3 ORDER OF AN ELEMENT

DEFINITION 3.1: (Order of an element) Let \( G \) be a multiplicatively-written group with identity element \( e \), and let \( x \in G \). Then one of the two following situations must apply to \( x \).

(1) There is no positive integer \( n \) such that \( x^n = e \); when this happens we say that \( x \) has, or is of, infinite order.

(2) There is a positive integer \( n \) such that \( x^n = e \); when this happens we say that \( x \) has finite order, and if \( n \) is the smallest positive integer such that \( x^n = e \) then we say that \( x \) has order \( n \) and write \( \text{ord}(x) = n \).

REMARKS 3.2:

(a) If you are asked to show that an element \( x \) of a group \( G \) has order \( n \) for a given positive integer \( n \), it is not enough to show simply that \( x^n = e \); you must also show that \( n \) is the smallest positive integer with \( x^n = e \). It is a COMMON ERROR to show that \( x^n = e \) and to leave it at that.

(b) Every group has at least one element of finite order, because the identity element has order 1. In fact an element has order 1 if and only if it is the identity element.

EXAMPLE 3.3: As in 1.5 let \( G \) be the multiplicative group which consists of the four complex numbers 1, \( i \), \( -1 \), \(-i\) where \( i^2 = -1 \). To find the order of \( i \) as an element of \( G \) we note that \( i^2 = -1 \neq 1 \), \( i^3 = -i \neq 1 \), and \( i^4 = 1 \). Therefore \( i \) has order 4, because when we go through the powers of \( i \) we have to go to \( i^4 \) before we get the answer 1. Similarly \(-i \) has order 4. But 
\((-1)^2 = 1 \) with \(-1 \neq 1 \), so that \(-1 \) has order 2.

EXAMPLE 3.4: As in 1.6 let \( G \) be the multiplicative group of non-zero rational numbers, and let \( x \in G \). Suppose that \( x^n = 1 \) for some positive integer \( n \). Because \( x \) is a non-zero rational number we can only have either \( x = 1 \) or \( x = -1 \). So the only two elements of \( G \) of finite order are 1 and \(-1 \), where \( \text{ord}(1) = 1 \) and \( \text{ord}(-1) = 2 \).

EXAMPLE 3.5: As in 1.13 let \( G \) be the multiplicative group of non-zero elements of \( \mathbb{Z}/5\mathbb{Z} \), i.e. \( G = U_5 \) in the notation of 1.33. Working in \( \mathbb{Z}/5\mathbb{Z} \) we have \( 2^2 = 4 \), \( 2^3 = 8 = 3 \), \( 2^4 = 2.2^3 = 2.3 = 6 = 1 \) so that \( \text{ord}(2) = 4 \); \( 3^2 = 9 = 4 \), \( 3^3 = 3.4 = 12 = 2 \), \( 3^4 = 3.2 = 6 = 1 \) so that \( \text{ord}(3) = 4 \); \( 4^2 = (-1)^2 = 1 \) so that \( \text{ord}(4) = 2 \).

EXAMPLE 3.6: As in 1.21 let \( G = D_3 \) with the elements of \( G \) denoted by \( e, a, a^2, b, ab, a^2b \) where \( e \) is the identity element, \( a^3 = e = b^2 \), and \( ab = ba^{-1} \). Then \( a \) and \( a^2 \) have order 3. Also \( b, ab, a^2b \) (geometrically, these are the reflections) have order 2.

EXAMPLE 3.7: As in 1.22 let \( G = D_4 \) with the elements of \( G \) denoted by \( e, a, a^2, a^3, b, ab, a^2b, a^3b \) where \( e \) is the identity element, \( a^4 = e = b^2 \), and \( ab = ba^{-1} \). Then \( a \) and \( a^3 \) have order 4; \( a^2 \) has order 2; the four reflections \( b, ab, a^2b, a^3b \) all have order 2.

EXAMPLE 3.8: The three non-identity elements of the Klein 4-group all have order 2.
EXAMPLE 3.9: Set \( G = (\mathbb{Z}, +) \) and let \( x \in G \). Because we are using additive notation, the element \( x \) has finite order if and only if \( nx = 0 \) for some positive integer \( n \). Clearly in this example \( x \) has finite order if and only if \( x = 0 \).

EXAMPLE 3.10: Set \( G = (\mathbb{Z}/4\mathbb{Z}, +) \). We will use 0, 1, 2, 3 to denote the elements of \( G \). Working in \( \mathbb{Z}/4\mathbb{Z} \) we have 1.1 = 1 ≠ 0, 2.1 = 2 ≠ 0, 3.1 = 3 ≠ 0, 4.1 = 4 = 0 so that \( \text{ord}(1) = 4 \). Also 2.2 = 4 = 0 so that \( \text{ord}(2) = 2 \). We have 2.3 = 6 = 2 ≠ 0, 3.3 = 9 = 1 ≠ 0, 4.3 = 12 = 0 so that \( \text{ord}(3) = 4 \).

PROPOSITION 3.11: Let \( G \) be a multiplicatively-written group and let \( x \) be an element of \( G \) of infinite order. Then the powers of \( x \) are distinct, i.e. if \( i \) and \( j \) are integers such that \( I \neq j \) then \( x^I \neq x^j \).

PROOF: Suppose that \( i \) and \( j \) are integers with \( x^i = x^j \). Without loss of generality we can suppose that \( i \geq j \). Multiplying both sides of the equation \( x^i = x^j \) by \( x^{-j} \) gives \( x^{i-j} = 1 \) where 1 is the identity element of \( G \) and \( i - j \) is a non-negative integer. But \( x \) has infinite order, so that \( i - j \) can not be positive. Therefore \( i - j = 0 \), i.e. \( i = j \).

COROLLARY 3.12: Let \( G \) be a finite group. Then every element of \( G \) has finite order.

PROOF: Let \( x \in G \) and suppose that the operation in \( G \) is multiplication. The powers of \( x \) are elements of the finite set \( G \), so that the powers of \( x \) can not all be distinct. Therefore \( x \) has finite order, by 3.11.

We shall show in Section 7 that if \( G \) is a finite group and \( x \in G \), then the order of \( x \) divides the order (i.e. number of elements of) \( G \).

PROPOSITION 3.13: Let \( G \) be a multiplicatively-written group with identity element 1 and let \( x \) be an element of \( G \) of finite order \( n \).

1. Let \( i \in \mathbb{Z} \). Then \( x^i = 1 \) if and only if \( n \) divides \( i \).

2. Let \( i, j \in \mathbb{Z} \). Then \( x^i = x^j \) if and only if \( n \) divides \( i - j \).

3. The inverse of \( x \) is \( x^{n-1} \).

4. The distinct powers of \( x \) are 1, \( x \), \( x^2 \), ..., \( x^{n-1} \).

PROOF:

1. Let \( i \in \mathbb{Z} \). Suppose firstly that \( n \) divides \( i \), so that \( i = nk \) for some \( k \in \mathbb{Z} \). Then \( x^i = x^{nk} = (x^n)^k = 1^k = 1 \) because \( x^n = 1 \). Conversely suppose that \( x^i = 1 \). By the division algorithm we have \( i = nq + r \) for some \( q, r \in \mathbb{Z} \) with \( 0 \leq r < n \). We have \( x^n = 1 \) and \( x^1 = 1 \), so that \( 1 = x^i = x^{nq+r} = (x^n)^q x^r = 1^q x^r = x^r \). Thus \( n \) is the smallest positive integer with \( x^n = 1 \), and we have \( x^r = 1 \) with \( 0 \leq r < n \). Therefore we must have \( r = 0 \), i.e. \( i = nq \), so that \( n \) divides \( i \).

2. Let \( i, j \in \mathbb{Z} \). Then \( x^i = x^j \) if and only if \( i-j = 1 \). Therefore it follows from (1) that \( x^i = x^j \) if and only if \( n \) divides \( i - j \).

3. We have \( x \cdot x^{n-1} = x^n = 1 = x^{n-1} \cdot x \), so that \( x^{n-1} \) is the inverse of \( x \).
(4) Let $y$ be a power of $x$, i.e. $y = x^i$ for some $i \in \mathbb{Z}$. We have $i = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Thus $y = x^i = x^nq^r = (x^n)^q x^r$, so that $y$ is one of the elements $1, x, x^2, \ldots, x^{n-1}$. We must also show that the elements 1, $x, x^2, \ldots, x^{n-1}$ are distinct. Suppose that $x^a = x^b$ for some $a, b \in \mathbb{Z}$ with $0 \leq a \leq n-1$ and $0 \leq b \leq n-1$. Without loss of generality we shall suppose that $a \geq b$. We have $x^{a-b} = 1$, where $a - b \in \mathbb{Z}$ and $0 \leq a - b \leq n - 1$. Because $n$ is the smallest positive integer with $x^n = 1$, we must have $a - b = 0$, i.e. $a = b$. This proves that the elements $1, x, x^2, \ldots, x^{n-1}$ are distinct. 

**THEOREM 3.14:** Let $G$ be a multiplicatively-written group with elements $x$ and $y$ of finite orders $a$ and $b$ respectively. Suppose further that $xy = yx$ and that $a$ and $b$ are relatively prime. Then $xy$ has order $ab$.

**PROOF:** Because $xy = yx$ we have $(xy)^n = x^ny^n$ for every positive integer $n$. Note that $x^n = 1 = y^b$ where 1 is the identity element of $G$. Hence $(xy)^n = x^{na}y^{na} = (x^a)^n(y^b)^n = 1^n1^n = 1$. Because $(xy)^{ab} = 1$ we know that $xy$ has finite order $n$ for some positive integer $n$ and that $n$ divides $ab$ (see 3.13(1)). Since ord$(xy) = n$ we have $(xy)^n = 1$. Therefore $1 = ((xy)^n)^a = (xy)^na = x^{na}y^{na} = (x^a)^ny^{na} = 1^n(y^b)^n = y^{na}$. Thus $y^{na} = 1$ where $y$ has order $b$, so that $b$ divides $na$ (see 3.13(1) again). But $b$ and $a$ are relatively prime, so it follows that $b$ divides $n$. Similarly $a$ divides $n$. So $a$ and $b$ are relatively prime and they both divide $n$, from which it follows that $ab$ divides $n$ (this is because $n = ac$ for some $c \in \mathbb{Z}$, so that $b$ divides $ac$ with hcf$(b, a) = 1$ so that $b$ divides $c$ and hence $ab$ divides $ac$). Thus the positive integers $ab$ and $n$ divide each other, so that $n = ab$ as required. 

**REMARKS 3.15:** Let $G$ be a group. If $G$ is Abelian then the elements of $G$ of finite order form a subgroup of $G$ known as the torsion subgroup of $G$ (you do not need to remember this). But if $G$ is not Abelian then the set of elements of $G$ of finite order may not be closed under multiplication, and hence in general this subset is not a subgroup of $G$.

**DEFINITION 3.16:** (Commuting elements) Elements $x$ and $y$ of a multiplicatively-written group are said to commute, or to commute with each other, if $xy = yx$.

Thus one of the assumptions in the statement of 3.14 was that $x$ and $y$ commute, and if this assumption is dropped then 3.14 may be false.