

MATH 433
Applied Algebra

Lecture 37:
Review for Exam 3.

Topics for Exam 3

- Order of an element in a group
- Subgroups
- Cyclic groups
- Cosets
- Lagrange's Theorem
- Isomorphism of groups, classification of groups

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

- Division of polynomials
- Greatest common divisor of polynomials
- Factorisation of polynomials

Sample problems

Problem 1. Suppose $\pi, \sigma \in S(5)$ are permutations of order 3. What are possible values for the order of the permutation $\pi\sigma$.

Problem 2. 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 3. Prove that the group $(\mathbb{Q} \setminus \{0\}, \times)$ is not cyclic.

Sample problems

Problem 4. Suppose G is a group of order 125. Show that G contains an element of order 5.

Problem 5. The group (G_{15}, \times) has subgroups of what orders?

Problem 6. For any two of the following groups of order 6, determine whether they are isomorphic or not: \mathbb{Z}_6 , $\mathbb{Z}_3 \times \mathbb{Z}_2$, $S(3)$, and $D(3)$.

Sample problems

Problem 7. Let $f : \mathbf{B}^3 \rightarrow \mathbf{B}^7$ 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 1's and $y = 1$ otherwise). How many errors will this code detect? correct? Is this code linear?

Problem 8. Let $f : \mathbf{B}^3 \rightarrow \mathbf{B}^6$ be a linear 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 9. Find a greatest common divisor of polynomials $p(x) = x^4 - 2x^3 + 5x^2 - 4x + 4$ and $q(x) = 2x^3 - 3x^2 + 5x - 2$ over \mathbb{R} .

Problem 10. Factorise a polynomial $p(x) = x^3 - 3x^2 + 3x - 2$ into irreducible factors over the field \mathbb{Z}_7 .

Problem 1. Suppose $\pi, \sigma \in S(5)$ are permutations of order 3. What are possible values for the order of permutation $\pi\sigma$.

The order of a permutation equals the least common multiple of the cycle lengths in its cycle decomposition. Hence it equals 3 only if the cycles are of length 1 or 3 (at least one cycle of length 3 is required). For permutations $\pi, \sigma \in S(5)$, this implies that both are cycles of length 3.

Note that any cycle of length 3 is an even permutation. Hence π and σ belong to the alternating group $A(5)$. Then $\pi\sigma \in A(5)$ as well. Possible orders of elements of $A(5)$ are: 1 (for the identity map), 2 (for a product of two disjoint transpositions), 3 (for a cycle of length 3), and 5 (for a cycle of length 5).

Consider the following cycles of length 3 in $A(5)$: $\pi = (1\ 2\ 3)$, $\sigma_1 = (1\ 4\ 5)$, $\sigma_2 = (1\ 2\ 4)$, $\sigma_3 = (1\ 2\ 3)$, and $\sigma_4 = (1\ 3\ 2)$. We have $\pi\sigma_1 = (1\ 4\ 5\ 2\ 3)$, $\pi\sigma_2 = (1\ 3)(2\ 4)$, $\pi\sigma_3 = (1\ 3\ 2)$, and $\pi\sigma_4 = \text{id}$. Thus the order of $\pi\sigma$ can be 1, 2, 3 or 5.

Problem 2. 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. Indeed, if neither of the subgroups contains the other, we can find an element $h \in H \setminus K$ and an element $k \in K \setminus H$. Let $g = hk$. Then $g \notin H$ as otherwise $k = h^{-1}g \in H$, a contradiction. Similarly, $g \notin K$ as otherwise $h = gk^{-1} \in K$, another contradiction. Thus $h, k \in H \cup K$ while $hk \notin H \cup K$.

The intersection $H \cap K$ of two subgroups is always a subgroup (see lecture notes and the textbook).

Problem 3. Prove that the group $(\mathbb{Q} \setminus \{0\}, \times)$ is not cyclic.

Take any non-zero rational number r . It can be represented as a reduced fraction: $r = \frac{m}{n}$, where m and n are non-zero integers and $\gcd(m, n) = 1$.

The cyclic group $\langle r \rangle$ consists of fractions $\frac{m}{n}, \frac{m^2}{n^2}, \frac{m^3}{n^3}, \dots$, fractions $\frac{n}{m}, \frac{n^2}{m^2}, \frac{n^3}{m^3}, \dots$, and 1. Note that all fractions are reduced.

The numbers m and n can have only finitely many prime divisors. Since there are infinitely many prime numbers, we can find a prime number p that divides neither m nor n . It is easy to see that $p \notin \langle r \rangle$. Thus $\langle r \rangle \neq \mathbb{Q} \setminus \{0\}$.

Problem 4. Suppose G is a group of order 125. Show that G contains an element of order 5.

It follows from Lagrange's Theorem that the order of any element of the group G divides 125. Hence the only orders we can expect are 1, 5, 25, and 125.

Let g be any element of G different from the identity element. Then the order of g is 5, 25 or 125.

If $o(g) = 5$ then we are done.

If $o(g) = 25$ then the element g^5 has order 5.

If $o(g) = 125$ then the element g^{25} has order 5.

Remarks. • In general, if the order of g is n , then the order of g^k is $\frac{n}{\gcd(k, n)}$.

• A theorem of Cauchy states that if the order of a finite group is divisible by a prime number p then the group contains an element of order p .

Problem 5. The group (G_{15}, \times) has subgroups of what orders?

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

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

By Lagrange's Theorem, a subgroup of G_{15} can be of order 1, 2, 4 or 8. First we find the cyclic subgroups of G_{15} . These are $\{[1]\}$, $\{[1], [4]\}$, $\{[1], [11]\} = \{[1], [-4]\}$, $\{[1], [14]\} = \{[1], [-1]\}$, $\{[1], [2], [4], [8]\}$, and $\{[1], [4], [7], [13]\} = \{[1], [-2], [4], [-8]\}$.

Hence we have cyclic subgroups of orders 1, 2 and 4. Also, the entire group G_{15} is a subgroup of order 8.

Remarks. • The only other subgroup of G_{15} is a non-cyclic group $\{[1], [4], [11], [14]\} = \{[1], [4], [-4], [-1]\}$.

- One can show that $G_{15} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Problem 6. For any two of the following groups of order 6, determine whether they are isomorphic or 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 as another cyclic group of order 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 6. For any two of the following groups of order 6, determine whether they are isomorphic or not: \mathbb{Z}_6 , $\mathbb{Z}_3 \times \mathbb{Z}_2$, $S(3)$, and $D(3)$.

Alternative solution: Let us use the classification of groups of small size. According to the classification, any group of order 6 is isomorphic either to \mathbb{Z}_6 or to $S(3)$. Notice that the group \mathbb{Z}_6 is Abelian while the group $S(3)$ is non-Abelian.

Since no Abelian group can be isomorphic to a non-Abelian one, it follows that every Abelian group of order 6 is isomorphic to \mathbb{Z}_6 while every non-Abelian group of order 6 is isomorphic to $S(3)$.

In particular, $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ and $D(3) \cong S(3)$.

Besides, neither of the Abelian groups \mathbb{Z}_6 and $\mathbb{Z}_3 \times \mathbb{Z}_2$ is isomorphic to non-Abelian groups $S(3)$ or $D(3)$.

Problem 7. Let $f : \mathbf{B}^3 \rightarrow \mathbf{B}^7$ 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 1's 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.

For any linear code, the set of codewords is a subspace of some \mathbf{B}^n . As a consequence, it contains the zero word. Since the zero word is not a codeword for the function f , this code cannot possibly be linear.

Problem 8. Let $f : \mathbf{B}^3 \rightarrow \mathbf{B}^6$ be a linear 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:

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

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 9. Find a greatest common divisor of polynomials

$$p(x) = x^4 - 2x^3 + 5x^2 - 4x + 4 \quad \text{and}$$

$$q(x) = 2x^3 - 3x^2 + 5x - 2 \quad \text{over } \mathbb{R}.$$

$\gcd(p, q)$ can be found using the Euclidean algorithm. First

$$\begin{aligned} \text{we divide } p \text{ by } q: \quad & x^4 - 2x^3 + 5x^2 - 4x + 4 = \\ & = (2x^3 - 3x^2 + 5x - 2)\left(\frac{1}{2}x - \frac{1}{4}\right) + \frac{7}{4}x^2 - \frac{7}{4}x + \frac{7}{2}. \end{aligned}$$

Hence $\gcd(p, q) = \gcd(q, r)$, where $r(x) = \frac{7}{4}x^2 - \frac{7}{4}x + \frac{7}{2}$ is the remainder of p by q . It is convenient to replace the polynomial r by its scalar multiple $\tilde{r}(x) = \frac{4}{7}r(x) = x^2 - x + 2$.

Clearly, $\gcd(q, r) = \gcd(q, \tilde{r})$.

Next we divide q by \tilde{r} :

$$2x^3 - 3x^2 + 5x - 2 = (x^2 - x + 2)(2x - 1).$$

Since \tilde{r} divides q , it follows that $\gcd(q, \tilde{r}) = \tilde{r}$.

Finally, $\gcd(p, q) = x^2 - x + 2$.

Problem 10. Factorise a polynomial $p(x) = x^3 - 3x^2 + 3x - 2$ into irreducible factors over the field \mathbb{Z}_7 .

A quadratic or cubic polynomial is irreducible if and only if it has no roots. Indeed, if such a polynomial splits into a product of two non-constant polynomials, then at least one of the factors is linear. This implies that the original polynomial has a root.

Let us look for the roots of $p(x)$: $p(0) = -2$, $p(1) = -1$, $p(2) = 0$. Hence $p(x)$ is divisible by $x - 2$ (over any field):

$$x^3 - 3x^2 + 3x - 2 = (x - 2)(x^2 - x + 1).$$

Now we look for roots of the polynomial $q(x) = x^2 - x + 1$. Note that values 0 and 1 can be skipped this time. We obtain $q(2) = 3$, $q(3) = 7 \equiv 0 \pmod{7}$. Hence $q(x)$ is divisible by $x - 3$ over \mathbb{Z}_7 : $x^2 - x + 1 = (x - 3)(x + 2)$.

Thus $x^3 - 3x^2 + 3x - 2 = (x - 2)(x - 3)(x + 2)$ over the field \mathbb{Z}_7 .