

MATH 433  
Applied Algebra

**Lecture 26:**  
**Review for Exam 2.**

## Topics for Exam 2

- Relations, properties of relations
- Finite state machines, automata
  
- Permutations
- Cycles, transpositions
- Cycle decomposition of a permutation
- Order of a permutation
- Sign of a permutation
- Symmetric and alternating groups
  
- Abstract groups (definition and examples)
- Semigroups
- Rings, zero-divisors
- Fields, characteristic of a field
- Vector spaces over a field
- Algebras over a field

# What you are supposed to remember

On permutations:

- Definition of a permutation, a cycle, and a transposition
- Theorem on cycle decomposition
- Definition of the order of a permutation
- How to find the order for a product of disjoint cycles
- Definition of even and odd permutations

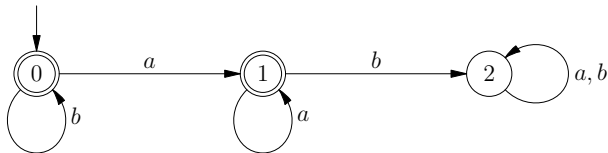
On algebraic structures:

- Definition of a group
- Definition of a semigroup
- Definition of a monoid
- Definition of a ring
- Definition of a field
- Definition of a vector space over a field

## Sample problems

**Problem 1.** Let  $R$  be a relation defined on the set of positive integers by  $xRy$  if and only if  $\gcd(x, y) \neq 1$  (“is not coprime with”). Is this relation reflexive? Symmetric? Transitive?

**Problem 2.** A Moore diagram below depicts a 3-state acceptor automaton over the alphabet  $\{a, b\}$  which accepts those input words that do not contain a subword  $ab$  (and rejects any input word containing a subword  $ab$ ). Prove that no 2-state automaton can perform the same task.



## Sample problems

**Problem 3.** List all cycles of length 3 in the symmetric group  $S(4)$ . Make sure there are no repetitions in your list.

**Problem 4.** Write the permutation  $\pi = (4\ 5\ 6)(3\ 4\ 5)(1\ 2\ 3)$  as a product of disjoint cycles.

**Problem 5.** Find the order and the sign of the permutation  $\sigma = (1\ 2)(3\ 4\ 5\ 6)(1\ 2\ 3\ 4)(5\ 6)$ .

**Problem 6.** What is the largest possible order of an element of the alternating group  $A(10)$ ?

## Sample problems

**Problem 7.** Consider the operation  $*$  defined on the set  $\mathbb{Z}$  of integers by  $a * b = a + b - 2$ . Does this operation provide the integers with a group structure?

**Problem 8.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

## Sample problems

**Problem 9.** Let  $L$  be the set of the following  $2 \times 2$  matrices with entries from the field  $\mathbb{Z}_2$ :

$$A = \begin{pmatrix} [0] & [0] \\ [0] & [0] \end{pmatrix}, \quad B = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix},$$
$$C = \begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix}, \quad D = \begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}.$$

Under the operations of matrix addition and multiplication, does this set form a ring? Does  $L$  form a field?

**Problem 10.** For any  $\lambda \in \mathbb{Q}$  and any  $v \in \mathbb{Z}$  let  $\lambda \odot v = \lambda v$  if  $\lambda v$  is an integer and  $\lambda \odot v = v$  otherwise. Does this “selective scaling” make the additive Abelian group  $\mathbb{Z}$  into a vector space over the field  $\mathbb{Q}$ ?

**Problem 1.** Let  $R$  be a relation defined on the set of positive integers by  $xRy$  if and only if  $\gcd(x, y) \neq 1$  (“is not coprime with”). Is this relation reflexive? Symmetric? Transitive?

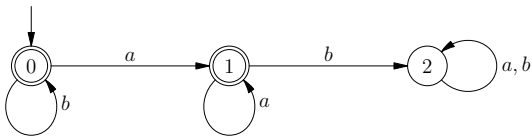
The relation  $R$  is not reflexive since 1 is not related to itself (actually, this is the only positive integer not related to itself by  $R$ ).

The relation is symmetric since  $\gcd(x, y) = \gcd(y, x)$  for all  $x, y \in \mathbb{P}$ .

The relation is not transitive as the following counterexample shows:  $2R6$  and  $6R3$ , but 2 is not related to 3 by  $R$ .



**Problem 2.** A Moore diagram below depicts a 3-state acceptor automaton over the alphabet  $\{a, b\}$  which accepts those input words that do not contain a subword  $ab$ . Prove that no 2-state automaton can perform the same task.



Assume the contrary: there is an automaton with two states 0 (initial) and 1 that does the job. We are going to reconstruct its transition function  $t$ .

**Claim 1:**  $t(0, a) = 1$ . Otherwise  $t(0, a) = 0$ , then we would not be able to distinguish inputs  $b$  and  $ab$ .

**Claim 2:**  $t(0, b) = 0$ . Otherwise  $t(0, b) = 1$ , then we would not be able to tell the input  $bb$  from  $ab$ .

**Claim 3:**  $t(1, a) = 1$  (otherwise we would not tell  $b$  from  $aab$ ).

**Claim 4:**  $t(1, b) = 0$  (otherwise we would not tell  $aa$  from  $ab$ ).

We still cannot distinguish  $bb$  from  $ab$ , a contradiction anyway.

**Problem 3.** List all cycles of length 3 in the symmetric group  $S(4)$ . Make sure there are no repetitions in your list.

Any cycle of length 3 in  $S(4)$  moves 3 elements and fixes the remaining one. Therefore there are 4 ways to choose three elements  $a, b, c$  moved by such a cycle. For any choice of these, there are two cycles of length 3 moving  $a, b, c$ , each written in three different ways:  $(a b c) = (b c a) = (c a b)$  and  $(a c b) = (b a c) = (c b a)$ .

The list:  $(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)$ .

**Problem 4.** Write the permutation  $\pi = (4\ 5\ 6)(3\ 4\ 5)(1\ 2\ 3)$  as a product of disjoint cycles.

Keeping in mind that the composition is evaluated from the right to the left, we find that  $\pi(1) = 2$ ,  $\pi(2) = 5$ ,  $\pi(5) = 3$ , and  $\pi(3) = 1$ . Further,  $\pi(4) = 6$  and  $\pi(6) = 4$ . Thus  $\pi = (1\ 2\ 5\ 3)(4\ 6)$ .

**Problem 5.** Find the order and the sign of the permutation  $\sigma = (1\ 2)(3\ 4\ 5\ 6)(1\ 2\ 3\ 4)(5\ 6)$ .

First we find the cycle decomposition of the given permutation:  $\sigma = (2\ 4)(3\ 5)$ . It follows that the order of  $\sigma$  is 2 and that  $\sigma$  is an even permutation. Therefore the sign of  $\sigma$  is  $+1$ .

**Problem 6.** What is the largest possible order of an element of the alternating group  $A(10)$ ?

The order of a permutation  $\pi$  is  $o(\pi) = \text{lcm}(l_1, l_2, \dots, l_k)$ , where  $l_1, \dots, l_k$  are lengths of cycles in the disjoint cycle decomposition of  $\pi$ .

The largest order for  $\pi \in A(10)$ , an even permutation of 10 elements, is 21. It is attained when  $\pi$  is the product of disjoint cycles of lengths 7 and 3, for example,  
 $\pi = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10)$ . One can check that in all other cases the order is at most 15.

*Remark.* The largest order for  $\pi \in S(10)$  is 30, but it is attained on odd permutations, e.g.,  
 $\pi = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8)(9\ 10)$ .

**Problem 7.** Consider the operation  $*$  defined on the set  $\mathbb{Z}$  of integers by  $a * b = a + b - 2$ . Does this operation provide the integers with a group structure?

We need to check 4 axioms.

**Closure:**  $a, b \in \mathbb{Z} \implies a * b = a + b - 2 \in \mathbb{Z}$ .

**Associativity:** for any  $a, b, c \in \mathbb{Z}$ , we have

$$(a * b) * c = (a + b - 2) * c = (a + b - 2) + c - 2 = a + b + c - 4,$$

$$a * (b * c) = a * (b + c - 2) = a + (b + c - 2) - 2 = a + b + c - 4,$$

hence  $(a * b) * c = a * (b * c)$ .

**Existence of identity:** equalities  $a * e = e * a = a$  are equivalent to  $e + a - 2 = a$ . They hold for  $e = 2$ .

**Existence of inverse:** equalities  $a * b = b * a = e$  are equivalent to  $b + a - 2 = e (= 2)$ . They hold for  $b = 4 - a$ .

Thus  $(\mathbb{Z}, *)$  is a group.

*Remark.* Consider a bijection  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(a) = a - 2$ .

Then  $f(a * b) = f(a) + f(b)$  for all  $a, b \in \mathbb{Z}$ .

**Problem 8.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

The set  $M$  is closed under matrix addition, taking the negative, and matrix multiplication as

$$\begin{aligned} \begin{pmatrix} n & k \\ 0 & n \end{pmatrix} + \begin{pmatrix} n' & k' \\ 0 & n' \end{pmatrix} &= \begin{pmatrix} n+n' & k+k' \\ 0 & n+n' \end{pmatrix}, \\ -\begin{pmatrix} n & k \\ 0 & n \end{pmatrix} &= \begin{pmatrix} -n & -k \\ 0 & -n \end{pmatrix}, \\ \begin{pmatrix} n & k \\ 0 & n \end{pmatrix} \begin{pmatrix} n' & k' \\ 0 & n' \end{pmatrix} &= \begin{pmatrix} nn' & nk' + kn' \\ 0 & nn' \end{pmatrix}. \end{aligned}$$

Also, the multiplication is commutative on  $M$ . The associativity and commutativity of the addition, the associativity of the multiplication, and the distributive law hold on  $M$  since they hold for all  $2 \times 2$  matrices. Thus  $M$  is a commutative ring.

**Problem 8.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} n & k \\ 0 & n \end{pmatrix}$ , where  $n$  and  $k$  are rational numbers. Under the operations of matrix addition and multiplication, does this set form a ring? Does  $M$  form a field?

The ring  $M$  is not a field since it has zero-divisors (and zero-divisors do not admit multiplicative inverses).

For example, the matrix  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M$  is a zero-divisor as

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

**Problem 9.** Let  $L$  be the set of the following  $2 \times 2$  matrices with entries from the field  $\mathbb{Z}_2$ :

$$A = \begin{pmatrix} [0] & [0] \\ [0] & [0] \end{pmatrix}, \quad B = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}, \quad C = \begin{pmatrix} [1] & [1] \\ [1] & [0] \end{pmatrix}, \quad D = \begin{pmatrix} [0] & [1] \\ [1] & [1] \end{pmatrix}.$$

Under the operations of matrix addition and multiplication, does this set form a ring? Does  $L$  form a field?

First we build the addition and multiplication tables for  $L$  (meanwhile checking that  $L$  is closed under both operations):

+		A	B	C	D
A		A	B	C	D
B		B	A	D	C
C		C	D	A	B
D		D	C	B	A

×		A	B	C	D
A		A	A	A	A
B		A	B	C	D
C		A	C	D	B
D		A	D	B	C

Analyzing these tables, we find that both operations are commutative on  $L$ ,  $A$  is the additive identity element, and  $B$  is the multiplicative identity element. Also,  $B^{-1} = B$ ,  $C^{-1} = D$ ,  $D^{-1} = C$ , and  $-X = X$  for all  $X \in L$ . The associativity of addition and multiplication as well as the distributive law hold on  $L$  since they hold for all  $2 \times 2$  matrices. Thus  $L$  is a field.



**Problem 10.** For any  $\lambda \in \mathbb{Q}$  and any  $v \in \mathbb{Z}$  let  $\lambda \odot v = \lambda v$  if  $\lambda v$  is an integer and  $\lambda \odot v = v$  otherwise. Does this “selective scaling” make the additive Abelian group  $\mathbb{Z}$  into a vector space over the field  $\mathbb{Q}$ ?

The group  $(\mathbb{Z}, +)$  with the scalar multiplication  $\odot$  is not a vector space over  $\mathbb{Q}$ . One reason is that the distributive law  $(\lambda + \mu) \odot v = \lambda \odot v + \mu \odot v$  does not hold.

A counterexample is  $\lambda = \mu = 1/2$  and  $v = 1$ . Then  $(\frac{1}{2} + \frac{1}{2}) \odot v = 1 \odot v = v = 1$  while  $\frac{1}{2} \odot v + \frac{1}{2} \odot v = v + v = 2$ .

*Remark.* The essential information about the scalar multiplication  $\odot$  used in the above counterexample is that  $1 \odot v = v$  and  $\frac{1}{2} \odot v$  is an integer. It follows that the additive group  $\mathbb{Z}$ , in principle, cannot be made into a vector space over  $\mathbb{Q}$ .