KTH Computer Science
and Communication

A summary of Groups and Rings SF2729

JIM HOLMSTRÖM

Abstract

This paper contains a brief summary of the course Groups and Rings which is given at KTH in Stockholm. The basis for this is the book: A First Course In Abstract Algebra by John B. Fraleigh.

Contents

Chapter 1

Definitions

1.1 Structures

1.1.1 Set

1.1.2 Binary algebraic structure

Denoted by $\langle \mathcal{S}, * \rangle$ is a set $\mathcal{S}$ with a binary operator $*$ on $\mathcal{S}$.

Identity element

An element e is an identity element in the structure $\langle \mathcal{S}, * \rangle$

$$e * x = x * e = x \quad \forall x \in \mathcal{S} \tag{1.1}$$

Theorem 1. *The identity element e is unique in the binary structure ... p32*

Proof. p32 □

Theorem 2. *If $\phi : \mathcal{S} \to \mathcal{S}'$ is an isomorphism of $\langle \mathcal{S}, * \rangle$ with $\langle \mathcal{S}', *' \rangle$ then $\phi(e)$ will be the identity in $\langle \mathcal{S}', *' \rangle$.*

Proof. Need to show

$$\phi(e) *' x' = x' *' \phi(e) = x' \quad \forall x' \in \mathcal{S}' \tag{1.2}$$

ϕ is onto(3.1.2).

$$e * x = x * e = x \Rightarrow \phi(e * x) = \phi(x * e) = \phi(x) \tag{1.3}$$

We chose $x : \phi(x) = x'$ using the homomorphism property we can rewrite it to

$$\phi(e) *' \phi(x) = \phi(x) *' \phi(e) = \phi(x) \tag{1.4}$$

□

1.1.3 Group

A group is a binary algebraic structure (1.1.2) with the following properties:
G1
G2 ...

1.1.4 Ring

1.1.5 Field

1.2 Substructures

1.2.1 Subgroup

1.2.2 Subring

1.2.3 Ideal

1.3 Relations between structures

1.3.1 Homomorphism

A map that preserves the algebraic structure between $\langle \mathcal{S}, * \rangle, \langle \mathcal{S}', *' \rangle$ by satisfying:

$$\phi(x * y) = \phi(x) *' \phi(y) \quad \forall x, y \in \mathcal{S} \tag{1.5}$$

1.3.2 Isomorphism

A isomorphism is a homomorphism (1.3.1) with the additional property of ϕ being a one-to-one map between $\mathcal{S}$ and $\mathcal{S}'$.

$\exists \phi$ isomorphism between $\langle \mathcal{S}, * \rangle, \langle \mathcal{S}', *' \rangle$ we say that those are isomorphic. Isomorphic is denoted by $\mathcal{S} \cong \mathcal{S}'$ omitting the $\langle \cdot, * \rangle$ since it almost always clear which operator is considered.

Showing that binary structures are isomorphic

Step 1 Define ϕ, that is describe $\phi(a) \forall a \in \mathcal{S}$

Step 2 Show that ϕ is one-to-one. (3.1.1)

Step 3 Show that ϕ is onto. (3.1.2)

Step 4 Show that ϕ is a homomorphism. (1.3.1)

1.3.3 Group action

1.4 Bijective functions

1.4.1 Permutation

Chapter 2

Useful theorems

2.1 LOREM IPSUM

2.1.1 Lagrange's Theorem

2.1.2 Cauchy's Theorem

Chapter 3

Misc. Later put into some of the above chapters

3.0.3 Equivalence relation $\mathfrak{R}$

$$\mathfrak{R} \text{ is an equivalence relation on a set } \mathcal{S}$$
$$\Leftrightarrow$$

$$\begin{cases} x\mathfrak{R}x \\ x\mathfrak{R}y \Rightarrow y\mathfrak{R}x \\ x\mathfrak{R}y \wedge y\mathfrak{R}z \Rightarrow x\mathfrak{R}z \end{cases} \quad , \forall x, y, z \in \mathcal{S} \tag{3.1}$$

The equivalence relation is often denoted with a $\sim$

3.0.4 Binary operations $*$

$$\begin{aligned} * : \mathcal{S} \times \mathcal{S} &\to \mathcal{S} \\ (x, y) &\mapsto *((x, y)) = x * y \end{aligned} \tag{3.2}$$

The binary function $*((x, y))$ is denoted by $x * y$.

$\mathcal{H}$ closed under $*$

$\mathcal{H} \subseteq \mathcal{S}$ closed under $*$:

$$a, b \in \mathcal{H} \Rightarrow (a * b) \in \mathcal{H} \tag{3.3}$$

Note that in the case $\mathcal{H} = \mathcal{S}$ will always be closed from the definition of the operation.

Commutative

Commutativity is the operation property:

$$a * b = b * a \quad \forall a, b \in \mathcal{S} \tag{3.4}$$

Associative

Associativity is the operation property:

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in \mathcal{S} \tag{3.5}$$

which basically means that the order of operation is invariant and we might as well denote both expressions in (3.5) unambiguously without specifying the operation order with $a * b * c$.

3.1 these are grouped somehow

3.1.1 One-to-one

A one-to-one map ϕ means that each element x has a corresponding $\phi(x)$.

Show one-to-one by showing:

$$\phi(x) = \phi(y) \in \mathcal{S}' \Rightarrow x = y \in \mathcal{S} \tag{3.6}$$

That is given the first statement in (3.6) deduce the next statement.

3.1.2 Onto

ϕ is onto $\mathcal{S}'$ if ... Show onto by showing:

$$\forall x' \exists x : \phi(x) = x' \quad x \in \mathcal{S}, x' \in \mathcal{S}' \tag{3.7}$$

That is assume x' is given show that $\exists$...