

Math 351:03 — Fall 1999  
MW4 SEC-217  
Prof. Bumby

**The Course Web Page.** Copies of all handouts and material prepared for lectures will be made available on the Web. You should be able to reach the page either from the Math Department courseware page or my personal page to locate the course material. The math department page is at

<http://www.math.rutgers.edu/>,

and this will have links for course material and faculty home pages.

**The next segment of the course.** We should follow the original plan for a second exam on Wednesday, November 17 since there is no other convenient date. This allows eight lectures and four workshops before the exam.

**Cycle notation.** Chapter 3 introduces a notation that allows easier computation in permutation groups —  $S_n$  and its subgroups. We consider  $S_n$  as  $A(\mathbf{n})$ , the permutations of a *standard set of  $n$  symbols*. I take  $\mathbf{n} = \{0, 1, \dots, (n - 1)\}$ , but some people prefer  $\{1, 2, \dots, n\}$ . We describe an element  $f$  that permutes the symbols in our standard set by writing the  $n$  equations of the form  $fi = j$ , usually sorted by the value of  $i$ . This is fairly convenient: if you want to find the image of  $i$  under  $f$ , you know exactly where to look for the equation that gives the answer. However, to verify that  $f \in S_n$  and find its inverse, you need to prepare a place to write a similar description of  $f^{-1}$  and use the description of  $f$  to write obtain the equation  $f^{-1}j = i$  for each  $i$  in order, and write it in the  $j^{\text{th}}$  line that you have prepared. This process will fail if the function  $f$  is not a permutation. Cycle notation rearranges the list and abbreviates it, so that you don't need to write as much. It will be harder to find how to apply  $f$  to a particular value  $i$  (unless  $n$  is small, as it *always* is in textbook examples), but the notation will certify that  $f$  is a permutation and clarify some of the structure of  $S_n$ . To create the cycle notation from a table of values, begin by denoting the action of  $f$  by an arrow. Start with 1, write the arrow, then the value of  $f1$ . If this is not 1, write another arrow and use the appropriate line of the definition of  $f$  to find what comes next. When a line of the definition of  $f$  has been used, cross it out (or mark it used in some other way); and when you come back to the number that started that cycle, end this chain and begin a new cycle starting from the first unused line in the definition of  $f$ . To get the abbreviated form, enclose each chain in parentheses and delete all the arrows and the last number in the chain (which is always the same as the first element in that chain). It has been conventional to remove cycles of length one, but this may be a false economy. While they have no effect on computing with the cycles they can be used to identify the symbol as belonging to  $S_n$  since there will be exactly  $n$  symbols mentioned in the description. If cycles of length one are not written, the proper notation for the identity would be an empty symbol, and this could be awkward.

As an example, suppose  $f0 = 1, f1 = 3, f2 = 6, f3 = 0, f4 = 5, f5 = 2, f6 = 9, f7 = 7, f8 = 4, f9 = 8$ . Then,  $0 \rightarrow 1 \rightarrow 3 \rightarrow 0, 2 \rightarrow 6 \rightarrow 9 \rightarrow 8 \rightarrow 4 \rightarrow 5 \rightarrow 2, 7 \rightarrow 7$ , and the cycle notation is  $(013)(269845)(7)$ .

Multiplying two such expressions is not convenient since you do not always know where a given number will appear in the cycle description, but *powers* are easy to find: to get the  $k^{\text{th}}$  power, you go through the cycles  $k$  steps at a time. The square of the element in our example is, after some rearrangement,  $(031)(294)(568)(7)$  and the cube is  $(0)(1)(28)(3)(46)(59)(7)$ .

**Beware! There are two different cycle notations.** Following the textbook, we write the name of a function to the left of its argument, so a composition of functions  $fg$  means, “first  $g$ , then  $f$ ”. However, we have also written the elements within each cycle in a left-to-right order. To multiply cycles start with the rightmost cycle going through it from the left. Write the first symbol in that cycle and note the symbol that follows it. Look for this symbol in cycles to the left of the one we are working with, and not the symbol to its right in that cycle, etc. When you have searched all cycles, write the number you last noted. Now go back the rightmost cycle and start looking for this symbol. The process is a little simpler if you are multiplying two permutations, since each symbol will appear exactly twice (if you don’t omit cycles of length 1), so the image of each element is the symbol in the first half of the product that follows the symbol that follows the given symbol in the second half of the product. Some people (probably almost everyone) find this confusing and reverse one of the conventions about the order in which things should be written to get a more natural multiplication. We won’t tamper with the conventions in the textbook. Instead, we will not do any computational work with this notation. In particular, I will waste no ink on an example here.

**Theoretical results revealed by cycle notation.** In the symmetric group  $S_n$ , consider the *inner automorphism*  $\sigma_a$  defined by  $\sigma_a(x) = axa^{-1}$ , and suppose that  $a$  is given by a complete table of values. For any  $x \in S_n$ , we investigate the relation between the table of values of  $x$  and that of  $\sigma_a(x)$ . To do this, take  $i$  in our standard set of  $n$  numbers and suppose  $xi = j$  for some  $j$  in the standard set. We now ask, “what equation in the description of  $\sigma_a(x)$  is determined by this?”. If it is  $(\sigma_a(x))r = s$ , then the definition of  $\sigma_a$  gives  $(axa^{-1})r = s$  where the first factor is a product in  $S_n$ , and this is a composition of mappings on the set of  $n$  elements. At the level of this set and its mappings, the parentheses can be dropped, and then reinserted in a different association, giving  $s = axa^{-1}r = a(x(a^{-1}r))$ . Since we want to use  $xi = j$ , we need  $i = a^{-1}r$ , which is equivalent to  $r = ai$ , and we get  $s = aj$ . That is, we apply  $a$  to the elements of the standard set appearing in the equations defining  $x$  to get the equations defining  $\sigma_a(x)$ . Of course, these equations need to be rewritten in a useful order, since we have found them sorted by the value of  $i$ .

However, if  $x$  is given in cycle notation, the description in the previous paragraph is enough to find the cycle notation for  $\sigma_a(x)$ . Suppose that  $x$  is given in cycle notation. The equations defining  $x$  say that each element is taken to the next element in the cycle containing it. Applying the previous paragraph to *all* of these equations is equivalent to applying  $a$  to the symbols appearing in the cycles. This proves a result that is hinted at in many exercises in the textbook. In particular, for any  $a$ , the action of  $\sigma_a$  takes every element into one that has the same number of cycles of each length.

**Generating the symmetric group by transpositions.** A **transposition** is a permutation that interchanges one pair elements and fixes everything else. We will show that every element of  $S_n$  can be written as a product of transpositions. This property is often stated as saying that the transpositions *generate*  $S_n$ . A simple counting argument shows that there are  $n(n - 1)/2$  transpositions in  $S_n$ . To prove that  $S_n$  is generated by transpositions, it is easier to show the stronger result that the  $n - 1$  transpositions  $(01), (12), \dots, (n - 2, n - 1)$  generate  $S_n$ . (Since  $S_1$  is the trivial group, it really can be generated by nothing.) This statement is proved by a process known as “bubble sort”.

To show this, identify  $f \in S_n$  with the sequence of numbers  $f0, f1, \dots, f(n - 1)$ . Multiplication of  $f$  on the right by the transposition  $(j, j + 1)$  has the effect of interchanging the  $j^{\text{th}}$  element of the sequence of values with the one following it. If we are able to sort the list by these operations, we will have  $f$  times a product of transpositions equal to the permutation whose sequence of values is  $0, 1, \dots, n - 1$ . The permutation with this list of values is the identity, so we have found an inverse of  $f$  as a product of transpositions. To get  $f$  we take product of the same transpositions in the opposite order.

It remains to have a procedure to pick the transpositions, i.e., the sequence of  $j$  for which we interchange the  $j^{\text{th}}$  element with the one following it. In the usual description of the bubble sort, this is done by starting at the beginning of the list: if the element in the  $j^{\text{th}}$  position is smaller than the next element, do nothing; if

not, put the old element from the  $(j + 1)^{\text{st}}$  place in the  $j^{\text{th}}$  place and treat the old  $j^{\text{th}}$  element as the  $(j + 1)^{\text{st}}$  element, and record the location of the interchange. In any case, you are now looking at the  $(j + 1)^{\text{st}}$  element, and you should continue performing the same test. When you reach the end, the list is known to be correctly sorted and contain the largest elements from the point of the last interchange on (it may have more elements that are correctly sorted, but we don't *know* that yet). Go back to the beginning of the list and repeat the process, although it is possible to stop when you reach the point beyond which the list has been sorted. On each pass, more of the list is sorted, so this process terminates. Although this is not an efficient method of sorting, this theoretical application earns the bubble sort a place in our toolkit.

**Parity and the alternating group.** There are some very slick ways to show that, if one expression of a permutation as a product of transpositions has an even number of factors, then every expression of that permutation as a product of transpositions has an even number of factors. Such permutations are called *even*. Once one has this, we show that the set of even permutations forms a subgroup. The identity is even since it is a product of zero factors. The inverse of an even permutation is even since it is the product of the same factors in the reverse order. A product of two even permutations is even since it is the product of the transpositions giving the first factor followed by the product giving the second factor. The total number of transpositions is the sum of those used to give the factors, and a sum of two even numbers is even. This shows that the even permutations form a subgroup. Indeed, it is a normal subgroup. This can be shown by showing counting the number of transpositions in  $aga^{-1}$  for arbitrary  $a$  and even  $g$ , or by showing that the function giving the number of transpositions modulo 2 is a homomorphism. The distinction between even and odd permutations is a key feature in defining the determinant of a square matrix, so you have probably already seen a proof that parity of permutations is well-defined. However, it may be useful to give a concrete proof of this fact.

From abstract considerations, it suffices to show that every representation of the identity has an even number of factors, and it will be in this form that the result will be proved. We outline a proof of the result for all symmetric groups  $S_n$  at the same time, treating each them as the set of all permutations of some set of nonnegative integers. It will be necessary to induction on the number of factors, the largest number appearing in one of the transpositions, and the position of the factor in which that largest number appears. Glossing over the details, the basis for this multiple induction is that an empty product contains zero, an even number, terms and represents the identity, and if the largest number  $N$  last appears in the first factor (in order of operation) of the permutation  $f$  and that factor is  $(i, N)$  with  $i < N$ , then  $f(i) = N$ , so  $f$  is not the identity. The innermost inductive step consists of some formulas showing that certain products of transpositions are equal. Again denoting the last factor containing  $N$  as  $(i, N)$  with  $i < N$ , and looking at the previous factor (this is the inductive step, so there is a previous term, the basis took care of the possibility that it is the first term). There are four possibilities for this previous term (which is written to the right of  $(i, N)$  because of the order of operation):  $(i, N)$ ,  $(i, a)$ ,  $(a, N)$ , or  $(a, b)$ , where  $a$  and  $b$  are different from  $i$  and  $N$ . In the first case,  $(i, N)(i, N)$  is the identity, so the two terms drop out and everything simplifies. In the remaining three cases, the appearance of  $N$  will shift from the term on the left to the term on the right. This uses an induction on the location of the last appearance of  $N$ . The formulas are:

$$(i, N)(i, a) = (i, a)(a, N)$$

$$(i, N)(a, N) = (i, a)(i, N)$$

$$(i, N)(a, b) = (a, b)(i, N)$$

In each of these cases, we have the same number of terms involving the same symbols, but  $N$  does not appear in the later operation.

This ends our discussion of groups. Exercises from the text are not particularly useful, so we will move ahead as quickly as possible. The extended discussion of the symmetric group above is intended to be more of a substitute for the text than a supplement.

**Rings.** Chapter 4 introduces the concept of a ring. The main example is the integers with the operations of addition and multiplication. Since we want our abstraction to reflect properties of the integers, it is better to insist that there be an identity element for multiplication, which will be denoted  $1$ , in the ring. The slight extra generality that you get by allowing things like the set of even integers to be a subring of the set of all integers does not seem to lead to anything useful. It seems better to have a definition in which the integers have no subrings. Although changes of definitions can change the statements of some theorems, there is no change in the way in which things are proved. As more theorems are accumulated, definitions can change in order to allow more useful statements of the better theorems. Not every proposed definition turns out to be useful, and as the subject matures, definitions can change. In particular, it now seems better to include  $1$  as a fundamental part of a ring.

One result of abstracting the idea of a ring will be that the similarity that we observe between properties of integers and properties of polynomials will be seen to allow an abstract explanation. Starting from the definition of a ring, we can ask what do we need in order to be able to have the sort of factorization theory that we observe for integers or polynomials, and we are led to an abstract version of the Euclidean algorithm.

It turns out that this is not the only way that one can have unique factorization. If possible, I will give example at the end of the course. Note that one needs an abstract theory to be able to *state* such a result, so it provides an answer to the question, “What can I do with abstract algebra that I can’t do without it?”

**Extensions.** The construction used to obtain the complex numbers from the real numbers can be described in a very general setting. The goal of our treatment of constructions in ring theory should be to show that, if a ring doesn’t contain a number that you think it should, you can create a new ring that will have that number.

**Matrices and Quaternions.** Although we can do a lot with commutative rings, our definition allows a noncommutative multiplication. The ring  $M$  of all  $n$  by  $n$  matrices with coefficients in your favorite ring  $R$  ( $R$  may be commutative, but the construction works over any ring) will not be commutative if  $n > 1$ , so we have a wealth of examples of noncommutative rings. One has the feeling that these examples are typical in the sense that much work consists of finding abstract conditions that will require a ring to look like a ring of matrices.

Another example that is given in Section 4.1 is the quaternions. Here, one adds a *different* square root of  $-1$  to the complex numbers, sacrificing commutativity while retaining a *group* of nonzero elements under multiplication. A similar construction starting from the integers instead of the real numbers is also possible. Using the algebra of these integer quaternions, it is possible to show that every integer is a sum of four squares.

**Fields.** A ring in which the nonzero elements form a (commutative) group under multiplication is called a field. The basic theory of *vector spaces*, except for topics involving the usual *inner product*, requires only a *field* of scalars. This plays a role in a first course in linear algebra by allowing all example to be defined over the rational numbers while we pretend that we are working over real numbers.

Another collections of examples are the finite fields. The most general examples are obtained by extension, but the *prime fields* already give useful examples. These are obtained by considering the integers modulo a prime.

**Homework.** Based on the results from the first part of the course, problems have been selected that should be interesting without slowing your progress very much. The aim in this section of the course will be to stay close to the textbook as much as possible while emphasizing topics that will provide a background for topics after the second hourly that reflect the interest of the lecturer.

A rapid pace has been set for Chapter 3 and the beginning of Chapter 4. Some of this material is sure to get light treatment as we rush through these sections. It is expected that there will be some time to fill in the details in the context of later topics. The value of the abstract approach lies in its ability to unify the study of questions arising in different settings. It seems better to try to get to the point where the abstraction is used rather than concentrating on working with the formal properties of the axioms. In many of the sections, none of the textbook exercises seem suitable. However, variants on them may appear as workshop problems.

Date	section	page	problems
October 20	3.1	110	NONE.
	3.2	117	16, 20.
	3.3	123	8.
October 25	4.1	133	30.
	4.2	139	4.
October 27	4.3	146	NONE.
	4.4	150	2.
November 01	4.5	163	14.
	4.6	171	NONE.
November 03	4.7	175	NONE.
November 08	5.1	179	7.
November 10	5.2	189	NONE.
November 15	5.3	197	7, 13.