

# Bridging the Group Definition Gap

Matthew G. Dawson<sup>†</sup>  
 Union University '08  
 Jackson, TN.

s285618@uu.edu  
 abc285618@gmail.com

## Abstract

In the early 1830s, a young French mathematician named Évariste Galois laid the foundations of group theory, although he never precisely defined groups. Galois studied groups in the context of sets of arrangements and his ideas were reformulated into a more abstract setting in the twentieth century. This paper provides precise definitions for constructs closely related to Galois's original notion of group theory and explores important group properties in that context, demonstrating that the modern concepts of the group, subgroup, normal subgroup, and solvable group can be expressed in terms of arrangement sets.

In the early nineteenth century, the theory of polynomials in a single variable was significantly advanced. Paolo Ruffini (1765–1822) discovered that the general quintic polynomial is not solvable by radicals and produced a nearly complete proof of this result. Niels Abel (1802–1829) was able to solve one of the greatest open questions of his day when he provided a correct and complete proof of Ruffini's discovery. A precocious French mathematician by the name of Evariste Galois (1811–1832) then made a surprisingly complete advancement, discovering a criterion that determines when a polynomial is solvable by radicals. Along the way, he stumbled upon the branch of mathematics now known as group theory. Galois associated groups with polynomial equations, showing that a polynomial equation is solvable by radicals when the associated group has a certain property now known as **solvability**.

Interestingly, although Galois was the first to study groups in the abstract setting, his concept of group bears no superficial resemblance to the more familiar definition that is found in modern textbooks. Today, a **group** is defined as a set, together with an associative binary operation, having both the **identity** and **inverse** properties.<sup>1</sup> Galois, however, thought of groups in the context of **arrangements**. A rigorous study of Galois's arrangement sets and their relation to modern group theory is not well known and is difficult to find, although such an exposition may be found in [Ti]. This paper reconciles the two definitions of group and studies the relationships between the two perspectives. Ultimately, we shall determine precisely how the modern definition of solvable group translates into Galois's terminology.

To begin our journey, we must provide precise definitions for the terminology that Galois used. First, we define the concept of arrangement key to Galois's formulation of group theory.

**Definition 1.** Given a nonempty finite set  $S$  of  $n$  elements, an **arrangement** of  $S$  is an  $n$ -tuple  $(a_1, a_2, \dots, a_n) \in S^n$  such that for every element  $s \in S$  there exists exactly one  $i$  such that  $a_i = s$ ,  $1 \leq i \leq n$ .

In addition, the set of all arrangements of a set  $S$  is denoted by  $\text{Arr}(S)$  and the set of all permutations on  $S$  is denoted by  $\text{Sym}(S)$ .

<sup>†</sup>Matthew Dawson, Union University '08, is a mathematics major who lives in Jackson, TN. Thanks to home education from his parents, he will be graduating four years early. In addition to mathematics, interests include physics, computer science, history, and music.

<sup>1</sup>That is, there is an identity element of the group and every element of the group has an inverse.

To illustrate this definition, let us consider a simple example. Suppose  $S = \{a, b, c\}$ . We list the elements of  $\text{Arr}(S)$ , denoting  $abc$  rather than  $(a, b, c)$  for brevity:

$$\text{Arr}(\{a, b, c\}) = \{abc, acb, bac, bca, cab, cba\}.$$

A **permutation** on  $S$  is simply a one-to-one correspondence mapping  $S$  into itself. Using the cyclic notation for permutations, we have that  $\text{Sym}(S) = \{(ab), (bc), (ac), (abc), (acb), \text{id}\}$ .

The power and versatility of arrangements is demonstrated by our first observation, which allows us to associate permutations on  $\text{Arr}(S)$  with permutations on  $S$ .

**Proposition 2.** *Let  $S$  be a finite set with  $n$  elements.*

1. *Let  $f \in \text{Sym}(S)$ , and consider the mapping  $P_f$  on  $\text{Arr}(S)$  such that for each arrangement  $\alpha = (a_1, a_2, a_3, \dots, a_n) \in \text{Arr}(S)$ ,*

$$P_f(\alpha) = (f(a_1), f(a_2), f(a_3), \dots, f(a_n)).$$

*Then  $P_f$  is a permutation on  $\text{Arr}(S)$ .*

2. *For all  $\alpha, \beta \in \text{Arr}(S)$ , there exists a unique permutation  $f \in \text{Sym}(S)$  such that  $P_f(\alpha) = \beta$ .*
3. *For all  $f, g \in \text{Sym}(S)$ ,  $P_f \circ P_g = P_{f \circ g}$ .*

The third part of Proposition 2 establishes that the map  $f \mapsto P_f$  is a homomorphism from  $\text{Sym}(S)$  to  $\{P_f \mid f \in \text{Sym}(S)\} \subset \text{Sym}(\text{Arr}(S))$ ; the second part tells us that it is an isomorphism; that is,  $P_f = P_g$  if and only if  $f = g$ .

The fact that such an isomorphism exists should not be surprising, when Cayley’s Theorem is considered: clearly, if a set  $S$  has  $n$  elements, then  $|\text{Sym}(S)| = n!$  and  $|\text{Arr}(S)| = n!$ . Cayley’s theorem tells us that because  $\text{Sym}(S)$  has  $n!$  elements, it will be isomorphic to a subgroup of  $S_{n!}$ . Since  $\text{Sym}(\text{Arr}(S))$  is isomorphic to  $S_{n!}$ , we see that there must be an isomorphism between  $\text{Sym}(S)$  and some subgroup of  $\text{Sym}(\text{Arr}(S))$ .

Proposition 2 assures us that the permutations in  $\text{Sym}(S)$  can be applied to arrangements in  $\text{Arr}(S)$  in a well-behaved fashion. Indeed, Proposition 2 sets up a group action of  $\text{Sym}(S)$  on  $\text{Arr}(S)$ . It does so because the map  $f \mapsto P_f$  is a homomorphism from  $\text{Sym}(S)$  to  $\text{Sym}(\text{Arr}(S))$ . Furthermore, the second part of Proposition 2 implies that the homomorphism is one-to-one, so that the group action is **faithful**.

**Corollary 3.** *Let  $S$  be a finite set. Then the mapping  $P : \text{Sym}(S) \rightarrow \text{Sym}(\text{Arr}(S))$  given by  $P(f) = P_f$  is a faithful action of  $\text{Sym}(S)$  on  $\text{Arr}(S)$ .*

Henceforth, we will drop the notation  $P_f$  and instead use the same notation to denote a permutation on  $S$  and the corresponding permutation on  $\text{Arr}(S)$ . In addition, we will denote function composition by juxtaposition.

Now that a group action has been set up, the concept of orbit may be discussed. The reader may recall that, given a group  $G$ , a set  $M$ , and an action of  $G$  on  $M$ , the orbit of  $m \in M$  is defined to be  $G(m) = \{g(m) \mid g \in G\}$ .

Now, if a set  $S$  and an arrangement  $\alpha \in \text{Arr}(S)$  are considered, then the orbit of  $\alpha$  is  $\text{Arr}(S)$  (that is,  $(\text{Sym}(S))(\alpha) = \text{Arr}(S)$ ). We know this by part two of Proposition 2, which tells us that given any arrangement in  $\text{Arr}(S)$ , we can find a permutation in  $\text{Sym}(S)$  that will map  $\alpha$  to that arrangement.

A more general concept similar to that of orbit will be quite useful in this paper; we need to consider the application of subsets of  $\text{Sym}(S)$  on a single arrangement.

**Definition 4.** Let  $S$  be a nonempty finite set and let  $H \subseteq \text{Sym}(S)$ . Then for all arrangements  $\alpha \in \text{Arr}(S)$ , we define  $H(\alpha) = \{f(\alpha) \mid f \in H\}$ .

To illustrate this definition, let  $H = \{\text{id}, (abc), (acb), (ac)\}$ . In this case, we have

$$H(abc) = \{abc, bca, cab, cba\}.$$

Now suppose we are given a finite set  $S$ , an arrangement  $\alpha$  of  $S$ , and a set  $M$  of arrangements of  $S$ . We define:

**Definition 5.** Let  $S$  be a nonempty finite set, let  $C \subseteq \text{Arr}(S)$ , and let  $\alpha \in C$ . Then the **permutation set** of  $\alpha$  in  $C$ , denoted  $\bowtie_\alpha(C)$ , is the set

$$\bowtie_\alpha(C) = \{f \in \text{Sym}(S) \mid f(\alpha) \in C\}.$$

Let us go back to our previous example, where  $S = \{a, b, c\}$ ,  $C = \{abc, bca, cab, cba\}$ , and  $\alpha = abc$ . Then  $\bowtie_\alpha(C)$  will be the set of all permutations that map  $abc$  to some arrangement in  $C$ . The reader can check that  $\bowtie_\alpha(C) = \{\text{id}, (abc), (acb), (ac)\}$ .

As suggested above, the  $\bowtie_\alpha(C)$  construction is the inverse of the  $H(\alpha)$  construction. We state this formally in the following lemma.

**Lemma 6.** Let  $S$  be a nonempty finite set, let  $H \subseteq \text{Sym}(S)$  and  $M \subseteq \text{Arr}(S)$ , and let  $\alpha \in M$ . Then  $H(\alpha) = M$  if and only if  $H = \bowtie_\alpha(M)$ .

*Proof.* First suppose that  $H(\alpha) = M$ . We wish to show that  $H = \bowtie_\alpha(M)$ . Let  $f \in H$ . Then  $f(\alpha) \in H(\alpha) = M$  and hence  $f \in \bowtie_\alpha(M)$ . Thus,  $H \subseteq \bowtie_\alpha(M)$ .

Next let  $h \in \bowtie_\alpha(M)$ . Thus  $h(\alpha) \in M = H(\alpha)$ , so that  $h(\alpha) = f(\alpha)$  for some  $f \in H$ . Therefore, by Proposition 2, we know that  $h = f$ , so that  $h \in H$ . Hence,  $\bowtie_\alpha(M) \subseteq H$ . Thus,  $H = \bowtie_\alpha(M)$ .

To prove the other half of the biconditional, suppose that  $H = \bowtie_\alpha(M)$ . We must show that  $H(\alpha) = M$ . Let  $\beta \in H(\alpha)$ , so that  $\beta = f(\alpha)$  for some  $f \in H = \bowtie_\alpha(M)$ . Now  $f \in \bowtie_\alpha(M)$  implies that  $\beta = f(\alpha) \in M$ . Thus  $H(\alpha) \subseteq M$ .

Finally let  $\beta \in M$ . Then by Proposition 2,  $\beta = g(\alpha)$  for some  $g \in \text{Sym}(S)$ . Clearly  $g \in \bowtie_\alpha(M) = H$ . Thus,  $g \in H$  implies that  $\beta = g(\alpha) \in H(\alpha)$ .  $\square$

So far, we have associated a permutation set with each pair  $(\alpha, M)$  where  $\alpha$  is an arrangement and  $M$  is an arrangement set. We can also define a permutation set directly associated to a given arrangement set.

**Definition 7.** Let  $S$  be a nonempty finite set, and let  $C \subseteq \text{Arr}(S)$ . Then the **total permutation set** associated with  $C$  (or total permutation set of  $C$ ),  $\bowtie(C)$ , is the set

$$\bowtie(C) = \{f \in \text{Sym}(S) \mid \exists \alpha \in C \text{ such that } f(\alpha) \in C\}.$$

By checking the relevant definitions, we see that

$$\bowtie(C) = \bigcup_{\alpha \in C} \bowtie_\alpha(C).$$

Hence, we have that  $\bowtie_\alpha(C) \subseteq \bowtie(C)$  for all  $\alpha \in C$ .

As before, an example will help to illustrate the definition. We consider again  $C = \{abc, bca, cab, cba\}$ . Then,

$$\begin{aligned} \bowtie(C) &= \bowtie_{abc}(C) \cup \bowtie_{bca}(C) \cup \bowtie_{cab}(C) \cup \bowtie_{cba}(C) \\ &= \{\text{id}, (abc), (acb), (ac), (ab), (bc)\} = \text{Sym}(S). \end{aligned}$$

Now that we can associate permutation sets with arrangement sets, we are ready to study the implications of those associated permutation sets having special properties, the most important of which is described in our next definition.

**Definition 8.** A set  $C$  of arrangements of a nonempty finite set  $S$  is a **Galois Set of Arrangements** (or **GSA**) if for all  $f \in \bowtie(C)$ ,  $\alpha \in C$  implies  $f(\alpha) \in C$ .

The above definition lays out the single most important concept in this paper, which is a close approximation to Galois’s original concept of the group. Recall that the more familiar definition states that a group is a set of objects with an associative binary operation such that the set has an identity element and contains inverses for every element in the set. Galois sets of arrangements bear no immediate resemblance to this algebraic structure. However, these two concepts are closely related. We shall soon see that the connection between GSAs and algebraic groups arises through the permutation sets associated with GSAs.

Before moving any further, let us determine whether  $C = \{abc, bca, cab, cba\}$  is a GSA. First recall that  $\bowtie(C) = \{\text{id}, (abc), (acb), (ac), (ab), (bc)\} = \text{Sym}(S)$ . In order for  $C$  to be a GSA, it must be the case that each permutation  $g \in \bowtie(C)$  maps every arrangement in  $C$  to another arrangement in  $C$ . Consider  $f = (ab)$ , which is an element of  $\bowtie(C)$ . Now  $f(abc) = bac$ , and  $bac \notin C$ . Therefore, because  $f = (ab) \in \bowtie(C)$  yet  $abc \in C$  and  $f(abc) \notin C$ , we see that  $C$  cannot be a GSA.

Let us consider another example: suppose that  $M = \{abc, acb\}$ . We shall first list out all of the elements of  $\bowtie(M)$ .

$$abc \xrightarrow{\text{id}} abc \quad abc \xrightarrow{(bc)} acb \quad acb \xrightarrow{(bc)} abc \quad acb \xrightarrow{\text{id}} acb$$

Hence  $\bowtie(M) = \{\text{id}, (bc)\}$ . Because all the permutations in  $\bowtie(M)$  map both  $abc$  and  $acb$  to either  $abc$  or  $acb$  (this fact can be checked by examining the above diagram), we have that  $M$  is a GSA.

The reader may have noticed that  $\bowtie_{abc}(M) = \bowtie_{acb}(M) = \bowtie(M)$ . The reader may also have noticed that  $\bowtie_{abc}(M)$  forms a group of permutations in the modern sense. These observations lead us to an interesting, general result.

**Lemma 9.** *If  $C$  is a set of arrangements of a finite set and  $\alpha \in C$  is such that  $\bowtie_{\alpha}(C)$  forms a group under composition, then  $\bowtie_{\alpha}(C) = \bowtie(C)$ .*

*Proof.* Suppose that  $\alpha \in C$  such that  $\bowtie_{\alpha}(C)$  forms a group under composition. First we show that  $\bowtie(C) \subseteq \bowtie_{\alpha}(C)$ . Let  $f \in \bowtie(C)$ . Then by definition of the associated permutation set, there exist  $\beta, \gamma \in C$  such that  $f(\beta) = \gamma$ . By Proposition 2, there exists exactly one permutation  $g \in \text{Sym}(S)$  such that  $g(\alpha) = \beta$ , and there exists exactly one permutation  $h \in \text{Sym}(S)$  such that  $h(\alpha) = \gamma$ . Note that by the definition of the permutation set of  $\alpha$  in  $C$ ,  $g \in \bowtie_{\alpha}(C)$  and  $h \in \bowtie_{\alpha}(C)$ . Consider the permutation  $hg^{-1}$ :

$$(hg^{-1})(\beta) = h(g^{-1}(\beta)) = h(g^{-1}(g(\alpha))) = h(\alpha) = \gamma.$$

By Proposition 2, there exists exactly one permutation  $f$  such that  $f(\beta) = \gamma$ . Thus we have  $f = hg^{-1}$ . But because  $\bowtie_{\alpha}(C)$  forms a group under composition, we know that  $hg^{-1} \in \bowtie_{\alpha}(C)$ . Hence  $f \in \bowtie_{\alpha}(C)$ . Thus,  $\bowtie(C) \subseteq \bowtie_{\alpha}(C)$ .

By the definition of  $\bowtie(C)$ , it is clear that  $\bowtie_{\alpha}(C) \subseteq \bowtie(C)$ . Therefore, we have that  $\bowtie_{\alpha}(C) = \bowtie(C)$ .  $\square$

With this last result, we have developed all of the necessary tools to establish the connection between groups and GSAs.

**Theorem 10.** *Let  $S$  be a nonempty finite set, let  $C \subseteq \text{Arr}(S)$ , and let  $\alpha \in C$ . Then  $C$  is a Galois Set of Arrangements if and only if  $\bowtie_{\alpha}(C)$  forms a group under composition.*

*Proof.* Suppose that  $C$  is a Galois Set of Arrangements. Then, for all  $f \in \bowtie(C)$ ,  $f(\beta) \in C$  for all  $\beta \in C$ . We wish to show that  $\bowtie_{\alpha}(C)$  forms a group with respect to function composition.

Let  $f, g \in \bowtie_{\alpha}(C)$ . Thus  $g(\alpha) \in C$ . Also,  $C$  is a GSA, so that  $f(\beta) \in C$  for all  $\beta \in C$ . It follows that  $(fg)(\alpha) = f(g(\alpha)) \in C$ . Therefore, by the definition of the permutation set of  $\alpha$  in  $C$ ,  $fg \in \bowtie_{\alpha}(C)$ . Hence  $\bowtie_{\alpha}(C)$  is closed under composition.

Now consider the identity permutation  $\text{id} : S \rightarrow S$ . Then  $\text{id}(\alpha) = \alpha$ , so that  $\text{id} \in \bowtie_{\alpha}(C)$ . Recall that, since  $\text{id}$  is the identity permutation,  $\text{id} \circ f = f \circ \text{id} = f$  for all permutations  $f \in \text{Sym}(S)$ . Therefore, the set  $\bowtie_{\alpha}(C)$  contains an identity element.

Next let  $f \in \bowtie_{\alpha}(C)$ . Then by the definition of the permutation set of  $\alpha$  in  $C$ ,  $f(\alpha) = \gamma$  for some  $\gamma \in C$ . Now  $f^{-1}(\gamma) = \alpha$  (recall that  $f$  is a permutation, so that  $f^{-1}$  exists), so that

$f^{-1} \in \bowtie(C)$ . Thus, since  $C$  is a GSA,  $f^{-1}(\beta) \in C$  for all  $\beta \in C$ . Hence,  $f^{-1}(\alpha) \in C$  so that  $f^{-1} \in \bowtie_\alpha(C)$ . Thus,  $\bowtie_\alpha(C)$  contains an inverse for each element, whence  $\bowtie_\alpha(C)$  forms a group with respect to function composition.

By Lemma 9 we know that  $\bowtie_\alpha(C) = \bowtie(C)$ . We wish to show that  $C$  is a GSA. Let  $f \in \bowtie(C)$ . In order to show that  $C$  is a GSA, we must show that  $f(\beta) \in C$  for all  $\beta \in C$ . Now  $f \in \bowtie_\alpha(C)$ , since  $\bowtie_\alpha(C) = \bowtie(C)$ . Next let  $\beta \in C$ . By Proposition 2, there exists exactly one permutation  $h : S \rightarrow S$  such that  $h(\alpha) = \beta$ . Clearly,  $h \in \bowtie_\alpha(C)$ . But  $\bowtie_\alpha(C)$  forms a group under composition, so that  $fh \in \bowtie_\alpha(C)$ . In other words,  $(fh)(\alpha) = f(h(\alpha)) = f(\beta) \in C$ . Therefore,  $C$  is a GSA.  $\square$

Let us look at Theorem 10 in light of the examples we have used so far. For the set  $C = \{abc, bca, cab, cba\}$ , we recall that  $\bowtie_{abc}(C) = \{\text{id}, (abc), (acb), (ac)\}$ . Now,  $\bowtie_{abc}(C)$  is not a group. Therefore, Theorem 10 tells us that  $C$  is not a GSA, confirming our earlier observation. Also, for  $M = \{abc, acb\}$ , we saw that  $\bowtie_{abc}(M)$  is a group. Theorem 10 then tells us that  $M$  is a GSA, as we determined above.

It should be noted that Theorem 10 finishes the task of reconciling the two group definitions. A set  $C$  of arrangements is a Galois set of arrangements if and only if at least one of the permutations sets of an arrangement in  $C$  is a group. Theorem 10 also implies that if  $C$  forms a GSA, then  $\bowtie_\alpha(C)$  forms a group for each  $\alpha \in C$ .

Now, we suppose that  $\bowtie_\alpha(C)$  forms a group with respect to function composition. Lemma 9 then guarantees that  $\bowtie_\alpha(C) = \bowtie(C)$ , so that  $\bowtie(C)$  is a group. Thus, if  $C$  is a GSA, then the total associated permutation set of  $C$  is a group. The converse, however, is not true—the total permutation set of  $C$  may be a group even if  $C$  is not a GSA. For instance, we showed that  $C = \{abc, bca, cab, cba\}$  is not a GSA and also determined that  $\bowtie(C) = \text{Sym}(S)$ . From group theory, we know that  $\text{Sym}(S)$  is a group that is isomorphic to  $S_3$ .

Our next priority is to determine how **solvability** translates to the language of permutation sets. Before doing that, we state a few more results and give one more definition.

**Lemma 11.** *Let  $S$  be a nonempty finite set, let  $H \subseteq \text{Sym}(S)$ , and let  $M$  be a GSA of  $S$ . Then for all  $\alpha \in M$ ,  $H(\alpha) = M$  if and only if  $H = \bowtie(M)$ .*

**Lemma 12.** *Let  $T$  and  $V$  be sets of permutations of a finite set  $S$ , and let  $\alpha$  be an arrangement of  $S$ . Then  $T(\alpha) = V(\alpha)$  if and only if  $T = V$ .*

We have already studied how to apply a permutation set to an arrangement. Next, we shall define the application of a single permutation to an arrangement set.

**Definition 13.** Let  $S$  be a nonempty finite set, and let  $M \subseteq \text{Arr}(S)$ . Then for all permutations  $g \in \text{Sym}(S)$ , we define  $g(M) = \{g(\gamma) \mid \gamma \in M\}$ .

To illustrate the above definition, let  $M = \{abc, acb\}$  and  $g = (ab)$  and consider the following diagram:

$$\begin{array}{l} abc \xrightarrow{(ab)} bac \\ acb \xrightarrow{(ab)} bca \end{array}$$

Then, we see that  $g(M) = \{bac, bca\}$ .

In what follows, we respectively denote  $gH$  and  $Hg$  for the **left and right cosets** of  $H \subset G$  in  $G$  associated to  $g \in G$ .

**Theorem 14.** *Let  $N$  be a GSA of a finite set  $S$ , and let  $H = \bowtie(N)$ . Then for all permutations  $g \in \text{Sym}(S)$ ,*

1. *The set  $g(N)$  is a GSA of  $S$  and  $\bowtie(g(N)) = gHg^{-1}$*
2. *For all  $\alpha \in N$ ,  $g(N) = g(H(\alpha)) = (gH)(\alpha)$ .*

*Proof.* First we prove the first statement. Let  $\alpha \in N$  and let  $g \in \text{Sym}(S)$ . Note that because  $N$  is a GSA of  $S$ , Theorem 11 assures us that  $N = H(\alpha)$ . Let  $\beta = g(\alpha)$ . We first show that  $\bowtie_{\beta}(g(N)) = gHg^{-1}$ .

Let  $k \in \bowtie_{\beta}(g(N))$ . Thus,  $k(\beta) = \gamma$  for some  $\gamma \in g(N)$ . Now,  $\gamma = g(\delta)$  for some  $\delta \in N$ . But  $N = H(\alpha)$ , so that  $\delta = h(\alpha)$  for some  $h \in H$ . Thus  $k(\beta) = g(h(\alpha))$ . But  $\alpha = g^{-1}(\beta)$ , whence  $k(\beta) = g(h(g^{-1}(\beta)))$ . Therefore, by Proposition 2, we have  $k = ghg^{-1}$ . Hence,  $\bowtie_{\beta}(g(N)) \subseteq gHg^{-1}$ .

Next let  $h \in H$  and consider  $ghg^{-1} \in gHg^{-1}$ . Then  $(ghg^{-1})(\beta) = (ghg^{-1})(g(\alpha)) = g(h(\alpha)) \in g(N)$ . Hence,  $ghg^{-1} \in \bowtie_{\beta}(g(N))$ . Thus,  $gHg^{-1} \subseteq \bowtie_{\beta}(g(N))$ .

Therefore,  $\bowtie_{\beta}(g(N)) = gHg^{-1}$ . As  $H$  is a group under composition, so is  $gHg^{-1}$ . Thus, by Theorem 10,  $g(N)$  is a GSA. Now, we suppose that  $\bowtie_{\alpha}(C)$  forms a group with respect to function composition. By Lemma 9 we know that  $\bowtie(g(N)) = gHg^{-1}$ .

Next, we prove the second component of the theorem. Let  $g \in \text{Sym}(S)$  and  $\alpha \in N$ . By Theorem 11,  $N = H(\alpha)$ , so that  $g(N) = g(H(\alpha))$ . It remains to show that  $g(N) = (gH)(\alpha)$ . Thus, suppose  $h \in H$  and consider  $gh \in gH$ . Note that  $(gh)(\alpha) = g(h(\alpha))$  and that  $h(\alpha) \in N$ . Thus,  $g(h(\alpha)) \in g(N)$ , whence  $(gH)(\alpha) \subseteq g(N)$ . Next, let  $\beta \in g(N)$ . Then,  $\beta = g(\gamma)$  for some  $\gamma \in N$  and so  $\gamma = h(\alpha)$  for some  $h \in H$ . Thus,  $\beta = g(h(\alpha)) = (gh)(\alpha)$ , whence  $g(N) \subseteq (gH)(\alpha)$ , whereby  $g(N) = (gH)(\alpha)$ .  $\square$

A few simple observations follow directly from Theorem 14. First, applying a permutation to a GSA yields another GSA. Next, the associated permutation set of the resulting GSA is a conjugate group of the associated permutation set of the original GSA. Finally, in the second part of Theorem 14, we see that the GSA obtained by applying a single permutation to a GSA can be obtained by applying a left coset of the original GSA's associated permutation set to an arrangement in the original GSA.

Thus, the application of a permutation to a GSA results in a GSA that captures the notions of conjugate groups and left cosets. Rigatelli [Ri, p. 124] noticed that Galois referred to cosets as “groups,” suggesting that the use of this word might confuse people attempting to understand his work. Perhaps Theorem 14 sheds some light on this issue: the application to an arrangement of the left coset of a permutation group results in a GSA, which is what Galois would call a “group.”

We also state a result similar to Theorem 14, which relates right cosets to the application of a permutation group to an arrangement.

**Theorem 15.** *Let  $N$  be a GSA of a finite set  $S$ , let  $H = \bowtie(N)$ , and let  $\alpha \in N$ . Then for all  $g \in \text{Sym}(S)$ ,  $H(g(\alpha)) = (Hg)(\alpha)$ .*

Before we can study solvability, we must first study **normal subgroups**. To that end, we shall refine our focus and work more specifically towards establishing a criterion which determines when a given GSA has an associated permutation set that is a normal subgroup of the permutation set of another GSA.

A question immediately arises: if one GSA is a subset of another GSA, is the permutation set of the former GSA a subgroup of the permutation set of the latter GSA? That is, suppose that  $M$  and  $N$  are GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ . One would expect that, since  $N \subseteq M$ , it must be true that  $H \leq G$  as groups. To establish the truth of this statement, suppose that  $f \in H$ . Then, there exists  $\alpha \in N$  such that  $f(\alpha) \in N$ . Since  $N \subseteq M$ , we have that  $f(\alpha) \in M$ . Thus, by definition of total associated permutation set,  $f \in G$ . Thus,  $H \subseteq G$ . Because  $M$  and  $N$  are GSAs, we know by Lemma 9 and Theorem 10 that  $G$  and  $H$  form groups. Therefore,  $H \leq G$ .

In order to establish a criterion that establishes when GSAs have associated permutation sets where one is a normal subgroup of the other, we need three lemmas and an intermediate theorem. The proofs of the lemmas are straightforward.

**Lemma 16.** *Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ . Then for all  $g \in G$  and  $\alpha \in N$ ,  $(Hg)(\alpha) \subseteq M$  and  $(gH)(\alpha) \subseteq M$ .*

**Lemma 17.** *Let  $M$  and  $N$  be GSAs of a finite set  $S$  such that  $N \subseteq M$ , let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ , and let  $\alpha \in N$ . Then, the following equalities hold:*

1.  $\{H(\beta) \mid \beta \in M\} = \{(Hg)(\alpha) \mid g \in G\}$
2.  $\{g(N) \mid g \in G\} = \{(gH)(\alpha) \mid g \in G\}$ .

**Lemma 18.** *Let  $S$  be a finite set, let  $A \subset \text{Arr}(S)$  and  $B \subset \text{Arr}(S)$ , and let  $\alpha \in \text{Arr}(S)$ . Then  $(A \cap B)(\alpha) = A(\alpha) \cap B(\alpha)$  and  $(A \cup B)(\alpha) = A(\alpha) \cup B(\alpha)$ .*

**Theorem 19.** *Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ . Then, the following sets are partitions of  $M$ :*

$$P_R(M, N) = \{H(\beta) \mid \beta \in M\},$$

$$P_L(M, N) = \{g(N) \mid g \in G\}.$$

*These sets are known, respectively, as the **right and left partitions of  $M$  by  $N$** .*

*Proof.* We must show that the sets  $P_R(M, N)$  and  $P_L(M, N)$  are partitions of  $M$ . By Lemma 17, we know that for all  $\alpha \in N$ ,  $P_R(M, N) = \{(Hg)(\alpha) \mid g \in G\}$  and  $P_L(M, N) = \{(gH)(\alpha) \mid g \in G\}$ .

We know from group theory that  $\{gH \mid g \in G\}$  forms a partition of  $G$  and that  $\{Hg \mid g \in G\}$  forms a partition of  $G$ . Hence, for all  $f, g \in G$ ,  $fH \cap gH = \emptyset$  and  $Hf \cap Hg = \emptyset$ . Also,  $G = \cup_{g \in G} gH$  and  $G = \cup_{g \in G} Hg$ .

Let  $f, g \in G$ . Then, we have by Lemma 18 that  $(fH)(\alpha) \cap (gH)(\alpha) = (fH \cap gH)(\alpha) = (\emptyset)(\alpha) = \emptyset$ . Similarly,  $(Hf)(\alpha) \cap (Hg)(\alpha) = (Hf \cap Hg)(\alpha) = (\emptyset)(\alpha) = \emptyset$ . Hence,  $P_L(M, N)$  and  $P_R(M, N)$  are pairwise disjoint.

Finally, Lemma 18 implies that  $\cup_{g \in G} ((gH)(\alpha)) = (\cup_{g \in G} gH)(\alpha) = G(\alpha) = M$ . Similarly,  $\cup_{g \in G} ((Hg)(\alpha)) = (\cup_{g \in G} Hg)(\alpha) = G(\alpha) = M$ . Since we know by Lemma 16 that  $gH \subset M$  and  $Hg \subset M$  for all  $g \in G$ , we have that  $P_L(M, N)$  and  $P_R(M, N)$  are partitions of  $M$ .  $\square$

As an example, let  $M = \{abc, acb, bac, bca, cab, cba\}$  and let  $N = \{abc, acb\}$ . Note that  $M$  and  $N$  are both GSAs. Now, let  $H = \bowtie(N) = \{\text{id}, (bc)\}$ . Then,  $H(abc) = \{abc, acb\} = N$  and  $H(bac) = \{bac, cab\}$  and  $H(cba) = \{cba, bca\}$ . Note that

$$\{H(abc), H(bac), H(cba)\} = \{\{abc, acb\}, \{bac, cab\}, \{cba, bca\}\}$$

forms a partition of  $M$ . This partition is the right partition of  $M$  by  $N$ , denoted  $P_R(M, N)$ .

Also, note that  $[\text{id}](N) = N = \{abc, acb\}$ ,  $[(ac)](N) = \{cba, cab\}$ , and  $[(ab)](N) = \{bac, bca\}$ . The reader can check that  $\{[\text{id}](N), [(ac)](N), [(ab)](N)\}$  forms a partition of  $M$ . This partition is the left partition of  $M$  by  $N$ , denoted  $P_L(M, N)$ . With this notation, we now continue.

**Theorem 20.** *Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ . Then  $H \triangleleft G$  if and only if  $P_L(M, N) = P_R(M, N)$ .*

*If  $H \triangleleft G$ , we shall say that  $N$  is a **normal subset of  $M$** .*

*Proof.* Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ . First, we show that  $H \triangleleft G$  implies  $P_L(M, N) = P_R(M, N)$ . Thus, suppose that  $H \triangleleft G$ . Then  $Hg = gH$  for all  $g \in G$ , so that by Lemma 12,  $(Hg)(\alpha) = (gH)(\alpha)$  for all  $\alpha \in N$ ,  $g \in G$ . Suppose that  $(Hg)(\alpha) \in P_R(M, N)$ , for some  $g \in G$ ,  $\alpha \in N$ ; then,  $(Hg)(\alpha) = (gH)(\alpha) \in P_L(M, N)$ . Similarly, suppose that  $(gH)(\alpha) \in P_L(M, N)$ , for some  $g \in G$ ,  $\alpha \in N$ ; thus  $(gH)(\alpha) = (Hg)(\alpha) \in P_R(M, N)$ . Hence,  $P_R(M, N) = P_L(M, N)$ .

Next, suppose that  $P_L(M, N) = P_R(M, N)$ . Then for all  $g \in G$ ,  $\alpha \in N$ , we know that  $(gH)(\alpha) \in P_L(M, N)$  and hence  $(gH)(\alpha) \in P_R(M, N)$ . Therefore, there exists  $\beta \in M$  such that  $(gH)(\alpha) = H(\beta)$ . Now Theorem 14 tells us that  $(gH)(\alpha)$  is a GSA and that  $\bowtie((gH)(\alpha)) = gHg^{-1}$ . Thus, by Theorem 11, we know that  $(gH)(\alpha) = (gHg^{-1})(\gamma)$  for all  $\gamma \in (gH)(\alpha) = H(\beta)$ . Therefore, since  $\beta \in H(\beta)$  (recall that  $\beta = \text{id}(\beta)$ , where  $\text{id}$  is the identity permutation in  $H$ ), we have that  $H(\beta) = (gH)(\alpha) = (gHg^{-1})(\beta)$  and since  $H(\beta) = gHg^{-1}(\beta)$ , Lemma 12 assures us that  $H = gHg^{-1}$ . Hence, since  $H = gHg^{-1}$  for all  $g \in G$ , we have that  $H \triangleleft G$ .  $\square$

We have now translated the concept of normal subgroups into the language of arrangement sets. Now that normality is understood in terms of arrangement sets, it would seem natural to consider **quotient groups**.

As cyclic quotient groups are deeply important to the concept of solvability, our final result establishes a criterion which determines when the quotient group of the associated permutation sets of two arrangement sets is cyclic.

**Theorem 21.** *Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ , such that  $H \triangleleft G$ , and let  $\alpha \in N$ . Then the quotient  $\frac{G}{H}$  of  $G$  by  $H$  is cyclic if and only if there exists a permutation  $f \in G$  such that there exists  $n \in \mathbb{N}$  for each  $T \in P_L(M, N) = P_R(M, N)$  with  $T = (f^n H)(\alpha) = f^n(N)$ .*

*Proof.* Let  $M$  and  $N$  be GSAs of a finite set  $S$ ,  $N \subseteq M$ , and let  $G = \bowtie(M)$  and  $H = \bowtie(N)$ , such that  $H \triangleleft G$ . Also, let  $\alpha \in N$ . Because  $H \triangleleft G$ , we know that  $P_L(M, N) = P_R(M, N)$ .

Next, suppose that  $\frac{G}{H}$  is cyclic; then, there exists  $f \in G$  such that  $\frac{G}{H}$  is  $\frac{G}{H} = \langle fH \rangle$ , the cyclic group generated by  $fH$ . Thus, we know that there exists  $n \in \mathbb{N}$  such that  $bH = (fH)^n$  for each  $bH \in \frac{G}{H}$ . Also, by the definition of quotient group,  $bH = (fH)^n = (f^n)H$ . Consider an arbitrary arrangement set  $T \in P_L(M, N) = P_R(M, N)$ . We know by Lemma 17 and Theorem 15 that there exists  $k \in G$  such that  $T = (kH)(\alpha)$ . But we already know that there exists  $n \in \mathbb{N}$  such that  $kH = f^n H$ , whence  $T = (f^n H)(\alpha)$ .

To show the converse, suppose that there exists  $f \in G$  such that there exists for each arrangement set  $T \in P_L(M, N) = P_R(M, N)$  an  $n \in \mathbb{N}$  such that  $T = (f^n H)(\alpha)$ . Then, for each  $b \in G$ , there exists  $n \in \mathbb{N}$  such that  $(bH)(\alpha) = (f^n H)(\alpha)$ , whence we have by Lemma 12 that  $bH = f^n H = (fH)^n$ . Therefore,  $\frac{G}{H} = \langle fH \rangle$ , whereby  $\frac{G}{H}$  is cyclic.  $\square$

Theorem 21 gives us all that we need to completely describe solvability in terms of GSAs. According to the modern definition of solvability, a group  $H_0$  is **solvable** if there exists a normal chain of groups

$$H_n = \{\text{id}\} \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_1 \triangleleft G = H_0,$$

where  $\frac{H_i}{H_{i+1}}$  is cyclic for  $0 \leq i < n$ . All of the pieces of this definition now have analogs in the language of GSAs.

However, more work can be done on the relationship between GSAs and groups. A complete description of quotient groups in terms of GSAs has not been provided; it is possible that Galois’s language of arrangement sets is not abstract enough to completely describe quotient groups.

Galois never provided a satisfactory definition of group in his memoir. However, it is clear that, to Galois, groups were always sets of permutations (Galois actually used the word “substitution” instead of “permutation”), and that Galois’s permutation groups were always assumed to act upon arrangements. Thus, he would denote a particular group of permutations by writing the list of arrangements created when that permutation group was applied to a single arrangement.

The GSA definition provided by this paper provides a precise definition for the group concept expressed by Galois. Notice that a set of arrangements must meet only one property to be a GSA, compared to the three or four properties required by the modern group definition. The property met by GSAs is loosely related to closure, which Galois recognized was essential to his group concept. The modern group properties are immediately met by the permutation set associated with a GSA, as Theorem 10 shows.

At the end of his memoir, Galois listed out all of the arrangements of a set with four elements. He then proceeded to show that the permutation group associated with that set of arrangements is solvable; he repeatedly partitioned his list of arrangements until he had a list of arrangements that contained only one arrangement. Similarly, he showed that the permutation group associated with the set of all arrangements of five elements is not solvable, thereby showing that the general quintic polynomial is not solvable. While this fact was known prior to Galois’s work, Galois was able to use his more general machinery to very quickly arrive at this result.

Galois greatly advanced in the knowledge of the theory of equations, at the same time revolutionizing modern algebra. It took others, however, to provide a satisfactory definition of the concepts Galois originated. Abstract groups today are studied in a more general context than were

Galois's permutation groups. It shall forever be true, however, that arrangement sets are key to the development of modern algebra.

## Acknowledgements and Remarks

Many thanks must be given to Dr. Matt Lunsford, who had the original idea for the project and gave me a few hints along the way when they were needed. Also, the research in this paper was supported by an Undergraduate Research Grant from Union University, for which the author is very thankful.

Finally, although the precise statements of all of the definitions and theorems, as well as the proofs, are entirely original to the author, many of the results are not. Also, some notation was borrowed from [Ti], including the  $\text{Sym}(S)$ ,  $H(\alpha)$ , and  $g(M)$  notations. The author takes responsibility for introducing the groovy bow tie notation.

Those who wish to learn more about the history of Galois theory should consult [Ed], which contains a translation of Galois's memoir. Finally, the referees of this paper must be thanked very much for many helpful comments that greatly improved the work.

## References

[Ed] Harold M. Edwards: *Galois Theory*. New York: Springer-Verlag 1984.

[Ri] Laura Toti Rigatelli: *Evariste Galois*. Basel, Switzerland: Birkhauser 1996.

[Ti] Jean-Pierre Tignol: *Galois Theory of Algebraic Equations*. New Jersey: World Scientific 2001.