Groups, Rings & Fields

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

09:00, Tuesday 22nd November 2011

Outline

1. Binary and Uniary Operations
   - Unary Operators
   - Binary Operators
2. Groups
   - Definition
3. Rings
   - Definition
4. Fields
   - Definition
5. Examples

Outline

1. Binary and Uniary Operations
   - Unary Operators
   - Binary Operators
2. Groups
   - Definition
3. Rings
   - Definition
4. Fields
   - Definition
5. Examples

Unary operators

An uinary operator is defined on a set A which takes one element from A as input and returns a single element of A.

A uinary operation on a nonempty set A is a map $f : A \to A$ such that

- f is defined for every element in A, and
- f uniquely associates each element in A to some element of A.

Examples of uinary operations include factorial, square root, or NOT.

Binary operators

An binary operator is defined on a set S which takes two elements from S as inputs and returns a single element of S.

A binary operation $f(x, y)$ is an operation that applies to two quantities or expressions x and y.

A binary operation on a nonempty set A is a map $f : A \times A \to A$ such that

- f is defined for every pair of elements in A, and
- f uniquely associates each pair of elements in A to some element of A.

Examples of binary operation on A from $A \times A$ to A include addition $(+)$, subtraction $(-)$, multiplication $(\times)$ and division $(\div)$.

Outline

1 Binary and Uniary Operations
- Unary Operators
- Binary Operators

2 Groups
- Definition

3 Rings
- Definition

4 Fields
- Definition

5 Examples

Definition of a Group

A group G is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property. The operation with respect to which a group is defined is often called the "group operation," and a set is said to be a group "under" this operation.

Definition of a Group

Elements $A, B, C, \ldots$ with binary operation between A and B denoted AB form a group if

- Closure: If A and B are two elements in G, then the product AB is also in G.
- Associativity: The defined multiplication is associative, i.e., for all A, B, C in G, $(AB)C = A(BC)$.
- Identity: There is an identity element I (a.k.a. 1, E, or e) such that $IA = AI = A$ for every element A in G.
- Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element $B = A^{(-1)}$ such that $AA^{(-1)} = A^{(-1)}A = I$.

Outline

1 Binary and Uniary Operations
- Unary Operators
- Binary Operators

2 Groups
- Definition

3 Rings
- Definition

4 Fields
- Definition

5 Examples

Definition of a Ring

A ring is a set S together with two binary operators $+$ and $*$ satisfying the following conditions:

- Additive associativity: For all a, b, c in S, $(a + b) + c = a + (b + c)$,
- Additive commutativity: For all a, b in S, $a + b = b + a$,
- Additive identity: There exists an element 0 in S such that for all a in S, $0 + a = a + 0 = a$,
- Additive inverse: For every a in S there exists $-a$ in S such that $a + (-a) = (-a) + a = 0$,
- Left and right distributivity: For all a, b, c in S, $a * (b + c) = (a * b) + (a * c)$ and $(b + c) * a = (b * a) + (c * a)$,
- Multiplicative associativity: For all a, b, c in S, $(a * b) * c = a * (b * c)$ (a ring satisfying this property is sometimes explicitly termed an associative ring).

Outline

1. Binary and Uniary Operations
   - Unary Operators
   - Binary Operators
2. Groups
   - Definition
3. Rings
   - Definition
4. Fields
   - Definition
5. Examples

Definition of a Field

Rings may also satisfy various optional conditions:

- Multiplicative commutativity: For all a, b in S, $a * b = b * a$ (a ring satisfying this property is termed a commutative ring),
- Multiplicative identity: There exists an element 1 in S such that for all $a! = 0$ in S, $1 * a = a * 1 = a$ (a ring satisfying this property is termed a unit ring, or sometimes a "ring with identity"),
- Multiplicative inverse: For each $a! = 0$ in S, there exists an element $a^{(-1)}$ in S such that for all $a! = 0$ in S, $a * a^{(-1)} = a^{(-1)} * a = 1$, where 1 is the identity element.

A ring satisfying all additional properties above is called a field.

Outline

1. Binary and Uniary Operations
   - Unary Operators
   - Binary Operators
2. Groups
   - Definition
3. Rings
   - Definition
4. Fields
   - Definition
5. Examples

Examples of Groups, Rings and Fields

- A group for which the elements commute (i.e., $AB = BA$ for all elements A and B) is called an Abelian group.
- A cyclic group is a group that can be generated by a single element X.
- The number systems $\mathbb{Z}$ (integers), $\mathbb{Z}_n$ (integers mod(n)), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) are all examples of rings.
- The number systems $\mathbb{Q}$, $\mathbb{R}$ are examples of fields, as is $\mathbb{Z}_n$ if n is prime.

So what is a group?

- The integers under addition form a group. The identity element of the group is 0, and the additive inverse is just the usual negative. In fact, the group of integers is an Abelian group: addition is commutative for integers.
- The rational numbers under addition form a group. The identity element of the group is 0, and the additive inverse is just the usual negative. This group is Abelian, and the integers form a subgroup.
- The real numbers also form a group under addition. The rational numbers form a subgroup of the group of real numbers, and the integers form a smaller subgroup.
- The nonzero rational numbers under multiplication form a group. The identity element for this group is 1. This group is also Abelian.

Groups from number theory

The group of integers modulo 2, termed the cyclic group of order two, has exactly two elements, one corresponding to the collection of even numbers and one corresponding to the collection of odd numbers. These are typically represented as 0 and 1. The group operation is then given by:

$$0 + 0 = 0, \qquad 0 + 1 = 1, \qquad 1 + 0 = 1, \qquad 1 + 1 = 0$$

Similarly, modulo 4, there are four equivalence classes of numbers: the multiples of 4, the numbers that leave a remainder of 1 modulo 4, the numbers that leave a remainder of 2 modulo 4, and the numbers that leave a remainder of 3 modulo 4.

Groups from functions

A permutation of a set S is a bijective map from S to itself. The symmetric group on a set is the set of all permutations on it, where:

- The product of two permutations is composition. If f and g are permutations, their product is the map $x \mapsto f(g(x))$
- The identity map is the identity element
- The inverse of a permutation is its inverse as a function

The symmetric groups are important examples of non-Abelian groups: in fact the symmetric group on a set of size at least three, is always non-Abelian. Moreover, it is surprisingly true that every finite group occurs as a subgroup of the symmetric group.