Exam 3: Algebra. Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Friday, 22 April 2022, 08:45-11:45

At the end of the exam:

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

All answers need to be motivated. You can also consult a two-page handwritten summary. There are **five** 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_9, the group of even permutations of nine symbols.

   (a) (2p) How many elements does A_9 have?

   (b) (3p) Let α be given by

   $$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 4 & 6 & 9 & 1 & 8 & 2 \end{bmatrix}$$

   Investigate whether $\alpha \in A_9$.
   What is the order, $|\alpha|$, of α?

   (c) (2p) If, for example, we want to write a non-identity permutation of 4 elements as a product of disjoint cycles (without 1-cycles), the possibilities are: a 4-cycle, a 3-cycle, a 2-cycle, or a product of two 2-cycles. What are the possibilities for non-identity permutations in A_9?

   (d) (2p) Does there exist $\alpha \in A_9$ such that $|\alpha| = 10$?

   (e) (3p) List all orders that occur in A_9?

   (f) (4p) Determine for each of the orders that occurs in A_9, a permutation $\alpha \in A_9$ of precisely that order.

2. Let the ring R be given by

   $$R = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}_3\}.$$

   Here, i is the imaginary unit, that is $\mathrm{i}^2 = 2$.

PTO

(a) (4p) Show that R is an integral domain.

(b) (4p) Show that every nonzero element in R has a multiplicative inverse.

(c) (3p) Find the multiplicative inverse of $1 + \mathrm{i}$.

(d) (4p) Show that the multiplicative group of nonzero elements is isomorphic to $\mathbb{Z}_8$.

3. Consider the cube in Figure 1 and let G be the group of rotations that transform the cube into itself. We want to paint the vertices of the cube using red, yellow and blue and at most two colours have to be used. The goal of this exercise is to find out how many different configurations there are when we take the rotational symmetries into account.

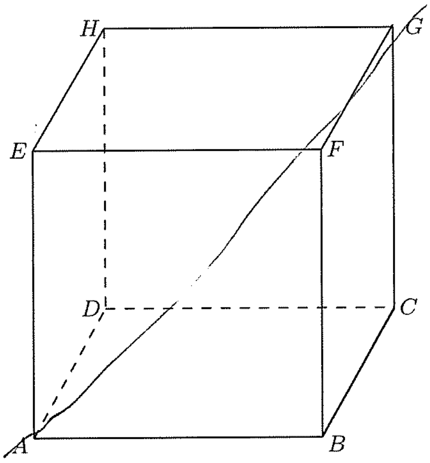

Figure 1: Cube

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

(b) (3p) Describe the rotations that rotate Vertex A to each of the other vertices, and determine $|\text{Orb}_G(A)|$.

(c) (3p) Show that G contains 24 elements, that is $|G| = 24$.

(d) (3p) G acts on the set S of different colour configurations for the cube in the position as depicted (so without taking into account the symmetries). Describe the set S. How many elements does S have?

(e) (2p) For each pair of opposite faces there are three rotations in G, disregarding the identity. Determine for each of these rotations ϕ, $|\text{fix}(\phi)|$. Hint: the rotations permute the vertices. Write the corresponding permutation in disjoint cycle form. For instance a rotation of 90 degrees has order 4, and leaves no vertices invariant. Therefore the corresponding permutation is of the form $(abcd(efgh)$. Notice that all vertices in each cycle should have the same colour.

(f) (2p) For each pair of opposite edges there is one rotation ϕ in G, disregarding the identity. Determine $|\text{fix}(\phi)|$. Hint: modify the hint in the previous item.

(g) (2p) For each pair of opposite vertices there are two rotations in G, disregarding the identity. Determine for each of these rotations ϕ, $|\text{fix}(\phi)|$. Hint: modify the hint in the previous item.

(h) (3p) Use Burnside's Theorem to determine the number of different orbits, that is, the number of different colour schemes.

(i) (2p) Characterise six colour schemes of which any two are in different orbits.

4. (a) (4p) Show that $x^2 + x + 1 \in \mathbb{Z}_2[x]$ is the only irreducible polynomial of degree two.

   (b) (3p) Let $p(x) = x^4 + x + 1$. Prove that

$$\mathbb{F} = \mathbb{Z}_2[x]/ < p(x) >$$

   is a field.

   (c) (3p) Describe the elements of $\mathbb{F}$. How many elements does $\mathbb{F}$ have?

   (d) (4p) Determine the multiplicative order of $x^2 + x + < p(x) >$ in $\mathbb{F}\backslash\{0\}$.

   (e) (4p) Determine $(x + < p(x) >)^{-1}$.

5. (a) i. (10p) Alice and Bob are using RSA to exchange messages. Assume that Alice has published modulus $n = 209$, and exponent $e = 31$. Bob sends ciphertext $C = 5$ 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, please write down all of the computational steps that you need to perform in order to obtain Bob's secret message M.

   ii. (8p) 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 5(a)ii is 0 points). **Instead of guessing, it may be better not giving an answer.**

   A. Alice and Bob are using RSA to exchange messages. Assume that Alice has published modulus n and exponent e. Eve is interested in Bob's secret message M to Alice and has intercepted cyphertext $C = M^e$. To this end Eve asks Alice if she would be kind enough to use her private key d to decrypt a different cyphertext $C \cdot X^e \pmod{n}$ for some X that she has chosen arbitrarily. **Claim:** Alice can safely decrypt $C \cdot X^e \pmod{n}$ for Eve.

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

   B. Computing $C^d \pmod{n}$ can be done with $O(\log_2 d)$ many multiplications.

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