

## Ugeseddel 9.

**Evaluer Mat 2AL indtil 8/4:** <http://www.math.ku.dk/kurser/mat2al/mat2al-0.htm>

**Program.** I den 9. og sidste uge er overskriften „Sideklasser og afrunding“. Bemærk, at undervisningen fredag den 15. april er flyttet til tirsdag sådan: De sidste forelæsninger i Matematik 2AL-0 ligger tirsdag den 12. april kl 11-13, og de to „fredagshold“ har øvelser for sidste gang tirsdag den 12. april kl 9-11. Der er ingen ændringer vedrørende øvelser for torsdagsholdet.

Ved øvelserne regnes følgende opgaver:

11/4-15/4: GRP4: 6, 7, 8, 10, 11, 12, 13, 14, 17\*.

I de to foregående uger gennemgik jeg GRP3 (resten) og GRP4.

**Nøgleord:** Klein's Vierer-gruppe  $V = C_2 \times C_2$ , sideklasse modulo  $H$ , klassesdeling, index af undergruppe, kongruens modulo  $H$ , Lagrange's indexsætning, Fermat's lille Sætning og Euler's generalisering.

**Kommentar.** Det er et vigtigt resultat, at hvis  $G = \langle g \rangle$  er en cyklisk gruppe, så er enhver undergruppe  $H$  af  $G$  igen cyklisk; yderligere er  $H$ 's orden en divisor i  $G$ 's orden  $n$ , og for hver divisor  $d$  i  $n$  findes præcis én undergruppe  $H$  af orden  $d$ . Det er nyttigt at vide, at produktgruppen  $C_n \times C_k$  er cyklisk, hvis og kun hvis  $(n, k) = 1$ .

I GPR4 brugte jeg for første gang det fundamentale tælleprincip: Når en mængde  $G$  er delt i klasser, kan man tælle elementerne i  $G$  ved at tælle antallet af elementer i klasserne og lægge disse antal sammen. Elementært, ikke? Men dette enkle princip er grundlaget for næsten al kombinatorik. Og i hvert fald er det grundlaget for Lagrange's Indexsætning og dermed for vores bevis for Fermat's lille Sætning og Euler's generalisering. Fermat's store sætning siger i øvrigt, at ligningen  $x^n + y^n = z^n$ , for en eksponent  $n \geq 3$ , ikke har løsninger med naturlige tal  $x, y, z$ .

- *Lagrange's Indexsætning.*  $|G| = |G:H| \cdot |H|$ . Konsekvens: ordenen af  $H$  er divisor i ordenen af  $G$ .

- *Der er kun én* gruppe af orden  $p$ , hvor  $p$  er et primtal, nemlig den cykliske gruppe  $C_p$ .

- *Korollar til Lagrange.* Med  $n := |G|$  er  $g^n = e$  for alle  $g \in G$ .

- *Euler's Sætning.*  $(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}$ .

Fx:  $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ , så  $2^8 = 256 \equiv 1 \pmod{15}$ .

- *Fermat's lille sætning.* For et primtal  $p$  gælder:  $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$ .

Fx:  $2^{10} = 1.024 \equiv 1 \pmod{11}$ .

7. april 2005

• *Min allerførste liste.* Du kan allerede nu lave din helt egen liste over smågrupper, som du „kender“. Nogle grupper kommer i uendelige familier, fx  $C_n$  af orden  $n$ ,  $D_n$  af orden  $2n$ ,  $S_n$  af orden  $n!$  og  $A_n$  af orden  $n!/2$ . Specielt kan du for hvert  $n$  anføre den cykliske gruppe  $C_n$ . Gruppen  $\mathbb{Z}/n$  er den „additive udgave“ af den cykliske gruppe  $C_n$ . Nogle grupper kan fås ud fra mindre grupper: Fx er Klein’s Vierer-gruppe lig med produktet  $V = C_2 \times C_2$  af to cykliske grupper af orden 2. Den har orden 4, men hvert element  $g \in V$  opfylder, at  $g^2 = e$ ; specielt er  $V$  ikke cyklisk, så både  $V$  og  $C_4$  skal optræde i listen.

Det er faktisk ikke så nemt at afgøre, om to forelagte grupper er „den samme“ eller „forskellige“. Fx er  $C_2 \times C_3$  cyklisk af orden 6, og altså lig med gruppen  $C_6$ , og diedergruppen  $D_3$  er „lig med“ den symmetriske gruppe  $S_3$ .

Din liste skulle gerne omfatte følgende:

1	2	3	4	5	6	7	8	12	24	60	61	119	120
$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	$C_6$	$C_7$	$C_8$	$C_{12}$	$C_{24}$	$C_{60}$	$C_{61}$	$C_{119}$	$C_{120}$
%	%	%	$V$	%	$S_3$	%	$D_4$	$D_6$	$D_{12}$	$D_{30}$	%	%	$D_{60}$
			%		%		$Q_8$	$A_4$	$S_4$	$A_5$			$S_5$
							$C_2 \times C_4$	$C_3 \times V$	$\vdots$	$\vdots$			$\vdots$

men den burde allerede nu være lidt større. Markeringen med ‘%’ i en søjle betyder, at listen her er komplet. Når  $n$  er et primtal, er enhver gruppe af orden  $n$  nødvendigvis cyklisk, så i søjler svarende til primtal  $n$  er der præcis én markering, nemlig  $C_n$ . Det er selvfølgelig lidt blæret at markere, at der kun er én gruppe for  $n = 119$ , men begrundelsen får du først i Algebra 2, hvor din liste også udvides ganske meget.

**Hvornår** var det nu det var? Pierre de Fermat 1601–1665, Joseph-Louis Lagrange 1736–1813, Leonhard Euler 1707–1783.

**På sigt:** *Min* plan omfatter undervisningen på Algebra 2.

Anders Thorup