Notations and Conventions

Let $(S,*)$ be a semigroup. For any $a,b \in S$ we usually write ab instead of $a*b$ (you should know that between a and b in ab there is the binary operation on S).

Let $(S,*)$ be a semigroup. We define the powers of elements of S as follows: Let $a \in S$. We define

$$a^n = \underbrace{a\,a \cdots a}_{n \text{ times}} = (a*a*\cdots*a), \text{ if } n \in \mathbb{Z}^+$$

$$a^0 = e, \text{ if } (S,*) \text{ has identity and } e \text{ is the identity of } (S,*)$$

$$a^n = (a^{-1})^{-n} = \underbrace{a^{-1}\,a^{-1} \cdots a^{-1}}_{-n \text{ times}}, \text{ if } n \in \mathbb{Z}^- \text{ and } (S,*) \text{ has identity and } a \text{ has inverse and } a^{-1} \text{ is the inverse of } a.$$

For instance, in $(\mathbb{R}, \overset{\text{usual addition}}{+})$,
$2^5 = 2+2+2+2+2 = 10$
$2^0 = 0$
$2^{-1} = -2$
$2^{-4} = (-2)+(-2)+(-2)+(-2) = -8$

but in $(\mathbb{N}, \overset{\text{usual multiplication}}{\cdot})$,
$2^5 = 2\cdot2\cdot2\cdot2\cdot2 = 32$
$2^0 = 1$
2^{-1} and 2^{-4} are undefined because 2 has no inverse.

<u>Remark</u>: (1) Any nonempty set S is a semigroup wrt some binary operation. Indeed, choose an element $s_0 \in S$ and consider the binary operation $*$ on S defined by $a*b = s_0$ for all $a,b \in S$.

Then $(S,*)$ is semigroup

(2) Let $(S,*)$ be a semigroup with identity 1 and with zero 0. If $1=0$ then $S=\{0\}=\{1\}$

<u>Proof</u>: (1): Exercise

(2): Let $a\in S$. Then $a \underset{\substack{\uparrow \\ 1 \text{ is the identity}}}{=} a1 \overset{\substack{1=0 \\ \uparrow}}{=} a0 \underset{\substack{\downarrow \\ 0 \text{ is the zero}}}{=} 0$. So $S\subseteq\{0\}$

$\square$

Whenever we have a semigroup $(S,*)$ it is reasonable to assume that $(S,*)$ is not the semigroup in part (1) of the above remark and that $|S|>1$ (so $1\neq 0$ if S has identity 1 and zero 0), because they are not interesting.

Adjoining the identity

<u>Remark</u>: Let $(S,*)$ be a semigroup without identity. Take a symbol 1 such that $1\notin S$ and consider $S^1=S\cup\{1\}$. Then S^1 becomes a semigroup with identity 1 (i.e., a monoid) wrt the binary operation $\circ$ defined on S^1 as follows:

$$a\circ b=a*b \text{ for all } a,b\in S, \quad a\circ 1=a=1\circ a \text{ for all } a\in S$$

<u>Proof</u>: Exercise $\square$

<u>Ex</u>: Let $S=\{4,5,6,\dots\}=\{n\in\mathbb{N}\mid n\geq 4\}$.

(1) $(S,\underset{\substack{\uparrow \\ \text{usual}}}{\cdot})$ is a semigroup without identity. Then $S^1=\{1,4,5,6,\dots\}$
$=\{1\}\cup S$

is a monoid wrt the usual multiplication.

(2) $(S, +)$ is a semigroup without identity. Then $S^1 = S \cup \{0\}$
usual add. $= \{0, 4, 5, 6 \dots\}$

is a semigroup wrt the usual addition

Subsemigroups

<u>Definition</u>: Let $(S, *)$ be a $\left\{\begin{matrix} \text{semigroup} \\ \text{monoid} \\ \text{group} \end{matrix}\right\}$. A <u>nonempty subset</u> T of S is called a $\left\{\begin{matrix} \text{subsemigroup} \\ \text{submonoid} \\ \text{subgroup} \end{matrix}\right\}$ of S if T is itself a $\left\{\begin{matrix} \text{semigroup} \\ \text{monoid} \\ \text{group} \end{matrix}\right\}$ wrt the binary $*$ on S.

<u>Ex:</u> (1) $(\mathbb{Z}, \underset{\text{usual addition}}{+})$ is a group. Then,

$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

$\mathbb{Z}_{\geq 0} = \{k \in \mathbb{Z} \mid k \geq 0\}$ is a submonoid of $(\mathbb{Z}, +)$ but not a subgroup of $(\mathbb{Z}, +)$.

$\mathbb{Z}^+$ is a subsemigroup of $(\mathbb{Z}, +)$ but not a submonoid of $(\mathbb{Z}, +)$.

(2) $M_{2\times 2}(\mathbb{R})$ = the set of all 2×2 matrices with real entries. Consider the subsets $U = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\}$ and $V = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbb{R} \right\}$

Then, $M_{2\times 2}(\mathbb{R})$ is a monoid wrt the matrix multiplication, and both U and V are submonoids of $M_{2\times 2}(\mathbb{R})$. Note that the identities of U and $M_{2\times 2}(\mathbb{R})$ are the same (which is the 2×2 identity matrix), but the identities of V and $M_{2\times 2}(\mathbb{R})$ are different

The identity of V is $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ but the identity of $M_{2\times 2}(\mathbb{R})$ is $\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

<u>Remark</u>: Let $(S,*)$ be a group and T be a subgroup of S. Then, the identities of the groups $(S,*)$ and $(T,*)$ are the same, that is $1_S = 1_T$. In particular, the identity of S is in T. Furthermore, for any $a \in T$, the inverses of a in the groups $(T,*)$ and $(S,*)$ are the same.

<u>Proof</u>: As $T \subseteq S$ and $1_T \in T$, $1_T \in S$. As $(S,*)$ is a group, every $a \in S$ has an inverse $a^{-1} \in S$ and $a * a^{-1} = 1_S = a^{-1} * s$. In particular, 1_T has an inverse 1_T^{-1} in S and $1_T * 1_T^{-1} = 1_S$

Now, consider the equation $1_T * 1_T = 1_T$ of the group $(T,*)$ as an equation in the group $(S,*)$. Multiply both sides with 1_T^{-1}

$$1_T * 1_T = 1_T \Rightarrow (1_T * 1_T) * 1_T^{-1} = 1_T * 1_T^{-1}$$

$$1_T * \underbrace{(1_T * 1_T^{-1})}_{1_S} = \underbrace{1_T * 1_T^{-1}}_{1_S} \quad \text{(associativity)}$$

$$1_T * 1_S = 1_S$$

$$1_T = 1_S$$

Hence, the identities of S and T are the same. Let $a \in T$ and $\bar{a}$ be the inverse of a in S and $\bar{\bar{a}}$ be the inverse of a in T. So $\bar{a} * a = 1_S = a * \bar{a}$ and $a * \bar{\bar{a}} = 1_T = \bar{\bar{a}} * a$. Note that

$$\bar{a} = \bar{a} * 1_S = \bar{a} * 1_T = \bar{a} * (a * \bar{\bar{a}}) = (\bar{a} * a) * \bar{\bar{a}} = 1_S * \bar{\bar{a}} = 1_T * \bar{\bar{a}} = \bar{\bar{a}}$$

$\square$

Definition: Let $(S,*)$ be a semigroup. We say that <u>cancellation holds</u> in $(S,*)$ (or $(S,*)$ is <u>cancellative</u>) if

$$(\forall a,b,c\in S)\Big((ab=ac \Rightarrow b=c) \text{ and } (ba=ca \Rightarrow b=c)\Big)$$

One may easily see that in a group cancellation holds. (Exercise)
Using this the previous result can be proved shortly as follows:

$$1_T * 1_T = 1_T = 1_T * 1_S \underset{\text{cancelling } 1_T\text{'s}}{\Rightarrow} 1_T = 1_S$$

$$\bar{a} * a = 1_S = 1_T = \bar{\bar{a}} * a \underset{\text{cancelling } a\text{s}}{\Rightarrow} \bar{\bar{a}} = \bar{a}$$

Proposition:

(1) Let $(S,*)$ be a semigroup. Then,

$$T \text{ is a subsemigroup of } S \Leftrightarrow \begin{cases} \text{(i)} & \emptyset \neq T \subseteq S \\ \text{(ii)} & a*b \in T \text{ for all } a,b\in T \\ & \text{(i.e. } T \text{ is closed under } *) \end{cases}$$

(2) Let $(S,*)$ be a monoid. Then,

$$T \text{ is a submonoid of } S \Leftrightarrow \begin{cases} \text{(i)} & \emptyset \neq T \subseteq S \\ \text{(ii)} & ab \in T \text{ for all } a,b\in T \\ & \text{(i.e., } T \text{ is closed under } *) \\ \text{(iii)} & T \text{ has an identity} \end{cases}$$

(3) Let $(S,*)$ be a group. Then,

$$T \text{ is a subgroup of } S \Leftrightarrow \begin{cases} \text{(i)} & \emptyset \neq T \subseteq S \\ \text{(ii)} & ab \in T \text{ for all } a,b\in T \\ & (T \text{ is closed under } *) \\ \text{(iii)} & a^{-1} \in T \text{ for all } a\in T \\ & (T \text{ is closed under taking inverse}) \end{cases}$$

Proof: (1) and (2) are exercise.

(3): The part "$\Rightarrow$" is clear (Why?).

($\Leftarrow$): Assume that T satisfies the conditions (i), (ii) and (iii). We want to show that $(T, *)$ is a group. For this we need to justify that $(T, *)$ satisfies the axioms in the definition of a group (which are "closedness, associativity, identity, inverse"). Firstly, note by (i) that T is a nonempty set. Closedness follows from (ii). Associativity is clear, because all elements of S satisfy the associativity (as S is a group) and $T \subseteq S$.

Identity: As $T \neq \emptyset$ by (i), there is an element $a \in T$. Then $a^{-1} \in T$ by (iii). Now, $a \in T$ and $a^{-1} \in T$. So, by using (ii) we see that $a * a^{-1} \in T$. As $a * a^{-1} = 1$, the identity 1 of S is in T. Note that $1 \in T$ and $1 * b = b = b * 1$ for all $b \in T$. So 1 is the identity of $(T, *)$

Inverse: Let $c \in T$. By (iii), $c^{-1} \in T$ where c^{-1} is the inverse of c in S. As $c * c^{-1} = 1 = c^{-1} * c$ and 1 is the identity of T, each element of $(T, *)$ has an inverse. $\square$

Subsemigroup generated by a subset

Remark: (1) Intersection of any number of subsemigroups of a semigroup is either the empty set or a subsemigroup. That is, if $(S, *)$ is a semigroup and S_i is a subsemigroup of S for all $i \in I$ where I is any index set, then $\bigcap_{i \in I} S_i = \emptyset$ or a subsemigroup of S

(2) Intersection of any number of subgroups of a group is a subgroup. That is, if $(S, *)$ is a group and S_i is a subgroup of S for all $i \in I$ where I is any index set, then $\bigcap_{i \in I} S_i$ is a subgroup of G.

Proof: Exercise $\square$

Definition: (1) Let $(S, *)$ be a semigroup and $U \subseteq S$ be a nonempty subset. (Then, it follows from the previous remark that the intersection of all subsemigroups of S containing U is nonempty and so a subsemigroup.) The subsemigroup of S generated by the subset U is defined to be

$$\langle U \rangle = \bigcap_{T \in \mathcal{F}} T \quad \text{where } \mathcal{F} = \{A \mid A \text{ is a subsemigroup of } S \text{ and } U \subseteq A\}$$

$=$ the intersection of all subsemigroups of S containing U.

(2) If $(S, *)$ is a group and $U \subseteq S$ is any subset, then the subgroup of S generated by the subset U is defined to be

$$\langle U \rangle = \bigcap_{T \in \mathcal{F}} T \quad \text{where } \mathcal{F} = \{A \mid A \text{ is a subgroup of } G \text{ and } U \subseteq A\}$$

$=$ the intersection of all subgroups of S containing U.

($\langle U \rangle$ is a subgroup of S by part (2) of the previous remark)

(3) U is called a generating set for $\langle U \rangle$.

(4) If $U = \{u_1, u_2, \dots, u_n\}$ is finite, we write $\langle u_1, u_2, \dots, u_n \rangle$ instead of $\langle \{u_1, u_2, \dots, u_n\} \rangle$.

(5) For any $a \in S$, $\langle a \rangle$ is called the cyclic subsemigroup / subgroup of the semigroup / group $(S, *)$; and a is called a generator of $\langle a \rangle$. (Some books may prefer to say monogenic instead of cyclic)

Fact:

(1) Let $(S, *)$ be a semigroup and $U \subseteq S$ be a nonempty subset. Then,

(a) $\langle U \rangle$ is the smallest (wrt $\subseteq$) subsemigroup of S containing U. That is, if K is a subsemigroup of S containing U, then $\langle U \rangle \subseteq K$.

(b) $\langle U \rangle = \{ u_1 u_2 u_3 \cdots u_n \mid n \in \mathbb{N}^+, u_i \in U \ \forall i \} =$ the set of all finite products of elements of U

(We may think that "U is an alphabet so that elements of U are letters, and $\langle U \rangle$ is the set of all words that can be form by using the letters in U").

(2) Let $(S, *)$ be a group and $U \subseteq S$ be a subset. Then,

(a) $\langle U \rangle$ is the smallest (wrt $\subseteq$) subgroup of S containing U. That is, if K is a subgroup of S containing U, then $\langle U \rangle \subseteq K$

(b) $\langle U \rangle = \{ u_1^{e_1} u_2^{e_2} \cdots u_n^{e_n} \mid n \in \mathbb{N}^+, u_i \in U \ \forall i, \ e_i \in \{-1, 1\} \ \forall i \}$

(Here note that $u_i^1 = u_i$ and u_i^{-1} is the inverse of u_i)

$= \{ v_1 v_2 \cdots v_n \mid n \in \mathbb{N}^+, v_i \in U \cup U^{-1} \}$ where $U^{-1} = \{ u^{-1} \mid u \in U \}$

= the set of all finite products of elements of $U \cup U^{-1}$

(We may think that "$\langle U \rangle$ is the set of all words that can be formed by using the alphabet $U \cup U^{-1}$)

Proof: We only prove part (1)(b) and left the rest as an exercise.

(1)(b): Let A be any subsemigroup of S containing U. Take any $n \in \mathbb{N}^+$ and take any $u_1, u_2, \dots, u_n \in U$ (not necessarily distinct). As $U \subseteq A$, $u_i \in A \; \forall i$. Being a subsemigroup, A is closed under product. As $u_i \in A \; \forall i$, $u_1 u_2 \cdots u_n \in A$. Since this is true for any subsemigroup A containing U, $u_1 u_2 \cdots u_n \in \bigcap_{A \in \mathcal{F}} A = \langle U \rangle$ where $\mathcal{F} = \{T \mid T$ is a subsemigroup of S and $U \subseteq T\}$. Hence, $\{u_1 u_2 \cdots u_n \mid n \in \mathbb{N}^+, u_i \in U \; \forall i\} \subseteq \langle U \rangle$.

For the converse containment, it is enough to show that $W = \{u_1 u_2 \cdots u_n \mid n \in \mathbb{N}^+, u_i \in U \; \forall i\}$ is a subsemigroup of S and $U \subseteq W$. Why? Exercise. $\square$

Fact: (1) Let $(S, *)$ be a semigroup and $a \in S$. Then,

$$\langle a \rangle = \{a, a^2, a^3, a^4, \dots\} = \{a^n \mid n \in \mathbb{N}^+\}$$

(2) Let $(S, *)$ be a group and $a \in S$. Then

$$\langle a \rangle = \{\dots, a^{-2}, a^{-1}, \underset{\substack{\| \\ aa^{-1} = 1}}{a^0}, a^1, a^2, a^3, \dots\}$$

$$= \{a^n \mid n \in \mathbb{Z}\}$$

Proof: We prove only part (2), leaving part (1) as an exercise.

(2) $\langle a \rangle = \{ \underbrace{\underbrace{a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n}}_{a^{e_1} a^{e_2} \cdots a^{e_n}}}_{a^{e_1+e_2+\cdots+e_n}} \mid n \in \mathbb{N}^+,\ a_i \in \{a\}\ \forall i,\ e_i \in \{-1,1\}\ \forall i \}$

$= \{ a^n \mid n \in \mathbb{Z} \}$ $\square$

Ex: (1) Consider the semigroup $(\mathbb{N}, \overset{\text{usual addition}}{+})$ and subset $\{3,5\}$.

Find the subsemigroup $\langle 3,5 \rangle$ generated by $\{3,5\}$.

Sol: $\langle 3,5 \rangle = \{ \underbrace{u_1 u_2 \cdots u_n}_{u_1+u_2+\cdots+u_n} \mid n \in \mathbb{N}^+,\ u_i \in \{3,5\}\ \forall i \}$

$= \{ 3a+5b \mid a,b \in \mathbb{N},\ 3a+5b \neq 0 \}$

$= \{ 3, 5, \underset{3+3}{6}, \underset{3+5}{8}, \underset{3+3+3}{9}, \underset{5+5}{10}, \underset{3+3+5}{11}, 12, \underset{3+5+5}{13}, \ldots ? \ldots \}$

Note that $4 \notin \langle 3,5 \rangle$ and $7 \notin \langle 3,5 \rangle$ because $3a+5b=4$, $3a+5b=7$ are not solvable for $a,b \in \mathbb{N}$

Observing that 3 consecutive integers $8, 9, 10 \in \langle 3,5 \rangle$, we see by using the fact $3 \in \langle 3,5 \rangle$ that every integer > 10 is in $\langle 3,5 \rangle$. Indeed, let $n > 10$. Then, $n-8, n-9, n-10$ are 3 distinct positive integers. So one of them must be divisible by 3. Say, for instance, $n-8 = 3q$. Then, Note that $n = 3q + 8 = \underbrace{3+3+\dots+3}_{q \text{ times}} + 3+5 \in \langle 3,5 \rangle$.

Hence, $\langle 3,5 \rangle = \{3,5,6\} \cup \{n \in \mathbb{N} \mid n \geq 8\}$

(2) Consider the group $(\mathbb{Z},+)$ and subset $\{3,5\}$.
Find the subgroup $\langle 3,5 \rangle$.

Sol: $\langle 3,5 \rangle = \{ \underbrace{u_1^{e_1} u_2^{e_2} \dots u_n^{e_n}}_{(\mp u_1)+(\mp u_2)+\dots+(\mp u_n)} \mid n \in \mathbb{N}^+,\ u_i \in \{3,5\}\ \forall i,\ e_i \in \{-1,1\}\ \forall i \}$

$= \{ 3a + 5b \mid a,b \in \mathbb{Z} \}$

Note that $3(-3) + 5(2) = 1$. So $3(\underset{a}{\underset{\parallel}{-3n}}) + 5(\underset{b}{\underset{\parallel}{2n}}) = n \quad \forall n \in \mathbb{Z}$.

Consequently, $\langle 3,5 \rangle = \mathbb{Z}$. We say that $\{3,5\}$ generates the group $(\mathbb{Z},+)$

(3) Consider the semigroup $(\mathbb{R}, \overset{\text{usual mult.}}{\cdot})$ and $2 \in \mathbb{R}$.
Find the cyclic subsemigroup $\langle 2 \rangle$.

Sol $\langle 2 \rangle = \{2^n \mid n \in \mathbb{N}^+\} = \{2, 4, 8, 16, 32, \dots\}$

(4) Consider the group $(\mathbb{R}-\{0\}, \overset{\text{usual mult.}}{\cdot})$ and $2 \in \mathbb{R}-\{0\}$.
Find the cyclic subgroup $\langle 2 \rangle$

Sol $\langle 2 \rangle = \{2^n \mid n \in \mathbb{Z}\} = \{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$

Index, period and order of an element

Definition: Let $(S, *)$ be a semigroup and $a \in S$.

(1) The order of a is defined to be $|\langle a \rangle| = |\{a, a^2, a^3, a^4, \dots\}|$

(2) Suppose that the order of a is finite. That is, $\{a, a^2, a^3, a^4, \dots\}$ is a finite set. So there must be a repeatition among the positive powers of a. Let n_0 be the smallest element of the set $\{n \in \mathbb{N}^+ \mid a^n = a^m \ \exists m < n\}$. Then there is a unique $m_0 \in \mathbb{N}^+$ such that $m_0 < n_0$ and $a^{n_0} = a^{m_0}$ (For uniqueness, suppose that $a^{n_0} = a^{m_1}$ and $a^{n_0} = a^{m_2}$ for some distinct positive integers m_1 and m_2 satisfying $m_1 < n_0$ and $m_2 < n_0$. As $m_1 \neq m_2$, say $m_1 < m_2$. As $a^{m_2} = a^{m_1}$, we see that $m_2 \in \{n \in \mathbb{N}^+ \mid a^n = a^m \ \exists m < n\}$. So $m_2 \geq n_0$ because n_0 is the smallest element of the set. Contradiction). Then, m_0 is called the index of a, $n_0 - m_0$ is called the period of a

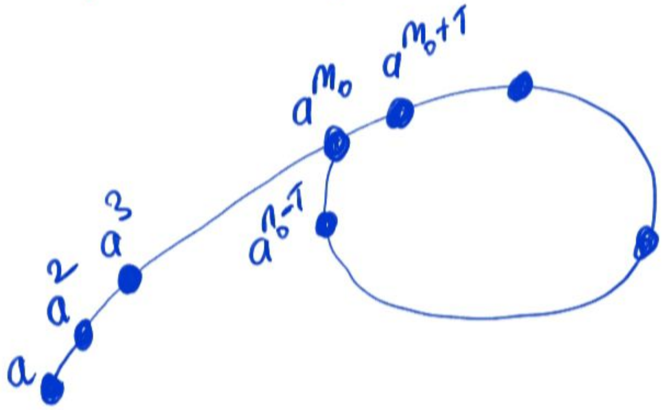
Note that

$$a, a^2, a^3, \dots, a^{m_0}, a^{m_0+1}, a^{m_0+2}, \dots, a^{n_0-1}$$

are all distinct and $a^{n_0} = a^{m_0}$. So, $\langle a \rangle = \{a, a^2, \dots, a^{m_0}, \dots, a^{n_0-1}\}$ and the order of a is $n_0 - 1$ (="index + period − 1").

(Finding index and period is easy: just calculate the positive powers a^k of a until the answer for the following question is Yes: "Is a^k equal to one of the previous powers $a, a^2, a^3, \dots, a^{k-1}$?"

Once the answer is yes for the first time for $k = n_0$, then $a^{n_0} = a^{m_0}$ for some unique $m_0 < n_0$. Then, m_0 is the index of a, $n_0 - m_0$ is the period of a, and $n_0 - 1$ is the order of a)



$$a^{n_0} = a^{m_0}$$

<u>Ex</u>: Let $I = \{1,2,3,4,5,6,7\}$ and $\mathcal{F}_I$ be the set of all functions $I \to I$. Recall that $\mathcal{F}_I$ becomes a semigroup wrt the function composition. Consider the element $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 5 \end{pmatrix}$

(i.e., $\alpha : I \to I$ is the function given by $\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 4, \ldots, \alpha(7) = 5$)

$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 5 & 6 \end{pmatrix}$, $\alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix}$

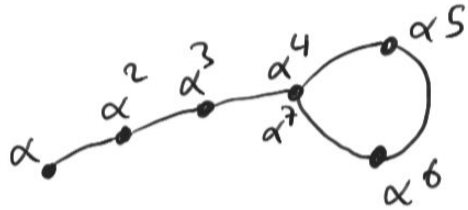
$\alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 5 & 6 & 7 & 5 \end{pmatrix}$, $\alpha^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 6 & 7 & 5 & 6 \end{pmatrix}$

$\alpha^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix}$, $\alpha^7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 5 & 6 & 7 & 5 \end{pmatrix}$

Note that
α, α^2
$\alpha, \alpha^2, \alpha^3$
$\alpha, \alpha^2, \alpha^3, \alpha^4$ $\to$ each line is distinct
$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$
$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$
$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7$ ✗ ! not distinct (it is the first time it is not distinct)

$\alpha^7 = \alpha^4$.

index = 4
period = 3
order = 6



$\alpha^4 = \alpha^7$

$\langle\alpha\rangle = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. For instance, let us find $\alpha^{101} \in \langle\alpha\rangle$

From $\alpha^4 = \alpha^7$ we see that $\alpha^{4+3q} = \alpha^4$ for any $q \geq 0$ (Why?)

$$\left(\alpha^4 = \alpha^{4+3};\quad \underbrace{\alpha^{4+3}}_{=\alpha^4} = \alpha^{4+3+3};\quad \underbrace{\alpha^{4+3+3}}_{=\alpha^4} = \alpha^{4+3+3+3}, \ldots\right)$$

$$\alpha^{101} = \alpha\,\alpha^{100} = \alpha\,\alpha^{4+3\cdot 32} = \alpha\,\alpha^4 = \alpha^5.$$

<u>Fact</u>: (1) Let $(S,*)$ be a semigroup, and $a \in S$ be an element of finite order. Assume that m is the index of a and r is the period of a. Then, $a^{m+qr} = a^m$ $\forall q \in \mathbb{N}$. More generally, for any $u, v \in \mathbb{N}$,

$$a^{m+u} = a^{m+v} \iff u \equiv v \mod r$$

(2) Let $(S,*)$ be a group, and $a \in S$ be an element of finite order. Then, the index of a is 1, and the period and the order of a are the same, and $\langle a\rangle = \{a, a^2, a^3, \ldots, a^r\}$ where r is the period (or the order) of a. Note that $a^{r+1} = a$ and $a^r = 1$, the identity of S.

<u>Proof</u>: We only prove part (2), leaving part (1) as an exercise.

(2) Suppose that m is the index of a and r is the period

of a. So $a^{m+r} = a^m$. Cancelling a^{m-1} (as $m \in \mathbb{N}^+$, we cancel a^{m-1} not a^m) we get $a^{1+r} = a^1$. As $m+r$ is the smallest positive integer such that a^{m+r} equals to a smaller power a^t $\exists t < m+r$, it follows that $m = 1$. The result follows. $\square$

Remark: Let $(G, *)$ a group and $g \in G$. Then,

(1) If exists, the smallest positive integer n such that $g^n = 1$ is the order of g and denoted by $|g|$, where 1 is the identity of G.

(2) Suppose that $|g| = n$ is finite. Then,

(a) $(\forall u, v \in \mathbb{Z}) \left(g^u = g^v \Leftrightarrow u \equiv v \mod n \right)$

(b) $g^0, g^1, g^2, \dots, g^{n-1}$ are all distinct and so

$$\langle g \rangle = \{ g^0, g^1, \dots, g^{n-1} \}.$$

(c) $(\forall m \in \mathbb{Z}) \left(g^m = 1 \Leftrightarrow n \mid m \right.$ (i.e., n divides m) $)$

Proof: Exercise $\square$

Homomorphisms

<u>Definition</u>: Let $(G, *)$ and $(H, \square)$ be semigroups/groups. By a <u>semigroup/group homomorphism</u> from G to H we mean a function $f: G \to H$ satisfying the following condition:

$$f(a * b) = f(a) \square f(b) \text{ for all } a, b \in G.$$

A homomorphism which is bijective is called an isomorphism.

<u>Ex</u>: (1) $f: (\mathbb{Z}, +) \longrightarrow (\mathbb{N}^+, \cdot)$, $n \mapsto 2^n$ is a semigroup homomorphism where the operations $+$ and $\cdot$ are the usual addition and multiplication.

Indeed, $f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$

(2) $f: (\mathbb{Z}, +) \longrightarrow (\mathbb{N}, +)$, $n \mapsto n^2$ is not a semigroup homomorphism.

Indeed, for instance, $1, 2 \in \mathbb{Z}$ but

$$\underset{9}{\underset{\parallel}{f(1+2)}} \neq \underset{1}{\underset{\parallel}{f(1)}} + \underset{4}{\underset{\parallel}{f(2)}}$$

(3) Let $(S, *)$ be a monoid, consider the semigroup $\mathcal{F}_S$ of all functions $S \to S$ where the operation is the function composition. Consider the map $\phi: S \longrightarrow \mathcal{F}_S$, $a \mapsto \sigma_a : S \to S$, $x \mapsto a * x$. Then ϕ is a semigroup homomorphism. (Exercise)