Gruppeteori

InterMat på Birkerød Gymnasium, efterår 2018

Andreas Obel-Jørgensen og Niels Erik Wegge

Indhold

0. Oversigt over de fire mødegange

Første mødegang: Introduktion til gruppeteori

1. Gruppebegrebet, aksiomerne
2. Gruppen $(U_{10},\cdot)$ af primiske tal modulo 10 med gange som komposition
3. Vi introducerer begrebet sideklasser (med udgangspunkt i $(U_{10},\cdot)$.
4. Eksemplet $(S_3,°)$: de seks symmetrier på en ligesidet trekant.
5. Konstaterer, at det er "det samme" som matrixmultiplikation af seks konkrete 2x2-matricer.

Anden mødegang: Katalog over små grupper, isomorfibegrebet, undergrupper.

1. Opvarmningsopgave: Udfylde og analysere kompositionstabel for gruppen $(Z_6,+)$, altså addition modulo 6.
2. Vi ser i fællesskab på tabellen:
    a. Konstaterer kommutativitet.
    b. Konstaterer associativitet med et enkelt regneeksempel.
    c. Identificerer inverse til udvalgte elementer, fx $4^{-1}=3$.
    d. Løser ligningen $x+4=3$.
    e. Konstaterer at 1 og 5 hver især frembringer hele gruppen.
    f. Finder to ægte undergrupper: {0,3} og {0,2,4}.
    g. Konstaterer at gruppen **alligevel** er forskellig fra S_3, som vi så på sidst (var ikke cyklisk).
3. Bestemmelse af de mindste grupper (orden 1, 2, 3, 4)
4. Vi afslutter med kort gennemgang af isomorfibegrebet: funktionen $f(x)=\log(x)$ giver en isomorfi $(R_+,\cdot)\to(R,+)$

Tredje mødegang: Lagranges sætning

1. Opvarmningsopgave om $(U_{16},\cdot)$.
2. Lagranges sætning
    a. Beviset gennemgås
    b. Konsekvenser
    c. Generering af cykliske undergrupper
    d. Vise at et element opløftet i gruppeordenen giver neutralelementet: $x^{|G|}=e$
3. RSA-kryptering (teaser før næste gang).

Fjerde mødegang: RSA-kryptering

- RSA-kryptering

1. Introduktion af begreber

1.1 Definition af en gruppe $(G,*)$

Se evt. først – eller efter endt læsning – følgende to videoer fra *Socratica*:

- Definition af en gruppe: *https://www.youtube.com/watch?v=g7L_r6zw4-c*
- Motivering af definitionen: *https://www.youtube.com/watch?v=yHq_yzYZV6U&index=14&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6*

En gruppe består løst sagt af en mængde G udstyret med en regneregel $*$, som kan bruges på mængdens elementer. Helt præcist:

$(G,*)$ udgør en **gruppe** når

1. G er **stabil/lukket** overfor den binære komposition $*$, dvs at for alle a, b i G er $a * b$ også i G. Man får altså ikke lige pludselig nye elementer, som ikke ligger i den mængde, man arbejder med.
2. Der skal findes et element e så $a * e = e * a = a$. Elementet e kaldes et **neutralt element**.
3. Ethvert element a i G skal have et **inverst element** betegnet a^{-1}, så $a * a^{-1} = a^{-1} * a = e$.
4. $*$ skal være **associativ.** Det betyder at $a * (b * c) = (a * b) * c$ for alle a, b, c i G. Da operationen * er binær, virker den jo kun på 2 elementer af gangen – og derfor er man nødt til at sætte parenteser i udtryk som $a * b * c$, for at det giver mening. Den associative egenskab af $*$ sikrer, at det er ligegyldigt, hvor man sætter parenteserne.

Hvis det derudover gælder, at $a * b = b * a$ for alle a, b i G – altså at man kan ombytte rækkefølgen – siges gruppen at være **kommutativ** eller **Abelsk**.

1.2 Eksempler på grupper og ikke-grupper

Eksempel 1: $(G,*) = (N, +)$

De naturlige tal $N = \{1,2,3, \dots\}$ udstyret med regnereglen +. N er lukket overfor + men der er ikke noget neutral element, så det er ikke en gruppe. Man kunne tage 0 med, men det ville ikke hjælpe, for tallene har ikke nogen inverse elementer.

Eksempel 2: $(G,*) = (Z, +)$

De hele tal $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$ med addition som komposition. Alle regler opfyldt: det er en gruppe!

Eksempel 3: $(G,*) = (Q\ ,\ \cdot)$

De rationelle tal (altså brøker med hel tæller og hel nævner) med gange som komposition. Alt opfyldt – på nær at 0 ikke har noget inverst element. Altså ikke en gruppe.

Eksempel 4: $(G,*) = (Q \backslash \{0\},\ \cdot)$

De rationelle tal *uden nul* med gange som komposition. Alle regler opfyldt: det er en gruppe.

1.3 Begreber knyttet til endelige grupper

Begreb: Kompositionstabel

Vi ser på tal, som er primiske med 10: $U_{10} = \{1,3,7,9\}$. Denne mængde udstyrer vi med kompositionen x_{10} som betegner multiplikation modulo 10, som igen betyder resten efter division med 10.

Et eksempel: $3\mathrm{x}_{10}9 = 7$, fordi $3 \cdot 9 = 27$ og 10 går 2 gange op i 27 med resten 7.

En **kompositionstabel** viser resultaterne af alle de mulige regnestykker man kan lave inden for U_{10} med x_{10}.

For at udfylde feltet med $a\ \mathrm{x}_{10}\ b$ tages a fra den vandrette række og b fra den lodrette søjle.

For eksempel: $a = 7$ og $b = 3$, $a\ \mathrm{x}_{10}\ b = 7\ \mathrm{x}_{10}\ 3 = 21 \bmod 10 = 1$

x_{10}	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	$7\ \mathrm{x}_{10}\ 3 = 1$	9	3
9	9	7	3	1

Kompositionstabellen kan bruges til at tjekke at alle betingelserne er opfyldt for at $(\{1,3,7,9\}, \mathrm{x}_{10})$ er en gruppe.

Bemærk at det inverse element til 7 er 3, altså $7^{-1} = 3$. Det ser jo sært ud!

Begreb: Undergruppe

Hvis man ser på kompositionstabellen ovenfor, ser man, at delmængden $\{1,9\}$ udgør en gruppe i sig selv (tjek betingelserne) – det kaldes en **undergruppe**. I enhver gruppe vil der altid være mindst 2 undergrupper, nemlig $(\{e\},*)$ bestående af det neutrale element, og hele gruppen selv. Det kaldes de **trivielle undergrupper**.

Begreber: Orden af gruppe, undergruppe, element, generator, cyklisk gruppe

Antallet af elementer i en gruppes mængde kaldes gruppens **orden**. I dette tilfælde er ordenen af (G, x_{10}) lig med 4, mens undergruppen $(\{1,9\}, \mathrm{x}_{10})$ har orden 2.

Hvis man tager et element i en endelig gruppe og komponerer det med sig selv gentagne gange, vil man før eller siden få det neutrale element – ellers ville det ikke være en endelig gruppe. (Denne påstand kræver et bevis!) Det antal gange, der skal til for at få neutralelementet frem, kaldes elementets orden. Eksempel:

$$3 \qquad 3\mathrm{x}_{10}3 = 9 \qquad 3\mathrm{x}_{10}3\mathrm{x}_{10}3 = 7 \qquad 3\mathrm{x}_{10}3\mathrm{x}_{10}3\mathrm{x}_{10}3 = 3^4 = 81 \bmod 10 = 1$$

Elementet 3 skal altså komponeres med sig selv 4 gange, før det giver neutral elementet 1, så ordenen af 3 er 4. Man kalder samtidig elementet 3 for en **generator**, fordi det åbenbart genererer alle elementer i gruppen "undervejs". En gruppe, hvor mængden af elementer kan frembringes af en generator, kaldes **cyklisk**.

Hvis man i eksemplet ovenfor ser på elementet 9, har det orden 2.

Vigtige observationer (som altid gælder og som vi beviser i kapitel 3)

Ordenen af undergruppen (her 2) går et helt antal gange op i ordenen af gruppen (her 4). Det er Lagranges sætning (kapitel 3). Ordenen af et element går ligeledes op i ordenen af gruppen. Og hvis man tager et hvilket som helst element i gruppen og opløfter i gruppens orden (komponerer med sig selv gruppens ordens gange (kors for et dansk!) får man gruppens neutral element.

Dette er baggrunden for RSA-Krypteringen virker!

Begreber: Sideklasser til en undergruppe og klassedeling af mængden

Vi tager undergruppen {1,9} og komponerer danner de såkaldte (venstre) **sideklasser** ved at komponere et element ind fra venstre:

- $1\mathrm{x}_{10}\{1,9\} = \{1,9\}$
- $3\mathrm{x}_{10}\{1,9\} = \{3,7\}$
- $7\mathrm{x}_{10}\{1,9\} = \{7,3\}$
- $9\mathrm{x}_{10}\{1,9\} = \{9,1\}$

Da den rækkefølge, vi lister elementerne i, ikke har betydning, er der altså i dette tilfælde kun 2 forskellige sideklasser: $\{1,9\}$ og $\{3,7\}$.

Vigtige observationer om sideklasser:

Sideklasserne har ikke nogen elementer tilfælles (de er "disjunkte"), og tilsammen indeholder de alle elementerne fra gruppen. Man siger at sideklasserne giver en **klassedeling** af mængden. Det kan sammenlignes med klasserne i en skole: tilsammen udgør de hele skolen (hver elev går i en eller anden klasse), og der er ikke noget overlap mellem klasserne (hver elev går kun i én klasse).

Bemærk også, at der er lige mange elementer i hver af sideklasserne! Det er dette, som ender med at give Lagranges sætning: nemlig at ordenen af en undergruppe går op i ordenen af en endelig gruppe.

1.4 Opgaver

Opgave 1: En restklassegruppe

Betragt de tal som er primiske med 14; $G = \{1,3,5,9,11,13\}$ og udstyr mængden med kompositionen "x_{14}", dvs. gange modulo 14.

Eksempel $9\mathrm{x}_{14}13 = 9 \cdot 13 \bmod 14 = 117 \bmod 14 = 5$, fordi 117 giver resten 5 efter division med 14.

1. Lav en kompostionstabel og vis at (G, x_{14}) er en gruppe
2. Find undergrupper. Hvor mange ikke-trivielle undergrupper kan du finde?
3. Bestem sideklasserne til en eller flere af de fundne undergrupper, og illustrer klassedelingen med et mængdediagram.

Opgave 2: En endelig matrixgruppe

1. Vis ved hjælp af en kompositionstabel at nedenstående 6 matricer med multiplikation som komposition udgør en gruppe.
2. Find undergrupper.
3. Bestem sideklasserne til de fundne undergrupper, og illustrer klassedelingen med et mængdediagram

$$A_1 = \begin{Bmatrix} 1 & 0 \\ 0 & 1 \end{Bmatrix} \qquad A_2 = \begin{Bmatrix} -1 & 0 \\ 0 & 1 \end{Bmatrix} \qquad A_3 = \begin{Bmatrix} \frac{1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{Bmatrix}$$

$$A_4 = \begin{Bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{Bmatrix} \qquad A_5 = \begin{Bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{Bmatrix} \qquad A_6 = \begin{Bmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{Bmatrix}$$

Hvis du vil vide mere om matrixgrupper så se følgende video:

https://www.youtube.com/watch?v=AJTRwhSZJWw&index=18&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6

Opgave 3: Symmetrigruppen på en ligesidet trekant: $(\boldsymbol{S_3}, \circ)$

Se evt. https://www.youtube.com/watch?v=DeCcqioogLY&index=17&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6

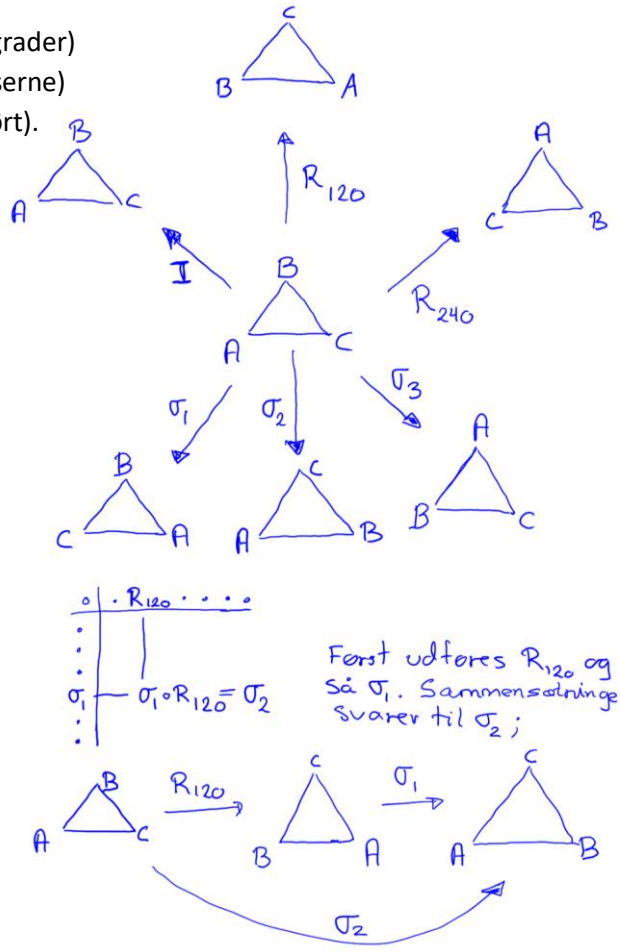
Der findes 6 symmetrioperationer, som kan udføres på en ligesidet trekant i planen, således at trekanten efter udført symmetri dækker sig selv:

- To forskellige rotationer (hhv. 120 grader og 240 grader)
- Tre forskellige spejlinger (en i hver af symmetriakserne)
- Den trivielle operation (at lade trekanten ligge urørt).

De 6 operationer er vist på figuren.

De 6 operationer kan sammensættes / sættes efter hinanden (en enkelt af disse sammensætninger er illustreret på figuren), og herved opstår gruppen $(S_3, \circ)$.

1. Lav en kompositionstabel og argumentér for at symmetrierne udgør en gruppe under kompositionen sammensætning.
2. Find undergrupper
3. Bestem sideklasserne til de fundne undergrupper, og illustrer klassedelingen med et mængdediagram.
4. Forsøg at forklare, hvorfor denne gruppe er "den samme" som matrixgruppen i forrige opgave.
5. Hvordan kan man "gange matricerne" ved at "flytte rundt" på trekanten?



2. Katalog over de mindste grupper

2.1 Opvarmning

Vi repeterer definitionen på en gruppe:

$(G, *)$ udgør en **gruppe** når

1. G er stabil/lukket overfor den binære komposition *, dvs at for alle a, b i G er $a * b$ også i G.
2. Der findes et element e i G så $a * e = e * a = a$. Elementet e kaldes et neutral element.
3. Ethvert element a i G skal have et inverst element betegnet a^{-1}, som opfylder $a * a^{-1} = a^{-1} * a = e$
4. * skal være associativ; $a * (b * c) = (a * b) * c$.

Hvis det derudover for alle a, b i G gælder at $a * b = b * a$, siges gruppen at være **kommutativ** eller **Abelsk**.

Og hvis der er n elementer i gruppen, siger vi, at den har **orden** $|G| = n$.

Kravene 1-4 viser sig at sætte kraftige sudoku-agtige begrænsninger på hvor mange grupper, der findes. Vi vil nedenfor se på grupper, der har lille orden, dvs. kun har få elementer (op til fire elementer). Specielt vil vi undersøge, hvor mange sådanne grupper der findes. Men først en opvarmningsopgave:

Opgave 4: Gruppen $(Z_6, +)$

Vi ser på mængden $Z_6 = \{0,1,2,3,4,5\}$ og udstyrer den med kompositionen "addition modulo 6".

Eksempel: $3 + 5 = 2$ og $4 + 2 = 0$.

a. Udfyld de manglende felter i kompositionstabellen.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2					1
3	3					2
4	4					3
5	5					4

b. Undersøg om aksiomerne 1-4 for en gruppe er opfyldt.
c. Er $(Z_6, +)$ en abelsk gruppe? Og hvad er dens orden?
d. Hvor mange gange optræder det neutrale element i hver række og i hver søjle?
e. Er der elementer, der optræder mere end én gang i hver række eller søjle?
f. Brug tabellen til at løse ligningen $x + 4 = 3$.
g. Brug tabellen til at finde det inverse element til 4.
h. Forklar for hvert skridt i følgende beregninger hvilken af gruppeteorireglerne man bruger:

$$x + 4 = 3$$
$$(x + 4) + 2 = 3 + 2$$
$$x + (4 + 2) = 5$$
$$x + 0 = 5$$
$$x = 5$$

i. Vis at gruppen har to ægte undergrupper: {0,3} og {0,2,4}.
j. Vis at 1 og 5 hver især frembringer hele gruppen (så $(Z_6, +)$ er altså en cyklisk gruppe).
k. Gruppen $(Z_6, +)$ og $(S_3, °)$, som vi så på sidst, har begge 6 elementer. Forklar hvorfor der alligevel ikke kan være tale om samme gruppe [hint: er de begge to cykliske?]

2.2 Entydighed af neutralt og inverst element i en gruppe.

Sætning 1: Der er kun ét neutralt element i en gruppe.

Bevis: Antag at både e_1 og e_2 er neutrale. Så gælder $e_1 = e_1 * e_2 = e_2$. Altså er e_1 lig med e_2, og så var der altså alligevel kun et neutralt element.

Sætning 2: I hver række og i hver søjle i en kompositionstabel for en gruppe skal alle gruppens elementer forekomme én og kun én gang.

Bevis: Lad gruppen have orden $|G| = n$. Så kan vi skrive $G = \{e, g_2, g_3, \dots, g_n\}$, hvor alle de anførte elementer er forskellige. De n stk. elementer i en række i kompositionstabellen er derfor $g * e$, $g * g_2$, $g * g_3$, … $g * g_n$. Tag to tilfældige elementer i en række, f.eks. $g * g_i$ og $g * g_j$ og antag at to af disse elementer er ens. Vi skal vise, at så er det det samme element, vi har taget to gange, altså $g_i = g_j$. Vi regner:

$$g_i = e * g_i = (g^{-1} * g) * g_i = g^{-1}(g * g_i) = g^{-1} * \big(g * g_j\big) = (g^{-1} * g) * g_j = e * g_j = g_j$$

som ønsket.

Vi har nu vist, at alle elementerne i en række er forskellige – og da der lige så mange pladser i en række, som der er elementer i gruppen, så må alle elementer i gruppen forekomme en og kun en gang i rækken.

Beviset for søjlerne føres tilsvarende.

2.3 Grupper af orden 1, 2 og 3

Orden 1: $|\boldsymbol{G}| = \mathbf{1}$

Der er kun et enkelt element i gruppen, så dette må være det neutrale element (som jo *skal* være der): $G = \{e\}$. Kompositionen er den trivielle: $e * e = e$ og $e^{-1} = e$.

Orden 2: $|\boldsymbol{G}| = \mathbf{2}$

Vi kan skrive $G = \{e, g\}$, hvor e er det neutrale element, og hvor g er et andet element. Der må gælde følgende kompositionstabel:

$*$	$\boldsymbol{e}$	$\boldsymbol{g}$
$\boldsymbol{e}$	e	g
$\boldsymbol{g}$	g	e

Ifølge Sætning 2 ovenfor er der ikke andre muligheder. Der er altså kun én gruppe af orden 2.

Orden 3: $|\boldsymbol{G}| = \mathbf{3}$

Vi kan skrive $G = \{e, a, b\}$, hvor e er det neutrale element, og hvor a, b er to andre elementer. Om kompositionstabellen må der gælde følgende:

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a		
$\boldsymbol{b}$	b		

I række 2 skal vi have placeret elementerne e og b. Da der ikke må stå mere end ét b i søjle 3 (iflg. sætning 2), er det nødt til at blive sådan:

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a	b	e
$\boldsymbol{b}$	b		

og så er der kun én mulighed for række 3:

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a	b	e
$\boldsymbol{b}$	b	e	a

Vi har altså fundet ud af, at der kun er én gruppe med orden 3.

Bemærk at gruppen er abelsk (tabellen er symmetrisk i diagonalen) og at den er cyklisk, frembragt af såvel a som b:

- $a^2 = a * a = b, \qquad a^3 = a^2 * a = b * a = e.$
- $b^2 = b * b = a, \qquad b^3 = b^2 * b = a * b = e.$

Dvs. $G = \{a, a^2, a^3\} = \{b, b^2, b^3\}$.

2.4 Grupper af orden 4

Indtil nu har det vist sig, at der er præcis én gruppe med orden hhv. 1, 2 og 3. Nu, ved orden 4, sker der nye ting!

Når $|G| = 4$ kan vi skrive $G = \{e, a, b, c\}$, hvor e er det neutrale element, og hvor a, b, c er tre andre elementer. Om kompositionstabellen må der til en start gælde følgende:

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a			
$\boldsymbol{b}$	b			
$\boldsymbol{c}$	c			

I række 2 skal vi have placeret elementet b. Der er kun to muligheder, da der kun må være ét b i søjle 3:

Mulighed 1

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	b		
$\boldsymbol{b}$	b			
$\boldsymbol{c}$	c			

Mulighed 2

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a			b
$\boldsymbol{b}$	b			
$\boldsymbol{c}$	c			

Vi arbejder først videre med mulighed 1, og kalder nu kompositionen $*_1$:

I søjle 2 er der (igen pga. sætning 2) kun ét sted, hvor c kan stå (og så må der stå e på den sidste plads):

$*_1$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b	c		
c	c	e		

Tilsvarende er der nu ikke noget valg for c og e i række 2:

$*_1$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c		
c	c	e		

De fire sidste pladser kan kun udfyldes på én måde:

$*_1$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Vi er endt med en abelsk, cyklisk gruppe (se opgaven nedenfor).

Opgave 5: Vis at gruppen $(G,*_1)$ med kompositionstabellen givet ovenfor frembringes af elementet a og af elementet c; altså at $G = \{a, a^2, a^3, a^4\} = \{c, c^2, c^3, c^4\}$. Vis også at G ikke er frembragt af elementet b!

Nu går vi tilbage og arbejder videre med mulighed 2:

$*_2$	e	a	b	c
e	e	a	b	c
a	a			b
b	b			
c	c			

I række 2 har vi to måder, hvorpå e og c kan placeres:

$*_{2A}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b			
c	c			

eller

$*_{2B}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b			
c	c			

Herefter er der kun én måde at gøre søjle 2 færdig på:

$*_{2A}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

hhv.

$*_{2B}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e		
c	c	b		

De sidste fire positioner kan udfyldes på hhv. 2 måder og 1 måde, nemlig

$*_{2A1}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

eller

$*_{2A2}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

samt

$*_{2B}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Alt i alt er vi – ved at bruge sudoku-agtige metoder – nået frem til, at der *ser ud til* at være fire grupper af orden 4:

$*_1$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*_{2A1}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$*_{2A2}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$*_{2B}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Men: af disse er den første, den tredje og den sidste faktisk ens! En gruppeteori-matematiker ville sige: de er **isomorfe.** Mere herom senere.

For at vise at den første er "mage til" (isomorf med) den sidste, omdøber vi elementerne i $(G,*_1)$:

$$a \to B, \qquad b \to C, \qquad c \to A;$$

og dernæst bytter vi om på søjlerne og til sidst bytter vi om på rækkerne:

$*_1$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

→

$*_1$	e	B	C	A
e	e	B	C	A
B	B	C	A	e
C	C	A	e	B
A	A	e	B	C

Ombytter søjle 2 og 4:

$*_1$	e	A	C	B
e	e	A	C	B
B	B	e	A	C
C	C	B	e	A
A	A	C	B	e

Ombytter søjle 3 og 4:

$*_1$	e	A	B	C
e	e	A	B	C
B	B	e	C	A
C	C	B	A	e
A	A	C	e	B

Ombytter række 1 og 4:

$*_1$	e	A	B	C
e	e	A	B	C
A	A	C	e	B
C	C	B	A	e
B	B	e	C	A

Til sidst ombyttes række 3 og 4 – og vi sammenligner med $(G,*_B)$:

$*_1$	e	A	B	C
e	e	A	B	C
A	A	C	e	B
B	B	e	C	A
C	C	B	A	e

$*_{2B}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Der er tydeligvis tale om en og samme gruppe, nemlig den cykliske gruppe $(G,*_1)$ ☺

På samme måde kan man indse, at også $(G,*_{2A2})$ er denne samme gruppe.

Derimod er gruppen $(G,*_{2A1})$ helt forskellig. Som det fremgår af kompositionstabellen står der e hele vejen ned i diagonalen, hvilket betyder at alle elementerne selv-inverse: $a * a = b * b = c * c = e$:

$*_{2A1}$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	e	c	b
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	b	a	e

Denne gruppe er derfor ikke cyklisk, og som kan derfor ikke være magen til den cykliske $(G,*_1)$.

Gruppen $(G,*_{2A2})$ er en vigtig gruppe, som kaldes **Kleins fire-gruppe**.

Konklusion: Der findes to forskellige grupper af orden 4,

nemlig Kleins fire-gruppe og en cyklisk gruppe.

Opgave 6: Hvilke undergrupper findes der i hver af de to grupper af orden fire?

Opgave 7: I afsnit 1.3 mødte vi en anden gruppe med fire elementer. Var det muligvis Kleins fire-gruppe i forklædning? Ellers må det jo have været den cykliske gruppe af orden 4…

Opgave 8: Hvor mange grupper mon der findes af orden 5 og 6 og …?

2.5 Isomorfibegrebet

Se evt. følgende video om isomorfi:

https://www.youtube.com/watch?v=BAmWgVjSosY&index=7&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6

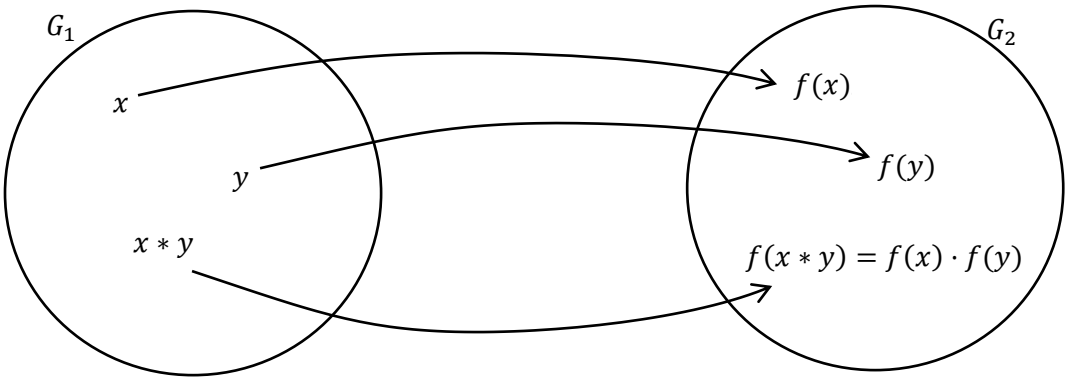
I det forrige afsnit brugte vi en del kræfter på at undersøge hvorvidt to tilsyneladende forskellige grupper var ens eller ej. Nu vil vi præcisere, hvad der menes med "ens".

Definition: To grupper $(G_1,*)$ og $(G_2,\cdot)$ kaldes **isomorfe** hvis

1. der findes en afbildning $f: G_1 \to G_2$ som kobler elementerne i G_1 og G_2 sammen to og to, sådan at hvert element i G_1 får én og kun én "makker" i G_2 og omvendt.
2. afbildningen f respekterer kompositionsreglen i begge grupper: $f(x * y) = f(x) \cdot f(y)$.

Betydning af krav 1: Der er lige mange elementer i G_1 og G_2, og f svarer til en om-navngivning af elementerne.

Betydning af krav 2: Se figuren. Man kan altid danne $x * y$ i G_1 og $f(x) \cdot f(y)$ i G_2 – men når f er en isomorfi, ved man at "makkeren" til $x * y$ ovre i G_2 (altså $f(x * y)$) netop er $f(x) \cdot f(y)$, og på den måde passer det hele sammen.



Man kan også sige, at f omdøber elementerne og at kravet to sørger for at kompositionstabellerne er ens i G_1 og G_2 – og det var jo det, der foregik i eksemplet ovenfor med grupperne af orden 4.

Sætninger om isomorfe grupper:

Sætning 1: Hvis f er en isomorfi mellem grupperne $(G_1,*)$ og $(G_2,\cdot)$, så afbilder f det neutrale element e_1 i G_1 ind i det neutrale element e_2 i G_2.

Bevis:

Lad y være et vilkårligt element i G_2. Vi skal vise at $f(e_1) \cdot y = y$ og $y \cdot f(e_1) = y$. Vælg derfor et element x i G_1 sådan at $f(x) = y$ (så x er altså makkeren til y). Så gælder $f(e_1) \cdot y = f(e_1) \cdot f(x) = f(e_1 * x) = f(x) = y$ som ønsket. På samme måde vises at $y \cdot f(e_1) = y$.

Sætning 2: Hvis f er en isomorfi mellem grupperne $(G_1,*)$ og $(G_2,\cdot)$, og hvis x^{-1} er det inverse element til x i G_1, så er $f(x^{-1})$ det inverse element til $f(x)$ i G_2.

Bevis: Vi skal bare vise at $f(x^{-1}) \cdot f(x) = e_2$ og $f(x) \cdot f(x^{-1}) = e_2$. Prøv selv!

Sætning: Grupperne $(G_1,*)$ og $(G_2,\cdot)$ givet ved nedenstående kompositionstabeller er isomorfe.

$(\boldsymbol{G_1},*)$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	b	c	e
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	e	a	b

$(\boldsymbol{G_2},\cdot)$	$\boldsymbol{E}$	$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{C}$
$\boldsymbol{E}$	E	A	B	C
$\boldsymbol{A}$	A	C	E	B
$\boldsymbol{B}$	B	E	C	A
$\boldsymbol{C}$	C	B	A	E

Bemærk at det drejer sig om de to grupper, vi kiggede på i analysen af grupperne af orden 4.

Bevis: Lad $f: G_1 \to G_2$ være afbildningen givet ved

- $e \mapsto E$
- $a \mapsto B$
- $b \mapsto C$
- $c \mapsto A$

Dette er er en-til-en afbildning, der danner "makker-par" mellem G_1 og G_2. Lad os se, om f respekterer kompositionsreglerne. Det er 16 regnestykker, der skal checkes, nemlig hele kompositionstabellen i G_1. Pyha! Vi nøjes med at checke de fire regnestykker der står i søjle 2:

- $f(e * a) = f(a) = B$, hvilket passer med at $f(e) \cdot f(a) = E \cdot B = B$
- $f(a * a) = f(b) = C$, hvilket passer med at $f(a) \cdot f(a) = B \cdot B = C$
- $f(b * a) = f(c) = A$, hvilket passer med at $f(b) \cdot f(a) = C \cdot B = A$
- $f(c * a) = f(e) = E$, hvilket passer med at $f(c) \cdot f(a) = A \cdot B = E$

Øvelse: Prøv at checke søjle 3 og 4 på samme måde!

Eksempel: Logaritmefunktioner som isomorfi

Du kender nok logaritmefunktion som dem, der laver eksponentialfunktioner om til lineære funktioner:

$$\log(b \cdot 10^{ax}) = \log(b) + a \cdot x.$$

I "gamle dage", hvor man ikke havde lommeregnere og computere, var logaritmefunktionerne imidlertid først og fremmest et uvurderligt hjælpemiddel til at kunne lave multiplikationsregnestykker med mange decimaler hurtigt. Man havde møjsommeligt udarbejdet store tabelværker med lister over logaritmen til alle mulige tal, og ved hjælp af dem lavede man gangestykkerne om til plusstykker (som jo er nemme at lave). Det kunne man, fordi logaritmefunktionen er en isomorfi mellem grupperne $(R_+,\cdot)$ og $(R,+)$:

Grafen for $\log(x)$ er en voksende funktion mellem de positive reelle tal og alle de reelle tal, så den etablerer en en-til-en forbindelse mellem tallene i R_+ og R. Og ikke mindst gælder regnereglen

$$\log(x \cdot y) = \log(x) + \log(y).$$

Hvis man skulle regne værdien af $x \cdot y$ ud, ville man først finde tallene $\log(x)$ og $\log(y)$ i sin logaritmetabel. Så ville man lægge sammen og finde tallet $\log(x) + \log(y)$ inde i logaritmetabellen – og til sidst ville man bruge tabellen baglæns og således finde $\log^{-1}(\log(x) + \log(y))$. Og dette tal er jo $x \cdot y$!

Opgaver i isomorfi

Antag at grupperne $(G_1,*)$ og $(G_2,\cdot)$ er isomorfe gennem en afbildning $f: G_1 \to G_2$.

Vi kalder det neutrale element i G_1 og G_2 for hhv. e_1 og e_2.

Antag endvidere, at elementet $a \in G_1$ har orden p, altså $a * a * a * \ldots * a = a^p = e_1$

1. Vis at billedet $f(a)$ i $(G_2,\cdot)$ også må have orden p.
   (Hint: benyt at $f(a^p) = f(a * a^{p-1}) = f(a) \cdot f(a^{p-1})$ gentagne gange, og husk at $f(e_1) = e_2$).
2. Benyt dette til at undersøge, om (U_{14}, x_{14}) kan være isomorf med de to andre grupper fra opgaverne i 1.4; matrixgruppen og symmetrierne i en trekant.
3. Vis at matrixgruppen og symmetrioperationerne i en trekant er isomorfe, ved at lave en tabel over sammenhørende elementer i de to grupper, altså f angivet som en tabel.
4. Prøv at beregne produktet af to matricer vha. følgende procedure:
   a. Find de to tilhørende symmetrioperationer i trekanten.
   b. Dan produktet af de to symmetrioperationer og find den matrix som svarer til produktet.
      Passer den matrix du fandt under b med det man får, hvis man bare ganger matricerne sammen?
      Det burde den. Og så har du altså set endnu et eksempel på, at besværlige udregninger (matrixmultiplikation) kan omgås ved at flytte problemet over i en andet gruppe via en isomorfi – en gruppe, hvor det er meget lettere at arbejde (trekantssymmetrier).

3. Lagranges sætning

3.1 Opvarmningsopgaver

Opgave A: Betydning af mængdetegnene ∪ (foreningsmængde) og ∩ (fællesmængde)

Givet mængderne $A = \{1, 2\}$ og $B = \{2,3\}$ og $C = \{1,2,3,4\}$.

1. Find $A \cup B$ og $A \cap B$
2. Find $B \cup C$ og $B \cap C$
3. Find $A \cap B \cap C$

Opgave B: Gruppen $(U_{16}, \mathrm{x}_{16})$

Betragt mængden af tal som er primiske med 16: $U_{16} = \{1,3,5,7,9,11,13,15\}$

1. Hvorfor er 9 med i mængden, men ikke 12?
2. Ved en gruppes orden forstås antallet af elementer i gruppen. Hvad er ordenen af U_{16}?

I mængden defineres nu kompositionen x_{16} ved $a \,\mathrm{x}_{16}\, b = ab \text{ modulo } 16$, som eksempelvis giver $9 \,\mathrm{x}_{16}\, 11 = 99 \text{ modulo } 16 = 3$, da 16 går 6 gange op i 99 med 3 til rest.

3. Check et par af tallene i følgende kompositionstabel – og udfyld de manglende rubrikker.

x_{16}	**1**	**3**	**5**	**7**	**9**	**11**	**13**	**15**
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	-	-	-	7	1	11
7	7	5	-	-	-	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

Opgave C: Cykliske undergrupper og deres frembringere

1 Dan for hvert element i $(U_{16}, \mathrm{x}_{16})$ mængden $\{a, a^2, a^3, \ldots, a^p = e\}$ som består af alle potenser indtil gruppens neutral element e frembringes og mængden begynder at gentager sig. Eksempel på mængde $\{3, 9, 11, 1\}$ som er alle potenserne af 3.
   a. Observer at $3^4 = 1$, så ordenen af 3 er 4.
   b. Tjek om de mængder, du får frembragt, er undergrupper
   c. Er der et element som frembringer hele gruppen?
2 Hvorfor må det for ethvert element a i en endelig gruppe, gælde at der er en potens p som giver neutralelementet; $a^p = e$? Potensen p kaldes elementets orden.
3 Hvorfor udgør $\{a, a^2, a^3, \ldots, a^p = e\}$ en undergruppe? En gruppe kaldes **cyklisk**, hvis den har en frembringer – her er frembringeren åbenlyst a.

Video om cykliske grupper: https://www.youtube.com/watch?v=8A84sA1YuPw

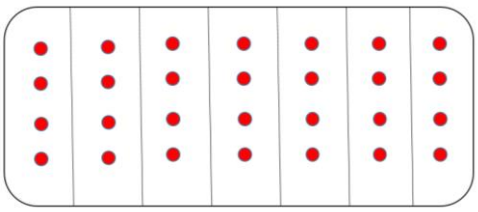
Opgave D: Sideklasser og klassedeling

Betragt talmængden $H = \{1,7\}$ og opfat den som en undergruppe af $(U_{16}, \mathrm{x}_{16})$.

1 Dan mængderne $aH = \{a \, \mathrm{x}_{16} \, 1, \; a \, \mathrm{x}_{16} \, 7\}$, hvor du systematisk lader a gennemløbe hele U_{16}.
   a. Hvor mange forskellige mængder får du?
2 De mængder du får frembragt kaldes **sideklasser** til H.
   a. Hvilke elementer er fælles for sideklasserne?
   b. Hvilken mængde danner sideklasserne tilsammen?
   c. Kan du illustrere a. og b. i et mængdediagram / Venn-diagram?
   d. Kan du skrive det med anvendelse af mængdetegnene fra opgave A?

3.2 Lagranges sætning

Hvis *H* er en undergruppe i en gruppe *G*,
så går ordenen af *H* op i ordenen af *G*



Denne tilsyneladende beskedne sætning har kolossal betydning, ikke mindst i krypteringsteori, hvor den danner hovedhjørnestenen i RSA-kryptering. Men Lagranges sætning er også et kraftigt redskab i gruppeteori, hvor den sætter begrænsninger på hvilke grupper, der findes. Hvis man fx har en gruppe med 10 elementer (orden 10), så nytter det ikke at lede efter undergrupper med 3 elementer (3 går jo ikke op i 10). Derimod kunne det godt tænkes, at der var en undergruppe med 2 eller 5 elementer (2 og 5 går op i 10). En anden umiddelbar konsekvens af Lagranges sætning er, at en gruppe der har et primtals antal elementer, ikke har andre undergruppe end de trivielle (nemlig gruppen selv og så $\{e\}$).

I dette afsnit vil vi nu bevise Lagranges sætning. Ideen i beviset er, at vi holder regnskab med antal og størrelse af sideklasserne til undergruppen.

Vi starter med et konkret tilfælde, hvor undergruppen har fire elementer.

Lad $(G,*)$ være en endelig gruppe med n elementer, dvs. af orden $|G| = n$.

I G betragter vi en undergruppe $(H,*)$ med $m = 4$ elementer, altså af orden $|H| = 4$, Så kan vi skrive $H = \{e, h_2, h_3, h_4\}$, hvor e, h_2, h_3, h_4 er forskellige elementer i H.

Vælg nu et element g i G og dan sideklassen

$$gH = \{g * e, g * h_2, g * h_3, g * h_4\} = \{g\ , g * h_2, g * h_3, g * h_4\}$$

Bemærk at g ligger i gH. Alle elementer i G ligger altså i en sideklasse til H.

Hjælpesætning 1: Sideklassen gH indeholder præcis lige så mange elementer som H.

Bevis: Vi viser det i tilfældet $m = 4$ som nævnt ovenfor. Beviset generaliseres let ☺

Der er tydeligvis ikke flere end 4 elementer i $gH = \{g\ , g * h_2, g * h_3, g * h_4\}$, og vi skal derfor bare vise at der heller ikke er færre end 4 elementer.

Modstridsbevis: vi antager at der er færre end 4 elementer og viser, at dette vil føre til en modstrid – hvoraf vi kan slutte at antagelsen er forkert – og så er der altså ikke færre end 4 elementer.

Hvis der er færre end 4 elementer, så må to af de fire på listen være ens. Det kunne fx være $g * h_2 = g * h_4$, hvor h_2 og h_4 er to forskellige elementer fra H. Komponér med g^{-1} fra venstre:

$$g^{-1}(g * h_2) = g^{-1}(g * h_4)$$
$$(g^{-1} * g) * h_2 = (g^{-1} * g) * h_4$$
$$e * h_2 = e * h_4$$
$$h_2 = h_4$$

Da vi gik ud fra at h_2 og h_4 var forskellige, er dette den ønskede modstrid. Og så er beviset for Hjælpesætning 1 slut ☺

Hjælpesætning 2: Ingen sideklasser overlapper med hinanden!

Vi viser nu, at fællesmængden mellem to sideklasser er tom, $g_1H \cap g_2H = \emptyset$, med mindre selvfølgelig de to sideklasser er ens. Beviset er føres generelt; det gælder også hvis der ikke er 4 elementer i H.

Bevis: Antag at der er et element a, der ligger i såvel g_1H som g_2H. Vi skal vise, at så er de to sideklasser ens.

Find først elementer h_i og h_j i H, således at

$$a = g_1 * h_i \qquad (1)$$

og også

$$a = g_2 * h_j \qquad (2)$$

Det kan vi, fordi a ligger både i g_1H og g_2H.

Tag nu et vilkårligt element b i sideklassen g_1H. Altså $b = g_1 * h_k$ for et passende valg af h_k i H. Hvis vi kan vise at b så også ligger i sideklassen g_2H, så betyder det at hele sideklassen g_1H ligger som en delmængde af g_2H. Og per symmetri må så også g_2H ligge inde i g_1H – og dermed er de to sideklasser ens, som ønsket.

For at vise at $b \in g_2H$ omskriver vi b med brug af ligningerne (1) og (2):

$$b = g_1 * h_k = \left(a * h_i^{-1}\right) * h_k = a * \left(h_i^{-1} * h_k\right) = \left(g_2 * h_j\right) * \left(h_i^{-1} * h_k\right) = g_2 * (h_j * h_i^{-1} * h_k)$$

Da H er en gruppe, vil $h_j * h_i^{-1} * h_j$ tilhøre H, og så har vi altså fået skrevet b som g_2 stjernet med et element fra H. Altså ligger g i g_2H. Og så har vi bevist Hjælpesætning 2 ☺

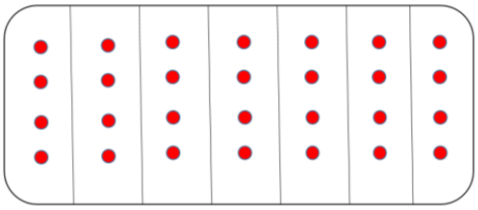
Nu er vi parat til at bevise Lagranges sætning: vi skal bare samle trådene!

For det første: hvert element i G ligger i en sideklasse til H.

For det andet: Ingen elementer fra G ligger i mere end én sideklasse til H (Hjælpesætning 2).

Altså udgør sideklasserne en såkaldt klassedeling af G. Det er lidt ligesom klasserne på en skole: alle elever er i en eller anden klasse, men ingen elever går i mere end én klasse. Derfor kan hele skolen opdeles klassevis.

Endelig – for det tredje – har vi i Hjælpesætning 1 set at alle sideklasserne har samme antal elementer, nemlig m, hvor m er ordenen af undergruppen H. Det ville svare til at alle klasser på skolen havde lige mange elever – så her bryder vores analogi sammen. Til gengæld kan vi lave en tegning af gruppen G på for eksempel denne måde:



Her ser vi, at G kan opdeles i 7 sideklasser, hver med 4 elementer. Det betyder, at der er $7 \cdot 4 = 28$ elementer i G, så G's orden er $|G| = 28$. Og da H's orden må være 4 i dette eksempel, så går tallet $|H|$ altså op i tallet $|G|$.

Mere generelt ville der på tegningen ovenfor være k klasser med hver $|H|$ elementer, så vi kan skrive $|G| = k \cdot |H|$. Da k er et helt tal, betyder det, at $|H|$ går op i $|G|$. Og så har vi bevist Lagranges sætning! ☺

Video om sideklasser og Lagranges sætning: *https://www.youtube.com/watch?v=TCcSZEL_3CQ&t=8s*

3.3 Konsekvenser af Lagranges sætning

Konsekvens 1: Hvis en gruppes orden er et primtal, har den ingen undergrupper (bortset selvfølgelig fra de to trivielle, nemlig $\{e\}$ og hele gruppen G).

Konsekvens 2: Hvis a er et vilkårligt element af en gruppe G, så vil der være et mindste heltal p for hvilket $a^p = e$. Dette tal p kaldes elementets orden, $|a| = p$. Det er let at se (?), at mængden $H = \{a, a^2, a^3, \dots, a^p\}$ er en undergruppe af orden $|H| = p$. Lagrange siger så, at ordenen af elementet a må være en divisor i hele gruppens orden: $|a|$ går op i $|G|$.

Konsekvens 3: Hvis a er et vilkårligt element i gruppen G, så vil $a^{|G|} = e$. Dette er (kommer vi til at se) et uhyre vigtigt resultat i forbindelse med RSA-kryptering. Det er nemt at bevise: hvis der er n elementer i G og G inddeles i k sideklasser til undergruppen $H = \{a, a^2, a^3, \dots, a^p\}$, hvor p er ordenen af elementet a, så er $|G| = k \cdot p$, og derfor er $a^{|G|} = a^{k \cdot p} = (a^p)^k = e^k = e$ ☺

Konsekvens 3 i detaljer

Sætning: Lad $(G, *)$ være en endelig gruppe med orden (antallet af elementer) $|G|$.

Så gælder der for ethvert element a i G, at a komponeret med sig selv $|G|$ gange giver gruppens neutral element; $a^{|G|} = e$

Bevis:

Vi tager et element a i G og danner mængden $H = \{a, a*a, a*a*a, \dots, a^k\}$ som nemmere kan skrives $\{a, a^2, a^3, \dots, a^k\}$, hvor vi antager at k er et tal som er 1 større end antallet af elementer i gruppen $(G,*)$. Siden antallet af opskrevne element i H er større end antallet af element i G, må nogle af dem være ens.

Lad os antage, at $a^n = a^m$ og at m er større end n, så vi kan skrive $m = n + p$. Vi har så $a^n = a^{n+p}$ som også kan skrive $a^n = a^n * a^p$. Herefter komponeres der ind fra venstre med det inverse element til a^n;

$(a^n)^{-1} * a^n = (a^n)^{-1} * a^n * a^p$ som giver $e = a^p$, hvor p højst er antallet af elementer i G.

Hvis vi fjerner dubletter fra Hstår vi tilbage med $H = \{a, a^2, a^3, \dots, a^p = e\}$, i det $a^{p+1} = a^p * a = e * a = a$, således at følgen af elementer begynder at gentage sig. p kaldes elementets orden.

At Hudgør en undergruppe er ikke så svært at vise:

- $a^n * a^m = a^{n+m \bmod p}$, hvilket er a komponeret med sig selv færre end p gange, så det er med i H og dermed er * lukket i H.
- Neutralelementet er oplagt med i H.
- Antag at $i + j = p$ så gælder identiteten: $e = a^p = a^i * a^j$, som viser at $(a^i)^{-1} = a^j$og j er mindre en p. Altså har ethvert element i H et inverst element som også ligger i H.
- Den associative regel gælder for alle elementerne i G og derfor også i H, som jo er en delmængde af G.

Så $(H,*)$ er en undergruppe i $(G,*)$. Man siger at $(H,*)$ er en cyklisk gruppe frembragt af a. Vi ved så fra Lagrange sætning at ordenen af H - dvs. p – går op i $|G|$; så $|G| = tp$, og dermed følger:

$$a^{|G|} = a^{tp} = (a^p)^t = e^t = e$$

QED.

4. RSA-kryptering forklaret ved hjælp af gruppeteori

To videoer om RSA-kryptering:

- James Grime: *https://www.youtube.com/watch?v=M7kEpw1tn50*
- Grundig gennemgang: *https://www.youtube.com/watch?v=wXB-V_Keiu8&t=820s*

4.0: Før start

4.0.1 Matematiske forudsætninger

- Diverse regler for modulo/restklasse beregninger.
- I en endelig gruppe G af orden n gælder $x^n = e$. Kan også skrives $x^{|G|} = e$.
- (U_n, X_n) er en gruppe. Her betegner U_n mængden af positive heltal mindre end n, som er primiske med n, og X_n er multiplikation modulo n. At vise at det virkelig er en gruppe kan klares vha. side 27-29 (Theorem 1.4) og side 39 fra [Judson] og side 82 sætning 4.19 fra [Landrock og Nissen].
- For at vise, at (U_n, x_n) er en gruppe: Eksistens af e giver sig selv. De følgende 3 henvisninger viser, at U_n er stabil, og at ethvert element har et inverst: [Judson] side 28-29 sætning 1.4 + korollar 1.5. og side 39 sætning 2.1 stk. 6. [Landrock] side 82 sætning 4.19 (der ved en fejl refererer til sætning 4.17 i stedet for 4.18 på side 81). Den associative egenskab følger af [Landrock] side 73 sætning 4.7 stk. 2. Det er i denne udledning en forudsætning at meddelelsen x er primisk med n. Hvis det ikke er tilfældet er man nødt til at undersøge, om RSA-systemet stadig fungerer. Det gør det, og det vises i appendiks 4 i Landrock. Det er også et problem i den almindelige talteoretiske fremstilling af RSA.

4.0.2 Nyttige links til RSA

1. Bestemmelse af primtal: https://www.browserling.com/tools/prime-numbers
2. Bestemmelse af "co-primes": http://codinglab.huostravelblog.com/math/coprime-finder/index.php
3. Bestemmelse af invers: https://planetcalc.com/3311/
4. Modulo beregning: https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

4.1. Sådan fungerer RSA: kryptering og dekryptering

4.1.1 Trin 1 af 3 – vælg to store primtal

Tag to primtal p og q (link 1) og dan deres produkt $n = p \cdot q$. Vi ser nu på gruppen (U_n, x_n), dvs. gruppen bestående af positive hele tal som er mellem 1 og n og som er primiske med n, udstyret med kompositionen gange modulo n. To tal kaldes **primiske**, hvis deres største fælles divisor er 1.

Antallet af tal mellem 1 og n som er primiske med n kaldes **Eulers φ-funktion**.

Eksempel på beregning af $\varphi(n)$

Sæt $p = 3$ og $q = 5$, så er $n = 15$. Og så er $\varphi(15) = 8$. Det ses i den følgende række af hele tal mindre end 15, hvor vi har fremhævet de 8 tal som er primiske med 15 med **fed** skrift:

$$\{\mathbf{1}, \mathbf{2}, 3, \mathbf{4}, 5, 6, \mathbf{7}, \mathbf{8}, 9, 10, \mathbf{11}, 12, \mathbf{13}, \mathbf{14}\}.$$

Eksempelvis er 8 primisk med 15, fordi divisorerne i 8 er 1,2,4,8 og i 15 er det 1,3,5,15 – den største fælles divisor er 1.

Men vi kan også tælle os frem til værdien af tallet $\varphi(15)$ ud fra listen på en anden måde. Vi ser nemlig, at de tal som ikke er primiske med 15 er $3 \cdot 1$, $3 \cdot 2$, $3 \cdot 3$, $3 \cdot 4$ og $5 \cdot 1$, $5 \cdot 2$. Vi skal altså fra listen med 14 tal fjerne

først 4 tal som har fælles divisor 3 med 15 (nemlig $3, 6, 9, 12$) og derefter yderligere 2 tal som har fælles divisor 5 med 15 (nemlig $(5, 10)$. Det giver $\varphi(15) = 14 - 6 - 2 = 8 = (3-1)(5-1)$. Vi bemærker, at det kan skrives $\varphi(n) = (p-1)(q-1)$. Vi beviser nu denne generelle formel for Eulers φ-funktion.

Sætning om Eulers φ-funktion

Eulers φ-funktion kan beregnes som $\varphi(n) = (p-1)(q-1)$.

Bevis:

I det generelle tilfælde skal man fra listen $\{1, 2, 3, \dots, p \cdot q - 1\}$ først fjerne tallene $p, 2p, 3p, \dots, (q-1)p$ da de vil have fælles divisor p. Det er $q-1$ tal. Dernæst skal man fjerne tallene $q, 2q, 3q, \dots, (p-1)q$. Det er $p-1$ tal.

Antal af tilbageværende tal vil så være $(pq-1) - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1)$

Og så skal man selvfølgelig lige overveje, at der ikke er andre tal der ikke er primiske med p, som også skulle have været fjernet.

4.1.2 Trin 2 af 3 – Dan en *offentlig* og en *privat* nøgle

Nu danner vi gruppen $\left(U_{\varphi(n)}, \mathrm{x}_{\varphi(n)}\right)$, som består af tallene der er primiske med $\varphi(n)$ med kompositionen gange modulo $\varphi(n)$.

I $U_{\varphi(n)}$ vælger man et tal E (i praksis skal man altså finde et tal som er primisk med $\varphi(n)$ – brug link 2).

Dernæst finder man det tal D der er det inverse element til E i gruppen $\left(U_{\varphi(n)}, \mathrm{x}_{\varphi(n)}\right)$. Det kan gøres ved hjælp af Euklids algoritme (link 3).

Så har man altså at $DE = 1 \bmod \varphi(n)$, hvilket betyder at DE giver resten 1 efter divison med $\varphi(n)$ eller at $DE = k \cdot \varphi(n) + 1$, hvor k er et eller andet helt tal.

Man deler nu tallene n, E og D op i to såkaldte "nøgler":

- en **offentlig** nøgle, som ligger frit tilgængelig, og som alle kan bruge til at kryptere en besked med. Det er nøglen (n, E).
- en **privat** nøgle, som modtageren kan brug til at dekryptere beskeden. Det er nøglen (n, D),

Eksempel på nøgledannelse

Vi vælger de to primtal 23 og 29. Så er $n = 23 \cdot 29 = 667$ og $\varphi(667) = (23-1)(29-1) = 616$ og $\left(U_{\varphi(n)}, \mathrm{x}_{\varphi(n)}\right) = (U_{616}, \mathrm{x}_{616})$.

Et tal som er primisk med 616 er f.eks. 487 (i nSpire kan man prøve $\gcd(616{,}487)$, som giver den største fælles divisor, som i dette tilfælde er 1).

Det inverse element til $E = 487$ i $(U_{616}, \mathrm{x}_{616})$ kan bestemmes til $D = 191$ ved hjælp af Euklids algoritme, så $487 \cdot 191 = 1 \bmod 616$.

Bob offentliggør den ene nøgle $(n, E) = (667, 487)$ og holder den anden nøgle $(n, D) = (667, 191)$ hemmelig.

4.1.3 Trin 3 af 3 – kryptering og dekryptering

Krypteringen

Alice vil sende beskeden (tallet) x til Bob. Hun slår Bobs offentlige nøgle $(n, E) = (667{,}487)$ op og beregner tallet $y = x^E \bmod n = x^{487} \bmod 667$, som hun derefter sender til Bob (benyt link 4).

Dekrypteringen

Bob (og alle andre som lytter med…) har modtaget beskeden y, som han nu underkaster følgende beregning:

$y^D \bmod n = y^{191} \bmod 667$ – og det resulterer magisk nok x ! Bob har dekrypteret Alices besked.

Hvorfor virker Bobs dekryptering?

Vi antager, at beskeden x er primisk med n. Tallet x er altså et element i gruppen (U_n , X_n). Denne gruppe har orden $\varphi(n)$. Dvs:

$$
\begin{aligned}
& y^D \bmod n = (x^E)^D \bmod n \\
& = x^{DE} \bmod n \\
& = x^{k\cdot\varphi(n)+1} \bmod n \\
& = \left(x^{\varphi(n)}\right)^k \cdot x \bmod n \\
& = 1^k \, x \bmod n \\
& = x \bmod n = x \ \text{☺}
\end{aligned}
$$

For at dette skal virke, skal x være mindre end n, ellers vil $x \bmod n$ ikke give x. Det væsentlige skridt i beregningen er at $x^{\varphi(n)} = 1 \bmod n$ – altså at et element i gruppen (U_n , X_n) opløftet i gruppens orden giver neutral elementet – en konsekvens af Lagranges sætning.

Eksempel med bogstavbesked

Alice vil nu sende beskeden bestående af det ene bogstav "x" til Bob. Bogstavet "x" har nummer 23 i det engelske alfabet (hvor "a" tælles som nr. 0). Bobs offentlige nøgle er $(n, E) = (667 , 487)$, så Alice beregner

$$23^{487} \bmod 667 = 368$$

Online modulus-beregner: https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

Bob finder sin hemmelige nøgle frem $(n, D) = (667, 191)$ og beregner:

$$368^{191} \bmod 667 = 23$$

og oversætter bogstav nr. 23 til det "x", som Alice har villet sende.

4.2. Er systemet sikkert?

Alle kender systemet og ved, at n er fremstillet ved at to primtal er ganget sammen. En primtalsfaktorisering af n er entydig – dvs. der findes kun de samme to primtal som ganget sammen giver n. Så hvis man har mod på det, kan man bryde koden ved at finde ud af, hvilke to primtal Alice har brugt. Og så kan man ved hjælp af hendes offentlige nøgle (n, E) finde hendes hemmelige nøgle (n, D). Men hvis de to primtal er valgt store nok, er det en arbejdsopgave, som – selv om den teoretisk set kan løses – er umulig at komme igennem inden for noget der minder om rimelig tid.

En anden ting man skal holde sig for øje, er at de samme meddelelsers tal altid krypteres på samme måde. Derfor kan man ikke nøjes med at sende teksten i små bidder – for så kan den onde Eve bare fremstille en ordbog over de mulige beskeder Bob kan få.

4.3. Opgaver i RSA-kryptering

Der er tre aktører som vil kommunikere: Rødhætte, Bedstemor og Ulven

Rødhætte:

Har valgt $p = 3499$, $q = 7937$, så $n = pq = 27771563$ og $\varphi(n) = (p-1)(q-1) = 27760128$.

$E = 27760133$ og $D = 16656077$.

Det vil sige at Rødhættes nøgler er:

Offentlig: $(n, E) = (27771563, 27760133)$

Privat: $(n, D) = (27771563, 16656077)$

Bedstemor:

Har valgt $p = 3137$, $q = 6899$ så $n = pq = 21642163$ og $\varphi(n) = (p-1)(q-1) = 21632128$

$E = 21632125$ og $D = 7210709$.

Det vil sige at Bedstemors nøgler er:

Offentlig: $(n, E) = (21642163\ , 21632125)$

Privat: $(n, D) = (21642163\ , 7210709)$

Ulven:

Har valgt $p = 4547$, $q = 6229$ så $n = pq = 28323263$ og $\varphi(n) = (p-1)(q-1) = 28312488$.

$E = 28312483$ og $D = 11324995$

Det vil sige at Ulvens nøgler er:

Offentlig: $(n, E) = (28323263, 28312483)$

Privat: $(n, D) = (28323263, 11324995)$

Det engelske alfabet bruges:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Rødhætte vil gerne besøge bedstemor, så hun sender forespørgslen:

MAY I COME	hvor hun først fjerner mellemrum
MAYICOME	og derefter oversætter til tal i blokke af to bogstaver.
MA YI CO ME	som bliver til
1301 2509 0315 1305	

Så benytter Rødhætte bedstemors offentlige nøgle til at fremstille den hemmelige besked som hun sender over den åbne kanal, som konstant overvåges af Ulven. De første to bogstaver giver

$$1301^{21632125} \bmod 21642163 = 6645729$$

Opgave 1

Brug online-beregneren www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html til at vise at bedstemor modtager de fire tal:

6645729 7101931 7411929 6188075

Opgave 2

Senere på dagen modtager Rødhætte beskeden som Bedstemor har kodet med Rødhættes offentlige nøgle:

20305389 10346414 16352605 2670413 22363095

Rødhætte går i gang med at dekryptere, med sin private nøgle: $(n, D) = (27771563, 16656077)$

Hvad står der? (Hint: hvis man møder et 3-cifret tal, skal man selv sætte et foranstillet 0 ind).

Rødhætte har nu et problem: Hun ved ikke, om det er Ulven, der har opsnappet beskeden, og nu sender en falsk invitation – eller om det faktisk er Bedstemor? Så Rødhætte beder Bedstemor sende en besked, som kun Bedstemor kan sende. Bedstemor tager derfor sin private nøgle og krypterer med den – det kan kun hun. Herefter krypterer hun resultatet af denne første kryptering med Rødhættes offentlige nøgle, og sender den dobbeltkrypterede besked afsted. Lad os vise det i detaljer:

Bedstemor tager sin besked "do…" og oversætter til blokke af tal:

do… = 0415 tal tal tal tal.

Det første af disse tal 0415 (som svarer til "do") bliver med Bedstes private nøgle til 14308158. Beskeden bliver altså omformet til

14308158 tal tal tal tal.

Disse tal krypterer Bedstemor nu med Rødhættes offentlige nøgle og får:

21150759 tal tal tal tal

- Bestem de manglende tal i eksemplet ovenfor!

Opgave 3

Rødhætte modtager nu følgende i sin inbox:

21150759 11935825 9569951 7482653 21375328

Hvordan verificerer Rødhætte, at det faktisk er fra Bedstemor – og hvad står der?

Hun dekrypterer først med sin egen private nøgle – det giver noget volapyk – og derefter låser hun volapykken op med Bedstemors offentlige nøgle – går det godt, er det fordi beskeden er blevet krypteret med Bedstemors private nøgle inden den blev sendt til Rødhætte. Og så er Rødhætte sikker på, at beskeden kom fra Bedstemor.

I detaljer: Ved dekryptering med Rødhættes private nøgle fås:

14308158 tal tal tal tal

Og så låser Rødhætte op med Bedstemors offentlige nøgle! Det første tal (14308158) bliver til 415, som Rødhætte sætter et manglende 0 foran. Så står der 0415, hvilket betyder "do".

- Prøv at finde ud af hvad (den rigtige?) Bedstemor har skrevet til Rødhætte!

Litteraturliste

Judson, Thomas W., *Abstract Algebra – Theory and Applications,* PWS Publishing Company, 1984.

Landrock og Nissen, *Kryptologi – fra viden til videnskab,* Abacus 1997.

Hele playlisten fra ”Socratica” anbefales. Specielt:

- https://www.youtube.com/playlist?list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6
- https://www.youtube.com/watch?v=TCcSZEL_3CQ Video hvor Socratica gennemgår beviset for Lagranges Sætning