

Note 2

Nu er to vigtige datoer endelig lagt fast. Der er tale om *fredag den 12/12-03* hvor instruktørøppet vil flyde i rigelige mængder i Matematisk Fredagsbar (fra ca. kl. 15), og *fredag den 16/1-03*, hvor I vil blive udsat for en lille test. Hvornår spørgetime(r) og deslige lægges er endnu ikke fastsat.

Hængepartier fra kapitel 2

Jeg lovede at formalisere en lille “sætning” jeg viste til TØ. Jeg har her valgt at splitte den op i to. Inden da vil jeg dog appellere til, at I husker på, at sætninger kun gælder under de forudsætninger som de gælder under. Det er muligvis trivielt, men det nytter altså ikke noget at referere til en sætning der starter “Lad G være en endelig gruppe” hvis den gruppe der arbejdes med ikke er endelig. Læs derfor sætningerne grundigt, og ikke kun konklusionerne i sætningerne.

Lemma 1. Lad G være en gruppe, og lad $H \subseteq G$ være en undergruppe. Lad $g \in G$ være et vilkårligt element. Så er mængden

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq G$$

en undergruppe af G .

Bevis. For at tjekke at en given delmængde er en undergruppe, er der tre ting at tjekke. For det første skal mængden være lukket under kompositionen fra gruppen, så lad x og y være to elementer i gHg^{-1} . Det betyder, at x og y kan skrives som $x = gh_1g^{-1}$ og $y = gh_2g^{-1}$. Men så er $xy = (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1}$ pga. associativitet. Da H er antaget at være en undergruppe af G , er h_1h_2 et element i H , og dermed er xy et element i gHg^{-1} .

Derudover skal neutralelementet ligge i mængden. Men da $e \in H$ har vi $e = geg^{-1} \in gHg^{-1}$.

Endelig skal det for ethvert $x \in gHg^{-1}$ gælde, at det inverse element til x tilhører gHg^{-1} . Dette er netop tilfældet, for hvis $x = ghg^{-1}$ er det ikke svært at indse, at $x^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$, da jo $h^{-1} \in H$. Dette færdiggør beviset. \square

Husk på, at hvis g er et element i en gruppe G , og h er et andet element i G , kaldes konstruktionen ghg^{-1} for *konjugering* af h med g . Man kan, som det fremgår ovenfor, naturligvis også konjugere delmængder. Ovenstående lemma kan således også formuleres som at “konjugering af en undergruppe med et element fra gruppen giver igen en undergruppe”. Hvis vi fortsætter ud ad denne tangent kan vi bruge dette til at definere en gruppevirkning. Lad $\mathcal{U}(G)$

betegne mængden af undergrupper af G . Så er afbildningen $\alpha: G \times \mathcal{U}(G) \rightarrow \mathcal{U}(G)$ defineret ved

$$\alpha(g, H) = gHg^{-1}$$

faktisk en gruppevirkning (tjek selv at aksiomerne er opfyldt). En smule eftertanke viser, at fixpunkterne for denne gruppevirkning lige præcis er de normale undergrupper i G .

Nuvel, det var et sidespring. Det næste lemma er det vi egentlig brugte til TØ:

Lemma 2. Lad G være en endelig gruppe af orden N , og lad d være en divisor i N . Hvis der findes *netop* en undergruppe $H \subseteq G$ af orden d , så er denne undergruppe normal i G .

Bevis. Vi skal vise, at H er normal. Pr. definition betyder det, at vi skal vise, at $gHg^{-1} = H$ for ethvert $g \in G$. For et givet $g \in G$ ved vi fra Lemma 1, at gHg^{-1} i hvert fald er en undergruppe af G . Men ydermere må der gælde, at ordenen (dvs. antallet af elementer deri) af denne undergruppe er d ; thi vi har en bijektiv afbildning fra H til gHg^{-1} givet ved $h \mapsto ghg^{-1}$ (find selv den inverse afbildning). Altså er gHg^{-1} en undergruppe af G af orden d . Pr. antagelse var der kun én sådan, så vi må have $gHg^{-1} = H$ for ethvert $g \in G$; altså er H en normal undergruppe af G . \square

Bemærk at dette giver endnu en metode til at vise normalitet af en undergruppe, og det var præcis det vi brugte i opgave II.45: Vi skal vise, at A_4 ikke er simpel; mao. skal vi vise der findes en normal undergruppe (som ikke er $\{e\}$ eller hele gruppen). Ovenikøbet får vi givet en god kandidat, nemlig delmængden H bestående af e og alle elementer af orden 2. Man finder ret hurtigt ud af, at H er en undergruppe, og at den har orden 4. For at kunne bruge ovenstående lemma skal vi blot overbevise os om, at H er den *eneste* undergruppe af A_4 med 4 elementer. Men da de øvrige 8 elementer i A_4 alle er 3-cykler (det ved vi fra en aflevering), og da 3-cykler har orden 3, kan vi ikke have en undergruppe med 4 elementer hvori der ligger en 3-cykel (husk på, at et elements orden går op i gruppens orden!). Derfor er en undergruppe af A_4 med 4 elementer pisket til at være H . Ergo er H normal i A_4 .

En anden ting der skulle vises i selvsamme opgave var, at A_3 er simpel. Den klart nemmeste måde at vise dette på er ved at appellere til Lagranges indexsætning. Thi hvis G er en endelig gruppe med p elementer, hvor p er et primtal, er G simpel. Dette skyldes det simple faktum, at hvis $H \subseteq G$ er en undergruppe, må H enten have 1 eller p elementer. Ergo er H enten $\{e\}$ eller G , og der kan derfor ikke findes (ikke-trivielle) normale undergrupper i G . Da $|A_3| = 3!/2 = 3$ er et primtal, er A_3 simpel.

En metode til at finde antallet af undergrupper af en given orden er Sylows sætninger; specielt Sylow-III. For eksempel i opgave II.52 viste det sig, at der i en gruppe med 15 elementer er netop en undergruppe med 3 elementer og netop en undergruppe med 5 elementer; og pr. ovenstående er disse derfor normale.

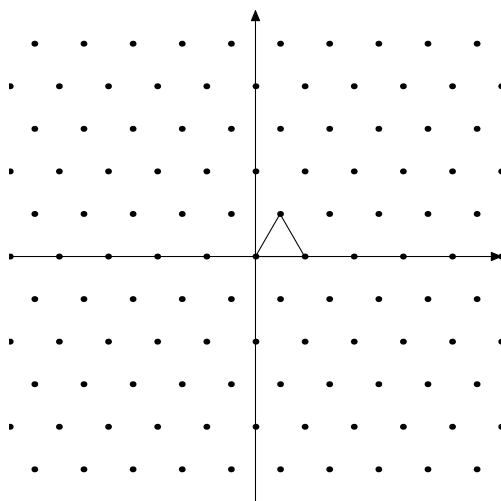
Kapitel 3

Jeg skylder en bedre gennemgang af afleveringsopgaven III.30. Den er her:

- (i) Observer først, at da ω er løsning til $x^2 + x + 1 = 0$, må $\bar{\omega}$ også være det (komplekse løsninger til polynomiumsligninger med reelle koefficienter optræder i konjugerede par). Desuden har vi, at produktet af de to rødder i et andengradspolynomium er konstantleddet, og summen er koefficienten til x med modsat fortegn; altså $\omega\bar{\omega} = 1$ og $\omega + \bar{\omega} = -1$. Vi har så $N(z) = z\bar{z} = (x + y\omega)(\overline{x + y\omega}) = (x + y\omega)(x + y\bar{\omega}) = x^2 + y^2\omega\bar{\omega} + xy(\omega + \bar{\omega}) = x^2 - xy + y^2$. Desuden følger $N(z_1z_2) = N(z_1)N(z_2)$ trivielt, da dette jo er sandt for alle komplekse tal z_1, z_2 ; men det kan også let udregnes: $N(z_1z_2) = z_1z_2\overline{z_1z_2} = z_1\bar{z}_1z_2\bar{z}_2 = N(z_1)N(z_2)$.

Antag $z \in \mathbb{Z}[\omega]$ er en enhed. Det betyder, at der findes $w \in \mathbb{Z}[\omega]$ så $zw = 1$. Så er $N(z)N(w) = N(1) = 1$, og da $N(z)$ er et naturligt tal, må vi have $N(z) = N(w) = 1$. Antag omvendt, at $N(z) = 1$. Da $N(z) = z\bar{z}$ ser vi, at z er en enhed såfremt vi blot kan vise, at $\bar{z} \in \mathbb{Z}[\omega]$. Men da jo $\bar{z} = x + y\bar{\omega} = x + y(-1 - \omega) = x - y - y\omega$ ser vi at $\bar{z} \in \mathbb{Z}[\omega]$.

- (ii) Antag $N(z)$ er et primtal, og lad $z = ab$. Så er $N(z) = N(a)N(b)$; da $N(z)$ er et primtal, må en af $N(a)$ og $N(b)$ være 1; pr. (i) har vi så, at enten a eller b er en enhed, og derfor er z irreducibel.
- (iii) Vi skal vise, at $\mathbb{Z}[\omega]$ er en Euklidisk ring. Mao. skal vi vise, at der findes en Euklidisk normfunktion på $\mathbb{Z}[\omega]$. Et udmærket bud er funktionen $N: \mathbb{Z}[\omega] \rightarrow \mathbb{N}$. Lad $z, d \in \mathbb{Z}[\omega]$, $d \neq 0$. Hvis $d \mid z$ (her betyder \mid at gå op i inden for $\mathbb{Z}[\omega]$) kan vi skrive $z = qd + 0$ for et passende valgt q . Vi kan tænke på $\mathbb{Z}[\omega]$ som den delmængde af de komplekse tal, der er markeret med prikker på figur 1. Man ser let, at der intetsteds i den komplekse plan er mere end 1 til det nærmeste punkt i $\mathbb{Z}[\omega]$ (sidelængden i den indtegnede trekant er netop 1). Hvis d ikke går op i z , vælger vi et punkt $q \in \mathbb{Z}[\omega]$ som ligger mindre end 1 fra det komplekse tal z/d , og

Figur 1: Mængden $\mathbb{Z}[\omega]$

vi definerer $r = z - qd$. Vi vil nu vise, at $N(r) < N(d)$. Vi har

$$\begin{aligned} \frac{N(r)}{N(d)} &= \frac{N(z - qd)}{N(d)} \\ &= N\left(\frac{z - qd}{d}\right) \\ &= N\left(\frac{z}{d} - q\right) \\ &< 1 \end{aligned}$$

da jo q var valgt så $|z/d - q| < 1$. Heraf følger det ønskede.

Der synes ikke at være nogen rent algebraisk måde at løse opgaven på; man kommer ikke udenom at skulle vurdere afstande i den komplekse plan.

- (iv) Da $N(1 - \omega) = 1 - (-1) + 1 = 3$ er et primtal, er $1 - \omega$ pr. (ii) et irreducibelt element. Da $\mathbb{Z}[\omega]$ er en Euklidisk ring, er den også et PID og dermed et UFD; derfor følger fra Proposition 3.5.3 at $1 - \omega$ er et primelement i $\mathbb{Z}[\omega]$.

En anden ting det lykkedes mig at kage rundt i var beviset for, at et endeligt integritetsområde er et legeme. Jeg vil formulere det lidt anderledes:

Lemma 3. Lad R være en endelig ring. Så er et element $x \in R$ enten 0, en nuldivisor eller en enhed (bemærk at et element ikke kan være flere af disse ting på én gang).

Bevis. Lad $x \in R$ være et element, som ikke er 0. Lad elementerne i ringen være nummereret $R = \{a_1, \dots, a_n\}$, og betragt de n elementer xa_1, xa_2, \dots, xa_n . Hvis disse alle er forskellige, må de udgøre samtlige elementer i R ; og dermed findes der et a_i så $xa_i = 1$; altså er x en enhed. Hvis elementerne ikke alle er forskellige, må der være to som er ens. Hvis $xa_i = xa_j$ har vi $x(a_i - a_j) = 0$. Da a_i og a_j er to forskellige elementer, er $a_i - a_j \neq 0$, og dermed er x en nuldivisor. \square

Med dette lemma i hånden er det nemt at løse opgave III.23; thi i et endeligt integritetsområde ved vi, at elementer som ikke er 0 nødvendigvis må være enheder.

Ordbog

På dansk er sammensatte ord sat sammen, hvilket fx vil sige at det hedder en ringhomomorfi og ikke "ring homomorfi".

Endnu en opdatering:

Engelsk	Dansk
term	term eller led
leading coefficient	ledende koefficient
degree	grad
leading term	ledende term
monic	monisk
root	rod
primitive root of unity	primitiv enhedsrod
cyclotomic	cyklotomisk ("cirkeldelingspolynomier")
Gröbner basis	Gröbnerbasis
term order	termordning
lexicographic	leksikografisk