Bridging the Group Definition Gap

Matthew Dawson

Evariste Galois (1811-1832)

- Political revolutionary
- Died in a duel under mysterious circumstances
- May have sacrificed his life (Rigatteli)
- Very sad, short life

Evariste Galois (1811-1832)

- Discovered criterion for polynomial equations to be solvable by radicals
- Founded group theory
- Defined groups differently from modern texts
- Thought of groups as sets of arrangements

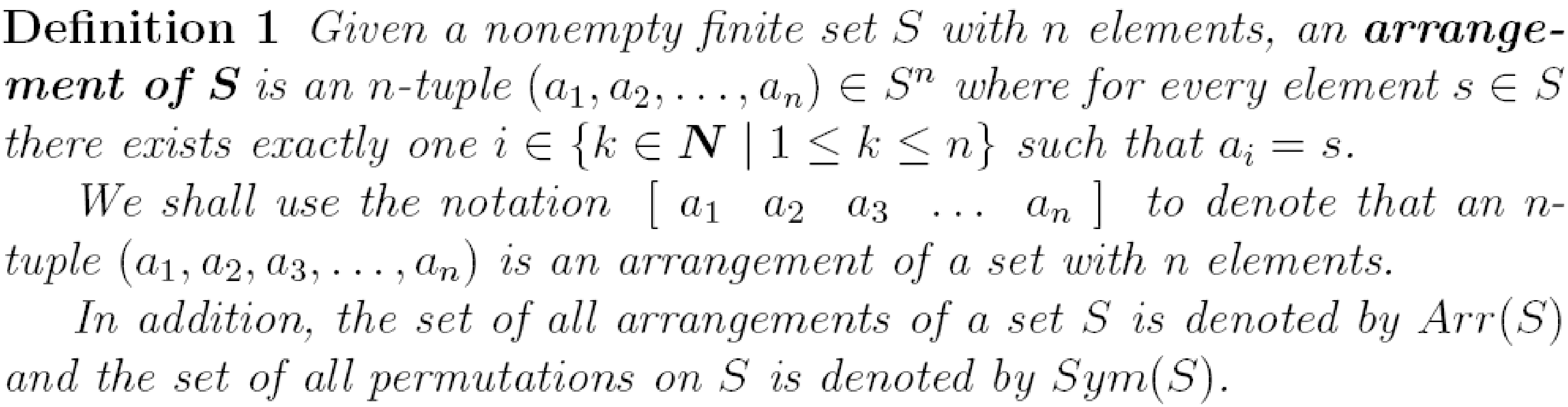
A Project is Born

- Most students never get exposed to Galois's original definition
- Group theory can be seen from interesting perspective
- Dr. Lunsford

A Project is Born

- Demonstrate connection of Galois’s arrangement sets to modern groups
- Determine what is meant by solvability in the context of Galois’s arrangement sets
- Provide correct and rigorous mathematical proofs
- Provide concrete example of showing that an arrangement set is solvable

Arrangements: The "New" Concept

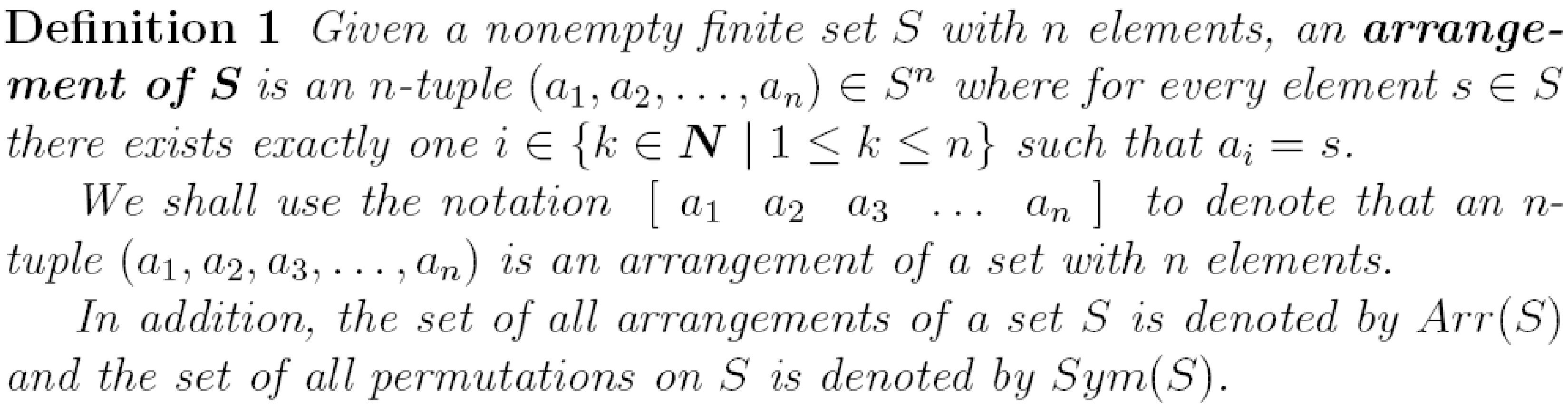


Definition 1 *Given a nonempty finite set S with n elements, an* ***arrangement of S*** *is an n-tuple $(a_1, a_2, \ldots, a_n) \in S^n$ where for every element $s \in S$ there exists exactly one $i \in \{k \in \boldsymbol{N} \mid 1 \leq k \leq n\}$ such that $a_i = s$.*

We shall use the notation $[\ a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n\ ]$ to denote that an n-tuple $(a_1, a_2, a_3, \ldots, a_n)$ is an arrangement of a set with n elements.

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

Arrangements: The “New” Concept



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

We shall use the notation $[\ a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n\ ]$ to denote that an n-tuple $(a_1, a_2, a_3, \ldots, a_n)$ is an arrangement of a set with n elements.

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

- Example:
  - Let S = {a, b, c}
  - (a, b, b) is not an arrangement of S
  - (a, c, b) is an arrangement of S

Arrangements: The “New” Concept

- Shorthand: write abc instead of

$$(a, b, c) \text{ or } \begin{bmatrix} a & b & c \end{bmatrix}$$

- Arrangements and permutations on S:

$Arr(S)$	$Sym(S)$
abc	(ab)
acb	(bc)
bac	(ac)
bca	(abc)
cab	(acb)
cba	$(ab)(ab)$

$$Sym(S) \sim S_3$$

- Sym(S) is a group in the modern sense

How to Apply a Permutation to an Arrangement

Theorem 1 *Let S be a finite set with n elements.*

1. *Let $f \in Sym(S)$, and consider the mapping P_f on $Arr(S)$ such that for each arrangment $\alpha = [\ a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n\ ] \in Arr(S)$,*

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

   Then P_f is a well-defined permutation on $Arr(S)$.

2. *For all $\alpha, \beta \in Arr(S)$, there exists a unique permutation $f \in Sym(S)$ such that $P_f(\alpha) = \beta$.*

3. *For all $f, g \in P$, $P_f \circ P_g = P_{f \circ g}$.*

How to Apply a Permutation to an Arrangement

- Example: $f = (ab)$

$$\begin{aligned}
P_f(abc) &= f(a)f(b)f(c) = bac \\
P_f(acb) &= f(a)f(c)f(b) = bca \\
P_f(bac) &= f(b)f(a)f(c) = abc \\
P_f(bca) &= f(b)f(c)f(a) = acb \\
P_f(cab) &= f(c)f(a)f(b) = cba \\
P_f(cba) &= f(c)f(b)f(a) = cab
\end{aligned}$$

- Notation P_f won’t be used again

How to Apply a Permutation to an Arrangement

Theorem 1 *Let S be a finite set with n elements.*

1. *Let $f \in Sym(S)$, and consider the mapping P_f on $Arr(S)$ such that for each arrangment $\alpha = [\ a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n\ ] \in Arr(S)$,*

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

Then P_f is a well-defined permutation on $Arr(S)$.

2. *For all $\alpha, \beta \in Arr(S)$, there exists a unique permutation $f \in Sym(S)$ such that $P_f(\alpha) = \beta$.*

3. *For all $f, g \in P$, $P_f \circ P_g = P_{f \circ g}$.*

Where Are we Going?

- Question: What do arrangements have to do with groups?
- Answer: Permutations
- Next step: associate two kinds of permutation sets with arrangement sets
- Determine when these permutation sets form groups

Permutation Sets of the First Kind

Definition 2 *Let S be a nonempty finite set, let $C \subseteq Arr(S)$, and let $\alpha \in C$. Then the* ***permutation set of*** α ***in*** C*, denoted* $\bowtie_\alpha (C)$ *, is the set*

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

- Example:

$$C = \{abc, bca, cab, cba\} \qquad \alpha = abc$$

$$\begin{aligned}
abc &\overset{(ab)(ab)}{\longrightarrow} abc \\
abc &\overset{(abc)}{\longrightarrow} bca \\
abc &\overset{(acb)}{\longrightarrow} cab \\
abc &\overset{(ac)}{\longrightarrow} cba
\end{aligned}$$

$$\bowtie_\alpha (C) = \{(ab)(ab), (abc), (acb), (ac)\}$$

Total Permutation Sets

Definition 3 *Let S be a nonempty finite set, and let $C \subseteq Arr(S)$. Then the* ***permutation set associated with*** *C, denoted $\bowtie(C)$, is the set*

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

- Example:

$$C = \{abc, bca, cab, cba\}$$

$$\begin{array}{ccccccccccccccc}
abc & \xrightarrow{(ab)(ab)} & abc & \quad & bca & \xrightarrow{(acb)} & abc & \quad & cab & \xrightarrow{(abc)} & abc & \quad & cba & \xrightarrow{(ac)} & abc \\
abc & \xrightarrow{(abc)} & bca & & bca & \xrightarrow{(ab)(ab)} & bca & & cab & \xrightarrow{(acb)} & bca & & cba & \xrightarrow{(bc)} & bca \\
abc & \xrightarrow{(acb)} & cab & & bca & \xrightarrow{(abc)} & cab & & cab & \xrightarrow{(ab)(ab)} & cab & & cba & \xrightarrow{(ab)} & cab \\
abc & \xrightarrow{(ac)} & cba & & bca & \xrightarrow{(bc)} & cba & & cab & \xrightarrow{(ba)} & cba & & cba & \xrightarrow{(ab)(ab)} & cba
\end{array}$$

$$\bowtie(C) = \{(ab)(ab), (abc), (acb), (ab), (ac), (bc)\}$$

The Permutation Sets are Different

- In our previous example,

$$\bowtie(C) = \{(ab)(ab), (abc), (acb), (ab), (ac), (bc)\}$$

$$\bowtie_\alpha(C) = \{(ab)(ab), (abc), (acb), (ac)\}$$

- Thus, $\bowtie_\alpha(C) \neq \bowtie(C)$
- In general, $\bowtie_\alpha(C) \subseteq \bowtie(C)$
- When are the sets equal?
- Stay tuned!

A Lemma Along the Way

Lemma 2 *If C is a set of arrangements of a finite set such that $\bowtie_\alpha(C)$ forms a group under composition, where $\alpha \in C$, then $\bowtie_\alpha(C) = \bowtie(C)$.*

- Examples:

$$M = \{abc, acb\}$$

$$abc \xrightarrow{(ab)(ab)} abc \qquad acb \xrightarrow{(ab)(ab)} acb$$

$$abc \xrightarrow{(bc)} acb \qquad acb \xrightarrow{(bc)} abc$$

$$\bowtie_{abc}(M) = \bowtie_{acb}(M) = \bowtie(M) = \{(ab)(ab), (bc)\}$$

- Note that $\bowtie_{acb}(M)$ is a group

A Lemma Along the Way

Lemma 2 *If C is a set of arrangements of a finite set such that $\bowtie_\alpha (C)$ forms a group under composition, where $\alpha \in C$, then $\bowtie_\alpha (C) = \bowtie (C)$.*

- In other example, we did not get a group:

$$\bowtie_\alpha (C) = \{(ab)(ab), (abc), (acb), (ac)\}$$

- Thus, $\bowtie_\alpha (C) \neq \bowtie (C)$

Galois Makes an Entrance

Definition 4 *A set C of arrangements of a nonempty finite set S is a **Galois Set of Arrangements (GSA)** if for all $f \in \bowtie(C)$, $\alpha \in C \Rightarrow f(\alpha) \in C$.*

- Example:

$$C = \{abc, bca, cab, cba\}$$

$$\bowtie(C) = \{(ab)(ab), (abc), (acb), (ab), (ac), (bc)\}$$

- Consider $f = (ab) \in \bowtie(C)$
- Since $abc \in C$ but $f(abc) = bac \notin C$, C is not a GSA

Galois Makes an Entrance

Definition 4 *A set C of arrangements of a nonempty finite set S is a* ***Galois Set of Arrangements (GSA)*** *if for all $f \in \bowtie(C)$, $\alpha \in C \Rightarrow f(\alpha) \in C$.*

- Example:

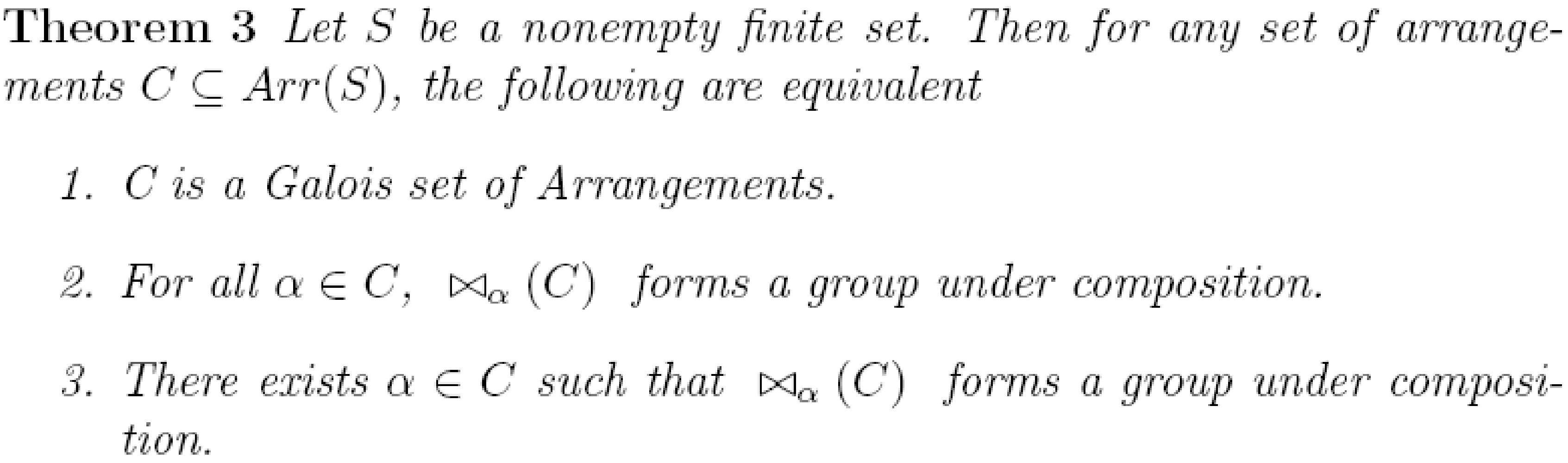
$$M = \{abc, acb\}$$

$$\begin{array}{cccccc} abc & \xrightarrow{(ab)(ab)} & abc & acb & \xrightarrow{(ab)(ab)} & acb \\ abc & \xrightarrow{(bc)} & acb & acb & \xrightarrow{(bc)} & abc \end{array}$$

$$\bowtie_{abc}(M) = \bowtie_{acb}(M) = \bowtie(M) = \{(ab)(ab), (bc)\}$$

- M is a GSA

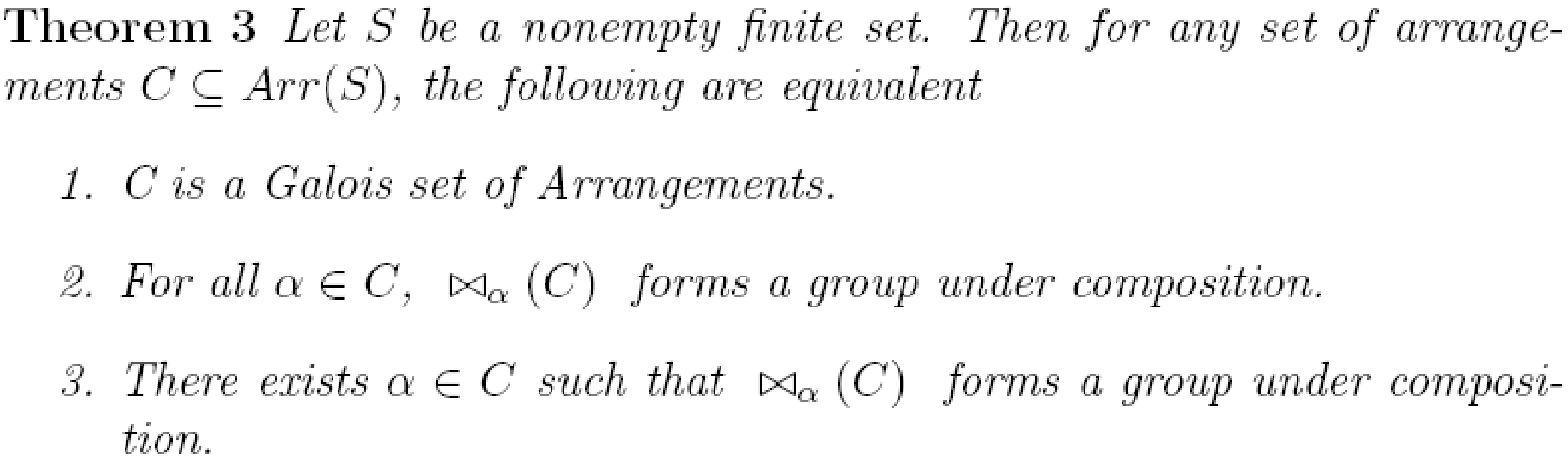
The Big Theorem: GSAs and Groups



Theorem 3 *Let S be a nonempty finite set. Then for any set of arrangements $C \subseteq Arr(S)$, the following are equivalent*

1. *C is a Galois set of Arrangements.*
2. *For all $\alpha \in C$, $\bowtie_\alpha (C)$ forms a group under composition.*
3. *There exists $\alpha \in C$ such that $\bowtie_\alpha (C)$ forms a group under composition.*

The Big Theorem: GSAs and Groups



Theorem 3 *Let S be a nonempty finite set. Then for any set of arrangements $C \subseteq Arr(S)$, the following are equivalent*

1. *C is a Galois set of Arrangements.*
2. *For all $\alpha \in C$, $\bowtie_\alpha (C)$ forms a group under composition.*
3. *There exists $\alpha \in C$ such that $\bowtie_\alpha (C)$ forms a group under composition.*

Let's prove (part of) it!

The Big Theorem: Proof

Proof We shall first show that (1) $\longrightarrow$ (2). Suppose that C is a Galois set of arrangements. Then for all $f \in \bowtie(C)$, $f(\beta) \in C$ for all $\beta \in C$. Now let $\alpha \in C$. 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 α in C, $fg \in \bowtie_\alpha(C)$. Hence $\bowtie_\alpha(C)$ is closed under composition.

Now consider the identity permutation $e : S \longrightarrow S$. Then $e(\alpha) = \alpha$. Thus, $e \in \bowtie_\alpha(C)$, so that $\bowtie_\alpha(C)$ contains an identity element.

Next let $f \in \bowtie_\alpha(C)$. Then by the definition of the permutation set of α 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, $f^{-1}(\alpha) \in C$. Therefore, $f^{-1} \in \bowtie_\alpha(C)$. Thus $\bowtie_\alpha(C)$ contains an inverse for each element. Therefore, $\bowtie_\alpha(C)$ forms a group with respect to function composition.

Where Are we Going?

- We know how groups relate to arrangement sets
- Next question: how does normality relate to arrangements?
- Answer: partitions
- First, we must know two ways to create GSAs

Permutation Groups Applied To Arrangement

- Applying a group of permutations to an arrangement produces a GSA
- Example

$$H = \{(ab)(ab), (abc), (acb)\} \qquad \alpha = abc$$

$$\begin{aligned} abc &\overset{(ab)(ab)}{\longrightarrow} abc \\ abc &\overset{(abc)}{\longrightarrow} bca \\ abc &\overset{(acb)}{\longrightarrow} cab \end{aligned}$$

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

Right Partitions

- Example:

$$M = \{abc, bca, acb, bac, cba, cab\} \quad N = \{abc, bac\}$$

$$H = \bowtie (N) = \{(ab)(ab), (ab)\}$$

- We can form a *right partition* of M using N

$$P_R(M, N) \quad = \quad \begin{array}{|c|c|c|} \hline abc & bca & cab \\ \downarrow^{(ab)} & \downarrow^{(ab)} & \downarrow^{(ab)} \\ bac & acb & cba \\ \hline \end{array}$$

N=H(abc) H(bca) H(cab)

A Permutation Applied to a GSA

- Applying a permutation to all elements of a GSA yields a new GSA
- Example

$$N = \{abc, bca, cab\} \qquad g = (ab)$$

$$\begin{aligned} abc &\xrightarrow{(ab)} bac \\ bca &\xrightarrow{(ab)} acb \\ cab &\xrightarrow{(ab)} cba \end{aligned}$$

$$g(N) = \{bac, acb, cba\}$$

Right Partitions

- Example:

$$M = \{abc, bca, acb, bac, cba, cab\} \quad N = \{abc, bac\}$$

$$H = \bowtie(N) = \{(ab)(ab), (ab)\}$$

- We can form a *left partition* of M using N

$$P_L(M,N) = \boxed{\begin{matrix} abc \\ bac \end{matrix}} \begin{matrix} \xrightarrow{(abc)} \\ \xrightarrow{(abc)} \end{matrix} \boxed{\begin{matrix} bca \\ cba \end{matrix}} \begin{matrix} \xrightarrow{(ab)} \\ \xrightarrow{(ab)} \end{matrix} \boxed{\begin{matrix} acb \\ cab \end{matrix}}$$

Two Important Partitions

- Summary:

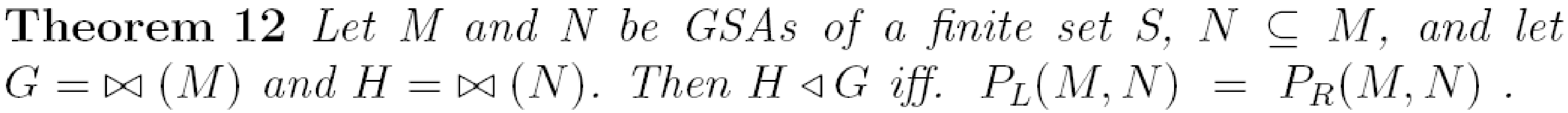
$M = \{abc, bca, acb, bac, cba, cab\} \quad N = \{abc, bac\}$

$$P_R(M, N) = \begin{array}{|c|c|c|}\hline abc & bca & cab \\ bac & acb & cba \\ \hline \end{array}$$

$$P_L(M, N) = \begin{array}{|c|c|c|}\hline abc & bca & acb \\ bac & cba & cab \\ \hline \end{array}$$

- In this case, the left and right partitions are not equal
- Question: will they ever be equal?

Normality



Theorem 12 *Let M and N be GSAs of a finite set S, $N \subseteq M$, and let $G = \bowtie(M)$ and $H = \bowtie(N)$. Then $H \triangleleft G$ iff. $P_L(M,N) = P_R(M,N)$.*

- If $H \triangleleft G$ then we say that N is a normal subset of M
- In previous example, N was not a normal subset of M
- Very important group property; implies the existence of quotient group
- Next task: When is a quotient group cyclic?

Cyclic Quotient Groups

Theorem 13 *Let* M *and* N *be GSAs of a finite set* S, $N \subseteq M$, *let* $G = \bowtie(M)$ *and* $H = \bowtie(N)$, *such that* $H \lhd G$, *and let* $\alpha \in N$. *Then* $\frac{G}{H}$ *is cyclic iff. there exists a permutation* $f \in G$ *such that for each* $T \in P_L(M, N) = P_R(M, N)$, *there exists* $n \in \mathbf{N}$ *such that* $T = (f^n H)(\alpha) = f^n(N)$

- A group H_0 is solvable when a normal chain exists:

$$H_n = \{e\} \lhd H_{n-1} \lhd \cdots \lhd H_2 \lhd H_1 \lhd H_0$$

where $\frac{H_i}{H_{i-1}}$ is cyclic

- We say that a GSA is solvable when its associated permutation set is solvable

A Simple Example

- Our final task is to show that quartic (degree four) polynomials are solvable by radicals
- Example was used by Galois in his memoir
- Notation a little different
- We must show that the set of all arrangements of a set with four elements forms is solvable

A Simple Example

- Let S = {a, b, c, d}
- Task: Show that Arr(S) is solvable

$$N_0 = Arr(S)$$

$abcd$

$abdc$

$acbd$

$acdb$

$adbc$

$adcb$

$bacd$

$badc$

$bcad$

$bcda$

$bdac$

$bdca$

$cabd$

$cadb$

$cbda$

$cbad$

$cdab$

$cdba$

$dabc$

$dacb$

$dbca$

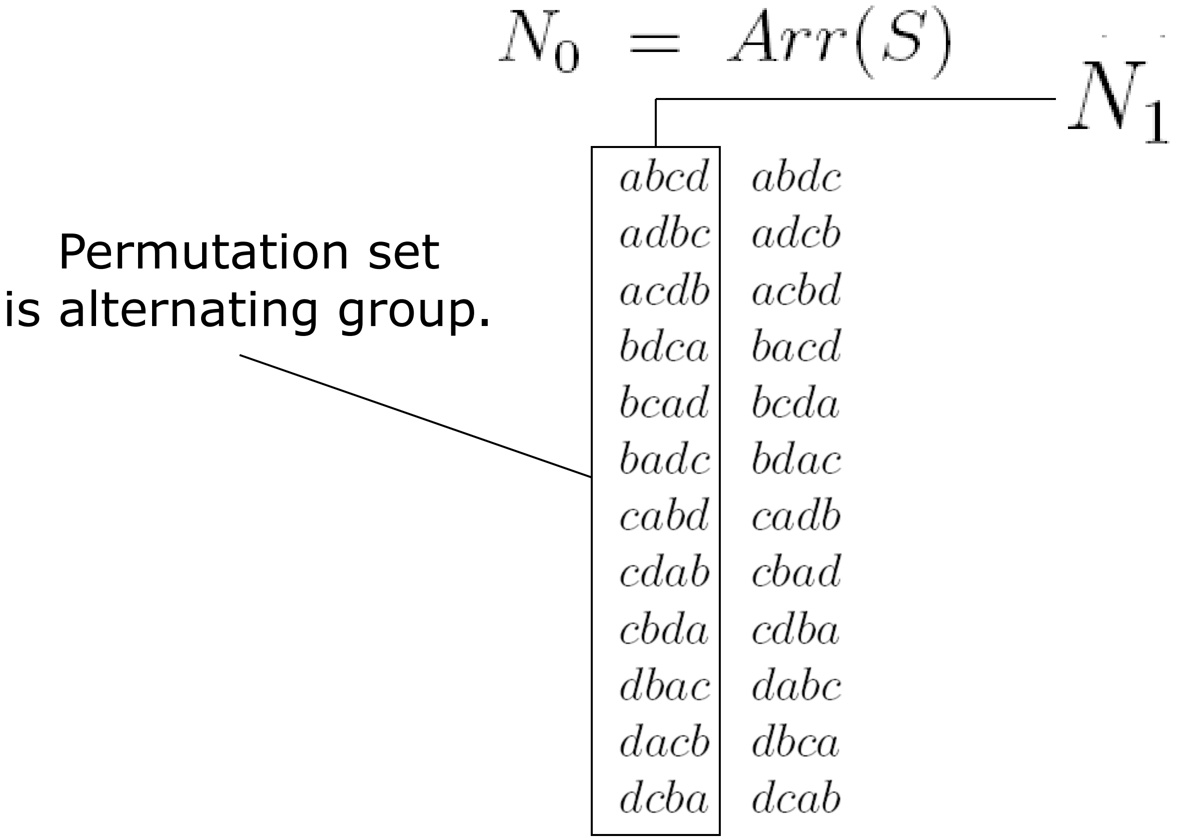
$dbac$

$dcab$

$dcba$

A Simple Example

- Let S = {a, b, c, d}
- Task: Show that Arr(S) is solvable



$$N_0 = Arr(S)$$

N_1

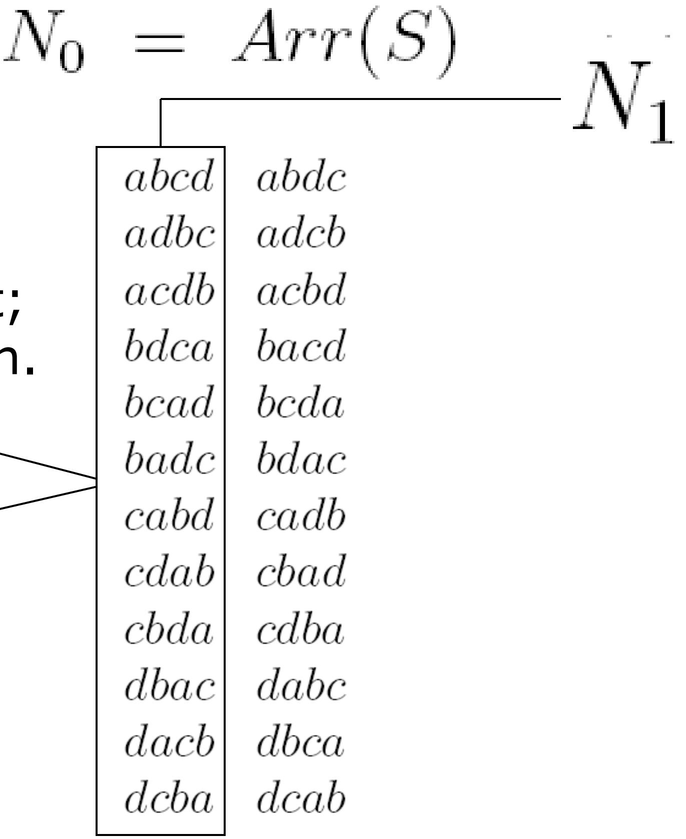
$abcd$	$abdc$
$adbc$	$adcb$
$acdb$	$acbd$
$bdca$	$bacd$
$bcad$	$bcda$
$badc$	$bdac$
$cabd$	$cadb$
$cdab$	$cbad$
$cbda$	$cdba$
$dbac$	$dabc$
$dacb$	$dbca$
$dcba$	$dcab$

Permutation set
is alternating group.

A Simple Example

- Let S = {a, b, c, d}
- Task: Show that Arr(S) is solvable

$$N_0 = Arr(S)$$



N_1

$abcd$	$abdc$
$adbc$	$adcb$
$acdb$	$acbd$
$bdca$	$bacd$
$bcad$	$bcda$
$badc$	$bdac$
$cabd$	$cadb$
$cdab$	$cbad$
$cbda$	$cdba$
$dbac$	$dabc$
$dacb$	$dbca$
$dcba$	$dcab$

Must be a normal subset;
there is only one partition.

Quotient group formed by
permutation sets must be
cyclic; it contains only
two elements

A Simple Example

- Problem reduces to:

  Is the set $N_1 = \begin{matrix} \underbrace{\boxed{\begin{matrix} abcd \\ badc \\ cdab \\ dcba \end{matrix}}}_{N_2} & \begin{matrix} acdb \\ bdca \\ cabd \\ dbac \end{matrix} & \begin{matrix} adbc \\ bcad \\ cbda \\ dacb \end{matrix} \end{matrix}$ solvable?

Because $\bowtie_{abcd}(N_2)$ forms a group (Klein four group), N_2 is a GSA.

A Simple Example

Left partition of N_1 by N_2

$$\begin{array}{|c|c|c|c|c|}
\hline
abcd & \xrightarrow{(bcd)} & acdb & \xrightarrow{(bcd)} & adbc \\
badc & \xrightarrow{(bcd)} & cabd & \xrightarrow{(bcd)} & dacb \\
cdab & \xrightarrow{(bcd)} & dbac & \xrightarrow{(bcd)} & bcad \\
dcba & \xrightarrow{(bcd)} & bdca & \xrightarrow{(bcd)} & cbda \\
\hline
\end{array}$$

Right partition of N_1 by N_2

$abcd$	$acdb$	$adbc$
$badc$	$bdca$	$bcad$
$cdab$	$cabd$	$cbda$
$dcba$	$dbac$	$dacb$

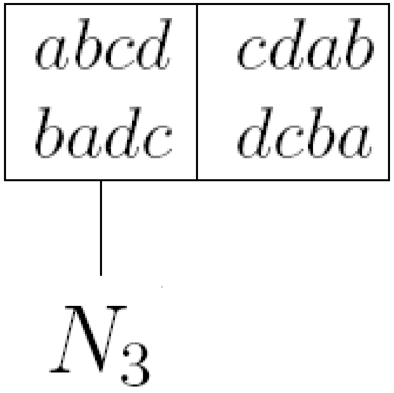
- The left and right partitions of N_1 by N_2 are the same, so that N_2 is a normal subset of N_1
- One permutation (i.e., (bcd)) connects arrangement sets in partition; quotient group is cyclic

A Simple Example

- Problem reduces to:

  Is the set $N_2 = \begin{matrix} abcd \\ badc \\ cdab \\ dcba \end{matrix}$ solvable?

- The set can be partitioned into two GSAs:



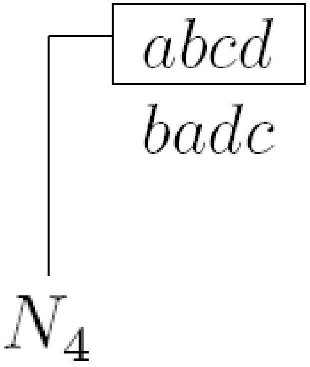
$abcd$ $badc$	$cdab$ $dcba$

N_3

A Simple Example

- Problem reduces to:
  Is the set $N_3 = \begin{matrix} abcd \\ badc \end{matrix}$ solvable?

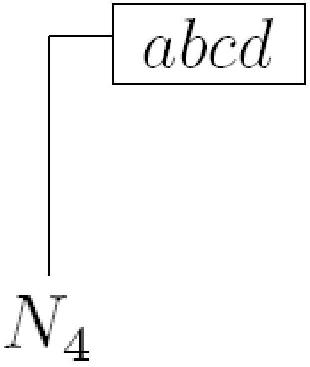
- The set can be partitioned into two GSAs:



A Simple Example

- Problem reduces to:

  Is the set $N_4 = \ abcd$ solvable?
- The associated permutation set of N_4 consists of identity permutation.



$abcd$

N_4

A Simple Example

- We have just created a normal chain of GSAs:

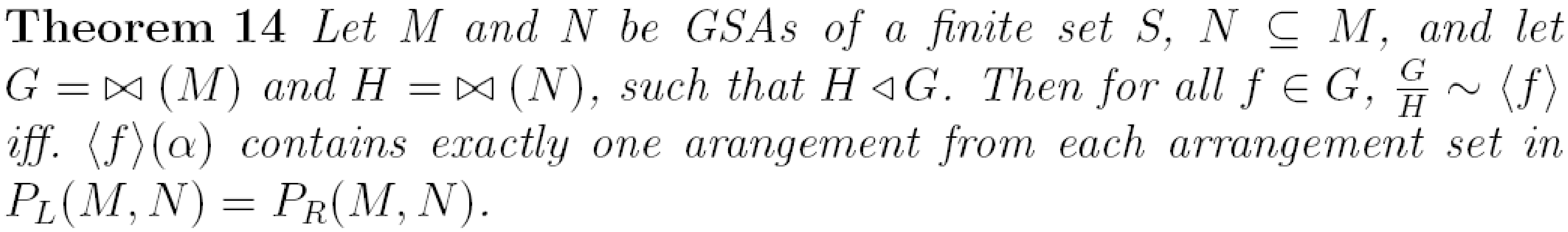
$$N_4 \subseteq N_3 \subseteq N_2 \subseteq N_1 \subseteq N_0$$

$$H_4 = \{e\} \lhd H_3 \lhd H_2 \lhd H_1 \lhd H_0$$

- Quotient groups are cyclic
- Yippee!
- N_0 (i.e., Arr(S)) is solvable!
- Fourth degree polynomials can be solved by radicals.

Parting Thoughts

- Inculcated in my mind the centrality of permutations
- Proving the theorems was fun
- Perhaps algebra students should be exposed to arrangements
- Much work can still be done
- Hunch:



Theorem 14 *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 $H \lhd G$. Then for all $f \in G$, $\frac{G}{H} \sim \langle f \rangle$ iff. $\langle f \rangle(\alpha)$ contains exactly one arangement from each arrangement set in $P_L(M,N) = P_R(M,N)$.*

Acknowledgements

- Dr. Lunsford
  - Made original suggestion
  - Always helpful

- Undergraduate research program
  - The grant money was nice
  - An excuse to keep working into spring

References

- Rigatelli, Laura Toti. Evariste Galois.
  Basel, Switzerland: Birkhauser, 1996.
- Tignol, Jean-Pierre. Galois' Theory of Algebraic Equations.
  New Jersey: World Scientific, 2001.
- Edwards, Harold M. Galois Theory.
  New York: Springer-Verlag, 1984.

May your arrangements always be normal!