Institut for Matematik og Datalogi
Odense Universitet

15. marts 1999
LF

DM11 — F99 — Ugeseddel 7

Forelæsningen d. 9/3

Vi afsluttede afsnit 2.5 i bogen. Derefter begyndte vi på afsnittet "Algebra" i noterne. Her nåede vi til midt på s. 7.

Forelæsningen d. 16/3

Vi fortsætter med algebra-afsnittet i noterne.

Forelæsningen d. 23/3

Vi afslutter algebra-afsnittet. Derefter begynder vi på kapitel 4 i bogen.

Opgaver til uge 12

Afleveringopgave: En kinesisk hærfører har været i krig med 800 soldater. Efter et blodigt slag vil han gerne vide, hvor mange soldater, han har tilbage. Han stiller derfor sine soldater op i geledder af 7, 8 og 15 soldater, og får til rest henholdsvis 1, 3 og 10 mand.
Hjælp hærføreren med at bestemme, hvor mange soldater han har tilbage.

Juni 98 opgave 4

1. Skriv $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ og $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ som produkter af disjunkte kredse og som produkter af transpositioner.
   Bestem deres orden.
2. Bevis, at $\{1, 2, 4\}$ er en undergruppe af $\mathbb{Z}_7^*$ m.h.t. multiplikation.
3. Bevis, at A_n (de lige permutationer i S_n) er en undergruppe af S_n.

4. Lad G være en gruppe, og lad $a \in G$.
   Bevis, at
   (a) Hvis a har endelig orden n, da gælder
      i. $a^k = e \;\Leftrightarrow\; n \mid k$
      ii. $a^i = a^j \;\Leftrightarrow\; i \equiv j \pmod{n}$
      iii. $n = td \;\Rightarrow\; a^t$ har orden d
   (b) Hvis a har uendelig orden, da er elementerne i $\{a^k \mid k \in \mathbb{Z}\}$ alle forskellige.
5. Lad G være en gruppe, og lad $Z(G) = \{a \in G \mid \forall b \in G : ab = ba\}$.
   Bevis, at $Z(G)$ er en undergruppe af G.
   Gør rede for, at G er abelsk, hvis og kun hvis $Z(G) = G$.
6. Bevis, at en cyklisk gruppe kan have mere end én frembringer.
7. Hvilke ordener kan undergrupper af $\mathbb{Z}_{35}^*$ have?

Bemærkning

I noterne defineres ordenen af et element a i en gruppe som ordenen af $\langle a \rangle$, og det bevises, at ordenen af a er det mindste positive heltal m, så $a^m = e$. Man kan også gøre det omvendt:

Definition: Lad a være et element i en gruppe.

- Hvis der eksisterer et $k \in \mathbb{Z}^+$, så $a^k = e$, da siges a at have endelig orden, og a's orden $|a|$ er det mindste positive heltal n, så $a^n = e$.
- Hvis der *ikke* eksisterer et $k \in \mathbb{Z}^+$, så $a^k = e$, da siges a at have uendelig orden.

Sætning: Lad G være en gruppe, og lad $a \in G$. Da gælder

1. Hvis a har endelig orden n, da er
   $\langle a \rangle = \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$, og $a^i \neq a^j$ for $0 \leq i < j \leq n-1$.
2. Hvis a har uendelig orden, da er
   $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$, og $a^i \neq a^j$ for $i \neq j$.

Bevis:

1. Følger af opgave 4 punkt (a)ii.
2. Følger af opgave 4 punkt (b).