Introduction to Permutation Groups
And
Card Tricks

Russell Richins

The purpose of this presentation is to explain the "trick" behind a couple of simple card tricks, and to develop some of the mathematical machinery that is used to describe such things. The card tricks and their explanations are taken from

"Invariants Under Group Actions to Amaze Your Friends" by Douglas E. Ensley in Mathematics Magazine, December 1999, pg 383.

First, lets look at a really simple trick. The magician takes a deck of cards and allows the volunteer to cut the deck, then choose the card that is on top. The volunteer memorizes the chosen card and returns it face down to the top of the deck. The volunteer then is allowed to cut the deck as many times as he or she desires. When the deck is returned to the magician, he spreads the cards face up on a table and is magically able to discern which card the volunteer selected.

The trick: While the volunteer is memorizing the card he or she chose, the magician looks at the bottom card in the deck. When the cards are spread at the end of the trick, these two cards will still be adjacent.

What is preserved by the operations performed by the volunteer?

Next trick: The volunteer is given an ace from each suit and is instructed to do the following:

1. Stack the four cards face-up with the heart at the bottom, then the club, then the diamond, and finally the spade.

2. Turn the spade (the uppermost card) face down.

3. Perform any of the following operations as many times as desired and in any order:
   (a) Cut any number of cards from the top to the bottom.
   (b) Turn the top two cards over as one.
   (c) Turn the entire stack over.

4. Turn the topmost card over, then turn the top two cards over as one, and then turn the top three cards over as one.

The magician then predicts that the club is the only card facing the opposite way from the others.

The trick: Just as in the first example, the operations that the volunteer is allowed to perform maintain a property in the packet of cards that the magician desires, namely, that the club faces a direction opposite from the other cards when the instructions are completed. To prove that these instructions do indeed accomplish this, we'll need the language of basic group theory.

Definition: Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

Examples: Let G be the real numbers. Then regular multiplication, addition, and subtraction are binary operations on G.

Is division a binary operation on the real numbers?

Is multiplication a binary operation on the irrational numbers?

Another way of saying that an operation is a binary operation is to say that the set is closed under that operation.

Definition: Let G be a nonempty set together with a binary operation (usually called multiplication) that assigns each ordered pair (a,b) of elements of G an element of G denoted by ab. We say that G is a group under this operation if the following three properties are satisfied.

(1) Associativity. The operation is associative; that is, (ab)c=a(bc) for all a,b,c in G.

(2) Identity. There is an element e (called the identity) in G such that ae=ea=a for all a in G.

(3) Inverses. For each element a in G, there is an element b in G (caled an inverse of a) such that ab=ba=e.

Example: The sets of Integers, Rational numbers, and Real numbers are all groups under ordinary addition.

What is the identity element in each case?

What is the inverse of an element a?

Example: The set {1, -1,i,-i} is a group under multiplication. Note that -1 is its own inverse.

Example: The set of real numbers excluding zero is a group under multiplication.

Example: The set {0,1,2,...,n-1} is a group under addition modulo n. (a+b(mod n)=r where r is the smallest integer such that a+b=qn+r for some integer q).

Problems: (In all of these, use the group axioms)

(1) Give two reasons why the set of odd intergers under addition is not a group.

(2) Show by example that subtraction of real numbers is not associative.

(3) An abstract algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead, one of the nine integers was inadvertently left out, so that the list appeared as
1,9,16,22,53,74,79,81.
Which integer was left out? (This really happened!)

(4) Suppose the table below is a group table. (Just like a multiplication table from elementary school.) Fill in the blank entries.

	e	a	b	c	d
e	e				
a		b			e
b		c	d	e	
c		d		a	b
d					

Here is another example of a group. It's also the example that we need for our card tricks. Consider the set {1,2,...,n}, and let S_n be the set of all bijections from {1,2,...,n} to itself. (Remember, a bijection is a function that is both one to one and onto.)

One can verify that S_n is a group under the operation of function composition. This means if we take two such functions f and g, then their group "product" is f(g(k)). This is the group of permutations on n objects, otherwise known as the symmetric group on n objects.

We will use this group to show why our second card trick should work. We can think about the operations the volunteer is allowed to perform as a subgroup H (a subgroup is a subset of a group that is a group itself under the same operation) of S_8 (the four cards with two sides each make 8 objects) that is generated by the permutations

(*) ß=ABCD->BCDA, ∂=ABCD->B*A*CD, and π=ABCD->D*C*B*A*.
(An asterisk means that the card has been flipped)

For a subgroup to be generated by a set of elements of the larger group means that each element of the subgroup can be "built up" by applying those generating elements the right number of times and in the right order.

Proposition 1: Let C_0 be the set of arrangements of the cards that have 1 or 3 face down cards. Then any of the permutations in H take an element of C_0 to another element of C_0.

We say that C_0 is invariant under the action of H.

Proof: This follows form inspection of the definitions of the permutations in H. See line (*).

After the first two steps of the trick are performed, the cards are arranged as an element of C_0. The proposition says that throughout step 3, the cards will remain arranged with one card facing opposite of the rest.

Proposition 2: Let C_1 denote the arrangements of the packet of cards so that the number 3 card is two cards away from the "wrong way" card. Then C_1 is invariant under the action of H.

Proof: A packet of cards p in C1 must originally look like one of the following, where here an asterisk indicates a card reversed from the rest of the packet:

3,A,B*,C   C,3,A,B*   B*,C,3,A   A,B*,C,3

The following table shows what happens as each of the mappings ß, ∂, and π act on a packet p:

p	ß	∂	π
3,A,B*,C	A,B*,C,3	A,3,B,C*	C,B*,A,3
C,3,A,B*	3,A,B*,C	3,C,A*,B	B*,A,3,C
B*,C,3,A	C,3,A,B*	C*,B,3,A	A,3,C,B*
A,B*,C,3	B*,C,3,A	B,A*,C,3	3,C,B*,A

In every case, the property that defines C_1 is preserved.

Again, after the first two steps are performed, the cards are arranged as an element of C_1. Proposition 2 tells us that they will remain arranged as an element of C_1 throughout step 3.

Proposition 3: If the packet starts with the club two places away from the wrong way card, then the club will be the wrong way card after the final operation.

Proof: The final step may be represented as

> ABCD->A*BCD->B*ACD->C*A*BD (here * denotes opposite orientation from the original)

Since the original packet starts off with the club two away from the wrong-way card, we need to consider just the cases where (1) A or C is the club or (2) B or D is the club. In case (1), the operations above will reverse both the club and the wrong way card, resulting in the club being the wrong way card. In case (2), the operations will reverse only the two cards that are neither the club nor the wrong way card, resulting in the club being the wrong way card.