

# MA3560 (4-0) Applied Modern Algebra and Number Theory

## Objectives

### Catalog Description:

This course is devoted to aspects of modern algebra and number theory that directly support applications, principally to communication. The algebraic emphasis is on ring and field theory, with special emphasis on the theory of finite fields, and on those aspects of group theory that are important in the development of coding theory. Elements of number theory include congruences and factorization. Applications are drawn from topics of interest to DoN/DoD. These include error correcting codes and cryptography. This course is a prerequisite for MA4560 (Coding Theory), MA4565 (Advanced Modern Algebra), and MA4570 (Cryptography).

Following is an illustrative list of objectives for MA3560. It should be noted that the successful student will be able to synthesize solutions to problems not explicitly indicated in this list, and to prove theorems in the subjects covered. The major headings in this list are taken from the corresponding chapter titles in *Introduction to Abstract Algebra*, 6th edition, Neal H. McCoy and Gerald J. Janusz, Harcourt/Academic Press 2001, but the objectives themselves are text-independent.

### 1. Rings

Define and give examples of the following:

- (a) Ring
- (b) Subring
- (c) Commutative Ring
- (d) Commutative Ring with Identity
- (e) Ordered Ring
- (f) Additive and Multiplicative Inverses
- (g) Zero element
- (h) Integral Domain

Demonstrate familiarity with the elementary theorems on Rings.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.

### 2. Congruences

Define and give examples of the following:

- (a) Integers modulo  $n$
- (b) The Ring of Integers Modulo  $n$

- (c) Solution of Congruences
- (d) Ring Homomorphism and Isomorphism
- (e) Ideal (left, right, two-sided)
- (f) The Kernel of a Homomorphism
- (g) Principal Ideal, generator
- (h) Congruence modulo an ideal
- (i) Coset
- (j) Factor Ring
- (k) Canonical Map

Demonstrate familiarity with the principal theorems on congruences and on the Ring of Integers Modulo  $n$ , e.g., the Division Algorithm, and the Chinese Remainder Theorem.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.

### 3. Integral Domains and Fields

Define and give examples of the following:

- (a) Field
- (b) Field of Quotients
- (c) The Field of Rational Numbers
- (d) The Field of Real Numbers
- (e) Extension Field
- (f) The Archimedean Property
- (g) Ordered Field

Compare the properties of the fields of rational numbers, real numbers, and complex numbers.

Demonstrate familiarity with the principal theorems on fields covered to this point, e.g., the Archimedean Property.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.

### 4. Factorization

Define and/or give examples of the following:

- (a) Divisor of an integer
- (b) Prime Number
- (c) Relative Primes
- (d) The Division Algorithm
- (e) Greatest Common Divisor

- (f) Extended Euclidean Algorithm
- (g) The Integral Domains  $\mathbf{Z}_n$
- (h) Unit
- (i) Euler's Phi Function
- (j) Primality Testing

Demonstrate familiarity with the principal theorems on factorization, e.g., Euclid's Lemma, The Fundamental Theorem of Arithmetic, Euler's Theorem, Fermat's Little Theorem.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.

## 5. Polynomials

Define and give examples of the following:

- (a) Polynomial
- (b) The Polynomial Ring  $F[x]$
- (c) Polynomial Function
- (d) The Evaluation Homomorphism
- (e) Divisors in  $F[x]$
- (f) The Division Algorithm for Polynomials
- (g) Greatest Common Divisors in  $F[x]$
- (h) Monic Polynomial
- (i) Euclidean Algorithm for Polynomials
- (j) Relatively Prime Polynomials
- (k) Irreducible Polynomial
- (l) Prime Polynomial
- (m) Roots of Polynomials
- (n) Evaluation Maps
- (o) Factor Rings in  $F[x]$
- (p) Splitting Field, Field Extension
- (q) Finite Field
- (r) Factorization of Polynomials Over a Field

Demonstrate familiarity with the principal theorems on Polynomial Rings, e.g., Euclid's Lemma for Polynomials, the Factor Theorem, Gauss's Lemma, Eisenstein's Criterion.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.

## 6. Groups

Define and give examples of the following:

- (a) Group
- (b) Additive Group
- (c) Multiplicative Group
- (d) Abelian Group
- (e) Powers of an Element in a Group
- (f) Subgroup
- (g) Direct Product of Groups
- (h) The Symmetric Groups
- (i) The Dihedral Groups
- (j) Group Homomorphisms, Isomorphisms
- (k) The Kernel of a Group Homomorphism
- (l) Cyclic Groups, Generators
- (m) Subgroups of Cyclic Groups
- (n) Coset
- (o) Normal Subgroup
- (p) Factor Group

Demonstrate familiarity with the principal theorems on Groups, e.g., Cayley's Theorem, Lagrange's Theorem, the First Isomorphism Theorem.

Demonstrate mastery of the concepts by constructing proofs of relevant theorems.