MATH 433

Applied Algebra

Lecture 22:
Review for Exam 2.

Topics for Exam 2

- 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, integral domains, zero-divisors
- Fields, characteristic of a field
- Vector spaces over a field
- Algebras over a field

Topics for Exam 2

- Order of an element in a group
- Subgroups, cyclic subgroups
- Cosets
- Lagrange's theorem
- Isomorphism of groups

- Binary codes, error detection and error correction
- Linear codes, generator matrix
- Coset leaders, coset decoding table
- Parity-check matrix, syndromes

What you are supposed to remember

- 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
- Definition of the symmetric group $S(n)$ and the alternating group $A(n)$

- Definition of a group
- Definition of a ring
- Definition of a field

What you are supposed to remember

- Definition of the order of a group element
- Definition of a subgroup
- How to check whether a subset of a group is a subgroup
- Definition of a cyclic subgroup
- Definition of a coset
- Lagrange's theorem

- Definition of a binary code and a codeword
- Definition of a linear code and a generator matrix
- How to determine the number of detected and corrected errors
- How to correct errors using the minimum distance approach

Sample problems

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

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

Problem 3. What is the largest possible order of an element of the alternating group $A(10)$?

Problem 4. 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?

Sample problems

Problem 5. Let M be the set of all 2×2 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?

Problem 6. Let L be the set of the following 2×2 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?

Sample problems

Problem 7. For any $\lambda \in \mathbb{Q}$ and any $v \in \mathbb{Z}$ let $\lambda \odot v = \lambda v$ if λv 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 8. Suppose H and K are subgroups of a group G. Is the union $H \cup K$ necessarily a subgroup of G? Is the intersection $H \cap K$ necessarily a subgroup of G?

Problem 9. Find all subgroups of the group $(G_{15}, \times)$.

Problem 10. Determine which of the following groups of order 6 are isomorphic and which are not: $\mathbb{Z}_6$, $\mathbb{Z}_3 \times \mathbb{Z}_2$, $S(3)$, and $D(3)$.

Sample problems

Problem 11. Let $f : \mathbf{B}^3 \to \mathbf{B}^7$ be the coding function that sends each three-character word *abc* in the alphabet $\mathbf{B} = \{0, 1\}$ to the codeword $abcabcy$, where y is the inverted parity bit of the word abc (i.e., $y = 0$ if abc contains an odd number of 1s and $y = 1$ otherwise). How many errors will this code detect? correct? Is this code linear?

Problem 12. Let $f : \mathbf{B}^3 \to \mathbf{B}^6$ be a coding function defined 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 that a message encoded by this function is received with errors as 101101 010101 011111. Correct errors and decode the received message.

Sample problems

Problem 13. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A			
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

Problem 1. 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 2. 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 σ is 2 and that σ is an even permutation. Therefore the sign of σ is $+1$.

Problem 3. What is the largest possible order of an element of the alternating group $A(10)$?

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

The largest order for $\pi \in A(10)$, an even permutation of 10 elements, is 21. It is attained when π 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 4. 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. The group $(\mathbb{Z}, *)$ is isomorphic to $(\mathbb{Z}, +)$ via the isomorphism $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = a - 2$. Indeed, $f(a * b) = f(a) + f(b)$ for all $a, b \in \mathbb{Z}$.

Problem 5. Let M be the set of all 2×2 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

$$\begin{pmatrix} n & k \\ 0 & n \end{pmatrix} + \begin{pmatrix} n' & k' \\ 0 & n' \end{pmatrix} = \begin{pmatrix} n+n' & k+k' \\ 0 & n+n' \end{pmatrix},$$

$$-\begin{pmatrix} n & k \\ 0 & n \end{pmatrix} = \begin{pmatrix} -n & -k \\ 0 & -n \end{pmatrix},$$

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

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 2×2 matrices. Thus M is a commutative ring.

Problem 5. Let M be the set of all 2×2 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 6. Let L be the set of the following 2×2 matrices with entries from the field $\mathbb{Z}_2$:

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

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 mutiplication 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

$\times$	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 2×2 matrices. Thus L is a field.

Problem 7. For any $\lambda \in \mathbb{Q}$ and any $v \in \mathbb{Z}$ let $\lambda \odot v = \lambda v$ if λv 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 axiom $\lambda \odot (\mu \odot v) = (\lambda\mu) \odot v$ does not hold.

A counterexample is $\lambda = 2$, $\mu = 1/2$, and $v = 1$. Then $\lambda \odot (\mu \odot v) = \lambda \odot v = 2$ while $(\lambda\mu) \odot v = 1 \odot v = 1$.

Problem 8. Suppose H and K are subgroups of a group G. Is the union $H \cup K$ necessarily a subgroup of G? Is the intersection $H \cap K$ necessarily a subgroup of G?

The union $H \cup K$ is a subgroup of G only if $H \subset K$ or $K \subset H$ (so that $H \cup K$ coincides with one of the subgroups H and K). Otherwise $H \cup K$ is not closed under the group operation.

The intersection $H \cap K$ of two subgroups is always a subgroup.

Problem 9. Find all subgroups of the group $(G_{15}, \times)$.

G_{15} is the multiplicative group of invertible congruence classes modulo 15. It has 8 elements:

$$[1], [2], [4], [7], [8], [11], [13], [14].$$

First we find the cyclic subgroups of G_{15}. These are $\{[1]\}$, $\{[1],[4]\}$, $\{[1],[11]\}$, $\{[1],[14]\}$, $\{[1],[2],[4],[8]\}$, and $\{[1],[4],[7],[13]\}$.

Any other subgroup is the union of several cyclic subgroups. By Lagrange's theorem, a subgroup of G_{15} can have the order 1, 2, 4, or 8. It follows that the only subgroup of G_{15} other than cyclic subgroups and G_{15} itself might be the union of three cyclic subgroups of order 2: $\{[1],[4],[11],[14]\}$. One can check that this is indeed a subgroup.

Problem 10. Determine which of the following groups of order 6 are isomorphic and which are not: $\mathbb{Z}_6$, $\mathbb{Z}_3 \times \mathbb{Z}_2$, $S(3)$, and $D(3)$.

$\mathbb{Z}_3 \times \mathbb{Z}_2$ is an additive group, where the addition is defined by $(g, h) + (g', h') = (g + g', h + h')$. It is easy to check that the element $([1]_3, [1]_2)$ has order 6. Therefore it generates the entire group so that $\mathbb{Z}_3 \times \mathbb{Z}_2$ is cyclic. Hence it is isomorphic to $\mathbb{Z}_6$.

$D(3)$ is a dihedral group, the group of symmetries of an equilateral triangle. Any symmetry permutes vertices of the triangle. Once we label the vertices as 1, 2, and 3, each symmetry from $D(3)$ is assigned a permutation from the symmetric group $S(3)$. This correspondence is actually an isomorphism.

Neither of the groups $\mathbb{Z}_6$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$ is isomorphic to $S(3)$ or $D(3)$ since the first two groups are commutative while the other two are not.

Problem 11. Let $f : \mathbf{B}^3 \to \mathbf{B}^7$ be the coding function that sends each three-character word *abc* in the alphabet $\mathbf{B} = \{0, 1\}$ to the codeword $abcabcy$, where y is the inverted parity bit of the word abc (i.e., $y = 0$ if abc contains an odd number of 1s and $y = 1$ otherwise). How many errors will this code detect? correct? Is this code linear?

First we list all 8 codewords for the given code:

$$0000001,\ \ 0010010,\ \ 0100100,\ \ 0110111,$$
$$1001000,\ \ 1011011,\ \ 1101101,\ \ 1111110.$$

Then we determine the minimum distance between distinct codewords. By inspection, it is 3. Therefore the code allows to detect 2 errors and to correct 1 error.

Since the zero word is not a codeword, it follows that the code is not linear.

Problem 12. Let $f : \mathbf{B}^3 \to \mathbf{B}^6$ be a coding function defined 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 that a message encoded by this function is received with errors as 101101 010101 011111. Correct errors and decode the received message.

The coding function is given by $f(w) = wG$, where G is the generator matrix and w is regarded as a row vector. The 8 codewords are linear combinations of rows of the generator matrix:

$$\begin{array}{cccc} 000000, & 001011, & 010110, & 011101, \\ 100101, & 101110, & 110011, & 111000. \end{array}$$

Every received word is corrected to the closest codeword. The corrected message is 100101 011101 011101. Since the code is systematic, decoding consists of truncating the codewords to 3 digits: 100 011 011.

Problem 13. Complete the following Cayley table of a group of order 9:

$*$	A	B	C	D	E	F	G	H	I
A	I								F
B		F						G	
C			H				E		
D				G		A			
E					E				
F				A		B			
G			E				A		
H		G						D	
I	F								C

First we observe that E is the identity element as $E^2 = E$. Next we observe that $A^2 = I$ and $A^3 = AI = F$ so that the order of A is greater than 3. Since the order of the group is 9, it follows from Lagrange's theorem that the group is cyclic and A is a generator. Further, $B = F^2 = A^6$, $C = I^2 = A^4$, $H = C^2 = A^8$, $D = H^2 = A^{16} = A^7$, $G = D^2 = A^{14} = A^5$. Also, $E = A^0$. Now that every element of the group is represented as a power of A, completing the table is a routine task. For example, $BC = A^6A^4 = A^{10} = A$.