Memo of C. C. Pinter, "A Book of Abstract Algebra"

Kwame Ackah Bohulu

March 5, 2019

0.1 Introduction to Groups

Groups, $< \mathcal{G}, * >$

Definition 1. A set $\mathcal{G}$ is called a group if it satisfies the axioms

1. operation $*$ is associative *i.e.* $(a * b) * c = a * (b * c))$
2. $\exists e \in \mathcal{G}$ such that $a * e = e * a = a$, $\forall a \in \mathcal{G}$
3. $\forall a \in \mathcal{G}$, $\exists a^{-1} \in \mathcal{G}$ suth that $a * a^{-1} = a^{-1} * a = e$

If the commutative law $(a * b = b * a)$ holds in the group, it is known as an Abelian group.

$< \mathbb{Z}, + >$ additive group of the integers

$< \mathbb{Q}, + >$ additive group of the rational numbers

$< \mathbb{R}, + >$ additive group of the real numbers

$< \mathbb{Q}^*, \cdot >$ multiplication group of the nonzero rational numbers

$< \mathbb{R}^*, \cdot >$ multiplication group of the nonzero real numbers

$\mathbb{Z}_n$ group of integers modulo n

0.2 Basic Properties of Groups

Theorem 1. if $\exists a, b, c \in < \mathcal{G}, * >$,then

1. $ab = ac \Rightarrow b = c$ and
2. $ba = ca \Rightarrow b = c$

Theorem 2. if $\exists a, b \in < \mathcal{G}, * >$,then

1. $ab = e \Rightarrow a = b^{-1}$ and
2. $ba = e \Rightarrow b = a^{-1}$

Theorem 3. if $\exists a, b \in < \mathcal{G}, * >$,then

1. $(ab)^{-1} = b^{-1}a^{-1}$
2. $(a^{-1})^{-1} = a$

$| < \mathcal{G}, * > |$ order (number of elements) of $< \mathcal{G}, * >$

Subgroups, $< \mathcal{S}, * >$

Definition 2. Assuming $\exists \ < \mathcal{G}, * >$ and $cS \neq \{\}, \ \mathcal{S} \subset \mathcal{G}$. If $< \mathcal{S}, * >$

1. is closed with respect to operation $*$ and
2. closed with respect to inverses

it is a subgroup of $< \mathcal{G}, * >$. Every subgroup is also a group on its own.

$< 2\mathbb{Z}, + >$ group of all even integers is subgroup of $< \mathbb{Z}, + >$

$< \{e\}, * >$ smallest trivial group of $< \mathcal{G}, * >$

$< \mathcal{G}, * >$ largest trivial group of $< \mathcal{G}, * >$

Cyclic (sub)Group, $< a >$

Definition 3. if $< \mathcal{G}, * >$ is generated by all possible combination of operations on a and a^{-1} it is a cyclic group.
If the element a from $< \mathcal{G}, * >$ is used to generate a subgroup $< \mathcal{S}, * >$ it is called a cyclic subgroup.

a Generator of cyclic group

Defining equation of $< \mathcal{G}, * >$ A set of equations involving only the generators and their inverses

Defining equation of $< \mathcal{G}, * >$ must completely describe operation table

0.3 Functions

$y = f(x)$, $f : A \mapsto B$

Definition 4. Let $\mathcal{A}$ and $\mathcal{B}$ be sets. A function is a rule which assigns every element of $\mathcal{A}$(the domain) to a unique element in $\mathcal{B}$(the range)

injective function each element of the range is the image of no more than one element of domain

surjective function each element of the range is the image of atleast one element of the domain

bijective function injective and surjective function

Composition of functions, $f \circ g$

Definition 5. Let $f : \mathcal{A} \mapsto \mathcal{B}$ and $g : \mathcal{B} \mapsto \mathcal{C}$ be functions. $[f \circ g](x) := f(g(x)) \ \forall x \in \mathcal{A}$

0.4 Groups of Permutations

Permutation of sets, $f : \mathcal{A} \to \mathcal{A}$

Definition 6. Permutation of sets is a bijective function $f : \mathcal{A} \to \mathcal{A}$. It forms a group with respect to composition.

Every permutation can be broken down into cycles.

cycles

Definition 7. let $a_1, ...a_n$ be distinct elements of $\{1, 2, ..., n\}$. A cycle $(a_1 a_2 ... a_s)$ is a permutation of $\{1, 2, ..., n\}$ which carries a_1 to a_2, a_2 to a_3,...,a_{s-1} to a_s and a_s to a_1 while leaving all the remaining elements of $\{1, 2, ..., n\}$ fixed.

Theorem 4. Every permutation is either the identity, a single cycle or a product of disjoint cycles.

A cycle of length 2 is called a transposition.

Every cycle can be expressed as a product of transpositions and for a given permutation, the number of transpositions is either always odd or always even

Theorem 5. No matter how the identity permutation is written as a product of transpositions, the number of transpositions is even.

Theorem 6. if $\Pi \in S_n$(group of permutations length n) then Π cannot be both an odd and even permutation

0.5 Isomorphism

for simplicity sake, we represent a group $< \mathcal{G}, * >$ by $\mathcal{G}$ unless otherwise stated.

$\mathcal{G}_1 \cong \mathcal{G}_2$

Definition 8. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be groups. A bijective function $f : \mathcal{G}_1 \to \mathcal{G}_2$ with the property that for any two elements $a, b \in G_1$

$$f(ab) = f(a)f(b)$$

is called an isomorphism from $\mathcal{G}_1$ to $\mathcal{G}_2$. if an isomorphism from $\mathcal{G}_1$ to $\mathcal{G}_2$ exist, then $\mathcal{G}_1$ is isomorphic $\mathcal{G}_2$ ($\mathcal{G}_1 \cong \mathcal{G}_2$)

Theorem 7. (Cayley's Theorem)
Every group is isomorphic to a group of permutations

0.6 Order of Group Elements

Theorem 8. (Law of exponents)
if $\mathcal{G}$ is a group and $a \in \mathcal{G}$ then $\forall\ m, n \in \mathbb{Z}$

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Theorem 9. (Division Algorithm)
if $m, n \in \mathbb{Z},\ n > 0$ there $\exists$ unique integers q, r s.t.

$$m = nq + r, \text{ and } 0 \leq r < n$$

Definition 9. if $\exists\ m \in \mathbb{Z}$ s.t $a^m = e$ then the order of a is the least positive integer m s.t $a^m = e$. if no such m exists, a has order infinity

Theorem 10. if the order of a is n, then there are exactly n powers of a given by

$$a^0, a^1, ..., a^{n-1}$$

Theorem 11. if the order of a is infinity, then all powers of a are different, ie

$$a^r \neq a^s$$

Theorem 12. if an element a in group $\mathcal{G}$ has order n. Then $a^t = e$ iff t is a multiple of n

ord(a) order of element $a \in \mathcal{G}$

0.6.1 Cyclic Groups ($\mathcal{G} = \{a^n : n \in \mathbb{Z}\}$)

order of generator a determines order of cyclic group $\mathcal{G}$

Theorem 13. Isomorphism of Cyclic Groups

1. $\forall n > 0$ every cyclic group of order n is isomorphic to $\mathbb{Z}_n$
2. every cyclic group of order ∞ is isomorphic to $\mathbb{Z}$

0.7 Partitions and Equivalence Relations

Partition of a Set $\mathcal{A}$

Definition 10. a family $\{\mathcal{A}_i : i \in I\}$ of non-empty subsets of $\mathcal{A}$ such that

1. if any 2 classes $\mathcal{A}_i,\ \mathcal{A}_j$ have a common element x, then $\mathcal{A}_i = \mathcal{A}_j$
2. Every element x of $\mathcal{A}$ lies in one of the classes

equivalence relation a relation $\sim$ which is

1. reflexive : if $x \sim x \forall\ x \in \mathcal{A}$
2. symmetric : if $x \sim y$ then $y \sim x$
3. reflexive : if $x \sim y$ and $y \sim z$ then $x \sim z$

equivalence of elements means two elements are members of the same class

equivalence class of x $[x] = \{y \in Ay \sim x\}$

Lemma: if $x \sim y$ then $[x] = [y]$

Theorem 14. if $\sim$ is an equivalence relation on $\mathcal{A}$ the family of all the equivalence classes is a partition of A

0.8 Counting Cosets

$\mathcal{G}$ represents a group

$\mathcal{H}$ represents a subgroup of $\mathcal{G}$

Cosets

Definition 11. For any element $a \in \mathcal{G}$, the symbol $a\mathcal{H}$ denotes the set of all products ah as a remains constant and h ranges over $\mathcal{H}$ and $a\mathcal{H}$ is called the *left coset.* The right coset may be defined in similar fashion.

Theorem 15. The family of all cosets $\mathcal{H}a$ as a range over $\mathcal{G}$ is a partition of $\mathcal{G}$

Theorem 16. if $\mathcal{H}a$ is any coset of $\mathcal{H}$, there is a one-to-one correspondence from $\mathcal{H}$ to $\mathcal{H}a$

Theorem 17. Assume that $\mathcal{G}$ is a finite group. then $\text{ord}(\mathcal{G}) = k\text{ord}(\mathcal{H})$ $k \in \mathbb{Z}$. This is known as Lagrange's theorem

Theorem 18. if $\text{ord}(\mathcal{G})$ is prime, then $\mathcal{G}$ is a cyclic group and all $a \in \mathcal{G},\ a \neq e$ is a generator of the group.

Theorem 19. The order of every element of a finite group divides the order of the group

index of $\mathcal{H}$ in $\mathcal{G}$ $(\mathcal{H} : \mathcal{G})$ is the number of cosets of $\mathcal{H}$ in $\mathcal{G}$

0.9 Homomorphism

$\mathcal{G}$ and $\mathcal{H}$ be groups.

xax^{-1} is a conjugate

Definition 12. A homomorphism from $\mathcal{G}$ to $\mathcal{H}$ is a function $f : \mathcal{G} \to \mathcal{H}$ s.t. for any 2 elements $a, b \in \mathcal{G}$

$$f(ab) = f(a)f(b)$$

The operations are preserved by the homomorphism

Theorem 20. if a homomorphism exist between $\mathcal{G}$ and $\mathcal{H}$, then $\forall a \in \mathcal{G}$

1. $f(e) = e$
2. $f(a^{-1}) = [f(a)]^{-1}$

Normal Subgroup

Definition 13. let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. $\mathcal{H}$ is called a normal subgroup of $\mathcal{G}$ if it is closed with respect to conjugates, ie

$$\forall\ a \in \mathcal{H},\ x \in \mathcal{G}\ xax^{-1} \in \mathcal{H}$$

Kernel

Definition 14. let $f : \mathcal{G} \to \mathcal{H}$ be a homomorphism. The kernel of f is the set $\mathcal{K}$ of all elements of $\mathcal{G}$ which are carried by f onto the neutral element of H ie

$$\mathcal{K} = \{x \in \mathcal{G} : f(x) = e\}$$

Theorem 21. let $f : \mathcal{G} \to \mathcal{H}$ be a homomorphism.

1. The kernel of f is a normal subgroup of $\mathcal{G}$
2. the range of f is a subgroup of $\mathcal{H}$

0.10 Quotient Groups

let $\mathcal{G}$ be a group and $\mathcal{H}$ be a normal subgroup of $\mathcal{G}$

Theorem 22. $a\mathcal{H} = \mathcal{H}a,\ \forall a \in \mathcal{G}$

Theorem 23. if $\mathcal{H}a = \mathcal{H}c$ and $\mathcal{H}b = \mathcal{H}d$. then $\mathcal{H}(ab) = \mathcal{H}(cd)$ (Coset Multiplication)

$\mathcal{G}/\mathcal{H}$: set of all cosets of $\mathcal{H}$

Theorem 24. $\mathcal{G}/\mathcal{H}$ with coset multiplication is a group. such a group is known as a quotient/factor group of $\mathcal{G}$ by $\mathcal{H}$

Theorem 25. $\mathcal{G}/\mathcal{H}$ is a homomorphic group of $\mathcal{G}$.

Theorem 26. if $\mathcal{G}$ is a group and $\mathcal{H}$ is its subgroup, then

1. $\mathcal{H}a = \mathcal{H}b$ iff $ab^{-1} \in \mathcal{H}$
2. $\mathcal{H}a = \mathcal{H}$ iff $a \in \mathcal{H}$

0.11 Fundemental Theorem of Homomorphism

Theorem 27. let $f : \mathcal{G} \to \mathcal{H}$ be a homomorphism with kernel $\mathcal{K}$. Then

$$f(a) = f(b) \text{ iff } \mathcal{K}a = \mathcal{K}b$$

Theorem 28. let $f : \mathcal{G} \to \mathcal{H}$ be a homomorphism with kernel $\mathcal{K}$. Then

$$\mathcal{H} \simeq \mathcal{G}/\mathcal{K}$$

.ie $\mathcal{H}$ is isomorphic image of $\mathcal{G}/\mathcal{K}$

0.12 Rings

Rings

Definition 15. A ring is a set $\mathcal{A}$ with two operations $(+, \cdot)$ which satisfy the following axioms

1. $\mathcal{A}$ with $+$ alone is an abelian group
2. $\cdot$ is associative
3. $\cdot$ is distributive over $+$

$\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ are examples of rings

Theorem 29. let a, b be elemets of ring $\mathcal{A}$. then

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

optional properties of rings

1. if $\cdot$ is commutative in a ring it is known as a *commutative ring*
2. if a multiplicative identity element exists in a ring, it is known as a ring with unity
3. if a ring $\mathcal{A}$ with unity has elements with multiplicative inverse we call such elements invertible
4. if $\mathcal{A}$ is a commutative ring with unity in which every nonzero element is invertible $\mathcal{A}$ is called a *Field*

5. in any ring, a nonzero element a is called a *divisor of zero* if there is a nonzero element b in the ring s.t. $ba = ab = 0$
6. A ring has a cancellation property if for any$a, b, c \in \mathcal{A}$, $a \neq 0,\ ab = ac$or $ba = ca \implies b = c$

Theorem 30. A ring has cancellation property iff it has no divisors of zero

Integral Domain

Definition 16. An integral domain is a commutative ring with unity which has the cancellation property

0.13 Ideals and Homomorphisms

Subring

Definition 17. $\mathcal{B}$ is a subring of $\mathcal{A}$ if it is closed with respect to addition multiplication and negatives

$\mathcal{B}$ absorbs products of $\mathcal{A}$ if $\forall b \in \mathcal{B}$ and $x \in \mathcal{A},\ xb \in \mathcal{B}$ and $bx \in \mathcal{B}$

Ideal

Definition 18. A nonempty subset$\mathcal{B}$ of a ring $\mathcal{A}$ which is closed with respect to addition multiplication and absorbs products in $\mathcal{A}$ negatives

A homomorphism from ring $\mathcal{A}$to ring $\mathcal{B}$ is a function $f : \mathcal{A} \to \mathcal{B}$ such that if $f(x_1) = y_1,\ f(x_2) = y_2$ then

1. $f(x_1 + x_2) = y_1 + y_2$
2. $f(x_1 x_2) = y_1 y_2$

if there exists a homomorphism from ring $\mathcal{A}$ to ring $\mathcal{B}$ then the kernel $\mathcal{K}$ is given by $\mathcal{K} = \{x \in \mathcal{A} : f(x) = 0\}$ and is an ideal of $\mathcal{A}$

0.14 Quotient Rings

$\mathcal{A},\ \mathcal{B}$ is a ring

$\mathcal{J}$ is an ideal of $\mathcal{A}$

Coset $\mathcal{J} + a$

Definition 19. For any element $a \in \mathcal{A},\ \mathcal{J} + a$ (coset) is the set of all sums $j + a$ as a remains constant and j ranges over $\mathcal{J}$, ie $\mathcal{J} + a = \{j + a : j \in \mathcal{J}\}$

Coset Addition $(\mathcal{J}+a)+(\mathcal{J}+b)=\mathcal{J}+(a+b)$

Coset Multiplication $(\mathcal{J}+a)(\mathcal{J}+b)=\mathcal{J}+(ab)$

Theorem 31. if $\mathcal{J}+a=\mathcal{J}+c$ and $\mathcal{J}+b=\mathcal{J}+d$ then

1. $\mathcal{J}+(a+b)=\mathcal{J}+(c+d)$
2. $\mathcal{J}+(ab)=\mathcal{J}+(cd)$

A/J set of all cosets of $\mathcal{J}$ in $\mathcal{A}$

Theorem 32. $\mathcal{A}/\mathcal{J}$ with coset addition and multiplication is a ring

Theorem 33. $\mathcal{A}/\mathcal{J}$ is a homomorphic image of $\mathcal{A}$

Theorem 34. $\mathcal{B}\equiv\mathcal{A}/\mathcal{K}$ ie $\mathcal{B}$ is a homomorphic image of $\mathcal{A}/\mathcal{K}$

An ideal $\mathcal{J}$ of a commutative ring $\mathcal{A}$ is said to be *prime ideal* if for any two elements a, b in the ring , if $ab\in\mathcal{J}$ then $a\in\mathcal{J}$ or $b\in\mathcal{J}$

Whenever $\mathcal{J}$ is a prime ideal of a commutative ring with unity $\mathcal{A}$, the quotient ring $\mathcal{A}/\mathcal{J}$ is an *ideal integral domain*

a proper ideal of a ring is not equal to the whole ring

a proper ideal is called *maximal ideal* if there exists no proper ideal $\mathcal{K}$ of $\mathcal{A}$ such that $\mathcal{J}\subset\mathcal{K},\ \mathcal{J}\neq\mathcal{K}$

if $\mathcal{A}$ is a commutative ring with unity, then $\mathcal{J}$ is a maximal ideal of $\mathcal{A}$ if $\mathcal{A}/\mathcal{J}$ is a field

0.15 Integral Multiples

Integral Domain

Definition 20. An integral domain is a commutative ring with the cancellation property(no divisors of zero)

Characteristic of a Ring

Definition 21. The characteristic of a ring $\mathcal{A}$ is the least positive integer n s.t. $n\cdot 1=0$. Else, $\mathcal{A}$ has characteristic 0

Theorem 35. all nonzero elements in an integral domain hhave the same additive order, where the additive order is the least positive integer n s.t $n \cdot a = 0$.

Theorem 36. in an integral domain with non-zero characteristic, the characteristic is a prime number p

Theorem 37. in any integral domain $\mathcal{A}$ with characteristic p, $(a+b)^p = a^p + b^p \forall a, bin\mathcal{A}$

Theorem 38. every finite integral domain is a field

0.16 The Integers

Ordered Integral Domain

Definition 22. An integral domain $\mathcal{A}$ with a relation symbolized by $<$ with the following properties

1. for any $a, b \in \mathcal{A}$ exactly one of the ff is true

$$a = b, \ a < b, \ b < a$$

. Furthermore, for any $a, b, c \in \mathcal{A}$

2. if $a < b$ and $b < c$ then $a < c$
3. if $a < b$, then $a + c < b + c$
4. if $a < b$, then $ac < bc$ if $0 < c$

Integral System

Definition 23. An ordered integral domain $\mathcal{A}$ is an integral system if every nonempty subset of $\mathcal{A}^+$ has a least element.
Every element of the integral system is a multiple of 1 and the integral system is isomorphic to $\mathbb{Z}$

Theorem 39. Let $\mathcal{K}$ represent a set of positive integers. Consider the following two conditions

1. $1 \in \mathcal{K}$
2. For any positive integer k if $k \in \mathcal{K}$, then also $k+1 \in \mathcal{K}$

if $\mathcal{K}$ is any set of positive integers satisfying these two conditions, then $\mathcal{K}$ consists of all positive integers

Theorem 40. Principle of Mathematical induction.
Consider the following conditions

1. S_1 is true
2. For any positive integer k if S_k is true, then S_{k+1} is true

if both of the above conditions are satisfied then S_n is true for every positive integer n

S_n reperesents a statement about the positive integer n

Theorem 41. if $m, n \in \mathbb{Z},\ 0 < n, \exists q, r$ such that

$$m = nq + r,\ 0 \leq r < n$$

q, r are the quotient and remainder respectively and they are both unique

0.17 Factoring into primes

Theorem 42. Every ideal of $\mathbb{Z}$ is principal

Theorem 43. The only invertible elements of $\mathbb{Z}$ are 1 and -1

Theorem 44. Any 2 nonzero integers r, s have a greatest common divisor(gcd) t. Also

$$t = kr + ls\ k, l \in \mathbb{Z}$$

Lemma 1 (Composite Number Lemma)**.** if a positive number m is composite, then $m = rs$ where

$$1 < r < m \text{ and } 1 < s < m$$

Lemma 2 (Euclids Lemma)**.** let $m, n \in \mathbb{Z}$ and p be a prime number. if $p|(mn)$then either $p|m$ or $p|n$

Theorem 45 (Factorization into prime)**.** Every $n \in \mathbb{Z}, n > 1$ can be expressed as a product of positive primes.

$$n = p_1 p_2 ... p_r$$

Theorem 46 (Uniqe Factorization)**.** Suppose n can be factorized into positive primes in two ways, namely $n = p_1 p_2 ... p_r = q_1 q_2 ... q_t$. Then $r = t$ and p_i, q_i are the same numbers except for the order in which they appear

0.18 Ring of Polynomials

a(x)

Definition 24. Let $\mathcal{A}$ be a commutative ring with unity and x an arbitrary symbol. Every expression of the form $a_0 + a_1 x + ... + a_n x^n$ is called *a polynomial in x with coefficients in $\mathcal{A}$*

$a_k x^k$ terms of the polynomial, $k \in \{0, 1, ..., n\}$

polynomial degree (deg $a(x)$) the greatest n such that $a_n \neq 0$

compact form of $a(x)$ $a(x) = \sum_{k=0}^{n} a_k x^k$

Theorem 47. Let $\mathcal{A}$ be a commutative ring with unity. Then $\mathcal{A}[x]$ is a commutative ring where $\mathcal{A}[x]$ is the set of polynomials in x with coefficients in $\mathcal{A}$

Theorem 48. if $\mathcal{A}$ is an integral domain, then $\mathcal{A}[x]$ is an integral domain and it is called *a domain of polynomials*

Theorem 49 (Division algorithm for polynomials)**.** If $a(x), b(x)$ are polynomials over a finite field $\mathcal{F}, b(x) \neq 0$ there exists polynomials $q(x), r(x)$ over $\mathcal{F}$ s.t

$$a(x) = b(x)q(x) + r(x)$$

$r(x) = 0$ or deg $r(x) <$ deg $b(x)$

0.19 Factoring Polynomials

Theorem 50. Every ideal of $\mathcal{F}[x]$ is principal

$a(x), b(x)$ are associates if they are constant multiples of each other

$d(x)$ is gcd of $a(x), b(x)$ if $d(x)|a(x),\ , d(x)|b(x)$

for any $u(x) \in \mathcal{F}[x]$ if $u(x)|a(x), u(x)|b(x)$ then $u(x)|d(x)$

Theorem 51. Any 2 polynomials $a(x), b(x) \neq 0,\ a(x), b(x) \in \mathcal{F}[x]$ have a gcd $d(x)$ which can be expressed as

$$d(x) = r(x)a(x) + s(x)b(x)$$

Reducible Polynomial

Definition 25. A polynomial $a(x)$ with positive degree is said to be reducibe over $\mathcal{F}$ if there are polynomials $b(x), c(x) \in \mathcal{F}[x]$ such that $a(x) = b(x)c(x),\ \deg b(x), \deg c(x) > 0$. otherwise $a(x)$ is irreducible over field $\mathcal{F}$

Lemma 3 (Euclids Lemma for Polynomials)**.** let $p(x)$ be irreducible if $p(x)|a(x)b(x)$, then $p(x)|a(x) \text{and} p(x)|b(x)$

Corollary 1. Let $p(x)$ be irreducible. if $p(x)|a_1(x)a_2(x)...a_n(x)$, then $p(x)|a_i(x)$ for one of the factors $a_i(x)$ among $a_1(x), ..., a_n(x)$

Corollary 2. Let $q_1(x), ...q_r(x)$ and $p(x)$ be a monic irreducible polynomials. if $p(x)|q_1(x).....q_r(x)$, then $p(x)$ is equal to one of the factors $q_1(x), ..., q_r(x)$

Theorem 52 (Factorization into irreducible polynomials)**.** Every polynomial $a(x)$ of positive degree in $f(x)$ can be written as a product

$$a(x) = kp_1(x)...p_r(x)$$

where k is a constant in $\mathcal{F}$ and $p_1(x), ..., p_r(x)$ are monic irreducible polynomials of $\mathcal{F}[x]$

Theorem 53 (Unique Factorization)**.** if $a(x)$ can be written in two ways as a product of irreducibles, say $a(x) = kp_1(x)...p_r(x) = lq_1(x)...q_s(x)$ then $k = l,\ r = s$ and each $p_r(x) = q_s(x)$

0.20 Substitution in Polynomials

Let $a(x) = a_0 + a_1x + ... + a_nx^n$. if $c \in \mathcal{F}$ then $a(c) = a_0 + a_1c + ... + a_nc^n$ is an element in $\mathcal{F}$ obtained by substituting c for x in $a(x)$ and $a(x)$ is a polynomial function

if $a(x)$ is a polynomial with coefficients in $\mathcal{F}$ and $c \in \mathcal{F}$ such that $a(c) = 0$, then c is a root of $a(x)$

Theorem 54. *c is a root of $a(x)$ iff $x - c$ is a factor of $a(x)$*

Theorem 55. *$a(x)$ has distinct roots $c_1, c_2, ..., c_m \in \mathcal{F}$, then $(x - c_1), .., (x - c_n)$ is a factor of $a(x)$*