bijvoorbeeld $R_0, R_1, \ldots, R_{m-1}$. Vaak geven we de restklasse R_i, waar i zelf in zit, aan met $\bar{i}$. Als i en j in dezelfde restklasse zitten, schrijven we $i \equiv j \bmod m$, en zeggen dat i *congruent* j *modulo* m is. Dus

$$i \equiv j \bmod m \quad \Longleftrightarrow \quad R_i = R_j \quad \Longleftrightarrow \quad \bar{i} = \bar{j} \quad \Longleftrightarrow \quad m \mid i - j.$$

We definiëren optelling en vermenigvuldiging van $\bar{i}$ en $\bar{j}$ door $\bar{i}+\bar{j} = \overline{i+j}$ en $\bar{i}\times\bar{j} = \overline{i\times j}$.

Nu is $\mathbb{Z}/m\mathbb{Z}$ de verzameling van de m restklassen modulo m met deze optelling en vermenigvuldiging. Niet alle elementen (ongelijk 0) hebben een inverse in $\mathbb{Z}/m\mathbb{Z}$ tenzij m een priemgetal is. Voor een priemgetal p is de ring $\mathbb{Z}/p\mathbb{Z}$ wel een lichaam dat uit precies p verschillende elementen bestaat. Zo'n eindig lichaam $\mathbb{Z}/p\mathbb{Z}$ wordt ook wel met $\mathbb{F}_p$ aangegeven.

Later zullen we zien dat voor elke *macht* $m = p^k$ van een priemgetal p er een eindig lichaam van m elementen bestaat (en voor geen enkel ander natuurlijk getal m). Bovendien is er in essentie maar één zo'n lichaam.

(vii) Als R een commutatieve ring met 1 is (bijvoorbeeld één van de ringen of lichamen die we hierboven zagen) kun je daaruit een nieuwe *ring* $R[x]$ *van polynomen met coëfficiënten in* R maken: de verzameling bestaat uit de polynomen of *veeltermen* $\sum_{i=0}^{n} a_i x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, waar $n \geq 0$ een geheel getal is. De operaties zijn de *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. In **Lineaire Algebra 1** en **2** heb je al kennis gemaakt met het speciale geval $R = \mathbb{R}$.

(viii) In **Lineaire Algebra 1** en **2** heb je ook gezien dat je vierkante matrices van reële getallen kunt optellen en vermenigvuldigen. Veel algemener kunnen we bij elke commutatieve ring met 1 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 *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

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

Met andere woorden: je telt zulke matrices op en je vermenigvuldigt ze op precies dezelfde manier als waarop je dat eerder hebt gezien in het speciale geval dat alle coëfficiënten reëel waren.

Voor elke n krijgen we zo (voor gegeven commutatieve ring R) een nieuwe ring. Als $n > 1$ is die ring $\mathrm{M}_n(R)$ niet commutatief!

Opgave 3. *Laat zien dat de deelverzameling van $\mathbb{Z}$ bestaande uit de even getallen voldoet aan L1–5 en L8–9. Dit is een commutatieve ring zonder eenheidselement, die we* niet *als deelring van $\mathbb{Z}$ beschouwen (omdat 1 er niet in zit).*

We hebben gezien dat elke ring R (dus in het bijzonder elk lichaam) in ieder geval de elementen $0, 1$ bevat. Maar dan moet ook $1+1$ in R zitten, een element dat we gewoonlijk met 2 aangeven. Maar let op: het kan best 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 1.1.5(iv)). 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 $1 + 1 = 0$).

1.1.6 Definitie

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 *injectie* van $\mathbb{Z} \to R$. Omgekeerd, als er zo'n injectieve afbeelding bestaat moet de karakteristiek wel 0 zijn.

Opgave 4. *Geef voor elk natuurlijk getal $m \geq 2$ twee verschillende voorbeelden van een ring van karakteristiek m.*

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

1.1.7 Definities

Een element r van een ring R (niet noodzakelijk commutatief) heet een *eenheid in R* als er een inverse voor r in R bestaat (dus 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 $s \times r = 0$.

Opgave 5. *Laat zien dat in een lichaam elk element dat niet 0 is een eenheid is.*

Opgave 6. *Geef twee elementen r, s van $\mathrm{M}_2(\mathbb{Z})$ met de eigenschap dat $r \times s = 0$ maar $s \times r \neq 0$.*

1.1.8 Stelling

Een eenheid in een ring R (niet noodzakelijk commutatief) kan geen nuldeler zijn.

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

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

(volgens opgave 2) 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.

1.1.9 Definitie

Een *domein* (of *integriteitsgebied*) is een ring (commutatief met 1) zonder nuldelers.

In de algebra spelen naast objecten met een bepaalde struktuur, zoals groep, ring, lichaam, en vectorruimte, *afbeeldingen* tussen zulke objecten *die de struktuur behouden* een belangrijke rol.

1.1.10 Definities

Een *ringhomomorfisme* is een afbeelding $f\colon R \to S$ tussen ringen R en S die voldoet aan de eigenschappen:

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

Een *ringisomorfisme* is een bijectief ringhomomorfisme. Een *ringautomorfisme* is een ringisomorfisme tussen R en zichzelf.

Opgave 7. *Laat zien dat de afbeelding $f\colon \mathbb{Z} \to \mathbb{Q}$ die aan een geheel getal n de breuk $n/1$ toevoegt een ringhomomorfisme is. Bestaat er een ringisomorfisme tussen $\mathbb{Z}$ en $\mathbb{Q}$?*

Opgave 8. *Laat zien dat de afbeelding $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ die aan een geheel getal n de restklasse $n \bmod m$ toevoegt een ringhomomorfisme is. Is dit een ringisomorfisme?*

De eis dat $f(1) = 1$ kunnen we stellen omdat we hebben aangenomen dat elke ring een eenheidselement heeft. De identieke afbeelding is altijd een ringisomorfisme. Een ringisomorfisme tussen twee ringen drukt uit dat de twee ringen dezelfde struktuur hebben (als ring); dit maakt het bijvoorbeeld mogelijk om preciezer uit te drukken (vgl. 1.1.5) dat er in essentie maar één lichaam van p elementen bestaat, voor een priemgetal p: elk lichaam van p elementen is isomorf met $\mathbb{Z}/p\mathbb{Z}$.

1.1.11 Opgaven

Opgave 9. *Wat is het eenheidselement, en wat is het nulelement in $R[x]$? En in $\mathrm{M}_n(R)$?*

Opgave 10. *Zij $\cdot$ een bewerking op een verzameling V. Definieer voor $n \geq 3$ het product $v_1 \cdot v_2 \cdots v_n$ inductief (voor $v_i \in V$) door $(v_1 \cdot v_2 \cdots v_{n-1}) \cdot v_n$. Laat (met behulp van inductie naar n) zien dat als $\cdot$ associatief is, voor alle $n \geq 3$ en alle k met $1 \leq k \leq n-1$ geldt:*

$$(v_1 \cdot v_2 \cdots v_k) \cdot (v_{k+1} \cdots v_n) = v_1 \cdot v_2 \cdots v_n.$$

Opgave 11. *Bewijs dat het eenheidselement $1 \in R$ uniek bepaald is.*

Opgave 12. *Laat $(R, +, \times)$ een ring zijn; bewijs dat een deelverzameling S van R een deelring is als:*

(i) $1_R \in S$;
(ii) *als* $a, b \in S$ *dan ook* $a - b \in S$;
(iii) *als* $a, b \in S$ *dan ook* $a \times b \in S$.

Opgave 13. *Laat zien dat de eenheden van een ring R een groep vormen onder $\times$. Deze groep geven we aan met R^*.*

Opgave 14. *Geef een voorbeeld van een ring zonder nuldelers waarin niet elk element (ongelijk aan 0) een eenheid is.*

Opgave 15. *Bewijs dat $\mathrm{M}_n(\mathbb{R})^*$ bestaat uit de $n \times n$ reële matrices met determinant ongelijk aan 0. Deze groep geven we ook wel met $\mathrm{GL}_n(\mathbb{R})$ aan. Waarom is dit geen ring (voor elke $n > 0$)?*

Opgave 16. *Beschrijf $\mathrm{GL}_n(\mathbb{Z})$, en algemener, de groep $\mathrm{GL}_n(R)$ voor een commutatieve ring R.*

Opgave 17. *Laat zien dat complexe conjugatie (de afbeelding die aan een complex getal $a + b\mathrm{i}$ het getal $a - b\mathrm{i}$ toevoegt) een isomorfisme $\mathbb{C} \to \mathbb{C}$ geeft.*

Opgave 18. *Bewijs dat de ring $\mathbb{Z}/n\mathbb{Z}$ een lichaam is dan en slechts dan als n een priemgetal is.*

Opgave 19. *Als V een verzameling is, geven we met $P(V)$ de machtsverzameling van V aan: $P(V)$ bestaat uit de deelverzamelingen van V. Laat zien dat $(P(V), +, \times)$ een commutatieve ring (met 1) wordt als we de optelling $+$ en vermenigvuldiging $\times$ definiëren door voor deelverzamelingen $A, B \subset V$ te nemen:*

$$A + B = (A \cup B) \setminus (A \cap B), \qquad A \times B = A \cap B.$$

Laat ook zien dat $P(V)$ zo alleen een lichaam wordt als $\#V = 1$.

Opgave 20. *De quaternionen van Hamilton $\mathbb{H}$ worden gedefinieerd als uitdrukkingen van de vorm $a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ met $a, b, c, d \in \mathbb{R}$. Twee zulke uitdrukkingen $a_1 + b_1\mathrm{i} + c_1\mathrm{j} + d_1\mathrm{k}$ en $a_2 + b_2\mathrm{i} + c_2\mathrm{j} + d_2\mathrm{k}$ zijn hetzelfde dan en slechts dan als $a_1 = a_2$ en $b_1 = b_2$ en $c_1 = c_2$ en $d_1 = d_2$. Optellen geschiedt componentsgewijs, hetgeen som $a_1 + a_2 + (b_1 + b_2)\mathrm{i} + (c_1 + c_2)\mathrm{j} + (d_1 + d_2)\mathrm{k}$ geeft, en vermenigvuldiging vindt plaats met de regels:*

$$\begin{array}{lllllll} \mathrm{i}^2 & = & \mathrm{j}^2 & = & \mathrm{k}^2 & = & -1 \\ \mathrm{i} \cdot \mathrm{j} & = & \mathrm{k} & & \mathrm{j} \cdot \mathrm{i} & = & -\mathrm{k} \\ \mathrm{j} \cdot \mathrm{k} & = & \mathrm{i} & & \mathrm{k} \cdot \mathrm{j} & = & -\mathrm{i} \\ \mathrm{k} \cdot \mathrm{i} & = & \mathrm{j} & & \mathrm{i} \cdot \mathrm{k} & = & -\mathrm{j}. \end{array}$$

Laat zien dat $\mathbb{H}$ met deze bewerkingen een niet-commutatieve ring vormt. (Voor het bewijs van associativiteit van vermenigvuldiging helpt het om $a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} = (a + b\mathrm{i}) + (c + d\mathrm{i})\mathrm{j}$ te schrijven.) Geef een isomorfisme aan van $\mathbb{H}$ met de deelring van $\mathrm{M}_2(\mathbb{C})$ bestaande uit matrices $A \cdot I + B \cdot J + C \cdot K + D \cdot L$, waar $A, B, C, D \in \mathbb{R}$ en

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

Laat ook zien dat $a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ een inverse heeft tenzij $a = b = c = d = 0$, door te kijken naar $(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}) \cdot (a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k})$. De quaternionen vormen een scheeflichaam: een ring die aan alle axioma's voor een lichaam voldoet behalve de commutativiteit [L8].