Eenheden in groepsringen

Hector Mommaerts

Hoofdstuk 1

Wat is een groepsring?

1.1 Basisverzameling

Stel dat G een groep is en R een associatieve ring met eenheidselement. Construeer nu de verzameling van alle R-lineaire combinaties van eindig veel elementen van G. Met andere woorden objecten van de vorm $r_1g_1 + r_2g_2 + \cdots + r_ng_n$ met $r_i \in R$ en $g_i \in G$. We noteren deze verzameling als RG.

$$RG = \{a = \sum_{g\in G} a_g g \text{ met } a_g \in R \text{ en supp(a)is eindig}\}$$

Hierbij is supp(a) $= \{g \in G : a_g \neq 0\}$.
We kunnen $r \in R$ identificeren met $r.e_G \in RG$, zodat R een deelverzameling is van RG. Analoog kunnen we $g \in G$ identificeren met $1_R.g \in RG$ zodat ook G een deelverzameling is van RG Dus :

$$R \subset RG \text{ en } G \subset RG$$

1.2 De optelling

We definieren een optelling in RG als volgt:

$$\forall a, b \in RG : a + b = \sum_{g\in G} (a_g + b_g)g$$

Stelling 1.1. *De optelling is commutatief in RG*

Bewijs. Stel $a = \sum_{g\in G} a_g g$ en $b = \sum_{g\in G} b_g g$, dan is

$$\begin{aligned} a+b &= \sum_{g\in G}(a_g+b_g)g \\ &= \sum_{g\in G}(b_g+a_g)g \text{ (want R is een ring)} \\ &= b+a \end{aligned}$$

$\square$

Stelling 1.2. *De optelling is associatief in RG*

Bewijs. Stel $a = \sum_{g\in G} a_g g$, $b = \sum_{g\in G} b_g g$ en $c = \sum_{g\in G} c_g g$, dan is

$$\begin{aligned} (a+b)+c &= \sum_{g\in G}(a_g+b_g)g + \sum_{g\in G} c_g g \\ &= \sum_{g\in G}((a_g+b_g)+c_g)g \\ &= \sum_{g\in G}(a_g+(b_g+c_g))g \text{ (want R is een ring)} \\ &= a+(b+c) \end{aligned}$$

$\square$

Stelling 1.3. *0 is het neutraal element voor de optelling in RG*

Bewijs. Omdat $0 \in R$ is 0 ook een element van RG. Stel $a = \sum_{g \in G} a_g g$

$$\begin{aligned} a + 0 &= \sum_{g \in G} a_g g + 0.g \\ &= \sum_{g \in G} (a_g + 0) g \\ &= \sum_{g \in G} a_g g \text{ (want 0 is neutraal element in R)} \\ &= a \end{aligned}$$

□

Stelling 1.4. *Elk element heeft een symmetrisch element voor de optelling in RG*

Bewijs. Stel $a = \sum_{g \in G} a_g g$. Construeer dan $-a = \sum_{g \in G} (-a_g) g$. Dan is $-a \in RG$ want $-a_g \in R$ en

$$\begin{aligned} a + (-a) &= \sum_{g \in G} a_g g + \sum_{g \in G} (-a_g) g \\ &= \sum_{g \in G} (a_g + (-a_g)) g \\ &= \sum_{g \in G} 0.g \text{ (want } -a_g \text{ is tegengesteld aan } a_g \text{ in R)} \\ &= 0 \end{aligned}$$

□

We besluiten:

$$RG, + \text{ is een commutatieve groep}$$

1.3 De vermenigvuldiging

We definieren een vermenigvuldiging in RG als volgt:

$$\forall a, b \in RG : a.b = \sum_{g \in G} \Big(\sum_{h \in G} a_h.b_{h^{-1}g} \Big) g$$

Stelling 1.5. *De vermenigvuldiging is associatief in RG*

Bewijs. Stel $a = \sum_{g \in G} a_g g$, $b = \sum_{g \in G} b_g g$ en $c = \sum_{g \in G} c_g g$, dan is

$$\begin{aligned}
(a.b).c =& \sum_{g \in G} \Big(\sum_{h \in G} a_h.b_{h^{-1}g} \Big) g. \sum_{g \in G} c_g g \\
=& \sum_{g \in G} \Big(\sum_{k \in G} \Big(\sum_{h \in G} a_h.b_{h^{-1}k} \Big).c_{k^{-1}g} \Big) g \\
=& \sum_{g \in G} \Big(\sum_{hk \in G} \Big(\sum_{h \in G} a_h b_k \Big).c_{k^{-1}h^{-1}g} \Big) g \\
=& \sum_{g \in G} \Big(\sum_{h \in G} a_h \Big(\sum_{hk \in G} b_k.c_{k^{-1}h^{-1}g} \Big) \Big) g \\
=& \sum_{g \in G} a_g g. \sum_{g \in G} \Big(\sum_{k \in G} b_k c_{k^{-1}g} \Big) g \\
=& \, a.(b.c)
\end{aligned}$$

□

Stelling 1.6. $1_R e_G$ *is het neutraal element voor de vermenigvuldiging in RG*

Bewijs. Noteer $1_R e_G$ als e.

$$\begin{aligned}
e.a =& 1_R e_G. \sum_{g \in G} a_g g \\
=& \sum_{g \in G} 1.a_{e_G g} g \\
=& \, a
\end{aligned}$$

Verder is ook:

$$
\begin{aligned}
a.e &= \sum_{g \in G} a_g g.1_R e_G. \\
&= \sum_{g \in G} a_g .1_R g \\
&= a
\end{aligned}
$$

□

Stelling 1.7. *De vermenigvuldiging is distributief ten opzichte van de optelling in RG*

Bewijs. Stel $a = \sum_{g \in G} a_g g$, $b = \sum_{g \in G} b_g g$ en $c = \sum_{g \in G} c_g g$, dan is:

$$
\begin{aligned}
a.(b+c) &= \sum_{g \in G} a_g g. \Big(\sum_{g \in G} (b_g + c_g) g \Big) \\
&= \sum_{g \in G} \Big(\sum_{h \in G} a_h (b_{h^{-1}g} + c_{h^{-1}g}) \Big) g \\
&= \sum_{g \in G} \Big(\sum_{h \in G} (a_h b_{h^{-1}g} + a_h c_{h^{-1}g}) \Big) g \\
&= \sum_{g \in G} \Big(\sum_{h \in G} a_h b_{h^{-1}g} \Big) g + \sum_{g \in G} \Big(\sum_{h \in G} a_h c_{h^{-1}g} \Big) g \\
&= a.b + a.c
\end{aligned}
$$

□

We besluiten:

$RG, +, .$ is een associatieve ring met eenheidselement

1.4 De skalaire vermenigvuldiging

We definieren een vermenigvuldiging in RG met elementen uit R

$$\forall r \in R, \forall a \in RG : r.a = \sum_{g \in G} (ra_g)g$$

Stelling 1.8. *De skalaire vermenigvuldiging is gemeng associatief in RG*

Bewijs. Neem $r, s \in R$ en $a = \sum_{g \in G} a_g g$.

$$\begin{aligned} r.(s.a) =& r.\Big(\sum_{g \in G} s.a_g g\Big) \\ =& \sum_{g \in G} r.(s.a_g)g \\ =& \sum_{g \in G} (r.s).a_g g \\ =& (r.s).a \end{aligned}$$

□

Stelling 1.9. *1 is het neutraal element voor de skalaire vermenigvuldiging in RG*

Bewijs. Omdat $1 = 1_R.e_G$ volgt dit uit stelling 1.6 □

Stelling 1.10. *De skalaire vermenigvuldiging is distributief ten opzichte van de optelling in RG*

Bewijs. Stel $a = \sum_{g\in G} a_g g$, $b = \sum_{g\in G} b_g g$ en $r \in R$.

$$\begin{aligned} r.(a+b) =& r.\Big(\sum_{g\in G}(a_g + b_g)g\Big) \\ =& \sum_{g\in G} r(a_g + b_g)g \\ =& \sum_{g\in G}(ra_g + rb_g)g \\ =& \sum_{g\in G} ra_g g + \sum_{g\in G} rb_g g \\ =& \, r.a + r.b \end{aligned}$$

□

Stelling 1.11. *De vermenigvuldiging in RG is distributief ten opzichte van de optelling in R*

Bewijs. Stel $a = \sum_{g\in G} a_g g$ en $r, s \in R$

$$\begin{aligned} (r+s).a =& (r+s).\sum_{g\in G} a_g g \\ =& \sum_{g\in G}(r+s)a_g g \\ =& \sum_{g\in G}(ra_g + sa_g)g \\ =& \sum_{g\in G} ra_g g + \sum_{g\in G} sa_g g \\ =& \, r.a + s.a \end{aligned}$$

□

We besluiten:

$R, RG, +$ is een R- module met G

1.5 Samenvatting

We weten dat RG een R-module is. Bovendien is G een basis voor de module, dus is RG een vrije R-module met basis G. Bovendien is $RG, +, .$ een ring. Dit alles benoemen we als:

$$R, RG, +, . \text{ is een groepsring}$$

Als R een veld is, dan is RG zelfs een algebra: $R, RG, +$ is een vectorruimte over R en $RG, +, .$ is een ring. We noemen RG dan een groepsalgebra.

$$R \text{ een veld} : R.RG, +, . \text{ is een groepsalgebra}$$