Exam 3, Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Thursday, April 8, 2021, 09:00 - 12:00

At the end of the exam:

1. Carefully check that your name and S-number is on the top of each page.
2. Put your student ID-card on the first page
3. Scan your work with your smartphone
4. Hand in your paper
5. Convert your scan into a SINGLE pdf file
6. Upload the pdf on the Module site of Canvas in the Assignment field Algebra Exam.

$(a)(bcd)$

$(ab)(cd)$

$(abcd)$

~~6~~, ~~12~~

$|R_{60}| = 6$

All answers need to be motivated. You can also consult a two-page handwritten summary. There are **four** exercises. This third exam of Module 7 consists of the **Algebra part** only, and is a **3h exam**. The total is 90 points. The grade, when you have P points, equals

$$1 + \frac{9P}{90}.$$

---

1. Consider the group A_4, the group of even permutations of four symbols.
   (a) (5p) How many elements does A_4 have?
   (b) (5p) What are the possible orders of the permutations in A_4?
   (c) (8p) Determine for each possible divisor of $|A_4|$, an $\alpha \in A_4$ with precisely that order or prove that such an α does not exist.
   (d) (4p) Is A_4 isomorphic to D_6, the symmetry group of a regular hexagon?

(a) $|A_4| = |S_4|/2 = \frac{4!}{2} = 12 \Leftarrow$

(b) 1, 2, 3, 4, 6, 12

(c) $|\varepsilon| = 1 \quad |(12)(34)| = 2$

$(12)(12) = (1$

$|(1)(234)| = 3 \quad (234) = (24)(23)$

$(1234) = (14)(13)(12) \rightarrow$ not in A_4

PTO

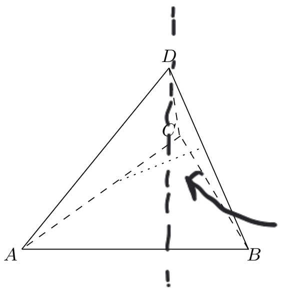

Figure 1: Tetrahedron

2. Consider the regular Tetrahedron in Figure 1 and let G be the group of rotations that transform the Tetrahedron into itself. Face 1: ABC (the base face or ground face), Face 2: BCD (the right side face), Face 3: ACD (the left side face), Face 4: ABD (the front face).

   (a) (3p) Describe the rotations that leave Face 1 invariant, and determine $|\text{Stab}_G(1)|$.

   (b) (4p) Describe the rotations that rotate Face 1 to each of the other faces, and determine $|\text{Orb}_G(1)|$.

   (c) (3p) Show that G contains 12 elements, that is $|G| = 12$.

   (d) (4p) For each vertex there are two rotations about the axis that connects that vertex and the center of the opposite face. What is the order of these rotations?

   (e) (4p) The 8 rotations described in Item 2d permute the faces. Write these 8 permutations in disjoint cycle form. Show that these are even permutations.

   (f) (4p) For each pair of opposite edges, (in Figure 1 one such axis is depicted: the dotted line that connects the centers of AC and BD), there is a rotation about the axis that connects the centers of the opposite edges. What is the order of these rotations? Write these 3 rotations in disjoint cycle form. Prove that these rotations are even.

   (g) (3p) Count the number of rotations, add the identity and conclude that $G = A_4$.

   (h) (5p) We want to paint the faces of the Tetrahedron using red and blue. Each $\phi \in G$ induces a permutation of the set of color schemes. Use Burnside's Theorem to determine number of different orbits, that is, the number of different color schemes.

(a) $R_0, R_{120}, R_{240} \Rightarrow |\text{Stab}_G(1)| = 3$

(b) $|\text{Orb}_G(1)| = 4$

(c) $|G| = |\text{Orb}_G(1)| \cdot |\text{Stab}_G(1)| = 4 \cdot 3 = 12$

(d) $|R_{120}| = |R_{240}| = 3$

~~(1~~)(2 3 4) = (1)(24)(23)
(1)(2 4 3)
(2)(1 3 4)
(2)(1 4 3)
(3)(1 2 4)
(3)(1 4 2)
(4)(1 2 3)
(4)(1 3 2)

8

(f) 180° ⇒ order is 2

$$\left.\begin{matrix}(12)(34)\\(13)(24)\\(14)(23)\end{matrix}\right\} \Rightarrow \text{even}$$

(g) G contains 12 even perm. on 4 symbols
⇒ $G = A_4$

$|\text{fix}(\varepsilon)| = 2^4 = 16$

$|\text{fix}((1)(234))| = 2^2 \cdot 8$

$|\text{fix}((12)(34))| = 2^2 \cdot 3$

$$\frac{1}{12}\sum_{\varphi\in G}|\text{fix}(\varphi)| = \frac{60}{12}$$

$= 5$

PTO

$(d)\ |\mathbb{F}\setminus\{0\}|$

$= 27 - 1 = \underline{26}$

$1, 2, 13, 26$

$|\alpha| = 26$

3. Let $p(x) \in \mathbb{Z}_3[x]$ be given by

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

(a) (4p) Show that $p(x)$ is irreducible.

(b) (4p) Define the field $\mathbb{F}$ as:

$$\mathbb{F} = \mathbb{Z}_3[x]/ < x^3 + 2x + 1 > .$$

Argue that

$$\mathbb{F} = \mathbb{Z}_3[x]/ < x^3 + 2x + 1 >= \{ax^2 + bx + c+ < x^3 + 2x + 1 > | \, a, b, c \in \mathbb{Z}_3\}.$$

(c) (4p) How many elements does $\mathbb{F}$ have?

(d) (3p) What are the possible orders of elements in the multiplicative group $\mathbb{F}\backslash\{0\}$?

(e) (5p) Determine the multiplicative order of $x+ < x^3 + 2x + 1 >$.

(a) $\deg p(x) = 3 \leftarrow$

$p(0) = 1 \quad p(1) = 1 \quad p(2) = 1$

$\Rightarrow p(x)$ irreducible

(b) $\mathbb{F} = \mathbb{Z}_3[x]/\langle p(x)\rangle$

$= \{ ax^2 + bx + c + \langle p(x)\rangle \mid a, b, c \in \mathbb{Z}_3 \}.$

$\rightarrow x^3 + \langle p(x)\rangle = \underline{x + 2} + \langle p(x)\rangle \leftarrow$

(c) $|\mathbb{F}| = 27. \leftarrow \leftarrow$

$\underline{ax^2 + bx + c} + \langle p(x)\rangle = \underline{ex^2 + fx + g} + \langle p(x)\rangle$

$\rightarrow (a-e)x^2 + (b-f)x + (c-g) + \langle p(x)\rangle \leftarrow$

$\underline{a = e} \quad \underline{b = f} \quad \underline{c = g}.$

$(2, 1, 1) \leftarrow$

$(1, 2, 0) \leftarrow$

$2x^2 + x + 1 + \langle p(x)\rangle$?

$\neq x^2 + 2x + \langle p(x)\rangle$

(e) $|\overbrace{x + \langle p(x)\rangle}^{\alpha}|$

$(x + p(x))^2 = x^2 + \langle p(x)\rangle$

$\rightarrow |\alpha| \neq 2$

$\alpha^{13} = \alpha \cdot \alpha^{12} = \alpha \cdot (\alpha^3)^4$

$= (x + \langle p(x)\rangle)(x + 2 + \langle p(x)\rangle)^4$

$= 2 + \langle p(x)\rangle \quad |\alpha| \neq 13$

$ax^3 + bx^2 + cx + d$

$+ \langle p(x)\rangle$

$x^3 + \langle p(x)\rangle$

$= x + 2 + \langle p(x)\rangle$

2x

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

PTO

$n = p \cdot q$ ←

$\gcd(M, n) > 1$

$- p$ ←

$- q$

4. (a) (10 points) Assume that Alice has published modulus $n = 91$, and exponent $e = 11$. Bob sends ciphertext $C = 3$ to Alice. You are eavesdropper Eve and you are interested in Bob's secret message M. Compute Bob's secret message M from ciphertext C. In doing that, write down all of the computational steps that you need to perform in order to obtain Bob's secret message M. List which of the steps can generally be done efficiently (in polynomial computation time), and which not.

   (b) (8 points) For each of the following two claims, decide if true or false. A correct answer counts **four points**, an incorrect answer counts **minus three points** (minimum for 4b is 0 points). **Instead of guessing, it may be better not giving an answer.**

   i. Consider the RSA method for public modulus $n = p \cdot q$ with primes p, q, and public exponent e relatively prime with $\phi(n)$, secret message $M \in \mathbb{Z}_n$, and cyphertext $C = M^e \pmod{n}$. **Claim:** If $\gcd(M, n) > 1$, then the cryptosystem can be broken in polynomial computation time by only using the publicly available information C, n, e.

   True .... ☒
   False.................................... □
   I prefer not to give an answer .... □

   ii. Consider the RSA method. **Claim:** If there is an efficient (polynomial computation time) algorithm to tell whether an arbitrary given number $n \in \mathbb{Z}$ is a prime or not, then the RSA cryptosystem can be broken in polynomial computation time by only using the publicly available information C, n, e.

   True .... □
   False.................................... ☒
   I prefer not to give an answer .... □

Space for answer 4a:

(a) $C = 3 \quad n = 91 = \underline{7 \cdot 13}$ ←

$m = 6 . 12 = 72$ ←

$e = 11 \qquad 11 . d \equiv 1 \mod 72$

$\Rightarrow \quad d = 59$

$M = C^d \mod 91 = 3^{59} \mod 91$

$3^{(2^5)} \cdot 3^{(3^3)}$

$59 = 32 + 27$

$= 2^5 + 3^3$

$3^{59} = 3^{2^5} \cdot (3^3)^3$

$\mod 91$

$= \underline{61}$

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....