# Exam for Algebra 1 at Aalborg University
## For 3. semester Mat
## Thursday, January 10th 2013, 8:30–12:30.

You are allowed to use books and your notes. However calculators, computers, pdas, tablets, ebooks or phones are not allowed.
A reasoned explanation should follow the solution of the exercises. Moreover, the intermediate steps leading to the solution should also be written down. You can write the exam in Danish or English.
The percentage following each exercise number stands for the exercise's value in the final mark. There are 5 exercises.

**Exercise 1** *(15%)* Let $G = (\mathbb{Z}/11\mathbb{Z})^*$. We consider an example of ElGamal cryptosystem using $G$:

1. Show that $g = 2$ generates $G$.
2. Let $a = 4$ be the secret deciphering key for $A$. What is the public key for $A$ (using the generator $g$)?
3. Send the message $P = 5$ to $A$ using ElGamal cryptosystem with the public key that you computed in (2.), assuming that we get the (random) integer $k = 3$.
4. Use the secret deciphering key of $A$ to retrieve the original message $P$ from the encrypted message that you obtained in (3.).

**Exercise 2** *(15%)* Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 4 & 2 & 6 & 1 & 8 & 7 \end{pmatrix} \in S_8$$

1. Compute the order of $\sigma$.
2. Compute the sign of $\sigma$.

**Exercise 3** *(15%)* Let $n \geq 2$ and let $\sigma$ be the $n$-cycle $\sigma = (1 \;\; 2 \;\; 3 \;\; \cdots \;\; n-1 \;\; n)$ in $S_n$.

1. Write $\sigma^2$ as the product of disjoint cycles, for $n$ even.
2. Write $\sigma^2$ as the product of disjoint cycles, for $n$ odd.

(Hint: If you do not know how to solve the exercise, you can try with some concrete values, for instance $n = 4, 5$, they can help you to solve the exercise)

**Exercise 4** *(35%)* Let $G$ be the dihedral group $G = D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, where $|a| = 4$, $|b| = 2$ and $aba = b$.

1. Compute the composition table of $G$ (Hints: $a^k b a^k = b$, $a^k b = ba^{-k} = ba^{4-k}$ and $|ba^k| = 2$ for all $k \in \mathbb{Z}$).
2. Prove that $\{1, a^2\}$ is a normal subgroup of $G$.
3. Compute $G/H$.
4. Compute the composition table of $G/H$.
5. What is the order of every element in $G/H$?, is $G/H$ a cyclic group?
6. Prove that $G/H$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^*$

(Hint: If you do not know how to solve one of the questions of exercise 4, you can try with the next ones.)

**Exercise 5** *(20%)*

1. Compute all the conjugacy classes in $G = (\mathbb{R}, +)$.
2. Compute $Z(G)$.
3. Compute all the conjugacy classes in the quaternion group $H$ (see exercise 2.16 in Lauritzen's book or see below).
4. Compute $Z(H)$.

One has that quaternion group is $H = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\} \subset GL_2(\mathbb{C})$, where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

*Husk at skrive jeres fulde navn på hver side af besvarelsen. Nummerer siderne, og skriv antallet af afleverede ark på 1. side af besvarelsen. God arbejdslyst.*