SOAR Math Course Homework Nine Spring, 2003

These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. Of the following numbers, one is prime and the others are composite. Of the composites, one is a base 2 pseudo-prime, another is a base 3 pseudo-prime, and the final one is simply composite. Discover which is which, and explain how you did it.

   (a) 2701 (b) 1441 (c) 1891 (d) 1531

Related to work we did in class today is the group $\mathbf{On}_2$, which consists of the set $\mathbf{Z}^{\geq 0} = \{0, 1, 2, 3, \ldots\}$ of non-negative integers with the operation $\oplus$ given by the following two rules:

(i) If $m \neq n$, then $2^m \oplus 2^n = 2^m + 2^n$ (here $+$ is ordinary addition).

(ii) $x \oplus x = 0$ for any $x \in \mathbf{Z}^{\geq 0}$.

These two rules generate $\oplus$ for any two non-negative integers as in the following example:

$$\begin{aligned} 7 \oplus 11 &= (4 + 2 + 1) \oplus (8 + 2 + 1) \\ &= 8 \oplus 4 \oplus (2 + 2) \oplus (1 + 1) \\ &= 8 + 4 + 0 + 0 \\ &= 12. \end{aligned}$$

The two rules for our addition can be re-written as

(i)′ If $y < x$ and $x = 2^k$, then $x \oplus y = x + y$ (ordinary addition).

(ii)′ If $x = 2^k$, then $x \oplus x = 0$.

You should convince yourself (by the end of these assignment) that these new rules are the same as the old rules. (I've taken this group from John H. Conway's book *On Numbers and Games*.)

2. Complete the following addition table for the group $\mathbf{On}_2$. This should help familiarize you with the operations, as well as convince you of some of the facts you will

need to explain in the next problem.

$\oplus$	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

3. We now show that this group $\mathbf{On}_2$ is actually a group. We verify each of the four axioms of groups as follows.

   (a) **[Identity]** Show that the element 0 is the identity in $\mathbf{On}_2$. That is, show that $x \oplus 0 = x$ and $0 \oplus x = x$ for any element x of $\mathbf{On}_2$. (There's really almost nothing to do here.)

   (b) **[Inverses]** Find the inverse of an element x of $\mathbf{On}_2$. That is, given x, find y such that $x \oplus y = 0$.

   (c) **[Closure]** If x and y are non-negative integers, then $x \oplus y$ is as well. Explain why this is so.

   (d) **[Associativity]** Show that $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ for any three elements x, y, and z of $\mathbf{On}_2$. (For simplicity, you may assume that $x \leq y \leq z$. Even in this case, there are still many cases: $x = y$, or $x \oplus y < z$, or $x \oplus y > z$, and so on. As usual, this is a bit tedious, so feel free to skip this part if you like.)

4. We now relate $\mathbf{On}_2$ to addition in base 2. We usually use base 10, which means that, for example, $17 = 1 \times 10^1 + 7 \times 10^0$. Another base (like 2) means we change the value 10 to 2. So 17 in base 10 is 10001 in base 2:

$$10001 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0.$$

   Addition is now just like base 10, except that $1 + 1 = 10$ in base 2, so carrying occurs quite a lot. For example:

$$\begin{array}{cccccccc} & & 1 & 1 & 0 & 0 & 1 & 0 \\ + & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

   (a) Compute $1001010101 + 1000111001$ in base 2. Check your answer by converting all three terms (the sum and the summands) into base 10.

(b) The addition in $\mathbf{On}_2$ is simply summation in base 2 *with no carrying*. That is, without any carrying, the above example would be:

$$\begin{array}{rcccccccc} & & 1 & 1 & 0 & 0 & 1 & 0 \\ + & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Explain why this is the same as addition in $\mathbf{On}_2$.

(c) Explain why one way to view the winning strategy in Nim is to use summation in $\mathbf{On}_2$. (This is why Conway calls $\oplus$ "Nim" and reads $2 \oplus 4$, for example, as "two Nim four.")

A new feature this week is the *group of the week*. We won't dwell on the abstract idea of a group, but with each homework for the next few weeks I'll give you a new group to play with.

This week's group is the set

$$G = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \text{ are real and } ad - bc \neq 0 \right\}$$

together with the operation $*$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{bmatrix}.$$

(These funny squares are called *matrices*, the plural of *matrix*, and the operation $*$ is called *matrix multiplication* (and the symbol $*$ is usually not written).)

For example, the matrix $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$ is in G since $2 \cdot 4 - 3 \cdot 1 = 5 \neq 0$, but the matrix $\begin{bmatrix} 2 & -2 \\ 1 & -1 \end{bmatrix}$ is *not* in G as $2 \cdot -1 - (-2) \cdot 1 = 0$. Also, as an example of multiplication,

$$\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} * \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 \cdot 0 + 3 \cdot 1 & 2 \cdot 2 + 3 \cdot 1 \\ 1 \cdot 0 + 4 \cdot 1 & 1 \cdot 2 + 4 \cdot 1 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 4 & 6 \end{bmatrix}.$$

The first of the following problems should help orient you with G, and the next four problems together form a proof that this week's example is a group.

5. Two of the following three matrices are in G, and one is not. Identify which one is not, and multiply the other two together both ways. (That is, both $A * B$ and $B * A$ if A and B are both in G.)

$$A = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix} \qquad B = \begin{bmatrix} -1 & 3 \\ -2 & 6 \end{bmatrix} \qquad C = \begin{bmatrix} 2 & -1 \\ 2 & 1 \end{bmatrix}.$$

6. [**Identity**] Show that the element $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity in G. This means you must show that $I \in G$ (that is, I is an element of G) and that $I * A = A = A * I$ for any element A of G.

7. [**Inverses**] Show that if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an element of G, then

$$A^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

is its inverse. Again, you must show both that $A^{-1} * A = I$ and $A * A^{-1} = I$. Also, you should show that A^{-1} is an element of G.

8. [**Closure**] Show that if A and B are elements of G, then so is $A * B$. Hint: show that

$$(ax + bz)(cy + dw) - (ay + bw)(cx + dz) = (ad - bc)(xw - yz).$$

9. [**Associativity**] (This is a bit tedious, so you should feel free to skip it.) Show that if A, B, and C are elements of G, then $A * (B * C) = (A * B) * C$.

10. In this problem, we show that for elements A and B of G, $A * B$ need not equal $B * A$. (This is different than ordinary multiplication, of course.) To see this, we need only produce an example.

    (a) Show that $A * B \neq B * A$ when

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}$$

    (b) Let

$$A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix}$$

    For what values of a and b does $A * B = B * A$? For what values of a and b does $A * B \neq B * A$?

    If $A * B$ always equals $B * A$, then a group is called *commutative* or *abelian*. You've just shown that $\mathrm{Gl}(2, \mathbf{R})$ is non-commutative (or non-abelian).

11. Why do we require $ad - bc \neq 0$? This problem gives the reason.

    (a) Show that $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is not in the group G.

    (b) Show that $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ has no inverse as follows. Assume that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the inverse, so

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

    Now try to solve for a, b, c, and d in this equation, and show that it isn't possible to do so.

You've just shown that a particular element is not in G *and* has no inverse. In fact, this is what always happens: a matrix has an inverse exactly when it is in G. Looked at another way: a matrix has *no* inverse exactly when it is *not* in G.

This week's group is usually called the *general linear group* of two-by-two real matrices, and written $\mathrm{Gl}(2, \mathbf{R})$. (The 2 is for the fact that the matrices each have two rows and two columns, and the $\mathbf{R}$ indicates that the elements in each matrix is a real number.) In fact, we've already seen these – each matrix corresponds to a transformation as in Homework 6, Problem 200:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad \text{corresponds to} \qquad \begin{aligned} x' &= ax + by \\ y' &= cx + dy \end{aligned}$$

(In fact, the unimodular transformations from Homework 6 can be thought of as a subgroup of $\mathrm{Gl}(2, \mathbf{R})$, but we won't go into that.) As you might expect, the 2 may be replaced by any other positive integer n, and the real numbers $\mathbf{R}$ may be replaced with the rationals (fractions), integers (as in Homework 6), complex numbers, or even such things as $\mathbf{Z}_p$ (the integers modulo a prime p). There are also matrices that aren't square – that is, that do not have the same number of rows and columns. The study of matrices is a rich and well-developed; an introductory course in the subject (usually called linear algebra) is often taken by second-year university students.