

## Note 1

Endelig har jeg fået mig taget sammen til at nedskrive endnu nogle få vise ord. Siden sidst er mangt og megen algebra blevet introduceret, og denne notes formål er at opsummere den megen lærdom. Jeg beklager den noget besynderlige strukturering af noten (eller nok rettere mangel på samme); jeg håber at få tid til at skrive noget mere forståeligt i løbet af efterårsferien.

### 1.1 Talteori

Kapitel 1 i lærebogen handler om de hele tal og deres egenskaber, herunder især primtallene og deres mange anvendelser. Som det efterhånden nok er gået op for de fleste er et vigtigt begreb “(parvis) indbyrdes primisk”. Det er en god ting at bemærke sig hvad der adskiller primtallene fra de sammensatte tal (altså ikke blot den definerende egenskab at de ikke har andre divisorer end 1 og sig selv). Den kinesiske restklassesætning er også tit anvendelig.

### 1.2 Grupper

I kapitel 2 bliver tingene mere abstrakte. Det er nok en god ide at repetere de fundamentale definitioner (gruppe, undergruppe, normal, sideklasse, homomorfi, cyklisk etc.) for sig selv indtil man kan dem udenad; på den måde bliver det mere naturligt at arbejde med de abstrakte begreber.

En undergruppe er en gruppe i sig selv. Fx er  $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$  et voksende hierarki af grupper (mht. +), men vi kan også opfatte hver enkelt mængde som en gruppe i sig selv (stadig mht. +).

Normale undergrupper fortjener et par ord med på vejen. Som skrevet bør man kunne definitionen af en undergruppe  $H$  af en gruppe  $G$  kaldes normal i  $G$ ; altså at  $gHg^{-1} = H$  for ethvert  $g \in G$ . Opgave II.13 viser (næsten) at denne definition er ækvivalent til at kræve  $gH = Hg$  for ethvert  $g \in G$ . Opgave II.14 fortæller at hvis gruppen  $G$  er abelsk, er enhver undergruppe automatisk normal.

Det pædagogiske formål med II.17 er at vise, at selvom alle undergrupper er normale, er gruppen ikke nødvendigvis abelsk.

En ting at bemærke om normalitet er at det er et *relativt* begreb. Først lidt notation: Hvis  $H$  er en normal undergruppe af gruppen  $G$ , skriver man nogle gange  $H \triangleleft G$ ; dette betyder altså dels at  $H$  er en undergruppe af  $G$ , dels at den er normal i  $G$ . Antag nu at  $H \triangleleft G$  og  $K \triangleleft H$ ; så er  $K$  også klart en undergruppe af  $G$ . Er den normal i  $G$ ? Svaret er nej (eller rettere sagt: svaret er “ikke nødvendigvis”). I har i en afleveringsopgave arbejdet med en gruppe som giver et glimrende modeksempel, nemlig gruppen  $D_4$  (rotationer

og spejlinger i  $\mathbb{R}^2$  som afbilder et kvadrat til sig selv). Lad nemlig  $H = \{\text{Id}, S_x, S_y, R_\pi\}$  være undergruppen bestående af identiteten, spejlingerne i henholdsvis  $x$ - og  $y$ -akserne og rotation på  $\pi$  (kontrollér selv at det rent faktisk er en undergruppe af  $D_4$ ). Pr. opgave II.15(iii) er  $H$  normal i  $D_4$ , da den har index 2. Lad nu  $K = \{\text{Id}, S_x\}$  være undergruppen af  $H$  bestående af identiteten og spejlingen i  $x$ -aksen. Samme argument giver, at  $K$  er normal i  $H$ . At  $K$  *ikke* er normal i  $G$  kan I selv overbevise jer om (prøv fx at se om  $S_d K S_d^{-1} = K$  hvor  $S_d$  er en spejling i en af diagonalerne).

Dette viser, at normalitet ikke (nødvendigvis) er transitiv, så  $\triangleleft$  er ikke (nødvendigvis) en partiel ordning på undergrupperne af en gruppe  $G$ .

Hvis  $N \triangleleft G$  kan vi gøre mængden af venstre sideklasser  $G/N$  til en gruppe; det er hvad der sker på side 63. Dette giver anledning til det vigtige begreb *kvotientgruppe*. Når man har en kvotientgruppe  $G/N$  har man også en afbildning  $\pi: G \rightarrow G/N$  som til et element  $g \in G$  knytter sideklassen  $gN$  (se Example 2.4.4). Dette er en gruppehomomorfi, og den er så vigtig at den kaldes den *kanoniske gruppehomomorfi* (eller den kanoniske projektion; deraf  $\pi$ ). Bemærk at  $\pi$  altid vil være surjektiv.

En sidste bemærkning om normale undergrupper: Hvis  $G$  er en vilkårlig gruppe og  $e$  betegner neutralelementet deri, er  $\{e\}$  og  $G$  klart normale undergrupper af  $G$ . Hvis det er de  *eneste* normale undergrupper, kaldes  $G$  *simpel*.

En (gruppe)homomorfi spiller samme rolle inden for gruppeteori som lineære afbildninger gør i vektorrumsteori. En lineær afbildning  $f: V \rightarrow W$  er en afbildning som bevarer vektorrumstrukturen; i den forstand at  $f(x+y) = f(x) + f(y)$  og  $f(\lambda x) = \lambda f(x)$  for alle  $x, y \in V$  og alle  $\lambda \in \mathbb{F}$  (hvor  $\mathbb{F}$  er det legeme som  $V$  og  $W$  nu engang er vektorrum over; som oftest  $\mathbb{R}$  eller  $\mathbb{C}$ ). På tilsvarende vis er en gruppehomomorfi  $f: G \rightarrow H$  en funktion som respekterer gruppestrukturen; altså at  $f(xy) = f(x)f(y)$  for alle  $x, y \in G$ , hvor  $xy$  naturligvis betyder sammensætningen af  $x$  og  $y$  i  $G$ , mens  $f(x)f(y)$  betyder sammensætningen af elementerne  $f(x)$  og  $f(y)$  i  $H$ . En bijektiv (gruppe)homomorfi kaldes en (gruppe)isomorfi. Ligesom man kan snakke om isomorfe vektorrum kan man snakke om isomorfe grupper; to grupper  $G$  og  $H$  kaldes isomorfe hvis der findes en gruppeisomorfi  $G \xrightarrow{\sim} H$ . Isomorfisætningen (se §2.5) er i denne sammenhæng ret vigtig; den kan ofte hjælpe til at få en bedre forståelse af en given kvotientgruppe.

Ordet “order” (orden på dansk) bruges i to forskellige sammenhænge. Dels tales der om ordenen af en gruppe; det er simpelthen antallet af elementer i gruppen (og kan altså være et helt positivt tal, eller eventuelt  $\infty$ ). Men det giver også mening at snakke om ordenen af et element  $g$  i en gruppe; med dette mener man antallet af elementer i (under)gruppen  $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$  frembragt af  $g$ , og dette kan altså ligeledes være  $1, 2, \dots$  eller  $\infty$ . Man kan også tænke på  $\text{ord}(g)$  som det mindste positive antal gange man

skal sammensætte  $g$  med sig selv for at få neutralelementet  $e$ ; altså  $\text{ord}(g) = \min\{n \in \mathbb{N}_+ \mid g^n = e\}$  med konventionen  $\min \emptyset = \infty$  (hvis  $g^n$  aldrig bliver  $e$  for positive  $n$ , sætter vi  $g$ 's orden til  $\infty$ ).

Proposition 2.7.4 og de indledende knæbøjninger øverst side 71 fortæller stort set alt hvad der er værd at vide om cykliske grupper. Bemærk at  $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ .

Den kinesiske restklassesætning bliver bevist (igen) i §2.8.3; denne gang i dens rette abstrakte kontekst. Det er en god ide at forsøge at forstå indholdet af denne sætning, og hvorfor der er de krav til  $n_i$ 'erne som der nu engang er.

Begrebet *gruppevirkning* er et af de vigtigste begreber overhovedet. I Algebra 1 anvendes konceptet ikke til meget andet end beviser for Burnside's formel og Sylows sætninger, men senere vil I støde på det igen og igen. Sylows sætninger er utrolig stærke når emnet er endelige grupper, og mange problemer løser næsten sig selv ved en simpel anvendelse af Sylow I–III.

### 1.3 Løst og fast fra opgaver

Som nævnt et par gange er resultatet fra opgave II.15(iii) yderst anvendeligt i mange situationer. Blandt andre opgaver i kapitel som jeg anser for vigtige er 4, 5, 12, 13, 20, 25, 26, 29, 40, 48, 53, 54 samt 56. HOF-opgaven 57 er en udmærket udfordring, som ikke er uoverkommelig.

## 1.4 Ordbog

En længe tiltrængt fornyelse af ordbogen er lige her:

Engelsk	Dansk
group	gruppe
composition	sammensætning eller komposition
abelian	abelsk
order (of a group)	orden (af en gruppe)
composition table	kompositionstabel
subgroup	undergruppe
coset	sideklasse
index	indeks
normal	normal
quotient group	kvotientgruppe
residue class	restklasse
group homomorphism	gruppethomomorfi
group isomorphism	gruppetisomorfi
order (of an element)	orden (af et element)
cyclic	cyklisk
generator	frembringer
product group	produktgruppe
canonical	kanonisk
symmetric group	symmetrisk gruppe
alternating group	alternerende gruppe
cycle	cykel
group action	gruppetvirkning
orbit	bane
stabilizer	stabilisator
conjugation	konjugering
conjugacy class	konjugeringsklasse

Nu begynder forelæsningerne snart at handle om ringe, og for at I ikke skal gå dette ganske uforberedt i møde er her en oversigt over nogle af de vigtigste termer i ringteorien:

Engelsk	Dansk
ring	ring
subring	delring (bemærk: <i>ikke</i> underring)
zero divisor	nuldivisor
unit	enhed
field	legeme
subfield	dellegeme
extension field	udvidelseslegeme
domain	domæne eller integritetsområde
(the) Gaussian integers	(de) Gaussiske heltal
ideal	ideal
principal ideal	hovedideal
principal ideal domain [PID]	hovedidealområde
quotient ring	kvotientring
prime ideal	primideal
maximal ideal	maksimalt ideal
ring homomorphism	ringhomomorfi
characteristic	karakteristik
Freshman's Dream	“russens drøm”
field of fractions	brøklegame

## 1.5 Matematisk rodekasse

I kapitlet om grupper (og formentlig også tidligere i jeres karriere) er I stødt på forskellige grupper med mere eller mindre standardiserede navne og betegnelser. Her er en oversigt over nogle af de vigtigste:

### Betegnelse Definition

$GL_n(\mathbb{F})$   $\{A \in \text{Mat}_n(\mathbb{F}) \mid \det A \neq 0\}$

$SL_n(\mathbb{F})$   $\{A \in \text{Mat}_n(\mathbb{F}) \mid \det A = 1\}$

$O_n(\mathbb{F})$   $\{A \in \text{Mat}_n(\mathbb{F}) \mid AA^T = I\}$

$SO_n(\mathbb{F})$   $SL_n(\mathbb{F}) \cap O_n(\mathbb{F})$

$D_n$  Gruppen af rotationer og spejlinger som bevarer en regulær  $n$ -kant.

$S_n$  Gruppen af bijektive afbildninger  $M \rightarrow M$  af en mængde  $M$  med  $n$  elementer til sig selv.

$A_n$  Gruppen af lige permutationer i  $S_n$ .

$\mathbb{Z}_n$  Dette er blot en lidt kortere skrivemåde for  $\mathbb{Z}/n\mathbb{Z}$ .

$\langle g \rangle$  Undergruppen  $\{g^n \mid n \in \mathbb{Z}\} \subseteq G$  frembragt af elementet  $g \in G$

Her betegner  $\mathbb{F}$  et vilkårligt legeme (som fx  $\mathbb{R}$  eller  $\mathbb{C}$ ), og  $\text{Mat}_n(\mathbb{F})$  er mængden af alle  $n \times n$ -matricer hvis indgange stammer fra det pågældende legeme.

Bemærk at definitionen af determinant af en matrix (som I kender fra Mat10) giver mening for matricer over et hvilket som helst legeme; determinanten bliver altså bare et element i det pågældende legeme. Bemærk yderligere, at i et legeme har vi altid et 0-element (neutralt element for addition) og et 1-element (neutralt element for multiplikation), så definitionerne af  $GL_n$  og  $SL_n$  er faktisk meningsfulde.