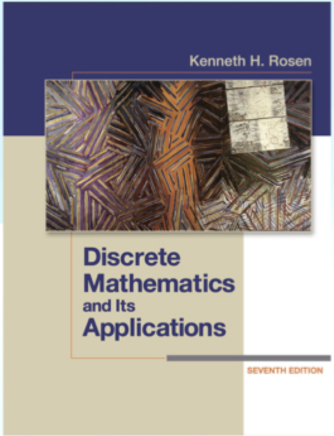
Discrete Mathematics



Lecture 15

Abstract Algebra (continue)

BTEC Alliance with FPT Education

Pearson

Objectives

In this lecture you learn

- the definition, properties, and types of group homomorphisms.
- to understand neutrality and invertibility.
- the definition and properties of semigroups and monoids.
- several notable group applications, with RSA encryption as an illustration.

Table of Contents

1. Group Homomorphisms
2. Neutrality and Invertibility
3. Semigroups and Monoids
4. Applications of Groups

Table of Contents

1. Group Homomorphisms
2. Neutrality and Invertibility
3. Semigroups and Monoids
4. Applications of Groups

Definition

Let G and H be groups with binary operations $*$ and $\cdot$, respectively. A function $f : G \to H$ is a **group homomorphism** if for all elements $a, b \in G$

$$f(a * b) = f(a) \cdot f(b)$$

In simpler terms, applying the group homomorphism to the product of two elements in G is the same as taking the product of their images in H.

Definition

The **set of all homomorphisms** from G to H is denoted by Hom(G, H).

Remark

The set Hom(G, H) is always nonempty since it contains the zero homomorphism $0 : G \to H$ which sends every element of G to 1_H.

Example

Consider two groups G and H where $G = (\mathbb{Z}, +)$ and $H = (\mathbb{Z}_2, +)$, where $\mathbb{Z}_2$ is the group of integers modulo 2. A function $f : \mathbb{Z} \to \mathbb{Z}_2$ is defined by

$$f(x) = \text{the remainder when } x \text{ is divided by } 2.$$

This function is a group homomorphism because it preserves addition

$$f(a+b) = (a+b) \mod 2 = (a \mod 2) + (b \mod 2) = f(a) + f(b).$$

Properties of Group Homomorphism

1. The identity element in the domain group maps to the identity element in the codomain group
$$f(e_G) = e_H.$$

2. The inverse of an element in the domain maps to the inverse of the corresponding element in the codomain
$$f(a^{-1}) = (f(a))^{-1}.$$

Types of Group homomorphism

1. **Monomorphism**: A group homomorphism that is injective (one-to-one), i.e., preserves distinctness.
2. **Epimorphism**: A group homomorphism that is surjective (onto), i.e., reaches every point in the codomain.
3. **Isomorphism**: A group homomorphism that is bijective, i.e., injective and surjective. Its inverse is also a group homomorphism. In this case, the groups G and H are called isomorphic; they differ only in the notation of their elements and are identical for all practical purposes.
4. **Endomorphism**: A group homomorphism, $h : G \to G$; the domain and codomain are the same. Also called an endomorphism of G.
5. **Automorphism**: A group endomorphism that is bijective, and hence an isomorphism. The set of all automorphisms of a group G, with functional composition as operation, itself forms a group, the automorphism group of G.

Definition (Kernel and Image)

We define the **kernel** of h to be the set of elements in G which are mapped to the identity in H, namely,

$$\ker(h) := \{u \in G \colon h(u) = e_H\}\,;$$

and the **image** of h to be

$$\operatorname{im}(h) := h(G) \equiv \{h(u) \colon u \in G\}\,.$$

Table of Contents

1. Group Homomorphisms
2. Neutrality and Invertibility
3. Semigroups and Monoids
4. Applications of Groups

Neutrality

Definition

In a group, the identity element, often denoted as e, is a special element that, when combined with any other element in the group, leaves that element unchanged. Formally, for any element a in the group,

$$a \cdot e = e \cdot a = a$$

The identity element serves as the **neutral element** under the group operation, ensuring that each element has an $opposite$ that does not change it when combined.

Invertibility

Definition

- An element a in a group is said to be invertible if there exists another element, denoted a^{-1}, such that
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$
Here, a^{-1} is called the **inverse** of a.
- Invertibility ensures that every element in the group has a *counterpart* such that their combination results in the identity element.
- In a group, every element must have an inverse, and this inverse is *unique*. If an element has an inverse, it is said to be **invertible**; otherwise, it is **non-invertible**.

Example

Consider the additive group of integers $\mathbb{Z}$ under addition. In this group:

- The neutrality (identity) element is 0 because $a + 0 = 0 + a = a$ for any a in $\mathbb{Z}$.
- Every element a has an inverse, which is $-a$, because $a + (-a) = (-a) + a = 0$.

Remark

In general, the concepts of neutrality and invertibility are fundamental properties of group elements, ensuring the well-behaved structure of groups under their defined operations.

Quiz

Let G be a group, and let e be the identity element in G. Which of the following statements is always true?

a) For any $g \in G$, $g \cdot e = g$.

b) There exists an element $g \in G$ such that $g \cdot e = e \cdot g = e$.

c) If $g \cdot h = e$ for some $g, h \in G$, then $h = g^{-1}$.

d) The equation $g \cdot x = x \cdot g = e$ has a unique solution for x in G.

Table of Contents

1 Group Homomorphisms

2 Neutrality and Invertibility

3 Semigroups and Monoids

4 Applications of Groups

Semigroups

Semigroups and *monoids* are algebraic structures that share similarities with groups but have fewer requirements.

Definition

A **semigroup** is a set equipped with an associative binary operation. Formally, a set S with a binary operation $\cdot : S \times S \to S$ is a semigroup if it satisfies the associative property

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in S$$

Note

Semigroups provide a level of generality in algebraic structures, allowing for the study of algebraic systems where the presence of an identity element or inverses is not assumed.

Example

1. The set of non-negative integers $\mathbb{N}$ with the operation of addition forms a semigroup. Addition is associative, and the sum of two non-negative integers is always a non-negative integer.

2. **Multiplication of Matrices:** The set of all $n \times n$ matrices with real entries, denoted as $M_n(\mathbb{R})$, forms a semigroup under matrix multiplication. Matrix multiplication is associative.

Properties of semigroups

Some key properties of semigroups:

1. **Associativity:** The defining property of a semigroup is associativity, as mentioned above.
2. **Closure:** The operation $\cdot$ must be closed on S, meaning that the result of $a \cdot b$ is an element of S for all a, b in S.
3. **Non-existence of Identity Element:** Unlike a monoid or a group, a semigroup does not necessarily have an identity element. There might not be an element e such that $a \cdot e = e \cdot a = a$ for all a in S.
4. **Non-uniqueness of Inverses:** In general, semigroups do not have inverses. That is, for an element a in S, there might not be an element b in S such that $a \cdot b = b \cdot a$ equals the identity element.
5. **Subsemigroup:** A subset T of a semigroup S is called a subsemigroup if T is itself a semigroup under the same binary operation $\cdot$.

Monoids

Definition

A **monoid** is a semigroup with the additional requirement of having an identity element. Formally, a set M with a binary operation $\cdot : M \times M \to M$ is a monoid if it satisfies the following

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in M$$

There exists an *identity element* e such that $a \cdot e = e \cdot a = a$ for all $a \in M$.

Note

Monoids provide a foundational structure in algebra and appear in various mathematical and computational contexts, including formal language theory, automata theory, and computer science.

Examples

1. The set of natural numbers $\mathbb{N}$, defined as $\{0, 1, 2, \ldots\}$, is a commutative monoid under both addition (with the identity element 0) and multiplication (with the identity element 1). A submonoid of $\mathbb{N}$ under addition is called a **numerical monoid**.
2. The set of positive integers $\mathbb{N} \setminus \{0\}$ is a *commutative monoid* under multiplication, with the identity element 1.
3. Given a set A, the set of subsets of A is a *commutative monoid* under intersection, with the identity element being A itself.
4. Given a set A, the set of subsets of A is a *commutative monoid* under union, with the identity element being the empty set.

Properties of Monoids

Some key properties of Monoids:

1. **Associativity:** Like a semigroup, a monoid is a set equipped with an associative binary operation.
2. **Closure:** The binary operation $\cdot$ must be closed on the set M, meaning that the result of $a \cdot b$ is an element of M for all a, b in M.
3. **Identity Element:** A monoid must have an identity element, denoted as e, such that $a \cdot e = e \cdot a = a$ for all a in M. The identity element is unique within the monoid.
4. **Non-uniqueness of Inverses:** In general, monoids do not require the existence of inverses for every element. That is, for an element a in M, there might not be an element b in M such that $a \cdot b = b \cdot a$ equals the identity element.
5. **Monoid Homomorphism:** A function $f : M \to N$ between two monoids M and N is called a monoid homomorphism if it preserves the binary operation and the identity element $$f(a \cdot b) = f(a) \cdot f(b) \quad \text{and} \quad f(e_M) = e_N.$$

Semigroups and Monoids: Relation to Groups

1. Every group is a monoid with the additional property that every element has an inverse.
2. Every monoid is a semigroup since it satisfies the associative property.
3. Semigroups, in general, do not guarantee the existence of an identity element or inverses.

Quiz

Let S be a semigroup and M be a monoid. Which of the following statements is true?

a) S must have an identity element.

b) M cannot have an inverse for any of its elements.

c) S may or may not have an identity element.

d) M must be commutative.

Table of Contents

1. Group Homomorphisms
2. Neutrality and Invertibility
3. Semigroups and Monoids
4. Applications of Groups

Notable Applications

Groups, a fundamental concept in abstract algebra, find numerous applications in discrete mathematics. Here are some notable applications:

1. **Cryptography**: Groups are used in the development of public-key cryptography systems. The security of these systems relies on the difficulty of certain mathematical problems, often related to group theory, such as the discrete logarithm problem.
2. **Coding Theory**: Groups, particularly finite groups, are employed in coding theory to construct error-correcting codes. The structure of groups helps design codes that can detect and correct errors in data transmission.
3. **Combinatorics**: Groups are involved in the study of permutations and combinations, essential in combinatorics. Symmetric groups, for example, are used to analyze permutations.

Notable Applications (continue)

4. **Graph Theory**: Group theory helps describe and analyze the symmetry properties of graphs. The study of automorphism groups provides insights into the structure and symmetries of graphs.
5. **Number Theory**: Groups, particularly those related to modular arithmetic, are crucial in number theory. The study of cyclic groups is especially relevant in understanding the properties of modular arithmetic.
6. **Algorithms**: Group theory is applied in algorithms for solving polynomial equations. The study of group symmetries can lead to efficient algorithms for solving certain types of equations.
7. **Geometry**: In geometry, groups are used to study transformation groups, which describe symmetries of geometric objects. Lie groups, a type of continuous group, have applications in differential geometry and physics.

Notable Applications (continue)

8. **Game Theory**: Group theory concepts are employed in analyzing the symmetries present in certain types of games, providing insights into optimal strategies.

Public-Key Cryptography: RSA

- **Public-key cryptography** is widely used for securing communications over the internet, including secure email communication, online banking transactions, and the establishment of secure connections (e.g., HTTPS) between web browsers and servers.
- Common public-key cryptography algorithms include RSA (Rivest–Shamir–Adleman), which is widely used for secure data transmission, and ECC (Elliptic Curve Cryptography), which is known for providing strong security with shorter key lengths compared to traditional algorithms.

In this lecture, we are interested in an outstanding application that is **RSA encryption**.

RSA Encryption

To encrypt messages using a particular key (n, e), we first translate a plaintext message M into sequences of integers. To do this, we proceed the following steps:

- First, we translate each plaintext letter into a two-digit number, using the same translation we employed for shift ciphers, with one key difference. That is, we include an initial zero for the letters A through J, so that A is translated into 00, B into $01, \dots$, and J into 09.
- Then, we concatenate these two-digit numbers into strings of digits.
- Next, we divide this string into equally sized blocks of $2N$ digits, where $2N$ is the largest even number such that the number $2525 \dots 25$ with $2N$ digits does not exceed n. (When necessary, we pad the plaintext message with dummy Xs to make the last block the same size as all other blocks.)

RSA Encryption (continue)

After these above steps, we have translated the plaintext message M into a sequence of integers $m_1, m_2, \ldots, m_k$ for some integer k. Encryption proceeds by transforming each block m_i to a ciphertext block c_i. This is done using the function

$$C = M^e \mod n.$$

We leave the encrypted message as blocks of numbers and send these to the intended recipient. Because the RSA cryptosystem encrypts blocks of characters into blocks of characters, it is a block cipher.

Example (RSA Encryption)

Encrypt the message STOP using the RSA cryptosystem with key $(2537, 13)$.

$Note\ that$ in this case, $2537 = 43 \cdot 59$, $p = 43$ and $q = 59$ are primes, and

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1.$$

Solution. To encrypt, we first translate the letters in STOP into their numerical equivalents.

- We group these numbers into blocks of four digits (since $2525 < 2537 < 252525$) to get

$$1819 \quad 1415.$$

- We encrypt each block using the mapping $C = M^{13} \mod 2537$.
- Computations using fast modular multiplication show that

$$2081 = 1819^{13} \mod 2537 \quad \text{and} \quad 2182 = 1415^{13} \mod 2537.$$

- The encrypted message is

$$2081 \quad 2182.$$

Summary

In this lecture, we have discussed

- the definition, properties, and types of group homomorphisms.
- understanding neutrality and invertibility.
- the definition and properties of semigroups and monoids.
- several notable group applications, with RSA encryption as an illustration.

Thank you!