, S., Categories for the Working Mathematician, Springer-Verlag, New York, 1971 Rotman, J.J., An Introduction to Algebraic Topology, Springer-Verlag, New York, 1988

Rotman, J.J., An Introduction to Homological Algebra, Springer-Verlag, New York, 1979

Weibel, C.A., An Introduction to Homological Algebra, Cambridge University Press, Cambridge, 1994

List of Symbols

```
Throughout the text, \subseteq means subset, \subset means proper subset
\mathbb{Z}_n integers modulo n 1.1
\mathbb{Z} integers 1.1
\langle A \rangle subgroup generated by A 1.1
S_n symmetric group 1.2
A_n alternating group 1.2
D_{2n} dihedral group 1.2
\varphi Euler phi function 1.1, 1.3
\leq normal subgroup 1.3
\triangleleft proper normal subground 1.3
ker kernel 1.3, 2.2
\cong isomorphism 1.4
Z(G) center of a group 1.4
H \times K direct product 1.5
\mathbb{Q} rationals 2.1
M_n(R) matrix ring 2.1
R[X] polynomial ring 2.1
R[[X]] formal power series ring 2.
End endomorphism ring 2.1
\langle X \rangle ideal generated by X
UFD unique factorization domain 2.6
PID principal ideal domain 2.6
ED Euclidean domain 2.7
min(\alpha, F) minimal polynomial 3.1
\bigvee_{i} K_{i} composite of fields 3.1
Gal(E/F) Galois group 3.5
0 the module \{0\} and the ideal \{0\} 4.1
\bigoplus_i M_i direct sum of modules 4.3
\sum_{i} M_{i} sum of modules 4.3
\overline{\operatorname{Hom}}_R(M,N) set of R-module homomorphisms from M to N
\operatorname{End}_R(M) endomorphism ring 4.4
g \bullet x group action 5.1
G' commutator subgroup 5.7
G^{(i)} derived subgroups 5.7
\langle S \mid K \rangle presentation of a group
\mathcal{F}(H) fixed field 6.1
\mathcal{G}(K) fixing group 6.1
GF(p^n) finite field with p^n elements 6.4
\Psi_n(X) n^{th} cyclotomic polynomial 6.5
\Delta product of differences of roots 6.6
D discriminant 6.6,7.4
N[E/F] norm 7.3
T[E/F] trace 7.3
char characteristic polynomial 7.3
n_P(I) exponent of P in the factorization of I 7.7
v_p p-adic valuation 7.9
| \cdot |_p p-adic absolute value 7.9
V(S) variety in affine space 8.1
I(X) ideal of a set of points 8.1
k[X_1,\ldots,X_n] polynomial ring in n variables over the field k 8.1
\sqrt{I} radical of an ideal 8.3
k(X_1, \ldots, X_n) rational function field over k = 8.4
```

 $S^{-1}R$ localization of the ring R by S 8.5

 $S^{-1}M$ localization of the module M by S 8.5

 $\mathcal{N}(R)$ nilradical of the ring R 8.6

 $M \otimes_R N$ tensor product of modules 8.7

UMP universal mapping property 8.7

 $A \otimes B$ tensor (Kronecker) product of matrices 8.7

kG group algebra 9.5

RG group ring 9.5

J(M), J(R) Jacobson radical 9.7

 $\operatorname{Hom}_R(M,-), \operatorname{Hom}_R(-,N)$ hom functors 10.3

 $M \otimes_R -, - \otimes_R N$ tensor fuctors 10.3

 \mathbb{Q}/\mathbb{Z} additive group of rationals mod 1 10.6 (also 1.1, Problem 7)

 $\mathbb{Z}(p^{\infty})$ quasicyclic group A10

G[n] elements of G annihilated by n A10

 H_n homology functor S1

 $f \simeq g$ chain homotopy S1

∂ connecting homomorphism S2, S3

 $P_* \to M$ projective resolution S4

 $M \to E_*$ injective resolution S4

 $L_n F$ left derived functor S5

 R^nF right derived functor S5

Tor derived functor of \otimes S5

Ext derived functor of Hom S5

INDEX

abelian category 10.4 abelian group 1.1 absolute value 7.9 action of a group on a set 5.1 adjoint associativity 10.7 adjoint functors 10.7 affine n-space 8.1 affine variety 8.1 AKLB setup 7.3 algebra 4.1 algebraic closure 3.3, 10.9 algebraic curve 8.3 algebraic element 3.1 algebraic extension 3.1 algebraic function field 6.9 algebraic geometry 8.1ff algebraic integers 7.1 algebraic number 3.3, 7.1 algebraic number theory 7.1ff, 7.3 algebraically closed field 3.3 algebraically independent set 6.9 algebraically spanning set 6.9 alternating group 1.2 annihilator 4.2, 9.2, 9.7 archimedian absolute value 7.9 Artin-Schreier theorem 6.7 Artinian modules 7.5 Artinian rings 7.5 ascending chain condition (acc) 2.6, 7.5 associates 2.6 associative law 1.1, 2.1 automorphism 1.3

Baer's criterion 10.6 base change 10.8 basis 4.3 bilinear mapping 8.7 binomial expansion modulo p 3.4 binomial theorem 2.1 boundary S1

canonical map 1.3 category 10.1 Cauchy's theorem 5.4 Cayley's theorem 5.1 center of a group 1.4 center of a ring 4.1 central series 5.7 centralizer 5.2 chain complex S1 chain homotopy S1 chain map S1 chain rule 1.3, 3.1 character 6.1 characteristic of a ring or field 2.1 characteristic polynomial 7.3 characteristic subgroup 5.7 chief series 5.6 Chinese remainder theorem 2.3 class equation 5.2 cokernel 10.1 colorings 5.3 commutative diagram 1.4 commutative ring 2.1 commutator 5.7 compatible morphisms 10.9 complete ring of fractions 2.8 composite of fields $3.1,\,6.2$ composition factors 5.6, 7.5 composition length 5.6, 7.5 composition of morphisms 10.1 composition series 5.6, 7.5 conjugate elements 5.1, 5.2 conjugate subfields 6.2 conjugate subgroups 5.1, 6.2 conjugates of a field ement 3.5 conjugation 5.1, 5.2-1connecting homomorphism S2, S3 constructible numbers and points 6.8 content 2.9 contravariant functor 10.3 coproduct 10.2 core 5.1 correspondence theorem for groups 1.4 correspondence theorem for modules 4.2 correspondence theorem for rings 2.3 coset 1.3counting two ways 5.3 covariant functor 10.3 cycle 1.2, S1 cyclic extension 6.7 cyclic group 1.1 cyclic module 4.2, 9.1, 9.2, 9.7 cyclotomic extension.5 cyclotomic field 6.5, 7.2 cyclotomic polynomial 6.5 decomposable module 9.6

decomposable module 9.6
Dedekind domain 7.6, 7.7
Dedekind's lemma 6.1, 6.7, 7.3, 7.4
degree 2.5
deleted projective (or injective) resolution S4
derivative of a polynomial 3.4
derived functors S5
derived length 5.7
derived series 5.7
descending chain condition 7.5

diagram chasing 4.7

differential S1

dihedral group 1.2, 5.8, 5.8 (infinite dilhedral group), 9.5

direct limit 10.9

direct product of groups 1.5

direct product of modules 4.3

direct product of rings 2.3

direct sum of modules 4.3

direct system 10.9

directed set 10.9

discriminant 6.6, A6, 7.4

divides means contains 2.6, 7.7

divisible abelian group A10

divisible module 10.6

division ring 2.1, 9.1

double centralizer 9.2

double dual functor 10.3

dual basis 7.4

duality 10.1

duplicating the cube 6.8

Eisenstein's irreducibility criterion 2.9

elementary divisors 4.6

elementary symmetric functions 6.1

embedding 3.3,3.5

embedding in an injective module 10.7

endomorphism 1.3,4.4

epic 10.1

epimorphism 1.3

equivalent absolute values 7.9

equivalent matrices 4.4

equivalent matrix representations 9.5

Euclidean domain 2.7

Euler's identity 2.1

Euler's theorem 1.3

evaluation map 2.1

exact functor 8.5, 10.4

exact sequence 4.7

exponent of a group 1.1, 6.4

Ext S5

extension of a field 3.1

extension of scalars 8.7, 10.8

exterior algebra 8.8

F-isomorphism, etc. 3.2

factor theorem for groups 1.4

factor theorem for modules 4.2

factor theorem for rings 2.3

faithful action 5.1

faithful module 7.1, 9.2, 9.4

faithful representation 9.5

Fermat primes 6.8

Fermat's little theorem 1.3

field 2.1

field discriminant 7.4

finite abelian groups 4.6

finite extension 3.1

finite fields 6.4

finitely cogenerated module 7.5

finitely generated algebra 10.8

finitely generated module 4.4

finitely generated submodule 7.5

five lemma 4.7

fixed field 6.1

fixing group 6.1

flat modules 10.8

forgetful functor 10.3

formal power series 2.1, 8.2

four group 1.2, 1.5, A6

four lemma 4.7

fractional ideal 7.6

Frattini argument 5.8-2

free abelian gup functor 10.3

free group 5.8-1

free module 4.3,15

free product 10.2-2

Frobenius automorphism 3.4, 6.4

full functor 10.3

full ring of fractions 2.8

full subcategory 10.3

functor 10.3

fundamental decomposition theorem (for finitely generated modules over a PID) 4.6

fundamental theorem of Galois theory 6.2-1

Galois extension 3.5, 6.1ff.

Galois group 3.5, 6.1ff

Galois group of a cubic, 6.6

Galois group of a polynomial 6.3

Galois group of a quadratic 6.3

Galois group of a quartic A6

Gauss' lemma 2.9

Gaussian integers 2.1, 2.7

general equation of degree n 6.8

general linear group 1.3

generating set 4.3

generators and relations 1.2, 4.6, 5.8

greatest common divisor 2.6, 7.7

group 1.1

group algebra 9.5

group representations 9.5

group ring 9.5

Hermite normal form 4.5

Hilbert basis theorem 8.2

Hilbert's Nullstellensatz 8.3, 8.4

Hilbert's Theorem 90 7.3

hom functors 10.3-1

homology functors S1

homology group S1

homology module S1

homomorphism from R to M determined by what it does to the identity, 9.4, S6

homomorphism of algebras 4.1

homomorphism of groups 1.3

homomorphism of modules 4.1

homomorphism of rings 2.2

Hopkins-Levitzki theorem 9.8

hypersurface 8.2

ideal 2.2, 8.1

ideal class group 7.8

idempotent linear transformation 9.5

image 2.3, 4.1

indecomposable module 9.6

index 1.3

inductive limit 10.9

initial object 10.1

injection (inclusion) 4.7

injective hull 10.7

injective modules 10.6

injective resolution S4

inner automorphism 1.4, 5.7

integral basis 7.2, 7.4

integral closure 7.1

integral domain 2.1

integral extensions 7.1

integral ideal 7.6

integrally closed 7.1

invariant factors 4.5

inverse limit 10.9

inverse system 10.9

inversions 1.2

irreducible element 2.6

irreducible ideal 8.6

irreducible polynomial 2.9

irreducible variety 8.1

isomorphic groups 1.1

isomorphism 1.3

isomorphism extension theorem 3.2

isomorphism theorems for groups 1.4

isomorphism theorems for modules 4.2

isomorphism theorems for rings 2.3

Jacobson radical 9.7

Jacobson's theorem 9.2

Jordan-Holder theorem 5.6, 7.5

kernel 1.3, 2.2, 10.1

kernel of an action 5.1

Kronecker product of matrices 8.7

Krull-Schmidt theorem 9.6

Kummer extension 6.7

Lagrange interpolation formula 2.5

Lagrange's theorem 1.3

Laurent series 7.9

leading coefficient 2.5

least common multiple 2.6, 7.7

left adjoint 10.7

left cancellable 10.1

left derived functors S5

left exact functor 10.4

left ideal 2.2

left resolution S4

left-Noetherian ring 9.8

left-quasiregular element 9.7

left-semisimple ring 9.6

length of a module 7.5

lifting of a map 4.3, 10.2

linearly indepdent set 4.3

local ring 2.4, 7.9, 8.5

localization 2.8, 8.5

long division 6.4

long exact homology sequence S3

Maschke's theorem 9.6

matrices 2.1, 4.4

maximal ideal 2.4, 8.3

maximal submodule 9.7

metric 7.9

minimal generating set 9.8

minimal left ideal 9.3

minimal polynomial 3.1

minimal prime ideal 8.4

modding out 5.7

modular law 4.1

module 4.1

modules over a principal ideal domain 4.6, 10.5

monic 10.1

monoid 1.1

monomorphism 1.3

morphism 10.1

Nakayama's lemma 9.8

natural action 5.3, 6.3

natural map 1.3

natural projection 4.7, 7.5, 9.2, 9.4, 9.5, 10.5

natural transformation 10.3

naturality S3

Newton's identities A6

nil ideal 9.7

nilpotent element 8.6, 9.7

nilpotent group 5.7

nilpotent ideal 9.7

nilradical 8.6

Noetherian modules 4.6, 7.5

Noetherian rings 4.6, 7.5

nonarchimedian absolute value 7.9

noncommuting indeterminates 9.8

nontrivial ideal 2.2

norm, 7.1, 7.3

normal closure, 3.5

normal extension 3.5 normal series 5.6 normal Sylow p-subgroup 5.5 normalizer 5.2 Nullstellensatz 8.3, 8.4 number field 7.1

objects 10.1 opposite category 10.1 opposite ring 4.4 orbit 5.2 orbit-counting theorem 5.3 orbit-stabilizer theorem 5.2 order 1.1 order ideal 4.2 orthogonal idempotents 9.6 Ostrowski's theorem 7.9

p-adic absolute value 7.9 p-adic integers 7.9 p-adic numbers 7.9 p-adic valuation 7.9 p-group 5.4 perfect field 3.4 permutation 1.2 permutation group 1.2 permutation module 9.5 polynomial rings 2.1, 2.5 polynomials over a field 3.1 power sums, A6 preordered set 10.2 primary component A10 primary decomposition 8.6 primary ideal 8.6 prime element 2.6hbn prime ideal 2.4 primitive element, theorem of 3.5, 6.6 primitive polynomial 2.9 principal ideal domain 2.6 product 10.2 product of an ideal and a module 9.3 product of ideals 2.3, 8.5, 7.6 projection 4.7, 9.2, 9.4, 9.5, 10.5 projection functor 10.3 projective basis lemma 10.5 projective limit 10.9 projective modules 9.8, 10.5 projective resolution S4 proper ideal 2.2 Prufer group A10 pullback 10.6 purely inseparable 3.4 pushout 10.6,3

quadratic extensions 6.3, 7.2 quasicyclic group A10

quasi-regular element 9.7

quaternion group 2.1

quaternions 2.1

quotient field 2.8

quotient group 1.3

quotient ring 2.2

R-homomorphism on R 9.4

Rabinowitsch trick 8.4

radical extension 6.8

radical of an ideal 8.3

rank of a free module 4.4

rational integer 7.2

rational root test 2.9

rationals mod 1 1.1 (Problem 7), 10.4, 10.6, A10

refinement 5.6

regular action 5.1, 5.2

regular n-gon 6.8

regular representation 9.5

relatively prime ideals 2.3

remainder theorem 2.5

representation 9.5

residue field 9.8

resolvent cubic A6

restriction of scalars 8.7, 10.8

right adjoint 10.7

right cancellable 10.1

right derived functors S5

right exact functor 10.4

right ideal 2.2

right resolution S4

right-Noetherian ring 9.8

right-quasiregular element 9.7

right-semisimple ring 9.6

ring 2.1

ring of fractions 2.8, 8.5

Schreier refinement theorem 5.6

Schur's lemma 9.2

semidirect product 5.8

semigroup 1.1

semisimple module 9.1

semisimple ring 9.3

separable element 3.4

separable extension 3.4

separable polynomial 3.4

series for a module 7.5

simple group 5.1, 5.5

simple left ideal 9.3

simple module 7.5, 9.1, 9.2

simple ring 9.3, 9.5

simplicity of the alternating group 5.6

simultaneous basis theorem 4.6

skew field 2.1

Smith normal form 4.5

snake diagram S2

snake lemma S2

solvability by radicals 6.8

solvable group 5.7

spanning set 4.3, 6.9

special linear group 1.3

split exact sequence 4.7, 5.8

splitting field 3.2

squaring the circle 6.8

standard representation of a p-adic integer 7.9

Steinitz exchange 6.9

Stickelberger's theorem 7.4

subcategory 10.3

subgroup 1.1

submodule 4.1

subnormal series 5.6

subring 2.1

sum of ideals 2.2

sum of modules 4.3

Sylow p-subgroup 5.4

Sylow theorems 5.4

symmetric group 1.2, 6.6

symmetric polynomial 6.1

tensor functors 10.3

tensor product of matrices 8.7

tensor product of module homomorphisms 8.7

tensor product of modules 8.7

terminal object 10.1

Tor S5

torsion abelian group 8.7 (Problem 3), 10.2

torsion element 4.6 torsion module 4.6

torsion subgroup A10

torsion submodule 4.6

torsion-free module 4.6

trace 7.3

transcendence basis 6.9

transcendence degree 6.9

transcendental element 3.1

transcendental extension 6.9

transcendental number 3.3

transitive action 5.2

transitive subgroup of S_n 6.3

transitivity of algebraic extensions 3.3

transitivity of separable extensions 3.4

transitivity of trace and norm 7.3

transposition 1.2

trisecting the angle 6.8

trivial absolute value 7.9

trivial action 5.1, 5.2

twisted cubic 8.3

two-sided ideal 2.2

ultrametric inequality 7.9

underlying functor 10.3

unimodular matrix 7.4 unique factorization domain 2.6 unique factorization of ideals 7.7 unit 2.1 universal mapping property (UMP) 8.7, 10.2 upper central series 5.7

valuation 7.9 valuation ideal 7.9 valuation ring 7.9 Vandermonde determinant A6, 7.4 vector space as an F[X]-module 4.1 Von Dyck's theorem 5.8

weak Nullstellensatz 8.3 Wedderburn structure theorem 9.5 Wedderburn-Artin theorem 9.4

Zariski topology 8.1 Zassenhaus lemma 5.6 zero object 10.1