Exam 3, Module 7, Codes 201400483 & 201800141

Discrete Structures & Efficient Algorithms

Thursday, April 9, 2020, 13:45 - 16:45

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. Let $\mathbb{F}$ be a finite field and $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ be its multiplicative group. The goal of this exercise is to prove, for a specific case, that the $\mathbb{F}^*$ is cyclic without involking Theorem 22.2. So you cannot refer to Theorem 22.2 for any of the items below.

   (a) (1 p) Assume that $\mathbb{F}^*$ has more than k elements. Let $f(x) \in \mathbb{F}[x]$ a polynomial with coefficients in $\mathbb{F}$ of degree k, $\deg f(x) = k$. At most how many different roots can $f(x)$ have in $\mathbb{F}^*$?

   (b) (2 p) Assume that $\mathbb{F}^*$ has more than three elements. At most how many elements $a \in \mathbb{F}$ of (multiplicative) order three can there exist in $\mathbb{F}^*$? Hint: an element of order three is a root of $x^3 - 1$.

   (c) (1 p) Consider from here on $\mathbb{F} = \mathbb{Z}_{23}$. Argue that $\mathbb{F}$ is a field.

   (d) (2 p) Let $a \in \mathbb{Z}_{23}^*$, what are the possibilities for the (multiplicative) order of a, that is, $|a|$?

   (e) (1 p) What is the maximum number of elements of (multiplicative) order two in $\mathbb{Z}_{23}^*$?

   (f) (3 p) What is the maximum number of elements $a \in \mathbb{Z}_{23}^*$ with $|a| < 22$?

PTO

(g) (3 p) Argue that there exist at least eight elements in $\mathbb{Z}_{23}^*$ of order 22 and conclude that $\mathbb{Z}_{23}^*$ is cyclic.

(h) (2 p) Find $a \in \mathbb{Z}_{23}^*$ such that $\mathbb{Z}_{23}^*$ is generated by a.

2. An octahedron is a regular solid consisting of 8 equilateral triangles, see Figure 1. We want to paint the faces of the octahedron using red and blue paint.

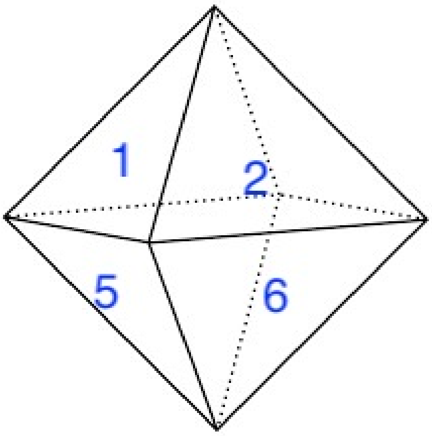

Figure 1: Octahedron with the visible faces numbered.

(a) (2 p) How many pairs of opposite edges are there?

(b) (2 p) How many pairs of opposite vertices are there?

(c) (2 p) Let G be the group of rotations about the symmetry axes of the octahedron. Which theorem can you use to determine the number of elements in G? Determine $|G|$.

(d) (2 p) Classify the rotations in three categories according to the type of symmetry axes, and verify that you have found all rotations by referring to 2c.

(e) (3 p) This item can be solved using your geometric 3D imagination or, alternatively, using an algebraic approach that does not involve how exactly the faces are mapped onto each other under the action of G.

Choose your favorite method.

Geometric approach

Determine for each $\phi \in G$ how the faces are mapped onto each other.

Hint. Label the faces as suggested in Figure 1: the faces in top half are labeled 1, 2, 3, 4, and the faces in the bottom half are labeled 5, 6, 7, 8 so that faces 1 and 5 are adjacent to each other. For instance, the rotation of 120 degrees counter clockwise about the axis that connect the centers of Face 1 and Face 7 leaves the Faces 1 and 7 invariant, Face 2 goes to Face 4, Face 3 goes to Face 8, Face 4 goes to Face 5, Face 5 goes to Face 2, Face 6 goes to Face 3 and Face 8 goes to Face 6. In disjoint cycle notation: (1)(245)(386)(7). It may be helpful to also label the vertices to keep track of what goes where.

Algebraic approach

Determine $|\phi|$, the order of ϕ, for all $\phi \in G$ and describe how each rotation $\phi \in G$ corresponds to a permutation of the faces written in disjoint cycle form.

Hint. For instance a rotation of 120 degrees about an axis that connects the centers of two opposite face has order three and the corresponding permutation of the faces is the product of disjoint cycles of length 1 or 3. Length 1 corresponds to a face that is left invariant and length 3 corresponds to three faces that are permuted cyclically. What the actual permutation is, is immaterial, it is the decomposition in disjoint cycles that matters.

(f) (2 p) For each $\phi \in G$ determine $|\mathrm{fix}(\phi)|$, do not forget the identity.

(g) (2 p) How many orbits are there? So, how many different color schemes are there?

3. (a) (1 p) Find all irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 2.

(b) (1 p) Find all irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 3.

(c) (1 p) Classify all possible factorisations of a polynomial $f(x) \in \mathbb{Z}_2[x]$ of degree 5 in terms of the degrees of the factors.

(d) (2 p) List all *reducible* polynomials in $\mathbb{Z}_2[x]$ of degree 5 that have no roots.

(e) (2 p) Argue that $p(x) = x^5 + x^3 + 1$ is irreducible in $\mathbb{Z}_2[x]$.

(f) (1 p) How many elements does the field $\mathbb{F}$ defined by

$$\mathbb{F} = \mathbb{Z}_2[x]/ < x^5 + x^3 + 1 >,$$

have?

(g) (2 p) Prove that $(x+ < x^5 + x^3 + 1 >)^{-1} = x^4 + x^2 + < x^5 + x^3 + 1 >$.

4. (a) (5 p) Let us assume that Alice has published modulus $n = 119$, and exponent $e = 35$. 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.

(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, $M^{ed} = M$ (mod 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.