

### Groups, in general

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

*Associativity:* For all  $a, b, c \in G$ , we have  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;

*Identity:* There exists an *identity element*  $e \in G$  such that  $e \cdot a = a$  and  $a \cdot e = a$  for all  $a \in G$ ;

*Inverses:* For each  $a \in G$  there exists an *inverse element*  $a^{-1} \in G$  such that  $a \cdot a^{-1} = e$  and  $a^{-1} \cdot a = e$ .

**3.1.7. 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  $a = b$ .

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

**3.1.10. 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  $|G|$ . If  $G$  is not finite, it is said to be an *infinite group*.

**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  $G$  is a finite group, then the order of any subgroup  $H \subseteq G$  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  $\phi$  is said to be a *group isomorphism* if  $\phi$  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.** (a) 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  $G$ .

**3.2.5 Definition.** (b) 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  $\langle a \rangle$ .

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

**3.5.4. Proposition.** Let  $G = \langle a \rangle$  be a finite group of order  $n$ .

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

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

That is, if  $H$  is any subgroup of  $G$ , then  $H = \langle a^k \rangle$  for some divisor  $k$  of  $n$ , and if  $m$  and  $k$  are divisors of  $n$ , then  $\langle a^m \rangle \subseteq \langle a^k \rangle$  if and only if  $k | m$ , so  $\langle a^m \rangle = \langle a^k \rangle$  if and only if  $k = m$ .

## 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  $\sigma$  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  $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ .

## TOP TEN GROUPS

1.  $\mathbf{Z}$  (under addition) p 97 Example 3.1.2
2.  $\mathbf{C}$  (under addition) p 97 Example 3.1.2
3.  $\mathbf{C}^\times$  (under multiplication) p 93 Example 3.1.1
4.  $\mathbf{Z}_n$  (under addition) p 98 Example 3.1.3
5.  $\mathbf{Z}^\times$  (under multiplication) p 99 Example 3.1.4
6.  $S_n$  (under multiplication of permutations) pp 93–95 Proposition 3.1.6
7.  $\text{GL}_n(F)$  (under matrix multiplication) p 100 Prop. 3.1.12 and pp 120–121 Prop. 3.3.7
8.  $G_1 \times G_2$  (under componentwise operations), for example, the Klein 4-group  $\mathbf{Z}_2 \times \mathbf{Z}_2$   
p 118 Prop 3.3.4 and pp 119–120
9.  $\text{Sym}(S)$  (under composition of functions) p 93 Prop 3.1.6
10. Any vector space (under vector addition)

## TOP TEN SUBGROUPS

1.  $m\mathbf{Z} \subseteq \mathbf{Z}$  p103 Example 3.2.1
- 2–4.  $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$  p103 Example 3.2.1
- 5–6.  $\mathbf{Q}^\times \subseteq \mathbf{R}^\times \subseteq \mathbf{C}^\times$  p103 Example 3.2.1
7.  $\langle a \rangle \subseteq G$  pp 136–137 Prop 3.5.3 and Prop 3.5.2
8.  $m\mathbf{Z}_n \subseteq \mathbf{Z}_n$  pp 137–138
9.  $H_1 \times H_2 \subseteq G_1 \times G_2$  p 133 Exercise 8
10. Any subspace of a vector space.

## TOP TEN ISOMORPHISMS

1.  $G \cong \mathbf{Z}_n$  if  $G$  is cyclic and  $|G| = n$  p 135 Theorem 3.5.2 (b)
2.  $G \cong \mathbf{Z}$  if  $G$  is cyclic and  $|G| = \infty$  p 135 Theorem 3.5.2 (a)
3. For any  $a \in G$ ,  $\phi_a : G \rightarrow G$  defined by  $\phi_a(x) = axa^{-1}$  is an isomorphism p 133 Exercise 15
4.  $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$  if  $\text{gcd}(m, n) = 1$  p 132 Prop 3.4.5
5.  $\mathbf{R}^+ \cong \mathbf{R}$  via  $\ln x : \mathbf{R}^+ \rightarrow \mathbf{R}$  and  $e^x : \mathbf{R} \rightarrow \mathbf{R}^+$  p 129 Example 3.4.2
6. If  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ , then  $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}}$  . p 138 Prop 3.5.5
7. If  $G$  is abelian, then  $\phi : G \rightarrow G$  defined by  $\phi(x) = x^{-1}$  is an isomorphism p 133 Exercise 16
8.  $\phi : \mathbf{C}^\times \rightarrow \mathbf{C}^\times$  defined by  $\phi(a + bi) = a - bi$  is an isomorphism p 133 Exercise 18
9.  $\mathbf{C}^\times$  is isomorphic to the subgroup  $\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a^2 + b^2 \neq 0 \right\}$  of  $\text{GL}_2(\mathbf{R})$  p 134 Exercise 19
10. If  $p$  is prime, then  $\mathbf{Z}_p^\times \cong \mathbf{Z}_{p-1}$  We can't prove this yet (see p 298 Theorem 6.5.10)