Hoofdstuk 6

Het karakteristieke polynoom

We herhalen eerst kort de definities van eigenwaarde en eigenvector, nu in een algemene vectorruimte.

Definitie 6.1 Een *eigenvector voor een lineaire transformatie* T van de L-vectorruimte V is een $v \in V$ zodanig dat $v \neq 0$ en $Tv = \lambda v$, voor zekere $\lambda \in L$; deze λ heet de (bij v behorende) *eigenwaarde* voor T. Een *eigenvector voor de matrix* $M \in \mathrm{M}_{n,n}(L)$ is een $0 \neq v \in V$ met $Mv = \lambda v$ voor zekere $\lambda \in L$; die λ heet de (bij v behorende) *eigenwaarde* voor M. De bij een eigenwaarde λ van een transformatie T behorende *eigenruimte* E_λ is de lineaire deelruimte:

$$E_\lambda = \{v \in V : Tv = \lambda v\}.$$

Opmerkingen 6.2 Per definitie is de eigenschap dat v een eigenvector is voor een lineaire transformatie T niet afhankelijk van de keuze van een basis $\mathcal{B}$ voor de vectorruimte V; in het bijzonder zal een eigenvector van T dus een eigenvector zijn voor $M_T^{\mathcal{B}}$, voor elke basis B. Omgekeerd zal een eigenvector voor een $M_T^{\mathcal{B}}$ eigenvector voor T en dus de matrix ten opzichte van elke basis zijn. De ruimte E_λ is dus ook hetzelfde als $\{v \in V : M^{\mathcal{B}}v = \lambda v\}$ voor elke keuze van basis $\mathcal{B}$ voor V en bijbehorende matrix voor T.

Het is duidelijk dat de eigenruimte bij de eigenwaarde 0 de kern van de transformatie (of matrix) is.

Meetkundig, over $\mathbb{R}$, is een vector v eigenvector voor T als zijn beeld een (reëel) veelvoud λv van v zelf is. Is $\lambda > 1$ dan wordt de vector opgeblazen, is $0 < \lambda < 1$ dan wordt v ingekrompen. Met $\lambda = 1$ blijft v invariant. Is $\lambda < 0$ dan wordt v eerst gespiegeld in de oorsprong, waarna hetzelfde geldt met $|\lambda|$ in plaats van λ.

Voorbeeld 6.3 Veronderstel dat A de matrix is van een lineaire transformatie van $\mathbb{Q}^2$ (ten opzichte van de standaardbasis) met

$$A = \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix}.$$

Een berekening leert onmiddellijk dat

$$A\begin{pmatrix} 1 \\ -1 \end{pmatrix} = -2\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad A\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 5\begin{pmatrix} 3 \\ 4 \end{pmatrix}.$$

Er zijn dus twee verschillende eigenwaarden, elk met een 1-dimensionale eigenruimte.

Het is niet moeilijk in te zien wat de eigenwaarden van een lineaire transformatie kunnen zijn. Immers, λ is een eigenwaarde voor T dan en slechts dan als $Tv = \lambda v$ voor een $v \in V$ met $v \neq 0$, dat wil zeggen $(\lambda - T)v = 0$, oftewel $v \in \mathrm{Ker}(\lambda - T)$. Hier is λ de vermenigvuldiging met de scalar λ, en dat schrijven we ook wel als λI, waar $I = \mathrm{id}_V$, de identieke afbeelding op V. Dat geeft de volgende stelling.

Stelling 6.4 *Zij V een eindig-dimensionale L-vectorruimte. Dan is $\lambda \in L$ een eigenwaarde voor T dan en slechts dan als $\mathrm{Ker}(\lambda I - T) \neq \{0\}$, en in dat geval is $E_\lambda = \mathrm{Ker}(\lambda I - T)$ de eigenruimte bij λ voor T.*

Omdat λ eigenwaarde voor T is dan en slechts dan als λ een eigenwaarde is voor $M = M_T^{\mathcal{B}}$, waar $\mathcal{B}$ een basis voor V is, geldt dit dan en slechts dan als $Mv = \lambda v = \lambda I_n v$ voor een $v \in V$ met $v \neq 0$, dat wil zeggen $(\lambda I_n - M)v = 0$, oftewel $v \in \mathrm{Ker}(\lambda I_n - M)$, waar I_n natuurlijk de $n \times n$ eenheidsmatrix is, met $n = \dim V$.

Gevolg 6.5 *Met notaties als boven, en $\mathcal{B}$ een basis voor V, geldt: $\lambda \in L$ is eigenwaarde voor T dan en slechts als $\det(\lambda I_n - M) = 0$, waar $M = M_T^{\mathcal{B}}$.*

Definitie 6.6 Zij $M \in \mathrm{M}_{n\times n}(L)$; het polynoom $p_M(x) = \det(xI_n - M) \in L[x]$ heet het *karakteristieke polynoom* van M.

Lemma 6.7 *Laat $\mathcal{B}$ en $\mathcal{C}$ beiden basis voor de eindig-dimensionale vectorruimte V zijn en T een transformatie van V. Met $B = M_T^{\mathcal{B}}$ en $C = M_T^{\mathcal{C}}$ geldt dan: $p_B = p_C$.*

Bewijs. Er geldt dat $C = \Phi^{-1} \cdot B \cdot \Phi$ voor $\Phi = {}^{\mathcal{B}}M_{\mathrm{id}}^{\mathcal{C}}$. Dan is p_C

$$\det(xI_n - C) = \det(xI_n - \Phi^{-1} \cdot B \cdot \Phi) = \det(\Phi(xI_n - B)\Phi^{-1}) = \det(xI_n - B)$$

(gebruik 5.22) en dat is p_B. Dat wil zeggen: de karakteristieke polynomen van B en C zijn gelijk.

Opmerkingen 6.8 Voor het karakteristieke polynoom doet het er dus niet toe ten opzichte van welke basis we een matrix voor T nemen: we kunnen spreken van *het karakteristieke polynoom van de transformatie T*, dat we met p_T aan zullen geven. Bovendien hebben we bewezen dat $\lambda \in L$ een eigenwaarde voor T is dan en slechts dan als $p_T(\lambda) = 0$.

Met volledige inductie (naar n) is het duidelijk dat p_T een polynoom in $L[x]$ is van graad n. We zullen verderop zien dat daaruit volgt dat T niet meer dan $n = \dim V$ eigenwaarden kan hebben.

Voorbeeld 6.9 Laat

$$A = \begin{pmatrix} 1 & 1 \\ 4 & 1 \end{pmatrix}$$

de matrix van een lineaire transformatie van $\mathbb{Q}^2$ ten opzichte van de standaardbasis zijn. Teneinde de eigenwaarden van A te vinden bepalen we

$$\det(\lambda I_2 - A) = \begin{vmatrix} \lambda - 1 & -1 \\ -4 & \lambda - 1 \end{vmatrix} = (\lambda - 1)^2 - 4 = (\lambda - 3)(\lambda + 1).$$

De eigenwaarden van de bij A horende transformatie zijn dus 3 en -1.

Om E_3 te vinden, moeten we $\mathrm{Ker}(3I_2 - A)$ bepalen:

$$E_3 = \mathrm{Ker}(3I_2 - A) = \mathrm{Ker}\begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = \langle\begin{pmatrix} 1 \\ 2 \end{pmatrix}\rangle.$$

Net zo is E_{-1} de kern van

$$E_{-1} = \mathrm{Ker}\begin{pmatrix} -2 & -1 \\ -4 & -2 \end{pmatrix} = \langle\begin{pmatrix} -1 \\ 2 \end{pmatrix}\rangle.$$

Om de matrix ten opzichte van de basis $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix} \right\}$ in plaats van de standaardbasis te bepalen, kunnen we volgens A conjugeren met de matrix ${}^{\mathcal{E}}M^{\mathcal{B}}_{\mathrm{id}}$ die een vector gegeven in basis $\mathcal{B}$ coordinaten uitdrukt in coordinaten ten opzichte van de standaardbasis:

$$A^{\mathcal{B}} = \left({}^{\mathcal{E}}M^{\mathcal{B}}_{\mathrm{id}}\right)^{-1} \cdot A \cdot {}^{\mathcal{E}}M^{\mathcal{B}}_{\mathrm{id}} = \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix}.$$

Anderzijds weten we natuurlijk al precies wat het resultaat zal zijn: immers $\mathcal{B}$ is een basis bestaande uit eigenvectoren, en omdat de bijbehorende eigenwaarden 3 en -1 zijn zal het resultaat

$$A^{\mathcal{B}} = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}$$

moeten zijn!

Om preciezere uitspraken over eigenruimten te doen kijken we eerst iets beter naar eigenschappen van polynomen.

Intermezzo: Polynoomringen

We vervolgen daarom dit hoofdstuk met een kort intermezzo waarin we belangrijke eigenschappen van ringen, in het bijzonder polynoomringen, samenvatten. Steeds zal L een lichaam zijn, en R een ring, waarvan we (tenzij anders vermeld) zullen aannemen dat deze commutatief met eenheidselement is (waarin elementen anders dan in lichamen niet noodzakelijk een inverse hebben).

Definities 6.10 Een *polynoom over* R van *graad* $n \geq 0$ is een element van $R[x]$, van de vorm $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, waar $a_i \in R$ en $a_n \neq 0$. De a_i uit R zijn de coëfficiënten van het polynoom; gewoonlijk schrijven we alleen termen met $a_i \neq 0$ op, tenzij alle coëfficiënten nul zijn: het *nulpolynoom* waarvoor we 0 schrijven. De graad van 0 is per definitie $-\infty$. De coëfficiënt van x^n heet de *kopcoëfficiënt*. Als de kopcoëfficiënt 1 is noemen we het polynoom *monisch*. De coëfficiënt a_0 heet de *constante coëfficiënt*. Als $a_i = 0$ voor alle $i > 0$ dan heet polynoom een *constant polynoom*. De x in deze uitdrukkingen is de *onbepaalde*, of *variabele*.

Het is belangrijk op te merken dat we polynomen hier niet in de eerste plaats als functies beschouwen, maar als elementen van een ring. Een polynoom $f \in R[x]$ definieert wel een afbeelding $f : R \to R$ omdat we f kunnen *evalueren*: zo is

$f(r) = a_n r^n + \cdots a_1 r + a_0 1 \in R$ voor f als boven. We noemen $f(r)$ ook wel de *waarde van f in r*. Een *nulpunt van f in R* is een $r \in R$ zodanig dat $f(r) = 0$.

Als R een deelring van S is, kunnen we elementen van R via de inbedding ook als elementen van S opvatten; dat betekent dat we in dit geval $f \in R[x]$ ook kunnen evalueren in een $s \in S$: $f(s) \in S$. Zo zul je geen moeite hebben om $f(\pi)$ uit te rekenen als het f het polynoom $x^2 - 1$ met gehele coëfficiënten is. En f kan dus ook nulpunten in de grotere ring S hebben: $x^2 + 1$ heeft geen nulpunten in $\mathbb{Z}$, of $\mathbb{Q}$ of $\mathbb{R}$, maar wel in $\mathbb{C}$.

Voorbeelden 6.11 De belangrijkste voorbeelden van ringen zijn, naast de lichamen, voor ons de volgende.

(0) Om complicaties te voorkomen, zullen we net als in het geval van lichamen, eisen dat een ring tenminste twee verschillende elementen $0, 1$ (de neutrale elementen ten opzichte van optelling vermenigvuldiging) bevat.

(i) De gehele getallen $\mathbb{Z}$, met de gewone optelling en vermenigvuldiging; dit is een commutatieve ring, met eenheidselement.

(ii) De ring $\mathbb{Z}/m\mathbb{Z}$, de restklassenring modulo m, voor een geheel getal $m > 1$, met de gebruikelijke optelling en vermenigvuldiging van restklassen, zoals gedefinieerd in 1.7. Dit is ook steeds een commutatieve ring, met 1.

(iii) Als R een commutatieve ring met 1 is (bijvoorbeeld één van de ringen hierboven, of een lichaam) kun je daaruit een nieuwe *ring $R[x]$ van polynomen met coëfficiënten in R* maken. De operaties zijn de gebruikelijke *optelling van polynomen*:

$$\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

en de *vermenigvuldiging van polynomen*

$$(\sum_{i=0}^{n} a_i x^i) \times (\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i \times b_{k-i}) x^k.$$

Hier nemen we $a_i = 0$ voor alle $i > n$ en $b_j = 0$ voor $j > m$. Deze polynoomring $R[x]$ is zelf weer een commutatieve ring met 1, maar geen lichaam omdat bijvoorbeeld het polynoom x geen inverse heeft.

(iv) Bij elke commutatieve ring met 1 kunnen we ook een nieuwe *ring van $n \times n$ matrices $\mathrm{M}_n(R)$ met coëfficiënten in R* maken: de verzameling bestaat uit vierkante $n \times n$ matrices, en de operaties zijn de gebruikelijke *optelling van matrices*, waar de som van

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

gedefinieerd is door

$$\begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{pmatrix}$$

en *vermenigvuldiging van matrices*, middels het product

$$\begin{pmatrix} \sum_{i=1}^n a_{1i}\cdot b_{i1} & \sum_{i=1}^n a_{1i}\cdot b_{i2} & \cdots & \sum_{i=1}^n a_{1i}\cdot b_{in} \\ \sum_{i=1}^n a_{2i}\cdot b_{i1} & \sum_{i=1}^n a_{2i}\cdot b_{i2} & \cdots & \sum_{i=1}^n a_{2i}\cdot b_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n a_{ni}\cdot b_{i1} & \sum_{i=1}^n a_{ni}\cdot b_{i2} & \cdots & \sum_{i=1}^n a_{ni}\cdot b_{in} \end{pmatrix}$$

Met andere woorden: optellen en vermenigvuldigen van zulke matrices doe je op precies dezelfde manier als waarop je dat eerder hebt gezien in het speciale geval dat alle coëfficiënten uit een lichaam kwamen.
Voor elke $n \geq 1$ krijgen we zo (voor gegeven commutatieve ring R) een ring $\mathrm{M}_n(R)$. Als $n > 1$ is die ring $\mathrm{M}_n(R)$ niet commutatief!

Definities 6.12 Een *ringhomomorfisme* is een afbeelding $f\colon R \to S$ tussen ringen $(R, +, \cdot)$ en $(S, +, \cdot)$ met eenheidselement die voldoet aan de eigenschappen:

(i) $f(1_R) = 1_S$;
(ii) $f(a + b) = f(a) + f(b)$, voor alle $a, b \in R$;
(iii) $f(a \cdot b) = f(a) \cdot f(b)$, voor alle $a, b \in R$.

Een *ringisomorfisme* is een bijectief ringhomomorfisme.

We hebben gezien dat elke ring R (en in het bijzonder elk lichaam) in ieder geval de elementen $0, 1$ moet bevatten. Maar dan moet ook $1+1$ in R zitten, een element dat we gewoonlijk met 2 aangeven. Maar let op: het zou kunnen zijn dat 2 gelijk is aan één van de elementen die we al opschreven: 0 of 1. Maar als $1 + 1 = 1$ dan moet $1 = 0$ (want tel bij beide kanten de tegengestelde -1 op), en dat hebben we juist verboden (in Voorbeeld 6.11(0)). Dus 2 is een nieuw element òf gelijk aan 0. Datzelfde argument kun je herhalen: $1 + 1 + 1 \in R$ komt al voor onder $\{0, 1, 2\}$ òf het is een nieuw element; in het eerste geval moet $1 + 1 + 1 = 0$ (tenzij al gold $1 + 1 = 0$).

Definitie 6.13 Laat R een ring zijn; als er een natuurlijk getal m bestaat zodanig dat $1 + 1 + \cdots + 1 = m \times 1 = 0 \in R$, dan is de *karakteristiek van* R het kleinste positieve natuurlijke getal met die eigenschap; als zo'n m niet bestaat is de karakteristiek per definitie 0.

Als de karakteristiek van R gelijk aan 0 is, dan zijn alle elementen $1, 2, 3, \ldots$ verschillend: er bestaat dan een *injectief ringhomomorfisme* $\mathbb{Z} \to R$. Omgekeerd, als er zo'n injectief homomorfisme bestaat, dan moet de karakteristiek wel 0 zijn.

Vervolgens kijken we naar twee speciale soorten elementen in een ring.

Definities 6.14 Een element r van een (niet noodzakelijk commutatieve) ring R met 1 heet een *eenheid in* R als er een inverse voor r in R bestaat, dat wil zeggen, een element $t \in R$ met $r \times t = t \times r = 1$. De inverse van r geven we meestal met r^{-1} aan.

Een element $r \in R$ heet een *nuldeler in* R als $r \neq 0$ en er een element $s \in R$ bestaat met $s \neq 0$ zodat $r \times s = 0$ of $s \times r = 0$.

Stelling 6.15 *Een eenheid in R (niet noodzakelijk commutatief) is geen nuldeler.*

Bewijs. Laat $r \in R$ een eenheid zijn, en veronderstel dat r ook een nuldeler is. Dan is $r \neq 0$ en we veronderstellen dat er een $s \in R$ is met $s \neq 0$ en $r \times s = 0 \in R$. Omdat r een eenheid is, is er een $t \in R$ met $t \times r = 1$. Dan is

$$s = 1 \times s = (t \times r) \times s = t \times (r \times s) = t \times 0 = 0,$$

dus $s = 0$, in tegenspraak met bovenstaande. Het geval $s \times r = 0$ gaat net zo, door rechts met t te vermenigvuldigen. De aanname dat r een nuldeler is leidt dus tot een tegenspraak.

Voorbeelden 6.16 Een lichaam L is per definitie precies een commutatieve ring met 1 waarin elk niet-nul element een eenheid is; er kunnen dus geen nuldelers in L zijn. Dat laat zien dat de ringen $\mathbb{Z}/m\mathbb{Z}$ voor m die geen priemgetal zijn, geen lichaam zijn: als $m = a \cdot b$, met $a, b > 1$, dan zijn a en b nuldelers in $\mathbb{Z}/m\mathbb{Z}$. Dat $\mathbb{Z}/m\mathbb{Z}$ wél een lichaam is als m een priemgetal is zien we beneden.

Overigens is $\mathbb{Z}$ een voorbeeld van een ring die geen nuldelers heeft maar toch geen lichaam is. Zo'n commutatieve ring met 1 heet een *domein* (of *integriteitsgebied*). Andere voorbeelden zijn $\mathbb{Z}[x]$ en $L[x]$ voor een lichaam L.

Opmerkingen 6.17 Eén van de belangrijkste eigenschappen van $\mathbb{Z}$ is dat elk getal is te schrijven als een teken maal een product van priemgetallen, en die schrijfwijze is op volgorde na uniek (de Hoofdstelling van de Rekenkunde). Ook belangrijk is de eigenschap dat bij elke $n, m \in \mathbb{Z}$ met $m \neq 0$ er unieke $q, r \in \mathbb{Z}$ bestaan zodat: $n = q \cdot m + r$, Met $0 \leq r < |m|$. Deze eigenschappen blijken ook voor veel polynoomringen te gelden, zoals we hieronder zullen zien.

Dat is ook het geval voor het bestaan van een *Euclidisch algoritme*, dat bij m, n (niet beide 0) de grootste gemene deler $g = \text{ggd}(m, n)$ vindt, maar in uitgebreidere vorm ook s, t zodanig dat $s \cdot m + t \cdot n = g$. Het is deze eigenschap die ervoor zorgt dat je bij een *priemgetal* p en een m met $1 \leq m < p$ altijd een inverse van m modulo p kunt vinden: er zijn s, t zodat $s \cdot m + t \cdot p = 1$, oftewel, er is een inverse s van m modulo p omdat $s \cdot m \equiv 1 \bmod p$. Dat laat zien dat de gehele getallen modulo p een lichaam vormen!

We willen nu eerst het begrip *deler* uit $\mathbb{Z}$ generaliseren.

Definities 6.18 Laat R weer een commutatieve ring met 1 zijn. Als $d, f \in R$ dan is d een *deler* van f (notatie $d \mid f$) als er een $q \in R$ bestaat met $f = q \cdot d$; we zeggen ook dat d het element f *deelt*, dat f *deelbaar* is *door* d *in* R, en dat f een *veelvoud* is van d. Een *gemene deler* van $f, g \in R$ is een $d \in R$ die zowel f als g deelt; een *grootste gemene deler van* f *en* g is een gemene deler $d \in R$ van f en g met de eigenschap dat elke andere gemene deler d' een deler van d is. Zo'n grootste gemene deler geven we aan met $\text{ggd}(f, g)$.

Stelling 6.19 *Laat R een commutatieve ring met 1 zijn; bij elke $f, g \in R[x]$, bestaan er polynomen $q, r \in R[x]$ zodat:*

$$f = q \cdot g + r, \qquad \deg r < \deg g;$$

mits de kopcoëfficiënt van g een eenheid in R is; deze q en r zijn uniek bepaald.

Bewijs. Het bestaan van q en r kun je met inductie naar de graad van f bewijzen.

Opmerkingen 6.20 Als g een deler van f is zal $r = 0$, en $\deg r = -\infty$. Dit is altijd het geval als $\deg g = 0$ en g een eenheid is.

Deling met rest is dus voor elke tweetal polynomen in $L[x]$ (over een lichaam L) mogelijk. Net als in $\mathbb{Z}$ kun je dit herhaald gebruiken om een Euclidisch algoritme te krijgen, dat bij $f, g \in L[x]$ een grootste gemene deler d produceert. Bovendien kun je dat algoritme uitbreiden zodat je bij f, g ook polynomen $s, t \in L[x]$ maakt waarvoor $s \cdot f + t \cdot g = \text{ggd}(f, g)$ (als niet f, g beide 0).

Een ander gevolg van deling met rest is de volgende stelling, die uitdrukt dat delers van graad 1 corresponderen met nulpunten van een polynoom.

Stelling 6.21 *Als $a \in R$ en $f \in R[x]$ dan geldt:*

$$x - a \quad \textit{deelt} \quad f \qquad \Longleftrightarrow \qquad f(a) = 0.$$

Bewijs. Als f deelbaar is door $x - a$ dan is $f = q \cdot (x - a)$, voor zekere $q \in R[x]$. Evalueren in a geeft $f(a) = q(a) \cdot 0 = 0 \in R$. Voor de omkering pas je deling met rest toe op f en $g = x - a$: er is een $q \in R$ en een $r \in R[x]$ van graad kleiner dan 1 (dus een constante $r_0 \in R$) zodat $f = q \cdot (x - a) + r_0$. Maar dan is $0 = f(a) = q(a) \cdot 0 + r_0$, dus $r_0 = 0$ en $f = q \cdot (x - a)$ is deelbaar door $(x - a)$.

De stelling geeft dus een eenvoudige methode om te controleren of een polynoom deelbaar is door $x - a$: reken $f(a)$ uit! Als de deling opgaat (dus $f(a) = 0$) zul je nog wel een berekening (bijvoorbeeld een staartdeling) uit moeten voeren om het quotient te vinden.

Definities 6.22 Een element $r \in R$ in een commutatieve ring R zonder nuldelers heet *irreducibel in* R als geldt: $r \neq 0$ en r is geen eenheid maar als $r = s \cdot t$ met $s, t \in R$ dan is s een eenheid of t is een eenheid in R. Als r wel als zo'n product van niet-eenheden is te schrijven heet hij *reducibel*.

Voorbeelden 6.23 In een lichaam is elk element nul of een eenheid en zijn er dus geen irreducibele elementen. In $\mathbb{Z}$ zijn de irreducibele elementen precies de *priemgetallen* en de reducibele elementen de *samengestelde getallen*. In een polynoomring $R[x]$ over een commutatieve ring R zonder nuldelers heten de irreducibele elementen *irreducibele polynomen*. Als $R = L$ een lichaam is, dan zijn de irreducibele elementen de polynomen $f \in R[x]$ met $\deg f \geq 1$ waarvoor geen polynomen $g, h \in R[x]$ bestaan van graad kleiner dan $\deg f$ met $f = g \cdot h$.

Als R geen lichaam is zijn er in het algemeen ook nog irreducibele elementen uit R in $R[x]$ (irreducibele polynomen van graad 0), zoals de priemgetallen in $\mathbb{Z}[x]$.

Stelling 6.24 *Elk monisch polynoom $f \in L[x]$ over een lichaam is te schrijven als product van positieve machten van monische, irreducibele polynomen uit $L[x]$; deze schrijfwijze is uniek op volgorde van de factoren na.*

Opmerkingen 6.25 We geven hier geen bewijs, en volstaan met de opmerking dat er bewijzen voor de Hoofdstelling van de Rekenkunde bestaan die direct kunnen worden gegeneraliseerd voor dit geval.

Een commutatieve ring zonder nuldelers waarin elk element (op volgorde van factoren en vermenigvuldiging met eenheden na) uniek als product van irreducibele elementen geschreven kan worden heet een *factorontbindingsring*. We weten nu dat

$\mathbb{Z}$ en $L[x]$ (voor elk lichaam L) een factorontbindingsring is. Algemener geldt zelfs dat $R[x]$ een factorontbindingsring is als R het zelf is; dus geldt bijvoorbeeld ook in $\mathbb{Z}[x]$ eenduidige priemfactorontbinding. Maar het algemene bewijs is iets lastiger.

Om de stelling te gebruiken zouden we nog graag willen kunnen herkennen wat de irreducibele polynomen zijn in $L[x]$; maar dat hangt sterk af van het lichaam L. De reden dat het lichaam der complexe getallen $\mathbb{C}$ zo'n belangrijke rol speelt is gelegen in het feit (zoals uitgedrukt in de volgende stelling) dat het *algebraïsch afgesloten* is: elke algebraïsche vergelijking over $\mathbb{C}$ heeft een oplossing! We bewijzen deze stelling hier niet.

Stelling 6.26 (Hoofdstelling van de Algebra) *Als $f \in \mathbb{C}[x]$ en $\deg f \neq 0$ dan is er een $z \in \mathbb{C}$ zodat $f(z) = 0$.*

Gevolg 6.27 *Als f een monisch polynoom is dan geldt:*

(i) $f \in \mathbb{C}[x]$ *is irreducibel* $\iff$ $\deg f = 1$*;*

(ii) $f \in \mathbb{R}[x]$ *is irreducibel* $\iff$ $\deg f = 1$ *of* $f = x^2 + bx + c$ *met* $b^2 - 4c < 0$.

Bewijs. Als $f \in \mathbb{C}[x]$ graad groter dan 1 heeft, is er een ontbinding van f van de vorm $f = (x - z) \cdot g$ op grond van 6.21 en 6.26, en dus is f reducibel. Bovendien is over een willekeurig lichaam elk polynoom van graad 1 irreducibel.

Als $f \in \mathbb{R}[x]$ en er is een $r \in \mathbb{R}$ met $f(r) = 0$, dan is, net als boven, f reducibel tenzij f van graad 1 is. Maar zo'n r bestaat niet altijd; wél is er altijd een $z \in \mathbb{C}$ met $f(z) = 0$. Neem nu dus aan dat zo'n $z \in \mathbb{C}$ bestaat met $z \notin \mathbb{R}$; dan is ook $f(\bar{z}) = 0$, en moet f deelbaar zijn door $g = (x-z)(x-\bar{z}) = x^2-(z+\bar{z})x+z\bar{z} \in \mathbb{R}[x]$. Maar $g \mid f$ en f is irreducibel in $\mathbb{R}[x]$, dus $f = g$ en g is irreducibel. Bovendien is $b^2 - 4c = (z + \bar{z})^2 - 4z\bar{z} = (z - \bar{z})^2 < 0$.

Voor een monisch kwadratisch polynoom $f = x^2+bx+c$ geeft de *wortelformule* natuurlijk altijd de twee nulpunten $-b \pm \sqrt{b^2 - 4c}$ en ook daaraan zie je dat f reducibel is over $\mathbb{R}$ als $b^2 - 4c \geq 0$.

Definitie 6.28 De *(algebraïsche) multipliciteit* van een nulpunt $\alpha \in L$ van een polynoom $f \in L[x]$ is de grootste $k \geq 1$ waarvoor $(x - \alpha)^k$ het polynoom f deelt in $L[x]$.

Gevolg 6.29 *Elk polynoom $f \neq 0$ uit $\mathbb{C}[x]$ heeft precies $\deg f$ nulpunten in $\mathbb{C}$ als we de multipliciteiten meetellen.*

Opmerkingen 6.30 Een polynoom in $L[x]$ kan in het lichaam L ten hoogste n nulpunten hebben (geteld met multipliciteiten); als we L door een commutatieve ring R vervangen is dat niet meer waar!

Over $\mathbb{Q}$ bestaan monisch irreducibele polynomen van willekeurige graad $m \geq 1$; de polynomen $x^m - 2$ zijn bijvoorbeeld irreducibel in $\mathbb{Q}[x]$, voor elke $m \geq 1$, maar we hebben nog niet de hulpmiddelen om dat hier te bewijzen.

Een laatste overeenkomst tussen $\mathbb{Z}$ en $L[x]$ ligt in de mogelijkheid tot het vormen van *restklassenringen*.

Omdat we in $L[x]$ deling met rest kunnen toepassen, krijgen we de *restklassenring* $L[x]/f$, voor een $f \in L[x]$ met $\deg f > 0$, die bestaat uit de verzameling equivalentieklassen

$$\bar{g} = \{h \in L[x] : h \equiv g \bmod f\} = \{g + tf : t \in L[x]\}$$

(waar $h \equiv g \bmod f$ dan en slechts dan als f een deler is van $h-g$), voorzien van optelling en vermenigvuldiging, gegeven door: $\bar{g}+\bar{h} = \overline{g+h}$ en $\bar{g}\cdot\bar{h} = \overline{g\cdot h}$. Er geldt weer: $L[x]/f$ is een lichaam dan en slechts dan als f irreducibel is in $L[x]$.

Dit geeft aan hoe *lichaamsuitbreidingen* gemaakt kunnen worden: begin met een lichaam L en vind een irreducibel polynoom $f \in L[x]$, dan is $K = L[x]/f$ een lichaam. Met $L = \mathbb{Q}$ vinden we zo *getallenlichamen*, zoals $\mathbb{Q}[\sqrt{2}]$.

Als L het lichaam $\mathbb{F}_p$ van p elementen is, kunnen we zo een lichaam met p^n elementen construeren door een monisch irreducibel polynoom van graad n over L te vinden. Voor elke p en elke $n \geq 2$ blijkt zo'n polynoom te bestaan; bovendien blijken twee eindige lichamen met evenveel elementen altijd isomorf te zijn.

Cayley-Hamilton

Doel van deze paragraaf is te laten zien dat lineaire transformaties aan zekere algebraïsche vergelijkingen voldoen. Daartoe blijkt het nuttig te zijn om, voor een niet-nul vector w in een eindig-dimensionale L-vectorruimte V waarop een lineaire transformatie T werkt, te kijken naar $w, Tw, T^2w, \ldots$ en in het bijzonder naar lineaire relaties daartussen.

Als Tw lineair afhankelijk is van $w = T^0w$ moet w wel een eigenvector van T zijn. Is Tw onafhankelijk van w, dan kan het zijn dat T^2w lineair afhankelijk is van w en Tw, enzovoorts. We kijken naar de kleinste k waarvoor T^kw lineair afhankelijk is van $w, Tw, T^2w, \ldots, T^{k-1}w$. Omdat de ruimte T_w die wordt opgespannen door alle T^iw, een lineaire deelruimte is van V, bestaat er zo'n k. Bovendien is T_w *invariant* onder T: het is duidelijk dat $T[T_w] \subset T_w$.

Er zijn coëfficiënten $c_0, c_1, \ldots, c_{k-1} \in L$ met

$$T^kw = c_0w + c_1Tw + \cdots + c_{k-1}T^{k-1}w,$$

en hierin zijn een matrix voor T beperkt tot T_w, en diens karakteristieke polynoom, nu eenvoudig uit te drukken.

Lemma 6.31 *Met notatie als boven geldt dat de matrix voor de beperking $T|_{T_w}$ van T tot T_w gegeven wordt door*

$$M_{T|_{T_w}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & c_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \\ 0 & 0 & & \ddots & 0 & 0 & c_{k-3} \\ 0 & 0 & 0 & \cdots & 1 & 0 & c_{k-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{k-1} \end{pmatrix},$$

ten opzichte van de basis $w, Tw, , \ldots, T^{k-1}w$. Bovendien is het karakteristieke polynoom van $T|_{T_w}$ gelijk aan $x^k - c_{k-1}x^{k-1} - \cdots - c_1x - c_0$.

Bewijs De kolommen van de matrix zijn de beelden van de vectoren T^iw, die door T opgeschoven opgeschoven worden, met uitzondering van T^kw, waarvoor we het beeld uit de relatie hierboven aflezen. De vorm van het karakteristiek polynoom volgt met inductie naar k.

Opmerkingen 6.32 De matrix uit het voorafgaande lemma wordt wel de *companion matrix* van het polynoom $x^k - c_{k-1}x^{k-1} - \cdots - c_1x - c_0$ genoemd.

In het volgende willen we uitdrukkingen van de vorm $a_0+a_1T+\cdots+a_{k-1}T^{k-1}$, voor een lineaire transformatie T van V, weer als lineaire transformatie van V opvatten. Het zal duidelijk zijn hoe dit moet:

$$(a_0 + a_1T + \cdots + a_{k-1}T^{k-1})v = a_0v + a_1Tv + \cdots + a_{k-1}T^{k-1}v,$$

een combinatie van vermenigvuldiging met een scalar en het herhaald loslaten van T op een vector. Zo vormen lineaire afbeeldingen een ring, die we wel met $L[T]$ aangeven.

Maken we een basiskeuze, dan kunnen we T door een matrix M_T voorstellen, en de lineaire afbeelding $a_0+a_1T+\cdots+a_{k-1}T^{k-1}$ door $a_0+a_1M_T+\cdots+a_{k-1}M_T^{k-1}$. We krijgen dan een ring $L[M_T]$, die een deelring is van $\mathrm{M}_{n\times n}(L)$.

Lemma 6.33 *Als U een onder T invariante deelruimte van V is, dan is $p_{T|_U}$, het karakteristieke polynoom van de beperking van T tot U, een deler van p_T.*

Bewijs. Vul een basis voor U aan tot een basis voor V; dan wordt T ten opzichte van die basis gegeven door de matrix

$$M = \begin{pmatrix} B & A \\ 0 & C \end{pmatrix},$$

waar B de matrix voor de beperking $T|_U$ is. De bewering volgt dan omdat $\det(\lambda I_n - M) = \det(\lambda I_k - B)\det(\lambda I_{n-k} - C)$.

Stelling 6.34 [Cayley-Hamilton] *Voor een lineaire transformatie T van een eindig-dimensionale vectorruimte V geldt $p_T(T) = 0$. Bovendien geldt, als M_T een matrix voor T is ten opzichte van een basis voor V, dat $p_T(M_T) = 0$. Dat wil zeggen: T en M_T voldoen aan hun eigen karakteristieke vergelijking.*

Bewijs. Om te laten zien dat $p_T(T) = 0$ (de nulafbeelding), moeten we laten zien dat $p_T(T) : v \mapsto 0$ voor elke $v \in V$.

Als $v = 0$, dan is $p_T(T)(0) = 0$, want dat geldt voor elke lineaire afbeelding.

Als $v \neq 0$, bekijk dan T_v, de ruimte opgespannen door $v, Tv, T^2v, \ldots$. Dit is een lineaire deelruimte van V, en daarom eindig-dimensionaal, zeg $\dim T_v = k$. Dan bestaan er coëfficiënten $c_0, c_1, \ldots, c_{k-1}$ in L zodat

$$T^kv = c_0v + c_1Tv \cdots + c_{k-1}T^{k-1}v.$$

Volgens Lemma 6.31 geldt nu

$$p_{T|_{T_v}}(x) = x^k - c_{k-1}x^{k-1} - \cdots - c_1x - c_0,$$

terwijl volgens Lemma 6.33 dit polynoom een deler is van p_T. Dus is er een polynoom $q(x) \in L[x]$ zodat

$$p_T(x) = q(x) \cdot (x^k - c_{k-1}x^{k-1} - \cdots + c_1x - c_0).$$

Substitueren we hierin T voor x, dan geeft dit

$$p_T(T) = q(T) \cdot (T^k - c_{k-1}T^{k-1} - \cdots - c_1T - c_0),$$

een gelijkheid tussen twee lineaire afbeeldingen waarvoor het rechterlid toegepast op v beeld 0 heeft, vanwege bovenstaande relatie. Maar dan is dus ook $p_T(T)(v) = 0$, zoals te bewijzen was.

De bewering voor matrices volgt hieruit (of volgens een analoog argument).

Voorbeeld 6.35 Laat $T : \mathbb{Q}^3 \to \mathbb{Q}^3$ gegeven zijn door

$$T : \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} -b+c \\ a+c \\ 3c \end{pmatrix},$$

zodat, ten opzichte van de standaardbasis $\{e_1, e_2, e_3\}$ de afbeelding gegeven wordt door:

$$M_T = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

Daaruit volgt direct dat $Te_1 = e_2$, en $T^2e_1 = Te_2 = -e_1$. Daarom is de ruimte T_{e_1} opgespannen door e_1, Te_1, T^2e_1, ... dezelfde als die opgespannen door e_1 en Te_1, dat wil zeggen door $\{e_1, e_2\}$. We zien op twee manieren dat het karakteristieke polynoom va de beperking tot T_{e_1} het kwadratische polynoom $x^2 + 1$ is: immers $T^2e_1 = -e_1$. Ook kunnen we kijken naar de matrix van beperking $T|_{T_{e_1}}$, namelijk

$$M_{T|_{T_1}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

zodat volgens de definitie van het karakteristiek polynoom we $p_{T|_{T_1}} = x^2 + 1$ krijgen. Dit polynoom deelt p_T.

Kijken we naar de ruimte T_{e_3} opgespannen door e_3, Te_3, T^2e_3, ..., dan vinden we:

$$e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad Te_3 = \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}, \quad T^2e_3 = T\begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 9 \end{pmatrix},$$

en vervolgens

$$T^3e_3 = T\begin{pmatrix} 2 \\ 4 \\ 9 \end{pmatrix} = \begin{pmatrix} 5 \\ 11 \\ 27 \end{pmatrix} = 3\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix} + 3\begin{pmatrix} 2 \\ 4 \\ 9 \end{pmatrix},$$

oftewel

$$T^3e_3 = 3T^2e_3 - Te_3 + 3e_3.$$

Het karakteristieke polynoom is dus

$$p_{T|_{T_{e_3}}}(x) = x^3 - 3x^2 + x - 3 = (x^2 + 1)(x - 3).$$

Op grond van de graad moet dit de hele p_T zijn!

Opmerking 6.36 De stelling van Cayley-Hamilton kan soms toegepast worden om handig een inverse te vinden. Laat de (inverteerbare) matrix $M \in \mathrm{M}_{n\times n}(K)$ gegeven zijn; gebruik de algebraïsche relatie $p_M(M) = 0$, dus

$$M(M^{k-1} - c_{k-1}M^{k-2} - \cdots - c_1) = c_0,$$

zodat

$$M^{-1} = \frac{M^{k-1} - c_{k-1}M^{k-2} - \cdots - c_1}{c_0}.$$