Forkunnskaper

I dette avsnittet skal vi raskt repetere enkelte av de grunnleggende resultatene fra kurset i kommutativ algebra.

De ringene som opptrer i algebraisk tallteori er spesielle ringer sammenlignet med ringene som kommutativ algebra — og for såvidt algebraisk geometri — kan oppvise. De har alle av Krull-dimensjon 0 eller 1, og ikke nok med det, deres restklassekropper er alle *endelige*. Til gjengjeld, dukker vi vesentlig dypere ned i strukturen deres enn man gjorde i kommutativ algebra.

Den typiske ringen som vi er interessert i er heltallsringen i en algebraisk tallkropp.

Gotisk skrift

Algebraisk tallteori var i lang tid dominert av tyske matematikere, man kan til og med gå så langt å si at det utelukkende var en tysk disiplin, selvsagt med enkelte isolerte unntak. Dette varte til langt inn på 1900-tallet, nesten frem til Annen Verdenskrig. Det er derfor ikke oppsiktsvekkende at gotiske bokstaver fortsatt er i utstrakt bruk i tallteorien, til og med i moderne anglo-saksiske lærebøker. Forøvrig er ikke gotisk skrift egentlig et tysk fenomen. Den oppstod i Frankrike, og ble brukt over hele det germanske Europa til langt in på 1800-tallet, også i Storbritania, men den ble holdt lengst i hevd i Tyskland. Der ble den avskaffet av det nazistiske regimet i 1941.

Her kommer de trykte bokstaven i den typen vi skal bruke, men vi skal heldigvis ikke trenge alle:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{e}$	$\mathfrak{f}$	$\mathfrak{g}$	$\mathfrak{h}$	$\mathfrak{i}$	$\mathfrak{j}$	$\mathfrak{k}$	$\mathfrak{l}$	$\mathfrak{m}$	$\mathfrak{n}$	$\mathfrak{o}$	$\mathfrak{p}$	$\mathfrak{q}$
$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	$\mathfrak{D}$	$\mathfrak{E}$	$\mathfrak{F}$	$\mathfrak{G}$	$\mathfrak{H}$	$\mathfrak{I}$	$\mathfrak{J}$	$\mathfrak{K}$	$\mathfrak{L}$	$\mathfrak{M}$	$\mathfrak{N}$	$\mathfrak{O}$	$\mathfrak{P}$	$\mathfrak{Q}$

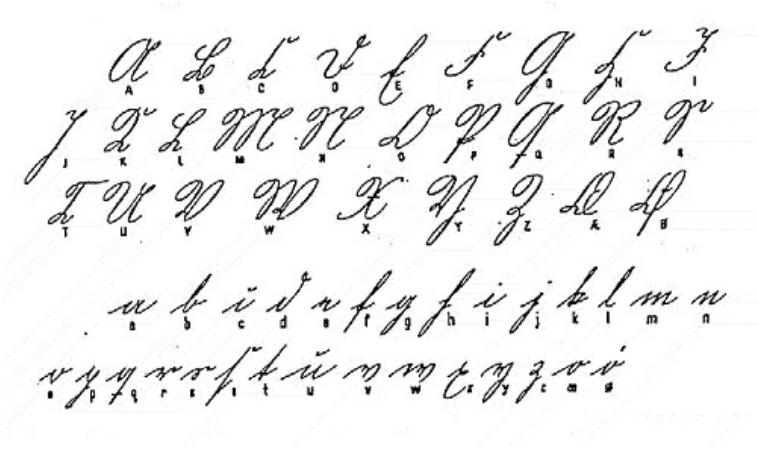
r	s	t	u	v	w	x	y	z
$\mathfrak{r}$	$\mathfrak{s}$	$\mathfrak{t}$	$\mathfrak{u}$	$\mathfrak{v}$	$\mathfrak{w}$	$\mathfrak{x}$	$\mathfrak{y}$	$\mathfrak{z}$
$\mathfrak{R}$	$\mathfrak{S}$	$\mathfrak{T}$	$\mathfrak{U}$	$\mathfrak{V}$	$\mathfrak{W}$	$\mathfrak{X}$	$\mathfrak{Y}$	$\mathfrak{Z}$

Håndskrevne gotiske alfabeter kommer i et uttall variasjoner, på figur 1 viser vi ett.

Enheter

Vi minner om at *en enhet* i en ring A ikke er annet enn et invertibelt element, *i.e.,* a er en enhet hvis $a^{-1} \in A$. Undermengden A^* av A bestående av enhetene er så klart lukket under multiplikasjon, og multiplikasjonen i A gir således en *gruppestruktur* til A^*. Enhetsgruppen er *funktoriell* i A, det vil si at om $f\colon A \to B$ er en ringavbildning, så avbildes A^* inn i B^*.

Enhetsgruppen til en kropp K er selvsagt per definisjon mengden av ikke-null-elementene: $K^* = \{\, x \in K \mid x \neq 0 \,\}$, mens for eksempel i $\mathbb{Z}$, er enhetsgruppen gitt som $\mathbb{Z}^* = \{\pm 1\} = \mu_2$.



Figur 1: Et håndskrevet gotisk alfabet.

Et noe mer subtilt eksempel finner vi i ringen av de *gaussiske heltallene*. Den er definert som $\mathbb{Z}[i] = \{\, a + ib \mid a, b \in \mathbb{Z} \,\}$. De eneste enhetene i denne ringen er ± 1 og $\pm i$. Enhetsgruppen faller sammen med gruppen μ_4 av fjerde enhetsrøtter og er isomorf med Kleins firer-gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

OPPGAVE 1. Vis at om $z \in \mathbb{Z}[i]$, så er $|z| \in \mathbb{Z}$. Vis videre at om $|z| = 1$, så er $z = \pm 1$ eller $z = \pm i$, og bruk det til å bestemme enhetsgrupen i $\mathbb{Z}[i]$, ✸

OPPGAVE 2. La $h = \exp 2\pi i/3$ være en tredje enhetsrot. Bestem enhetene i ringen $\mathbb{Z}[\eta]$ (hvis elementer stundom omtales som *Eisensteinske heltall* oppkalt etter den tyske matematikeren Eisenstein; det er ham med kriteriet). HINT: om $z = a + \eta b$ med $a, b \in \mathbb{Z}$, så er $|z|^2 = a^2 - ab + b^2$. ✸

OPPGAVE 3. Vis at ringen $\mathbb{Z}[\sqrt{2}]$ har uendelig mange forskjellige enheter. HINT: Se på $1 + \sqrt{2}$ og $1 - \sqrt{2}$. ✸

Primelementer og irredusible elementer

Hvis man vil generalisere definsjonen av et primtall til en vilkårlig ring kan dette gjøres på to forskjellig måter som ikke er ekvivalente i generelle ringer.

Et element a i et integritetsområde A kalles for et *primelement* dersom a deler et produkt av elementer fra A, så må dele en av faktorene; eller uttrykt i symboler: $a|xy$ medfører at $a|x$ eller $a|y$. En annen måte å uttrykke dette på, er å si at hovedidealet (a) er et *primideal*.

Den andre generaliseringen er som følger. Et element $a \in A$ kalles for *irredusibelt* dersom det *ikke* kan skrives som et produkt av to ikke-eneheter i A; eller sagt annerledes, om $a = xy$ så er enten $x \in A^*$ eller $y \in A^*$.

Det er klart at et hvert primelement er irredusibelt, for om a er prim og $a = xy$, så vil for eksempel $a|x$, *i.e.*, $x = za$. Det gir $a = azy$ og siden A er et integritetsområde, kan vi kansellere a, og vi finner $1 = zy$. Omvendingen gjelder ikke generelt, og neste oppgave gir et *generisk* eksempel på det:

OPPGAVE 4. La k være en kropp, *e.g.*, $k = \mathbb{C}$, og la u, v, s og t være uavhengig variable. La videre $A = k[u, v, s, t]/(uv - st)$. Vis at u, v, s og t alle er irredusible elementer i A, men ikke primelementer. HINT: : Bruk at A er en gradert ring (siden $uv - st$ er homogent) og at u, v, s og t er homogene av grad én. ✸

ENTYDIG FAKTORISERING Det er selvsagt av interesse å forstå når disse to generaliseringen faller sammen, og det skjer presis dersom vi har *entydig faktorisering* i A. Hvis man vil, kan man si at diskrepansen mellom de to begrepene er obstruksjonen for å ha entydig faktorisering. Det går tydelig frem av eksemplet i oppgaven der $uv = st$ er to *distinkte* faktoriseringer av et element i irredusible faktorer.

I et integritetsområde der alle irredusible elementer er primelementer, viser man ved en enkel induksjon (på r eller s) at om $a_1, \ldots, a_r = b_1, \ldots, b_s$ og alle a_i-ene og b_i-ene er irredusible, så $r = s$ og $a_i = u_i b_{\sigma(i)}$ for en passende permutasjon σ og dertil høvelige enheter u_i. I kortversjon: Faktorene er entydig opptil rekkefølge og skalering med enheter, slik vi kjenner fra *Aritmetikkens fundamentalteorem* for de hele tallene $\mathbb{Z}$.

OPPGAVE 5. Gjennomfør induksjonen. ✸

I en noethersk ring sjekker man lett at ethvert element er produkt av endelig mange irredusible elementer, slik at vi har følgende setning:

Setning 1 *Et noethersk integritetsområde er* UFD[1] *hvis og bare hvis ethvert irredusibelt element er et primelement.*

OPPGAVE 6. Anta at A er et noethersk integritetsområde. Hvis at ethvert element kan skrives som et produkt av (endelig mange) irredusible elementer. HINT: La a være et moteksempel slik at hovedidealet (a) er maksimalt blant hovedidealene generert av et moteksempel. ✸

Vi avslutter denne paragrafen med en oppgave som omhandler erkeeksemplet fra tallteoreien på en ring som ikke er UFD, og som figurerer i begynnelsen på stort sett hver eneste tekst om algebraisk tallteori:

OPPGAVE 7. Ringen $A = \mathbb{Z}[\sqrt{-5}]$ er ikke UFD. Vis at de eneste enhetene i A er ± 1. Vis at $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ er to forskjellige faktoriseringer i irredusible elementer (Likheten er opplagt. Oppgaven går utpå å vise at de fire involverte elementene er irredusible, og at de ikke ikke går opp i hverandre.) HINT: Bruk at $|z|^2 = a^2 + 5b^2$ om $z = a + 5b$. ✸

ET PID ER ET UFD Akromynet PID står for "Principal ideal domain ". At A er et PID innebærer at alle idealer i A er hovedidealer, altså, som vi sier på norsk, at A er et hovedidealområde. Vi skal se at vi da har entydig faktorisering i A. La a være et irredusibelt element fra A. Da er (a) et maksimalt ideal, for om $(a) \subseteq (b)$, kan vi skrive

[1] *Entydigfaktoriseringsområder* er et fornøyelig ord som kunne komme langt opp i konkurransen om årets lengste ord, men det er tungvint, så vi skal systematisk bruke det anglisistiske akronymet UFD, også adjektivisk. Vi minner at det står for *Unique Factorization Domain*.

$a = cb$, og siden a er irredusibelt, har vi to muligheter. Enten er c en enhet, og $(a) = (b)$, eller så er b en enhet, noe som innebærer at $(b) = A$.

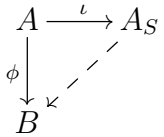
Maksimale idealer er primidealer, og det følger at a er et primelement.

Lokalisering

Vi minner om at et *multiplikativt system* i en ring S er en undermengde som er lukket under multiplikasjon og som inneholder 1. *Lokaliseringen* av A i det multiplikative systemet S er ringen A_S bestående av "brøker" med teller fra A og nevner fra S, *i.e.,* av elementer som skrives på formen a/s der $s \in S$ og $a \in A$. To slike, a/s og a'/s', er like dersom $t(s'a - a's) = 0$ for en $t \in S$. der I tilfellet A er et integritetsområde, kan t-en droppes, og vi er tilbake til det vante kriteriet for at to brøker er like.

Det er kanonisk avbildning $A \to A_S$ som sender a til $a/1$. Om denne er injektiv, vil vi dentifisere A med sitt bilde og skrive a for $a/1$. At a abvbildes på null, betyr ar $ta = 0$ for en $t \in S$, slik at om *e.g.,* A er et integritetsområde, er den kanoniske avbildningen automatisk injektiv. Og i dette tilfellet vil vi betrakte alle lokaliseringer A_S som underringer av kvotientkroppen K til A.

EN UNIVERSELL EGENSKAP Det er klart at elementene fra S alle blir invertible i A_S, og A_S er *universell* eller *minimal*, hvis man vil, for denne egenskapen. Det betyr at at avbildningen $A \to A_S$ er karakterisert ved følgende universelle egenskap: Enhver ringavbildning $\phi\colon A \to B$ som avbilder det multiplikative systemet S inn i gruppen B^* av enheter i B faktoriserer på en entydig måte gjennom A_S. Dette er ikke mer hokus pokus enn at om $\phi(s)$ er invertibel i B, så har uttrykket $\phi(a)/\phi(s)$ mening og betegner et element i B. Digramfreaks uttrykker dette slik:



Å gjøre en pil prikket symboliserer at utsagnet er at en tilsvarende avbildningen skal finnes.

PRIMIDEALER I A_S Primidealene i A_S står i en grei relasjon til primidealene i A. Om $\mathfrak{p} \cap S \neq \emptyset$, vil $\mathfrak{p}A_S$ inneholde en enhet og blåses dermed opp til hele A_S — og grunnleggende er det bare dette som skjer. Vi har en en-en-tydig korrespondanse mellom mengdene

- ☐ av primidealer $\mathfrak{p}$ i A med $S \cap \mathfrak{p} = \emptyset$
- ☐ av primidealer $\mathfrak{q}$ i A_S

som er gitt ved de gjensidig inverse tilordningene $\mathfrak{p} \mapsto \mathfrak{p}A_S$ og $\mathfrak{q} \mapsto \mathfrak{q} \cap A$.

OPPGAVE 8. Bevis denne påstanden. ✸

De suverent viktigste multiplikative systemene er komplementene til primidealer. For et primideal $\mathfrak{p}$ i A lar vi $A_\mathfrak{p}$ betegne lokalisering av A i komplementet til $\mathfrak{p}$, *i.e.,*

i det multiplikative systemet $S = \mathfrak{p}^c = \{ s \in A \mid s \notin \mathfrak{p} \}$. Dette er en lokal ring hvis (eneste) maksimale ideal er $\mathfrak{p}A_\mathfrak{p}$ (siden $\mathfrak{p}$ er maksimalt blant idealene som ikke treffer $\mathfrak{p}^c$!). Restklassekroppen $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ skal vi betegne med $k(\mathfrak{p})$. Dersom $\mathfrak{p}$ er et maksimalt ideal, er $k(\mathfrak{p}) = A/\mathfrak{p}$.

EKSEMPEL 1. Om $p \in \mathbb{Z}$ er et primtall, er lokaliseringen $\mathbb{Z}_{(p)}$ undermengden av $\mathbb{Q}$ av brøker med en nevner (når de skrives på redusert form) som er relativt primisk til p, *i.e.*, $\mathbb{Z}_{(p)} = \{ a/b \mid a, b \in \mathbb{Z}, p \text{ er ikke faktor i } b \}$. Restklassekroppen $\mathbb{Z}_p/p\mathbb{Z}_{(p)} = \mathbb{Z}/p\mathbb{Z}$ er kroppen med p elementer, og vi skal betegne den med $\mathbb{F}_p$. ❄

LOKALISERING AV MODULER Moduler kan også lokaliseres. Om M er en A-modul, lar vi $M_S = M \otimes AA_S$. Elementene i M_S er igjen en slags brøker m/s, der nå telleren m er et element fra modulen M, mens neveren s fortsatte skal være i S. To slike, m/s og m'/s', faller sammen hvis og bare hvis $t(s'm - sm') = 0$ for iallefall en t i S. Vi har en kanonisk avbildning $M \to M_S$ som avbilder m på $m/1$.

Denne avbildningen kan gjerne ha en kjerne, og kjernen består av de elementene $m \in M$ som drepes av et element i S, eller, uttrykt med symboler, der ι for anledningen betegner den kanoniske avbildningen, har vi $\operatorname{Ker} \iota = \{ m \in M \mid \exists s \in S \text{ med } sm = 0 \}$.

OPPGAVE 9. Vis at $M_\mathfrak{p} \neq 0$ hvis og bare hvis $\operatorname{Ann}(M) \subseteq \mathfrak{p}$. HINT: Om $s \in \operatorname{Ann}(M)$ så er $sm = 0$ for alle $m \in M$. ✸

FUNKTORIELLE EGENSKAPER Lokaliseringen er en funktor. Om $\phi\colon M \to N$ er en avbildning (av A-moduler så klart) har vi den induserte avbildningen (av A_S-moduler så klart) $\phi_S := \phi \otimes 1_{A_S}\colon M_S \to N_S$. Elementvis er denne beskrevet ved $m/s \mapsto \phi(m)/s$.

Lokalisering har to to fundamentale egenskaper:

- ☐ Lokalisering er en eksakt funktor. I klartekst betyr dette at om

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$$

er en eksakt sekvens av A-moduler[2], så er den lokaliserte sekvensen

$$M'_S \xrightarrow{\alpha_S} M_S \xrightarrow{\beta_S} M''_S$$

eksakt. Dette innebærer at enhver sekvens av A-modulavbildninger som er eksakt i hvert ledd (kort sagt, som er eksakt), forblir eksakt (i hvert ledd) etter lokalisering.

- ☐ Om M er en A-modul og $M_\mathfrak{p} = 0$ for alle primidealer i A, så er $M = 0$. (Dette gjelder virkelig for alle M uten noen endelighetsbetingelser.)

OPPGAVE 10. Vis den andre egenskapen ovenfor. HINT: La $m \in M$ være et element. Da finnes et maksimalt ideal $\mathfrak{m}$ slik at $\operatorname{Ann}(m) \subseteq \mathfrak{m}$. ✸

[2]Husk at eksakthet av sekvensen betyr at $\operatorname{Ker} \beta = \operatorname{Im} \alpha$

OPPGAVE 11. Hvis du en regnværsdag er ensom og kjeder deg og ikke bedre å foreta deg, bevis den første egenskapen. ✸

Den neste setningen vi skal omtale er en viktig setning, som vi ved mange anledninger skal støtte oss på. Mange egenskaper ved moduler er *lokale* . Det betyr at dersom alle lokaliseringene $M_\mathfrak{p}$ av M i primidealer har har egenskapen (vi sier isåfall at egenskapen gjelder *lokalt*), så har M selv egenskapen (den gjelder da *globalt*). Lokal algebra er enklere enn global, så lokale egenskaper er ofte behagelig å arbeide med og dermed stundom enkle å verifisere. Et eksempel på en lokal egenskap vi nettopp så, er å være en triviell modul (*i.e.,* nullmodulen). For A-modulavbildninger har vi en helt tilsvarende terminologi.

Løselig uttrykt sier neste setning at å være en isomorfi er en *lokal* egenskap for A-modulavbildninger. Den følger lett fra de to egenskapen vi nettopp omtalte.

Setning 2 *La $\phi\colon M \to N$ være en A-modulavbildning, og anta at $\phi_\mathfrak{p} = \phi \otimes 1_{A_\mathfrak{p}} \colon M_\mathfrak{p} \to N_\mathfrak{p}$ er en isomorfi for alle primidealer $\mathfrak{p}$. Da er ϕ en isomorfi.*

OPPGAVE 12. Bruk de to egenskapene til å vise denne setningen. HINT: Vi har en eksakt sekvens

$$0 \longrightarrow \operatorname{Ker}\phi \longrightarrow M \xrightarrow{\phi} N \longrightarrow \operatorname{Coker}\phi \longrightarrow 0$$

✸

Brudne idealer og deres yoga

Gauss' siste student Julius Wilhelm Richard Dedekind (1831–1916) var den som på en systematisk måte introduserte idealer i matematikken. Tidligere hadde Kummer snakker om "ideelle tall", men på en svevende og upresis måte. Etter å ha avsluttet sin doktorgrad knyttet Dedkind seg nært til Dirichlet, og i 1863 utga han *Vorlesungen über Zahlentheorie* som er bygget over Dirichlets forelesninger, men mye var allikevel suget av eget bryst. I den boken introduses idealer, og mange regner boken som starten på den moderne matematikken med mengder som den terminologiske ryggrad.

BRUDNE IDEALER Vi lar A være et noethersk integritetsområde med kvotientkropp K. Et *bruddent ideal* er en A-undermodul $\mathfrak{a}$ av K som er slik at det finnes en $d \in A$, slik at $d \cdot \mathfrak{a} \subseteq A$.

Siden A er en noethersk ring, er denne betingelsen ekvivalent med at $\mathfrak{a}$ er en *endeliggenerert* A-modul; for $d \cdot \mathfrak{a}$ og $\mathfrak{a}$ er isomorfe som A-moduler (multiplikasjon med d gir en isomorfi), men $d \cdot \mathfrak{a}$ er jo et ideal (godt gammeldags) i den noetherske ringen A, og derfor er det endeliggenerert. Den andre veien krever ikke noetherskhet: La $f_1, \ldots, f_r$ være generatorer for $\mathfrak{a}$. Hver av dem kan skrives som kvotienter $f_i = a_i/b_i$ der a_i-ene og b_i-ene er elementer fra A. La d være produktet av alle nevnerne som opptrer, *i.e.,* $d = b_1 \cdot \cdots \cdot b_r$. Da er klart $d \cdot \mathfrak{a} \subseteq A$.

BRUDNE HOVEDIDEALER Som for idealer, kaller vi et bruddent ideal for et *hovedideal* dersom det er monogent, *i.e.,* det er generert av ett element. Om $f \in K$, betegner vi hovedidealet generert av f med (f). Vi har altså $(f) = \{\, af \mid a \in A \,\} \subseteq K$. Siden et bruddent ideal $\mathfrak{a}$ er inneholdt i K, og dermed uten torsjon, er det isomorft med A som A-modul hvis og bare hvis det er et hovedideal. Alle idealer $\mathfrak{a} \subseteq A$ er naturligvis også brudne idealer.

Vi lar $I(A)$ betegne mengden av brudne idealer i A. Den kalles *idealgruppen*[3] til A. Undermengden P_A av I_A som består av hovedidealer, kalles for *hovedidealgruppen* til A (P for prinicipal).

MULTIPLIKASJON OG ADDISJON AV BRUDNE IDEALER Så til yogaen: Brudne idealer kan, som de vanlig idealene, adderes og multipliseres. Om $\mathfrak{a}$ og $\mathfrak{b}$ er to brudne idealer, er summen of produktet deres definert på vanlig måte ved:

- $\mathfrak{a} + \mathfrak{b} = \{\, a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b} \,\}$
- $\mathfrak{a} \cdot \mathfrak{b} = \{\, \sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \,\}$

I den siste definisjonen er summene selvsagt er endelige (men av vilkårlig lengde). At dette virklig gir brudne idealer er klart, for om $d \cdot \mathfrak{a} \subseteq A$ og $f \cdot \mathfrak{b} \subseteq A$, så er $df \cdot \mathfrak{ab} \subseteq A$ og $df \cdot (\mathfrak{a}+\mathfrak{b}) \subseteq A$. Man sjekker uten vanskeligheter at de vanlige aksiomene for assosiativitet og distributivitet er oppfyllt og — hva som er opplagt — at de to operasjonene begge er kommutative.

Det er særlig multiplikasjonen som spiller en stor rolle i kurset. Den organiserer I_A til en *monoid*, *i.e.,* de to første gruppeaksiomene er oppfylt, men inverser finnes ikke nødvendigvis. Åpenbart er $(f)(g) = (fg)$, så hovedidealgruppen P_A er lukket under multiplikasjon, og er derfor en undermonoid av I_A.

Som sagt, vi streber etter en gruppestruktur på I_A, og til det trenges en inversdannelse. Et godt forsøk på lage inverse brudne idealer er å la $\mathfrak{a}^{-1}$ være definert som

- $\mathfrak{a}^{-1} = \{\, x \in K \mid x\mathfrak{a} \subseteq A \,\}$

Da er så klart $\mathfrak{a}\mathfrak{a}^{-1} \subseteq A$, men likhet gjelder ikke generelt. Et bruddent ideal kalles *invertibelt* dersom $\mathfrak{a}\mathfrak{a}^{-1} = A$. Brudne hovedeidealer er alltid invertible. Vi finner at $(f)^{-1} = (f^{-1})$; for om $xf = b \in A$, så er $x = bf^{-1} \in (f^{-1})$.

Det er ikke vanskelig å verifisere at $\mathfrak{a}^{-1}$ er endeliggeneret, det følger *e.g.,* enkelt av den første av påstandene i lemmaet nedenfor. Det forteller oss at multiplikasjon og inversdannelse i I_A respekterer inklusjonsrelasjonene (inversdannelsen snur den selvsagt):

Lemma 1 *Om $\mathfrak{a}$,$\mathfrak{b}$ og $\mathfrak{c}$ er tre brudne idealer i A, så gjelder*

- *Om $\mathfrak{a} \subseteq \mathfrak{b}$, så er $\mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$*

[3] Dette er en dårlig betegnelse siden I_A for de fleste ringer *ikke* er en gruppe! Kun om A er dedekindsk er navnet dekkende, og det kommer vi snart tilbake til

- *Om* $\mathfrak{a} \subseteq \mathfrak{b}$, *så er* $\mathfrak{ca} \subseteq \mathfrak{cb}$

BEVIS: Den første påstanden er nærmest selvinnlysende: Om $x \in \mathfrak{b}^{-1}$ og $a \in \mathfrak{a}$, så er $xa \in A$, siden $a \in \mathfrak{b}$. Den andre er selvinnlysende. ❑

La oss så verifisere at $\mathfrak{a}^{-1}$ er endeliggenerert. Til det, la $a \in \mathfrak{a}$ være et element som ikke er null. Da har vi etter den første av påstandene ovenfor inklusjonen $\mathfrak{a}^{-1} \subseteq (a^{-1})$. Som modul over A er det brudne idealet (a^{-1}) isomorf med A, og fordi A er noethersk, er enhver undermodul, spesielt $\mathfrak{a}^{-1}$, endeliggenerert.

SPRÅKBRUK En tradisjonell språkbruk er å si at et element $a \in A$ er en divisor i elementet $b \in A$ dersom $b = ca$ for en $c \in A$, vi sier også at a går opp i b. Oversatt til hovedidealer er dette ekvivalent med at $(b) \subseteq (a)$. Vi utvider nå denne språkbruken til også å omfatte brudne idealer i A, og vi sier at idealet $\mathfrak{a}$ er *en divisor* eller *går opp i* det brudne idealet $\mathfrak{b}$ dersom $\mathfrak{b} \subseteq \mathfrak{a}$.

LOKALISERING Mange viktige egenskaper til ringer og moduler er lokale av natur — om de oppfylles lokalt, *i.e.,* etter lokalisering i primidealer, gjelder de også globalt— og slike egenskaper er det derfor relativt lette å etablere. Vi ser derfor på hvordan monoidstukturen til I_A forholder seg under lokalisering.

La $S \subseteq A$ være et multiplikativt system. Lokaliseringen $\mathfrak{a}_S$ av et bruddent ideal $\mathfrak{a}$ er gitt ved $\mathfrak{a}_S = \{\, as^{-1} \mid a \in \mathfrak{a} \text{ og } s \in S \,\}$. Dette er klart en A_S-undermodul av K, og om $d \cdot \mathfrak{a} \subseteq A$, så er $d \cdot \mathfrak{a}_S \subseteq A_S$, så derfor er $\mathfrak{a}_S$ et bruddent ideal i A_S (eller om man fortrekker en mer prinispiell begrunnelse: lokaliseringer av endeliggenererte moduler er alltid endeliggenererte). Multiplikasjonen og inversdannelsen av brudne idealer er kompatible med lokalisering:

Lemma 2 *Anta at* $S \subseteq A$ *er et multiplikativt system og at* $\mathfrak{a}$ *og* $\mathfrak{b}$ *er to brudne idealer i* A*. Da er*

- $\mathfrak{a}_S \mathfrak{b}_S = (\mathfrak{ab})_S$
- $(\mathfrak{a}_S)^{-1} = (\mathfrak{a}^{-1})_S$

BEVIS: Om $\sum a_i s_i^{-1} b_i t_i^{-1}$ er i $\mathfrak{a}_S \mathfrak{b}_S$ kan vi for passende $s, t \in S$, og passende $a_i' \in \mathfrak{a}$ og $b_i' \in \mathfrak{b}$, skrive $\sum a_i s_i^{-1} b_i t_i^{-1} = s^{-1}t^{-1} \sum a_i' b_i'$, og det siste elemenent ligger i $(\mathfrak{ab})_S$. Derfor er $\mathfrak{a}_S \mathfrak{b}_S \subseteq (\mathfrak{ab})_S$. At $(\mathfrak{ab})_S \subseteq \mathfrak{a}_S \mathfrak{b}_S$ er klart.

Anta at $x \in (\mathfrak{a}_S)^{-1}$. Da er $xa/s \in \mathbb{A}_S$ for alle $a \in A$ og alle $s \in S$. ❑

EKSEMPEL 2. Vi skal gi et eksempel på en ring A og et ideal $\mathfrak{a}$ som ikke er invertibelt, og vi velger et av de enkleste eksemplene fra tallteori. Det er $A = \mathbb{Z}[\sqrt{5}]$ og $\mathfrak{a} = (2, 1-\sqrt{5})$.

Vi skal se at $1 \notin \mathfrak{a}\mathfrak{a}^{-1}$, og for å innse det, trenger vi å forstå $\mathfrak{a}^{-1}$. La derfor $z \in \mathbb{Q}(\sqrt{5})$ være slik at $z \cdot \mathfrak{a} \subseteq \mathbb{Z}[\sqrt{5}]$ og skriv $z = a + b\sqrt{5}$ med a og b rasjonale tall. Siden $2z \in \mathbb{Z}[\sqrt{5}]$, er $a = n/2$ og $b = m/2$ der n og m er hele rasjonale tall. Vi har

$$z(1 - \sqrt{5}) = (a - 5b) + (a - b)\sqrt{5}$$

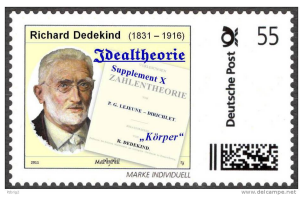
så $z(1-\sqrt{5}) \in \mathbb{Z}[\sqrt{5}]$ er ekvivalent med at $n \equiv m \mod 2$, altså at n og m er av samme paritet. Det betyr at $z = \epsilon \cdot (1+\sqrt{5})/2 + w$ med $w \in \mathbb{Z}[\sqrt{5}]$, og der ϵ enten er 0 eller 1. Med dette er det lett å verifisere at vi har likheten

$$\frac{(1+\sqrt{5})}{2} \cdot (2, 1-\sqrt{5}) = (1+\sqrt{5}, 2),$$

og dermed er $\mathfrak{a}\mathfrak{a}^{-1} = (1+\sqrt{5}, 2)$.

❄

OPPGAVE 13. Vis at $(2, 1-\sqrt{5})$ er et maksimalt ideal i $\mathbb{Z}[\sqrt{5}]$ med restklassekropp lik kroppen $\mathbb{F}_2$ med to elementer. HINT: $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$, og i polynomringen $\mathbb{Z}[x]$ har vi $(x^2-5, 2, 1-x) = (2, x-1)$. ✸



Figur 2: Et tysk frimerke til minne om *Vorlesungen über Zahlentheorie*

IDEALKLASSEGRUPPEN TIL DEDEKINDSKE RINGER Vi skal senere studere dedekindske ringer i detalj, men siden en av de viktigste egenskapen til dedekindske ringer er at idealgruppen I_A er en gruppe, vil vi foregriper begivenhetenes gang noe. Det passer godt inn i dette avsnittet om idelaklassegrupper. At alle brudne idealer er invertible, karakteriserer faktisk dedekinske ringer, som vi senere skal se.

Det finnes en rekke ekvivalente karakteriseringer av dedekindske ringer, og det kan være hipp som happ hvilken man bruker som definisjon. Vi skal si at en *dedekindsk ring* er et noetherske integritetsområde A slik alle lokaliseringene $A_\mathfrak{p}$ i primidealer er hovedidealområder. Vi kommer tilbake til de andre karakteriseringene ved en senere anledning.

Setning 3 *Alle ikke-trivielle brudne idealer i en dedekindsk ring A er invertible.*

BEVIS: La $\mathfrak{a}$ være et ikke-trivielt bruddent ideal. Vi har en naturlig inklusjon $\mathfrak{a}\mathfrak{a}^{-1} \subseteq A$. Dersom A er et hovedidealområde er denne inklusjonen en likhet fordi hovedidealer er invertible. Vi skal bruke at likhet er en lokal egenskap og lokaliserer derfor i et primideal $\mathfrak{p}$. Det gir likheten

$$(\mathfrak{a}\mathfrak{a}^{-1})_\mathfrak{p} \overset{①}{=} \mathfrak{a}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}^{-1} \overset{②}{=} A_\mathfrak{p}$$

der likheten merket ① holder fordi multiplikasjon av brudne idealer er kompatibel med lokalisering, og der ② holder siden $A_\mathfrak{p}$ er et hovedidealområde per antagelse. ❑

Dette betyr at idealgruppen I_A er en gruppe for alle *dedekinske* ringer A. Lemma 1 på side 7 forteller oss at multiplikasjon av brudne idealer bevarer inklusjonsrelasjoner, så I_A er en *ordnet gruppe* med inklusjon som ordningsrelasjon. Gruppen I_A oppfører seg pent ved lokalisering. Det finnes en opplagt avbildnining $I_A \to I_{A_S}$ (som sender $\mathfrak{a}$ til $\mathfrak{a}_S$), og som er en gruppehomorfi fordi multiplikasjon av brudne idealer er kompatibel med lokalisering, lemma 2 på side 8. Vi oppsummerer:

- Om A er dedekinsk, er idealgruppen I_A en ordnet, abelsk gruppe.
- Om S er et multiplikativt system i A, er lokaliseringsavbildningen $I_A \to I_{A_S}$ en gruppehomorfi.

Den har undergruppen P_A bestående av alle brudne hovedidealer i A, og kvotienten C_A kalles *idealklassegruppen* til A. Den er kanskje den mest prominente invarianten til en dedekindsk ring. En umiddelbar observasjon er at A er et hovedidealområde hvis og bare hvis $P_A = I_A$, slik at vi har

Setning 4 *En dedekindsk ring A er et hovedidealområde hvis og bare hvis idealklassegruppen C_A er triviell.*

Det kinesiske restteoremet

Gitt en endelig samling idealer $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ i ringen A. Da har vi en kanonisk avbildning

$$\Psi \colon A \to \prod_{i=1}^{r} A/\mathfrak{a}_i.$$

På hver koordinat virker den som den kanoniske avbildningen $A \to A/\mathfrak{a}_i$,det vil si at r i-te koordinat til bildet $\Psi(x)$ av x er lik restklassen $x + \mathfrak{a}_i$ til x mod $\mathfrak{a}_i$.

Det er klart at kjernene til Ψ er lik snittet $\bigcap_i \mathfrak{a}_i$ siden restklassen til x mod $\mathfrak{a}_i$ er null hvis og bare hvis $x \in \mathfrak{a}_i$.

Anta så at idealene $\mathfrak{a}_i$ er *parvis komaksimale*, altså at de oppfyller $\mathfrak{a}_i + \mathfrak{a}_j = A$ for hvert par av forskjellige indekser i og j. Utsagnet som går under navnet det kinesiske resttoeremet, er at avbildningen Ψ da er surjektiv.

I produktet $\prod_{i=1}^{r} A/\mathfrak{a}_i$ har vi de r elementene $e_i = (0, \ldots, \overset{i}{1}, \ldots, 0)$ som har en ener på i-te plass og ellers bare nuller. Det er tilstrekkelig å vise at hvert av disse ligger i bildet til Ψ. For om $\Psi(a_i) = e_i$, er $\Psi(\sum_i b_i a_i) = \sum_i b_i e_i = (\bar{b}_1, \ldots, \bar{b}_r)$, der $\overline{x}$ betegner restklassen til x mod det behørige idealet. Siden idealene $\mathfrak{a}_i$ er parvis komaksimale, kan vi for hvert par av indekser k og i finne elementer $a_{k,i} \in \mathfrak{a}_k$ slik at $1 = a_{k,i} + a_{i,k}$. Det betyr at vi har

$$a_{k,i} \equiv \begin{cases} 1 & \mod \mathfrak{a}_i \\ 0 & \mod \mathfrak{a}_k. \end{cases}$$

Følgelig er produktet $a_i = \prod_{k,k\neq i} a_{k,i}$ kongruent 1 mod $\mathfrak{a}_i$, men kongruent null mod k for alle andre k, og det betyr at $\Psi(a_i) = e_i$. Vi har også at $\bigcap_i \mathfrak{a}_i = \prod \mathfrak{a}_i$, derfor

Setning 5 *Anta at idealene* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *er gjensidig komaksimale. Da er*

$$A/\bigcap_i \mathfrak{a}^i \simeq \prod_i A/\mathfrak{a}_i.$$

Det er velkjent at om $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, så er $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. Ved induksjon utvider vi dette til en endelig samling parvis komaksimale idealer.

Lemma 3 *Dersom* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *er parvis komaksimale idealer, så faller snittet deres og produktet deres sammen, i.e.,*

$$\bigcap \mathfrak{a}_i = \prod_i \mathfrak{a}_i.$$

BEVIS: Vi bruker induksjon på r, og som sagt, om $r = 2$ er dette velkjent: Skriv $1 = a_1 + a_2$ med $a_i \in \mathfrak{a}_i$ og la $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$. Da er $x = xa_1 + xa_2 \in \mathfrak{a}_1\mathfrak{a}_2$.

For induksjonssteget er det tilstrekkelig å vise at $\bigcap_{i=1}^{r-1} \mathfrak{a}_i$ og $\mathfrak{a}_r$ er komaksimale, det gir nemlig

$$\bigcap_{i=1}^{r} \mathfrak{a}_i = \bigcap_{i=1}^{r-1} \mathfrak{a}_i \cap \mathfrak{a}_r \overset{\downarrow}{=} \prod_{i=1}^{r-1} \mathfrak{a}_i\mathfrak{a}_r = \prod_{i=1}^{r} \mathfrak{a}_i$$

der likheten merket med pilen $\downarrow$ følger fra tilfellet $r = 2$.

Vi kan, fordi hvert av idealene $\mathfrak{a}_i$ er komaksimalt til $\mathfrak{a}_r$, skrive $1 = a_i + b_i$ for $1 \leq i \leq r-1$ der hver a_i ligger i $\mathfrak{a}_i$, mens alle b_i-ene er elementer i $\mathfrak{a}_r$. Det følger at

$$1 = \prod_{i=1}^{r-1}(a_i + b_i) = \prod_{i=1}^{r-1} a_i + b$$

der $b \in \mathfrak{a}_r$. Nå er $\prod_{i=1}^{r-1} a_i \in \prod_{i=1}^{r-1} \mathfrak{a}_i$, og ved induksjon er $\prod_{i=1}^{r-1} \mathfrak{a}_i = \bigcap_{i=1}^{r-1} \mathfrak{a}_i$. Så vi er fremme. ❏

Setter vi dette sammen, får vi den vanlige versjonen av det kinesiske restteoremet.

Setning 6 *Anta at* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *er parvis komaksimale idealer i en ring* A*. Da er induserer avbildningen* Ψ *en isomorfi*

$$A/(\prod_{1\leq i\leq r} \mathfrak{a}_i) \to \prod_{1\leq i\leq r} (A/\mathfrak{a}_i)$$

Heltallselementer og helavslutninger

La nå A være et integritetsområde og K en kropp som inneholder A. Et eksempel å ha i tankene kan være $A = \mathbb{Z}$ og K algebraisk tallkropp.

Den tradisjonelle definisjonen på at et element $x \in K$ er *helt* over A, er at α er rot i et *monisk* polynom med koeffisienter fra A:

$$P(x) = x^n + a^{n-1}x^{n-1} + \cdots + a^1 x + a^0 \qquad (\maltese)$$

der altså a_i-ene alle ligger i A. Det er klart vi kan anta at polynomet er av minimal grad, og da kaller vi det for *minimalpolynomet* til α over A. Det er automatisk irredusibelt, og graden kaller vi for *graden til* α. Om B er en ring som ligger mellom A og K — vi har altså at $A \subseteq B \subseteq K$ — så sier vi at B er *hel* over A dersom alle elementene i B er hele over A.

EKSEMPEL 3. Elementet $(1+\sqrt{5})/2$ i $\mathbb{Q}(\sqrt{5})$ er helt over $\mathbb{Z}$. Det er en rot i polynomet $x^2 - x - 1$. ❄

EKSEMPEL 4. Elementet $(1+\sqrt{-19})/2$ i $\mathbb{Q}(\sqrt{-19})$ er helt over $\mathbb{Z}$. Det er en rot i polynomet $x^2 - x + 5$. ❄

En annen og kanskje mer konseptuell definisjon er at α er egenverdi til en matrise[4] med koeffisienter i A. De to definisjonene er selvsagt ekvivalente. Det karakteristiske polynomet til en slik matrise er et monisk polynom med koeffisienter fra A, og $P(\alpha) = 0$. Omvendt, et hvert monisk polynom med koefisienter fra a, er det karakteristiske polynomet til en matrise over A, den såkalte "companion"-matrisen til P:

$$\begin{pmatrix} 0 & \dots & \dots & \dots & -a_0 \\ 1 & 0 & \dots & \dots & -a_1 \\ 0 & 1 & \ddots & \dots & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & 1 & -a_{n-1} \end{pmatrix}$$

OPPGAVE 14. Vis dette. HINT: Induksjon på n kombinert med utvikling etter første søyle er en mulighet. ✸

En umiddelbar følge av dette er det neste teoremet som går tilbake til Dedekind. Scenebildet er som tidliger i denne paragrafen med A et integritetsområde som er innehold i kroppen K. Vi lar $\bar{A}$ betegne mengden av elementer i K som er hele over A (dette er selvsagt en konstruksjon som vel så mye avhenger av K som av A, men i forenklingens navn sløyfer vi K i notasjonen).

Teorem 1 *Anta at K er en kropp og at $A \subseteq K$ er en underring. Da er $\bar{A}$ en underring av K.*

BEVIS: Hvis α og β er egenverdier i henholdsvis $m \times m$-matrisen M og $n \times n$-matrisen N og med henholdsvis v og w som egenvektor, så er $\alpha+\beta$ egenverdi til $M \otimes I_n + I_m \otimes N$ og $\alpha\beta$ til $M \otimes N$. I begge tilfellene er $v \otimes w$ den tilhørende egenvektoren. ❑

[4] Eller helbourbakistisk: α er egenverdi til en endeligdimensjonal, lineær K-endomorfi definert over A.

En grunnleggende egenskap ved et element $\alpha \in K$ som er helt over A, er at A-modulen $A[\alpha]$ er endeliggenerert. Noe mer presisyt, den er generert av de n første potensene $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ av α, der n er graden til α. Dette følger enkelt ved polynomdivisjon. Anta at $g(x)$ er et vilkårlig polynom fra $A[x]$ og la $f(x)$ betegne minimalpolynomet til α (som altså er av grad n). Vi dividerer g med f og finner $f(\alpha) = h(\alpha)g(\alpha) + r(\alpha)$ der restpolynomet $r(x)$ er av grad mindre enn n; men $g(\alpha) = 0$ per definisjon, så $f(\alpha) = r(\alpha)$. Det betyr at ethvert element i $A[\alpha]$ er en lineærkombinasjon av de n første potensen til α.

Vi kaller $\bar{A}$ for *helavslutningen av A i K*, og vi sier at A er *helavsluttet* i K, dersom $A = \bar{A}$; *i.e.,* ethvert element i K som er helt over A, ligger allerede i A. Dette er en relativ betingelse, men som også har en absolutt form. Hvis vi kort og godt sier at A er helavsluttet, uten referanse til noen kropp, er det underfortstått av A er helavsluttet i sin kvotientkropp.

EKSEMPEL 5. Underringen $\mathbb{Z}[\sqrt{5}]$ er ikke helavsluttet i $\mathbb{Q}(\sqrt{5})$. Vi så at $\alpha = (1+\sqrt{5})/2$ var hel over $\mathbb{Z}$ — og derfor over $\mathbb{Z}[\sqrt{5}]$ — men $\alpha \notin \mathbb{Z}[\sqrt{5}]$. ❄

Dersom K er en algebraisk tallkropp, kaller i helavslutningen av $\mathbb{Z}$ i K, for *heltallsringen i K*. Det er altså de elementene som er rot i et polynom (❋) med koeffisienter fra $\mathbb{Z}$. Vi kan vel uten å nøle utnevne disse ringen til hovedpersonene i hva vi skal fortelle.

Følgende karakterisering er noen ganger nyttig:

Lemma 4 *La K være en kropp og $A \subseteq K$ være en underring. Anta at $M \subseteq K$ er en endeliggenerert A-undermodul. Dersom $\alpha \in K$ er slik at $\alpha \cdot M \subseteq M$, så er α hel over A.*

BEVIS: La $m_1, \ldots, m_r$ være generatorer for M (som alle er elementer i K). Vi kan for hver i skrive $\alpha m_i = \sum_{1 \le j \le r} a_{ij} m_j$ der $a_{ij} \in A$. Men det betyr at om D er matrisen $D = (a_{ij})$, så er α en egenverdi for D med egenvektorr $v = (m_1 m, \ldots, m_r)$. ❑

Vi bemerker at omvendingen til dette lemmaet også holder. Er α hel over A, så er jo ringen $A[\alpha]$ vi for ved å adjungere α til A, en endeliggenerert A-modul. Det fines også en generalisering av dette lemmaet der M erstattes med en torsjonsfri A-modul med en virkning av α, *i.e.,* en $A[\alpha]$-modul. Den må såklart fortsatt være endeliggenerert over A; det er en fundamental forutsetning. Beviset er i bunn og grunn det samme, men det er noe mer omstendelig siden $v = (m_1, \ldots, m_r)$ ikke lenger er anstendig vektor, men en "vektor" med "koeffisienter" hentet fra modulen M.

OPPGAVE 15. La $D = (m_{ij})$ være en matrise med koeffisienter i en ring A. La c_{ij} være underdeterminanten til $\det D$ vi får ved å stryke søyle nummer i og rad nummer j (merk rekkefølgen). Da er *kofaktormatrisen $D^\dagger$ til D* gitt som $D^\dagger = ((-1)^{i+j} c_{ij})$. Vis at $D^\dagger D = \det D \cdot I$. HINT: Utvikl determinanten $\det N$ etter søyler (eller rader). ✸

OPPGAVE 16. Bruk forrige oppgave til å vise generaliserinengen av lemma 4: Anta at $A \subseteq K$ er en ring i en kropp. La $\alpha \in K$ være et element og la M være en $A[\alpha]$-modul. Dersom M er *endeliggenerert* og *torsjonsfri* over A, så er α hel over A. ✸

Setning 7 *La $A \subseteq B \subseteq C \subseteq K$ være et tårn av integritetsområder inneholdt i kroppen K. Da er C hel over A hvis og bare hvis C er hel over B og B hel over A.*

BEVIS: Vi antar først at C er hel over B og B hel over A. La $\alpha \in C$ være et element. Det er helt over B per antagelse, og vi lar a_i være koeffisientene i en helhetsrelasjon $\sum_i^{a_i} \alpha^i = 0$. Da er hver $a_i \in B$ og altsåer alle hele over A. Det medfører at ringen $R = A[a_1, \ldots, a_{n-1}]$ er en endeliggenerert A-modul. Nå er $R[\alpha]$ en endeliggenerert modul over R, fordi α er hel over R, og det følger at $R[\alpha]$ er endeliggenerert over A. Vi avslutter med lemma 4. Den andre implikasjonen er en trivialitet. ❑

En direkte følge av denne setningen er at

Setning 8 *La $A \subseteq K$ være en underring i en kropp. Helavslutningen av A i K er helavsluttet i K.*

BEVIS: La $\alpha \in K$ være hel over $\overline{A}$. Bruk setning 7 over med $A = A$, $B = \overline{A}$ og $C = B[\alpha]$. ❑

OPPGAVE 17. Vis at dersom A er UFD så er A helavsluttet. ✸

HELAVSLUTTETHET ER EN LOKAL EGENSKAP Dette henger på to observasjoner. Den første er

Lemma 5 *La A være et integritetsområde inneholdt i kroppen K og la S være et multiplikativt system i A. Da er $\overline{(A_S)} = (\overline{A})_S$. Eller sagt med ord, lokalisering og helavslutning (i kroppen K) kommuterer.*

BEVIS: Betrakt egenverdibetingelsen

$$\alpha v = Mv \qquad (\maltese)$$

der $\alpha \in K$, der v er en vektor og M en matrise, begge med koeffisienter fra K. Om $\alpha \in \overline{(A_S)}$ finnes en slik relasjon slik at koeffisientene til matrisen M ligger i A_S. La s betegne produktet av alle nevnere som opptrer i koeffisientene til M. Da er $s\alpha v = sMv$ en egenverdibetingelse over A, og $s\alpha \in \overline{A}$, *i.e.*, $\alpha \in \overline{(A)}_S$.

Den andre veien: Om $\beta \in \overline{(A)}_S$, kan vi skrive $\beta = \alpha/s$ med $s \in S$ og med en α som tilfredtstiller betingelsen ($\maltese$) der M har koeffisienter fra A. Det følger at $\beta v = s^{-1}Mv$ er en egenverdibetingelse over A_S, og dermed er $\beta \in \overline{(A_S)}$. ❑

Setning 9 *Et integritetsområde A inneholdt i kroppen K er helavsluttet i K hvis og bare hvis lokaliseringen $A_{\mathfrak{p}}$ er helavsluttet i K for alle primidelaer $\mathfrak{p}$ i A.*

BEVIS: At A helavsluttet i K medfører at $A_{\mathfrak{p}}$ er, er ikke annet enn lemma 5 ovenfor med $S = A \setminus \mathfrak{p}$. Anta så at hver lokalisering $A_{\mathfrak{p}}$ er helavsluttet i K. Betrakt den kanoniske inklusjonen $A \hookrightarrow \overline{A}$. Lokaliserer vi denne i $\mathfrak{p}$, finner vi den kanoniske inklusjonen $A_{\mathfrak{p}} \hookrightarrow \overline{(A)}_{\mathfrak{p}} \overset{\downarrow}{=} \overline{(A_{\mathfrak{p}})}$, som er identiteten per hypotese (likheten merket med en rød pil kommer fra lemma 5). Siden å være iso er en lokal egenskap for modulavbildninger, følger det at $A = \overline{A}$. ❑

Lar vi K være kvotientkroppen til A. får vi

Setning 10 *Et integritetsområde A er helavsluttet hvis og bare hvis lokaliseringen $A_{\mathfrak{p}}$ er helavsluttet for alle primidelaer $\mathfrak{p}$ i A.*