Algebra 1 (2012)-Aalborg University
Lectures 14 and 15, October 23rd and 25th

I will not be present during these lectures.

In these lectures we will see an application of group theory (cosets, quotient group) to coding theory, we will see how to correct errors over a noisy channel. We will consider linear codes, a family of error correcting codes. You can have a look at wikipedia: http://en.wikipedia.org/wiki/Linear_code. This theory is part of coding theory.

A message is encoded in a redundant way and the extra information is used to correct errors that may occur during the communication. For instance, the information in a DVD is encoded using some linear codes called Reed-Solomon codes. You can see a demonstration in Tom Høholdt's web page (from DTU):
http://www2.mat.dtu.dk/people/T.Hoeholdt/DVD/index.html

14th and 15th Lectures: Tuesday October 23rd and Thursday October 25th.

- Self-study of Error-Correcting codes. The bibliography will be: pages 49–58 in A course in Group Theory by John F. Humphreys.
- Work in groups: Exercises in Chapter 6 of Humpreys book (page 58): 1, 2, 3, 4, 5. You can solve some of them using Maple as well.

  Each group can write their solution for three exercises and leave it in my mailbox or send it by email (just one set of exercises per group). You are welcome to orientate me, by e-mail, about the successes and difficulties during the lecture.

The length, dimension and minimum distance of a linear code C are called the parameters of C, usually they are denoted by $[n, k, d]$. For n fixed, we would like to have k as high as possible to have an efficient communication (since we are considering $n - k$ redundant symbols) and d as high as possible to have a safe communication (to correct as many errors as possible). However, there are some limitations: the higher k is, the lower d is (and vice versa). For instance, one may easily prove that, for any linear code, $k + d \leq n + 1$. You can see in this web page a table containing the codes with best parameters (up to certain size): http://codetables.de/ (click in linear codes). For instance, the codes over $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \mathrm{GF}(2)$ can be seen here. You can click in the numbers to see the code.

Researchers in coding theory work finding codes with good parameters and with a fast decoding algorithm (faster than the one we learned in these lectures).

Best regards,

Diego