Exam 3, Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Thursday, July 16th, 2020, 08:45 - 11:45

All answers need to be motivated. Simple calculators are allowed. You are also allowed to use the book. 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 50 points. The grade, when you have P points, equals

$$1 + \frac{9P}{50}.$$

Please read carefully: By testing you remotely in this fashion, we express our trust that you will adhere to the ethical standard of behaviour expected of you. This means that we trust you to answer the questions and perform the assignments in this test to the best of your own ability, without seeking or accepting the help of any source that is not explicitly allowed by the conditions of this test. In case of doubt, it might be that we have to decide not to count the test result, which could include invalidating the test results of all other students, too. Therefore, our appeal is to your own responsibility:

You maximise your own, and all your fellow students' chance to have this test result remain valid, by adhering to the rules as stated below.

In order for the test to be graded, the following text must be copied on the first page of your solutions:

> **"I have made this test to the best of my own ability, without seeking or accepting the help of any source not explicitly allowed by the conditions of the test" [Name, Student no., Location, Date, Signature].**

Algebra

1. Consider the group $U(20)$.

   (a) (3 p) List the elements of $U(20)$ and determine for each element its order.

   (b) (2 p) Provide an isomorphism

   $$\phi : U(20) \to U(4) \oplus U(5)$$

   (c) (3 p) Provide isomorphisms

   $$\psi_1 : U(4) \to \mathbb{Z}_2 \quad \psi_2 : U(5) \to \mathbb{Z}_4$$

   (d) (3 p) Provide an isomorphism

   $$\rho : U(20) \to \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

2. A fan, attached to the ceiling, has three wings that can be rotated about their axes. We want to paint each wing on both sides using two colors.

   The fan is schematically depicted in Figure 1. It consist of a solid black disk to which three identical flaps are attached through spokes about which the flaps can rotate independently. In the neutral position the upsides of the flaps are numbered 1-3, while the downsides are numbered 4-6. We want to paint both sides of each flap using two colors: red and blue. The goal of this exercise is to find out in how may different ways this can be done taking into account the symmetries present in the fan. The symmetries are determined by the symmetry group G consisting of rotations of the fan and flipping the flaps. Take, e.g., a rotation about the center of 120 degrees counterclockwise followed by flipping the flap $1/4$.

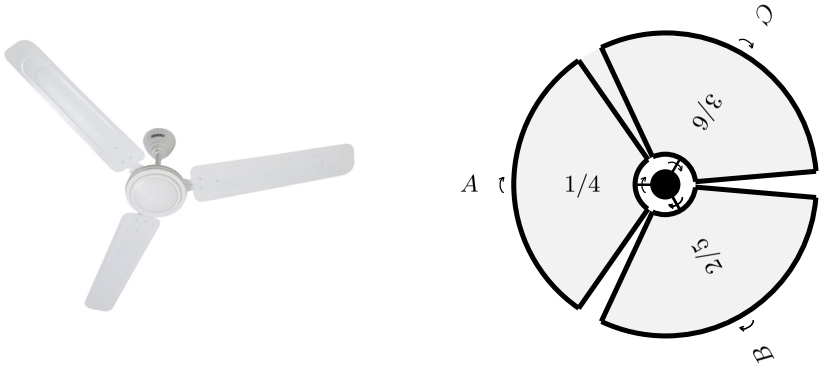

Figure 1: Fan with rotating wings

   (a) Let us first determine the order of the symmetry group G:
      i. (2 p) Determine $\mathrm{Stab}_G(1)$.
      ii. (2 p) Determine $\mathrm{Orb}_G(1)$.
      iii. (1 p) Determine $|G|$.

   (b) (3 p) Let us denote the elements of G as (R, i, j, k) with the intepretation that $R \in \{0, 120, 240\}$ denotes the rotation of the fan about the centre, $i, j, k \in \{0, 1\}$, $i = 0$ means that the flap in position A is not flipped, $i = 1$ means that the flap in position A is flipped. Likewise for j and k with respect to positions B and C respectively. We adopt the following convention about the order in which the rotations and flips are performed. For a specific element, e.g., $(120, 0, 1, 1)$, the flap in position C is flipped, followed by a flip of the flap in position B, the flap in position A is not flipped and finally the resulting fan is rotated about 120 degrees counterclockwise.

   The group element $(120, 0, 1, 1)$ corresponds to a permutation σ of $(1, 2, 3, 4, 5, 6)$. Write σ in disjoint cycle form.

   (c) (1 p) In the previous item we wrote the elements of G as (R, i, j, k), so

$$G = \{(R, i, j, k) \mid R \in \{0, 120, 240\}, i, j, k \in \{0, 1\}\}$$

   How many elements does G have according to this representation of G. Compare your answer with your answer in 2a.

   (d) (4 p) Determine for each $\phi \in G$ $|\mathrm{fix}(\phi)|$. A systematic way to do this is to consider the cases with no flip, one flip, two flips, and three flips separately and write for each of these the corresponding permutation in disjoint cycle form.

(e) (2 p) Which theorem can you now use to determine the number of different colourings? Do it.

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

$$p(x) = x^4 + x + 2.$$

(a) (1 p) (2 p) What do we need to check if we want to find out whether or not $p(x)$ is irreducible.

(b) (2 p) Assume that $p(x)$ can be written as the product of two polynomials of degree 2:

$$p(x) = a(x)b(x).$$

Show that if such a factorisation exists, then there also exists such a factorisation with both $a(x)$ and $b(x)$ monic, that is, the quadratic term has coefficient equal to one.

(c) (3 p) Assume that

$$p(x) = (x^2 + a_1x + a_0)(x^2 + b_1x + b_0). \quad (1)$$

Show, by systematic investigation, that there do not exist $a_i, b_i \in \mathbb{Z}_3$ such that (1) is satisfied. Hint: as a first step, argue that $a_0b_0 = 2$ and therefore either $a_0 = 1$ and $b_0 = 2$ or $a_0 = 2$ and $b_0 = 1$ and proceed with one of these possibilities.

(d) (3 p) Show that $\mathbb{F} = \mathbb{Z}_3[x]/ < p(x) >$ is a field.

(e) (2 p) How many elements does $\mathbb{F}$ have?

(f) (2 p) Show that $(x^3 + 1 + < p(x) >)^{-1} = x + < p(x) >$.

4. (a) (5 p) Let us assume that Alice has published modulus $n = 65$, and exponent $e = 11$. Bob sends ciphertext $C = 2$ to Alice. You are eavesdropper Eve and you are interested in Bob's secret messag e M. Compute Bob's secret message M from ciphertext C. In doing that, please write down all of the computational s teps that you need to perform in order to obtain Bob's secret message M.

(b) (5 p) Consider the RSA method for public modulus $n = p \cdot q$ with primes p, q, and public exponent e. In the tutorial exercises we have seen that, when d is the secret decryption key, $M^{ed} = M \pmod{n}$ for *all* $M \in \mathbb{Z}_n$. Hence the decryption delivers the correct answer, for any $M \in \mathbb{Z}_n$, by computing $C^d = (M^e)^d$. However, assuming that $M \notin U_n$, in other words, $\gcd(M, n) > 1$, the cryptosystem is no longer safe. Explain why. Describe how the system can now be broken, only using computationally efficient steps, and only using the publicly available information C, n, e.