CHAPTER III

DIGRAPHS DEFINED FROM ALGEBRAIC SYSTEMS

In this chapter we associate digraphs to algebraic systems in a certain ways, and try to characterize these digraphs.

3.1 Groupoids, Quasi-groups, Loops and Groups

By a groupoid we mean an ordered pair $(G, \circ)$, where G is a nonempty set and $\circ$ is a binary operation on G. If for each a, b of G, there exists unique elements x and y such that $a \circ x = b$ and $y \circ a = b$. Then $(G, \circ)$ is called a quasi - group. By a loop we mean a quasi - group $(G, \circ)$ in which there exists an element 1 in G such that for each x in G, $1 \circ x = x \circ 1 = x$. Such an element 1 is unique and is called the identity of the loop. If a loop $(G, \circ)$ is associative, i.e. for every x, y, z in G, $(x \circ y) \circ z = x \circ (y \circ z)$. Then we call $(G, \circ)$ a group. A group$(G, \circ)$ is a cyclic group iff there exists an element a in G such that every element of G is a power of a. We say that a is a generator of G. The number of element in a group$(G, \circ)$, $|G|$, is called the order of G. For each a in G, the order of a is the least positive integer m such that $a^m = 1$, and denoted by $|a|$. It is well - known that if $|G| = p$, p a prime, then G is a cyclic group.

3.1.1 Remark Let $(G, \circ)$ be a loop. Then for each a in G, there exists unique x in G such that $a \circ x = 1$ and there exists unique y in G such that $y \circ a = 1$. We shall call x the right inverse of a and y the left inverse of a. They will be denoted by a_r^{-1} and a_l^{-1} respectively. It can be shown that if $(G, \circ)$ is a group then the right and left inverses of a are equal. It will be called the inverse of a and denoted by a^{-1}.

3.1.2 Remark Given any finite set V we can always define a binary operation $\circ$ on V such that $(V, \circ)$ forms a group. This can be done as follows.

Let $(G, *)$ be any cyclic group of order $|V|$. Let f be a one - to - one mapping from V onto G. Define a binary operation $\circ$ on V by the equation $x \circ y = f^{-1}(f(x) * f(y))$. Then $(V, \circ)$ forms a cyclic group of order $|V|$.

Since cyclic groups are loops, quasi - groups and groupoids. Hence on any finite set V we can define a binary operation $\circ$ on V so that $(V, \circ)$ forms a loop, or a quasi - group or a groupoid.

3.2 Isomorphisms, Automorphisms and Isomorphic Groupoids.

Let $(G, \circ)$ and $(G^*, *)$ be groupoids. A mapping Θ from G into G^* is called a homomorphism from a groupoid $(G, \circ)$ into a groupoid $(G^*, *)$ if for each x,y in G, $(x \circ y)\Theta = x\Theta * y\Theta$.

If a homomorphism θ is one - to - one and onto, then θ is called an <u>isomorphism</u> from $(G, \circ)$ onto $(G^*, *)$. If there is an isomorphism from $(G, \circ)$ onto $(G^*, *)$, then we say that $(G, \circ)$ is <u>isomorphic</u> to $(G^*, *)$ and write $G \cong G^*$. If θ is an isomorphism from $(G, \circ)$ onto itself, then θ is called an <u>automorphism</u> of $(G, \circ)$.

3.2.1 <u>Remark</u> If θ is an isomorphism from a groupoid $(G, \circ)$ onto groupoid $(G^*, *)$. Then it is clear that $|G| = |G^*|$.

3.3 Digraph Induced by the Groupoid $(G, \circ)$ and a Subset A.

Let $(G, \circ)$ be a groupoid, and A a subset of G. Let

$$E_A = \{ (x, x \circ a) \in G \times G \mid x \in G, a \in A \}.$$

Then (G, E_A) is called the <u>digraph induced by the groupoid $(G, \circ)$ and a subset A</u>.

For example, let $(G, \circ)$ be a groupoid with the following multiplication table.

o	a	b	c
a	a	a	c
b	a	c	b
c	b	c	a

Let $A = \{ a, b \}$.

Then $E_A = \{ (a,a), (b,a), (b,c), (c,b), (c, c) \}$.

Hence (G, E_A) can be represented by the following diagram.

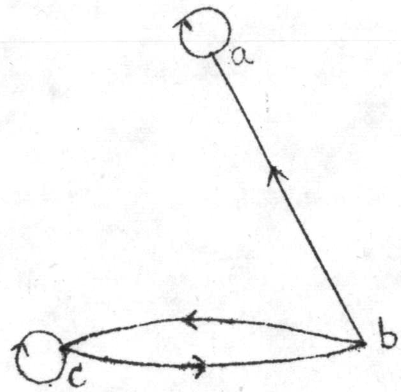

Fig. 3.3.1

3.3.1 <u>Remark</u> If $(G, \circ)$ is a group, then E_A can be written in the following forms :

$$E_A = \left\{ (x, x \circ a) \in G \times G \;\middle|\; x \in G, a \in A \right\}$$

$$= \left\{ (x, y) \in G \times G \;\middle|\; x, y \in G, \exists\, a \in A \ni y = x \circ a \right\}$$

$$= \left\{ (x, y) \in G \times G \;\middle|\; x, y \in G, x^{-1} \circ y \in A \right\}.$$

3.3.2 <u>Theorem</u> Let $(G, \circ)$ be a quasi - group and A', A'' be subsets of G. If $A = A' - A''$, then $E_A = E_{A'} - E_{A''}$.

<u>Proof</u> Let (x, y) be any element of E_A. Therefore $y = x \circ a$ for some $a \in A$. Since $A = A' - A''$, therefore $a \in A'$ and $a \notin A''$. Since $a \in A'$, therefore $(x, y) \in E_{A'}$. If $(x, y) \in E_{A''}$ we would have $y = x \circ a''$ for some $a'' \in A''$,

which shows that there exist distinct elements a, a'' in G such that $x \circ a = y = x \circ a''$. This is a contradiction. Thus $(x, y) \notin E_{A''}$. Hence $(x, y) \in E_{A'} - E_{A''}$. Therefore $E_A \subseteq E_{A'} - E_{A''}$.

Conversely, let (x, y) be any element of $E_{A'} - E_{A''}$. Therefore $(x, y) \in E_{A'}$ and $(x, y) \notin E_{A''}$. Since $(x, y) \in E_{A'}$, hence $y = x \circ a$ for some $a \in A'$. Since $(x, y) \notin E_{A''}$, therefore $a \notin A''$. Hence $a \in A' - A'' = A$. Therefore $(x, y) \in E_A$. Thus $E_{A'} - E_{A''} \subseteq E_A$

Hence $E_A = E_{A'} - E_{A''}$

<u>Q.E.D.</u>

3.3.3 <u>Theorem</u> Let Θ be an isomorphism from a groupoid $(G, \circ)$ to a groupoid $(G^*, *)$. Let A, A^* be subsets of G, G^* respectively. If $A^* = A\Theta$, where $A\Theta = \{ a\Theta \mid a \in A \}$, then $(G, E_A) \cong (G^*, E_{A^*})$.

<u>Proof</u> Let $\Theta : G \longrightarrow G^*$ be an isomorphism. That is Θ is one - to - one and onto and for each x, y in G, $(x \circ y)\Theta = x\Theta * y\Theta$.

We shall show that Θ is also a digraph isomorphism from (G, E_A) onto (G^*, E_A^*).

Since Θ is one - to - one and onto. Hence we have only to show that for each x, y in G

$$(x, y) \in E_A \Longleftrightarrow (x\Theta, y\Theta) \in E_A^* .$$

Let $(x, y) \in E_A$. Then there exists $a \in A$ such that $y = x \circ a$. So we have $y\theta = (x \circ a)\theta = x\theta * a\theta$. Since $a \in A$, then $a\theta \in A\theta = A^*$. Therefore there exists $a\theta \in A^*$ such that $y\theta = x\theta * a\theta$. Hence $(x\theta , y\theta) \in E_{A^*}$.

Conversely, let $(x\theta , y\theta) \in E_A^*$. Then there exists $a^* \in A^*$ such that $y\theta = x\theta * a^*$. Since $a^* \in A^* = A\theta$, hence $a^* = a\theta$ for some $a \in A$. So we have $y\theta = x\theta * a^* = x\theta * a\theta = (x \circ a)\theta$. Since θ is one - to - one, hence $y = x \circ a$ where $a \in A$. That is $(x, y) \in E_A$.

Hence θ is a digraph isomorphism from (G, E_A) onto (G^*, E_{A^*}) . Therefore $(G, E_A) \cong (G^*, E_A^*)$

Q.E.D.

3.4 Groupoid Digraphs, Quasi - group Digraphs, Loop Digraphs and Group Digraphs

Let (V, E) be a digraph. If there exists a groupoid $(G, \circ)$ and a subset A of G such that $(V, E) \cong (G, E_A)$, then we say that (V, E) is a groupoid digraph. If the groupoid can be chosen to be a quasi - group, or a loop, or a group, or a cyclic group, the groupoid digraph will be called a quasi - group digraph, or a loop digraph or a group digraph or a cyclic group digraph respectively.

3.5 Characterization of a Groupoid Digraph

3.5.1 Theorem Let (V, E) be a digraph. Then (V, E) is a groupoid digraph if and only if $E = \phi$ or for each $v \in V$, there exists $u \in V$ such that $(v, u) \in E$.

Proof : Let (V, E) be a groupoid digraph. Then there exists a groupoid $(G, \circ)$ and a subset A of G such that $(V, E) \cong (G, E_A)$. Let $\varphi : G \rightarrow V$ be a digraph isomorphism from (G, E_A) onto (V, E).

If $E_A = \phi$, it is clear that $E = \phi$.

If $E_A \neq \phi$, then there exist $x, y \in G$ such that $(x, y) \in E_A$. Therefore there exists $a \in A$ such that $y = x \circ a$. Hence $A \neq \phi$. Let v be any element of V. Hence $v = x'\varphi$ for some $x' \in G$. Let $a' \in A$. Put $y' = x' \circ a'$. Hence $(x', y') \in E_A$. Let $u \in V$ such that $u = y'\varphi$. Therefore $(v, u) = (x'\varphi, y'\varphi) \in E$. Hence for each $v \in V$ there exists $u \in V$ such that $(v, u) \in E$.

Conversely, let (V, E) be a digraph such that $E = \phi$ or for each $v \in V$, there exists $u \in V$ such that $(v, u) \in E$.

Case 1 Suppose $E = \phi$. Let $\circ$ be any groupoid operation of V. Let $A = \phi$. Then $E_A = \phi$, and the identity mapping on V is a digraph isomorphism from (V, E) onto (V, E_A). Hence (V, E) is a groupoid digraph.

<u>Case 2</u> Suppose that for each $v \in V$ there exists $u \in V$ such that $(v, u) \in E$. Hence for each $v \in V$,

$$b(v) = \{ w \in V \mid (v, w) \in E \} \neq \phi .$$

Hence $d(v) = | b(v) |$ is a positive integer. Since $\{ d(v') \mid v' \in V \}$ is finite. Hence it has a maximum value.
Let $d = \max \{ d(v') \mid v' \in V \}$. Hence there exists $w \in V$ such that $d(w) = d$. Since $d(v') > 0$ for all $v' \in V$, hence $d > 0$.

For each $v \in V$, let $u_1(v), u_2(v), \ldots, u_{d(v)}(v)$ be the distinct elements of $b(v)$.

Put $$A = b(w) = \{ u_1(w), u_2(w), \ldots, u_d(w) \}$$

Define a binary operation $\circ$ on V as follows :

For each $v, u \in V$, we put

$$v \circ u = \begin{cases} u_i(v) & \text{if } u = u_i(w) \text{ and } 1 \leq i \leq d(v) \\ u_{d(v)}(v) & \text{for otherwise} . \end{cases}$$

Under this binary operation, $(V, \circ)$ is a groupoid.

We shall show that $E = E_A$.

Let $(v,u) \in E$. Hence $u \in b(v)$. Then $u = u_i(v)$ for some i, $1 \leq i \leq d(v)$. Since $v \circ u_i(w) = u_i(v)$, hence $v \circ u_i(w) = u$.
Therefore $(v, u) \in E_A$. That is $E \subseteq E_A$.

Conversely, let $(v, u) \in E_A$. Then there exists $u_j(w) \in A$ for some j, $1 \leq j \leq d$ such that $u = v \circ u_j(w)$. Since $v \circ u_j(w) = u_i(v)$ for some i, $1 \leq i \leq d(v)$, hence $u = u_i(v)$. Therefore $u \in \delta(v)$. That is $(v, u) \in E$. Hence $E_A \subseteq E$. Therefore $E = E_A$.

Hence (V, E) is a groupoid digraph.

Q.E.D.

3.6 Characterization of a Quasi - group Digraph.

Characterizations of quasi - group digraphs and loop digraphs were given by H.H. Teh [2]. To prove a theorem which characterizes a quasi - group digraph, we need the Hall's Representation Theorem [6] which states as follows.

3.6.1 Hall's Representation Theorem Let $S_1, S_2, \ldots, S_n$ be any finite system of subsets of a set S(S_i's need not be distinct). We can choose $a_i \in S_i$, $i = 1, 2, \ldots, n$ such that a_i's are distinct if and only if every k set of the subsets S_i contain among them at least k distinct elements.

3.6.2 Theorem Let (V, E) be a digraph. Then (V,E) is a quasi - group digraph if and only if (V, E) is a regular digraph.

<u>Proof</u>: Let (V,E) be a quasi - group digraph. Hence there exists a quasi - group$(G, \circ)$ and a subset A of G such that $(V, E) \cong (G, E_A)$. Let $\varphi : V \longrightarrow G$ be a digraph isomorphism from (V, E) onto (G, E_A). Since $(x, y) \in E_A$ if and only if $y = x \circ a$ for some $a \in A$. Hence for each $x \in G$, we have

$$\delta(x) = \left\{ y \in G \Big/ (x, y) \in E_A \right\} = \left\{ x \circ a \Big/ a \in A \right\}.$$

Observe that $\theta : A \longrightarrow \delta(x)$ defined by $a\theta = x \circ a$, for each $a \in A$ is a one - to - one onto . Hence we have $\left| \delta(x) \right| = \left| A \right|$. Similarly, for each x of G we have

$$\rho(x) = \left\{ y \in G \,\Big|\, (y, x) \in E_A \right\} = \left\{ x * a \Big/ a \in A \right\},$$

where $x * a$ denotes the solution y of $y \circ a = x$, and $\left| \rho(x) \right| = \left| A \right|$.

For each $v \in V$ we have $v\varphi = x$ for some $x \in G$. It follows from the digraph isomorphism property of φ that the restriction $\varphi / \delta(v)$, where

$$\delta(v) = \left\{ u \in V \,\Big|\, (v, u) \in E \right\},$$

is a one - to - one correspondence from $\delta(v)$ to $\delta(x)$. Hence $\left| \delta(v) \right| = \left| \delta(x) \right| = \left| A \right|$ for all $v \in V$. Similarly, we can show that $\left| \rho(v) \right| = \left| \rho(x) \right| = \left| A \right|$ for all $v \in V$. Here $\rho(v)$ is as usual, i.e. $\rho(v) = \left\{ u \in V \,\Big|\, (u, v) \in E \right\}$.

Hence (V, E) is regular of degree $\left| A \right|$.

Conversely, let (V, E) be a regular digraph of degree k say.

Case 1 : Suppose $k = 0$. Then $E = \phi$. Let o be any quasi - group operation of V. Let $A = \phi$. Then $E_A = \phi$, and the identity mapping on V is a digraph isomorphism from (V, E_A) onto (V, E). Hence (V, E) is a quasi - group digraph.

Case 2 : Suppose $k > 0$.

Let $V = \{v_1, v_2, \ldots, v_n\}$ and let $A = \{v_1, v_2, \ldots, v_k\}$.

Our object is to show that there exists at least one quasi - group operation o of V such that $E = E_A$.

Consider the following subsets of V,

(3.6.1) $\qquad b(v_1), b(v_2), \ldots, b(v_n)$.

Since (V, E) is a regular digraph of degree k, we have

$$|b(v_1)| = |b(v_2)| = \ldots = |b(v_n)| = k > 0 .$$

We shall show that for any m sets $b(v_{i_1}), b(v_{i_2}), \ldots, b(v_{i_m})$ contain at least m elements.

Since for each $v \in V$, $|\rho(v)| = k$, we see that v can belong to at most k members of $\{b(v_{i_1}), b(v_{i_2}), \ldots, b(v_{i_m})\}$.

Suppose $b(v_{i_1}) \cup b(v_{i_2}) \cup \ldots \cup b(v_{i_m}) = \{u_1, u_2, \ldots, u_p\}$ where $u_1, u_2, \ldots, u_p$ are distinct elements. Suppose u_j belongs to k_j members of $\{b(v_{i_1}), b(v_{i_2}), \ldots, b(v_{i_m})\}$ where $1 \leq j \leq p$.

Hence $k_j \leq k$ for $1 \leq j \leq p$. Therefore $\sum_{j=1}^{p} k_j \leq pk$

Since $\sum_{j=1}^{p} k_j = mk$, Hence $mk \leq pk$. Therefore $m \leq p$.

Hence $\left| \sigma(v_{i_1}) \cup \sigma(v_{i_2}) \cup \ldots \cup \sigma(v_{i_m}) \right| \geq m$.

Hence by theorem 3.6.1, there exists a complete set of distinct representatives for the system (3.6.1) say

$$(S_{11}, S_{21}, \ldots, S_{n1})$$

such that $S_{i1} \in \sigma(v_i)$ for $1 \leq i \leq n$, and $S_{p1} \neq S_{q1}$ when $p \neq q$.

Let $E' = E - \left\{ (v_1, S_{11}), (v_2, S_{21}), \ldots, (v_n, S_{n1}) \right\}$.

Claim that (V, E') is a regular digraph of degree $k - 1$.

Since $S_{i1} \in \sigma(v_i)$, hence $(v_i, S_{i1}) \in E$. Therefore $v_i \in \rho(S_{i1})$.

Hence we have $\left\{ S_{i1} \right\} \subseteq \sigma(v_i)$ and $\left\{ v_i \right\} \subseteq \rho(S_{i1})$.

Let $\sigma'(v_i) = \left\{ u \in V \;\middle|\; (v_i, u) \in E' \right\}$. For an arbitrary element $w \in V$, we have

$$w \in \sigma'(v_i) \iff (v_i, w) \in E'$$

$$\iff (v_i, w) \in E \text{ and } (v_i, w) \notin \left\{ (v_1, S_{11}), \ldots, (v_n, S_{n1}) \right\}$$

$$\iff w \in \sigma(v_i) \text{ and } w \notin \left\{ S_{i1} \right\}$$

$$\iff w \in \sigma(v_i) - \left\{ S_{i1} \right\}.$$

Hence $\sigma'(v_i) = \sigma(v_i) - \{S_{i1}\}$.

Similarly we can prove that

$$\rho'(S_{i1}) = \{u \in V \mid (u, S_{i1}) \in E'\} = \rho(S_{i1}) - \{v_i\}.$$

Hence $|\sigma'(v_i)| = k - 1$ and $|\rho'(S_{i1})| = k - 1$.

Since $\{S_{11}, S_{21}, \ldots, S_{n1}\} = \{v_1, v_2, \ldots, v_n\}$.

Therefore, for each $v_i \in V$,

$$|\sigma'(v_i)| = |\rho'(v_i)| = k - 1 .$$

Hence (V, E') is a regular digraph of degree $k - 1$.

Consider the following subsets of V,

(3.6.2) $\sigma'(v_1), \sigma'(v_2), \ldots, \sigma'(v_n)$.

If $k - 1 > 0$, then $\sigma'(v_i) \neq \phi$. By similar argument, we see that there exists a complete set of distinct representatives for the system (3.6.2) say

$$(S_{12}, S_{22}, \ldots, S_{n2})$$

such that $S_{i2} \in \sigma'(v_i) \subseteq \sigma(v_i)$ for $1 \leq i \leq n$ and $S_{p2} \neq S_{q2}$ when $p \neq q$.

As far as $k - (j - 1) > 0$ we may repeat and obtain for each j , $1 \leq j \leq k$ a permutation of V say

$$(S_{1j}, S_{2j}, \ldots, S_{nj})$$

such that $S_{ij} \in \delta(v_i)$ for $1 \leq i \leq n$, and $S_{pj} \neq S_{qj}$ when $p \neq q$.

Therefore, for each i, $1 \leq i \leq n$

$$\delta(v_i) = \left\{ S_{i1}, S_{i2}, \ldots, S_{ik} \right\}$$

such that $S_{il} \neq S_{im}$ when $l \neq m$.

Let $E^* = V \times V - E$.

By theorem 2.3.1, $(V, V \times V)$ is a regular digraph of degree n. Hence by theorem 2.3.2, (V, E^*) is a regular digraph of degree $n - k$.

If $n - k > 0$, then $\delta^*(v_i) \neq \phi$. By applying the forgoing argument to the regular digraph (V, E^*), we obtain for each $j = k + 1, k + 2, \ldots, n$ a permutation of V say

$$(S_{1j}, S_{2j}, \ldots, S_{nj})$$

such that $S_{ij} \in \delta^*(v_i)$, $1 \leq i \leq n$ and $S_{pj} \neq S_{qj}$ when $p \neq q$.
Therefore for each i, $1 \leq i \leq n$

$$\delta^*(v_i) = \left\{ S_{ik+1}, S_{ik+2}, \ldots, S_{in} \right\}$$

such that $S_{il} \neq S_{im}$ when $l \neq m$.

Hence $\delta(v_i) \cup \delta^*(v_i) = \left\{ S_{i1}, S_{i2}, \ldots, S_{in} \right\} = V$.

Define the binary operation $\circ$ on V as follows.

For each v_i, $v_j \in V$, we put

$$v_i \circ v_j = S_{ij} .$$

For each v_i, $v_j \in V$, if there exists v_r, $v_t \in V$ such that $v_i \circ v_r = v_j = v_i \circ v_t$, then $S_{ir} = S_{it}$, which would imply that $r = t$. Hence there exists a unique $v_r \in V$ such that $v_i \circ v_r = v_j$. Similarly, for each v_i, $v_j \in V$, there exists a unique $v_c \in V$ such that $v_c \circ v_i = v_j$. Therefore $(V, \circ)$ is a quasi - group.

Next we shall show that $E = E_A$.

Let $(u, v) \in E$. Hence $v \in \mathcal{b}(u)$. Since $u \in V$, then $u = v_i$ for some i, $1 \leq i \leq n$. Therefore $v \in \mathcal{b}(v_i)$. Thus $v = S_{ij}$ for some j, $1 \leq j \leq k$. Hence $v = v_i \circ v_j$ where $1 \leq j \leq k$. Since $v_j \in A$, hence $(v_i, v_i \circ v_j) \in E_A$. Therefore $(u, v) = (v_i, v_i \circ v_j) \in E_A$. Hence $E \subseteq E_A$.

Conversely, let $(u, v) \in E_A$. Then $v = u \circ v_j$ for some $v_j \in A$, $1 \leq j \leq k$. Since $u \in V$, hence $u = v_i$ for some i, $1 \leq i \leq n$. Hence $v = v_i \circ v_j = S_{ij}$ where $1 \leq j \leq k$. Thus $v \in \mathcal{b}(v_i)$. Therefore $(v_i, v) \in E$. Hence $(u, v) = (v_i, v) \in E$. Therefore $E_A \subseteq E$.

Hence $E = E_A$

Therefore (V, E) is a quasi - group digraph.

<u>Q.E.D.</u>

3.7 Characterization of a Loop Digraph

3.7.1 Theorem Let (V, E) be a digraph. Then (V, E) is a loop digraph if and only if (V, E) is a normal regular digraph.

Proof. Let (V, E) be a loop digraph. Hence there exists a loop $(G, \circ)$ and a subset A of G such that $(V, E) \cong (G, E_A)$.
Let $\varphi : V \to G$ be a digraph isomorphism from (V, E) onto (G, E_A). By the same argument as in the proof of theorem 3.6.2, we see that (V, E) is a regular digraph.

Let 1 denote the identity of G. Then either $1 \in A$ or $1 \notin A$.

Case 1 If $1 \in A$, then for each $x \in G$ we have $(x, x) = (x, x \circ 1) \in E_A$
Let v be any element of V. Hence $v\varphi = x_0$ for some $x_0 \in G$. Hence $(v\varphi, v\varphi) = (x_0, x_0) \in E_A$. Therefore $(v, v) \in E$. Hence (V, E) is a normal regular digraph.

Case 2 If $1 \notin A$. Suppose that $(v_0, v_0) \in E$ for some $v_0 \in V$. Hence $(v_0\varphi, v_0\varphi) \in E_A$. Therefore $v_0\varphi = v_0\varphi \circ a$ for some $a \in A$. Since 1 is the unique element in G such that $v_0\varphi = v_0\varphi \circ 1$. Therefore $a = 1$. Hence $1 \in A$, which is a contradiction. Therefore there does not exist $v_0 \in V$ such that $(v_0, v_0) \in E$. Hence (V, E) is a normal regular digraph.

Conversely, let (V, E) be a normal regular digraph of degree k say. First, we shall assume that $(v, v) \in E$ for each $v \in V$.

Case 1 Suppose $k = 1$. Hence $E = \{ (v, v) \mid v \in V \}$. Let $\circ$ be any loop operation on V. Let $A = \{ 1 \}$, where 1 denotes the identity of $(V, \bullet)$. Then $E_A = \{(v, v) \mid v \in V\}$, and the identity mapping on V is a digraph isomorphism from (V, E) onto (V, E_A). Hence (V, E) is a loop digraph.

Case 2. Suppose $k > 1$.

Let v_1 be any element of V.

Let $A = b(v_1) = \{ v_1, v_2, \ldots, v_k \}$ say.

Let $B = V - A = \{ v_{k+1}, v_{k+2}, \ldots, v_n \}$ say.

Then $V = \{ v_1, v_2, \ldots, v_k, v_{k+1}, \ldots v_n \} = A \cup B$.

Consider the following system of subsets of V,

(3.7.1) $b(v_1), b(v_2), \ldots, b(v_n)$.

Since $(v_i, v_i) \in E$ for each $i = 1, 2, \ldots, n$, therefore $v_i \in b(v_i)$. Hence $(v_1, v_2, \ldots, v_n)$ is a complete set of distinct representatives of the system (3.7.1). Let us rewrite

$$(v_1, v_2, \ldots, v_n) = (S_{11}, S_{21}, \ldots, S_{n1}).$$

That is, $v_i = S_{i1}$ for each $i = 1, 2, \ldots, n$.

By following the same argument used in the proof of theorem 3.6.2 we can construct another $k - 1$ permutations of V say

$(s_{12}, s_{22}, \ldots, s_{n2})$

$(s_{13}, s_{23}, \ldots, s_{n3})$

.

.

.

$(s_{1k}, s_{2k}, \ldots, s_{nk})$

such that

$$\sigma(v_1) = \{s_{11}, s_{12}, \ldots, s_{1k}\}$$
$$\sigma(v_2) = \{s_{21}, s_{22}, \ldots, s_{2k}\}$$

.

.

.

$$\sigma(v_n) = \{s_{n1}, s_{n2}, \ldots, s_{nk}\} .$$

Since $\{s_{12}, s_{13}, \ldots, s_{1k}\} = \{v_2, v_3, \ldots, v_k\}$, without loss of generality we may presume that

$$s_{12} = v_2 , \; s_{13} = v_3, \ldots, s_{1k} = v_k .$$

Now let $E^* = V \times V - E$. By theorem 2.3.1 and theorem 2.3.2, (V, E^*) is a regular digraph of degree $n - k$. By the same argument used before we can construct $n - k$ permutations of V say

$(S_{1k+1}, S_{2k+1}, \ldots, S_{nk+1})$

$(S_{1k+2}, S_{2k+2}, \ldots, S_{nk+2})$

.

.

.

$(S_{1n}, S_{2n}, \ldots, S_{nn})$,

such that for each $j = k+1, k+2, \ldots, n$,

$$b^*(v_j) = \{S_{jk+1}, S_{jk+2}, \ldots, S_{jn}\} = V - b(v_j).$$

Since $b^*(v_1) = V - b(v_1)$, then we have

$$\{S_{1k+1}, S_{1k+2}, \ldots, S_{1n}\} = \{v_{k+1}, v_{k+2}, \ldots, v_n\}.$$

Without loss of generality we may presume that

$$S_{1k+1} = v_{k+1}, S_{1k+2} = v_{k+2}, \ldots, S_{1n} = v_n .$$

Therefore, for each $j = 1, 2, \ldots, n$ we have $S_{1j} = v_j$.

Now define the binary operation $\circ$ in V as follows.

For each $v_i, v_j \in V$ we put

$$v_i \circ v_j = S_{ij}.$$

By the same proof as in theorem 3.6.2, $(V, \circ)$ is a quasi - group. Since $v_1 \circ v_j = S_{1j} = v_j$, and $v_i \circ v_1 = S_{i1} = v_i$. Hence v_1 is an identity of V. Therefore $(V, \circ)$ is a loop with v_1 as its identity.

By the same proof as in theorem 3.6.2, we have $E = E_A$.

Hence (V, E) is a loop digraph.

Now we shall assume that (V, E) is a normal regular digraph of degree k such that $(v, v) \notin E$ for every $v \in V$.

By hypothesis, $(v, v) \notin E$ for every $v \in V$. Hence $v \notin \sigma(v)$ and $v \notin \rho(v)$.

Let $E' = E \cup \{(v, v) \mid v \in V\}$.

Let $\sigma'(v) = \{u \in V \mid (v, u) \in E'\}$. For an arbitrary $w \in V$ we have

$$\begin{aligned} w \in \sigma'(v) &\iff (v, w) \in E' \\ &\iff (v, w) \in E \text{ or } (v, w) \in \{(v, v) \mid v \in V\} \\ &\iff w \in \sigma(v) \text{ or } w = v \\ &\iff w \in \sigma(v) \cup \{v\}. \end{aligned}$$

Hence $\sigma'(v) = \sigma(v) \cup \{v\}$.

Similarly we can prove that

$$\rho'(v) = \{u \in V \mid (u, v) \in E'\} = \rho(v) \cup \{v\}.$$

Hence $|\sigma'(v)| = k + 1$ and $|\rho'(v)| = k + 1$.

Therefore (V, E') is a normal regular digraph of degree k + 1 such that for every $v \in V$, $(v, v) \in E'$.

By the same proof used above, we get a loop $(V, \circ)$ with v_1 as its identity and have a subset A' of V such that $E' = E_{A'}$ where

$$E_{A'} = \left\{ (v, v \circ v') \; V \times V \;\middle|\; v \in V, v' \in A' \right\} .$$

Let $A = A' - \{ v_1 \}$.

Hence by theorem 3.3.2, we have

$$\begin{aligned} E_A &= E_{A'} - E_{\{v_1\}} \\ &= E_{A'} - \left\{ (v, v \circ v_1) \;\middle|\; v \in V \right\} \\ &= E_{A'} - \left\{ (v, v) \;\middle|\; v \in V \right\} \\ &= E' - \left\{ (v, v) \;\middle|\; v \in V \right\} . \end{aligned}$$

Since $(v, v) \notin E$ for any $v \in V$ and $E' = E \cup \left\{ (v, v) \;\middle|\; v \in V \right\}$,

hence $E' - \left\{ (v, v) \;\middle|\; v \in V \right\} = E$.

Therefore $E_A = E$.

Hence (V, E) is a loop digraph.

Q.E.D.