Bewijs. (1) Volgt uit gevolg 2.40 vermits het stelsel een unieke oplossing heeft als geen enkele variabele vrij kan gekozen worden, dit komt overeen met $d = 0$.

(2) Volgt uit de formule in gevolg 2.40. □

Opmerking 2.42. Een stelsel lineaire vergelijkingen van de vorm $AX = 0$ heet een *homogeen stelsel*. De oplossingen van een homogeen stelsel $AX = 0$ kan men gebruiken om de oplossingen van een niet strijdig stelsel $AX = B$ te bepalen. Zij S een oplossing van $AX = B$ en C een willekeurige oplossing van $AX = 0$ dan geldt

$$A(S + C) = AS + AC = B + 0 = B.$$

De kolom $S+C$ is dus een oplossing van $AX = B$. Anderzijds geldt dat, als T een oplossing is van $AX = B$, de kolom $S - T$ een oplossing is van het homogeen stelsel $AX = 0$, immers

$$A(S - T) = AS - AT = B - B = 0.$$

Besluit: al de oplossingen van een stelsel $AX = B$ bekomt men door bij één (particuliere) oplossing S alle oplossingen van het geassocieerde homogeen stelsel $AX = 0$ op te tellen.

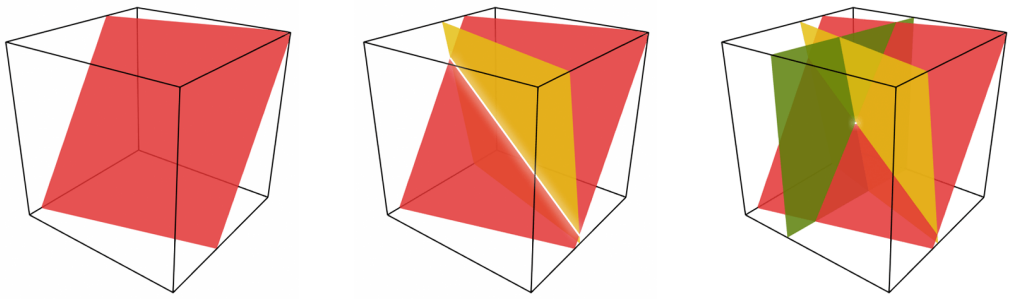
Opmerking 2.43. Zij $AX = 0$ een homogeen stelsel lineaire vergelijkingen van n vergelijkingen in m onbekenden over een veld K. We kunnen, door links vermenigvuldiging, A opvatten als een lineaire afbeelding van $K^m \to K^n$. De kern van deze afbeelding is juist de oplossingsverzameling van het stelsel $AX = 0$. Het beeld van de afbeelding is de deelruimte voortgebracht door de kolommen van A, de dimensie van het beeld is dus de rang van A. De dimensie formule in stelling 2.57 is dus niets anders dan de formule 2.40 voor de dimensie van de oplossingsverzameling van een stelsel lineaire vergelijkingen.

2.3 Secret sharing - een toepassing

Het doel van een "secret sharing systeem" is om bepaalde data (bv. de combinatie van een kluis) zo in n delen te verdelen, dat:

- de kennis van k delen de mogelijkheid geeft de data te berekenen,
- bij de kennis van minder dan k delen de data onbepaald is. (Onbepaald betekent hier dat alle mogelijke waarden "even mogelijk" zijn.)

Bijvoorbeeld, onderstel een groep van vier mensen krijgt slechts toegang tot een bepaalde geheime code (een getal) als drie van deze vier mensen samenkomen. Om een "secret sharing systeem" te maken gebruiken we het feit dat in de drie-dimensionale ruimte $\mathbb{R}^3$, drie vlakken "in algemene ligging" in een *uniek punt snijden*.



Onderstel dat g het geheime getal is. Beschouw dan een punt (g, k, l) in de 3-dimensionale ruimte (kies k en l willekeurig). Het idee is dat we aan elk van de vier personen de vergelijking van een vlak $ax + by + cz = d$ door het punt (g, k, l) geven. (Dit kunnen we doen door aan elk van de vier personen de rij (a, b, c, d) te geven.) Stel dat we aan persoon i de rij (a_i, b_i, c_i, d_i) geven. In het algemene geval zal wanneer drie van de vier personen samenkomen het getal g bepaald kunnen worden. Als bv. de personen $1, 2$ en 3 samenkomen, kunnen ze samen het stelsel

$$\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \end{cases}$$

vormen. Het oplossen van dit stelsel komt overeen met het bepalen van de doorsnede van drie vlakken. Dit stelsel heeft dus in het algemeen de unieke oplossing (g, k, l), zodat de drie personen weldegelijk het getal g kunnen achterhalen.

Het stelsel zou meer dan 1 oplossing kunnen hebben. Dit doet zich voor als de doorsnede van drie vlakken geen punt is, maar een rechte of een vlak. Algebraïsch moet *elk stel van drie vergelijkingen lineair onafhankelijk zijn,* dan zal de doorsnede van elke drie vlakken precies een punt zijn.

Eén of twee personen zouden kunnen in staat zijn het geheim te achterhalen zonder een groep van drie te vormen. Dit doet zich voor als en slechts als de oplossingen van het stelsel bekomen door één of twee personen geen vrijheidsgraad heeft in de x-component. Meetkundig betekent dit dat we een vlak of een rechte evenwijdig met het yz-vlak vinden.

Beide problemen kunnen we vermijden. Belangrijk is dat we inzien dat alle aspecten van het probleem kunnen geformuleerd worden in vectorruimten van willekeurige dimensie. Het is dus heel eenvoudig om met behulp van vectorruimten secret sharing systemen te maken voor een willekeurig grote groep van n personen, zodat elke k, $k \leq n$, personen samen de code kunnen berekenen.

- Kies in de k-dimensionale ruimte n vectoren $(a_{1i}, \ldots, a_{ki})$, $i = 1, \ldots, n$, zodat elke k vectoren in dit stel lineair onafhankelijk zijn.
  De lineair onafhankelijkheid van elk stel van k vectoren is equivalent met het feit dat elk stelsel van k vergelijkingen $a_{1i}x_1 + \cdots + a_{ki}x_k = 0$, de nulvector als unieke oplossing heeft. Maak een matrix A met deze n vectoren als rijen.
- Bepaal de vectoren zo dat geen van de deelruimten opgespannen door een stel van l vectoren, met $l < k$, gelijk is aan de deelruimte gegeven door de vergelijking $x_1 = 0$.
- Bepaal een punt $(p_1, \ldots, p_k)^t$ in de k-dimensionale ruimte, met als eerste coördinaat (de x_1-coördinaat) p_1 het codegetal. Bereken
$$A \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_k \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$
  De vergelijkingen
$$a_{1i}x_1 + \cdots + a_{ki}x_k = w_i, i = 1, \ldots, n,$$
  bepalen de deelcodes, elk van de n personen bekomt één van deze vergelijkingen.

We merken op dat deze instructies met behulp van de theorie van de matrices en de stelsels lineaire vergelijkingen kunnen uitgevoerd worden.

Voorbeeld. We bespreken een secret sharing systeem voorgesteld door Adi shamir. Het idee achter Shamir's schema is dat 2 punten in het vlak een rechte definiëren, 3 punten een parabool, 4 punten een kubische kromme enzovoort, $l + 1$ punten definiëren een kromme van graad l.

Om een secret sharing systeem voor een groep van n personen te bekomen zodat elke k personen uit de groep samen de geheime code kunnen bekomen gaat men als volgt te werk:

(1) Kies willekeurig $k - 1$ getallen, $a_1, \ldots, a_{k-1}$. Stel a_0 gelijk aan de geheime code en beschouw het polynoom
$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}a^{k-1}.$$

De coëfficiënten van f kunnen bekomen worden door het polynoom in k verschillende waarden te evalueren. Daarvoor gebruikt men een interpolatie formule. Zij $w_1 = f(b_1), \ldots, w_k = f(b_k)$, de waarden van het polynoom f in k verschillende getallen $b_1, \ldots, b_k$. Dan is
$$f(x) = \sum_{j=1}^{k} P_j(x) \text{ met } P_j := w_j \prod_{\substack{i=1 \\ i \neq j}}^{k} \frac{x - b_i}{b_j - b_i}.$$

Merk op dat de $\prod_{\substack{i=1 \\ i \neq j}}^{k} \frac{x-b_i}{b_j-b_i}$ daarbij een stel basisvectoren vormen voor de ruimte van mogelijke veeltermen, analoog aan hoe de matrixeenheden een basis vormen voor de ruimte der matrices.

(2) De informatie die ieder persoon in de groep krijgt is nu een punt op de kromme (de oplossingsverzameling van de vergelijking $y = f(x)$). Dus voor elke persoon genereert men een niet-nul getal b en geven de persoon $(b, f(b))$ als deel van de code.

(3) Als k personen samenkomen kan f berekend worden met de bovenstaande formule en dan kan dus ook de geheime code a_0 bepaald worden. Voor minder dan k personen zijn er nog oneindig veel krommen van graad $k-1$ waarop de punten van deze groep personen liggen.

Dit secret sharing systeem is equivalent met de systemen die met behulp van vectorruimten bekomen worden. De polynomen van graad $k-1$ vormen immers een k-dimensionale vectorruimte (over $\mathbb{R}$). Elk van de n punten $(b, f(b))$ geeft een k-dimensionale vector $(1, b, b^2, \ldots, b^{k-1})$. De code bekomt men door uit de oplossing van elk stelsel met k vergelijkingen van de vorm $x_0 + bx_1 + \cdots + b^{k-1}x_{k-1} = f(b) = w$, de eerste coördinaat te nemen.

2.4 Basisovergangen

We weten intussen al dat de keuze van de basis in een vectorruimte allesbehalve uniek is. Tegenover elke basis kunnen we een vector uniek voorstellen, zoals Voorbeeld 2.44 illustreert.

Voorbeeld 2.44. bijvoorbeeld de vector $(1, 2, 3) \in \mathbb{R}^3$ heeft:

- ten opzichte van de basis $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ coördinaten $(1, 2, 3)$, want
$$(1, 2, 3) = 1 \cdot (1, 0, 0) + 2 \cdot (0, 1, 0) + 3 \cdot (0, 0, 1);$$
- ten opzichte van de basis $(1, 1, 0), (0, 1, 1), (1, 0, 1)$ coördinaten $(0, 2, 1)$, want
$$(1, 2, 3) = 0 \cdot (1, 1, 0) + 2 \cdot (0, 1, 1) + 1 \cdot (1, 0, 1);$$
- ten opzichte van de basis $(1, 3, 7), (-1, 1, 2), (2, 0, 5)$ coördinaten $\left(\frac{17}{18}, -\frac{5}{6}, -\frac{7}{18}\right)$, want
$$(1, 2, 3) = \frac{17}{18} \cdot (1, 3, 7) - \frac{5}{6} \cdot (-1, 1, 2) - \frac{7}{18} \cdot (2, 0, 5).$$

Als er geen basis expliciet vermeld staat, maar wel coördinaten, dan gaan we er altijd van uitgaan dat die coördinaten tegenover de standaardbasis zijn. Maar andere basissen zijn zeker nuttig, zoals we in het volgende hoofdstuk uitgebreid gaan zien.

De voornaamste vraag waar we echter nog geen antwoord op weten: gegeven de coördinaten ten opzichte van één bepaalde basis, hoe vinden we de coördinaten ten opzichte van een andere basis? Laten we daartoe eerst eens kijken hoe we algoritmisch de waarden Voorbeeld 2.44 gevonden hebben. We hebben dat

$$\begin{array}{rcl} (1,1,0) & = & 1(1,0,0) + 1(0,1,0) + 0(0,0,1) \\ (0,1,1) & = & 0(1,0,0) + 1(0,1,0) + 1(0,0,1) \\ (1,0,1) & = & 1(1,0,0) + 0(0,1,0) + 1(0,0,1) \end{array}$$

en dus $\left(\begin{smallmatrix} 1&1&0\\0&1&1\\1&0&1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&1&0\\0&1&1\\1&0&1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&1 \end{smallmatrix}\right)$.

We zoeken de voorstelling (x, y, z) tegenover de basis $(1, 1, 0), (0, 1, 1), (1, 0, 1)$, zodanig dat dit dezelfde vector voorstelt als $(1, 2, 3)$ tegenover de basis $(1, 0, 0), (0, 1, 0), (0, 0, 1)$. Met andere woorden, we willen dat

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

wat dus uiteraard gegeven wordt door $\left(\begin{smallmatrix} x&y&z \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1&1&0\\0&1&1\\1&0&1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 0&2&1 \end{smallmatrix}\right)$.

Analoog vinden we voor de coördinaten (x', y', z') in de andere basis

$$\begin{pmatrix} x' & y' & z' \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 7 \\ -1 & 1 & 2 \\ 2 & 0 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{17}{18} & -\frac{5}{6} & -\frac{7}{18} \end{pmatrix}.$$

Algemeen, als we de coördinaten van een rijvector v krijgen als $x = (x_1, \ldots, x_n)$ ten opzichte van een basis $\mathcal{B} = b_1, \ldots, b_n$, en we willen de coördinaten $x' = (x'_1, \ldots, x'_n)$ vinden ten opzichte van een basis $\mathcal{B}' = b'_1, \ldots, b'_n$, dan hebben we dat

$$x \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = x' \cdot \begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{pmatrix} \text{ en dus } x' = x \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \cdot \begin{pmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{pmatrix}^{-1}.$$

Analoog [2], als we de coördinaten van een kolomvector v krijgen als $x = (x_1, \ldots, x_n)$ ten opzichte van een basis $\mathcal{B} = b_1, \ldots, b_n$, en we willen de coördinaten $x' = (x'_1, \ldots, x'_n)$ vinden ten opzichte van een basis $\mathcal{B}' = b'_1, \ldots, b'_n$, dan hebben we dat

$$\begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix} \cdot x = \begin{pmatrix} b'_1 & b'_2 & \cdots & b'_n \end{pmatrix} \cdot x' \text{ en dus } x' = \begin{pmatrix} b'_1 & b'_2 & \cdots & b'_n \end{pmatrix}^{-1} \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix} \cdot x.$$

Definitie 2.45. De *transitiematrix* tussen basis $\mathcal{B}$ en $\mathcal{B}'$ is de matrix

$$\begin{pmatrix} b'_1 & b'_2 & \cdots & b'_n \end{pmatrix}^{-1} \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix}.$$

De transitiematrix van een basis naar de standaardbasis is dus gewoon de matrix met als kolommen de basisvectoren van $\mathcal{B}$.

Definitie 2.45 is in de onderstelling dat je kolommen als rijvectoren interpreteert. Je kunt uiteraard ook transitiematrices invoeren als je basissen van rijvectoren beschouwd, dan bestaan de matrices uit rijvectoren en staat de nieuwe basis rechts in plaats van links (maar dat had je zelf al kunnen afleiden door dat matrixproduct in zijn geheel te transponeren).

2.5 Lineaire afbeeldingen

Een transformatie voorstellen als een matrix is dus altijd ten opzichte van een zekere basis. Soms willen we de basis intelligent kunnen kiezen (bv. bij een draaiing is het handig om de rotatie-as als één van de basisvectoren te hebben), maar willen we wel al over de transformatie kunnen spreken van voor dat we de basis vastgelegd kunnen hebben. Daarom voeren we een begrip in dat lineaire transformaties in het algemeen beschrijft, los van hun concrete matrixvoorstelling.

Definitie 2.46. Zij V en W twee vectorruimten over het veld K. Dan noemen we een afbeelding $T : V \to W$ een *lineaire afbeelding* als[3]

$$\forall \lambda, \mu \in K : \forall v_1, v_2 \in V : T(\lambda v_1 + \mu v_2) = \lambda T(v_1) + \mu T(v_2).$$

Een lineaire afbeelding zet dus lineaire combinaties om in lineaire combinaties:

$$T\left(\sum_i \lambda_i v_i\right) = \sum_i \lambda_i T(v_i).$$

Definitie 2.47. Een lineaire afbeelding van een vectorruimte V naar zichzelf noemen we een *lineaire operator op* V.

Opmerking 2.48. Zij V en W eindigdimensionale K-vectorruimten. Zij $\{b_1, \ldots, b_n\}$ een basis voor V. Een lineaire afbeelding $T : V \to W$ is volledig bepaald door de beelden van de basisvectoren $T(b_1), \ldots, T(b_n)$. Dit volgt onmiddellijk uit de rekenregels vermits elke vector $v \in V$ gelijk is aan een lineaire combinatie $\sum_i \lambda_i b_i$, $\lambda_i \in K$, dus $T(v) = \sum_i \lambda_i T(b_i)$.

Omgekeerd bepaalt elke afbeelding van de verzameling $\{b_1, \ldots, b_n\}$ naar W een lineaire afbeelding tussen V en W. Stel $R : \{b_1, \ldots, b_n\} \to W : b_i \mapsto w_i$, dan is

$$V \to W : \sum_i \lambda_i b_i \mapsto \sum_i \lambda_i R(b_i) = \sum_i \lambda_i w_i$$

een lineaire afbeelding tussen V en W, die we eveneens R noemen.

[2] Gewoon beide leden transponeren en herinneren dat transponering de volgorde van producten omkeert.

[3] Merk op dat de eerste $+$ de optelling is in V en dat de tweede $+$ de optelling is in de ruimte W.

De volgende observatie is heel nuttig.

Stelling 2.49. Zij $\{b_1, \ldots, b_n\}$ een basis voor de K-vectorruimte V en $w_1, \ldots, w_n$ elementen in een K-vectorruimte W. Zij $R : V \to W$ de lineaire afbeelding die bepaald wordt door $b_i \mapsto w_i$. Dan gelden de volgende eigenschappen:

(1) R is injectief als en slechts als $\{w_1, \ldots, w_n\}$ een lineair onafhankelijk stel is in W.

(2) R is surjectief als en slechts als $\{w_1, \ldots, w_n\}$ een voortbrengend stel is in W.

(3) R is bijectief als en slechts als $\{w_1, \ldots, w_n\}$ een basis is in W.

Bewijs. We bewijzen punt (1), de andere punten kan men als oefening zelf bewijzen.

Zij R een injectieve afbeelding en onderstel $\sum \lambda_i w_i = 0$ is een lineaire relatie tussen de vectoren w_i. Dan is $R(\sum \lambda_i b_i) = \sum \lambda_i w_i = 0$. Dus is, vanwege de injectiviteit van R, $\sum \lambda_i b_i = 0$. Dit impliceert voor alle $i = 1, \ldots, n$ dat $\lambda_i = 0$, dus de vectoren w_i zijn lineair onafhankelijk.

Omgekeerd onderstel dat de vectoren w_i lineair onafhankelijk zijn. Uit $R(\sum_i \lambda_i b_i) = R(\sum_i \mu_i b_i)$ volgt $\sum(\lambda_i - \mu_i)R(b_i) = \sum(\lambda_i - \mu_i)w_i = 0$. Dit impliceert dat voor alle $i = 1, \ldots, n$, $\lambda_i - \mu_i = 0$ en dus is $\sum_i \lambda_i b_i = \sum_i \mu_i b_i$. De afbeelding R is dus injectief. □

Gevolg 2.50. Zij $T : V \to W$ een bijectieve lineaire afbeelding, dan is $\dim V = \dim W$.

Bewijs. Dit volgt onmiddellijk uit punt (3) van stelling 2.49. □

Definitie 2.51. Een bijectieve lineaire afbeelding tussen twee vectorruimten noemen we ook een *isomorfisme*.

Als er tussen twee vectorruimten een bijectieve lineaire afbeelding bestaat dan zeggen we dat de vectorruimten *isomorf* zijn.

Gevolg 2.52. (1) Zij $T : V \to W$ een lineaire afbeelding op een eindigdimensionale ruimte V. Als $\dim V = \dim W$ dan zijn de volgende eigenschappen equivalent:

(a) T is injectief.

(b) T is surjectief.

(c) T is bijectief.

(2) Zij $T : V \to V$ een lineaire operator op een eindigdimensionale ruimte V. Dan is de injectiviteit van T equivalent met de surjectiviteit en de bijectiviteit van T.

Bewijs. (1) Zij $\dim V = n$, de equivalenties volgen uit stelling 2.49 vermits een stel van n elementen in een n-dimensionale ruimte lineair onafhankelijk is als en slechts als het voortbrengend is.

(2) Volgt onmiddellijk uit (1). □

Gevolg 2.53. Twee vectorruimten zijn isomorf als en slechts als ze dezelfde dimensie hebben.

Bewijs. Dat de voorwaarde nodig is volgt uit gevolg 2.50. De voorwaarde is voldoende omdat een bijectie, van een basis van de ene ruimte naar een basis van de andere ruimte, een bijectieve lineaire afbeelding tussen de ruimten bepaalt. □

Definitie 2.54. Zij $T : V \to W$ een lineaire afbeelding tussen twee willekeurige vectorruimten dan is de *kern* van T de deelruimte

$$\ker T = \{v \in V | T(v) = 0\}.$$

Het *beeld* van T is de deelruimte van W gegeven door $\mathrm{im}(T) = T(V) = \{w \in W | \exists v \in V, T(v) = w\}$.

Opmerking 2.55. De definitie bepaalt ***kern*** en ***beeld*** van een lineaire afbeelding als verzamelingen. Dat dit deelruimten zijn van respectievelijk V en W vraagt een bewijs.

Als $\lambda, \mu \in K$ en $v, v' \in \ker T$ dan moeten we aantonen dat $\lambda v + \mu v' \in \ker T$. Dit volgt uit

$$T(\lambda v + \mu v') = \lambda T(v) + \mu T(v') = 0 + 0 = 0.$$

Als $w, w' \in T(V)$ dan bestaan er vectoren $v, v' \in V$ zodat $T(v) = w$ en $T(v') = w'$. Er geldt

$$\lambda w + \mu w' = \lambda T(v) + \mu T(v') = T(\lambda v + \mu v') \in T(V),$$

waaruit volgt dat $T(V)$ een deelruimte is van W.

Lemma 2.56. Een lineaire afbeelding $T : V \to W$ is injectief als en slechts als $\ker T = \{0\}$.

Bewijs. Dat de kern van een injectieve afbeelding gelijk is aan de nulruimte volgt onmiddellijk uit de definities van injectiviteit en kern. Onderstel omgekeerd dat $\ker T = \{0\}$. Uit $T(v) = T(w)$ volgt dat $T(v-w) = 0$, dus $v-w \in \ker T$. maar dan is $v - w = 0$, i.e. $v = w$, dus T is injectief. □

Zij T een lineaire afbeelding van een ruimte V naar een ruimte W. De volgende stelling geeft een verband tussen de dimensie van een ruimte V, de dimensie van het beeld $T(V)$ en de dimensie van $\ker T$.

Stelling 2.57. Zij $T : V \to V'$ een lineaire afbeelding, waarbij V een eindigdimensionale vectorruimte is. Dan is $\dim V = \dim \ker T + \dim T(V)$.

Bewijs. Kies een basis $\{b_1, \ldots, b_k\}$ voor de deelruimte $\ker T$, dus $k = \dim \ker T$. Deze basis kunnen we wegens Lemma 1.67 uitbreiden tot een basis $\{b_1, \ldots, b_k, b_{k+1}, \ldots, b_n\}$ voor V. Zij W de deelruimte voortgebracht door het lineair onafhankelijk stel $\{b_{k+1}, \ldots, b_n\}$. Dan is $V = \ker T \oplus W$, en dus is $(\ker T) \cap W = \{0\}$. De restrictie van T tot W is dus een injectieve lineaire afbeelding. Dit impliceert dat $T_{|W}$ een isomorfisme is tussen W en $T(V)$. Gevolg 2.50 impliceert $\dim T(V) = \dim W$. Vermits $\dim V = \dim \ker T + \dim W$ volgt de dimensie formule $\dim V = \dim \ker T + \dim T(V)$. □

Voorbeeld 2.58.

1. Zij P_n de vectorruimte van de veeltermen van graad $\leq n$ in één variabele x over K. De *afleiding*[4]
$$\frac{d}{dx} : P_n \to P_{n-1} : f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \frac{df(x)}{dx} = \sum_{i=1}^{n} i \cdot a_i x^{i-1},$$
is een lineaire afbeelding. Deze afbeelding bepaalt ook een lineaire operator op de ruimte $K[X]$ van de veeltermen over een veld K.
2. Zij $V = \mathbb{F}_2^n$ de standaardvectorruimte over het eindig veld $\mathbb{F}_2 = \{0, 1\}$ met 2 elementen. De "shiftoperator" $(\varepsilon_1, \ldots \varepsilon_n) \mapsto (0, \varepsilon_1, \ldots, \varepsilon_{n-1})$ definieert een lineaire afbeelding op V (met dus $\varepsilon_i \in \{0, 1\}$).
3. Er zijn verschillende lineaire operatoren op het vlak $\mathbb{R}^2$ en op de driedimensionale ruimte $\mathbb{R}^3$ met een meetkundige betekenis, bijvoorbeeld projecties en rotaties. We zullen de rotaties nog uitvoerig behandelen in andere lessen.

Alle dergelijke transformaties tussen eindigdimensionale ruimtes V en W kunnen we nu voorstellen aan de hand van een matrix. We hebben immers dat de basisvectoren $b_1, \ldots, b_k$ van V afgebeeld worden op $T(b_1), \ldots, T(b_k)$. Als, voor een basis $b'_1, \ldots, b'_n$ van W geldt dat $b'_i = a_{i,1}b_1 + a_{i,2}b_2 + \cdots + a_{i,k}b_k$, voor elke i, dan bevat $A = (a_{ij})$ alle gegevens nodig om het beeld van een deelruimte van V te berekenen. We zullen dit noteren met $W = A \cdot V$, en het beeld van een ruimte $V' \leq V$ zullen we noteren met $A \cdot V'$. We zullen dit matrixproduct nu formeel invoeren.

Wat met basisovergangen? Zij $T : V \to W$ een lineaire afbeelding tussen een n-dimensionale ruimte V en een m-dimensionale ruimte W. Kiezen we (geordende) basissen $\mathcal{B}_V = f_1, \ldots, f_n$ in V en $\mathcal{B}_W = g_1, \ldots, g_m$ in W, dan is

$$T(f_j) = a_{1j}g_1 + \cdots + a_{mj}g_m.$$

Zij $A = (a_{ij})$ en $(c_1, \ldots, c_n)^t$ de coördinatenvector van v ten opzichte van de gekozen basis $\mathcal{B}_V$. We bekomen dan de coördinaten van de beeldvector $T(v)$ via de matrixvermenigvuldiging:

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

Dus een lineaire afbeelding tussen twee (eindigdimensionale) vectorruimten komt overeen met het links vermenigvuldigen met een matrix op de kolommenruimte (bestaande uit de coördinaatvectoren). De matrix A noemen we de matrixvoorstelling van de lineaire afbeelding T, ten opzichte van de basissen $\mathcal{B}_V$ en $\mathcal{B}_W$.

Opmerking 2.59. Merk op dat er dus eerst een basis $\mathcal{B}_V$ in de vectorruimte V en een basis $\mathcal{B}_W$ in de vectorruimte W moeten gekozen worden, voor er een matrixvoorstelling A voor de lineaire afbeelding $T : V \to W$ opgesteld kan worden.

[4] Merk op dat de afleiding op deze manier voor veeltermen over een willekeurig veld gedefinieerd is.

Opmerking 2.60. Het beeld en de kern van een lineaire afbeelding kunnen we ook interpreteren in termen van de matrixvoorstelling.

De beelden $T(f_i)$ van de basisvectoren in $\mathcal{B}_V$ hebben als coördinaatvectoren ten opzichte van de basis $\mathcal{B}_W$ juist de kolommen van de matrix A. De dimensie van $T(V)$ is dus precies het aantal lineair onafhankelijke kolommen van A, dit is de *rang* van A.

Een vector behoort tot de kern van T juist dan als de corresponderende coördinaatvector (ten opzichte van de basis $\mathcal{B}_V$) een oplossing is van het homogene lineaire stelsel $AX = 0$. De dimensie van $\ker T$ komt overeen met het aantal "vrijheidsgraden" voor die oplossing (we noemden dit ook de *dimensie van het stelsel*).

Als we andere basissen kiezen in de ruimte V, respectievelijk W, dan zal T een andere matrixvoorstelling hebben. Wat is het verband tussen verschillende matrixvoorstellingen? We kiezen basissen $\mathcal{B}_V$ en $\mathcal{B}'_V$ voor de ruimte V en basissen $\mathcal{B}_W$ en $\mathcal{B}'_W$ voor de ruimte W. Zij Q de transitiematrix van de basis $\mathcal{B}_V$ naar de basis $\mathcal{B}'_V$, en P de transitiematrix van de basis $\mathcal{B}_W$ naar de basis $\mathcal{B}'_W$. Dan is volgens het vorige hoofdstuk $Q^{-1}X = X'$ en $P^{-1}Y = Y'$, met X de coördinaatvector van een vector $v \in V$ ten opzichte van de basis $\mathcal{B}_V$, X' de coördinaatvector van v ten opzichte van de basis $\mathcal{B}'_V$, Y de coördinaatvector van een vector $w \in W$ ten opzichte van de basis $\mathcal{B}_W$ en Y' de coördinaatvector van w ten opzichte van de basis $\mathcal{B}'_W$.

Als $T : V \to W$ een lineaire afbeelding is, heeft T een matrixvoorstelling A die overeenkomt met de basissen $\mathcal{B}_V$ en $\mathcal{B}_W$, en een matrixvoorstelling A' die overeenkomt met de basissen $\mathcal{B}'_V$ en $\mathcal{B}'_W$. Dus is $A'X' = Y'$ en uit $X' = Q^{-1}X$ en $Y' = P^{-1}Y$ volgt dat $A'Q^{-1}X = P^{-1}Y$, ofte $PA'Q^{-1}X = Y$. De matrix $PA'Q^{-1}$ is dus de matrixvoorstelling van de lineaire afbeelding T ten opzichte van de basissen $\mathcal{B}_V$ en $\mathcal{B}_W$, deze matrix is dus gelijk aan de matrix A. Dit betekent dat $PA'Q^{-1} = A$ ofte $A' = P^{-1}AQ$.

Zij $T : V \to V$ een lineaire operator op een eindigdimensionale vectorruimte V, A de matrixvoorstelling ten opzichte van de basis $\mathcal{B}_V$ en A' de matrixvoorstelling ten opzichte van de basis $\mathcal{B}'_V$. Dan is $A = QA'Q^{-1}$ en $A' = Q^{-1}AQ$, met Q de transitiematrix van de basis $\mathcal{B}_V$ naar de basis $\mathcal{B}'_V$.

Opmerking 2.61. Als we basissen in de ruimten V en W vast kiezen is er dus een 1-1 verband tussen de $m \times n$-matrices en de verzameling van alle lineaire afbeeldingen tussen V en W. We noteren deze verzameling met $\mathrm{Hom}(V, W)$; ze heeft dus dezelfde structuur als $M_{m,n}(K)$, i.e. het is een $m \times n$-dimensionale vectorruimte over K.

De ruimte $\mathrm{Hom}(V, V)$ is de ruimte van de endomorfismen op V, deze noteren we met $\mathrm{End}(V)$. Op $\mathrm{End}(V)$ kunnen we ook een ringstructuur, dus een vermenigvuldiging, definiëren, namelijk deze die overeenkomt met het matrixproduct. De vermenigvuldiging op $\mathrm{End}(V)$ is niets anders dan de samenstelling van afbeeldingen. Als we in V een basis vast kiezen en de operatoren in $\mathrm{End}(V)$ voorstellen door $n \times n$-matrices ten opzichte van deze basis, bekomen we de matrixring $M_n(K)$.