184. *Notes on Groupoids and their Automorphism Groups*

By Takayuki TAMURA
University of California, Davis, California, U.S.A.

(Comm. by Kenjiro SHODA, M.J.A., Nov. 13, 1967)

A groupoid is a set with a binary operation which need not be associative. The group of all automorphisms of a groupoid G is called the automorphism group of G and it is denoted by $\mathfrak{A}(G)$. Let $\mathfrak{S}(G)$ denote the symmetric group on the set G. In [2] the author determined the structure of G satisfying $\mathfrak{A}(G)=\mathfrak{S}(G)$. This paper supplements equivalent conditions to the theorem in case $|G|>4$, and adds some related results.

In [2] the author gave the following theorem.

Theorem 1. *Let G be a groupoid. $\mathfrak{A}(G)=\mathfrak{S}(G)$ if and only if G is either isomorphic or anti-isomorphic onto one on the following types*:

(1.1) *A right zero semigroup*: $xy=y$ *for all* x, y.

(1.2) *The idempotent quasigroup of order* 3.

(1.3) *The groupoid* $\{1, 2\}$ *of order* 2 *defined by*

$$x\cdot 1=2,\ x\cdot 2=1 \quad \textit{for } x=1, 2.$$

Before introducing the main theorem in this paper, we mention some remarks on the terminology (see [1]). We do not assume the finiteness of G.

By a finite permutation φ of a set G we mean a permutation φ of G such that the set $\{x \in G; x\varphi \neq x\}$ is finite. A permutation φ of G is called even if and only if φ is a finite permutation which is the product of even number of substitutions (i.e. cycles of length 2). An odd permutation is defined in a similar way. Let $\mathfrak{H}$ be a permutation group on G. Let k be a positive integer with $k \leqq |G|$. $\mathfrak{H}$ is called k-ply transitive if and only if for an arbitrary set of k distinct elements $a_1, \cdots, a_k$ and for an arbitrary set of k distinct elements $a'_1, \cdots, a'_k$, there is $\varphi \in \mathfrak{H}$ such that $a_i\varphi = a'_i$ for $i=1, \cdots, k$. Let $\mathfrak{B}(G)$ denote the group of all automorphisms and all anti-automorphisms of G. $\mathfrak{A}(G)$ is a subgroup of $\mathfrak{B}(G)$ and the index of $\mathfrak{A}(G)$ in $\mathfrak{B}(G)$ is 2. Let $\mathfrak{S}^*(G)$ denote the group of all finite permutations of G.

Theorem 2. *Let G be a groupoid with $|G|>4$. Then the following statements are equivalent.*

(2.1) A groupoid G is isomorphic onto either a right zero semigroup or a left zero semigroup.

(2.2) $\mathfrak{A}(G)=\mathfrak{S}(G)$.

(2.3) $\mathfrak{B}(G)=\mathfrak{S}(G)$.

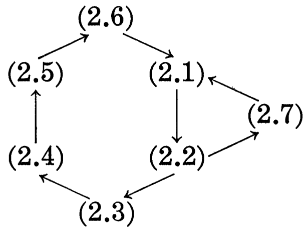
(2.4) $\mathfrak{S}^*(G)\subseteq\mathfrak{B}(G)$.

(2.5) Every even permutation of G is contained in $\mathfrak{A}(G)$.

(2.6) $\mathfrak{A}(G)$ is triply transitive.

(2.7) $\mathfrak{A}(G)$ is doubly transitive and there is $\varphi\in\mathfrak{A}(G)$ such that $a\varphi=a$, $b\varphi=b$ for some $a, b\in G$, $a\neq b$, but $x\varphi\neq x$ for all $x\neq a$, $x\neq b$.

Proof. The proof will be done in the following direction.



(2.1)$\to$(2.2) is given by Theorem 1; (2.2)$\to$(2.3) and (2.3)$\to$(2.4) are obvious.

Proof of (2.4)$\to$(2.5): By the assumption

(3) $\mathfrak{S}^*(G)=\overline{\mathfrak{A}(G)}\cup\overline{\mathfrak{A}'(G)}$ where

$\mathfrak{A}'(G)=\mathfrak{B}(G)\backslash\mathfrak{A}(G)$, $\overline{\mathfrak{A}(G)}=\mathfrak{A}(G)\cap\mathfrak{S}^*(G)$, $\overline{\mathfrak{A}'(G)}=\mathfrak{A}'(G)\cap\mathfrak{S}^*(G)$,

clearly $\overline{\mathfrak{A}(G)}\neq\phi$ but $\overline{\mathfrak{A}'(G)}$ could be empty. Also

(4) $\mathfrak{S}^*(G)=\mathcal{A}(G)\cup\mathcal{B}(G)$

where $\mathcal{A}(G)$ is the alternating group on G, namely, the group of all even permutations on G, and $\mathcal{B}(G)=\mathfrak{S}^*(G)\backslash\mathcal{A}(G)$. Since both $\overline{\mathfrak{A}(G)}$ and $\mathcal{A}(G)$ are[1] of index at most 2 in $\mathfrak{S}^*(G)$, they are normal subgroups of $\mathfrak{S}^*(G)$, and $\mathfrak{S}^*(G)=\mathcal{A}(G)\cdot\overline{\mathfrak{A}(G)}$. By the isomorphism theorem

$$\mathcal{A}(G)/\mathcal{A}(G)\cap\overline{\mathfrak{A}(G)}\cong\mathfrak{S}^*(G)/\overline{\mathfrak{A}(G)}\ .$$

Hence $\mathcal{A}(G)$ contains a normal subgroup $\mathcal{A}(G)\cap\overline{\mathfrak{A}(G)}$. On the other hand it is well known that $\mathcal{A}(G)$ is simple if $|G|\geqq 5$ (see p. 71 [1]) and that $|\mathcal{A}(G)|>2$ if $|G|\geqq 5$. Consequently $\mathcal{A}(G)=\mathcal{A}(G)\cap\overline{\mathfrak{A}(G)}$ or $\mathcal{A}(G)\subseteq\overline{\mathfrak{A}(G)}$. Moreover it holds that $\mathfrak{S}^*(G)=\overline{\mathfrak{A}(G)}$, or $\mathfrak{S}^*(G)\subseteq\mathfrak{A}(G)$.

Proof of (2.5)$\to$(2.6): Let a_1, a_2, a_3 be arbitrary distinct elements of G and b_1, b_2, b_3 be also arbitrary distinct in G. Let T be a subset of G such that $|T|=m$, $5\leq m<\infty$, and $\{a_1, a_2, a_3\}\cup\{b_1, b_2, b_3\}\subseteq T$. Let $\mathfrak{S}(T)$ be the subgroup (of $\mathfrak{S}(G)$) consisting of all permutations which fix each element outside T. $\mathfrak{S}(T)$ is isomorphic with the symmetric group of degree m. Let $\mathcal{A}(T)$ be the alternative group in $\mathfrak{S}(T)$. It is known that $\mathcal{A}(T)$ is $(m-2)$-ply transitive, hence triply

1) Strictly, $\overline{\mathfrak{A}(G)}$ is of index at most 2, but $\mathfrak{A}(G)$ is of index 2.

transitive. Hence there is $\varphi \in \mathcal{A}(T)$ such that $a_i\varphi = b_i (i=1, 2, 3)$. Since $\mathcal{A}(T) \subseteq \mathfrak{A}(G)$ by the assumption, we can find φ in $\mathfrak{A}(G)$. Thus we have (2.6).

Proof of (2.6)$\rightarrow$(2.1): To prove the idempotency of G, suppose $a^2 = b$ and $a \neq b$ for some $a, b \in G$. Let a, b, c, be three distinct elements of G. By the assumption there is an automorphism φ of G such that $a\varphi = a$, $b\varphi = c$. Applying φ to $a^2 = b$, we have $a^2 = c$. This is a contradiction since the binary operation is single-valued. Therefore $a^2 = a$ for all $a \in G$. Suppose $ab = c$ for some $a, b, c, a \neq b$, $a \neq c, b \neq c$. Let $d \neq a, d \neq b, d \neq c$. Consider an automorphism Ψ with $a\Psi = a$, $b\Psi = b$, $c\Psi = d$. Then Ψ transfers $ab = c$ to $ab = d$. This is also a contradiction. Hence we have proved $ab = a$ or b.

If $ab = a$, an automorphism $\begin{pmatrix} a, b, \cdots \\ x, b, \cdots \end{pmatrix}$[2], $b \neq x$, carries $ab = a$ to $xb = x, b \neq x$; and then $\begin{pmatrix} x, b, \cdots \\ x, y, \cdots \end{pmatrix}$, $x \neq y$, carries $xb = x$ to $xy = x, x \neq y$. Consequently we have $xy = x$ for all $x, y \in G$. Likewise $ab = b$ implies $xy = y$ for all $x, y \in G$.

Proof of (2.7)$\rightarrow$(2.1): By the double transitivity of $\mathfrak{A}(G)$, we have $a^2 = a$ for all $a \in G$. By the assumption there is an automorphism φ such that

$$a_0\varphi = a_0,\ b_0\varphi = b_0 \text{ for some } a_0, b_0, a_0 \neq b_0$$

and no other elements of G are fixed. On the other hand

$$(a_0b_0)\varphi = (a_0\varphi)(b_0\varphi) = a_0b_0$$

which implies that a_0b_0 is either a_0 or b_0. By the same arguments in the proof of (2.6)$\rightarrow$(2.1), we have $xy = x$ for all $x, y \in G$. Similarly $a_0b_0 = b_0$ implies $xy = y$ for all $x, y \in G$.

(2.2)$\rightarrow$(2.7) is obvious.

Thus the proof of the theorem has been completed.

Remark. In case $|G| = 4$, (2.1), (2.2), (2.6), and (2.7) are equivalent, and (2.3), (2.5), and (2.8) below are equivalent:

(2.8) G is a right zero semigroup, or a left zero semigroup or the idempotent quasigroup.[3] (see [3].)

In case $|G| = 3$, (2.2), (2.6), (2.7), and (2.8) are equivalent.

Theorem 3. *Let S be a set with $|S| \leqq 4$. For every subgroup $\mathfrak{H}$ of $\mathfrak{S}(S)$ there is at least one groupoid G defined on S such that $\mathfrak{A}(G) = \mathfrak{H}$.*

Theorem 3 is proved in [3] and the number of groupoids for each $\mathfrak{H}$ can by computed.

Combining Theorem 2 with Theorem 3, we have

Theorem 4. *For each subgroup $\mathfrak{H}$ of $\mathfrak{S}(S)$ there is at least a*

---

2) For convenience we use this notation although G need not be countable.

3) An idempotent quasigroup of order 4 or of order 3 is unique up to isomorphism.

groupoid G defined on S such that $\mathfrak{A}(G)=\mathfrak{H}$ if and only if $|S|\leqq 4$.

In fact there is no groupoid G for the alternating group $\mathfrak{H}$ if $|G|\geqq 5$. If we admit the well ordering theorem, we have

Theorem 5. *Let S be an infinite or finite set. There is a groupoid G defined on S such that $\mathfrak{A}(G)$ consists of the identical mapping alone.*

Proof. S can be well ordered, and let $\leq$ be the ordering. We define a binary operation on S as follows:

$$x\cdot y=\min\{x, y\}$$

Then we can prove there is no automorphism except the identical mapping by using the transfinite induction.

The following problem is raised:

Let S be a fixed set and $\mathfrak{H}$ be a permutation group on S, that is, $\mathfrak{H}\subseteq\mathfrak{S}(S)$. Under what condition on $\mathfrak{H}$ and S does there exist a groupoid G defined on S such that $\mathfrak{A}(G)=\mathfrak{H}$?

At the present time we can not completely solve this problem but, by Theorem 2, it is necessary that $\mathfrak{H}$ is not a triply transitive proper subgroup of $\mathfrak{S}(S)$.

Addendum. Let (2.5′) be the statement that $\mathfrak{S}^*(G)\subseteq\mathfrak{A}(G)$. As seen in the proof of (2.4)→(2.5), we have also (2.4)→(2.5′), while (2.5′)→(2.4) is obvious. Thus (2.5′) is also equivalent to each of (2.1) through (2.7).

References

[1] A. G. Kurosch: The Theory of Groups, Vol. 1 (Translation). Chelsea, New York (1960).

[2] T. Tamura: Some special groupoids. Math. Jap., **8**, 23-31 (1963).

[3] ——: Some contribution of computation to semigroups and groupoids. The proceeding of the conference on computational problems in abstract algebra (to appear).