Abstract algebra and coding

Rafał Włodarczyk

INA 2, 2024

Contents

1 Definitions

1.1 Group

A group is a set G along with an operation $\cdot$ satisfying the following axioms:

1. **Operation is defined**: $\forall a, b \in G : a \cdot b \in G$
2. **Operation is associative**: $\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3. **Identity element exists**: $\exists e \in G : \forall a \in G : a \cdot e = e \cdot a = a$

4. **Inverse element exists**: $\forall a \in G : \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

1.2 Subgroup

A subset H of a group G is a subgroup if:

1. H is closed under the operation: $\forall a, b \in H : a \cdot b \in H$

2. H is closed under inverses: $\forall a \in H : a^{-1} \in H$

3. H contains the identity element: $e \in H$

4. H is closed under associativity: $\forall a, b \in H : a \cdot b \in H$

It suffices to check closure under operation and inverses for H.

1.3 Normal Subgroup

A subgroup H of a group G is normal in G if:

1. H is a subgroup of G:
   - H is closed under the operation: $\forall a, b \in H : a \cdot b \in H$
   - H has an inverse element: $\forall a \in H : a^{-1} \in H$

2. H is closed under conjugation: $\forall a \in G : aHa^{-1} = H$

1.4 Group Homomorphism

A group homomorphism is a function $f : G \to H$ satisfying:

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

1.5 Kernel of a Homomorphism

The kernel of a homomorphism f is the set of elements in G mapped to the identity element in H:

$$\ker f = \{a \in G : f(a) = e_H\}$$

1.6 Image of a Homomorphism

The image of a homomorphism is the set of elements in H obtained by applying f to elements in G:

$$\mathrm{Im} f = \{f(a) \in H : a \in G\}$$

1.7 Order of an Element in a Group

The order of an element a in a group G is defined as:

$$\mathrm{ord}(a) = \min\{n \in \mathbb{N} : a^n = e\}$$

If no such n exists, a has infinite order.

1.8 Generator of a Group

An element a in a group G is a generator if:

$$\forall b \in G : \exists n \in \mathbb{Z} : b = a^n$$

1.9 Coset of a Group

The coset of a subgroup H in a group G is defined as:

- Left coset: $aH = \{a \cdot h : h \in H\}$
- Right coset: $Ha = \{h \cdot a : h \in H\}$
- Double coset: $aH = Ha$

1.10 Cyclic Group

A group G is cyclic if there exists an element $a \in G$ such that:

$$G = \{a^n : n \in \mathbb{Z}\}$$

Thus, G is generated by one element a.

1.11 Dihedral Group

The dihedral group D_n is the group of symmetries of a regular n-gon.

1.12 Quotient Group

The quotient group G/H of a group G by a normal subgroup H is the set of cosets of H in G with the operation:

$$(aH) \cdot (bH) = (a \cdot b)H$$

1.13 Ring

A ring R is a set with two operations $+$ and $\cdot$ satisfying:

1. $(R, +)$ is an abelian group
2. $\cdot$ is associative: $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Distributivity of multiplication over addition:

$$\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

1.14 Invertible Element in a Ring

An element a in a ring R is invertible if there exists an element $b \in R$ such that:

$$a \cdot b = b \cdot a = 1$$

The set of invertible elements is denoted as $R^* = \{a \in R : a \text{ is invertible}\}$

1.15 Subring

A subring of a ring R is a subset $S \subseteq R$ with operations $+$ and $\cdot$ such that:

1. S is closed under addition: $\forall a, b \in S : a + b \in S$
2. S is closed under multiplication: $\forall a, b \in S : a \cdot b \in S$

1.16 Ring Homomorphism

A ring homomorphism is a function $f : R \to S$ satisfying:

1. f is a group homomorphism: $f(a + b) = f(a) + f(b)$
2. f is a ring homomorphism: $f(a \cdot b) = f(a) \cdot f(b)$

1.17 Ideal

An ideal of a ring R is a subset $I \subseteq R$ satisfying:

1. $(I, +)$ is a subgroup of the abelian group $(R, +)$
2. I is closed under multiplication: $\forall a, b \in I : a \cdot b \in I$
3. I is closed under addition: $\forall a, b \in I : a + b \in I$
4. I is closed under multiplication by ring elements: $\forall a \in I, r \in R : a \cdot r \in I$ and $r \cdot a \in I$

1.18 Principal Ideal

A principal ideal generated by an element $a \in R$ is the set:

$$\langle a \rangle = \{a \cdot r : r \in R\}$$

1.19 Quotient Ring

The quotient ring R/I of a ring R by an ideal I is the set of cosets of I in R with operations:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

2 Theorems

2.1 Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G:

$$|G| = |H| \cdot [G : H]$$

Or equivalently:

$$|H| \mid |G|$$

2.2 Chinese Remainder Theorem

If $m_1, m_2, \ldots, m_n$ are pairwise coprime integers, then the system of congruences:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

has exactly one solution modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

2.3 Euler's Theorem

For any integer a coprime to n, it holds that:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$