

Groups, in general

3.1.3. Definition. A *group* (G, \cdot) is a nonempty set G together with a binary operation \cdot on G such that the following conditions hold:

- (i) *Closure:* For all $a, b \in G$ the element $a \cdot b$ is a uniquely defined element of G .
- (ii) *Associativity:* For all $a, b, c \in G$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- (iii) *Identity:* There exists an *identity element* $e \in G$ such that $e \cdot a = a$ and $a \cdot e = a$ for all $a \in G$.
- (iv) *Inverses:* For each $a \in G$ there exists an *inverse element* $a^{-1} \in G$ such that $a \cdot a^{-1} = e$ and $a^{-1} \cdot a = e$.

3.1.6. Proposition. (Cancellation Property for Groups) Let G be a group, and let $a, b, c \in G$.

- (a) If $ab = ac$, then $b = c$.
- (b) If $ac = bc$, then $a = b$.

3.1.8. Definition. A group G is said to be a *finite group* if the set G has a finite number of elements. In this case, the number of elements is called the *order* of G , denoted by $|G|$.

A group G is said to be *abelian* if $a \cdot b = b \cdot a$ for all $a, b \in G$.

3.2.7. Definition. Let a be an element of the group G . If there exists a positive integer n such that $a^n = e$, then a is said to have *finite order*, and the smallest such positive integer is called the *order* of a , denoted by $o(a)$. If there does not exist a positive integer n such that $a^n = e$, then a is said to have *infinite order*.

3.2.1. Definition. Let G be a group, and let H be a subset of G . Then H is called a *subgroup* of G if H is itself a group, under the operation induced by G .

3.2.2. Proposition. Let G be a group with identity element e , and let H be a subset of G . Then H is a subgroup of G if and only if the following conditions hold:

- (i) $ab \in H$ for all $a, b \in H$; (ii) $e \in H$; (iii) $a^{-1} \in H$ for all $a \in H$.

3.2.4. Corollary. Let G be a group, and let H be a finite, nonempty subset of G . Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

3.2.10. Theorem. (Lagrange) If H is a subgroup of the finite group G , then the order of H is a divisor of the order of G .

3.2.11. Corollary. Let G be a finite group of order n .

- (a) For any $a \in G$, $o(a)$ is a divisor of n .
- (b) For any $a \in G$, $a^n = e$.

3.2.12. Corollary. Any group of prime order is cyclic.

3.4.1. Definition. Let G_1 and G_2 be groups, and let $\phi : G_1 \rightarrow G_2$ be a function. Then ϕ is said to be a *group isomorphism* if ϕ is one-to-one and onto and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$. In this case, G_1 is said to be *isomorphic* to G_2 , and this is denoted by $G_1 \cong G_2$.

3.4.3. Proposition. Let $\phi : G_1 \rightarrow G_2$ be an isomorphism of groups.

- (a) If a has order n in G_1 , then $\phi(a)$ has order n in G_2 .
- (b) If G_1 is abelian, then so is G_2 .
- (c) If G_1 is cyclic, then so is G_2 .

Cyclic groups

3.2.5 Definition. The group G is called a *cyclic group* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbf{Z}\}$. In this case a is called a *generator* of G . More generally, for any group G and any element $a \in G$, the set $\{a^n \mid n \in \mathbf{Z}\}$ is called the *cyclic subgroup generated by a* , and is denoted by

3.2.6 Proposition. Let G be a group, and let $a \in G$.

- (a) $\langle a \rangle$ is a subgroup of G .
- (b) If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.

3.2.8. Proposition. Let a be an element of the group G .

(a) If a has infinite order, then $a^k \neq a^m$ for all integers $k \neq m$.

(b) If a has finite order and $k \in \mathbf{Z}$, then $a^k = e$ if and only if $o(a) | k$.

(c) If a has finite order $o(a) = n$, then for all integers k, m , we have $a^k = a^m$ if and only if $k \equiv m \pmod{n}$.

Furthermore, $|\langle a \rangle| = o(a)$.

Corollaries to Lagrange's Theorem (restated):

(a) For any $a \in G$, $o(a)$ is a divisor of $|G|$.

(b) For any $a \in G$, $a^{|G|} = e$.

(c) Any group of prime order is cyclic.

3.5.1. Theorem. Every subgroup of a cyclic group is cyclic.

3.5.2 Theorem. Let G be a cyclic group.

(a) If G is infinite, then $G \cong \mathbf{Z}$.

(b) If $|G| = n$, then $G \cong \mathbf{Z}_n$.

3.5.3. Proposition. Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$.

(a) If $m \in \mathbf{Z}$, then $\langle a^m \rangle = \langle a^d \rangle$, where $d = \gcd(m, n)$, and a^m has order n/d .

(b) The element a^k generates G if and only if $\gcd(k, n) = 1$.

(c) The subgroups of G are in one-to-one correspondence with the positive divisors of n .

Permutation groups

3.1.4. Definition. The set of all permutations of a set S is denoted by $\text{Sym}(S)$. The set of all permutations of the set $\{1, 2, \dots, n\}$ is denoted by S_n .

3.1.5. Proposition. If S is any nonempty set, then $\text{Sym}(S)$ is a group under the operation of composition of functions.

2.3.5. Theorem. Every permutation in S_n can be written as a product of disjoint cycles. The cycles that appear in the product are unique.

2.3.8 Proposition. Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its cycles.

Other examples

Example 3.1.4. (Group of Units Modulo n) Let n be a positive integer. The set \mathbf{Z}_n^\times of units modulo n is an abelian group under multiplication of congruence classes. The group \mathbf{Z}_n^\times is finite and $|\mathbf{Z}_n^\times| = \varphi(n)$.

3.3.6. Definition. Let F be a field. The set of all invertible $n \times n$ matrices with entries in F is called the *general linear group of degree n over F* , and is denoted by $GL_n(F)$.

3.3.7. Proposition. Let F be a field. Then $GL_n(F)$ is a group under matrix multiplication.

3.3.3. Definition. Let G_1 and G_2 be groups. The set of all ordered pairs (a_1, a_2) such that $a_1 \in G_1$ and $a_2 \in G_2$ is called the *direct product* of G_1 and G_2 , denoted by $G_1 \times G_2$.

3.3.4. Proposition. Let G_1 and G_2 be groups. The direct product $G_1 \times G_2$ is a group under the multiplication $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$. If $a_1 \in G_1$ and $a_2 \in G_2$ have orders n and m , respectively, then in $G_1 \times G_2$ the element (a_1, a_2) has order $\text{lcm}[n, m]$.

3.4.5. Proposition. If m, n are positive integers such that $\gcd(m, n) = 1$, then $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$.