

Opgave 4.6.2

We geven eerst even wat **achtergrond** over de opgave. We starten met de polynoomring $\mathbb{R}[X, Y]$ in twee variabelen. Een polynoom in twee variabelen definieert een functie $\mathbb{R}^2 \rightarrow \mathbb{R}$. Neem nu de éénheidscirkel $X^2 + Y^2 = 1$. Op deze cirkel kunnen we kijken naar functies die een beperking van een functie uit $\mathbb{R}[X, Y]$ tot de cirkel zijn. We kunnen dit doen door de poolcoördinaat parametrisatie $(\cos \phi, \sin \phi)$ van de cirkel te nemen en aan het polynoom $P(X, Y)$ de functie $P(\cos \phi, \sin \phi)$ op de cirkel toe te kennen. De polynoomfuncties op de cirkel worden dus gegeven door de ring $\mathbb{R}[\cos \phi, \sin \phi]$. Dit is het beeld van $\mathbb{R}[X, Y]$ onder het homomorfisme $X \mapsto \cos \phi$ en $Y \mapsto \sin \phi$. De kern van dit homomorfisme wordt gegeven door het ideaal $(X^2 + Y^2 - 1)$ (omdat $\cos^2 \phi + \sin^2 \phi = 1$). Conclusie:

$$\mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \cong \mathbb{R}[\cos \phi, \sin \phi].$$

De **vragen** in Opgave 4.6.2 hadden iets duidelijker geformuleerd moeten worden. Een betere volgorde had als volgt gemoeten.

1. Bewijs dat elke restklasse in $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ een unieke representant van de vorm $A(X) + B(X)Y$ heeft met $A, B \in \mathbb{R}[X]$.

Oplossing: Stel $P(X, Y) \in \mathbb{R}[X, Y]$ en beschouw deze als polynoom in Y met coëfficiënten in $\mathbb{R}[X]$. Neem voor $A(X) + B(X)Y$ de rest van deling van $P(X, Y)$ door $Y^2 + X^2 - 1$. Deze rest heeft graad ≤ 1 in Y en is uniek bepaald.

Met de notatie x, y voor de restklassen $X \pmod{X^2 + Y^2 - 1}$, $Y \pmod{X^2 + Y^2 - 1}$ kunnen we ook zeggen dat elk element in $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ op unieke manier in de vorm $A(x) + B(x)y$ geschreven kan worden.

Informeel kun je bij $A(x) + B(x)y$ ook denken aan $A(X) + B(X)\sqrt{1 - X^2}$. De ring $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ zou dus ook beschreven kunnen worden door $\mathbb{R}[X, \sqrt{1 - X^2}]$.

2. Definieer de norm afbeelding $N : \mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \rightarrow \mathbb{R}[X]$ door $N : A(x) + B(x)y \mapsto A(X)^2 - (1 - X^2)B(X)^2$. Bewijs dat N multiplicatief is, dat wil zeggen $N(\alpha\beta) \equiv N(\alpha)N(\beta)$.

Oplossing: Uitschrijven. Merk op dat de informele definitie $N(A(X) + B(X)\sqrt{1 - X^2}) = A(X)^2 - (1 - X^2)B(X)^2$ heel erg lijkt op de norm in $\mathbb{Z}[i]$ of $\mathbb{Z}[\sqrt{-5}]$.

3. Bewijs dat $\alpha \in \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ een éénheid is precies dan als $N(\alpha) \in \mathbb{R}^*$.

Oplossing: Merk op dat als $\alpha = A(x) + B(x)y$ dan $N(\alpha) \equiv (A(x) + B(x)y)(A(x) - B(x)y)$ (informeel, $A(X)^2 - (1 - X^2)B(X)^2 = (A(X) + B(X)\sqrt{1 - X^2})(A(X) - B(X)\sqrt{1 - X^2})$). Dus, als $N(\alpha) \in \mathbb{R}^*$ dan moet $A(x) + B(x)y$ een éénheid zijn. Omgekeerd, als α een éénheid is, dan is er een element β zó dat $\alpha\beta = 1$. Neem nu de norm, $N(\alpha)N(\beta) = 1$. Conclusie, $N(\alpha)$ is een deler van 1, dus een constant niet-triviaal polynoom in $\mathbb{R}^*$.

4. Nu komt vraag (a) pas, laat zien dat $x - 1$ en $y - 1$ irreducibel zijn in onze ring.

Oplossing: Stel $x - 1$ is reducibel, dat wil zeggen er zijn niet-eenheden α, β zó dat $x - 1 = \alpha\beta$. Stel $\alpha = A(x) + B(x)y$ en $\beta = C(x) + D(x)y$. Nemen we de norm van $x - 1 = \alpha\beta$ dan krijgen we

$$(X - 1)^2 = (A(X)^2 - (1 - X^2)B(X)^2)(C(X) - (1 - X^2)D(X)^2).$$

Omdat α, β geen éénheid zijn, is hun norm een niet constant polynoom in X . Het product van de normen is $(X - 1)^2$. Dat betekent dat $N(\alpha)$ en $N(\beta)$ beiden van de vorm $\epsilon(X - 1)$ zijn met $\epsilon \in \mathbb{R}^*$. Dus bijvoorbeeld

$$N(\alpha) = A(X)^2 - (1 - X^2)B(X)^2 = \epsilon(X - 1).$$

Nu komt er een subtiel argument. De kopcoëfficiënt van $A(X)^2$ is positief, want een kwadraat van een reëel getal, en de kopcoëfficiënt van $-(1 - X^2)B(X)^2$ is ook positief. Dat betekent dat deze kopcoëfficiënten bij de optelling $A(X)^2 - (1 - X^2)B(X)^2$ niet tegen elkaar kunnen wegvallen. In het bijzonder is de graad ≥ 2 of $B(X) = 0$. In het eerste geval hebben we een tegenspraak, in het tweede geval geldt $\epsilon(X - 1) = A(X)^2$. Maar ook dat kan niet, want $X - 1$ is geen kwadraat van een polynoom. Analoog argument voor $y - 1$ en ook $x + y - 1$.

Opmerking: In dit argument gebruiken we de positiviteit van kwadraten in $\mathbb{R}$. Het argument gaat mis als we $\mathbb{C}$ in plaats van $\mathbb{R}$ zouden hebben. Sterker nog, $x - 1$ is reducibel in $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$, want we hebben $-2(X - 1) \equiv (X - 1 + iY)(X - 1 - iY) \pmod{X^2 + Y^2 - 1}$, ofwel $-2(x - 1) = (x - 1 + iy)(x - 1 - iy)$.

5. Onderdeel (c) volgt nu uit de voorgaande opgave.
6. De filosofie bij onderdeel (d) is dat de functie $(x - 1)(y - 1)$ als functie op de cirkel een dubbel nulpunt heeft in de punten $(1, 0)$ en $(0, 1)$. Hetzelfde geldt voor $(x + y - 1)^2$ omdat de rechte $X + Y = 1$ de cirkel in $(1, 0), (0, 1)$ snijdt. Dat is de reden dat $(x + y - 1)^2$ en $(x - 1)(y - 1)$ een éénheid verschillen. Hetzelfde verhaal kan nu gehouden worden voor ieder tweetal rechte lijnen dat raakt aan de cirkel in de punten P, Q (zeg) en de rechte lijn door P en Q .