UITWERKINGEN

1. Zij $P(X) = X^4 + X^3 + 2X^2 - 2$.

   (a) (1/2 pt) Ontbindt $P(X)$ in irreducibele factoren in $\mathbb{Q}[X]$.

   antwoord: We zoeken eerst naar rationale nulpunten. Dat moeten gehele getallen zijn die 2 delen. Proberen geeft -1 als nulpunt. Ontbinden: $P(X) = (X+1)(X^3 + 2X - 2)$. De tweede factor is een Eisenstein polynoom ten aaanzien van $p = 2$.

   (b) (1 pt) Ontbindt $P(X)$ in irreducibele factoren in $(\mathbb{Z}/5\mathbb{Z})[X]$.

   antwoord: We hadden al $P(X) \equiv (X+1)(X^3 + 2X - 2) (\text{mod } 5)$. De derde graads factor heeft een nulpunt $-1 (\text{mod } 5)$. Dit geeft weer een factor $X+1$, dus $P(X) \equiv (X+1)^2(X^2-X+2) (\text{mod } 5)$. De kwadratische factor ontbindt als $(X+1)(X+2) (\text{mod } 5)$.

   (c) (1/2 pt) Bewijs voor elke $n \in \mathbb{Z}_{\geq 1}$ dat het polynoom $X^n + Y^n - 1$ irreducibel is in $\mathbb{C}[X, Y]$ (hint: gebruik Eisenstein).

   antwoord: Bekijk het polynoom als element van $\mathbb{C}[Y][X]$. Dan is het een Eisensteinpolynoom ten aanzien van het irreducibele element $Y - 1$.

   (d) (1/2 pt) Bewijs dat $\mathbb{Q}[X]/(X^4 + 5)$ een lichaam is.

2. Zij R een ring en I een ideaal ongelijk aan R. Geef het natuurlijke homomorfisme $R \to R/I$ aan met ϕ.

   (a) (1/2 pt) Zij J een ideaal in R/I. Bewijs dat $\phi^{-1}(J)$ een ideaal in R is.

   antwoord: Omdat $\phi(0) = 0 \in J$ geldt $0 \in \phi^{-1}(J)$.

   Stel $a, b \in \phi^{-1}(J)$. Dan geldt $\phi(a+b) = \phi(a) + \phi(b) \in J$ want $\phi(a), \phi(b) \in J$. Dus $a + b \in$
   $phi^{-1}(J)$.

   antwoord: Stel $r \in R$ en $a \in \phi^{-1}(J)$. Dan geldt $\phi(ra) = \phi(r)\phi(a) \in J$ want $\phi(a) \in J$. Dus $ra \in \phi^{-1}(J)$.

   (b) (1/2 pt) Stel dat R een hoofdideaalring is. Bewijs dat R/I een hoofdideaalring is.

   antwoord: Kies een ideaal $J \in R/I$. Volgens bovenstaande is $\phi^{-1}(J)$ een ideaal in R en dus is er $r \in R$ zó dat $\phi^{-1}(J) = (r)$. Dus $J = (\phi(r))$.

   (c) (1/2 pt) Geef een voorbeeld van R, I waarin R/I een hoofdideaalring is en R niet.

   antwoord: $R = \mathbb{C}[X, Y]$ en $I = (Y)$. Of $R = \mathbb{Z}[X]$ en $I = (2)$.

   (d) (1 pt) Bewijs dat J een priemideaal in R/I is precies dan als $\phi^{-1}(J)$ een priemideaal in R is.

   antwoord: Stel J is een priemideaal and $a, b \in R$ met $ab \in \phi^{-1}(J)$. Dan geldt $\phi(a)\phi(b) = \phi(ab) \in J$ en dus (omdat J priem is) $\phi(a) \in J$ of $\phi(b) \in J$. Gevolg: $a \in \phi^{-1}(J)$ of $b \in \phi^{-1}(J)$.

Stel dat $\phi^{-1}(J)$ een priemideaal is en $a, b \in R/I$ met $ab \in J$. Kies $A, B \in R$ zó dat $\phi(A) = a, \phi(B) = b$. Merk nu op dat $\phi(AB) = \phi(A)\phi(B) \equiv ab \in J$. Dus $AB \in \phi^{-1}(J)$. Omdat $\phi^{-1}(J)$ priem is geldt $A \in \phi^{-1}(J)$ of $B \in \phi^{-1}(J)$. En dus $a = \phi(A) \in J$ of $b = \phi(B) \in J$.

3. Beschouw de afbeelding $\phi : \mathbb{Q}[X] \to \mathbb{Q} \times \mathbb{Q}$ gegeven door $\phi : F(X) \mapsto (F(1), F(-1))$.

   (a) (1/2 pt) Bewijs dat ϕ een ringhomomorfisme is.
   antwoord: Er geldt

$$\begin{aligned} \phi(F(X)+G(X)) &= (F(1)+G(1), F(-1)+G(-1)) \\ &= (F(1),G(1)) + (F(-1),G(-1)) = \phi(F(X)) + \phi(G(X)) \\ \phi(F(X)G(X)) &= (F(1)G(1), F(-1)G(-1)) \\ &= (F(1),G(1)) + (F(-1),G(-1)) = \phi(F(X)) + \phi(G(X)) \end{aligned}$$

   (b) (1/2 pt) Geef een voortbrenger van de kern van ϕ.
   antwoord: $\phi(F(X)) = 0 \Rightarrow F(1) = F(-1) = 0$. Dus is F deelbaar door zowel $X+1$ als $X-1$. Ze zijn relatief priem, dus $F(X)$ is deelbaar door hun product X^2-1. Verder zit X^2-1 ook in de kern. Dus de kern is (X^2-1).

   (c) (1/2 pt) Bewijs dat $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q} \times \mathbb{Q}$.
   antwoord 1: Pas de homorfiestelling toe. De afbeelding ϕ is surjectief, want $\phi(b(1-X)/2 + a(1+X)/2) = (a, b)$ voor alle $a, b \in \mathbb{Q}$.
   antwoord 2: Chinese reststelling. Er geldt dat de som van idealen $(X+1)$ en $(X-1)$ gelijk is aan (1) want $(1-X)/2 + (1+X)/2 = 1$. En dus $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q}[X]/(X+1) \times \mathbb{Q}[X]/(X-1)$. Laatste twee zijn isomorf met $\mathbb{Q}$ vanwege de isomorfiestelling toegepast op de afbeeldingen $F(X) \mapsto F(1)$ en $F(X) \mapsto F(-1)$.

   (d) (1/2 pt) Bepaal de oplossingen van de vergelijking $y^2 = 1$ in $y \in \mathbb{Q} \times \mathbb{Q}$.
   antwoord: Los op $(x, y)^2 = (1, 1)$. Hieruit volgt $x^2 = 1, y^2 = 1$. En dus $x \equiv \pm 1, y \equiv \pm 1$. Conclusie: 4 oplossingen $(\pm 1, \pm 1)$.

   (e) (1/2 pt) Los $y^2 \equiv 1 (\text{mod } X^2-1)$ in $y \in \mathbb{Q}[X]/(X^2-1)$.
   antwoord 1: Iedere oplossing heeft representant modulo X^2-1 van de vorm $y \equiv aX + b$. Dus $y^2 = 1$ impliceert $(aX+b)^2 \equiv 1 (\text{mod } X^2 - 1)$. Hieruit: $2abX + a^2 + b^2 \equiv 1 (\text{mod } X^2-1)$. Hieruit $ab = 0$ en $a^2 + b^2 = 1$. Hieruit volgen de oplossingen $(0, \pm 1)$ en $(\pm 1, 0)$. Dus $\pm 1, \pm X (\text{mod } X^2-1)$.
   antwoord 2: Uit voorgaande twee onderdelen volgt dat we de inverse beelden van $(\pm 1, \pm 1)$ kunnen bepalen van $F(X) (\text{mod } X^2-1) \mapsto (F(1), F(-1))$. Het inverse beeld van $(1, 1)$ en $(-1, -1)$ zijn de constante polynomen 1 en -1. Het inverse beeld van $(1, -1)$ is X en dat van $(-1, 1)$ is $-X$.

4. Beschouw de ring

$$\mathbb{Z}[1/5] := \{a/5^k |\ a \in \mathbb{Z}, k \in \mathbb{Z}_{\geq 0}\},$$

dat wil zeggen de ring $\mathbb{Z}$ samen met de rationale getallen waarvan de noemer een macht van 5 is.

(a) (1 pt) Bepaal de éénheden in $\mathbb{Z}[1/5]$.

antwoord: Geef de ring aan met R. Stel $a/5^k \in R^*$. Als a een priemfactor $p \neq 5$ zou bevatten, dan zou $5^k/a$ niet in R liggen. Tegenspraak met $a/5^k \in R^*$. Dus moet $a/5^k$ van de vorm $\pm 5^m$ zijn met $m \in \mathbb{Z}$.

(b) (1 pt) Bepaal de irreducibele elementen in $\mathbb{Z}[1/5]$.

antwoord: Elk element van R ongelijk 0 is geassocieerd met een element van $\mathbb{N}$ dat niet deelbaar is door 5. We hoeven dus alleen naar $\mathbb{N}$ te kijken. Het getal 1 is per definitie niet irreducibel. Stel $n \in \mathbb{N}$, niet deelbaar door 5. Als n niet priem is dan is er een ontbinding $n = ab$ met met $a, b \in \mathbb{Z}_{>1}$, en $a, b \in \mathbb{Z}$ niet deelbaar door 5, dus geen eenheden in R. We hebben dus een niet-triviale ontbinding in R en n is reducibel in R.

Stel nu dat n priem is $\neq 5$. Schrijf $a = \alpha 5^k, b = \beta 5^l$ met $k, l \in \mathbb{Z}$ en $\alpha, \beta \in \mathbb{Z}$, niet deelbaar door 5. Hieruit volgt dat $n = \alpha\beta 5^{k+l}$. Omdat n, α, β geheel zijn en niet deelbaar door 5 volgt hieruit dat $k + l = 0$. Dus $n = \alpha\beta$. Dit is een niet-triviale ontbinding in $\mathbb{Z}$, in tegenspraak met de primaliteit van n. Het element is dus irreducibel.

De irreducibele elementen zijn dus $\pm p5^k$ met p priem $\neq 5$ en $k \in \mathbb{Z}$.

(c) (1/2 pt) Bewijs dat $\mathbb{Z}[1/5]$ een unieke ontbindingsring is. (Je mag gebruiken dat $\mathbb{Z}$ een unieke ontbindingsring is).

antwoord: Elk irreducibel element in R is geassocieerd met een priemgetal $p \neq 5$. Elk element in R kan ontbonden worden als $5^k p_1 \cdots p_r$ met $p_1, \ldots, p_m \neq 0$ priem. Stel er is een andere ontbinding, $5^l q_1 \cdots q_s$. Uit de gelijkheid van de twee en unieke ontbinding in $\mathbb{Z}$ volgt dat $k = l$ en de sets $\{p_1, \ldots, p_r\}$ en $\{q_1, \ldots, q_s\}$ zijn hetzelfde.