Lineære avbildninger og Lineær rekursjon

Dan Laksov

Matematiska Institutionen, KTH
SE-100 44 Stockholm
laksov@math.kth.se

I forbindelse med semiariet holdt til minne om E.S. Selmer den 16/2-07 på Matematisk Institutt ved Universitetet i Bergen hadde jeg den selvpåtatte oppgaven å si noen ord om *lineær rekursjon* over *endelig kropper* slik området fortonet seg i Bergen på 1960'tallet. Mens jeg forebredte mitt foredrag slo det meg at man kan betrakte løsningene til lineære rekursjonsrelasjoner som spesielle *lineære avbildninger* på *polynomringer* i en variabel. Dette er på en måte det *duale* synspunktet til det som finnes i litteraturen, og gir en naturlig innfallsport til teorien for lineær rekursjon. Resultatene kommer på denne måten i et *klarere lys*, bevisene blir *lettere*, og man bli på en naturlig måte ledet til *generaliseringer* av teorien. Spesielt blir det klart at begrensningene til endelige kropper, eller mer generelt, til *periodiske sekvenser*, er unødvendig for de fleste betraktningene. Dette illustrerer vi nedenfor ved å gi en detaljert fremtilling av teorien for *multigrammer*. Jeg mistenker at jeg ikke er den første som har oppdaget det *duale* perspektivet, men ettersom jeg ikke kan finne det i litteraturen, og ettersom Selmer så godt som egenhendig drev Normat i 25 år vil jeg med disse notatene gjøre synspuktet tilgjengelig for Normats lesere.

Jeg har ikke gjort noe forsøk på å skrive en komplett fremstilling av teorien for lineære rekursjoner, men har illustrert den *duale metoden* ved å velge ut karakteristiske deler av [L1], [L2], [P], [S] og [Z].

Som leseren vil oppdage er språket utpreget matematisk, med termer som *ringer*, *kropper*, *grupper*, *moduler* og *idealer*. Ingen bør imidlertid blir avskrekket av dette. Nå man ser *ringer* behøver man bare tenke på de *hele tallene* eller de *hele tallene modulo et helt tall*, og når man ser *kropper* skal man tenke på de *rasjonale tallene* eller de *hele tallene modulo primtall*. Moduler, grupper og idealer er eksplisitt gitt, og regnerelgene i hvert konkret tilfelle er lette å verifisere. Grunnen til at vi bruker en mer høytravende terminologi er at dette er praktisk, og antyder at materialet er en del av en mer generell forestillingsverden.

Innledning

De aller fleste har noen gang kommet i kontakt med *lineære rekursjoner*. I det minste har de hørt om *Fibonacci sekvensen*

$$1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad \ldots,$$

der hvert tall efter de to første er summen av de to foregående. Fibonacci sekvensen forekommer overalt i matematikken og i naturen, og den har masser av interessante egenskaper ([V], [VS]). Den har blitt studert fra en rekke ulike synspunkter og det er skrevet titusentalls artikler om den.

En annen velkjent og flittig studert løsning til den samme lineære relasjonen er *Lucas sekvensen*

$$1, \quad 3, \quad 4, \quad 7, \quad 11, \quad 18, \quad 29, \quad 47, \quad 76, \quad \ldots,$$

der også hvert tall etter de to første er summen av de to foregående.

De to første tallene $1, 1$, og $1, 3$, i Fibonacci sekvensen, respektive i Lucas sekvensen, kalles *begynnelsesverdiene* til sekvensene. Det er klart at begynnelsesverdiene, sammen med regelen om at hvert tall etter de to første er summen av de to foregående, bestemmer resten av sekvensen. For eksempel gir begynnelsesverdien $3, 1$ sekvensen

$$3, \quad 1, \quad 4, \quad 5, \quad 9, \quad 14, \quad 23, \quad 37, \quad 60, \quad \ldots.$$

Et viktig problem for slike sekvenser er å bestemme, for et gitt primtall, hvilke av medlemmene i sekvensen som er delbare med dette primtallet. Vil vi, for eksempel, bestemme hvilke av tallene i sekvensene ovenfor som er delbare med to, kan vi regne i tallkroppen $\{0, 1\}$ med to elementer der $1 + 1 = 0$. Vi får at alle tre sekvensene ovenfor gir sekvensen

$$1, \quad 1, \quad 0, \quad 1, \quad 1, \quad 0, \quad 1, \quad 1, \quad 0, \quad \ldots$$

i denne kroppen, det vil si, en *periodisk sekvens* med *periode* 3. Ettersom termene nummer $3, 6, 9, \ldots$ er 0 vil det være termene med disse nummerene, og bare disse, som er delbare med 2. Er vi interesserte i hvilke av medlemmene i de tre sekvensene som er delbare med 3 kan vi regne i *tallkroppen* $\{0, 1, 2\}$ med tre elementer, der $1 + 2 = 0, 2 + 2 = 1 = 2 \cdot 2$. Vi får da de tre sekvensene

$$\begin{array}{cccccccccccccccc}
1, & 1, & 2, & 0, & 2, & 2, & 1, & 0, & 1, & 1, & 2, & 0, & 2, & 2, & 1, & 0, & \ldots \\
1, & 0, & 1, & 1, & 2, & 0, & 2, & 2, & 1, & 0, & 1, & 1, & 2, & 0, & 2, & 2, & \ldots \\
0, & 1, & 1, & 2, & 0, & 2, & 2, & 1, & 0, & 1, & 1, & 2, & 0, & 2, & 2, & 1, & \ldots
\end{array}$$

alle med periode 8. Vi ser at de tre sekvensene er *forskyvninger* av hverandre. I den første sekvensen hara vi nuller på plassene $4, 8, 12, 16, \ldots$, så tallene i Fibonacci sekvensen er delbare med 3 nøyaktig på disse plassene. Den andre sekvensen har nuller på plassene $2, 6, 10, 14, \ldots$ så tallene i Lucas sekvensen er delbare med 3 nøyaltig på disse plassene.

Delbarhet med primtall er bare en side av lineære rekursjoner. Slike rekursjoner forekommer i mange forkledninger i matematikken. De har også store anvendelser, spesielt ved *elektronisk* overføring av *informasjon*, der de er nær forbundet med *skift registre*. De spiller en stor rolle i *feilkorrigerende koder* og ved *krypering* av meddelelser, og brukes til å generere *pseudoslumptall*.

I det følgende skal vi konsentrere oss om egenskaper som er felles for sekvensene vi får for en gitt lineær rekursjon når vi varierer begynnelsesverdiene. For eksempel, i kroppen med to elementer vil den lineære rekursjonen der hvert tall etter de to

første er summen av de to foregående ha fire løsninger svarende til de fire mulige begynnelsesverdiene $0,0$, og $0,1$ og $1,0$ og $1,1$. Disse er

$$\begin{array}{cccccccccc} 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & \dots \\ 0, & 1, & 1, & 0, & 1, & 1, & 0, & 1, & 1, & \dots \\ 1, & 0, & 1, & 1, & 0, & 1, & 1, & 0, & 1, & \dots \\ 1, & 1, & 0, & 1, & 1, & 0, & 1, & 1, & 0, & \dots \end{array}$$

der de tre siste har periode 3 og er samme sekvens forskjøvet et eller to steg. Det er for slike samlinger av løsninger vårt perspektiv på lineære rekursjonsrelasjoner er mest fruktbar.

1 Lineære avbildninger og sekvenser

Som nevnt i innledningen danner lineære avbildninger fundamentet for vår innfallsvinkel til lineære sekvenser. I denne sekjonen innfører vi den nødvendige notasjonen og gir noen av de grunnleggende resultatene. Vi viser også sammenhengen mellom lineære avbildninger og løsningene til lineære rekursjonsrelasjoner.

1.1 Lineære avbildninger og idealer. Vi skal betrakte *lineære rekursjoner* over en vilkårlig kommutativ *ring* A med *enhet*. En sentral rolle spiller *gruppen* $\mathrm{Hom}_A(A[T], A)$ av *A-lineære avbildninger*, eller som vi nøyer oss med å si, *lineære avbildninger*

$$x : A[T] \to A$$

fra *polynomringen* $A[T]$ i den *variable* T til A. For hvert polynom g i $A[T]$ betegner vi med $L_A(g)$ de lineære avbildningene $x : A[T] \to A$ som er null på elementene $T^i g$ for $i = 0, 1, \dots$, eller ekvivalent, de lineære avbildningene som er null på *idealet*

$$(g) = \{hg : h \in A[T]\}$$

generert av g, Det vil si

$$L_A(g) = \{x \in L_A(0) : x(hg) = 0 \quad \text{for alle} \quad h \in A[T]\}. \tag{1.1.1}$$

Vi ser at $L_A(0) = \mathrm{Hom}_A(A[T], A)$ og av (1.1.1) ser vi at om g deler h i $A[T]$ vil $L_A(g) \subseteq L_A(h)$.
Det er klart at $L_A(g)$ er en *gruppe*. Videre er $L_A(g)$, på en *naturlig* måte, en $A[T]$-*modul* ved at *produktet* av et polynom h i $A[T]$ med et element x i $L_A(g)$ er definert av

$$(hx)(k) = x(hk) \quad \text{for alle} \quad k \in A[T].$$

For å se at hx er i $L_A(g)$ rekker det å observere at $(hx)(gk) = x(hkg) = 0$. Det er klart av definisjonen av *modulstrukturen* at $L_A(g)$ er en *undermodul* av $L_A(0)$.

En fordel ved å betrakte $L_A(0)$ som en $A[T]$-modul er at vi får den smidige skrivemåten

$$L_A(g) = \{x \in L_A(0) : gx = 0\}.$$

Vi betegner med L_A *unionen* av alle modulene $L_A(g)$ for g et *monisk* polynom i $A[T]$, det vil si, polynomene g slik at koeffisienten for den høyeste potensen av T i g er 1. Da er L_A en undermodul av $L_A(0)$ fordi for $x \in L_A$ finnes det et monisk polynom f i $A[T]$ slik at $x \in L_A(f)$ og derfor vil hx være i $L_A(f)$ for alle $h \in A[T]$. Videre finnes det for $y \in L_A$ et monisk polynom g slik at $y \in L_A(g)$, og da vil $x + y \in L_A(fg)$.

1.2 Lineære avbildninger, sekvenser og lineær rekursjon. Til hver *sekvens* $x_0, x_1, \dots$ av elementer i A svarer det nøyaktig en lineær avbildning $x : A[T] \to A$ bestemt av

$$x(T^i) = x_i \quad \text{for} \quad i = 0, 1, \dots .$$

Med andre ord har vi en bijeksjon

$$L_A(0) \longleftrightarrow \{\text{sekvenser av elementer i} \quad A\} \tag{1.2.1}$$

som avbilder den lineære avbildningen x til sekvensen $x(1), x(T), x(T^2), \dots$.
La

$$f(T) = T^n - c_1T^{n-1} + \cdots + (-1)^n c_n$$

være et polynom i $A[T]$. En lineær avbildning $x \in L_A(0)$ ligger i $L_A(f)$ hvis og bare hvis $x(T^i f) = x(T^{n+i} - c_1T^{n+i-1} + \cdots + (-1)^n c_n T^i) = 0$ for $i = 0, 1, \dots$. Setter vi $x_i = x(T^i)$ for $i = 0, 1, \dots$ kan dette skrives

$$x_{n+i} - c_1x_{n+i-1} + \cdots + (-1)^n c_n x_i = 0 \quad \text{for} \quad i = 0, 1, \dots . \tag{1.2.2}$$

Vi sier at sekvensen $x_0, x_1, \dots$ *tilfredsstiller* den *lineære rekursjonen* (1.2.2) med *karakteristisk polynom* $f(T)$. Bijeksjonen (1.2.1) induserer følgelig en bijeksjon

$$L_A(f) \longleftrightarrow \{\text{sekvenser i } A \text{ som tilfredsstiller den lineære rekursjonen (1.2.2)}\}.$$

For å fordype forståelsen av sammenhengen mellom lineære avbildninger og sekvenser merker vi at i bijeksjonen (1.2.1) svarer Tx til den *translaterte sekvensen* $x_1, x_2, \dots$.

Eksempel I. Vi gir et eksempel som illustrerer hvordan sekvenser som tilfredsstiller en lineær relasjon kan oppstå, og hvordan sekvensene er knyttet til lineære avbildninger. La $K = \{0, 1\}$ være kroppen med to elementer, så $1 + 1 = 0$. Vi definerer en lineær avbildning $x : K[T] \to K$ ved

$$x(T^i) = \begin{cases} 0 & \text{når} \quad i \quad \text{eller} \quad i-1 \quad \text{er delbar med} \quad 4 \\ 0 & \text{når} \quad i-2 \quad \text{eller} \quad i-3 \quad \text{er delbar med} \quad 4, \end{cases}$$

det vil si, sekvensen $x(T^0), x(T^1), x(T^2), \dots$ er $0, 0, 1, 1, 0, 0, 1, 1, \dots$, som er *periodisk* med *periode* 4. Vi verifiserer lett at

$$x(T^{i+3} - T^{i+2} + T^{i+1} - T^i) = x(T^{i+3}) - x(T^{i+2}) + x(T^{i+1}) - x(T^i) = 0,$$

så x er null på alle elementer på formen $T^i(T^3 - T^2 + T - 1)$, det vil si, på alle elementer i *idealet* (f), der

$$f = T^3 - T^2 + T - 1.$$

Den lineære avbildningen x er følgelig i $L_K(f)$, eller ekvivalent, sekvensen

$$0, \quad 0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 1, \quad \dots$$

tilfredsstiller den lineære rekursjonen

$$x_{3+i} - x_{2+i} + x_{1+i} - x_i = 0.$$

Det er instruktivt å bestemme flere liknende eksempler der man definerer verdiene $x(T^i)$ ved egenskaper som kommer fra delbarhet med et av tallene $3, 4, 5, \dots$.

2 Modulen av lineære avbildninger

I forrige seksjon viste vi sammenhengen mellom lineære avbildninger og løsninger av linære rekursjonsrelasjoner. Her viser vi hvordan hovedsatsene for løsningene av lineære rekursjonsrelasjoner ser ut når de formuleres og vises for lineære avbildninger. Spesielt merker vi hvor lett, naturlig og generell teorien blir.

2.1 Lemma. *La f i $A[T]$ være et* monisk *polynom av grad n og la $x_0, \dots, x_{n-1}$ være elementer i A. Da finnes det nøyaktig en lineær avbildning x i $L_A(f)$ slik at $x(T^i) = x_i$ for $i = 0, \dots, n-1$.*

Mer presist, A-modulen $L_A(f)$ er fri *med* basis *$e_0, \dots, e_{n-1}$ bestemt av*

$$e_i(T^j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

for $i, j = 0, \dots, n-1$.

Bevis. Som vi så i Seksjon 1.1 gir hver sekvens $x_0, x_1, \dots$ i A en entydig lineær avbildning x i $L_A(0)$ slik at $x(T^i) = x_i$ for $i = 0, 1, \dots$. Videre så vi at x er i $L_A(f)$ hvis og bare hvis $x_0, x_1, \dots$ tilfredsstiller den lineære rekursjonen (1.2.2). Vi ser umiddelbart, ved induksjon etter i, at (1.2.2) entydig bestemmer $x_n, x_{n+1}, \dots$ når $x_0, \dots, x_{n-1}$ er gitt. Dette viser første delen av lemmaet.

For å vise den andre delen av lemmaet observerer vi at de lineære avbildningene x og $x_0e_0 + \cdots + x_{n-1}e_{n-1}$ begge ligger i $L_A(f)$, og de tar samme verdier på $1, T, \dots, T^{n-1}$. Det følger da av den første delen av lemmaet at $x = x_0e_0 + \cdots + x_{n-1}e_{n-1}$, så $e_0, \dots, e_{n-1}$ genererer A-modulen $L_A(f)$. At $e_0, \dots, e_{n-1}$ er lineært uavhengige over A er opplagt. □

2.2 En fundamental lineær avbildning. La f være et monisk polynom av grad n som ligger i $A[T]$. Vi betegner med $u = u_f$ elementet i $L_A(f)$ bestemt av

$$u(T^i) = \begin{cases} 0 & i = 0, \dots, n-2 \\ 1 & i = n-1 \end{cases} .$$

Eksempel II. Vi forsetter Eksempel I. I dette eksempelet er $n = 3$ og vi kan velge *begynnelsesverdiene* x_0, x_1, x_2 på $2^3 = 8$ måter. Dette gir sekvensene

I:	0,	0,	0,	0,	0,	0,	0,	0,	...
II:	0,	1,	0,	1,	0,	1,	0,	1,	...
III:	0,	0,	1,	1,	0,	0,	1,	1,	...
IV:	0,	1,	1,	0,	0,	1,	1,	0,	...
V:	1,	0,	0,	1,	1,	0,	0,	1,	...
VI:	1,	1,	0,	0,	1,	1,	0,	0,	...
VII:	1,	0,	1,	0,	1,	0,	1,	0,	...
VIII:	1,	1,	1,	1,	1,	1,	1,	1,	...

Sekvensene I og VIII har *periode* 1, sekvensene II og VII har periode 2, og resten periode 4. Vi ser at sekvensen tilsvarende u i 2.2 er III, og at III, IV, VI, V er u, Tu, T^2u, T^3u respektive.

2.3 Setning. *La f i $A[T]$ være et monisk polynom av grad n. Da er $L_A(f)$ en fri A-modul med basis $u, Tu, \dots, T^{n-1}u$.*

Bevis. Det følger av Lemma 2.1 at vi må vise at det, for hver sekvens $x_0, x \dots, x_{n-1}$ av elementer i A, finnes nøyaktig et polynom $g = a_{n-1} + a_{n-2}T + \cdots + a_0T^{n-1}$ i $A[T]$ slik at $(gu)(T^i) = x_i$ for $i = 0, \dots, n-1$, det vil si, slik at $a_{n-1}u(T^i) + a_{n-2}u(T^{i+1}) + \cdots + a_0u(T^{i+n-1}) = x_i$ for $i = 0, \dots, n-1$. Av definisjonen på u er dette det samme som ligningssystemet

$$a_iu(T^{n-1}) + a_{i-1}u(T^n) + \cdots + a_0u(T^{i+n-1}) = x_i \quad \text{for} \quad i = 0, \dots, n-1,$$

eller

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ u(T^n) & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ u(T^{2n-2}) & u(T^{2n-3}) & u(T^{2n-4}) & \dots & u(T^n) & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

Det er opplagt at dette ligningssystemet har en entydig løsning i $a_0, \dots, a_{n-1}$ når $x_0, \dots, x_{n-1}$ er gitt. □

2.4 Korollar. *La f og g være polynomer i $A[T]$ med f monisk. Da vil f dele g hvis og bare hvis $L_A(f) \subseteq L_A(g)$.*

Bevis. Vi observerte i Seksjon 1 at om f deler g så vil $L_A(f) \subseteq L_A(g)$.

Ettersom f er monisk kan vi bruke Euklids algoritme i $A[T]$. Vi får at $g = qf + r$ med q og r i $A[T]$, og der graden til r er strikt mindre enn graden til f.

Anta at $L_A(f) \subseteq L_A(g)$. Da vil $u_f \in L_A(g)$ så $0 = gu_f = (qf)u_f + ru_f = ru_f$. Men av setningen følger det at $ru_f = 0$ medfører at $r = 0$, det vil si, f deler g. □

2.5 Bemerkning. Korollar 2.4 er en vesentlig generalisering av et resultat av N. Zierler [Z].

Eksempel III. Vi bruker Eksemplene I og II til å illustrere Korollar 2.4. Merk at

$$f = T^3 - T^2 + T - 1 = (T - 1)(T^2 + 1).$$

Vi har at $L_K(T^2 + 1)$ består av de fire lineære avbildningene som tilsvarer sekvensene

I:	0,	0,	0,	0,	0,	0,	0,	0,	...
II:	0,	1,	0,	1,	0,	1,	0,	1,	...
VII:	1,	0,	1,	0,	1,	0,	1,	0,	...
VIII:	1,	1,	1,	1,	1,	1,	1,	1,	...

og at $L_K(T - 1)$ består av to lineære avbildninger som tilsvarer sekvensene

I:	0,	0,	0,	0,	0,	0,	0,	0,	...
VIII:	1,	1,	1,	1,	1,	1,	1,	1,	....

Som påstått i Korollar 2.4 ser vi at $L_K(T^2 + 1)$ og $L_K(T - 1)$ begger er inneholdt i $L_K(f)$. Tar vi et polynom som ikke deler f, for eksempel $T^2 - T + 1$ får vi for eksempel at

$$0, \quad 1, \quad 1, \quad 0, \quad 1, \quad 1, \quad 0, \quad 1, \quad \ldots$$

tilsvarende en lineær avbildning som ligger i $L_K(T^2 - T + 1)$, men ikke i $L_K(f)$.

2.6 Bemerkning. La f være et monisk polynom i $A[T]$ og la $(f) = \{gf : g \in A[T]\}$ være idealet generert av f. *Restklasseringen* til $A[T]$ *modulo* f betegner vi med $A[T]/(f)$. Vi har en isomorfi av $A[T]$-moduler

$$A[T]/(f) \longrightarrow L_A(f) \tag{2.6.1}$$

entydig bestemt av at *klassen* til et polynom g i $A[T]$ modulo f avbildes til $gu = gu_f$.

Dette følger av Setning 2.3, for vi har en avbildning av $A[T]$-moduler $A[T] \to L_A(f)$ som avbilder g til gu. Denne avbildningen er surjektiv ved Setning 2.3 og kjernen inneholder (f) ved definisjonen av $L_A(f)$. Derfor får vi indusert en avbildning $A[T]/(f) \to L_A(f)$ som påstått. Men denne avbilder A-modul basisen i $A[T]/(f)$ som består av restlassene til $1, T, \ldots, T^{n-1}$ modulo f, til elementene $u, Tu, \ldots, T^{n-1}u$. Men disse elementene i $L_A(f)$ danner en A-modul basis for

$L_A(f)$ ved Setning 2.3. Avbildningen 2.6.1 er derfor en isomorfi av A-moduler, og derfor en isomorfi av $A[T]$-moduler.

Bruker vi isomorfien 2.6.1 kan vi vise at Korollaret 2.4 følger av Setning 2.3 uten å bruke *Euklids algoritme*. Dette er en mer naturlig måte å vise Korollar 2.4 på. Grunnen til at vi velger en annen vei er at vi vil unngå bruken av restklassringen. På den andre siden er dette litt av en illusjon ettersom Euklids algoritme oftest brukes til å vise $A[T]/(f)$ er en fri A-modul.

3 Lineære rekursjoner over kropper

Det vesentlige skillet mellom teorien for lineære rekursjonsrelasjoner over ringer og kropper er at vi over kropper har tilgang til *minimalpolynomer*. I denne seksjonen definerer vi minimalpolynomer for samlinger av lineære avbildninger og gir de viktigste resultatene om minimalpolynomer.

3.1 Idealer. La K være en *kropp*. Da vil polynomringen $K[T]$ være et *prinsipalidealområde*. Det vil si, for hver *undergruppe* $\mathcal{I} \neq 0$ av $K[T]$ slik at $hg \in \mathcal{I}$ for alle $g \in \mathcal{I}$ og $h \in K[T]$, finnes det et *entydig* monisk polynom f i $K[T]$ slik at $\mathcal{I} = (f)$. En undergruppe $\mathcal{I}$ med egenskapen ovenfor kalles et *ideal* i $K[T]$.

3.2 Minimalpolynom. For hver undermengde S av L_K skriver vi

$$\mathcal{I}_S = \{g \in K[T] : gx = 0 \quad \text{for alle} \quad x \in S\},$$

eller ekvivalent

$$\mathcal{I}_S = \{g \in K[T] : S \subseteq L_K(g)\}. \tag{3.2.1}$$

Det er klart at $\mathcal{I}_S$ er et ideal i $K[T]$.

Om $\mathcal{I}_S \neq 0$ betegner vi med f_S det entydige moniske polynomet slik at $\mathcal{I}_S = (f_S)$ og vi kaller f_S for *minimalpolynomet* for S. Det er klart at

$$S \subseteq L_K(f_S). \tag{3.2.2}$$

Om $S = \{x\}$ har S alltid et minimalpolynom siden $x \in L_K(f)$ for et monisk polynom f. Vi skriver da $f_S = f_x$ og kaller f_x for *minimalpolynomet* for x.

3.3 Lemma. *La S være en undermengde av L_K.*

1. *S har et minimalpolynom hvis og bare hvis det finnes et monisk polynom $f \in K[T]$ slik at $S \subseteq L_K(f)$. Når dette holder vil f_S dele f.*
2. *Om $S = L_K(f)$ vil $f_S = f$.*

Bevis. Første delen av (1) følger umiddelbart av uttrykket (3.2.1) for $\mathcal{I}_S$ og definisjonen av minimalpolynom. At f_S deler f følger da av definisjonen på minimalpolynomet f_S.

Av (3.2.2) har vi at når $S = L_K(f)$ vil $L_K(f) \subseteq L_K(f_S)$. Men av Korollar 2.4 har vi at $L_K(f) \subseteq L_K(f_S)$ medfører at f deler f_S, så vi har $f_S = f$, det vil si, utsagnet (2) holder. □

Eksempel IV. Vi viser hvordan vi kan bruke Lemma 3.3 til å bestemme minimalpolynomene til de lineære avbildningene i Eksemplene I, II og III. La f_i være minimalpolynomet for den lineære avbildningen som tilsvarer sekvens nummer i. Av Lemma 3.3 følger at minimalpolynomet til en lineæravbildning x i $L_K(f)$ deler f. Av $f = (T-1)(T^2+1) = (T-1)(T+1)^2$ ser vi derfor med det samme at $f_{\rm I} = 1$, $f_{\rm VIII} = T-1$, $f_{\rm II} = T^2+1 = f_{\rm VII}$, og at $f_{\rm III}, f_{\rm IV}, f_{\rm V}$ og $f_{\rm VI}$ alle er f.

Følgende resultat er *klassisk* og ryktet sier at det var kjent for L. Kronecker.

3.4 Proposisjon. *La $x \in L_K$ og la f være et monisk polynom i $K[T]$. Da vil*

$$L_K(f) = K[T]x$$

hvis og bare hvis $f = f_x$.

Bevis. Ved definisjonen av $\mathcal{I}_{\{x\}} = (f_x)$ vil $\mathcal{I}_{\{x\}}$ være kjernen i den surjektive avbildningen $K[T] \to K[T]x$ som avbilder g til gx. Derfor har vi en isomorfi $K[T]/(f_x) \to K[T]x$ fra restklasseringen av $K[T]$ modulo f_x til $K[T]x$. Spesielt har vektorrommet $K[T]x$ dimensjon lik graden til f_x. Av Lemma 2.1 følger det at dimensjonen til $L_K(f_x)$ også er graden til f_x. Ettersom $K[T]x \subseteq L_K(f_x)$ vil derfor $K[T]x = L_K(f_x)$. Vi har dermed vist at om $f = f_x$ så vil $L_K(f) = K[T]x$.

Omvendt, anta at $L_K(f) = K[T]x$. Da vil spesielt $fx = 0$ så det følger av Lemma 3.3 (1) at f_x deler f. Vi har alltid at $K[T]x \subseteq L_K(f_x)$, så vi får at $L_K(f) \subseteq L_K(f_x)$. Derfor følger det av Korollar 2.4 at f deler f_x. Derfor er $f = f_x$, som vi ville vise. □

Eksempel V. Vi bruker Eksemplene I-IV for å illustrere Proposisjon 3.4. La u i $L_K(f)$ tilsvare sekvensen $0,0,1,1,0,0,1,1,\dots$, så $f_u = f_{\rm III} = f$. Vi har at de lineære avbildningene u, Tu, T^2u, T^3u tilsvarer sekvensene III, IV, VI og V respektive, og at $u+Tu$ og $Tu+T^2u$ tilsvarer sekvensene II, respektive VII. Til slutt svarer $u+T^2u$ til sekvensen VIII. Vi har derfor at $L_K(f) = K[T]u$ som påstått i Proposisjon 3.4.

La x i $L_K(f)$ tilsvare sekvensen II: $0,1,0,1,0,1,0,1,\dots$ så $f_x = f_{\rm II} = T^2+1$. Da vil $T^ix = x$ for $i = 0,2,4,\dots$ og $T^ix = y$ for $i = 1,3,5,\dots$, der y er den lineære avbildningen som tilsvarer VII: $1,0,1,0,1,0,1,0,\dots$. Derfor vil $K[T]x = L_K(T^2+1)$ og ikke $L_K(f)$, som også er påstått i Proposisjon 3.4.

Følgende resultat ble brukt av M. Ward i ulike former og vist over endelige kropper av N. Zierler [Z].

3.5 Lemma. *La $f_1, \dots, f_m$ i $K[T]$ være moniske polynomer.*

1. *Om f er minste felles multiplum av $f_1, \dots, f_m$ vil*

$$L_K(f) = L_K(f_1) + \cdots + L_K(f_m).$$

2. *Om g er største felles divisor i $f_1, \dots, f_m$ vil*

$$L_K(g) = L_K(f_1) \cap \cdots \cap L_K(f_m).$$

Bevis. (1) Vi har at f_i deler f så vi får av Korollar 2.4 at $L_K(f_i) \subseteq L_K(f)$ og derfor en inklusjon $L_K(f_1) + \cdots + L_K(f_m) \subseteq L_K(f)$.

For å vise den omvendte inklusjonen bruker vi at polynomene $f/f_1, \ldots, f/f_m$ i $K[T]$ er innbyrdes primiske. Det finnes derfor polynomer $g_1, \ldots, g_m$ i $K[T]$ slik at $g_1 f/f_1 + \cdots + g_m f/f_m = 1$. La $x \in L_K(f)$. For hvert i har vi $f_i(g_i f/f_i)x = g_i f x = 0$ så $(g_i f/f_i)x \in L_K(f_i)$. Av $x = (g_1 f/f_1)x + \cdots + (g_m f/f_m)x$ følger det derfor at $x \in L_K(f_1) + \cdots + L_K(f_m)$, så vi har vist at $L_K(f) \subseteq L_K(f_1) + \cdots + L_K(f_m)$.

(2) Vi har at g deler f_i så vi får av Korollar 2.4 at $L_K(g) \subseteq L_K(f_i)$. Derfor har vi en inklusjon $L_K(g) \subseteq L_K(f_1) \cap \cdots \cap L_K(f_m)$.

For å vise den omvendt inklusjonen bruker vi at polynomene $f_1/g, \ldots, f_m/g$ er innbyrdes primiske i $K[T]$. Det finnes derfor polynomer $h_1, \ldots, h_m$ i $K[T]$ slik at $1 = h_1 f_1/g + \cdots + h_m f_m/g$. La $x \in L_K(f_1) \cap \cdots \cap L_K(f_m)$. For hvert i har vi $g(h_i f_i/g)x = h_i f_i x = 0$ så $(h_i f_i/g)x \in L_K(g)$. Av $x = (h_1 f_1/g)x + \cdots + (h_m f_m/g)x = 0$ ser vi at $x \in L_K(f)$ så vi har vist at $L_K(f_1) \cap \cdots \cap L_K(f_m) \subseteq L_K(g)$. □

Følgende resultat ble vist og brukt av Zierler [Z] over endelige kropper. Spesielt er da S endelig.

3.6 Setning. *La $S \subseteq L_K$. Da er $S = L_K(f)$ for noe monisk polynom f i $K[T]$ hvis og bare hvis S er en endelig generert $K[T]$-modul.*

Bevis. Vi har sett i Lemma 2.1 at om $S = L_K(f)$ så er S en $K[T]$-modul som er endelig generert som K-modul, og derfor en endelig generert $K[T]$-modul.

Omvendt, om S er en endelig generert $K[T]$-modul vil $S = K[T]y_1 + \cdots + K[T]y_m$ for noen $y_1, \ldots, y_m$ i L_K. La $f_i = f_{y_i}$. Av Proposisjon 3.4 vil $K[T]y_i = L_K(f_i)$ for $i = 1, \ldots, m$. Derfor er $S = L_K(f_1) + \cdots + L_K(f_m)$. Det følger av Lemma 3.5 at $S = L_K(f)$ der f er minste felles multiplum av $f_1, \ldots, f_m$. □

4 Multigrammer

For å illustrere hvordan det *duale* synspunktet på lineære avbildninger gjør det mulig, og naturlig, å generalisere teorien for løsningene til linære rekursjonsrelasjoner behandler vi i denne seksjonen *multigrammer* ganske detaljert.

4.1 Notasjon. La K være en kropp og la $f(T) = T^n - c_1 T^{n-1} + \cdots + (-1)^n c_n$ være i $K[T]$. For alle x i $L_K(f)$ skriver vi

$$x_i = x(T^i) \quad \text{for} \quad i = 0, 1, \ldots.$$

4.2 Definisjon. La $0 \leq l_1 < \cdots < l_m$ være heltall. *Multigrammet*

$$\mathcal{M}_f = \mathcal{M}_f(l_1, \ldots, l_m)$$

til $L_K(f)$ tilsvarende $l_1, \ldots, l_m$ består av m'tuplene $(x_{l_1}, \ldots, x_{l_m})$ for alle x i $L_K(f)$.

Eksempel VI. For å forstå multigrammer er det viktig å se på eksempler. Her bruker vi de lineære avbildningene i Eksemplene I-V til å gi noen multigrammer

for ulike m og $l_1, \dots, l_m$. Vi har

$$\begin{aligned}
\mathcal{M}_f(0,1,2) &= \{(0,0,0),(0,1,0),(0,0,1),(0,1,1),(1,0,0),(1,1,0),(1,0,1),(1,1,1)\}\\
\mathcal{M}_f(0,2,3) &= \{(0,0,0),(0,0,1),(0,1,1),(0,1,0),(1,0,1),(1,0,0),(1,1,0),(1,1,1)\}\\
\mathcal{M}_f(0,2,4) &= \{(0,0,0),(0,0,0),(0,1,0),(0,1,0),(1,0,1),(1,0,1),(1,1,1),(1,1,1)\}\\
\mathcal{M}_f(0,1) &= \{(0,0),(0,1),(0,0),(0,1),(1,0),(1,1),(1,0),(1,1)\}\\
\mathcal{M}_f(0,4) &= \{(0,0),(0,0),(0,0),(0,0),(1,1),(1,1,),(1,1,),(1,1)\}.
\end{aligned}$$

4.3 Bemerkning. Vi regner m'tuplene i $\mathcal{M}_f$ med *multiplisitet*. Det følger av Setning 2.3 at vektorene $u, Tu, \dots, T^{n-1}u$ genererer $L_K(f)$. Derfor vil den underliggende mengden til $\mathcal{M}_f$ bestå av *rekkerommet* til matrisen

$$\begin{pmatrix} u_{l_1} & u_{l_2} & \dots & u_{l_m} \\ u_{l_1+1} & u_{l_2+1} & \dots & u_{l_m+1} \\ \vdots & \vdots & \ddots & \vdots \\ u_{l_1+n-1} & u_{l_2+n-1} & \dots & u_{l_m+n-1} \end{pmatrix}. \tag{4.3.1}$$

Om vi for hvert m'tuppel $(a_1, \dots, a_m)$ i rekkerommet til (4.3.1) skriver

$$L_f(a_1, \dots, a_m) = \{x \in L_K(f) : (x_{l_1}, \dots, x_{l_m}) = (a_1, \dots, a_m)\}$$

så vil det følgelig være en bijeksjon mellom elementene i $L_K(a_1, \dots, a_m)$ og forekomsten av m'tuplet $(a_1, \dots, a_m)$ i $\mathcal{M}_f$.

Eksempel VII. Vi gir her matrisene (4.3.1) tilsvarende multigrammene i Eksempel VI. Betegn matrisen (4.3.1) med $\mathcal{U}_f(l_1, \dots, l_m)$. Vi har

$$\begin{aligned}
\mathcal{U}_f(0,1,2) &= \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)\\
\mathcal{U}_f(0,2,3) &= \left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)\\
\mathcal{U}_f(0,2,4) &= \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)\\
\mathcal{U}_f(0,1) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)\\
\mathcal{U}_f(0,4) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{smallmatrix}\right)
\end{aligned}$$

4.4 Proposisjon. *Vi har at $L_f(0, \dots, 0)$ er et underrom av L_K av dimensjon $n-r$, der n er graden til f og r er rangen til matrisen (4.3.1). Videre har vi, for hver lineær avbildning x i $L_f(a_1, \dots, a_m)$, at*

$$L_f(a_1, \dots, a_m) = x + L_f(0, \dots, 0).$$

Bevis. La V være rekkerommet til matrisen (4.3.1). Vi har en surjektiv homomorfi $L_K(f) \to V$ som avbilder x til $(x_{l_1}, \dots, x_{l_m})$. Den første delen av proposisjonen følger av at $L_f(0, \dots, 0)$ er kjernen i denne avbildningen.

Påstanden i den andre delen er at $L_f(a_1, \dots, a_m)$ er restklassen til x modulo $L_f(0, \dots, 0)$ når $(x_{l_1}, \dots, x_{l_m}) = (a_1, \dots, a_m)$. Det er klart at denne påstanden holder. □

4.5 Bemerkning. Av Proposition 4.4 følger det at multiplisiteten til hvert element i $\mathcal{M}_f$ er lik *antallet* elementer i $L_f(0,\dots,0)$. Mer presist, for hvert m'tuppel $(a_1,\dots,a_m)$ i rekkerommet til matrisen (4.3.1) er det en bijeksjon mellom medlemmene i $\mathcal{M}_f$ som er lik $(a_1,\dots,a_m)$ og $L_f(0,\dots,0)$.

Ettersom dimensjonen til $L_f(0,\dots,0)$ er $n-r$ vil multiplisiteten til hvert element i $\mathcal{M}_f$ være *minimal* når r er *maksimal*, det vil si når $r=m$.

4.6 Definisjon. Vi sier at multigrammet $\mathcal{M}_f=\mathcal{M}_f(l_1,\dots,l_m)$ er *skjevt* om rangen r til matrisen (4.3.1) er strikt mindre enn m.

Eksempel VIII. Vi bruker Eksemplene I-VII til å illustrere Proposisjon 4.4 og Bemerkning 4.5, og for å motivere Definisjon 4.6. La $m_f(l_1,\dots,l_m)$ være multiplisiteten til elementene i $\mathcal{M}_f(l_1,\dots,l_m)$ og la $r_f(l_1,\dots,l_m)$ være rangen til matrisen $\mathcal{U}_f(l_1,\dots,l_m)$. Vi får

m	(l_1,l_2,l_3)	$r_f(l_1,l_2,l_3)$	$n-r_f(l_1,l_2,l_3)$	$m_f(l_1,l_2,l_3)$	$m-r$
3	$(0,1,2)$	3	0	1	0
3	$(0,2,3)$	3	0	1	0
3	$(0,2,4)$	2	1	2	1
2	$(0,1)$	2	1	2	0
2	$(0,4)$	1	2	4	1

4.7 Setning. *Multigrammet $\mathcal{M}_f=\mathcal{M}_f(l_1,\dots,l_m)$ er skjevt hvis og bare hvis det finnes elementer $a_1,\dots,a_m$ i K slik at f deler polynomet $g=a_1T^{l_1}+\cdots+a_mT^{l_m}$.*

Bevis. Ettersom rekkerangen og søylerangen til en matrise sammenfaller er $\mathcal{M}_f$ skjevt hvis og bare hvis søylene i (4.3.1) er lineært avhengige, det vil si, hvis og bare hvis det finnes elementer $a_1,\dots,a_m$ i K slik at

$$a_1\begin{pmatrix} u_{l_1}\\ u_{l_1+1}\\ \vdots\\ u_{l_1+n-1}\end{pmatrix}+\cdots+a_m\begin{pmatrix} u_{l_m}\\ u_{l_m+1}\\ \vdots\\ u_{l_m+n-1}\end{pmatrix}=0,$$

eller ekvivalent, $a_1u_{l_1+i}+\cdots+a_mu_{l_m+i}=0$ for $i=0,\dots,n-1$. Det følger av Setning 2.3 at de lineære avbildningene $u,Tu,\dots,T^{n-1}u$ genererer $L_K(f)$. Derfor vil

$$a_1x_{l_1+i}+\cdots+a_mx_{l_m+i}=0\quad\text{for}\quad i=0,1,\dots\quad\text{for alle}\quad x\in L_K(f).$$

Dette betyr at x er i $L_K(g)$ for alle $x\in L_K(f)$, det vil si, $L_K(f)\subseteq L_K(g)$. Men ved Korollar 2.4 er $L_K(f)\subseteq L_K(g)$ ekvivalent med at f deler g. Vi har derfor vist at $\mathcal{M}_f$ er skjevt hvis og bare hvis det finnes $a_1,\dots,a_m$ slik at $L_K(f)\subseteq L_K(g)$ med $g=a_1T^{l_1}+\cdots+a_mT^{l_m}$. □

4.8 Bemerkning. Ordet *multigram* ble innført av Selmer i tilfellet da K er en *endelig kropp*. Om K har q elementer består da multigrammet $\mathcal{M}_f$ av q^n vektorer, *innregnet multiplisiteten*. Rekkerommet til matrisen (4.3.1) består av q^r vektorer der r er rangen til matrisen, så multiplisiteten til hver vektor er q^{n-r}. Når $\mathcal{M}_f$ *ikke* er skjev vil multiplisiteten derfor være q^{n-m}.

Setningen 4.7 ble funnet eksperimentelt av Selmer og bevist i [L1] og [L2] (se også [S]).

Eksempel IX. Vi viser at Eksempel VIII er en utmerket illustrasjon på Setning 4.7. Polynomet $f = T^3 - T^2 + T - 1$ deler opplagt ikke polynomene på formen $a_1 + a_2T + a_3T^3$, eller $b_1 + b_2T$. Dette betyr av Setning 4.7 at $\mathcal{M}_f(0, 2, 3)$, respektive $\mathcal{M}_f(0, 1)$ ikke er skjeve, hvilket vi også ser av tabellen i Eksempel VII.

På den annen side er $T^4 - 1 = (T - 1)(T^3 - T^2 + T - 1)$ så f deler $T^4 - 1$. Av Setning 4.7 betyr dette at $\mathcal{M}_f(0, 2, 4)$ og $\mathcal{M}_f(0, 4)$ er skjeve, hvilket bekreftes av tabellen i Eksempel VII.

5 Periodiske sekvenser

I de arbeidene vi refererer til er de lineære sekvensene gitt over den endelige kroppen $\mathrm{GF}(q)$ med q elementer. Alle sekvensene som tilfredsstiller en lineær rekursjon blir da *periodisk* fra et visst punkt av. Dette spiller en stor rolle for teknikkene og teorien i disse arbeidene. Som vi har observert spiller dette ikke noen rolle i vår teori. Det kan imidlertid være vært å nevne *periodisitet* for å se relasjonen mellom presentasjonen av lineære rekursjonsrelasjoner her og den i tidligere arbeider. I det følgende setter vi for hver x i $L_A(0)$,

$$x_i = x(T^i) \quad \text{for} \quad i = 0, 1, \ldots.$$

5.1 Definisjon. Et element $x \in L_A(0)$ er har *preperiode* m og *en periode* q om

$$x_{i+q} = x_i \quad \text{for} \quad i \geq m.$$

Det minste positive tallet q som er en periode kalles *perioden* for x, og om $m = 0$ sier vi at x er *periodisk*.

5.2 Lemma. *Om q er en periode for en sekvens x i $L_A(0)$ med periode p vil p dele q.*

Bevis. Vi har $x_{i+p} = x_i$ for $i \geq m_p$ og $x_{i+q} = x_i$ for $i \geq m_q$ for noen preperioder m_p og m_q, og $q \geq p$. Skriv $q = sp + r$ med q og r heltall og $0 \leq r < p$. Vi får for $i \geq \mathrm{maks}(m_p, m_q)$ at $x_{i+r} = x_{i+r+sp} = x_{i+q} = x_i$. Derfor er r enten lik 0 eller r er en periode. Men p var den minste perioden så $r = 0$. Det vil si, p deler q. □

5.3 Lemma. *Sekvensen x i $L_A(0)$ har preperiode m og en periode q hvis og bare hvis $x \in L_A(T^m(T^q - 1))$. Spesielt er $x \in L_A$.*

Bevis. Betingelsen $x_{i+q} = x_i$ for $i \geq m$ kan klart skrives som $T^m(T^q - 1)x = 0$ fordi dette betyr at $T^{m+q}x(T^i) = T^m x(T^i)$, eller $x_{m+q+i} = x_{m+i}$ for $i = 0, 1, \ldots$. □

5.4 Proposisjon. *Om u i $L_A(f)$ har preperiode m og periode q så har alle sekvensene i $L_A(f)$ preperiode m og periode q.*

Bevis. Proposisjonen følger av at elementene $u, Tu, \dots, T^{n-1}u$ ifølge Setning 2.3 genererer A-moduler $L_A(f)$, og alle disse elementene har en preperiode m og en periode q. □

5.5 Proposisjon. *La $f = T^n - c_1T^{n-1} + \cdots + (-1)^n c_n$ og anta at alle sekvensene x i $L_A(f)$ har en preperiode m_x og en periode q_x. Da er alle sekvensene i $L_A(f)$ periodiske hvis og bare hvis c_n ikke er en null divisor, det vil si $ac_n = 0$ medfører at $a = 0$.*

Bevis. La x være en lineær avbildning i $L_A(f)$ og la $m = m_x$ være den minste preperioden for x og la $q = q_x$ være en periode. Vi skal vise at $m = 0$. Anta at $m > 0$. Ettersom $x_{i+q} = x_i$ for $i = m, m+1, \dots$ får vi av $x_{n+m-1+q} - c_1x_{n+m-1+q-1} + \cdots + (-1)^{n-1}c_{n-1}x_{m+q} + (-1)^n c_n x_{m-1+q} = 0$ at $x_{n+m-1} - c_1x_{n+m-2} + \cdots + (-1)^{n-1}c_{n-1}x_m + (-1)^n c_n x_{m-1+q} = 0$.

På den annen side har vi

$$x_{n+m-1} - c_1x_{n+m-2} + \cdots + (-1)^{n-1}c_{n-1}x_m + (-1)^n c_n x_{m-1} = 0.$$

Det følger at $c_n x_{m-1+q} = c_n x_{m-1}$. Antar vi derfor at c_n ikke er en nulldivisor får vi at $x_{m-1+q} = x_{m-1}$. Derfor er $x_{i+q} = x_i$ for $i = m-1, m, \dots$ så $m-1$ er en preperiode. Men dette motsier antagelsen at $m = m_x$ er den minste preperioden for x. Derfor er $m_x = 0$ som vi ville vise.

Omvendt, anta at c_n er en nulldivisor, og la $a \neq 0$ i A være slik at $ac_n = 0$. Da vil $a, 0, 0, \dots$ være en sekvens som svarer til en linearavbildning x i $L_A(f)$, og denne lineæravbildningen har minste preperiode 1 og periode 1. □

Eksempel X. I alle Eksemplene I-V har vi en kropp K med to elementer og $c_n = 1$. Derfor er alle lineære avbildningene i disse eksemplene periodiske.

6 Relasjon til andre metoder

Det *duale synspuktet* på lineære rekursjonsrelasjoner passer vel inn med tidligere metoder. Her gir vi de eksakte relasjonene mellom metodene.

6.1 Potensrekker. Vi betegner med $A[[T]]$ de *formelle potensrekkene* $a_0 + a_1T + \cdots$ i den variable T med koeffisienter i den kommutative ringen A med enhet. Potensrekkene adderes *komponentvis* og *multiplikasjonen* er den vanlige

$$(a_0+a_1T+\cdots)(b_0+b_1T+\cdots) = a_0b_0+(a_1b_0+a_0b_1)T+(a_2b_0+a_1b_1+a_0b_2)T^2+\cdots .$$

Det er vært å merke seg at vi kan *dividere* med alle potensrekker $a_0 + a_1T + \cdots$ der a_0 er *invertibel* i A. Dette sees ved ren *utregning*, det vil si, vi prøver

$$(a_0 + a_1T + \cdots)(x_0 + x_1T + \cdots) = 1$$

og får ligninger $a_0x_0 = 1$ og

$$x_ia_0 + x_{i-1}a_1 + \cdots + x_0a_i = 0 \quad \text{for} \quad i = 1, 2, \dots,$$

for $x_0, x_1, \dots$. Disse har klart en entydig løsning for $x_0, x_1, \dots$ når $a_0, a_1, \dots$ er gitt og a_0 er invertibel. For eksempel vil

$$x_0 = a_0^{-1}, x_1 = -a_0^{-2}a_1, x_2 = a_0^{-3}(a_1^2 - a_0a_2), x_3 = -a_0^{-4}(a_1^3 - 2a_0a_1a_2 + a_0^2a_3).$$

6.2 Potensrekker og sekvenser. De fleste metodene for å behandle lineære rekursjoner bruker at det er en entydig korrespondanse mellom sekvenser av elementer i A og formelle potensrekker med koeffisienter i A, ved at sekvensen $x_0, x_1, \dots$ svarer til den formelle potensrekken $x_0 + x_1T + \cdots$. Tilsvarende har vi en bijeksjon

$$L_K(0) \longleftrightarrow A[[T]]$$

som avbilder x til $x_T = x(1) + x(T)T + x(T^2)T^2 + \cdots$. I det følgende skal vi, for hver $x \in L_K(0)$, skrive

$$x(T^i) = x_i \quad \text{for} \quad i = 0, 1, \dots.$$

6.3 Bemerkning. Med notasjonen i Seksjon 2.2 setter vi

$$u_f = u = (u_0, u_1, \dots) = (0, \dots, 0, 1, s_1, s_2, \dots)$$

med $n-1$ nuller i begynnelsen. Da kan relasjonen $fu = 0$ skrives som

$$(1 - c_1T + \cdots + (-1)^nc_nT^n)(1 + s_1T + s_2T^2 + \cdots) = 1.$$

Dette er samme relasjon som gir sammenhengen mellom *Chern klasser* og *Segre klasser* i geometrien. Dette forklarer vår lett bisarre notasjon for lineære rekursjoner med *alternerende* fortegn.

6.4 Potensrekker og lineær rekursjon. La

$$f(T) = T^n - c_1T^{n-1} + \cdots + (-1)^nc_n$$

være i $A[T]$. Vi har

$$\begin{aligned}
&(1 - c_1T + \cdots + (-1)^nc_nT^n)(x_0 + x_1T + x_2T^2 + \cdots) \\
&= x_0 + (x_1 - c_1x_0)T + (x_2 - c_1x_1 + c_2x_0)T^2 + \cdots \\
&+ (x_{n-1} - c_1x_{n-2} + \cdots + (-1)^{n-1}c_{n-1}x_0)T^{n-1} \\
&+ (x_n - c_1x_{n-1} + \cdots + (-1)^nc_nx_0)T^n + \cdots.
\end{aligned}$$

Gitt $a_0 + a_1T + \cdots$ i $A[[T]]$. Ligningene

$$\begin{aligned}
&x_0 = a_0, x_1 - c_1x_0 = a_1, x_2 - c_1x_1 + c_2x_0 = a_2, \dots, \\
&x_{n-1} - c_1x_{n-2} + \cdots + (-1)^{n-1}c_{n-1}x_0 = a_{n-1}, \\
&x_n - c_1x_{n-1} + \cdots + (-1)^nc_nx_0 = a_n, \dots
\end{aligned}$$

har klart en entydig løsning i $x_0, x_1, \dots$. Derfor vil avbildningen

$$L_K(0) \to A[[T]] \tag{6.4.1}$$

som avbilder x til $(1 - c_1T + \cdots + (-1)^n c_n T^n)x_T$ være en bijeksjon. Videre ser vi at denne bijeksjonen induserer en bijeksjon

$$L_K(f) \longleftrightarrow \{\text{polynomer av grad høyst} \quad n-1 \quad \text{i} \quad A[T]\}.$$

6.5 Ward and Halls metoder. Den metoden som ofte ble anvendt av M. Hall [H1]–[H2] og Ward [W1]–[W4] bruker isomorfien

$$A[T]/(f) \to L_A(f)$$

som avbilder restklassen til $a_0T^{n-1} + \cdots + a_{n-1}$ til den lineære avbildningen x som tilfredsstiller

$$(1 + c_1T + \cdots + (-1)^n c_n T^n)x_T = a_0 + a_1T + \cdots + a_{n-1}T^{n-1}. \tag{6.5.1}$$

6.6 Zierlers metode. Metoden som Zierler bruker [Z] bygger direkte på korrespondansen (6.4.1) mellom sekvenser og potensrekker. Det viktigste verktøyet er relasjonen

$$(a_0 + a_1T + \cdots + a_{n-1}T^{n-1})/(1 - c_1T + \cdots + (-1)^n c_n T^n) = x_0 + x_1T + x_2T^2 \cdots$$

i 6.4 mellom polynomer av grad høyst $n-1$ og potensrekker.

6.7 Petersons metode. Denne metoden ble brukt av Peterson i [P] og danner også det teoretiske grunnlaget for arbeidene [L1] og [L2]. Metoden fungerer best for periodiske sekvenser. Vi antar derfor at alle sekvensene i $L_K(f)$ er periodiske med en periode p, det vil si, $x_{i+p} = x_i$ for $i = 0, 1, \dots$. For $x \in L_K(f)$ har vi da

$$x_T = (x_0 + x_1T + \cdots + x_{p-1}T^{p-1})/(1 - T^p).$$

Substituerer vi dette i (6.5.1) får vi

$$\begin{aligned}(a_0 + a_1T + \cdots + a_{n-1}T^{n-1})(1 - T^p) \\ = (1 - c_1T + \cdots + (-1)^n c_n T^n)(x_0 + x_1T + \cdots + x_{p-1}T^{p-1}).\end{aligned} \tag{6.7.1}$$

Substituerer vi $1/T$ for T i (6.7.1) og tar bort *overflødige* nevnere får vi

$$\begin{aligned}(T^p - 1)(a_0T^{n-1} + a_1T^{n-2} + \cdots + a_{n-1}) \\ = f(T)(x_0T^{p-1} + x_1T^{p-2} + \cdots + x_{p-1}).\end{aligned} \tag{6.7.2}$$

Ettersom vi har antatt at alle elementene i $L_K(f)$ er periodiske med periode p vil f dele polynomet $T^p - 1$, så vi får $T^p - 1 = fg$ med g i $A[T]$. Substituerer vi dette i (6.7.2) og forkorter med f får vi

$$g(T)(a_0T^{n-1} + a_1T^{n-2} + \cdots + a_{n-1}) = x_0T^{p-1} + x_1T^{p-2} + \cdots + x_{p-1}.$$

Det er klart at denne relasjonen gir en bijeksjon

$$(g)/(T^p-1) \to L_A(f)$$

mellom elementene i idealet i $A[T]/(T^p-1)$ generert av restklassen til g og $L_A(f)$ ved at klassen til $g(a_0T^{n-1}+a_1T^{n-2}+\cdots+a_{n-1})$ avbildes til elementet x i $L_A(f)$ bestemt av $x_T=(x_0+x_1T+\cdots+x_{p-1}T^{p-1})/(1-T^p)$.

6.8 Klassisk metode. Denne metoden bygger på *partialbrøkoppspaltning*. Ettersom denne er velkjent og notasjonsmessig litt komplisert skal vi bare skisse metoden. Vi antar at $f(T)=(T-b_1)^{m_1}\cdots(T-b_r)^{m_r}$ er en *oppspalting* av polynomet f og at vi har en *partialbrøkoppspaltning*

$$1/f(T)=g_1(T)/(T-b_1)^{m_1}+\cdots+g_r(T)/(T-b_r)^{m_r}.$$

En slik oppspaltning finnes alltid når A er en kropp, eventuelt efter å ha utvidet kroppen så $f(T)$ *splitter* fullstendig. Ved å substituere $1/T$ for T og ta bort *overflødige nevnere* i T får vi

$$\begin{aligned}1/(1-c_1T+\cdots+(-1)^nc_nT^n) &= h_1(T)/(1-b_1T)^{m_1}+\cdots+h_r(T)/(1-b_rT)^{m_r}\\ &= h_1(T)(1+b_1T+b_1^2T^2+\cdots)^{m_1}+\cdots+h_r(T)(1+b_rT+b_r^2T^2+\cdots)^{m_r}\end{aligned}$$

for noen polynomer $h_1,\ldots,h_r$. Multiplisert med polynomet $a_0+a_1T+\cdots+a_{n-1}T^{n-1}$ gir dette x_T uttykt som potenssummer i røttene $b_1,\ldots,b_r$. Vi gir ingen detaljer, men påminner om *Fibonacci tallene* $1,1,2,3,5,8,\ldots$, gitt av den lineære rekursjonen med karakteristisk polynom T^2-T-1. Vi har

$$f(T)=T^2-T-1=(T-\frac{1+\sqrt{5}}{2})(T-\frac{1-\sqrt{5}}{2})=(T-\alpha)(T-\beta).$$

Dette gir

$$\begin{aligned}1/(1-T-T^2) &= (1/(\alpha-\beta))\,(\alpha/(1-T\alpha)-\beta/(1-T\beta))\\ &= \sum_{i=0}^{\infty}\big((\alpha^{i+1}-\beta^{i+1})/(\alpha-\beta)\big)\,T^i.\end{aligned}$$

6.9 Kompanjongmatrisen. Vi kaller $n\times n$-matrisen

$$C=\begin{pmatrix}0&0&\ldots&0&(-1)^{n+1}c_n\\1&0&\ldots&0&(-1)^nc_{n-1}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\ldots&0&-c_2\\0&0&\ldots&1&c_1\end{pmatrix}$$

for *kompanjongmatrisen* til polynomet $f(T)=T^n-c_1T^{n-1}+\cdots+(-1)^nc_n$. Denne matrisen har karakteristisk polynom $f(T)$ og vi ser at

$$\begin{aligned}(6.9.1)\quad &(x_i,x_{i+1},\ldots,x_{n+i-1})C\\ &\quad=(x_{i+1},x_{i+2},\ldots,x_{n+i-1},x_{n+i-1}c_1-x_{n+i-2}c_2+\cdots+(-1)^{n+1}x_ic_n)\end{aligned}$$

slik at vi får de suksessive verdiene i sekvensen $x_0, x_1, \dots$ ved multiplikasjon med kompanjongmatrisen.

6.10 Matrisemetoden. *Cayley-Hamilton's sats* sier at hver $n \times n$-matrise A med karakteristisk polynom $f(T)$ tilfredsstiller ligningen

$$A^n - c_1 A^{n-1} + \cdots + (-1)^n c_n I_n = 0$$

slik at

$$A^{n+i} - c_1 A^{n+i-1} + \cdots + (-1)^n c_n A^i = 0.$$

Ettersom *sporet* $\operatorname{tr}(A) = \operatorname{tr}(a_{ij}) = a_{11} + \cdots + a_{nn}$ av en matrise er *additiv*, det vil si $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$, har vi at

$$\operatorname{tr}(A^{n+i}) - c_1 \operatorname{tr}(A^{n+i-1}) + \cdots + (-1)^n c_n \operatorname{tr}(A^i) = 0.$$

Det vil si,

$$\operatorname{tr}(A^0), \operatorname{tr}(A), \operatorname{tr}(A^2), \dots \tag{6.10.1}$$

er en løsning til den lineære rekursjonen med karakteristisk polynom $f(T)$.

Vi merker at når A har koeffisienter i en kropp K og $f(T)$ splitter fullstendig i en overkropp som $f(T) = (T - b_1) \cdots (T - b_n)$ så er løsningen (6.10.1) nær beslektet til den klassiske metoden i 6.8. Dette er fordi det følger av *Spektralavbildningssatsen* [LST] at det karakteristiske polynomet for A^i er $(T - b_1^i) \cdots (T - b_n^i)$, slik at $\operatorname{tr}(A^i) = b_1^i + \cdots + b_n^i$. Sekvensen (6.10.1) blir altså

$$b_1^0 + \cdots + b_n^0, \quad b_1 + \cdots + b_n, \quad b_1^2 + \cdots + b_n^2, \quad \dots.$$

Et spesialtilfelle av *matrisemetoden* får vi når vi har en kropp K, en overkropp L, og en basis med n elementer for L betraktet som et vektorrom over K. Multiplikasjon med et element b i L gir da, relativt til denne basen, en matrise A_b. Sporet til A_b er, per definisjon, sporet $\operatorname{tr}(b)$ til b. Sekvensen (6.10.1) blir

$$\operatorname{tr}(b^0), \quad \operatorname{tr}(b^1), \quad \operatorname{tr}(b^2), \quad \dots$$

som er en løsning til den lineære rekursjonen med *karakteristisk polynom* lik *minimalpolynomet* for b over K. Arnfinn Laudal forteller at denne løsningen, for endelige kroppsutvidelser, var kjent for gruppen rundt ham i Forsvarsstaben i Norge på 60-tallet, og så vidt han kan huske, skyldes John Johnsen.

6.11 Bemerkning. Sekvensen (6.10.1) gir ikke nødvendigvis interessante løsninger til den lineære rekursjonen med karakteristisk polynom lik det karakteristiske polynomet til A.

La $K = \{0, 1\}$ være kroppen med to elementer og la $C = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ være kompanjongmatrisen til polynomet $T^2 + 1$. Vi har $C^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ så $\operatorname{tr}(C^i) = 0$ for $i = 0, 1, \dots$, og sekvensen (6.10.1) bli null sekvensen $0, 0, 0, \dots$.

Referanser

[H1] Marshall Hall. *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. 44 (1938). 196–218.

[H2] Marshall Hall. *A survey of difference sets.* Proc. Amer. Math. Soc.7 (1956). 975–986.

[L1] Dan Laksov. *Lineær rekursjon* Master Thesis. University of Bergen 1964.

[L2] Dan Laksov. *Linear recurring sequences over finite fields.* Math. Scand. 16 (1965). 181–196.

[LST] Dan Laksov, Lars Svensson & Anders Thorup *The Spectral Mapping Theorem, norms on rings, and resultants.* L'Enseignement Mathématique 46 (2000) 349-358.

[P] Peterson, W. Wesley. *Error-correcting codes* The M.I.T. Press, Cambridge, Mass. John Wiley & Sons, Inc. New York-London 1961.

[S] Ernst S. Selmer. *Linear recurrence relations over finite fields.* Mimeographed notes. Department of Mathematics, Bergen 1966.

[V] N.N. Vorobyov. *The Fibonacci numbers.* Translated and adapted from the first Russian edition (1951) by Norman D. Whaland, Jr., and Olga A. Titelbaum. Survey of Recent East European Mathematical Literature, a project conducted by Alfred L. Putnam and Izaak Wirszup. Topics in Mathematics D. C. Heath and Co. Boston, Mass. 1963.

[VS] *Välj specialarbete i matematik.* Institut Mittag-Leffler. Djursholm, Sweden 1960.

[W1] Morgan Ward. *The algebra of recurring series.* Ann. of Math.32 (1931). 1–9.

[W2] Morgan Ward. *The characteristic number of a sequence of integers satisfying a linear recursion relation.* Trans. Amer. Math. Soc. 33 (1931). 153–165.

[W3] Morgan Ward. *Some arithmetical properties of sequences satisfying a linear recursion relation.* Ann. of Math. 32 (1931).734–738.

[W4] Morgan Ward. *The arithmetical theory of linear recurring series.* Trans. Amer. Math. Soc. 35 (1933). 600–628.

[Z] Zierler, Neal. *Linear recurring sequences.* J. Soc. Indust. Appl. Math. 7 (1959). 31–48.