Ringen en Lichamen - Opdracht 4

Luc Veldhuis - 2538227

November 2017

1. Zij $R = Z[\sqrt{-7}] = \{a + b\sqrt{-7}$ met a en b in $\mathbb{Z}\}$, een deelring van $\mathbb{C}$. Bepaal alle verschillende ontbindingen van 8 in R. Hierbij beschouwen we twee ontbindingen $8 = p_1 \cdot \cdots \cdot p_m$ en $8 = q_1 \cdot \cdots \cdot q_n$ met alle p_i en q_j irreducibel in R als gelijk als $m = n$ en we na eventuele herordening van de q_j hebben dat $q_1 = \pm p_1, \ldots q_m = p_m$. (Merk op dat $R^* = \{\pm 1\}$.) *Aanwijzing: gebruik de norm.* We nemen als norm: $N(a + b\sqrt{-7}) = a^2 + 7b^2$. Dan geldt nu voor eenheden $u, v \in R$ dat $1 = uv = vu$. Maar dan moet gelden dat: $1 = N(1) = N(uv) = N(u)N(v)$, dus $N(u) = \pm 1$ en $N(v) = \pm 1$, dus $u, v \in \{\pm 1\}$. Dus $R^* = \{\pm 1\}$.
   Dus we weten nu dat we de elementen $\{0, -1, 1\}$ niet mogen gebruiken in onze ontbinding, omdat deze niet irreducibel zijn.
   Dan hebben we nu dat als $8 = p_1 \cdots p_n$ dan $N(8) = N(p_1 \cdots p_n) = N(p_1) \cdots N(p_m)$.
   Dit geeft $64 = N(p_1) \cdots (p_n)$.
   Dit geeft als mogelijke ontbindingen: $64 = 2 \cdot 32 = 4 \cdot 16 = 8 \cdot 8 = 16 \cdot 4 = 32 \cdot 2$.
   We zien dat:
   $32 = 2 \cdot 16 = 4 \cdot 8 = 8 \cdot 4 = 16 \cdot 2$.
   $16 = 2 \cdot 8 = 4 \cdot 4 = 8 \cdot 2$.
   $8 = 2 \cdot 4 = 4 \cdot 2$
   $4 = 2 \cdot 2$.
   Omdat voor $N(p_i) = 2$ geen oplossingen bestaan met $a \in R$, want dan hebben we dat $a = \pm\sqrt{2}$, vallen alle ontbindingen met een element met norm 2 erin af.
   Dan kijken we naar de ontbindingen: $64 = 4 \cdot 16 = 8 \cdot 8 = 16 \cdot 4$ met $16 = 4 \cdot 4$.
   Dan beschouwen we nu alle elementen die voldoen aan $N(p_i) \in \{4, 8, 16\}$.
   Dit geeft als $N(p_i) = 4$, dan $p_i \in \{\pm 2\}$.
   Dit geeft als $N(p_i) = 8$, dan $p_i \in \{\pm(1 \pm \sqrt{-7})\}$.
   Dit geeft als $N(p_i) = 16$, dan $p_i \in \{\pm 4, \pm(3 \pm \sqrt{-7})\}$.
   Volgens dit schema is een mogelijke ontbinding met beschouwing tot de norm: $8 = \pm 2 \cdot \pm(3 \pm \sqrt{-7})$.
   Deze ontbinding is niet correct, want $Im(8) = 0$, maar $Im(\pm 2 \cdot \pm(3 \pm \sqrt{-7})) = \pm 2\sqrt{-7}$. Dus deze ontbinding valt af.
   Ook zien we dat $4 = 2 \cdot 2$, maar 2 is geen eenheid, dus 4 is niet irreducibel. Dus dit element valt ook af.
   Dan hebben we nu de ontbindingen:

   - $8 = 2 \cdot 2 \cdot 2 = -2 \cdot -2 \cdot 2 = 2 \cdot -2 \cdot -2 = -2 \cdot 2 \cdot -2$. Deze ontbindingen tellen als 1 ontbinding.
   - $8 = (1 + \sqrt{-7}) \cdot (1 - \sqrt{-7}) = (1 - \sqrt{-7}) \cdot (1 + \sqrt{-7}) = -(1 + \sqrt{-7}) \cdot -(1 - \sqrt{-7}) = -(1 - \sqrt{-7}) \cdot -(1 + \sqrt{-7})$. Deze ontbindingen tellen als 1 ontbinding.

2. Zij $R = \{\frac{a}{b}$ in $\mathbb{Q}$ met a en b in $\mathbb{Z}$ en b oneven$\}$. Gegeven is dat R een deelring is van $\mathbb{Q}$ die de identiteit $\frac{1}{1}$ van $\mathbb{Q}$ bevat.

(a) Laat zien dat $R^* = \{\frac{a}{b}$ in R met a en b oneven$\}$.
Een element in $a \in R$ is een eenheid en dus in R^* als geldt dat $ab = ba = 1$ voor een $b \in R$.
Neem een element $\frac{a}{b} \in R$, dan geldt $\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = 1$ als $\frac{b}{a} \in R$.
Dit element $\frac{b}{a} \in R$ bestaat alleen als a oneven is per definitie. Ook moet er gelden dat b oneven is per definitie van R. Dus elk element $\frac{a}{b} \in R$ met a en b oneven is een eenheid.
Dus $R^* = \{\frac{a}{b}$ in R met a en b oneven$\}$.

(b) Toon aan dat de irreducibele elementen van R de elementen $2u$ met u in R^* zijn. *Aanwijzing: elk element in R kun je schrijven als $\frac{a2^n}{b}$ met a en b oneven en $n \geq 0$.*
We kunnen elk getal in $\mathbb{Z}$ schrijven als $a2^n$ voor $n \geq 0$ voor een oneven getal a.
We moeten bewijzen dat $r \in R$ irreducibel $\Leftrightarrow r = 2u$ met $u \in R^*$.
Bewijs $r \in R$ irreducibel $\Rightarrow r = 2u$.
Neem een irreducibel element $r = \frac{a}{b} \in R$. Schrijf dit vervolgens als $\frac{c2^n}{b} \in R$ met $a = c2^n$ en $c \in \mathbb{Z}$ oneven. Omdat per definitie $r \notin R^*$, moet gelden dat $n \geq 1$, omdat anders a oneven is.
Neem nu een $d, e \in R$ met $d = \frac{f2^m}{g}$ en $e = \frac{h2^l}{j}$ met $f, g, h, j \in \mathbb{Z}$ oneven en $m, l \geq 0$ zodat $r = de$.
Deze bestaan altijd, neem namelijk $d = r$ en $e = \frac{1}{1}$.
We gaan nu kijken naar de vorm van het element de.

- Stel $m + l = 0$.
  Dan zijn d en e eenheden, want de tellers zijn oneven.
  Dan geldt $\frac{c2^n}{b} = \frac{f}{g}\frac{h}{j} = \frac{fh}{gj}$.
  Dus $\frac{c2^n gj}{bgj} = \frac{fhb}{bgj}$.
  Dus er moet gelden dat $c2^n gj = fhb$.
  Maar fhb is oneven, en omdat $n \geq 1$ is $c2^n gj$ even. Dus het is niet mogelijk dat $m + l = 0$.
- Stel $m + l = 1$.
  Dan geldt dat $r = de = \frac{f2^m}{g}\frac{h2^l}{j} = \frac{fh2}{gj} = 2\frac{fh}{gj}$. Maar nu is $fh, gj \in \mathbb{Z}$ oneven, dus er bestaat een $u \in R^*$, zodat $u = \frac{fh}{gj}$ en $r = 2u$.
- Stel $m + l > 1$. Dan hebben we dat $de = \frac{f2^m}{g}\frac{h2^l}{j} = \frac{fh2^{m+l}}{gj}$.
  Dan kunnen we dit ook schrijven als $\frac{fh2^{m+l}}{gj} = \frac{fh2^{m+l-1}}{gj}\frac{2}{1}$.
  Maar $\frac{2}{1} \notin R^*$, want 2 is even, en $\frac{fh2^{m+l-1}}{gj} \notin R^*$, want $m + l - 1 > 0$, dus $fh2^{m+l-1}$ is even.
  Dit is een tegenspraak dat r irreducibel is, want $r = \frac{fh2^{m+l-1}}{gj}\frac{2}{1}$, maar geen van beide termen uit R is een eenheid. Dus het is onmogelijk dat $m + l > 1$.

Hieruit blijkt dat als er 2 elementen $d, e \in R$ zijn zodat $r = de$, dan moet gelden dat $de = 2u$ met $u \in R^*$. Dus elk irreducibel element $r \in R$ is te schrijven als $r = 2u$ met $u \in R^*$.

Bewijs $r \in R$ irreducibel $\Leftarrow r = 2u$.
Neem een element $r \in R$ zodat $r = 2u$. Omdat $0 \notin R^*$, geldt dat $r \neq 0$.
Stel $u = \frac{a}{b} \in R^*$, dan zijn a en b oneven per definitie.
Maar dan is $r = \frac{2a}{b}$, en $2a$ is even, dus $r \notin R^*$.
Nu rest ons nog te bewijzen dat voor elke andere elementen $d, e \in R$ zodat $r = 2u = de$, moet gelden dat d of e een eenheid is.
Stel d en e zijn geen eenheid, dan moet gelden dat $d = \frac{f2^m}{g}$ met $m \geq 1$ en $e = \frac{h2^l}{j}$ met $l \geq 1$ en met $f, g, h, j \in \mathbb{Z}$ oneven.
Dan hebben we dat $de = \frac{f2^m}{g}\frac{h2^l}{j} = \frac{fh2^{m+l}}{gj} = 2u = \frac{2a}{b}$.
Dit geeft $\frac{fhb2^{m+l}}{gjb} = \frac{2agj}{gjb}$ met $fhb, gjb, agj \in \mathbb{Z}$ oneven.

Dus er moet gelden dat $2agj = fhb2^{m+l}$. Omdat deze vergelijking in $\mathbb{Z}$ moet gelden, kunnen we beide kanten door 2 delen. Dit geeft $agj = fhb2^{m+l-1}$, met $m + l - 1 \geq 1$, dus $fhb2^{m+l-1}$ is even, maar agj oneven. Dit is een tegenspraak.
Dus tenminste 1 van d of e moet een eenheid zijn.
Dus voor elke ontbinding $r = 2u = de$, geldt dat dat d of e een eenheid is, en u is per aanname een eenheid.
Aan alle eisen voor een irreducibel element zijn nu voldaan, dus r is een irreducibel element.
We hebben nu bewezen dat $r \in R$ irreducibel $\Leftrightarrow r = 2u$ met $u \in R^*$.

(c) Zijn de elementen uit (b) ook priemelementen? We zien in (b) dat voor een $r \in R$ geldt dat, als deze irreducibel is, dan is geldt $r = 2u$ met $u \in R^*$.
Hieruit volgt dat $(r) = (2u)$. Dus geldt nu ook $2uu^{-1} = 2 \in (r)$, en u^{-1} bestaat, want $u \in R^*$.
Dus $(2) \subseteq (r)$.
Stel $1 \in (r)$, dan moet gelden $1 = rk$, voor een $k \in R$, maar dan is r een eenheid, maar r is irreducibel. Dit is onmogelijk.
Dus $(r) \neq R$.
Als we nu kunnen laten zien dat (2) een maximaal ideaal is, dan moet gelden dat $(2) = (r)$, en dan volgt direct dat (2) een priem ideaal is.
Stel er is een ideaal $I \subseteq R$ zodat $(2) \subsetneq I$. We zien direct dat $(2) = 2R$, dus elk element $\frac{a2^m}{b} \in 2R$ heeft tenminste $m \geq 1$.
Omdat $(2) \subsetneq I$, moet er een element $t \in I$ bestaan zodat t niet in (2), dus $t = \frac{c2^n}{d}$, met $n = 0$ en $c, d \in \mathbb{Z}$, want als $n \geq 1$, dan zit $t \in (2)$.
Maar als $n = 0$ dan zit t in R^* en is nu een eenheid. Als een ideaal een eenheid bevat is het gelijk aan de hele ring, dus geldt nu $I = R$.
Dus (2) is een maximaal ideaal.
Hieruit volgt dat $(2) = (r)$, omdat $(r) \neq R$ en dus is (r) een maximaal ideaal en ook direct een priem ideaal.
Een element $p \in R$ is een priem element als geldt dat (p) een priem ideaal is.
Dus elk irreducibel element is ook een priem element.