

Learning objectives after Learning Module 10.1 (10.1)

After completing this module, you should be able to:

- 1. Explain the concept of a group and its properties.
- 2. Explain the concept of a subgroup and its properties.
- 3. Explain the concept of a coset and its properties.
- 4. Explain the concept of a normal subgroup and its properties.
- 5. Explain the concept of a quotient group and its properties.
- 6. Explain the concept of a homomorphism and its properties.
- 7. Explain the concept of an isomorphism and its properties.
- 8. Explain the concept of an automorphism and its properties.
- 9. Explain the concept of a permutation and its properties.
- 10. Explain the concept of a symmetric group and its properties.
- 11. Explain the concept of an alternating group and its properties.
- 12. Explain the concept of a simple group and its properties.
- 13. Explain the concept of a solvable group and its properties.
- 14. Explain the concept of a nilpotent group and its properties.
- 15. Explain the concept of a p-group and its properties.
- 16. Explain the concept of a Sylow subgroup and its properties.
- 17. Explain the concept of a Frobenius group and its properties.
- 18. Explain the concept of a Galois group and its properties.
- 19. Explain the concept of a field extension and its properties.
- 20. Explain the concept of a Galois field and its properties.

10.1 Groups

10.1.1 Definition 10.1.1 A group is a set G with a binary operation \cdot satisfying the following properties:

- (G1) $a \cdot b \in G$ for all $a, b \in G$.
- (G2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.
- (G3) There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
- (G4) For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

10.1.2 Definition 10.1.2 A subgroup of a group G is a subset H of G such that H is a group under the same operation as G .

10.1.3 Definition 10.1.3 A coset of a subgroup H of a group G is a subset aH of G such that $aH = \{a \cdot h \mid h \in H\}$.

10.1.4 Definition 10.1.4 A normal subgroup of a group G is a subgroup N of G such that $gN = Ng$ for all $g \in G$.

10.1.5 Definition 10.1.5 A quotient group of a group G by a normal subgroup N is the set of cosets aN of N in G with the operation $(aN) \cdot (bN) = (a \cdot b)N$.

10.1.6 Definition 10.1.6 A homomorphism from a group G to a group H is a function $\phi: G \rightarrow H$ such that $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G$.

10.1.7 Definition 10.1.7 An isomorphism from a group G to a group H is a homomorphism $\phi: G \rightarrow H$ such that ϕ is bijective.

10.1.8 Definition 10.1.8 An automorphism of a group G is an isomorphism from G to G .

10.1.9 Definition 10.1.9 A permutation of a set S is a bijection from S to S .

10.1.10 Definition 10.1.10 A symmetric group on a set S is the group of all permutations of S .

10.1.11 Definition 10.1.11 An alternating group on a set S is the subgroup of the symmetric group on S consisting of all even permutations.

10.1.12 Definition 10.1.12 A simple group is a group that has no non-trivial normal subgroups.

10.1.13 Definition 10.1.13 A solvable group is a group that has a subnormal series with abelian factors.

10.1.14 Definition 10.1.14 A nilpotent group is a group that has a central series.

10.1.15 Definition 10.1.15 A p-group is a group whose order is a power of a prime p .

10.1.16 Definition 10.1.16 A Sylow subgroup of a group G is a maximal p-subgroup of G .

10.1.17 Definition 10.1.17 A Frobenius group is a group G that has a normal subgroup N and a subgroup H such that $G = NH$ and $H \cap N = \{e\}$.

10.1.18 Definition 10.1.18 A Galois group of a field extension is the group of all automorphisms of the extension.

10.1.19 Definition 10.1.19 A Galois field is a finite field.