Introduction to Group Theory

Tatiana Shubin
shubin@math.sjsu.edu

INTRODUCTION

When we think of algebra the first thing that comes to mind is the study of polynomial equations and their solution. And duly so – for a long, long time algebra essentially had been that very study.

Of course, any linear or quadratic equation can easily be solved, and there's evidence suggesting that already Babylonians as early as 1800 BCE knew general procedures for solving both.

Solving cubic equations proved to be much trickier – the first description of a general way to solve them appeared in *Ars Magna* published in 1545 by Gerolamo Cardano, and the method was actually found shortly before that date. Soon after, Cardano's pupil invented a nice reduction procedure which allowed to solve quartic (4th degree) equations by constructing an associated cubic equation, solving it and then using its roots to find solution of the original equation. This method seemed to promise that a similar approach could be used to higher degree equations – just keep constructing auxiliary lower degree equations and solving them. Unfortunately, this did not work – so much so that all attempts to find a general method for solving even 5th degree equations failed.

Mathematicians were really perplexed. But of course they kept working. Instead of direct attacks, they turned their attention to the relationships between the roots of a given equation, and that finally led to the discovery of the marvelous world of symmetry and ultimately, to the idea of a group and other algebraic structures and the whole new field of mathematics which is called abstract algebra. But what about higher degree equations? It was by means of abstract algebra that the question was finally settled in the first half of 19th century – it's been proved that, in general, a polynomial equation of degree five and above cannot be solved in radicals (i.e., there is no way to get a solution formula which uses only algebraic operations of addition, subtraction, multiplication, division, and root extraction).

Meanwhile, the notion of a group has become one of the most important notions in mathematics. At the same time, it is also very widely used in applications. Finite groups are indispensable, besides studying algebraic equations, in as distinct fields as crystallography and coding theory, just to name a few.

Let us start with some very simple examples.

ACTION GROUPS

A nonempty collection of actions that can be performed one after another is called a *group* if every action has a counteraction also included in this collection, and the result of performing any two of these actions in a row is also included in the collection.

EXAMPLE 1. [5] "Turning Soldier" group. The group consists of the following four actions: stand still (*s*); turn right (*r*); turn left (*l*); turn around 180 degrees (*b*). Let's denote this group by $T = \{s, r, l, b\}$.

In order to see what happens when various actions are performed one after another, it is convenient to construct a table, called *multiplication table of the group*: we label each row and each column of the table by the elements of the group in some order, and we place in the matrix cell (i, j) the element that is *equal* to the *produc*t of the elements labeling the i^{th} row and j^{th} column of the table.

Now just stop for a second and see whether what you have just read makes any sense to you. You certainly should be perplexed by certain words! In particular, what exactly is meant by the product of actions? Actions are not numbers, so how do we multiply them? When we deal with an action group, we can combine a pair of actions by performing one of them and then following with the other one; and – just for convenience! – we say that we have multiplied these two actions. Now, we are really interested only in the final result and not in a particular way by which that result has been achieved. So if the soldier turns 180 degrees around and then turns right, the result is the same as if he simply turned left to begin with. **(Can you see it?)** Thus we say that the product of actions *b* and *r* equals *l*, and we write $rb = l$. (Notice the order in which we list the actions.)

Now let's go back to the multiplication table: if the 2^{nd} row is labeled by *r* and the 4^{th} column is labeled *b*, then we place *l* in the cell (2, 3). (**Can you fill in the entire table?**)

Notice that *s* = "doing nothing" is a very special action. Every group must have such an element. (**Why?**)

EXAMPLE 2. [5] "One Sock" group. $S = \{n, c, i, t\}$, where the actions are: *n* = do nothing; *c* = take the sock off and put it on the other foot; *i* = take it off, turn it inside out, then put it on the same foot again; *t* = take it off, turn it inside out, then put it on the other foot.

The next example is much more interesting (and important). While numbers measure size, groups measure symmetry. Symmetry is the property of an object to remain unchanged while undergoing changes. For every geometric figure *F* there exists its group of symmetry *S*(*F*), and the structure of this group tells us how much symmetry does the figure possess. In a more precise form, a *symmetry* is a motion that maps a figure onto itself. *Euclidean* motions are translations, rotations, reflections, and glides.

EXAMPLE 3. Let Δ denote an equilateral triangle. $S(\Delta)$ consists of 6 actions: 3 rotations with respect to the center (including 0 degree rotation), and 3 flips (reflections) around its medians. $S(\Delta)$ is usually denoted by D_3, and is called *the third dihedral group*. In general, D_n, the n^{th} dihedral group, is the group of symmetries of a regular n-gon.

Exercise 1. Find the number of elements in D_4; in D_n.

The number of elements of a group *G* is its important characteristic. It is called the order of the group *G* and it is denoted by $|G|$. If *G* is a finite set, $|G|$ is a positive integer; otherwise we say that *G* is of infinite order or simply infinite.

EXAMPLE 4. [1] Consider three solids: (1) a pyramid whose base is a regular polygon with 12 sides; (2) a regular hexagonal plate (a hexagonal prism); (3) a regular tetrahedron.

For simplicity, consider only rotational symmetries of these solids. For each solid, these symmetries form a group, G_1, G_2, and G_3, respectively.

G_1 consists of 12 rotations about the vertical axis, including the *identity* rotation.

G_2 consists of 5 rotations about the vertical axis; 1 rotation about each of 3 axes through the midpoints of the opposite vertical edges; 1 rotation about each of 3 axes through the center of the opposite rectangular side faces; the identity.

G_3 contains 2 rotations about each of the 4 axes through a vertex and the center of the opposite face; 1 rotation about each of the 3 axes through the midpoints of the opposite edges; the identity.

Thus $|G_1| = |G_2| = |G_3| = 12$. But clearly, the symmetries of these solids are distinctly different. One striking difference is the fact that one single rotation, when repeated, generates all rotations of the pyramid, but there is no such single rotation of the plate or the tetrahedron. There are other differences, as well. To name just one more, for the pyramid there is only one rotation which combined once with itself equals the identity. (**Which one?**) For the plate there are more such rotations (**how many?**); and for the tetrahedron, the number is still different (**what is it?**).

All these differences have to do with the way in which symmetries combine; in each case, the group of symmetries has a certain *algebraic structure*. Group theory studies this structure.

Before we go to the general group discussion, let's look once again at the group D_4. We can notice that some actions in this group form a group by themselves (can you list these actions?). We call such a subset a *subgroup*.

Exercise 2. Find all subgroups of D_4.

One of these subgroups contains 4 elements; it consists of all proper rotations of a square. Let us call it $R_4 = \{r_0, r_1, r_2, r_3\}$. Now, if we compare the multiplication tables of R_4 and *T* (see Example 1), we can see that these tables differ only by the letters used to denote the elements. After a suitable renaming ($s \to r_0$, $r \to r_1$, etc.) one table will become exactly the same as the other. Therefore these groups are indistinguishable from algebraic point of view, and they are called *isomorphic* groups.

Exercise 3. Are the groups R_4 and *S* isomorphic?

GENERAL GROUPS

A *group* is a nonempty set *G* together with a binary operation $\ast$ on *G* with the following properties:

(i) $a\ast(b\ast c) = (a\ast b)\ast c$ for all $a,b,c \in G$ (i.e., $\ast$ is *associative*);

(ii) There is an *identity* element $e \in G$ such that for all $a \in G, a\ast e = e\ast a = a$;

(iii) For each $a \in G$, there is an *inverse* element $a^{-1} \in G$ such that $a\ast a^{-1} = a^{-1}\ast a = e$.

Implicit in this definition is that the set G is *closed under the operation*, namely that $a\ast b \in G$ for all $a,b \in G$. It's worth to spend a few moments thinking about the notion of being closed. Let's recall the set T (Example 1) where the operation is that of performing actions one after another. Is T closed under this operation? What if instead of the entire set T we consider its various subsets? Which of them are closed? Now let $S = \{0, 1\}$. Is *S* closed under multiplication? under addition? Can you add one real number to S so that the new set would be still closed under multiplication? more than one number?

Now let's go back to the definition of a group. We will denote a group G with an operation $\ast$ by $(G,\ast)$. If in addition to the properties (i), (ii), and (iii), $(G,\ast)$ has the property that $a\ast b = b\ast a$ for all $a,b \in G$, then it is said to be *commutative* (or *abelian*).

Exercise 4. Can a group have two different identity elements?
Exercise 5. Can an element of a group have two different inverse elements?

Problem 1. Show that if $a\ast a = e$ for all $a \in G$ then *G* is abelian.

SOME MORE EXAMPLES OF GROUPS:

1. $(R,+)$, where R is the set of all real numbers, and + is ordinary addition.
2. $(Z_n,+)$, where $Z_n = \{0, 1, 2, \ldots, n-1\}$, and + denotes addition modulo *n*.
3. $(R^*, \cdot)$, where $R^* = R - \{0\}$, the set of all non-zero real numbers, and the operation is ordinary multiplication.
4. $(D_\infty, \circ)$, infinite dihedral group. Consider the real number line with the dots marking integers. Let t be the translation to the right through one unit, and let s be reflection in the origin. We set $D_\infty = \{e, t, t^{-1}, t^2, t^{-2}, \ldots, s, ts, t^{-1}s, t^2s, t^{-2}s, \ldots\}$; the operation is composition of transformations. This group has some properties similar to those of D_n: for example, $s^2 = e$ and $st^k = t^{-k}s$ (**Check!**), but unlike D_n, $t^k \neq e$ for any integer *k*.
5. $(\{z \in C \mid |z| = 1\}, \cdot)$. This is the set of all complex numbers with magnitude 1 under ordinary multiplication.

6. Let $n \geq 2$ be an integer, and let C_n be the set of all roots of the polynomial equation of degree *n*, $x^n - 1 = 0$. For example, if $n = 2$, $C_n = \{1, -1\}$, and if $n = 4$, $C_n = \{1, i, -1, -i\}$. In general, $C_n = \{1, \zeta_n, \zeta_n^2, \zeta_n^3, \ldots, \zeta_n^{n-1}\}$, where $\zeta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ is *the primitive* n^{th} *root of unity.* You can check that C_n is a cyclic group under multiplication of complex numbers.

Of course, $x^n - 1 = 0$ is a very special and simple equation; in order to fully understand when a general polynomial equation can or can't be solved in radicals, and why, you would need to learn a very beautiful part of abstract algebra called Galois Theory. The theory is named after a French mathematician, Évariste Galois who died in 1832 at the age of 21 but who had managed to make fundamental mathematical discoveries and create a whole new branch of mathematics. By the way, Galois was the first to use the word "group" in our present sense.

If $(G,\ast)$ is a group, we often refer to the group operation $\ast$ as "multiplication", and we omit writing the symbol $\ast$. Thus we write *ab* for $a \ast b$. Also, if $a \in G$, we denote the product of n copies of *a* by a^n, and the product of n copies of a^{-1}, by a^{-n} (of course, n must be a counting number). We also set $a^0 = e$.

Exercise 6. We agreed above that $a^{-n} = (a^{-1})^n$ for every positive integer *n* (this is simply the meaning of our notation). Is it true that $(a^{-1})^n = (a^n)^{-1}$? Why?

If G is finite and $a \in G$, there exists a positive n such that $a^n = e$. (**Why?**) The smallest positive integer n for which $a^n = e$ is called the *order* of *a*.

Problem 2. Can an infinite group have elements of finite order? Give an example of an infinite group that contains an element of order *n* for every $n \geq 1$.

Now we will consider one more, very important, example of a group.

PERMUTATION (OR SYMMETRIC) GROUPS

Let A be a set consisting of a finite number n of elements. For example, let *n* = 5, and let us denote the elements of A by numbers, A = {1, 2, 3, 4, 5}. A *permutation* α of A is a one-to-one function from A onto A (i.e., it is simply a rearrangement of the elements of A). It is convenient to denote a permutation by a table as follows.

$\alpha : \begin{pmatrix} 1 2 3 4 5 \\ 4 3 5 1 2 \end{pmatrix}$, where $\alpha(1) = 4, \alpha(2) = 3, \alpha(3) = 5, \alpha(4) = 1, \alpha(5) = 2.$

The product of two permutations is a permutation as well. If $\beta : \begin{pmatrix} 1 2 3 4 5 \\ 2 3 1 5 4 \end{pmatrix}$, then

$\alpha\beta = \begin{pmatrix} 1 2 3 4 5 \\ 4 3 5 1 2 \end{pmatrix} \begin{pmatrix} 1 2 3 4 5 \\ 2 3 1 5 4 \end{pmatrix} : \begin{pmatrix} 1 2 3 4 5 \\ 3 5 4 2 1 \end{pmatrix}$. Notice that we apply first β and then α.

The set of all permutations on *n* elements forms a group, S_n.

EXAMPLE 5. (This example is taken verbatim from [4].) In a high court of the kingdom of Permuterland, there are three judges for every trial. In the grand tradition of algebra, let's call them A, B, and C. They file in at the beginning of any trial and sit at the table in the order ABC.

But when the eccentric king of Permuterland who attends all trials yells “Promenade 1”, B and C change places; and when he yells “Promenade 2”, A and B change places; and when he yells “Promenade 3”, A goes to where C was sitting, B goes to where A was sitting, and C goes to where B was sitting.

Now in a hectic mood one day, the king yells “Promenade 1” and, two minutes later, yells “Promenade 2”. To his royal amazement, the king realizes that the judges are now seated exactly as they would be if, instead of yelling “Promenade 1” and then “Promenade 2”, he had just yelled “Promenade 3”.

The next day he decides to try this procedure again – but with a slight variation: now he yells “Promenade 2” first and then yells “Promenade 1” – and he is amazed to find out that the result is not the same as Promenade 3; indeed, the result is what he has been calling Promenade 4.

Of course, you recognize that the “Promenades” in this example are simply elements of S_n (**what is *n*?**), and that this example shows that S_n is non-abelian.

Exercise 7. What is the order of S_3? Of S_4? Of S_n?

Exercise 8. Find the order of every element of S_3.

In general, if $\pi \in S_n$, we denote it by $\pi = \begin{pmatrix} 1 & 2 & \ldots\ldots n \\ \pi(1) & \pi(2) & \ldots\ldots \pi(n) \end{pmatrix}$.

Exercise 9. Perform the indicated operations.

(i) Find $\pi\rho$ and $\rho\pi$ if $\pi = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$ and $\rho = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 2 & 6 & 7 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 4 & 1 & 3 & 5 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 1 & 5 \end{pmatrix}^{-1}$

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 7 & 6 & 2 & 3 \end{pmatrix}^{3}$

(v) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 2 & 9 & 8 & 12 & 3 & 4 & 1 & 11 & 5 & 7 & 6 \end{pmatrix}^{-2}$

Notice that the permutation π above has the effect of moving the elements around in a cycle. Thus we call it a *cycle of length* 3 and we write it as (1 3 2). This is just another notation for the same permutation: $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$, but it's actually more convenient.

We think of (1 3 2) as representing the following mapping: 1 → 3 → 2 → 1. Clearly, (1 3 2) = (3 2 1) = (2 1 3).

A cycle of length r is called an *r-cycle*. A 2-cycle is also called a *transposition* since it transposes two elements.

Exercise 10. Calculate $(1\ 3\ 5\ 6\ )^2$; $(1\ 3\ 5\ 6)^3$; $(1\ 3\ 5\ 6\ )^4$. What is the order of (1 3 5 6)?

Problem 3. Prove that an r-cycle is of order r.

Exercise 11.

Calculate the given expression.

(i) (1 3 4 2)(1 2 3);

(ii) $(1\ 5\ 3\ 4\ 2\ 6\ 9)^{-1}$;

(iii) Write the permutation $\begin{pmatrix} 12345678 \\ 32567814 \end{pmatrix}$ as a product of cycles.

Problem 4. Let π be any element of S_n and let ρ be an *r*-cycle. Prove that the product $\pi\rho\pi^{-1}$ is an *r*-cycle. (Hint: If $\rho = (x_1, x_2, \dots, x_r)$, then $\pi\rho\pi^{-1} = (\pi(x_1), \pi(x_2), \dots, \pi(x_r))$.)

Problem 5. Prove the following statements.

(i) Every permutation can be expressed as a product of *disjoint* cycles, i.e., cycles which have no common elements.

(ii) Every permutation can be expressed as a product of transpositions.

(iii) The order of the product of disjoint cycles is the least common multiple of the lengths of these cycles.

A permutation is said to be *even* if it can be expressed as the product of an even number of transpositions. A permutation is *odd* if it can be expressed as the product of an odd number of transpositions. For example, (123) and (12)(2543) are even since (123) = (13)(12), and (12)(2543) = (12)(23)(24)(25); while (1234) is odd since (1234) = (14)(13)(12). The identity permutation is even since (1) = (12)(12).

Problem 6. (i) Prove that the identity permutation is not odd.

(ii) Prove that every permutation in S_n is either even or odd but not both.

(iii) Prove that an *r*-cycle is even if and only if *r* is odd.

(iv) Prove that the product of two permutations is even if and only if they are of the same parity.

(v) Let A_n be the set of all even permutations of S_n. Prove that A_n is a subgroup of S_n. The group A_n is called the *alternating group on n elements.*

Let's recall now the group of all rotations of a regular tetrahedron (group G_3 of Example 4). Since the tetrahedron has four vertices and every rotation permutes them, it is obvious that G_3 must be a subgroup of S_4 (**Is it really clear to you? Why?**) But it is not the entire S_4 - rather it is set of all even permutations, A_4. (**Any explanation?**). On the other hand, the group of all rotations of a cube is really the entire S_4 ! Can you think of the four things in the cube which are being permuted by every rotation of the cube and whose group of permutations 'coincides' with the group of rotations of the cube?

GENERAL GROUPS AGAIN

Problem 7. (i) If $a \in G$ and *a* is of order k, what is the order of a^{-1}?

(ii) If the order of *a* is k, what is the order of a^m?

(iii) Prove that if the order of *ab* is k, then the order of *ba* is also k.

(iv) Suppose that the order of *a* is k, and let $H = \{e, a, a^2, a^3, \ldots a^{k-1}\}$. Prove that *H* is a subgroup of *G* (called the *cyclic subgroup generated by a*).

If the whole group *G* is generated by one of its elements, it is called a *cyclic group*.

Problem 8. (i) If *G* is cyclic, show that it is abelian.

(ii) If *G* is cyclic of order n, show that it contains an element of order n.

Problem 9. Show that D_n is non-abelian and hence non-cyclic, but it contains a cyclic subgroup of order n. (Hint: consider the set of all proper rotations of a regular n-gon.)

Cyclic groups have the simplest structure of all the groups. On the other hand, symmetric groups are, in a sense, the most complicated, and the most general. Arthur Cayley (1821-1895) was the first mathematician to deal with groups abstractly in terms of axioms, and he showed that any abstract group can be considered as a subgroup of a symmetric group.

Cayley's Theorem. Every group *G* is isomorphic to a subgroup of its symmetric group.

Problem 10. Prove Cayley's Theorem. (Hint: For each element g of *G*, define a permutation$\pi_g : G \to G$ by $\pi_g(x) = gx$. Then show that *G* is isomorphic to the subgroup $H = \{\pi_g \mid g \in G\}$.)

Because of this theorem, if you know all about permutation groups, you know all about group theory!

We have talked about two different orders: the order of a group, and the order of an element of the group. Is there any relationship between these two orders? The answer is yes, and the relationship is (partially) explained by the following theorem and its corollary.

Lagrange's Theorem. If G is a finite group and H is its subgroup, then the order of H divides the order of G.

Corollary. The order of an element divides the order of the group. (**Why?**)

ADDITIONAL PROBLEMS

11. (a) Let p be a prime, and let $Z_p^* = \{1,2,3,...p-1\}$. Prove that $(Z_p^*, \cdot)$ is a group, where the operation is multiplication modulo p. Now use Lagrange's Theorem to deduce ***Fermat's Little Theorem***: If p is a prime and b is any integer not divisible by p, then

$$b^{p-1} \equiv 1(\text{mod } p).$$

(b) Let n be a positive integer, $n > 1$, and let $U(n) = \{x \in Z \mid 1 \le x \le n, \textit{ and } \gcd(x, n) = 1\}$. Prove that $(U(n), \cdot)$ is a group, where the operation is again multiplication modulo n. What conclusion can you derive using Lagrange's theorem?

12. Let G be a collection of all rational numbers x which satisfy $0 \le x < 1$. Show that the operation

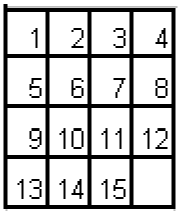
$$x + y = x + y \quad \textit{if} \quad 0 \le x + y < 1, \qquad \text{and} \qquad x + y = x + y - 1 \quad \textit{if} \quad x + y \ge 1$$

makes G into an infinite abelian group all of whose elements have finite order.

13. [3] A perfect interlacing shuffle (an in-shuffle) of a deck of 2n cards is the permutation I defined as follows: I(1)=2; I(2)=4; … ; I(n)=2n: I(n+1)=1; I(n+2)=3; … ; I(2n)=2n-1. In general, $I(k) \equiv 2k \ (\text{mod } (2n+1))$. For example, if the cards in an 8-card deck are originally in the order 12345678, after applying the perfect in-shuffle the order becomes 51627384.

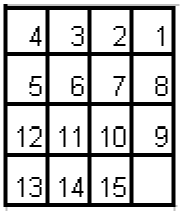
What is the least number of perfect in-shuffles that have to be performed on a deck of 52 cards before the cards are back in their original position? If there were 50 cards, what would be the least number?

14. [2] The well-known 15-puzzle consists of a shallow box filled with 16 squares in a 4×4 array. The bottom right corner square is removed, and the other squares are labeled as in Figure 1. We can slide the squares around without lifting them up. Which of the positions of the 15-puzzles shown in Figures 2, 3, and 4 can be achieved? Why?



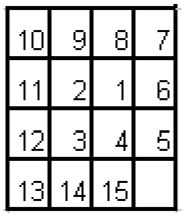
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Figure 1



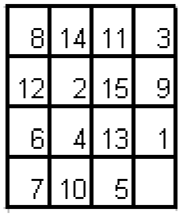
4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	

Figure 2



10	9	8	7
11	2	1	6
12	3	4	5
13	14	15	

Figure 3



8	14	11	3
12	2	15	9
6	4	13	1
7	10	5	

Figure 4

15. Prove that the converse of Lagrange's Theorem is not true: find the order of A_4 and then prove that it does not contain a subgroup of order 6.

16. Describe the group of all proper rotations of each of 5 regular polyhedra: (i) a tetrahedron; (ii) a cube; (iii) an octahedron; (iv) an icosahedron; (v) a dodecahedron.

17. Glue two regular dodecahedra together along a pentagonal face, and find the rotational symmetry group of this new solid.

18. (Putnam, 1972) Let S be a set, and let $\ast$ be a binary operation on S satisfying the two laws: (i) $x\ast(x\ast y)=y$ for all x, y in S; and (ii) $(y\ast x)\ast x=y$ for all x, y in S. Show that $x\ast y=y\ast x$ for all x, y in S.

19. (Putnam, 2006) Let 1, 2, 3, … ,2005, 2006, 2007, 2009, 2012, 2016, … be a sequence defined by $x_k=k$ for k = 1, 2, … , 2006 and $x_{k+1}=x_k+x_{k-2005}$ for $k\geq 2006$. Show that the sequence has 2005 consecutive terms each divisible by 2006.

REFERENCES AND FURTHER READING

1. Mark A. Armstrong, *Groups and Symmetry*, Springer, 1987
2. Neal H. McCoy, *Introduction to Modern Algebra,* 4th Edition (Revised by G. J. Janusz), Allyn and Bacon, Inc., 1987
3. S. Brent Morris, *Magic Tricks, Card Shuffling and Dynamic Computer Memories*, The Mathematical Association of America, 1998
4. Roy Dubish, *Groups*, (Topics For Mathematics Clubs), National Council of Teachers of Mathematics, 1973
5. Alexei Sosinski, *Finite Groups* (Kvant, 1996, no. 6; in Russian)
6. Joseph Gallian, *Contemporary Abstract Algebra*, 7th Edition, Brooks/Cole
7. David W. Farmer, *Groups and Symmetry, A Guide to Discovering Mathematics*, The American Mathematical Society