# Permutation Groups and Polynomials

Sarah Kitchen

April 25, 2005

## Finite Permutation Groups

Given a set $S$ with $n$ elements, consider all the possible one-to-one and onto functions from $S$ to itself. This collection of functions is called the permutation group of $S$, because the functions are simply permuting the elements of $S$. We notice immediately that it doesn't matter what the elements of $S$ are (numbers, planets, tacos, etc) just that there are $n$ distinct ones in the set, so we may refer to the collection of functions independantly of the set they are acting on as the symmectric group of degree $n$ or the permutation group on $n$ letters and denote it $S_n$.

Example: Let $n = 3$ and $S = \{1, 2, 3\}$. What functions are in $S_3$?

The word "group" means that $S_n$ satisfies some special properties, which are given in the following definition:

Definition: A set $G$ together with an operation $*$ is a group if

1. For $g, g'$ in $G$, $g * g'$ is in $G$. We say $G$ is multiplicatively closed.
2. There is an element $e$ in $G$ such that for every $g$ in $G$, $e * g = g * e = g$. We call this element the identity.
3. For every $g$ in $G$ there is an element $g'$ in $G$ such that $g * g' = g' * g = e$. We say every element $g$ has an inverse $g'$, which we typically denote as $g^{-1}$.
4. The operation is associative. That is, for $f, g, h$ in $G$, $f * (g * h) = (f * g) * h$.

Remark: Every group we deal with today will satisfy 4, so we will not be checking this condition in examples or exercises.

Example: The natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ with addition is not a group. Take natural numbers $n$ and $m$. Since the sum of two natural numbers is a natural number, we satisfy condition 1. However, if $n + m = n$ then $m = 0$, but 0 is not in $\mathbb{N}$, so we don't satisfy condition 2. Even if we add 0 to the set, we do not get a group because if $n + m = 0$, then $m = -n$, but we have no negative numbers in our set, so we don't satisfy condition 3. If we add all the negatives of the natural numbers to the set, we get the integers with addition, which satisfies all the conditions so is a group.

Exercise: The integers with multiplication is not a group. Which condition(s) do we fail to satisfy? What group can we get by correcting the set (as we did in the example)?

We claim $S_n$ with composition is a group. If $f$ and $g$ are in $S_n$, they are both bijective maps on $S$, an arbitrary set with $n$ elements. So, $f \circ g$ is a map from $S$ to $S$, and we have to check it is one-to-one and onto. To prove injectivity, let $x$ and $y$ be in $S$ and suppose $f \circ g(x) = f \circ g(y)$. Then, since $f$ is one-to-one, $g(x) = g(y)$, and since $g$ is one-to-one, we conclude $x = y$, so $f \circ g$ is one-to-one. For surjectivity, choose any $z$ in $S$. Since $f$ is onto, there exists a $y$ in $S$ such that $f(y) = z$. Since $g$ is also onto, there is an $x$ in $S$ such that $g(x) = y$. Therefore, $f \circ g(x) = f(y) = z$ so $f \circ g$ is onto. Hence, $f \circ g$ is in $S_n$, so $S_n$ is multiplicatively closed under composition. Let $i$ be the map from $S$ to $S$ that fixes all the elements–we call this the identity map. Then, for any $f$ in $S_n$, $x$ in $S$, $i \circ f(x) = i(f(x)) = f(x) = f(i(x)) = f \circ i(x)$, so $f \circ i = i \circ f = f$, so $i$ is the identity element of condition 2. Finally, for any $f$ in $S_n$, for any $y$ in $S$, there is an $x$ in $S$ such that $f(x) = y$, since $f$ is onto. Define a map $g$ from $S$ to $S$ so that $g(y) = x$. Then $f \circ g(y) = f(x) = y$ and $g \circ f(x) = g(y) = x$, so $f \circ g = g \circ f = i$, so $g = f^{-1}$ and we satisfy condition 3. Therefore, $S_n$ is a group.

# Cycle Decomposition

We would like a way to write down the elements of $S_n$ efficiently in a way that makes the elements and multiplication less abstract. To do so, we will introduce cycle notation. As an example, recall the function of $S_3$ that takes $1 \mapsto 2$, $2 \mapsto 3$,

and $3 \mapsto 1$. In cycle notation, we would write this $(1 \quad 2 \quad 3)$. But our functions won't always permute the elements of the set cyclically. Consider the function in $S_4$ that takes $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$ and $4 \mapsto 3$. This function permutes the set $\{1, 2, 3, 4\}$ in two disjoint cycles: $(1 \quad 2)$ and $(3 \quad 4)$. In cycle notation, we would write this function $(1 \quad 2)(3 \quad 4)$. As a convention, if a function fixes an element, e.g. the fuction $1 \mapsto 2$, $2 \mapsto 1$, and $3 \mapsto 3$ in $S_3$, we omit the one element cycle from the notation: $(1 \quad 2)(3) = (1 \quad 2)$.

Now that we've seen how to write permutations as cycles, we can see how to multiply cycles. Let $f = (1 \quad 2 \quad 3)$ and $g = (1 \quad 2)$ in $S_3$. Then $f \circ g = (1 \quad 2 \quad 3)(1 \quad 2)$. Since we regard the product as a composition of functions, the convention is to "multiply right to left," in that $g$ takes $1 \mapsto 2$ and $f$ takes $2 \mapsto 3$, so $f \circ g : 1 \mapsto 3$.

Exercise: Repeat the above calculation to find $f \circ g(2)$ and $f \circ g(3)$. What is the cycle notation for $f \circ g$?

Exercise: What is the cycle notation for $g \circ f = (1 \quad 2)(1 \quad 2 \quad 3)$? Remember to multiply right to left.

We notice something very important: That $(1 \quad 2 \quad 3)(1 \quad 2) \neq (1 \quad 2)(1 \quad 2 \quad 3)$. This is why, when multiplying elements of the group, we need to remember to multiply right to left, or we'll end up with the wrong answer! There is a special kind of group where we do not have to worry about the order of multiplication:

Definition: A group $G$ is said to be abelian if for any $g$, $g'$ in $G$, $g * g' = g' * g$.

Observe further that $(1 \quad 2)(3 \quad 4) = (3 \quad 4)(1 \quad 2)$. We say these cycles are disjoint, because they share no numbers. It is true in general that for disjoint cycles $\sigma, \tau$ that $\sigma\tau = \tau\sigma$.

## Exercises

1. We have seen $(1 \quad 2)$ and $(1 \quad 2 \quad 3)$ are two elements of $S_3$. Express the other 4 elements of $S_3$ as products of these two elements.

2. Express the following as the product of disjoint cycles:

   (a) $(1 \quad 2 \quad 3 \quad 5 \quad 7)(2 \quad 4 \quad 7 \quad 6)$

(b) $(1 \quad 2)(1 \quad 3)(1 \quad 4)$

(c) $(1 \quad 2 \quad 3 \quad 4 \quad 5)^3$

(d) $(1 \quad 2 \quad 3)(3 \quad 5 \quad 7 \quad 9)(1 \quad 2 \quad 3)^{-1}$

3. Express the following as a product of two-cycles:

   (a) $(1 \quad 2 \quad 3 \quad 4)$

   (b) $(1 \quad 2 \quad 3)(4 \quad 5 \quad 6)$

   (c) $(2 \quad 3 \quad 5 \quad 7)(2 \quad 4 \quad 7 \quad 6)$

4. The order of a permutation is the number of times you have to repeat the permutation before you return to the identity permutation (the one that fixes everything). What is the order of an $n$-cycle?

5. If you have two disjoint cycles, both of order $n$, what is the order of their product?

6. Given a 2-cycle and a 3-cycle, what is the order of their product? For example, what is the order of $(1 \quad 2)(3 \quad 4 \quad 5)$? Find the orders of the cycles in problem 3.

7. With the previous three problems in mind, find a shuffle of a deck of 13 cards that requires 42 repeats to return the cards to their original order.

# Elementary Symmetric Polynomials

Suppose you are given the equations $x+y+z = a$ and $\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{a}$, and are asked to prove that one of $x$,$y$, and $z$ is equal to $a$. We are used to solving problems of this type by finding out where the graphs of those equations intersect–i.e. by solving for one variable in terms of the others and checking a bunch of cases. I claim that one of $x$, $y$, and $z$ must be equal to $a$ because $a$ is a root of the polynomial $p(t) = t^3 - at^2 + bt - ab$ for any $b$. This solution is much faster, but it is not at all obvious why this observation leads to our desired conclusion. The idea is to find $b$ such that $x$, $y$, and $z$ are all the roots of $p(t)$. Then, since $a$ is also a root, $a$ must coincide with one of $x$, $y$, and $z$. But how do we find such a $b$? To investigate, we will explore the general relationship between the roots of a polynomial and its coefficients.

Definition: A polynomial in $n$ variables is homogeneous of degree $k$ if all the monomials have degrees which sum to $k$.

Examples:

1. $p(x) = x$ is a homogeneous polynomial of degree 1 in one variable.
2. $q(x, y, z) = x^4 + y^2z^2$ is a homogeneous polynomial of degree 4 in three variables.
3. $r(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$ is a homogeneous polynomial of degree 2 in four variables.

We notice something special about $r$. For $q$, if we swap $x$ and $z$, $q(z, y, x) = z^4 + y^2x^2$ is not the same polynomial as $q(x, y, z)$, but for any permutation of the $x_i$, $r$ remains the same. We say $r$ is symmetric.

Definition: A polynomial $p$ in $n$ variables, $x_1, x_2, \ldots, x_n$ is symmetric if for any permutation $\sigma \in S_n$, $p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.

Exercise: Is $p(x, y, z) = x + y + z$ symmetric? Is $p(x, y, z) = x + y$?

Definition: The $k$th elementary symmetric polynomial in $n$ variables, denoted $s_k(x_1, \ldots, x_n)$ is the sum of all possible degree $k$ monomials in $n$ variables with each $x_i$ appearing no more than once in each monomial. Formally, for $k \leq n$,

$$s_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}$$

Example: $p(x, y) = xy^2 + yx^2$ is symmetric and homogeneous, but not an elementary symmetric polynomial. The polynomial $r(x_1, x_2, x_3, x_4)$ above is an elementary symmetric polynomial.

Exercise: How many monomials are there of degree $k$ in $n$ variables?

Exercise: How many monomials are there in the elementary symmetric polynomial of degree $k$ in $n$ variables?

You may have learned in algebra while learning how to factor polynomials that any integer root of a polynomial with integer coefficients will divide the degree

zero term. It is not difficult to see why this should be so–Suppose $a$ and $b$ are roots of $x^2 - cx + d$. Since we know the roots, we know how factor this polynomial as $(x-a)(x-b)$. When we multiply out the factors, we see $x^2 - (a+b)x + ab = x^2 - cx + d$; consequently, $a + b = c$ and $ab = d$, so $a$ and $b$ must divide $d$. Observe further that $a + b = s_1(a, b)$ and $ab = s_2(a, b)$, so we can rewrite the polynomial as $x^2 - s_1(a, b)x + s_2(a, b)$. It happens to be true in general, that if $a_1, a_2, \ldots, a_n$ are the roots of a degree $n$ polynomial, then

$$\prod_{i=1}^{n}(x - a_i) = x^n + \sum_{i=1}^{n}(-1)^i s_i(a_1, \ldots, a_n)x^{n-i}.$$

We will prove this by induction on the degree of the polynomial. If our polynomial is of degree $n = 1$ with root $a$, the left hand side is $x - a$, and the right hand side is $x - s_1(a) = x - a$, so the equation holds for $n = 1$. Suppose the equation holds for all polynomials of degree $n$. Let $p(x)$ be of degree $n+1$ with roots $a_1, \ldots, a_{n+1}$. Then, we can write

$$p(x) = (x - a_{n+1})\prod_{i=1}^{n}(x - a_i) = (x - a_{n+1})(x^n + \sum_{i=1}^{n}(-1)^i s_i x^{n-i}),$$

where we let $s_i$ denote $s_i(a_1, \ldots, a_n)$ for brevity. By multiplying out the right hand side:

$$p(x) = x^{n+1} - (s_1 + a_{n+1})x^n + \sum_{i=1}^{n-1}(-1)^{i+1}(s_{i+1} + a_{n+1}s_i)x^{n-i} + (-1)^{n+1}a_{n+1}s_n$$

Since

$$s_1 + a_{n+1} = (a_1 + \ldots + a_n) + a_{n+1} = s_1(a_1, \ldots, a_{n+1})$$

and

$$s_n a_{n+1} = (a_1 a_2 \ldots a_n)a_{n+1} = s_{n+1}(a_1, \ldots, a_n, a_{n+1}),$$

if we can show $s_{i+1} + s_i a_{n+1} = s_{i+1}(a_1, \ldots, a_{n+1})$ for all the other $i$, we conclude the equation holds for $n + 1$, hence for all $n$. By definition,

$$s_{i+1}(a_1, \ldots, a_{n+1}) = \sum_{1 \le j_1 < \ldots < j_{i+1} \le n+1} a_{j_1}a_{j_2}\ldots a_{j_{i+1}}$$

By separating the sum with respect to monomials divisible by $a_{n+1}$, we see the above is equal to

$$\sum_{1 \le j_1 < \ldots < j_{i+1} \le n} a_{j_1}a_{j_2}\ldots a_{j_{i+1}} \quad + a_{n+1}\sum_{1 \le j_1 < \ldots < j_i \le n} a_{j_1}a_{j_2}\ldots a_{j_i} = s_{i+1} + a_{n+1}s_i$$

so it is clear the relationship we wanted holds.

Returning to our original problem, let $b = xy+xz+yz$, then $(t-x)(t-y)(t-z) = t^3-(x+y+z)t^2+(xy+xz+yz)t-(xyz) = t^3-at^2+bt-ab$, since $\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{a}$ implies $\frac{b}{xyz} = \frac{1}{a}$.

Exercise: Compute the following polynomials in two ways–multiplying everything out manually first, then computing the coefficients via the elementary symmetric polynomials to verify they yield the same answer.

1. $(x-1)(x-2)(x-3)$
2. $(x-1)(x+2)(x-3)$
3. $(x-2)^3(x-3)^2$

Exercise: Using a combination of elementary symmetric polynomials and other techniques, expand the product

$$(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$$

## Exercises

Solve the following problems using elementary symmetric polynomials.

1. Find $a, b, c$ such that the roots of $f(x) = x^3+ax^2+bx+c$ are $a, b, c$.
2. Let $a_1, a_2, a_3$ be roots of $6x^3-2x^2+3x+5$. Find a polynomial with roots $\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}$.
3. Let $a_1, a_2, a_3$ be roots of $2x^3-7x+8$. Find a polynomial with roots $\frac{1}{a_1a_2}, \frac{1}{a_2a_3}, \frac{1}{a_1a_3}$.
4. Let $a_1, a_2, a_3$ be the three roots of $x^3+3x+1$.
   (a) Find a polynomial with roots $a_1^2, a_2^2, a_3^2$.
   (b) Find a polynomial with roots $a_1+a_2, a_1+a_3, a_2+a_3$.
5. The Wicked Witch said that the following polynomial has 2005 integer roots: $x^{2005}+2x^{2004}+3x^{2003}+\ldots$. Prove she is a liar.