Chap 10. Order of group elements

only allow integer exponents

Exponential notation: $a^n = \underbrace{a \cdots a}_{n \text{ times}}$ $\quad a^{-n} = \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{n \text{ times}}$ $\quad a^0 = e$

law of exponents: (i) $a^m \cdot a^n = a^{m+n}$ (ii) $(a^m)^n = a^{mn}$ (iii) $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Thm: Division algorithm: If m and n are integers and n is positive, there exist unique integers q and r. s.t. $m = nq + r$ and $0 \le r < n$. q: quotient r: remainder.

observe: If $\exists\, m \in \mathbb{Z}$ s.t. $a^m = e$, then $\exists\, n > 0 \in \mathbb{Z}$ s.t. $a^n = e$.

Def: If $\exists\, m \in \mathbb{Z}$ s.t. $a^m = e$, then the order of the element a (ord(a)) is defined to be the least positive integer n s.t. $a^n = e$. If there does not exist any nonzero integer m s.t. $a^m = e$, we say that a has order infinity. $(\text{ord}(a) = \infty)$

Thm: If $\text{ord}(a) = n$, then there are exactly n different powers of a: $a^0, a, a^2, \ldots, a^{n-1}$

Thm: If a has order infinity, then all the powers of a are different: If $r \ne s$, then $a^r \ne a^s$.

Thm: Suppose $\text{ord}(a) = n$. Then $a^t = e$ iff t is a multiple of n, i.e. $t = nq$ for some $q \in \mathbb{Z}$.

Pf. $t = nq + r$, $0 \le r < n$ $\quad \underset{e}{a^t} = a^{nq+r} = (a^n)^q \cdot a^r = a^r$ $\quad$ t is least positive $\Downarrow$ $r = 0$

Ex. A1: $a^m \cdot a^n \overset{m=-k<0}{\underset{n>0}{=\!=}} a^{-k} \cdot a^n = \underbrace{a^{-1} \cdots a^{-1}}_{k \text{ times}} \underbrace{a \cdots a}_{n \text{ times}} = a^{-k+n} = a^{m+n}$

B1: $\overline{10} \in \mathbb{Z}_{25}$. $\overline{10}, \overline{20}, \overline{30} = \overline{5}, \overline{40} = \overline{15}, \overline{50} = 0 \Rightarrow \text{ord}(\overline{10}) = 5$

B3: $\underset{f}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}} = (1\,6\,4\,2)(3)$ $\quad \text{ord}(f) = 4$

C4: $a^n = e \Leftrightarrow (bab^{-1})^n = b \cdot a^n b^{-1} = e \Rightarrow \mathrm{ord}(a) = \mathrm{ord}(bab^{-1})$

C6: $(ab)^n = e \Leftrightarrow \underbrace{a(ba)^{n-1}b}_{=(ab)^n} = e \Leftrightarrow \underbrace{(ba)^{n-1}b \cdot a}_{=(ba)^n} = e \Rightarrow \mathrm{ord}(ab) = \mathrm{ord}(ba)$

D2: $\left.\begin{array}{l} \mathrm{ord}(a^k) = m \\ \mathrm{ord}(a) = n \Rightarrow a^{kn} = (a^n)^k = e \end{array}\right\} \Rightarrow n = m \cdot q$ for $q \in \mathbb{Z}_{>0}$

E1: $ab = ba \quad (ab)^{\mathrm{lcm}(m,n)} = a^{\mathrm{lcm}(m,n)} \cdot b^{\mathrm{lcm}(m,n)} = e \Rightarrow \mathrm{ord}(ab) \mid \mathrm{lcm}(m,n)$

E2: $(m,n) = 1$. $\left.\begin{array}{l} \mathrm{ord}(a^k) \mid m \\ \mathrm{ord}(b^l) \mid n \\ a^k = b^l \end{array}\right\} \Rightarrow \mathrm{ord}(a^k) = \mathrm{ord}(b^l) = 1 \Rightarrow a^k = b^l = e$

E3: $a^i b^j = a^k b^l \Rightarrow a^{i-k} = b^{l-j} \xRightarrow{E2} a^{i-k} = b^{l-j} = e \Rightarrow \begin{array}{l} m \mid i-k \\ n \mid l-j. \end{array}$

E4: $(ab)^k = e \Rightarrow a^k = b^{-k} \xRightarrow{E2} a^k = b^{-k} = e \Rightarrow m \mid k$ and $n \mid k \Rightarrow \mathrm{lcm}(m,n) \mid k$

$\left(E1: (ab)^{\mathrm{lcm}(m,n)} = e\right) \Rightarrow \mathrm{ord}(ab) = \mathrm{lcm}(m,n)$.

E5 assume $\gcd(m,n) = c$ then $\mathrm{lcm}(m,n) = \frac{mn}{c}$ and $\left(\frac{m}{c}, n\right) = 1$

$\mathrm{ord}(a^c) = \frac{m}{c}$ and $\mathrm{ord}(b) = n \xRightarrow{E4} \mathrm{ord}(a^c b) = \frac{m}{c} \cdot n = \mathrm{lcm}(m,n)$.

G1: $(m,n) = 1$. $\underbrace{(a^m)^k}_{=a^{mk}} = e \Rightarrow n \mid mk \xRightarrow{(m,n)=1} n \mid k \Rightarrow \mathrm{ord}(a^m) = n$.

G2: If $\exists\, q > 1$, $q \mid m$ and $q \mid n$. then $(a^m)^{\frac{n}{q}} = (a^n)^{\frac{m}{q}} = e \Rightarrow \mathrm{ord}(a^m) \leq \frac{n}{q} < n$.

G3: $l = \mathrm{lcm}(m,n) \Rightarrow (a^m)^{\frac{l}{m}} = a^l = (a^n)^{\frac{l}{n}} = e$.

$\ell \mid mt$

<u>G4</u>: $(a^m)^t = e \Rightarrow \begin{matrix} n \mid mt \\ m \mid mt \end{matrix} \Rightarrow \ell = \mathrm{lcm}(m,n) \leq mt$

<u>G5</u>: $(a^m)^{\frac{\ell}{m}} = e \Rightarrow \mathrm{ord}(a^m) \mid \frac{\ell}{m} \Rightarrow \mathrm{ord}(a^m) \leq \frac{\ell}{m}$

$(a^m)^t = e \overset{G4}{\Rightarrow} \ell \mid mt \Rightarrow \frac{\ell}{m} \leq t \Rightarrow \mathrm{ord}(a^m) \geq \frac{\ell}{m}$

$\Rightarrow \mathrm{ord}(a^m) = \frac{\ell}{m} = \frac{\mathrm{lcm}(m,n)}{m}$

<u>B7</u>: In $\mathbb{Z}_{24}$. $\mathrm{ord}(a) \mid 24 \Rightarrow \mathrm{ord}(a) = 1, 2, 3, 4, 6, 8, 12, 24$

- $\boxed{\mathrm{ord}(a^m) = \frac{\mathrm{lcm}(m,n)}{m}}$
- $\mathrm{ord}(a) = mk \Rightarrow \mathrm{ord}(a^m) = k$

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$	$\overline{19}$	$\overline{20}$	$\overline{21}$	$\overline{22}$	$\overline{23}$
ord	0	24	12	8	6	24	4	24	3	8	12	24	2	24	12	8	3	17	4	24	6	8	12	24
										$\frac{72}{9}$	$\frac{120}{10}$				$\frac{168}{14}$	$\frac{120}{15}$	$\frac{48}{16}$		$\frac{72}{18}$		$\frac{120}{20}$	$\frac{168}{21}$	$\frac{264}{22}$	

ord=1: $\bar{0}$ $\quad \langle \bar{0} \rangle = \{\bar{0}\}$

ord=2: $\overline{12}$ $\quad \langle \overline{12} \rangle = \{\bar{0}, \overline{12}\}$

ord=3: $\bar{8}, \overline{16}$ $\quad \langle \bar{8} \rangle = \{\bar{0}, \bar{8}, \overline{16}\} = \langle \overline{16} \rangle$

ord=4: $\bar{6}, \overline{18}$ $\quad \langle \bar{6} \rangle = \{0, \bar{6}, \overline{12}, \overline{18}\} = \langle \overline{18} \rangle$

ord=6: $\bar{4}, \overline{20}$ $\quad \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \overline{12}, \overline{16}, \overline{20}\} = \langle \overline{20} \rangle$

ord=8: $\bar{3}, \bar{9}, \overline{15}, \overline{21}$ $\quad \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\}$

ord=12: $\bar{2}, \overline{10}, \overline{14}, \overline{22}$ $\quad \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}\}$

ord=24: $\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}$ $\quad \langle \bar{1} \rangle = \mathbb{Z}_{24}$