Abstract Algebra Theorems and Definitions

Alexander J. Clarke

January 9, 2024

All theorems, corollaries, lemmas, remarks, and asides are direct quotes from Contemporary Abstract Algebra, 8th Edition, by Joseph A. Gallian

Contents

I Integers and Equivalence Relations **7**

0 Preliminaries **8**
0.1 Properties of Integers . . . 8
0.2 Modular Arithmetic . . . 9
0.3 Complex Numbers . . . 9
0.4 Mathematical Induction . . . 9
0.5 Equivalence Relations . . . 9
0.6 Functions (Mappings) . . . 10

II Groups **11**

2 Groups **12**
2.1 Definition and Examples of Groups . . . 12
2.2 Elementary Properties of Groups . . . 12

3 Finite Groups; Subgroups **13**
3.1 Terminology and Notation . . . 13
3.2 Subgroup Tests . . . 13

4 Cyclic Groups **15**
4.1 Properties of Cyclic Groups . . . 15
4.2 Classification of Subgroups of Cyclic Groups . . . 15

5 Permutation Groups **17**
5.1 Definition and Notation . . . 17
5.2 Cycle Notation . . . 17
5.3 Properties of Permutations . . . 18

6 Isomorphisms **20**
6.1 Definition and Examples . . . 20
6.2 Cayley's Theorem . . . 20
6.3 Properties of Isomorphisms . . . 20
6.4 Automorphisms . . . 21

7 Cosets and Lagrange's Theorem **22**
7.1 Properties of Cosets . . . 22
7.2 Lagrange's Theorem and Consequences . . . 23
7.3 An Application of Cosets to Permutation Groups . . . 23
7.4 The Rotation Group of a Cube and a Soccer Ball . . . 24

8 External Direct Products **25**
8.1 Definition and Examples . . . 25
8.2 Properties of External Direct Products . . . 25
8.3 The Group of Units Modulo **n** as an External Direct Product . . . 25

9 Normal Subgroups and Factor Groups **27**
9.1 Normal Subgroups . . . 27
9.2 Factor Groups . . . 27
9.3 Applications of Factor Groups . . . 27
9.4 Internal Direct Products . . . 27

10 Group Homomorphisms **29**
10.1 Definition and Examples . . . 29
10.2 Properties of Homomorphisms . . . 29
10.3 The First Isomorphism Theorem . . . 30

11 Fundamental Theorem of Finite Abelian Groups **31**
11.1 The Fundamental Theorem . . . 31
11.2 The Isomorphism Classes of Abelian Groups . . . 31
11.3 Proof of the Fundamental Theorem . . . 32

III Rings **33**

12 Introduction to Rings **34**
12.1 Motivation and Definition . . . 34
12.2 Properties of Rings . . . 34
12.3 Subrings . . . 35

13 Integral Domains **36**
13.1 Definition and Examples . . . 36
13.2 Fields . . . 36
13.3 Characteristic of a Ring . . . 36

14 Ideals and Factor Rings **38**
14.1 Ideals . . . 38
14.2 Factor Rings . . . 38
14.3 Prime Ideals and Maximal Ideals . . . 38

15 Ring Homomorphisms 40
15.1 Definition and Examples . . . 40
15.2 Properties of Ring Homomorphisms . . . 40
15.3 The Field of Quotients . . . 41

16 Polynomial Rings 42
16.1 Notation and Terminology . . . 42
16.2 The Division Algorithm and Consequences . . . 43

17 Factorization of Polynomials 44
17.1 Reducibility Tests . . . 44
17.2 Irreducibility Tests . . . 44
17.3 Unique Factorization In $\mathbb{Z}[\mathbf{x}]$ . . . 45

18 Divisibility in Integral Domains 46
18.1 Irreducibles, Primes . . . 46
18.2 Unique Factorization Domains . . . 46
18.3 Euclidean Domains . . . 47

IV Fields 48

19 Vector Spaces 49
19.1 Definition and Examples . . . 49
19.2 Subspaces . . . 49
19.3 Linear Independence . . . 49

20 Extension Fields 51
20.1 The Fundamental Theorem of Field Theory . . . 51
20.2 Splitting Fields . . . 51
20.3 Zeros of an Irreducible Polynomial . . . 52

21 Algebraic Extensions 54
21.1 Characterization of Extensions . . . 54
21.2 Finite Extensions . . . 54
21.3 Properties of Algebraic Extensions . . . 55

22 Finite Fields 56
22.1 Classification of Finite Fields . . . 56
22.2 Structure of Finite Fields . . . 56
22.3 Subfields of a Finite Field . . . 56

23 Geometric Constructions 57

V Special Topics 58

24 Sylow Theorems **59**
24.1 Conjugacy Classes . . . 59
24.2 The Class Equation . . . 59
24.3 The Sylow Theorems . . . 59
24.4 Applications of Sylow Theorems . . . 60

25 Finite Simple Groups **61**
25.1 Historical Background . . . 61
25.2 Nonsimplicity Tests . . . 61

26 Generators and Relations **62**
26.1 Motivation . . . 62
26.2 Definitions and Notation . . . 62
26.3 Free Group . . . 63
26.4 Generators and Relations . . . 63
26.5 Classification of Groups of Order Up to 15 . . . 63
26.6 Characterization of Dihedral Groups . . . 63

27 Symmetry Groups **64**
27.1 Isometries . . . 64
27.2 Classification of Finite Plane Symmetry Groups . . . 64
27.3 Classification of Finite Groups of Rotations in $\mathbb{R}^3$ . . . 64

28 Frieze Groups and Crystallographic Groups **65**
28.1 The Frieze Groups . . . 65
28.2 The Crystallographic Groups . . . 65
28.3 Identification of Plane Periodic Patterns . . . 65

29 Symmetry and Counting **67**
29.1 Motivation . . . 67
29.2 Burnside's Theorem . . . 67
29.3 Group Action . . . 67

30 Cayley Digraphs of Groups **69**
30.1 The Cayley Digraph of a Group . . . 69
30.2 Hamiltonian Circuits and Paths . . . 69

31 Introduction to Algebraic Coding Theory **70**
31.1 Linear Codes . . . 70
31.2 Parity-Check Matrix Decoding . . . 70
31.3 Coset Decoding . . . 71

32 An Introduction to Galois Theory **72**
32.1 Fundamental Theorem of Galois Theory 72
32.2 Solvability of Polynomials by Radicals 72

33 Cyclotomic Extensions **74**
33.1 Cyclotomic Polynomials 74
33.2 The Constructible Regular **n**-gons 75

Part I

Integers and Equivalence Relations

Chapter 0

Preliminaries

0.1 Properties of Integers

Well Ordering Principle
Every nonempty set of positive integers contains a smallest number.

Theorem 0.1.1 ***Division Algorithm***
Let a and b be integers with $b > 0$. then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

Definition 0.1.1 ***Greatest Common Divisor, Relatively Prime Integers***
The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $\gcd(a, b)$. When $\gcd(a, b) = 1$, we say that a and b are *relatively prime.*

Theorem 0.1.2 ***GCD Is a Linear Combination***
for any nonzero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Corollary 0.1.1
If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

Lemma 0.1.3 ***Euclid's Lemma*** $p \mid ab$ implies $p \mid a$ or $p \mid b$
If p is a prime that divides ab, then p divides a or p divides b.

Theorem 0.1.4 ***Fundamental Theorem of Arithmetic***
Every integer greater than 1 is a prime or a product of primes. this product is unique, except for the order in which the factors appear. That is, if $n = p_1p_2 \dots p_r$ and $n = q_1q_2 \dots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.

Definition 0.1.2 ***Least Common Multiple***
The *least common multiple* of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b. We will denote this integer by $\operatorname{lcm}(a, b)$.

0.2 Modular Arithmetic

0.3 Complex Numbers

Theorem 0.3.1 ***Properties of Complex Numbers***

1. Closure under addition: $(a+bi)+(c+di)=(a+c)+(b+d)i$
2. Closure under multiplication: $(a+bi)(c+di)=(ac)+(ad)i+(bc)i+(bd)i^2=(ac-bd)+(ad+bc)i$
3. Closure under division ($c+di \neq 0$): $\dfrac{(a+bi)}{(c+di)}=\dfrac{(a+bi)}{(c+di)}\dfrac{(c-di)}{(c-di)}=\dfrac{(ac+bd)+(bc-ad)i}{c^2+d^2}=\dfrac{(ac+bd)}{c^2+d^2}+\dfrac{(bc-ad)}{c^2+d^2}i$
4. Complex conjugation: $(a+bi)(a-bi)=a^2+b^2$
5. Inverses: For every nonzero complex number $a+bi$ there is a complex number $c+di$ such that $(a+bi)(c+di)=1$. (That is, $(a+bi)^{-1}$ exists in $\mathbb{C}$.)
6. Powers: For every complex number $a+bi=r(\cos\theta+i\sin\theta)$ and every positive integer n, we have $(a+bi)^n=[r(\cos\theta+i\sin\theta)]^n=r^n(\cos n\theta+i\sin n\theta)$.
7. Radicals: For every complex number $a+bi=r(\cos\theta+i\sin\theta)$ and every positive integer n, we have $(a+bi)^{\frac{1}{n}}=[r(\cos\theta+i\sin\theta)]^{\frac{1}{n}}=r^{\frac{1}{n}}(\cos\frac{\theta}{n}+i\sin\frac{\theta}{n})$.

0.4 Mathematical Induction

Theorem 0.4.1 ***First Principle of Mathematical Induction***
Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n+1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Theorem 0.4.2 ***Second Principle of Mathematical Induction***
Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

0.5 Equivalence Relations

Definition 0.5.1 ***Equivalence Relation***
An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that

1. $(a,a) \in R$ for all $a \in S$ (reflexive property).

2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).

3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).

Definition 0.5.2 ***Partition***
A *partition* of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Theorem 0.5.1 ***Equivalence Classes Partition***
The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

0.6 Functions (Mappings)

Definition 0.6.1 ***Function (Mapping)***
A *function* (or *mapping*) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain of* ϕ, and B is called the *range of* ϕ. If ϕ assigns b to a, then b is called the *image of* a *under* ϕ. The subset of B comprising all the images of elements of A is called the *image of* A *under* ϕ.

Definition 0.6.2 ***Composition of Functions***
Let $\phi : A \to B$ and $\psi : B \to C$. The *composition* $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A.

Definition 0.6.3 ***One-to-One Function***
A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

Definition 0.6.4 ***Functions from A onto B***
A function ϕ from a set A to a set B is said to be *onto* B if each element of B is the image of at least one element of A. In symbols, $\phi : A \to B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.

Theorem 0.6.1 ***Properties of Functions***
Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).

2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.

3. If α and β are onto, then $\beta\alpha$ is onto.

4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.

Part II

Groups

Chapter 2

Groups

2.1 Definition and Examples of Groups

Definition 2.1.1 ***Binary Operation***
Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.

Definition 2.1.2 ***Group***
Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.

1. *Associativity.* The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.
2. *Identity.* There is an element e (called the *identity*) in G such that $ae = ea = a$ for all a in G.
3. *Inverses.* For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.

2.2 Elementary Properties of Groups

Theorem 2.2.1 ***Uniqueness of the Identity***
In a group G, there is only one identity element.

Theorem 2.2.2 ***Cancellation***
In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Theorem 2.2.3 ***Uniqueness of Inverses***
For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Theorem 2.2.4 ***Socks-Shoes Property***
For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

Chapter 3

Finite Groups; Subgroups

3.1 Terminology and Notation

Definition 3.1.1 ***Order of a Group***
The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

Definition 3.1.2 ***Order of an Element***
The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

Definition 3.1.3 ***Subgroup***
If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

3.2 Subgroup Tests

Theorem 3.2.1 ***One-Step Subgroup Test***
Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H is a subgroup of G.)

Theorem 3.2.2 ***Two-Step Subgroup Test***
Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

Theorem 3.2.3 ***Finite Subgroup Test***
Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Theorem 3.2.4 **$\langle$a$\rangle$)** ***Is a Subgroup***
Let G be a group, and let a be any element of G. Then, $\langle a \rangle)$ is a subgroup of G.

Definition 3.2.1 ***Center of a Group***
The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G \mid ax = xa, \ \forall \ x \in G\}$$

[The notation $Z(G)$ comes from the fact that the German word for center is *Zentrum.* The term was coined by J.A. de Séguier in 1904.]

Theorem 3.2.5 ***Center Is a Subgroup***
The center of a group G is a subgroup of G.

Definition 3.2.2 ***Centralizer of* a *in* G**
Let a be a fixed element of a group G. The *centralizer of* a *in* G, $C(a)$, is the set of all elements in G that commute with a. In symbols,

$$C(a) = \{g \in G \mid ga = ag\}$$

Theorem 3.2.6 C(a) ***Is a Subgroup***
For each a in a group G, the centralizer of a is a subgroup of G.

Chapter 4

Cyclic Groups

4.1 Properties of Cyclic Groups

Theorem 4.1.1 ***Criterion for*** $\mathbf{a^i = a^j}$
Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say, n, then $\langle a \rangle) = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Corollary 4.1.1 $|\mathbf{a}| = |\langle \mathbf{a} \rangle)|$
For any group element a, $|a| = |\langle a \rangle)|$.

Corollary 4.1.2 $\mathbf{a^k = e}$ ***Implies That*** $|\mathbf{a}|$ ***Divides*** $\mathbf{k}$
Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

Theorem 4.1.2 $\langle \mathbf{a^k} \rangle) = \langle \mathbf{a}^{gcd(\mathbf{n},\mathbf{k})} \rangle)$ ***and*** $\left|\mathbf{a^k}\right| = \mathbf{n}/gcd(\mathbf{n},\mathbf{k})$
Let a be an element of order n in a gruop and let k be a positive integer. Then $\langle a^k \rangle) = \langle a^{\gcd(n,k)} \rangle)$ and $\left|a^k\right| = n/\gcd(n,k)$.

Corollary 4.1.3 ***Orders of Elements in Finite Cyclic Groups***
In a finite cyclic group, the order of an element divides the order of the group.

Corollary 4.1.4 ***Criterion for*** $\langle \mathbf{a^i} \rangle) = \langle \mathbf{a^j} \rangle)$ ***and*** $\left|\mathbf{a^i}\right| = \left|\mathbf{a^j}\right|$
Let $|a| = n$. Then $\langle a^i \rangle) = \langle a^j \rangle)$ if and only if $\gcd(n,i) = \gcd(n,j)$, and $|a^i| = |a^j|$ if and only if $\gcd(n,i) = \gcd(n,j)$.

Corollary 4.1.5 ***Generators of Finite Cyclic Groups***
Let $|a| = n$. Then $\langle a \rangle) = \langle a^j \rangle)$ if and only if $\gcd(n,j) = 1$, and $|a| = |\langle a^j \rangle)|$ if and only if $\gcd(n,j) = 1$.

Corollary 4.1.6 ***Generators of*** $\mathbb{Z}_\mathbf{n}$
An integer k in $\mathbb{Z}_n$ is a generator of Z_n if and only if $\gcd(n,k) = 1$.

4.2 Classification of Subgroups of Cyclic Groups

Theorem 4.2.1 ***Fundamental Theorem of Cyclic Groups***
Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle)| = n$, then the order of any

subgroup of $\langle a \rangle)$ is a divisor of n; and, for each, positive divisor k of n, the group $\langle a \rangle)$ has exactly one subgroup of order k – namely, $\langle a^{n/k} \rangle)$.

Corollary 4.2.1 ***Subgroups of*** $\mathbb{Z}_\mathbf{n}$
For each positive divisor k of n, the set $\langle n/k \rangle)$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Theorem 4.2.2 ***Number of Elements of Each Order in a Cyclic Group***
If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Corollary 4.2.2 ***Number of Elements of Order*** **d** ***in a Finite Group***
In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Chapter 5

Permutation Groups

5.1 Definition and Notation

Definition 5.1.1 ***Permutation of* A*, Permutation Group of* A**
A *permutation* of a set A is a function from A to A that is both one-to-one and onto. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

5.2 Cycle Notation

Definition 5.2.1
Consider the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$

The assignment of values is as follows:

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 4 \\ 4 &\mapsto 6 \\ 5 &\mapsto 5 \\ 6 &\mapsto 3 \end{aligned}$$

Although mathematically satisfactory, such diagrams are cumbersome. Instead, we leave out the arrows and simply write $\alpha = (1,2)(3,4,6)(5)$.

It is also worth noting that an expression of the form $(a_1, a_2, \ldots, a_m)$ is called a *cycle of length* m, or an m*-cycle*.

Example
To multiply cycles, consider the following permutations from S_8. Let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. (When the domain consists of single-digit integers, it is common practice

to omit the commas between the digits.) What is the cycle form of $\alpha\beta$? Of course, one could say that $\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$, but it is usually more desirable to express a permutation in a *disjoint* cycle form (that is, the various cycles have no number in common). Well, keeping in mind that function composition is done from right to left and that each cycle that does not contain a symbol fixes the symbol, we observe that (5) fixes 1; (648) fixes 1; (1237) sends 1 to 2, (8) fixes 2; (456) fixes 2; (27) sends 2 to 7; and (13) fixes 7. So the net effect of $\alpha\beta$ is to send 1 to 7. Thus, we begin $\alpha\beta = (17\dots)\dots$. Now, repeating the entire process beginning with 7, we have, cycle by cycle, right to left,

$$7 \to 7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3,$$

so that $\alpha\beta = (173\dots)\dots$. Ultimately, we have $\alpha\beta = (1732)(48)(56)$. The import thing to bear in mind when multiplying cycles is to "keep moving" from one cycle to the next from right to left.

5.3 Properties of Permutations

Theorem 5.3.1 ***Products of Disjoint Cycles***
Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 5.3.2 ***Disjoint Cycles Commute***
If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.3.3 ***Order of a Permutation (Ruffini, 1799)***
The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Theorem 5.3.4 ***Product of 2-Cycles***
Every permutation in $S_n,\ n > 1$ is a product of 2-cycles.

Lemma
If $\varepsilon = \beta_1\beta_2\dots\beta_r$, where the β's are 2-cycles, then r is even.

Theorem 5.3.5 ***Always Even or Always Odd***
If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

$$\alpha = \beta_1\beta_2\dots\beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2\dots\gamma_s,$$

where the β's and the γ's are 2-cycles, then r and s are both even or both odd.

Definition 5.3.1 ***Even and Odd Permutations***
A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

Theorem 5.3.6 ***Even Permutations Form a Group***
The set of even permutations in S_n forms a subgroup of S_n.

Definition 5.3.2 ***Alternating Group of Degree* n**
The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree* n.

Theorem 5.3.7
For $n > 1$, A_n has order $n!/2$.

Chapter 6

Isomorphisms

6.1 Definition and Examples

Definition 6.1.1 ***Group Isomorphism***
An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b),\ \forall a, b \in G$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.

6.2 Cayley's Theorem

Theorem 6.2.1 ***Cayley's Theorem (1854)***
Every group is isomorphic to a group of permutations.

6.3 Properties of Isomorphisms

Theorem 6.3.1 ***Properties of Isomorphisms Acting on Elements***
Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$.
3. For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G = \langle a \rangle)$ if and only if $\overline{G} = \langle \phi(a) \rangle)$.
5. $|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).
6. For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.

7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Theorem 6.3.2 ***Properties of Isomorphisms Acting on Groups***
Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ^{-1} is an isomorphisms from $\overline{G}$ onto G.

2. G is Abelian if and only if $\overline{G}$ is Abelian.

3. G is cyclic if and only if $\overline{G}$ is cyclic.

4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

5. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\}$ is a subgroup of G.

6. $\phi(Z(G)) = Z(\overline{G})$.

6.4 Automorphisms

Definition 6.4.1 ***Automorphism***
An isomorphism from a group G onto itself is called an *automorphisms* of G.

Definition 6.4.2 ***Inner Automorphism Induced by*** **a**
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the *inner automorphism of G induced by a*.

Theorem 6.4.1 ***Aut(G) and Inn(G) Are Groups***
The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

When G is a group, we use $\mathrm{Aut}(G)$ to denote the set of all automorphisms of G and $\mathrm{Inn}(G)$ to denote the set of all inner automorphisms of G.

Theorem 6.4.2 ***Aut***$(\mathbb{Z}_\mathbf{n}) \approx \mathbf{U}(\mathbf{n})$
For every positive integer n, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.

Chapter 7

Cosets and Lagrange's Theorem

7.1 Properties of Cosets

Definition 7.1.1 ***Coset of* H *in* G**
Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a subgroup of G, the set aH is called the *left coset of H in G containing a*, whereas Ha is called the *right coset of H in G containing a*. In this case, the element a is called the *coset representative of aH (or Ha)*. We use $|aH|$ to denote the number of elements in the set aH, and $|Ha|$ to denote the number of elements in Ha.

Lemma ***Properties of Cosets***
Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$.

2. $aH = H$ if and only if $a \in H$.

3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.

4. $aH = bH$ if and only if $a \in bH$.

5. $aH = bH$ or $aH \cap bH = \emptyset$.

6. $aH = bH$ if and only if $a^{-1}b \in H$.

7. $|aH| = |bH|$.

8. $aH = Ha$ if and only if $H = aHa^{-1}$.

9. aH is a subgroup of G if and only if $a \in H$.

7.2 Lagrange's Theorem and Consequences

Theorem 7.2.1 ***Lagrange's Theorem:*** **$|\mathbf{H}|$ *Divides* $|\mathbf{G}|$**
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G| \,/\, |H|$.

Remark
A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group. The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G : H|$.

Corollary 7.2.1 $|\mathbf{G} : \mathbf{H}| = |\mathbf{G}| \,/\, |\mathbf{H}|$
If G is a finite group and H is a subgroup of G, then $|G : H| = |G| \,/\, |H|$.

Corollary 7.2.2 $|\mathbf{a}|$ *Divides* $|\mathbf{G}|$
In a finite group, the order of each element of the group divides the order of the group.

Corollary 7.2.3 ***Groups of Prime Order Are Cyclic***
A group of prime order is cyclic.

Corollary 7.2.4 $\mathbf{a}^{|\mathbf{G}|} = \mathbf{e}$
Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

Corollary 7.2.5 ***Fermat's Little Theorem***
For every integer a and every prime p, $a^p \mod p = a \mod p$.

Theorem 7.2.2 $|\mathbf{HK}| = |\mathbf{H}| \, |\mathbf{K}| \,/\, |\mathbf{H} \cap \mathbf{K}|$
For two finite subgroups H and K of a group, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = |H| \, |K| \,/\, |H \cap K|$.

Theorem 7.2.3 ***Classification of Groups of order 2*p**
Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.

7.3 An Application of Cosets to Permutation Groups

Definition 7.3.1 ***Stabilizer of a Point***
Let G be a group of permutations of a set S. For each i in S, let $\mathrm{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. We call $\mathrm{stab}_G(i)$ the *stabilizer of i in G*.

Definition 7.3.2 ***Orbit of a Point***
Let G be a group of permutations of a set S. For each s in S, let $\mathrm{orb}_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $\mathrm{orb}_G(s)$ is a subset of S called the *orbit of s under G*. We use $|\mathrm{orb}_G(s)|$ to denote the number of elements in $\mathrm{orb}_G(s)$.

Theorem 7.3.1 ***Orbit-Stabilizer Theorem***
Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |\mathrm{orb}_G(i)| \, |\mathrm{stab}_G(i)|$.

7.4 The Rotation Group of a Cube and a Soccer Ball

Theorem 7.4.1 ***The Rotation Group of a Cube***
The group of rotations of a cube is isomorphic to S_4.

Chapter 8

External Direct Products

8.1 Definition and Examples

Definition 8.1.1 ***External Direct Product***
Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

8.2 Properties of External Direct Products

Theorem 8.2.1 ***Order of an Element in a Direct Product***
The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the component of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = \mathrm{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$$

Theorem 8.2.2 ***Criterion for* $\mathbf{G \oplus H}$ *to be Cyclic***
Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

Corollary 8.2.1 ***Criterion for* $\mathbf{G_1 \oplus G_2 \oplus \cdots \oplus G_n}$ *to Be Cyclic***
An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Corollary 8.2.2 ***Criterion for* $\mathbb{Z}_{\mathbf{n_1 n_2 \ldots n_k}} \approx \mathbb{Z}_{\mathbf{n_1}} \oplus \mathbb{Z}_{\mathbf{n_2}} \oplus \cdots \oplus \mathbb{Z}_{\mathbf{n_k}}$**
Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

8.3 The Group of Units Modulo n as an External Direct Product

Remark
The U-groups provide a convenient way to illustrate the preceding ideas. We first introduce

some notation. If k is a divisor of n, let

$$U_k(n) = \{x \in U(n) \mid x \mod k = 1\}$$

Theorem 8.3.1 U(n) ***as an External Direct Product***
Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,

$$U(st) \approx U(s) \oplus U(t)$$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

Corollary 8.3.1
Let $m = n_1 n_2 \ldots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$$

Chapter 9

Normal Subgroups and Factor Groups

9.1 Normal Subgroups

Definition 9.1.1 ***Normal Subgroup***
A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \triangleleft G$.

Theorem 9.1.1 ***Normal Subgroup Test***
A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all x in G.

9.2 Factor Groups

Theorem 9.2.1 ***Factor Groups (O. Hölder, 1889)***
Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.

9.3 Applications of Factor Groups

Theorem 9.3.1 G/Z ***Theorem***
Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

Theorem 9.3.2 $\mathbf{G/Z(G) \approx}$ *Inn*(G)
For any group G, $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

Theorem 9.3.3 ***Cauchy's Theorem for Abelian Groups***
Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

9.4 Internal Direct Products

Definition 9.4.1 ***Internal Direct Product of* H *and* K**
We say that G is the *internal direct product* of H and K and write $G = H \times K$ if H and K are

normal subgroups of G and

$$G = HK \quad \text{and} \quad H \cap K = \{e\}$$

Definition 9.4.2 ***Internal Direct Product*** $\mathbf{H_1 \times H_2 \times \cdots \times H_n}$
Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the *internal direct product* of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if

1. $G = H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n \mid h_i \in H_i\}$,

2. $(H_1 H_2 \ldots H_n) \cap H_{i+1} = e$ for $i = 1, 2, \ldots, n-1$.

Theorem 9.4.1 $\mathbf{H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n}$
If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2 \ldots, H_n$.

Theorem 9.4.2 ***Classification of Groups of Order*** $\mathbf{p^2}$
Every group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Corollary 9.4.1
If G is a group of order p^2, where p is a prime, then G is Abelian.

Chapter 10

Group Homomorphisms

10.1 Definition and Examples

Definition 10.1.1 ***Group Homomorphism***
A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Definition 10.1.2 ***Kernel of a Homomorphism***
The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by $\ker \phi$.

10.2 Properties of Homomorphisms

Theorem 10.2.1 ***Properties of Elements Under Homomorphisms***
Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then

1. ϕ carries the identity of G to $\overline{G}$.

2. $\phi(g^n) = (\phi(g))^n$ for all n in $\mathbb{Z}$.

3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.

4. $\ker \phi$ is a subgroup of G.

5. $\phi(a) = \phi(b)$ if and only if $a \ker \phi = b \ker \phi$.

6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \ker \phi$.

Theorem 10.2.2 ***Properties of Subgroups Under Homomorphisms***
Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.

2. If H is cyclic, then $\phi(H)$ is cyclic.

3. If H is Abelian, then $\phi(H)$ is Abelian.

4. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.

5. If $|\ker\phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.

6. If $|H| = n$, then $|\phi(H)|$ divides n.

7. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.

8. If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.

9. If ϕ is onto and $\ker\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

Corollary 10.2.1 ***Kernels Are Normal***
Let ϕ be a group homomorphism from G to $\overline{G}$. Then $\ker\phi$ is a normal subgroup of G.

10.3 The First Isomorphism Theorem

Theorem 10.3.1 ***First Isomorphism Theorem (Jordan, 1870)***
Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\ker\phi$ to $\phi(G)$, given by $g\ker\phi \to \phi(g)$, is an isomorphism. In symbols, $G/\ker\phi \approx \phi(G)$.

Corollary 10.3.1
If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $\left|\overline{G}\right|$.

Theorem 10.3.2 ***Normal Subgroups Are Kernels***
Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

Chapter 11

Fundamental Theorem of Finite Abelian Groups

11.1 The Fundamental Theorem

Theorem 11.1.1 ***Fundamental Theorem of Finite Abelian Groups***
Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

11.2 The Isomorphism Classes of Abelian Groups

Remark ***Greedy Algorithm for an Abelian Group of Order*** $\mathbf{p^n}$
The Fundamental Theorem is extremely powerful. As an application, we can use it as an algorithm for constructing all Abelian groups of any order. Let's look at Abelian groups of a certain order n, where n has two or more distinct prime divisors.

1. Compute the orders of the elements of the group G

2. Select an element a_1 of maximum order and define $G_1 = \langle a_1 \rangle)$. Set $i = 1$.

3. If $|G| = |G_i|$, stop. Otherwise, replace i by $i + 1$.

4. Select an element a_i of maximum order p^k such that $p^k \leq |G| \,/\, |G_{i-1}|$ and none of $a_i, a_i^p, a_i^{p^2}, \ldots, a_i^{p^{k-1}}$ is in G_{i-1}, and define $G_i = G_{i-1} \times \langle a_i \rangle)$.

5. Return to step 3.

Corollary 11.2.1 ***Existence of Subgroups of Abelian Groups***
If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

11.3 Proof of the Fundamental Theorem

Lemma 11.3.1
Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

Lemma 11.3.2
Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a\rangle) \times K$.

Lemma 11.3.3
A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

Lemma 11.3.4
Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H's and K's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

Part III

Rings

Chapter 12

Introduction to Rings

12.1 Motivation and Definition

Definition 12.1.1 ***Ring***
A *ring* R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all a, b, c in R:

1. $a+b=b+a$.
2. $(a+b)+c=a+(b+c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0=a$ for all a in R.
4. There is an element $-a$ in R such that $a+(-a)=0$.
5. $a(bc)=(ab)c$.
6. $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

Remark
Note that multiplication need not be commutative. When it is, we say that the ring is *commutative*. Also, a ring need not have an identity under multiplication. A *unity* (or *identity*) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a unit of the ring. Thus, a is a unit if a^{-1} exists.
The following terminology and notation are convenient. If a and b belong to a commutative ring R and a is nonzero, we say that a *divides* b (or that a is a *factor* of b) and write $a|b$, if there exists an element c in R such that $b=ac$. If a does not divide b, we write $a \nmid b$.

12.2 Properties of Rings

Theorem 12.2.1 ***Rules of Multiplication***
Let a, b, and c belong to a ring R. Then

1. $a0 = 0a = 0$.

2. $a(-b) = (-a)b = -(ab)$.

3. $(-a)(-b) = ab$.

4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore, if R has a unity element 1, then

5. $(-1)a = -a$.

6. $(-1)(-1) = 1$.

Theorem 12.2.2 ***Uniqueness of the Unity and Inverses***
If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

12.3 Subrings

Definition 12.3.1 ***Subring***
A subset S of a ring R is a *subring of* R if S is itself a ring with the operations of R.

Theorem 12.3.1 ***Subring Test***
A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication – that is, if $a - b$ and ab are in S whenever a and b are in S.

Chapter 13

Integral Domains

13.1 Definition and Examples

Definition 13.1.1 ***Zero Divisors***
A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition 13.1.2 ***Integral Domain***
An *integral domain* is a commutative ring with unity and no zero-divisors.

Theorem 13.1.1 ***Cancellation***
Let a, b, and c belong to an integral domain If $a \neq 0$ and $ab = ac$, then $b = c$.

13.2 Fields

Definition 13.2.1 ***Field***
A *field* is a commutative ring with unity in which every nonzero element is a unit.

Theorem 13.2.1 ***Finite Integral Domains are Fields***
A finite integral domain is a field.

Corollary 13.2.1 $\mathbb{Z}_\mathbf{p}$ ***Is a Field***
For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p is a field.

13.3 Characteristic of a Ring

Definition 13.3.1 ***Characteristic of a Ring***
The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

Theorem 13.3.1 ***Characteristic of a Ring with Unity***
Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Theorem 13.3.2 ***Characteristic of an Integral Domain***
The characteristic of an integral domain is 0 or prime.

Chapter 14

Ideals and Factor Rings

14.1 Ideals

Definition 14.1.1 ***Ideal***
A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

Theorem 14.1.1 ***Ideal Test***
A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$.

2. ra and ar are in A whenever $a \in A$ and $r \in R$.

14.2 Factor Rings

Theorem 14.2.1 ***Existence of Factor Rings***
Let R be a ring and let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

14.3 Prime Ideals and Maximal Ideals

Remark
A *proper* ideal is an ideal I of some ring R such that it is a proper subset of R; that is, $I \subset R$.

Definition 14.3.1 ***Prime Ideal, Maximal Ideal***
A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring R is a *proper* ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Theorem 14.3.1 R/A ***Is an Integral Domain If and Only If*** **A** ***Is Prime***
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Theorem 14.3.2 R/A *Is a Field If and Only If* A *Is Maximal*
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Chapter 15

Ring Homomorphisms

15.1 Definition and Examples

Definition 15.1.1 ***Ring Homomorphism, Ring Isomorphism***
A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b)$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

15.2 Properties of Ring Homomorphisms

Theorem 15.2.1 ***Properties of Ring Homomorphisms***
Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1. For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.
3. If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.
5. If R is commutative, then $\phi(R)$ is commutative.
6. If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.
7. ϕ is an isomorphism if and only if ϕ is onto and $\ker \phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.

Theorem 15.2.2 ***Kernels Are Ideals***
Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\ker \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.2.3 ***First Isomorphism Theorem for Rings***
Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker\phi$ to $\phi(R)$, given by $r + \ker\phi \to \phi(r)$, is an isomorphism. In symbols, $R/\ker\phi \approx \phi(R)$. This theorem is often referred to as the *Fundamental Theorem of Ring Homomorphisms*.

Theorem 15.2.4 ***Ideals Are Kernels***
Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an idea lA is the kernel of the mapping $r \to r + A$ from R to R/A. This mapping is known as the *natural homomorphism* from R to R/A.

Theorem 15.2.5 ***Homomorphism from $\mathbb{Z}$ to a Ring with Unity***
Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n{\cdot}1$ is a ring homomorphism.

Corollary 15.2.1 ***A Ring with Unity Contains $\mathbb{Z}_\mathbf{n}$ or $\mathbb{Z}$***
If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 15.2.2 ***$\mathbb{Z}_\mathbf{m}$ Is a Homomorphic Image of $\mathbb{Z}$***
For any positive integer m, the mapping of $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \mod m$ is a ring homomorphism.

Corollary 15.2.3 ***A Field Contains $\mathbb{Z}_\mathbf{p}$ or $\mathbb{Q}$ (Steinitz, 1910)***
If $\mathbb{F}$ is a field of characteristic p, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a subfield isomorphic to the rational numbers.

15.3 The Field of Quotients

Theorem 15.3.1 ***Field of Quotients***
Let D be an integral domain. Then there exists a field $\mathbb{F}$ (called the field of quotients in D) that contains a subring isomorphic to D.

Chapter 16

Polynomial Rings

16.1 Notation and Terminology

Definition 16.1.1 ***Ring of Polynomials over*** **R**
Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{Z}^+\}$$

is called the *ring of polynomials over R in the indeterminate x.*
Two elements

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers i. (Define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$.)

Definition 16.1.2 ***Addition and Multiplication in*** **R[x]**
Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0$$

where s is the maximum of m and n, $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, \ldots, m + n$.

Theorem 16.1.1 D ***an Integral Domain Implies*** **D[x]** ***an Integral Domain***
If D is an integral domain, then $D[x]$ is an integral domain.

16.2 The Division Algorithm and Consequences

Theorem 16.2.1 ***Division Algorithm for*** $\mathbb{F}[\mathbf{x}]$
Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = g(x)q(x)+r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Corollary 16.2.1 ***Remainder Theorem***
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 16.2.2 ***Factor Theorem***
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Corollary 16.2.3 ***Polynomials of Degree*** **n** ***Have at Most*** **n** ***Zeros***
A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Definition 16.2.1 ***Principal Ideal Domain (PID)***
A *principal ideal domain* is an integral domain R in which every ideal has the form $\langle a \rangle) = \{ra \mid r \in R\}$ for some a in R.

Theorem 16.2.2 $\mathbb{F}[\mathbf{x}]$ ***Is a PID***
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principal ideal domain.

Theorem 16.2.3 ***Criterion for*** $\mathbf{I} = \langle \mathbf{g(x)} \rangle)$
Let $\mathbb{F}$ be a field, I a nonzero ideal in $\mathbb{F}[x]$, and $g(x)$ an element of $\mathbb{F}[x]$. Then, $I = \langle g(x) \rangle)$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

Chapter 17

Factorization of Polynomials

17.1 Reducibility Tests

Definition 17.1.1 ***Irreducible Polynomial, Reducible Polynomial***
Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over* D, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible over* D.

Theorem 17.1.1 ***Reducibility Test for Degrees 2 and 3***
Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

Definition 17.1.2 ***Content of a Polynomial, Primitive Polynomial***
The *content* of a nonzero polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the a'a are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_0$. A *primitive polynomial* is an element of $\mathbb{Z}[x]$ with content 1.

Lemma 17.1.2 ***Gauss's Lemma***
The product of two primitive polynomials is primitive.

Theorem 17.1.3 ***Reducibility over*** $\mathbb{Q}$ ***Implies Reducibility over*** $\mathbb{Z}$
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

17.2 Irreducibility Tests

Theorem 17.2.1 ***Mod* p *Irreducibility Test***
Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \overline{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 17.2.2 ***Eisenstein's Criterion (1850)***
Let
$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

If there is a prime p such that $p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary 17.2.1 ***Irreducibility of*** **p*th Cyclotomic Polynomial***
For any prime p, the pth cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Theorem 17.2.3 $\langle \mathbf{p}(\mathbf{x}) \rangle$ ***Is Maximal If and Only If*** $\mathbf{p}(\mathbf{x})$ ***Is Irreducible***
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over $\mathbb{F}$.

Corollary 17.2.2 $\mathbb{F}[\mathbf{x}]/\langle \mathbf{p}(\mathbf{x}) \rangle$ ***Is a Field***
Let $\mathbb{F}$ be a field and $p(x)$ be an irreducible polynomial over $\mathbb{F}$. Then $\mathbb{F}[x]/\langle p(x) \rangle$ is a field.

Corollary 17.2.3 $\mathbf{p}(\mathbf{x}) \mid \mathbf{a}(\mathbf{x})\mathbf{b}(\mathbf{x})$ ***Implies*** $\mathbf{p}(\mathbf{x}) \mid \mathbf{a}(\mathbf{x})$ ***or*** $\mathbf{p}(\mathbf{x}) \mid \mathbf{b}(\mathbf{x})$
Let $\mathbb{F}$ be a field and let $p(x), a(x), b(x) \in \mathbb{F}[x]$. If $p(x)$ is irreducible over $\mathbb{F}$ and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

17.3 Unique Factorization In $\mathbb{Z}[\mathbf{x}]$

Theorem 17.3.1 ***Unique Factorization in*** $\mathbb{Z}[\mathbf{x}]$
Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x)$, where the b_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x) = c_1 c_2 \ldots c_t q_1(x) q_2(x) \ldots q_n(x)$$

where the b_i's and the c_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t, m = n$, and, after renumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$, for $i = 1, \ldots, s$, and $p_i(x) = \pm q_i(x)$, for $i = 1, \ldots, m$.

Chapter 18

Divisibility in Integral Domains

18.1 Irreducibles, Primes

Definition 18.1.1 ***Associates, Irreducibles, Primes***
Elements a and b of an integral domain D are called *associates* if $a = ub$, where u is a unit of D. A nonzero element a of an integral domain D is called an *irreducible* if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit. A nonzero element a of an integral domain D is called a *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Theorem 18.1.1 ***Prime Implies Irreducible***
In an integral domain, every prime in an irreducible.

Theorem 18.1.2 ***PID Implies Irreducible Equals Prime***
In a principal ideal domain, an element is an irreducible if and only if it is a prime.

18.2 Unique Factorization Domains

Definition 18.2.1
An integral domain D is a *unique factorization domain* if

1. every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and

2. the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Lemma 18.2.1 ***Ascending Chain Condition for a PID***
In a principal ideal domain, any stricly increasing chain of ideals $I_1 \subset I_2 \subset \ldots$ must be finite in length.

Theorem 18.2.2 ***PID Implies UFD***
Every principal ideal domain is a unique factorization domain.

Corollary 18.2.1 $\mathbb{F}[\mathbf{x}]$ ***Is a UFD***
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a unique factorization domain.

18.3 Euclidean Domains

Definition 18.3.1 ***Euclidean Domain (ED)***
An integral domain D is called a *Euclidean domain* if there is a function d (called the *measure*) from nonzero elements of D to the nonnegative integers such that

1. $d(a) \leq d(ab)$ for all nonzero $a, b \in D$; and

2. if $a, b \in D,\ b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Theorem 18.3.1 ***ED Implies PID***
Every Euclidean domain is a principal ideal domain.

Corollary 18.3.1 ***ED Implies UFD***
Every Euclidean domain is a unique factorization domain.

Theorem 18.3.2 D ***a UFD Implies*** **D[x]** ***a UFD***
If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

Part IV

Fields

Chapter 19

Vector Spaces

19.1 Definition and Examples

Definition 19.1.1 ***Vector Space***
A set V is said to be a *vector space* over a field $\mathbb{F}$ if V is an Abelian group under addition (denoted by $+$) and, if for each $a \in \mathbb{F}$ and $v \in V$, there is an element $av \in V$ such that the following conditions hold for all $a, b \in \mathbb{F}$ and all $u, v \in V$.

1. $a(v + u) = av + au$

2. $(a + b)v = av + bv$

3. $a(bv) = (ab)v$

4. $1v = v$

Remark
The members of a vector space are called *vectors*. The members of the field are called *scalars*. The operation that combines a scalar a and a vector v to form the vector av is called *scalar multiplication*. In general, we will denote vectors by letters from the end of the alphabet, such as u, v, w, and scalars by letters from the beginning of the alphabet, such as a, b, c.

19.2 Subspaces

Definition 19.2.1 ***Subspace***
Let V be a vector space over a field $\mathbb{F}$ and let U be a subset of V. We say that U is a *subspace* of V if U is also a vector space over $\mathbb{F}$ under the operations of V.

19.3 Linear Independence

Definition 19.3.1 ***Linearly Dependent, Linearly Independent***
A set S of vectors is said to be *linearly dependent* over a field $\mathbb{F}$ if there are vectors $v_1, v_2, \ldots, v_n$ from S and elements $a_1, a_2, \ldots, a_n$ from $\mathbb{F}$, not all zero, such that $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$. A set of vectors that is not linearly dependent over $\mathbb{F}$ is called *linearly independent* over $\mathbb{F}$.

Definition 19.3.2 ***Basis***
Let V be a vector space over $\mathbb{F}$. A subset B of V is called a *basis* for V if B is linearly independent over $\mathbb{F}$ and every element of V is a linear combination of elements of B.

Theorem 19.3.1 ***Invariance of Basis Size***
If $\{u_1, u_2, \ldots, u_m\}$ and $\{w_1, w_2, \ldots, w_n\}$ are both bases of a vector space V over a field $\mathbb{F}$, then $m = n$.

Definition 19.3.3 ***Dimension***
A vector space that has a basis consisting of n elements is said to have *dimension* n. For completeness, the trivial vector space $\{0\}$ is said to be spanned by the empty set and to have dimension 0.
A vector space that has a finite basis is called *finite dimensional*; otherwise, it is called *infinite dimensional*.

Chapter 20

Extension Fields

20.1 The Fundamental Theorem of Field Theory

Definition 20.1.1 ***Extension Field***
A field $\mathbb{E}$ is an *extension field* of a field $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{E}$ and the operations of $\mathbb{F}$ are those of $\mathbb{E}$ restricted to $\mathbb{F}$.

Theorem 20.1.1 ***Fundamental Theorem of Field Theory (Kronecker's Theorem, 1887)***
Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant polynomial in $\mathbb{F}[x]$. Then there is an extension field $\mathbb{E}$ of $\mathbb{F}$ in which $f(x)$ has a zero.

20.2 Splitting Fields

Definition 20.2.1 ***Splitting Field***
Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ and let $f(x) \in \mathbb{F}[x]$ with degree at least 1. We say that $f(x)$ *splits* in $\mathbb{E}$ if there are elements $a \in \mathbb{F}$ and $a_1, a_2, \ldots, a_n \in \mathbb{E}$ such that

$$f(x) = a(x - a_1)(x - a_2) \ldots (x - a_n)$$

We call $\mathbb{E}$ a *splitting field for $f(x)$ over* $\mathbb{F}$ if

$$\mathbb{E} = \mathbb{F}(a_1, a_2, \ldots, a_n)$$

Theorem 20.2.1 ***Existence of Splitting Fields***
Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant element of $\mathbb{F}[x]$. Then there exists a splitting field $\mathbb{E}$ for $f(x)$ over $\mathbb{F}$.

Theorem 20.2.2 $\mathbb{F}(\mathbf{a}) \approx \mathbb{F}[\mathbf{x}]/\langle\mathbf{p}(\mathbf{x})\rangle)$
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension $\mathbb{E}$ of $\mathbb{F}$, then $\mathbb{F}(a)$ is isomorphic to $\mathbb{F}[x]/\langle p(x)\rangle)$. Furthermore, if $\deg p(x) = n$, then every member of $\mathbb{F}(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}$.

Corollary 20.2.1 $\mathbb{F}(\mathbf{a}) \approx \mathbb{F}(\mathbf{b})$
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension $\mathbb{E}$ of $\mathbb{F}$ and b is a zero of $p(x)$ in some extension $\mathbb{E}'$ of $\mathbb{F}$, then the fields $\mathbb{F}(a)$ and $\mathbb{F}(b)$ are isomorphic.

Lemma 20.2.3
Let $\mathbb{F}$ be a field, let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$, and let a be a zero of $p(x)$ in some extension of $\mathbb{F}$. If ϕ is a field isomorphism from $\mathbb{F}$ to $\mathbb{F}'$ and b is a zero of $\phi(p(x))$ in some extension of $\mathbb{F}'$, then there is an isomorphism from $\mathbb{F}(a)$ to $\mathbb{F}'(b)$ that agrees with ϕ on $\mathbb{F}$ and carries a to b.

Theorem 20.2.4 ***Extending*** $\phi : \mathbb{F} \to \mathbb{F}'$
Let ϕ be an isomorphism from a field $\mathbb{F}$ to a field $\mathbb{F}'$ and let $f(x) \in \mathbb{F}[x]$. If $\mathbb{E}$ is a splitting field for $f(x)$ over $\mathbb{F}$ and $\mathbb{E}'$ is a splitting field for $\phi(f(x))$ over $\mathbb{F}'$, then there is an isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ that agrees with ϕ on $\mathbb{F}$.

Corollary 20.2.2 ***Splitting Fields Are Unique***
Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. Then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic.

20.3 Zeros of an Irreducible Polynomial

Definition 20.3.1 ***Derivative***
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ belong to $\mathbb{F}[x]$. The *derivative* of $f(x)$, denoted by $f'(x)$, is the polynomial $na_n x^{x-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ in $\mathbb{F}[x]$.

Lemma 20.3.1 ***Properties of the Derivative***
Let $f(x)$ and $g(x) \in \mathbb{F}[x]$ and let $a \in \mathbb{F}$. Then

1. $(f(x) + g(x))' = f'(x) + g'(x)$.

2. $(af(x))' = af'(x)$.

3. $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

Theorem 20.3.2 ***Criterion for Multiple Zeros***
A polynomial $f(x)$ over a field $\mathbb{F}$ has a multiple zero in some extension $\mathbb{E}$ if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $\mathbb{F}[x]$.

Theorem 20.3.3 ***Zeros of an Irreducible***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$. If $\mathbb{F}$ has characteristic 0, then $f(x)$ has no multiple zeros. If $\mathbb{F}$ has characteristic $p \neq 0$, then $f(x)$ has a multiple zero if it is of the form $f(x) = g(x^p)$ for some $g(x)$ in $\mathbb{F}[x]$.

Definition 20.3.2 ***Perfect Field***
A field $\mathbb{F}$ is called *perfect* if $\mathbb{F}$ has characteristic 0 or if $\mathbb{F}$ has characteristic p and $\mathbb{F}^p = \{a^p \mid a \in \mathbb{F}\} = \mathbb{F}$.

Theorem 20.3.4 ***Finite Fields Are Perfect***
Every finite field is perfect.

Theorem 20.3.5 ***Criterion for No Multiple Zeros***
If $f(x)$ is an irreducible polynomial over a perfect field $\mathbb{F}$, then $f(x)$ has no multiple zeros.

Theorem 20.3.6 ***Zeros of an Irreducible over a Splitting Field***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$ and let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$. Then all the zeros of $f(x)$ in $\mathbb{E}$ have the same multiplicity.

Corollary 20.3.1 ***Factorization of an Irreducible over a Splitting Field***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$ and let $\mathbb{E}$ be a splitting field of $f(x)$. Then $f(x)$ has the form

$$a(x-a_1)^n(x-a_2)^n \ldots (x-a_t)^n$$

where $a_1, a_2, \ldots, a_t$ are distinct elements of $\mathbb{E}$ and $a \in \mathbb{F}$.

Chapter 21

Algebraic Extensions

21.1 Characterization of Extensions

Definition 21.1.1 ***Types of Extensions***
Let $\mathbb{E}$ be an extension field of a field $\mathbb{F}$ and let $a \in \mathbb{E}$. We call *a algebraic over* $\mathbb{F}$ if a is the zero of some nonzero polynomial in $\mathbb{F}[x]$. If a is not algebraic over $\mathbb{F}$, it is called *transcendental over* $\mathbb{F}$. An extension $\mathbb{E}$ of $\mathbb{F}$ is called an *algebraic* extension of $\mathbb{F}$ if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$. If $\mathbb{E}$ is not an algebraic extension of $\mathbb{F}$, it is called a *transcendental* extension of $\mathbb{F}$. An extension of $\mathbb{F}$ of the form $\mathbb{F}(a)$ is called a *simple* extension of $\mathbb{F}$.

Theorem 21.1.1 ***Characterization of Extensions***
Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$ and let $a \in \mathbb{E}$. If a is transcendental over $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}(x)$. If a is algebraic over $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}[x]/\langle p(x)\rangle)$, where $p(x)$ is a polynomial in $\mathbb{F}[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over $\mathbb{F}$.

Theorem 21.1.2 ***Uniqueness Property***
If a is algebraic over a field $\mathbb{F}$, then there is a unique monic irreducible polynomial $p(x)$ in $\mathbb{F}[x]$ such that $p(a) = 0$. The polynomial with this property is called the *minimal polynomial for a over* $\mathbb{F}$.

Theorem 21.1.3 ***Divisibility Property***
Let a be algebraic over $\mathbb{F}$, and let $p(x)$ be the minimal polynomial for a over $\mathbb{F}$. If $f(x) \in \mathbb{F}[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $\mathbb{F}[x]$.

21.2 Finite Extensions

Definition 21.2.1 ***Degree of an Extension***
Let $\mathbb{E}$ be an extension field of a field $\mathbb{F}$. We say that $\mathbb{E}$ *has degree n over* $\mathbb{F}$ and write $[\mathbb{E} : \mathbb{F}] = n$ if $\mathbb{E}$ has dimension n as a vector space over $\mathbb{F}$. If $[\mathbb{E} : \mathbb{F}]$ is finite, $\mathbb{E}$ is called a *finite extension* of $\mathbb{F}$; otherwise, we say that $\mathbb{E}$ is an *infinite extension* of $\mathbb{F}$.

Theorem 21.2.1 ***Finite Implies Algebraic***
If $\mathbb{E}$ is a finite extension of $\mathbb{F}$, then $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$.

Theorem 21.2.2 $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$
Let $\mathbb{K}$ be a finite extension field of the field $\mathbb{E}$ and let $\mathbb{E}$ be a finite extension field of the field $\mathbb{F}$. Then $\mathbb{K}$ is a finite extension field of $\mathbb{F}$ and $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$.

Theorem 21.2.3 ***Primitive Element Theorem (Steinitz, 1910)***
If $\mathbb{F}$ is a field of characteristic 0, and a and b are algebraic over $\mathbb{F}$, then there is an element c in $\mathbb{F}(a, b)$ such that $\mathbb{F}(a, b) = \mathbb{F}(c)$.

21.3 Properties of Algebraic Extensions

Theorem 21.3.1 ***Algebraic over Algebraic Is Algebraic***
If $\mathbb{K}$ is an algebraic extension of $\mathbb{E}$ and $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

Corollary 21.3.1 ***Subfield of Algebraic Elements***
Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$. Then the set of all elements of $\mathbb{E}$ that are algebraic over $\mathbb{F}$ is a subfield of $\mathbb{E}$.

Chapter 22

Finite Fields

22.1 Classification of Finite Fields

Theorem 22.1.1 ***Classification of Finite Fields***
For each prime p and each positive integer n, there is, up to isomorphism, a unique finite field of order p^n.

22.2 Structure of Finite Fields

Theorem 22.2.1 ***Structure of Finite Fields***
As a group under addition, $\mathrm{GF}(p^n)$ is isomorphic to

$$\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ factors}}$$

As a group under multiplication, the set of nonzero elements of $\mathrm{GF}(p^n)$ is isomorphic to $\mathbb{Z}_{p^n-1}$ (and is, therefore, cyclic).

Remark
Because there is only one field for each prime-power p^n, we may unambiguously denote it by $\mathrm{GF}(p^n)$, in honor of Galois, and call it the *Galois field of order* p^n.

Corollary 22.2.1

$$[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$$

Corollary 22.2.2 ***GF*$(\mathbf{p^n})$ *Contains an Element of Degree* n**
Let a be a generator of the group of nonzero elements of $\mathrm{GF}(p^n)$ under multiplication. Then a is algebraic over $\mathrm{GF}(p)$ of degree n.

22.3 Subfields of a Finite Field

Theorem 22.3.1 ***Subfields of a Finite Field***
For each divisor m of n, $\mathrm{GF}(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $\mathrm{GF}(p^n)$.

Chapter 23

Geometric Constructions

Part V

Special Topics

Chapter 24

Sylow Theorems

24.1 Conjugacy Classes

Definition 24.1.1 ***Conjugacy Class of* a**
Let a and b be elements of a group G. We say that a and b are *conjugate* in G (and call b the *conjugate* of a) if $xax^{-1} = b$ for some x in G. The *conjugacy class of* a is the set $\mathrm{cl}\,(()\,a) = \{xax^{-1} \mid x \in G\}$.

Theorem 24.1.1 ***Number of Conjugates of* a**
Let G be a finite group and let a be an element of G. Then, $|\mathrm{cl}\,(()\,a)| = |G : C(a)|$.

Corollary 24.1.1 $|\boldsymbol{cl}\,(()\,\mathbf{a})|$ ***Divides*** $|\mathbf{G}|$
In a finite group, $|\mathrm{cl}\,(()\,a)|$ divides $|G|$.

24.2 The Class Equation

Corollary 24.2.1 ***Class Equation***
For any finite group G,

$$|G| = \sum |G : C(a)|$$

where the sum runs over one element of a from each conjugacy class of G.

Theorem 24.2.1 p-*Groups Have Nontrivial Centers*
Let G be a nontrivial finite group whose order is a power of a prime p. Then $\mathbb{Z}(G)$ has more than one element.

Corollary 24.2.2 ***Groups of Order*** $\mathbf{p^2}$ ***Are Abelian***
If $|G| = p^2$, where p is prime, then G is Abelian.

24.3 The Sylow Theorems

Theorem 24.3.1 ***Existence of Subgroups of Prime-Power Order (Sylow's First Theorem, 1872)***
Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

Definition 24.3.1 ***Sylow* p*-Subgroup***
Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a *Sylow p-subgroup of G*.

Corollary 24.3.1 ***Cauchy's Theorem***
Let G be a finite group and let p be a prime that divides the order of G. Then G has an element of order p.

Definition 24.3.2 ***Conjugate Subgroups***
Let H and K be subgroups of a group G. We say that H and K are *conjugate* in G if there is an element in G such that $H = gKg^{-1}$.

Theorem 24.3.2 ***Sylow's Second Theorem***
If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.

Theorem 24.3.3 ***Sylow's Third Theorem***
Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to 1 modulo p and divides m. Furthermore, any two Sylow p-subgroups of G are conjugate.

Corollary 24.3.2 ***A Unique Sylow* p*-Subgroup Is Normal***
A Sylow p-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p-subgroup of G.

24.4 Applications of Sylow Theorems

Theorem 24.4.1 ***Cyclic Groups of Order* pq**
If G is a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$, then G is cyclic. In particular, G is isomorphic to $\mathbb{Z}_{pq}$.

Chapter 25

Finite Simple Groups

25.1 Historical Background

Definition 25.1.1 ***Simple Group***
A group is *simple* if its only normal subgroups are the identity subgroup and the group itself.

25.2 Nonsimplicity Tests

Theorem 25.2.1 ***Sylow Test for Nonsimplicity***
Let n be a positive integer that is not prime, and let p be a prime divisor of n. If 1 is the only divisor of n that is equal to 1 modulo p, then there does not exist a simple group of order n.

Theorem 25.2.2 2·*Odd Test*
An integer of the form $2 \cdot n$, where n is an odd number greater than 1, is not the order of a simple group.

Theorem 25.2.3 ***Generalized Cayley Theorem***
Let G be a group and let H be a subgroup of G. Let S be the group of all permutations of the left cosets of H in G. Then there is a homomorphism from G into S whose kernel lies in H and contains every normal subgroup of G that is contained in H.

Corollary 25.2.1 ***Index Theorem***
If G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G:H|!$, then H contains a nontrivial normal subgroup of G. In particular, G is not simple.

Corollary 25.2.2 ***Embedding Theorem***
If a finite non-Abelian simple group G has a subgroup of index n, then G is isomorphic to a subgroup of A_n.

Chapter 26

Generators and Relations

26.1 Motivation

Remark
In this chapter, we present a convenient way to define a group with certain prescribed properties. Simply put, we begin with a set of elements that we want to generate the group, and a set of equations (called *relations*) that specify the conditions that these generators are to satisfy. Among all such possible groups, we will select one that is as large as possible. This will uniquely determine the group up to isomorphism.

26.2 Definitions and Notation

Remark
For any set $S = \{a, b, c, \dots\}$ of distinct symbols, we create a new set $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, \dots\}$ by replacing each x in S by x^{-1}. Define the set $W(S)$ to be the collection of all formal finite strings of the form $x_1 x_2 \dots x_k$, where each $x_i \in S \cup S^{-1}$. The elements of $W(S)$ are called *words from* S. We also permit the string with no elements to be in $W(S)$. this word is called the *empty word* and is denoted by e.

We may define a binary operation on the set $W(S)$ by juxtaposition; that is, if $x_1 x_2 \dots x_k$ and $y_1 y_2 \dots y_t$ belong to $W(S)$, then so does $x_1 x_2 \dots x_k y_1 y_2 \dots y_t$. Observe that this operation is associative and the empty word is the identity. Also, notice that a word such as aa^{-1} is not the identity, because we are treating the elements of $W(S)$ as formal symbols with no implied meaning.

Definition 26.2.1 ***Equivalence Classes of Words***
For any pair of elements u and v of $W(S)$, we say that u is related to v if v can be obtained from u by a finite sequence of insertions or deletions of words of the form xx^{-1} or $x^{-1}x$, where $x \in S$.

26.3 Free Group

Theorem 26.3.1 ***Equivalence Classes Form a Group***
Let S be a set of distinct symbols. For any word u in $W(S)$, let $\overline{u}$ denote the set of all words in $W(S)$ equivalent to u (that is, $\overline{u}$ is the equivalence class containing u). Then the set of all equivalence classes of elements of $W(S)$ is a group under the operation $\overline{u} \cdot \overline{v} = \overline{uv}$. This group is called a *free group on S*.

Theorem 26.3.2 ***Universal Mapping Property***
Every group is a homomorphic image of a free group.

Corollary 26.3.1 ***Universal Factor Group Property***
Every group is isomorphic to a factor group of a free group.

26.4 Generators and Relations

Definition 26.4.1 ***Generators and Relations***
Let G be a group generated by some subset $A = \{a_1, a_2, \ldots, a_n\}$ and let F be the free group on A. Let $W = \{w_1, w_2, \ldots, w_t\}$ be a subset of F and let N be the smallest normal subgruop of F containing W. We say that G is *given by the generators $a_1, a_2, \ldots, a_n$ and the relations* $w_1 = w_2 = \cdots = w_t = e$ if there is an isomorphism from F/N onto G that carries a_iN to a_i. The notation for this situation is

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e \rangle)$$

Theorem 26.4.1 ***Dyck's Theorem (1882)***
Let

$$G = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = e \rangle)$$

and let

$$\overline{G} = \langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t = w_{t+1} = \cdots = w_{t+k} = e \rangle)$$

Then $\overline{G}$ is a homomorphic image of G.

Corollary 26.4.1 ***Largest Group Satisfying Defining Relations***
If K is a group satisfying the defining relations of a finite group G and $|K| \geq |G|$, then K is isomorphic to G.

26.5 Classification of Groups of Order Up to 15

Theorem 26.5.1 ***Classification of Groups of Order 8 (Cayley, 1859)***
Up to isomorphism, there are only five groups of order 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_4, and the quaternions.

26.6 Characterization of Dihedral Groups

Theorem 26.6.1 ***Characterization of Dihedral Groups***
Any group generated by a pair of elements of order 2 is dihedral.

Chapter 27

Symmetry Groups

27.1 Isometries

Remark
It is convenient to begin our discussion with the definition of an isometry (from the Greek *isometros*, meaning "equal measure") in $\mathbb{R}^n$.

Definition 27.1.1 ***Isometry***
An *isometry* of n-dimensional space $\mathbb{R}^n$ is a function from $\mathbb{R}^n$ onto $\mathbb{R}^n$ that preserves distance.

Definition 27.1.2 ***Symmetry Group of a Figure in*** $\mathbb{R}^{\mathbf{n}}$
Let F be a set of points in $\mathbb{R}^n$. the *symmetry group of* F in $\mathbb{R}^n$ is the set of all isometries of $\mathbb{R}^n$ that carry F onto itself. The group operation is function composition.

27.2 Classification of Finite Plane Symmetry Groups

Theorem 27.2.1 ***Finite Symmetry Groups in the Plane***
The only finite plane symmetry groups are $\mathbb{Z}_n$ and D_n.

27.3 Classification of Finite Groups of Rotations in $\mathbb{R}^3$

Theorem 27.3.1 ***Finite Groups of Rotations in*** $\mathbb{R}^3$
Up to isomorphism, the finite groups of rotations in $\mathbb{R}^3$ are $\mathbb{Z}_n$, D_n, A_r, S_4, and A_5.

Chapter 28

Frieze Groups and Crystallographic Groups

28.1 The Frieze Groups

Remark
In this chapter, we discuss an interesting collection of infinite symmetry groups that arise from periodic designs in a plane. There are two types of such groups. The *discrete frieze groups* are the plane symmetry groups of patterns whose subgroups of translations are isomorphic to $\mathbb{Z}$. These kinds of designs are the ones used for decorative strips and for patterns on jewelry. In mathematics, familiar examples include the graphs of $y = \sin(x)$, $y = \tan(x)$, $y = |\sin(x)|$, and $|y| = \sin(x)$. After we analyze the discrete frieze groups, we examine the discrete symmetry groups of plane patterns whose subgroups of translations are isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.

28.2 The Crystallographic Groups

Remark
The seven frieze groups catalog all symmetry groups that leave a design invariant under all multiples of just one translation. However, there are 17 additional kinds of discrete plane symmetry groups that arise from infinitely repeating designs in a plane. these groups are the symmetry groups of plane patterns whose subgroups of translations are isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. Consequently, the patterns are invariant under linear combinations of two linearly independent translations. These 16 groups were first studied by the 19th-century crystallographers and often called the *plane crystallographic groups*. Another term occasionally used for these groups is *wallpaper groups*.

28.3 Identification of Plane Periodic Patterns

Remark
A *lattice of points* of a pattern is a set of images of any particular point acted on by the translation group of the pattern. A *lattice unit* of a pattern whose translation subgroup is

generated by u and v is a parallelogram formed by a point of the pattern and its image under u, v, and $u+v$. A *generating region* (or *fundamental region*) of a periodic pattern is the smallest portion of the lattice unit whose images under the full symmetry of the group of the pattern cover the plane.

Chapter 29

Symmetry and Counting

29.1 Motivation

Remark
In general, we say that two designs (arrangements of beads) A and B are *equivalent under a group* G of permutations of the arrangements if there is an element ϕ in G such that $\phi(A) = B$. That is, two designs are equivalent under G if they are in the same orbit of G. It follows, then, that the number of nonequivalent designs under G is simply the number of orbits of designs under G. (The set being permuted is the set of all possible designs or arrangements.)

29.2 Burnside's Theorem

Definition 29.2.1 ***Elements Fixed by*** ϕ
For any group G of permutations on a set S and any ϕ in G, we let $\text{fix}(\phi) = \{i \in S \mid \phi(i) = i\}$. This set is called the *elements fixed by* ϕ (or more simply, "fix of ϕ").

Theorem 29.2.1 ***Burnside's Theorem***
If G is a finite group of permutations on a set S, then the number of orbits of elements of S under G is

$$\frac{1}{|G|}\sum_{\phi \in G} |\text{fix}(\phi)|$$

29.3 Group Action

Remark
Our informal approach to counting the number of objects that are considered nonequivalent can be made formal as follows. If G is a group and S is a set of objects, we say that G *acts on* S if there is a homomorphism γ from G to $\text{sym}(S)$, the group of all permutations on S. (The hommomorphism is sometimes called the *group action.*) For convenience, we denote the image of g under γ as γ_g. Then two objects x and y in S are viewed as equivalent under the action of G if and only if $\gamma_g(x) = y$ for some g in G. Notice that when γ is one-to-one, the elements of G may be regarded as permutations on S. On the other hand, when γ is not one-to-one, the

elements of G may still be regarded as permutations on S, but there are distinct elements g and h in G such that γ_g and γ_h induce the same permutation on S [that is, $\gamma_g(x) = \gamma_h(x)$ for all x in S]. Thus, a group acting on a set is a natural generalization of the permutation group concept.

Chapter 30

Cayley Digraphs of Groups

30.1 The Cayley Digraph of a Group

Definition 30.1.1 ***Cayley Digraph of a Group***
Let G be a finite group and let S be a set of generators for G. We define a digraph $\text{Cay}(S : G)$, called the *Cayley digraph of G with generating set S*, as follows.

1. Each element of G is a vertex of $\text{Cay}(S : G)$.

2. For x and y in G, there is an arc from x to y if and only if $xs = y$ for some $s \in S$.

30.2 Hamiltonian Circuits and Paths

Remark
Obviously, this idea can be applied to any digraph; that is, one starts at some vertex and attempts to traverse the digraph by moving along arcs in such a way that each vertex is visited exactly once before returning to the starting vertex. (To go from x to y, there must be an arc from x to y.) Such a sequence of arcs is called a *Hamiltonian circuit* in the digraph. A sequence of arcs that passes through each vertex exactly once without returning to the starting point is called a *Hamiltonian path*. In the rest of this chapter, we concern ourselves with the existence of Hamiltonian circuits and paths in Cayley digraphs.

Theorem 30.2.1 ***A Necessary Condition***
$\text{Cay}(\{(1, 0), (0, 1)\} : \mathbb{Z}_m \oplus \mathbb{Z}_n)$ does not have a Hamiltonian circuit when m and n are relatively prime and greater than 1.

Theorem 30.2.2 ***A Sufficient Condition***
$\text{Cay}(\{(1, 0), (0, 1)\} : \mathbb{Z}_m \oplus \mathbb{Z}_n)$ has a Hamiltonian circuit when n divides m.

Theorem 30.2.3 ***Abelian Groups Have Hamiltonian Paths***
Let G be a finite Abelian group, and let S be any (nonempty*) generating set for G. Then $\text{Cay}(S : G)$ has a Hamiltonian path.

*If S is the empty set, it is customary to define $\langle S \rangle)$ as the identity group. We prefer to ignore this trivial case.

Chapter 31

Introduction to Algebraic Coding Theory

31.1 Linear Codes

Definition 31.1.1 ***Linear Code***
An (n, k) *linear code* of a finite field $\mathbb{F}$ is a k-dimensional subspace V of the vector space

$$\mathbb{F}^n = \underbrace{\mathbb{F} \oplus \mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n \text{ copies}}$$

over $\mathbb{F}$. The members of V are called the *code words.* When $\mathbb{F}$ is $\mathbb{Z}_2$, the code is called *binary.*

Definition 31.1.2 ***Hamming Distance, Hamming Weight***
The *Hamming distance* between two vectors in $\mathbb{F}^n$ is the number of components in which they differ. The *Hamming weight* of a vector is the number of nonzero components of the vector. The *Hamming weight* of a linear code is the minimum weight of any nonzero vector in the code.

Theorem 31.1.1 ***Properties of Hamming Distance and Hamming Weight***
For any vectors u, v and w, $d(u, v) \leq d(u, w) + d(w, v)$ and $d(u, v) = \mathrm{wt}(u - v)$.

Theorem 31.1.2 ***Correcting Capability of a Linear Code***
If the Hamming weight of a linear code is at least $2t + 1$, then the code can correct any t or fewer errors. Alternatively, the same code can detect any $2t$ or fewer errors.

31.2 Parity-Check Matrix Decoding

Lemma 31.2.1 ***Orthogonality Relation***
Let C be a systematic (n, k) linear code over $\mathbb{F}$ with a standard generator matrix G and parity-check matrix H. Then, for any vector v in $\mathbb{F}^n$, we have $vH = 0$ (the zero vector) if and only if v belongs to C.

Theorem 31.2.2 ***Parity-Check Matrix Decoding***
Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no one row is a scalar multiple of any other row.

31.3 Coset Decoding

Theorem 31.3.1 ***Coset Decoding Is Nearest-Neighbor Decoding***
In coset decoding, a received word w is decoded as a code word c such that $d(w, c)$ is a minimum.

Definition 31.3.1 ***Syndrome***
If an (n, k) linear code over $\mathbb{F}$ has parity-check matrix H, then, for any vector u in $\mathbb{F}^n$, the vector uH is called the *syndrome* of u.

Theorem 31.3.2 ***Same Coset-Same Syndrome***
Let C be an (n, k) linear code over $\mathbb{F}$ with a parity-check matrix H. Then, two vectors of $\mathbb{F}^n$ are in the same coset of C if and only if they have the same syndrome.

Chapter 32

An Introduction to Galois Theory

32.1 Fundamental Theorem of Galois Theory

Definition 32.1.1 ***Automorphism, Galois Group, Fixed Field of* H**
Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$. An *automorphism of* $\mathbb{E}$ is a ring isomorphism from $\mathbb{E}$ onto $\mathbb{E}$. The *Galois group* of $\mathbb{E}$ over $\mathbb{F}$, $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, is the set of all automorphisms of $\mathbb{E}$ that take every element of $\mathbb{F}$ to itself. If H is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then set

$$\mathbb{E}_H = \{x \in \mathbb{E} \mid \phi(x) = x, \ \forall\ \phi \in H\}$$

is called the *fixed field of* H.

Theorem 32.1.1 ***Fundamental Theorem of Galois Theory***
Let $\mathbb{F}$ be a field of characteristic 0 or a finite field. If $\mathbb{E}$ is the splitting field over $\mathbb{F}$ for some polynomial in $\mathbb{F}[x]$, then the mapping from the set of subfields of $\mathbb{E}$ containing $\mathbb{F}$ to the set of subgroups of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ given by $\mathbb{K} \to \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a one-to-one correspondence. Furthermore, for any subfield $\mathbb{K}$ of $\mathbb{E}$ containing $\mathbb{F}$,

1. $[\mathbb{E} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{K})|$ and $[\mathbb{K} : \mathbb{F}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})| \,/\, |\mathrm{Gal}(\mathbb{E}/\mathbb{K})|$. [The index of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ in $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ equals the degree of $\mathbb{K}$ over $\mathbb{F}$.]

2. If $\mathbb{K}$ is the splitting field of some polynomial in $\mathbb{F}[x]$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is isomorphic to $\mathrm{Gal}(\mathbb{E}/\mathbb{F})/\mathrm{Gal}(\mathbb{E}/\mathbb{K})$.

3. $\mathbb{K} = \mathbb{E}_{\mathrm{Gal}(\mathbb{E}/\mathbb{K})}$. [The fixed field of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is $\mathbb{K}$.]

4. If H is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then $H = \mathrm{Gal}(\mathbb{E}/\mathbb{E}_H)$. [The automorphism group of $\mathbb{E}$ fixing $\mathbb{E}_H$ is H.]

32.2 Solvability of Polynomials by Radicals

Definition 32.2.1 ***Solvable by Radicals***
Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ is *solvable by radicals over* $\mathbb{F}$ if $f(x)$ splits in some extension $\mathbb{F}(a_1, a_2, \ldots, a_n)$ of $\mathbb{F}$ and there exist positive integers $k_1, \ldots, k_n$ such that $a_1^{k_1} \in \mathbb{F}$ and $a_i^{k_i} \in \mathbb{F}(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, n$.

Definition 32.2.2 *Solvable Group*
We say that a group G is *solvable* if G has a series of subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_k = G$$

where, for each $0 \leq i < k$, H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

Theorem 32.2.1 *Splitting Field of* $\mathbf{x^n - a}$
Let $\mathbb{F}$ be a field of characteristic 0 and let $a \in \mathbb{F}$. If $\mathbb{E}$ is the splitting field of $x^n - a$ over $\mathbb{F}$, then the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

Theorem 32.2.2 *Factor Group of a Solvable Group is Solvable*
A factor group of a solvable group is solvable.

Theorem 32.2.3 N *and* G/N *Implies* G *Is Solvable*
Let N be a normal subgroup of a group G. If both N and G/N are solvable, then G is solvable.

Theorem 32.2.4 *(Galois) Solvable by Radicals Implies Solvable Group*
Let $\mathbb{F}$ be a field of characteristic 0 and let $f(x) \in \mathbb{F}[x]$. Suppose the $f(x)$ splits in $\mathbb{F}(a_1, a_2, \ldots, a_t)$, where $a_1^{n_1} \in \mathbb{F}$ and $a_i^{n_i} \in \mathbb{F}(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, t$. Let $\mathbb{E}$ be the splitting field for $f(x)$ over $\mathbb{F}$ in $\mathbb{F}(a_1, a_2, \ldots, a_t)$. Then the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is solvable.

Chapter 33

Cyclotomic Extensions

33.1 Cyclotomic Polynomials

Remark
Recall from Example 2 in Chapter 16 that the complex zeros of $x^n - 1$ are 1, $\omega = \cos(2\pi/n) = i\sin(2\pi/n)$, $\omega^2, \omega^3, \ldots, \omega^{n-1}$. Thus, the splitting field of $x^n - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega)$. This field is called the *nth cyclotomic extension of* $\mathbb{Q}$, and the irreducible factors of $x^n - 1$ over $\mathbb{Q}$ are called the *cyclotomic polynomials*.

Since $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$ generates a cyclic group of order n under multiplication, we know from Corollary 3 of Theorem 4.2 that the generators of $\langle\omega\rangle)$ are the elements of the form ω^k, where $1 \leq k \leq n$ and $\gcd(n,k) = 1$. These generators are called the *primitive nth roots of unity*. Recalling that we use $\phi(n)$ to denote the number of positive integers less than or equal to n and relatively prime to n, we see that for each positive integer n there are precisely $\phi(n)$ primitive nth roots of unity. The polynomials whose zeros are the $\phi(n)$ primitive nth roots of unity have a special name.

Definition 33.1.1
For any positive integer n, let $\omega_1, \omega_2, \ldots, \omega_{\phi(n)}$ denote the primitive nth roots of unity. the *nth cyclotomic polynomial over* $\mathbb{Q}$ is the polynomial $\Phi_n(x) = (x-\omega_1)(x-\omega_2)\ldots(x-\omega_{\phi(n)})$.

Theorem 33.1.1
For every positive integer n, $x^n - 1 = \Pi_{d|n}\Phi_d(x)$, where the product runs over all positive divisors d of n.

Theorem 33.1.2
For every positive integer n, $\Phi_n(x)$ has integer coefficients.

Theorem 33.1.3 ***(Gauss)***
The cyclotomic polynomials $\Phi_n(s)$ are irreducible over $\mathbb{Z}$.

Theorem 33.1.4
Let ω be a primitive nth root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \approx U(n)$.

33.2 The Constructible Regular n-gons

Lemma 33.2.1
Let n be a positive integer and let $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$. Then $\mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{Q}(\omega)$.

Theorem 33.2.2 ***(Gauss, 1796)***
It is possible to construct the regular n-gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \ldots p_t$, where $k \geq 0$ and the p_i's are distinct primes of the form $2^m + 1$.