Applied Algebra

Instructions Please answer these questions on your own paper. Explain your work in complete sentences.

1. Write the permutation (1 2 3)(3 4 5)(4 5 6) as a product of *disjoint* cycles.

   Solution. Remembering to read the product from right to left, you can trace the image of each number as follows: $1 \to 1 \to 1 \to 2$, $2 \to 2 \to 2 \to 3$, $3 \to 3 \to 4 \to 4$, $4 \to 5 \to 3 \to 1$, $5 \to 6 \to 6 \to 6$, $6 \to 4 \to 5 \to 5$. Thus the permutation equals the product of disjoint cycles (1 2 3 4)(5 6).

2. What is the highest possible order of an element of the symmetric group $S(10)$?

   Solution. You know that every permutation can be written as a product of disjoint cycles, and the order of such a product equals the least common multiple of the lengths of the cycles. The product of a 7-cycle and a 3-cycle has order 21, and that is the highest order you can get with a product of two cycles. But you can do better with a product of three cycles: the product of a 5-cycle, a 3-cycle, and a transposition has order 30. That 30 is the maximum can be seen by considering all the possible partitions of 10.

3. Consider the operation $*$ defined on the positive real numbers as follows: $a * b = 5ab$ (where ab on the right-hand side denotes ordinary multiplication). Does this operation $*$ provide the positive real numbers with a group structure?

   Solution. The operation is well defined: if a and b are positive, then so is $5ab$. The operation is associative: both $(a * b) * c$ and $a * (b * c)$ are equal to $25abc$. The number $1/5$ is an identity element for the operation: $a * (1/5) = a$ for every a. The inverse of a is $1/(25a)$. Thus all the properties of a group are satisfied.

   Remark This group is isomorphic to the group of positive real numbers under the usual multiplication operation. Indeed, if $f\colon (\mathbb{R}^+, *) \to (\mathbb{R}^+, \cdot)$ is defined by setting $f(a)$ equal to $5a$, then $f(a*b) = f(a) \cdot f(b)$.

Applied Algebra

4. Consider the set of 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$, where a and b are elements of $\mathbb{Z}_2$ (the integers mod 2). Suppose such matrices are added and multiplied in the usual way, but with the arithmetic done in $\mathbb{Z}_2$. Is this structure a ring?

   Solution. First of all, the additive structure is a group: the sum of two matrices of the indicated form is another one (closure); addition of matrices is associative; the zero matrix (the additive identity) has the indicated form ($a = b = 0$); and every matrix is its own additive inverse under addition mod 2. Secondly, since

$$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} = \begin{pmatrix} ac & 0 \\ ad + bc & ac \end{pmatrix},$$

   the set is closed under matrix multiplication, and the multiplication operation is even commutative; matrix multiplication is an associative operation; and matrix multiplication distributes over matrix addition. Thus all the properties of a ring are satisfied.

5. Suppose H and K are subgroups of a group G. Is the union $H \cup K$ necessarily a subgroup of G?

   Solution. Almost any example you try will provide a counterexample. For instance, let G be the group of integers under addition, let H be the subgroup consisting of even integers, and let K be the subgroup consisting of integers divisible by 3. The set $H \cup K$ is not a subgroup, for it is not closed under addition: both 2 and 3 are elements of $H \cup K$, but their sum 5 is not an element of $H \cup K$.

6. Let G denote the multiplicative group of invertible congruence classes of integers modulo 15. The group G has subgroups of what orders?

   Solution. The group G has order 8, as you can see either by computing that $\varphi(15) = \varphi(3)\varphi(5) = 2 \times 4 = 8$ or by simply listing the elements of G: namely, [1], [2], [4], [7], [8], [11], [13], and [14]. By Lagrange's theorem, the only conceivable orders of subgroups are divisors of 8: namely, 1, 2, 4, and 8. All of these candidates actually are orders of subgroups of G in this example, for the trivial subgroup $\{[1]\}$ has

order 1, the whole group G itself has order 8, the subgroup $\{[1],[4]\}$ has order 2, and the subgroup $\{[1],[2],[4],[8]\}$ has order 4.

7. Give an example of two finite groups of the same order that are not isomorphic groups.

Solution. The Klein 4-group has order 4 but is not cyclic, so it is not isomorphic to $(\mathbb{Z}_4,+)$; the symmetric group $S(3)$ has order 6 but is not abelian, so it is not isomorphic to $(\mathbb{Z}_6,+)$; other examples are possible.

8. Suppose a coding function $f\colon \mathbf{B}^3 \to \mathbf{B}^6$ is determined by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Suppose a message encoded by this function is received with errors as

$$101101 \quad 010101 \quad 011111.$$

Decode the received message.
[If you write your decoded message as three words in $\mathbf{B}^3$ and convert each binary word into an equivalent single decimal digit, then you will know if you have the right answer.]

Solution. Method 1. Here is a list of the eight codewords (linear combinations over $\mathbb{Z}_2$ of the rows of the generator matrix):

000000
100101
010110
001011
110011
101110
011101
111000

By inspection, you can see that the first received word, 101101, must decode to the second codeword, 100101, from which it differs in one

place. The second received word, 010101, decodes to the seventh codeword, 011101, from which it differs in one place. The third received word, 011111, also decodes to the seventh codeword, from which it differs in one place.

The original words in $\mathbf{B}^3$ are the first three binary digits of the decoded words: 100 011 011. Since 100 in binary converts to 4 in base ten, and 11 in binary converts to 3 in base ten, the base ten equivalent of the message is 4 3 3, the course number.

Method 2. This code has the following parity-check matrix:

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Here are the first seven coset leaders and corresponding syndromes:

000	000000
001	000001
010	000010
100	000100
011	001000
110	010000
101	100000

The first received word, 101101, has syndrome 011, so this word decodes to 101101 + 001000, which equals 100101. The second received word, 010101, has syndrome 011, so this word decodes to 010101 + 001000, or 011101. The third received word, 011111, has syndrome 010 and decodes to 011111 + 000010, or 011101. The answer is the same as before.

Bonus problem for extra credit Complete the following group table. (Although the group elements are labeled 1 through 9, the group operation $*$ is neither ordinary addition nor ordinary multiplication, and the number 1 is not the identity element.)

Applied Algebra

$*$	1	2	3	4	5	6	7	8	9
1	9								6
2		6						7	
3			8				5		
4				7		1			
5					5				
6				1		2			
7			5				1		
8		7						4	
9	6								3

Notice that this problem is not a sudoku! On the one hand, there is no constraint on 3×3 subsquares. On the other hand, you have the full power of a group law to help fill in the entries.

Solution. You can get a lot of information from the group law. For instance, since $5 * 5 = 5$, the element 5 is the identity element, so you can immediately fill in the middle row and the middle column of the table. Since $(1 * 1) * 9 = 9 * 9 = 3$, and $1 * (1 * 9) = 1 * 6$, the associative law reveals that $3 = 1 * 6$. Although you can continue to play games with the associative law to get more entries, there is a systematic way to complete the table.

Since $1 * 1 * 1 = 1 * 9 = 6$, the element 1 does not have order three. By Lagrange's theorem, the only possible orders of elements in a group of order nine are one, three, and nine. Therefore the element 1 must have order nine. Thus the group is cyclic, and the element 1 is a generator. If you write g as an alternate designation of the element 1, then you can use multiplicative notation for the group operation.

Applied Algebra

Now $g^2 = 1*1 = 9$, $g^4 = 9*9 = 3$, $g^8 = 3*3 = 8$, $g^7 = g^{16} = 8*8 = 4$, $g^5 = g^{14} = 4*4 = 7$, $g^3 = 1*1*1 = 6$, $g^6 = 6*6 = 2$, and $g^0 = 5$. The identification of each group element as a power of g makes it simple to determine any product in the group. For instance, $7*2 = g^5 g^6 = g^{11} = g^2 = 9$. Here is the complete table:

	g	g^6	g^4	g^7	id	g^3	g^5	g^8	g^2
$*$	1	2	3	4	5	6	7	8	9
g 1	9	4	7	8	1	3	2	5	6
g^6 2	4	6	1	3	2	5	9	7	8
g^4 3	7	1	8	9	3	4	5	6	2
g^7 4	8	3	9	7	4	1	6	2	5
id 5	1	2	3	4	5	6	7	8	9
g^3 6	3	5	4	1	6	2	8	9	7
g^5 7	2	9	5	6	7	8	1	3	4
g^8 8	5	7	6	2	8	9	3	4	1
g^2 9	6	8	2	5	9	7	4	1	3