AALBORG UNIVERSITET
INSTITUT FOR
MATEMATISKE FAG
EVU2011
ALGEBRA 1
SPISESEDDEL 1.
LISBETH FAJSTRUP

Mål og indhold:

En gruppe er en ret simpel matematisk struktur: En mængde G, en komposition, $* : G \times G \to G$, altså en måde, hvorpå to elementer i mængden, $(g_1, g_2) \in G$ giver anledning til et nyt element $g_1 * g_2$ i mængden. $G, *$ udgør en gruppe, hvis

- Kompositionen er associativ.
- Der findes $e \in G$, så $g * e = e * g = g$ for ethvert $g \in G$. (e er en *neutralt* element.)
- For ethvert $g \in G$ findes g', så $g * g' = g' * g = e$

Det er den struktur, der studeres i Algebra 1. Dels som struktur i sig selv, og dels gennem alle de overraskende mange eksempler.
Permutationer giver et væsentligt eksempel på gruppestruktur. En permutation af tallene $1, 2, 3, 4$ er en omordning af tallene - til eksempelvis $2, 1, 4, 3$. En permutation kan betragtes som en bestemt type afbildning $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$. En afbildning $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ er en permutation, hvis og kun hvis σ er *bijektiv*. Hvis σ_1 og σ_2 er permutationer, er den sammensatte afbildning $\sigma_2 \circ \sigma_1$ også en permutation. Notationen for den sammensatte permutation er $\sigma_2\sigma_1$, som således er permutationen σ_1 efterfulgt af σ_2. Lad $X_n = \{1, 2, 3, \cdots, n\}$ repræsentere mængder med n elementer og lad S_n være *mængden af permutationer* på X_n. Da er S_n med kompositionen givet ved sammensætning af permutationer, $\sigma \star \tau = \sigma\tau$ en gruppe. S_n kaldes den *symmetriske gruppe* af grad n.
I opgaverne hjemme, skal I se på regning modulo et helt tal: $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ betegner *ækvivalensklasser* eller *restklasser* ved division med n. $\bar{3}$ repræsenterer således alle hele tal, som ved division med n giver rest 3, eller m.a.o. alle tal, som kan skrives $3 + nk$ for et helt tal k. Sædvanlig addition og multiplikation af hele tal giver addition og multiplikation af restklasser. $\mathbb{Z}_n, +$ er en gruppe med neutralt element $\bar{0}$. $\mathbb{Z}_n, \cdot$ er ikke en gruppe. Men det er $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | gcd(a, n) = 1\}$.

Torsdag 9-12

Forelæsning: 9-11. Introduktion, grupper, permutationsgrupper, cykler.

Øvelser: 11-12. Opgaver om permutationer Nicholson p.61:

1. Exercise 1.4.1
2. Exercise 1.4.3
3. 1.4.4
4. 1.4.6
5. 1.4.8

FREDRIK BAJERSVEJ 7G
9220 AALBORG ØST
9940 8848
FAJSTRUP@MATH.AAU.DK

Se desuden på oplægget til arbejdet i mellemperioden.

Fredag 9-12

Forelæsning: 9-11. Cykler, dekomposition, transpositioner, den alternerende gruppe, paritet.

Øvelser: 11-12.

1. Nicholson p. 62 Opg. 1.4.13 a), b) e) f)
2. Nicholsom 1.4.14
3. 1.4.15a)
4. 1.4.17 1.4.18 (Vink: Eksempel 10 p. 58)
5. 1.4.26

Arbejde i mellemperioden: Disse øvelser er til arbejdet i mellemperioden inden næste samling.

Opgave 1: Gør opgaverne fra torsdag og fredag om permutationsgrupper færdige. Lav gerne flere, hvis det stadig er svært.

Opgave 2: Lad $GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) | \det(A) \neq 0\}$. (Alle 2x2 matricer, som har determinant forskellig fra 0). Vis, at $GL_2(\mathbb{R})$ er en gruppe under matrixmultiplikation.

Opgave 3: Er et miniprojekt.

Lad $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ betegne *ækvivalensklasser* eller *restklasser* ved division med n. Således repræsenterer $\bar{3}$ tallene $\{\cdots, 3-3n, 3-2n, 3-n, 3, 3+n, 3+2n, 3+3n, 3+4n, \cdots\}$ eller m.a.o. alle hele tal, som kan skrives $3+kn$ for et helt tal k, i.e., $\bar{3} = \{3+kn | k \in \mathbb{Z}\} = \{m \in \mathbb{Z} | m \equiv 3 \ mod \ n\}$. Se også Nicolson p.41-42 og Rosen p.556 Eksempel 3 og p.558 Eksempel 9.

1. Vis (genopfrisk fra kurset Diskret matematik eller find hos Nicholson 1.3), at addition og multiplikation af hele tal giver mening for $\mathbb{Z}_n$, altså
   (a) $a_1, a_2 \in \bar{a}$ hvis og kun hvis $a_1 \equiv a_2 \ mod \ n$
   (b) Hvis $a_1, a_2 \in \bar{a}$ og $b_1, b_2 \in \bar{b}$, så er $\overline{a_1 + b_1} = \overline{a_2 + b_2} = \overline{a+b}$ og $\overline{a_1 b_1} = \overline{a_2 b_2} = \overline{ab}$.

   Definer nu $\bar{a} + \bar{b} = \overline{a+b}$ og $\bar{a}\bar{b} = \overline{ab}$
2. Vis, at $\mathbb{Z}_n, +$ er er gruppe.

3. Se på $\mathbb{Z}_6$ med multiplikation. Opskriv multiplikationstabellen. Find et neutralelement i $\mathbb{Z}_6$ ved at se på multiplikationstabellen. Hvilke elementer er invertible?

4. Samme som ovenfor med $\mathbb{Z}_5$.

5. Vis, at hvis p er et primtal, så er $\mathbb{Z}_p \setminus \{0\}$ en gruppe med multiplikation. [1]

6. Vis, at $\mathbb{Z}_n \setminus \{0\}$ med multiplikation er en gruppe hvis *og kun hvis* n er et primtal.[2]

7. Vis, $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n | gcd(a, n) = 1\}$ er en gruppe med multiplikation.[3]

Litteratur:

Til både torsdag og fredag: Nicholson. Kapitel 1.4 og desuden 1.3 til selvstudier hjemme. Samt naturligvis introduktion til kurset og denne spiseseddel.

Med venlig hilsen
Lisbeth Fajstrup

[1] Vink: Nicholson Sætning 5 p. 45 eller Rosen Sætning 3 p. 234

[2] Vink: Antag, $n = pq$. Så er $pq \equiv 0 \ mod \ n$. Hvorfor gør det, at $\mathbb{Z}_n \setminus \{0\}$ ikke er en gruppe under multiplikation??

[3] Vink: Nicholson Sætning 5 p.45 eller Rosen Sætning 3 p.232.Husk også at vise, at $a, b \in \mathbb{Z}_n^* \Rightarrow ab \in \mathbb{Z}_n^*$

FREDRIK BAJERSVEJ 7G 9940 8848 FAJSTRUP@MATH.AAU.DK
9220 AALBORG ØST