Algebra 2

Collegeaantekeningen

- Naam: Pim Meulensteen
- Student nr.: 12751510
- Contact: pim.meulensteen@student.uva.nl

- Datum: 29 september 2020

Inhoudsopgave

Deel I

Generalizatie van Algebra 1

Ringen en licahamen zijn beide generalisaties van groepen. De eerste vier weken van het vak zullen ook vooral generalisaties zijn van dingen die we weten over groepen naar ringen.

Hoorcollege 1

Ringen en Licahamen

1.1 Definities en opmerkingen

Definitie 1.1.1. Een *ring* is een vijftupel $(R, +, \cdot, 0, 1)$ met R een verzameling, $+$ en $\cdot$ afbeeldingen:

$$+ : R \times R \to R, (a, b) \mapsto a + b$$
$$\cdot : R \times R \to R, (a, b) \mapsto ab$$

en 0 en 1 elementen van R, zodanig dat de volgende eigenschappen (R1) t/m (R4) gelden:

(R1) $(R, +, 0)$ is een abelse groep; dit houdt in:

- (G1) $a + (b + c) = (a + b) + c$ voor alle $a, b, c \in R$;
- (G2) $0 + a = a + 0 = a$ voor alle $a \in R$;
- (G3) voor elke $a \in R$ is er een tegengestelde $-a \in R$ waarvoor geldt $a + (-a) = (-a) + a = 0$;
- (G4) $a + b = b + a$ voor alle $a, b \in R$.

(R2) $a(bc) = (ab)c$ voor alle $a, b, c \in R$ (associativiteit van $\cdot$);

(R3) $a(b+c) = ab+ac$ en $(b+c)a = ba+ca$ voor alle $a, b, c \in R$ (de distributieve wetten).

(R4) $1 \cdot a = a = a \cdot 1$ voor alle $a \in R$.

Definitie 1.1.2. Een ring R heet *commutatief* als bovendien voldaan is aan (R5):

(R5) $ab = ba$ voor alle $a, b \in R$.

Definitie 1.1.3. Een *delingsring* (of *scheeflichaam*) is een ring R die behalve aan (R1) t/m (R4) ook voldoet aan (R6):

(R6) $1 \neq 0$, en voor alle $a \in R$, $a6 = 0$ is er een inverse $a' \in R$ waarvoor geldt $a \cdot a' = a' \cdot a = 1$.

Definitie 1.1.4. Een lichaam (Engels: field; Frans: corps; Duits: Körper) is een commutatieve delingsring (dus (R1) t/m (R6))

Opmerking 1.1.5. Soms worden 1 en R4 weggelaten

Opmerking 1.1.6. Het kan zo zijn dat $1 = 0$. De ring is dan triviaal $(\{1\}, +, 1, \cdot, 1)$

Opmerking 1.1.7. R1 vertelt ons dat R een abelse groep is. We gebruikNL 2 en R^+ als we de groep $(R, +, 0)$ bedoelen.

1.2 Voorbeelden

Voorbeeld 1.2.1. We geven enkelen voorbeelden van ringen:

- $(\mathbb{Z}, +, 0, \cdot, 1)$ is commutatief en maar geen delingsring, en daarmee geen lichaam.
- $(\mathbb{Z}/n\mathbb{Z}, +, 0, \cdot, 1)$ is altijd commutatief en een delingsring als n priem is (en dan ook een lichaam).
- $(M(n, \mathbb{R}), +, 0_n, \cdot, \mathbb{I}_n)$ (vierkanten matrices) is commutatief $\iff$ $n = 1$ maar geen delingsring.
- $(\mathbb{R}, +, 0, \cdot, 1)$ is commutatief en een delingsring, en daarmee een lichaam.
- $(\mathbb{C}, +, 0, \cdot, 1)$ is commutatief en een delingsring, en daarmee een lichaam.
- $(\mathbb{H}, +, 0, \cdot, 1)$ (de quaternionen) is niet commutatief maar wel een delingsring.

We bewijzen de claim dat $\mathbb{H}$ een delingsring is. Voor $q = a + bi + cj + dk$, zij $\overline{q} = a - bi - cj - dk$ en $N(q) = q \cdot \overline{q} = a^2 + b^2 + c^2 + d^2$. Nu is het zo dat

$$q^{-1} = \frac{\overline{q}}{N(q)}$$

Voorbeeld 1.2.2. Een minder triviaal voorbeeld zijn de vierkante matrices van groote n met elementen uit een andere ring R. De notatie hiervoor is $M(n, \mathbb{R})$

Stelling 1.2.3 (Sylabus 1.8)**.** Zij R een ring.

(i) $a(b_1 + \ldots + b_n) = ab_1 + \ldots + ab_n$

(ii) $(b_1 + \ldots + b_n)a = b_1a + \ldots + b_na$

(iii) $a(b - c) = ab - ac$

(iv) $a \cdot 0 = 0 \cdot a = 0$

Bewijs. Het bewijs is triviaal.[1] □

Gevolg 1.2.4. $1 = 0 \iff R = \{0\}$

Bewijs.

$$1 = 0 \iff \forall x \in R, x = x \cdot 1 = x \cdot 0 = 0 \iff R = \{0\}$$

□

[1] Het bewijs is ook te vinden op bladzijde 10 van de sylabus

1.3 Eenheid

Er zijn ringen waar sommige - maar niet alle - elementen een inverse hebben. Dit noemen we *eenheden.*

Definitie 1.3.1. Een element $a \in R$ heet een *eenheid* (of inverteerbaar) als er een $b \in R$ bestaat met $ab = ba = 1$. Een element $a \in R$ noemt men een *linkseenheid* als er een $b \in R$ is met $ab = 1$ en een *rechtseenheid* als er een $c \in R$ bestaat met $ca = 1$.

Definitie 1.3.2. De verzameling eenheden van R wordt genoteerd R^* en heet de *eenhedengroep* van R. $(R^*, \cdot, 1)$ is een groep.

Voorbeeld 1.3.3. We geven enkelen voorbeelden van ringen:

- $R = (\mathbb{Z}, +, 0, \cdot, 1)$ heeft $R^* = \{1, -1\}$
- $R = (\mathbb{Q}, +, 0, \cdot, 1)$ heeft $R^* = \mathbb{Q} \setminus \{0\}$
- $R = (M(n, \mathbb{R}), +, 0_n, \cdot, \mathbb{I}_n)$ heeft $R^* = \{n \in M(n, \mathbb{R}) \mid \det(n) \neq 0\}$
- $R = (\mathbb{R}, +, 0, \cdot, 1)$ heeft $R^* = \mathbb{R} \setminus \{0\}$
- $R = (\mathbb{C}, +, 0, \cdot, 1)$ heeft $R^* = \mathbb{C} \setminus \{0\}$
- $R = (\mathbb{H}, +, 0, \cdot, 1)$ heeft $R^* = \mathbb{H} \setminus \{0\}$
- $R = (\mathbb{Z}/n\mathbb{Z}, +, 0, \cdot, 1)$ heeft $R^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggd}(a, n) = 1\}$

Opmerking 1.3.4. $1 \in R^*$.

Opmerking 1.3.5. $0 \in R^* \iff 1 = 0$.

Opmerking 1.3.6. R is een delingsring $\iff R^* = R \setminus \{0\}$.

Gevolg 1.3.7. $\mathbb{Z}/n\mathbb{Z}$ is een lichaam $\iff n$ is priem.[2]

Opmerking 1.3.8. Voor p priem is $\mathbb{F}_p$ het lichaam $\mathbb{Z}/p\mathbb{Z}$.

1.4 Deelringen

Definitie 1.4.1. Een deelverzameling R' van een ring R heet een *deelring* van R als aan (D1), (D2) en (D3) voldaan is:

(D1) $1 \in R'$;

(D2) R' is een ondergroep van de additieve groep van R;

(D3) $ab \in R'$ voor alle $a, b \in R'$

$(R', +, \cdot, 0, 1)$ is dan ook een ring.

Opmerking 1.4.2. Als R commutatief is, dan is elke deelring ook commutatief. Het omgekeerde is niet waar, want $R' = \{0\}$.

[2] zie ok stelling 1.20

Definitie 1.4.3. Het *centrum* van een ring is

$$Z(R) = \{a \in R \mid ax = xa \forall x \in R\}.$$

Dit is altijd een commutatieve deelring.

Voorbeeld 1.4.4. De ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is de "ring van gehele getallen van Gauss" met 1 en 0. Ook geldt voor $x = a + bi$ en $y = c + di$ dat

- $x + y = (a + c) + (b + d)i$
- $-x = -a - bi$
- $xy = (ac - bd) + (ad + bc)i$

Ofwel: $\mathbb{Z}[i]$ is commutatief en een deelring van $\mathbb{C}$. Het is geen lichaam: sommgie elementen (bijv 2.) hebben geen inversen.

Voorbeeld 1.4.5. De ring $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ is wel een lichaam.

Voorbeeld 1.4.6. Als $m \in \mathbb{Z}$ geen kwadraat is, dan zijn $\mathbb{Z}[\sqrt{m}]$ een coummutatieve deeling en $\mathbb{Q}[\sqrt{m}]$ een lichaam.

1.5 Nuldelers

Definitie 1.5.1. Een element $a \in R \setminus \{0\}$ heet een *linkernuldeler* als er een $b \in R \setminus \{0\}$ $ab = 0$. Evenzo heet $a \neq 0$ een *rechternuldeler* als er een $c \in R \setminus \{0\}$ $ac = 0$. We noemen a een *nuldeler* als het een linker- of rechternuldeler is.

Definitie 1.5.2. Een *nilpotent* element is een $a \in R \setminus \{0\}$ zo dat $a^n = 0$ voor zekere $n \in N$. Een nilpotent element is een nuldeler, zowel links als rechts.

Definitie 1.5.3. Een element $a \in R$ noemt men een *idempotent element*, of *idempotent*, als a 2 = a. Een idempotent element a met $a \notin \{0, 1\}$ is een nuldeler (zowel links als rechts),

Stelling 1.5.4. Een ring heeft geen elementen die zowel nuldeler als eenheid zijn.

Opmerking 1.5.5. In een niet comuutatieve ring kan een linksnuldeler geen rechtsnuldelerzijn, waar wel een linkseenheid.

Gevolg 1.5.6. Een delingsring heeft geen nuldelers.

Hoorcollege 2

Domeinen

2.1 Voorbereidende opgaves

- $A = (\mathbb{Z}/2\mathbb{Z}, +, 0)$ heeft $\mathrm{End}(A) \cong \mathbb{Z}/2\mathbb{Z}$
- $A = (\mathbb{Z}/3\mathbb{Z}, +, 0)$ heeft $\mathrm{End}(A) \cong \mathbb{Z}/3\mathbb{Z}$
- $\ldots$
- $A = (\mathbb{Z}/k\mathbb{Z}, +, 0)$ heeft $\mathrm{End}(A) \cong \mathbb{Z}/k\mathbb{Z}$

Bewijs. merk op dat $f(0) = 0$ (per definitie). Voor $\overline{m}$ geldt $f(\overline{m}) = f(1 + 1 \ldots 1) = f(1) + \ldots + f(1)$. Daarnast

$$\mathrm{End}(A) = \{f_i : 1 \to \imath \mid i \in \mathbb{Z}/k\mathbb{Z}\} \cong \mathbb{Z}/k\mathbb{Z}$$

□

2.2 Vervolg stelling vorig college

Theorem 2.2.1. *Een linkernuldeler in een ring is geen rechtseenheid.*

Bewijs. Bewijs. Neem $a \in R$ een linkdernuldeler, met $b \in R \setminus \{0\}$ zodat $ab = 0$, en ook een rechtseenheid $c \in R$ zodat $ca = 1$. Dan

$$b = 1b = cab = c0 = 0$$

□

Analoog geldt een rechternuldeler in een ring is geen linkereenheid.

2.3 Domeinen

Definitie 2.3.1 (Domein)**.** Een *domein* is een communtateive ring met $1 \neq 0$ zonder nuldelers.

Remark 2.3.1. *Alle lichamen zijn domeinen, net als* $\mathbb{Z}$ *en* $\mathbb{Z}[\sqrt{n}]$.

Remark 2.3.2. $\mathbb{H}, \mathbb{Z}/n\mathbb{Z}$ *(n niet priem),* $M(n, \mathbb{R})$ *zijn geen domeinen.*

Theorem 2.3.2 (1.23)**.** *Zij R een ring zonder nuldelers (bijv. een domein). Dan*

1. *Voor alle $a, b \in R$ geldt: $ab = 0 \iff a = 0$ of $b = 0$,*
2. *Voor alle $a, b, c \in R$ geldt: $ab = ac \iff a = 0$ of $b = c$.*

Bewijs.
1. $\Longleftarrow$ volgt gelijk. $\Longrightarrow$ als $ab = 0$ en $a \neq 0 \neq b$, dan zijn a en b nuldelers. Dus een tegenspraak.
2. $ab = ac \iff ab - ac = 0 \iff a(b-c) = 0$. Uit (1) volgt $a = 0$ of $b - c = 0 \iff b = c$.

□

2.4 Polynoomringen

Zij R een ring. Een polynoom met coëficienten a_i in R is een uitdrukking van de vorm

$$a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^n = \sum_{i=0}^{\infty} a_i X^n = R[X]$$

waar $N \in \mathbb{N}$ en $a_i \in R$. Claim: dit is een ring met

$$\sum_{i=0}^{\infty} a_i X^n + \sum_{i=0}^{\infty} b_i X^n = \sum_{i=0}^{\infty} (a_i + b_i) X^n$$

en

$$\sum_{i=0}^{\infty} a_i X^n \cdot \sum_{i=0}^{\infty} b_i X^n = \sum_{i=0}^{\infty} c_i X^n$$

waar

$$c_i = \sum_{j+k=1} a_j b_k.$$

Let op:

$$\sum_{j+k=1} a_j b_k \neq \sum_{j+k=1} b_j a_k.$$

Ook geldt

$$0 = \sum_{i=0}^{\infty} 0 X^n$$

en

$$1 = 1 + \sum_{i=1}^{\infty} 0 X^n$$

Een voorbeeld in $\mathbb{C}[X]$:

$$(i + X)(-i + X) = 1 + X^2.$$

De *constante coefficient* van $\sum_{i=0}^{\infty} a_i X^n$ is a_0 De *graad* is $\deg(f) = \mathrm{gr}(f)$ is hoogste n zodat $a_n \neq 0$. We noemen dan a_n de *kopcoöfficient* van f. Als de kopcoöfficient 1 is, dan is f *monisch*. De graad van het nulpolynoom is $-\infty$. Als $\deg(f) \leq 0$ (ofwel $f = a_0$), dan is f *constant*.

2.5 Polynomen in meerdere variabelen

Polynomen in meerdere variabelen worden inductief defefinieerd door $R[X, \ldots X_n] = (R[X, \ldots X_{n-}])[X_n]$. Een $f \in R[X, \ldots X_n]$ is van de vorm

$$\sum_{i_1 \geq 0, i_2 \geq 0, \ldots i_n \geq 0} = a_{i_1, i_2 \ldots, i_n} X_1^{i_1} \cdot X_2^{i_2} \ldots X_n^{i_n}$$

of met multi-indexnotatie

$$\sum_I a_I X^I$$

met

$$X^I = X_1^{i_1} \cdot X_2^{i_2} \ldots X_n^{i_n}$$

Example 2.5.1. Een linksnuldeler die een linkseenheid is. Zij R een nietcommuntatieve ring. Als inleiding bekijken we $A_n = (\mathbb{R}^n, +, 0)$. Merk op dat elke lineraire afbeelding van $\mathbb{R}^n \to \mathbb{R}^n$ een groepshomomorphisme is. Dit laat zien dat $M(n, R) \subset \mathrm{end}(A_n)$

Nu is het zo dan $M(n, R)$ een deelring van $\mathrm{End}(A_n)$ is. Omdat $M(n, R)$ niet communtetief, is $\mathrm{End}(A_n)$ dat ook niet.

We bekijken nu vectoren van willekeurige lengte. Neem $A = \mathbb{R}[X]^+$. Definieer $f, g, h \in \mathrm{End}(A)$:

- $f : a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \mapsto a_1 + a_2 X + a_3 X^2 + \ldots + a_n X^{n-1}$
- $g : a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \mapsto a_0$
- $h : a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \mapsto a_0 X + a_1 X^2 + a_2 X^3 + \ldots + a_n X^{n+1}$

Nu is het zo dat

- $fh = 1$, dus f is een linkseenheid[1].
- $fg = 0$, dus f is een linkernuldeler.

2.6 Quotiëntenlichaam

Het doel van een Quotiëntenlichaam is uit een ring een lichaam construreren. Dit kennen wel al:

$$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$$

Zij R een domein en $S = R \setminus \{0\}$. Dan definieren we de equiavalentierelatie $\sim$ van R op S. Namelijk

$$(a, s) \sim (b, t) \iff at = bs.^2$$

We laten transitivieit ziet, gezien dit niet triviaal is. Neem $(a, s \sim (b, t)$ en $(b, t) \sim (c, u)$, dus $at = bs$ en $bu = ct$. Nu volgt uit $at = bs$ dat $atu = bsu$ en uit $bu = ct$ volgt dat $bus = cts$. R is een domein, dus $atu = bsu = bus = cts$. Nu geldt: $0 = atu - cts = t(au - cs)$. We weten $t \neq 0$, dus wegens stelling 1.23 is het zo dat $au = cs$.

[1] Als je een polynoom opvat als rijtje, dan kun je zien dat h het rijtje naar rechts verschuift en f het rijtje naar links verschuift. Als je eerst naar rechts verschuift en dan weer naar link dan heb je uiteindelijk niks gedaan

[2] In $\mathbb{Q}$ is dit logisch: $\frac{a}{b} = \frac{c}{d} \iff ad = bc$. W

Laat $Q(R) := (R \times S)/\sim$. We gebruiken de notatie $\frac{a}{s} := [(a,s)]$. Dus $Q(R) = \{\frac{a}{s} \mid a, s \in R, s \neq 0\}$.

We definieren $+$ en $\cdot$:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

en

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Dit hangt niet af van de keuze van representanten.

We nemen $(Q(R), +, \cdot, 0 = \frac{0}{1}, 1 = \frac{1}{1})$. Nu is dit een lichaam.

Ook is R een deelring van $Q(R)$. Neem $f : R \to Q(R) : r \mapsto \frac{r}{1}$ als injectieve afbeelding. Dus kunnen we R identificeren met het beeld/deelverzameling $\{\frac{r}{1} \mid r \in R\} \subset Q(R)$. Nu is het zo dat $\forall a, b \in R$ de optelling en vermenigvuldiging "hetzelfde" als in $Q(R)$: $\frac{a}{1} + \frac{b}{1} = \frac{a1+b1}{1 \cdot 1} = \frac{a+b}{1}$ en $\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$. Ergo: elk domein is een deelring.

We noemen $R(X) := Q(R[X])$ het *lichaam van rationale functies*.

Hoorcollege 3

Ringmorfismes

Voorbeeld 3.0.1. (a) Laat R een ring, $R' \subset R$ een deelring. De inclusiefabeelding $R' \to R$ is een ringhomomorfisme. Als $f : A \to B$ een ringhomomorfisme is, dan geldt dat $A \cong \text{Im}(f) \subset B$. We kunnen A dus beschouwen als deelring van B. Namelijk: laat R een domein, als $R \to Q(R) : r \mapsto \frac{r}{1}$. Dit is injectief.

(b) $\forall n \in \mathbb{Z}_{>0}$ is de afbeelding $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto \overline{a}$ een ringhomomorfisme.

(c) In $R = R_1 * R_2$ kan je een ringhomomorfisme maken met de *projectie*afbeelding $f : R \to R_1 : (a, b) \mapsto a$.

(d) Laat $s \in R^*$. Dan is conjucatie met $\gamma_s : R \to R : r \mapsto srs^{-1}$ een ringhomomorfisme. Dan $\gamma_s(r+r') = s(r+r')s^{-1} = srs^{-1}+sr's^{-1} = \gamma_s(r)+\gamma_s(r')$ en $\gamma_s(rr') = s(rr')s^{-1} = srs^{-1}sr's^{-1} = \gamma_s(r)\gamma_s(r')$.

Opmerking 3.0.2.
- Als R commutatief is, dan is γ_s de indentiteit.
- Als $R = M(n, \mathbb{R})$ dan is s een inverteerbare matrix. Dan corresnpondeert γ_s met een basistranformatie.

Definitie 3.0.3. $f : R_1 \to R_2$

1. Het *Beeld* is de verzameling $\{f(x) \mid x \in R_2\} \subset R_2$
2. De *Kern* is de verzameling $\{x \in R_1 \mid f(x) = 0\} \subset R_1$

Opmerking 3.0.4. $f(1) = 1$, dus $1 \notin \text{Ker}(f)$ tenzij $1 = 0$ in R_2. Dit impliceert dat $\text{Ker}(f)$ op de triviale ring nooit een deelring is.

Opmerking 3.0.5. $\text{Ker}(f) = \{0\} \iff f$ is injectief.

3.1 Idealen

Uit algebra 1 weten we dat kernen van groepshomomorfismen zijn normaaldelers. Nu gaan we zien dat kernen van ringhomomorfismen *idealen* zijn.

Definitie 3.1.1. Een *ideaal* I van een ring R is een deelverzameling $I \subset R$ zodat

(I1) I is een ondergroep van R^+.

(I2) $\forall r \in R, a \in I$ geldt dat $ra \in I$.

Opmerking 3.1.2. Als $1 \in I$, dan $r1 = r \in I$ voor alle x. Ergo: $I = R$.

Definitie 3.1.3. (1) Een *rechtsideaal* I van een ring R is een deelverzameling $I \subset R$ zodat

(I1) I is een ondergroep van R^+.

(I2) $\forall r \in R, a \in I$ geldt dat $ra, ar \in I$.

(2) Een *rechtsideaal* I van een ring R is een deelverzameling $I \subset R$ zodat

(I1) I is een ondergroep van R^+.

(I2) $\forall r \in R, a \in I$ geldt dat $ar \in I$.

Voorbeeld 3.1.4. Neem $n \in \mathbb{Z}$. Dan is $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ een ideaal van $\mathbb{Z}$.

Stelling 3.1.5 (Kernen zijn idealen)**.** De kern van een ringhomomorfisme $f : R_1 \to R_2$ is een ideaal van R_1

Bewijs. (I1) I is een ondergroep van R^+: dit is bewezen in Algebra 1.

(I2) $\forall r \in R, a \in I$ geldt dat $ar \in I$. Er geldt: $f(ra) = f(r)f(a) = f(r)0 = 0$, dus $ra \in \ker(f)$.

□

Voorbeeld 3.1.6. $\ker(f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto \overline{a}) = n\mathbb{Z}$

3.2 Voorgebrachte ideaalen en hoofdideaalen

Definitie 3.2.1. R ring, $a_i \in R$ voor alle i. Stel R comuutatief. Het ideaal *voorgebracht* door a_i, $0 < i \leq 1$ is

$$\sum_{i=1}^{n} Ra_i = \{\sum_{i=1}^{n} ra_i \mid r \in R\} =: (a_1, \ldots a_n)$$

Opmerking 3.2.2. Als R niet comuutatief is, dan geeft de vorige definitie een linksideaal.

Voorbeeld 3.2.3. Bekijk $(4, 6) \in \mathbb{Z}$. Dit is $(4, 6) = \{m4 + n6 \mid m, n \in zz\}$. Dit is $2\mathbb{Z}$.

Definitie 3.2.4. Als een ideaal door één element kan worden voortgebracht, heeft het een *hoofdideaal*.

Voorbeeld 3.2.5. Het ideaal $(2, 1 + i) \subset \mathbb{Z}[i]$ is een hoofdideaal met voorbrenger $(1 + i)$.

Opmerking 3.2.6. $I = Ra_i \ldots + Ra_n$ is het kleinste ideaal wat $a_i, \ldots, a_n$ bevat.

Voorbeeld 3.2.7. Het ideaal $(x, y) \subset \mathbb{R}[x, y]$ is geen hoofdideaal.

Definitie 3.2.8. Voor $f = \sum_{i,j>0} a_{i,j}x^iy^j \in R[x, y]$ is de *graad in* x als $gr_x(f) = \max\{m \in z_{\geq 0} \mid \exists i, j \text{ met } a_{i,j} \neq 0 \text{ en } i = m\}$. Analoog definiteren we $gr_y(f)$

Bewijs. Stel dat $f \in \mathbb{R}[x, y]$ het ideaal (x, y) voorbrengt. Dan zijn X, Y veevlouden van g, zeg $X = f_ig$ en $Y = f_2g$. Dan geldt:

- De enige ideaalen van een deelring R zijn $\{0\}$ en R. g, f_1, f_2 niet nul

- $0 = gr_y(x) = gr_y(f_1 g) = gr_y(f_1) + gr(y)(g) \implies gr(y)(g) = 0.$
- Analoog: $gr(x)(g) = 0$.

Maar $(x, y) = \{aX + bY \mid a, b \in \mathbb{R}[x]\}$ bevat enkel (naast nul) elementen elemeten f waarvoor geldt $gr_x(f) \geq 1$ of $gr_y(f) \geq 1$. Dit is een tegenspraak. $\square$

Gevolg 3.2.9. De enige ideaalen van een deelring R zijn $\{0\}$ en R.

Gevolg 3.2.10. Elk ringhomomorfisme van $f : K \to R$ van een lichaam K naar ring $R \neq \{0\}$ is injectief.

Bewijs. $\ker(f)$ is een ideaal van een delingsring. Dus $\ker(f) = \{0\}$ of $\ker(f) = \{K\}$. Dit tweede kan niet: $R \neq \{0\}$ dus $1 \notin \ker(f)$. Nu gelt $\ker(f) = \{0\}$, en daarmee is f injectief. $\square$

3.3 Uitdelen naar ideealen

Idealen hebben te maken met quotienten.

Zij R een ring, $I \subset R$ een ideaal. Dan is I een ondergroep van R^+ per definitie. I is automatisch een normaaldeler, want R^+ is abels.

Nu kunnen we *uitdelen*:

$$R/I = (\{a + I = \overline{a} \mid a \in R\}, +, \overline{0})$$

is een groep. Hiermee kunnen we een ring maken: definieer $\cdot : R/I \times R/I \to R/I : \overline{a} \cdot \overline{b} \mapsto \overline{ab}$

Merk op: het maak niet uit welke representanten we kiezen. Als $\overline{a} = \overline{a'}$ en $\overline{b} = \overline{b'}$, dan

$$ab - a'b' = a(b - b') + (a - a')b' \in I$$

want $(b - b'), (a - a') \in I$.

Nu is het makkelijk te zien dat $(R/I, +, \overline{0}, \cdot, \overline{1})$ een ring is.

Opmerking 3.3.1. Als R commutatief is, dan is R/I ook commutatief.

Voorbeeld 3.3.2. Neem $R = \mathbb{Z}$ met het ideaal $n\mathbb{Z}$. Bekijk $R/I = \mathbb{Z}/n\mathbb{Z}$. Nu heeft R/I wel nuldelers, terwijl R dit niet heeft. Dit in tegenstelling tot deelringen.

Stelling 3.3.3. Laat R een ring zijn en I een ideaal van R. Dan is de natuurlijke afbeelding $\phi : R \to R/I$ een surjectief ringhomomorfisme met $\ker(\phi) = I$.

Bewijs. Het volgt dat ϕ een surjectief groepshomomorfisme is, weten we al uit algebra 1. Ook is het zo dat $\phi(1) = \overline{1}$ en $\phi(ab) = \overline{ab} = \overline{a}\overline{b} = \phi(a)\phi(b)$. $\square$

Gevolg 3.3.4. Zij R een ring. I is een ideaal van $R \iff I$ is de kern van een ringhomomorfisme.

3.4 Evaluatieafbeelding

Stelling 3.4.1. Laat R een commutatieve ring zijn en $\alpha \in R$. Dan is de afbeelding

$$\Phi_\alpha : R[X] \to R,$$

gegeven door

$$\Phi_\alpha(\sum b_i X^i) \mapsto \sum b_i \alpha^i$$

een surjectief ringhomomorfisme. (Merk op dat $\Phi_\alpha(f) = f(\alpha)$.) Bovendien geldt:

$$\ker(\Phi_\alpha) = (X - \alpha) = \{(X - \alpha)f \mid f \in R[X]\}$$

.

Voorbeeld 3.4.2. Niet alle idealen zijn hoofdidealen, zoals we al in 2.12 hebben gezien, en zoals ook het volgende voorbeeld laat zien. Laat $R = \mathbb{Z}[X]$ en zij $I \subset R$ gedefnieerd door

$$I = \{f \in Z[X]f(0) \text{ is even}\} = \{a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X] \mid a_0 \in 2\mathbb{Z}\}$$

.

Om te bewijzen dat I een ideaal is van $\mathbb{Z}[X]$ kan men bijvoorbeeld opmerken dat I de kern is van het samengestelde ringhomomorfisme

$$\mathbb{Z}[X] \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

en de Stelling toepassen.

Stel dat I een hoofdideaal is: $I = (g) = \mathbb{Z}[X] \cdot g$ met $g \in \mathbb{Z}[X]$. Uit $2 \in I = (g)$ volgt dan dat $2 = h \cdot g$ voor een zekere $h \in \mathbb{Z}[X]$. Kijken we naar de graden van deze polynomen, dan zien we dat dit alleen kan als h en g constanten in $\mathbb{Z}$ zijn, dus $g = \pm 1$ of ± 2.

Ook is $X \in I = (g)$, maar dit is voor $g = \pm 2$ onmogelijk. Dus $g = \pm 1$. Uit de definitie van I blijkt echter dat $\pm 1 \notin I$, een tegenspraak.

We concluderen dat I geen hoofdideaal is.

Hoorcollege 4

Isomorfiestellingen, Chinese reststelling

4.1 Voorbereidende opgave

Welke getallen horen er op de open plaatsen?

- $14\mathbb{Z} + 15\mathbb{Z} = ??\mathbb{Z}$
- $6\mathbb{Z} \cap 15\mathbb{Z} = ??\mathbb{Z}$
- $14\mathbb{Z} \cdot 6\mathbb{Z} = ??\mathbb{Z}$

Getallen die voldoen

- $14\mathbb{Z} + 15\mathbb{Z} = \mathbb{Z}$ (grootste gemene deler)
- $6\mathbb{Z} \cap 15\mathbb{Z} = 30\mathbb{Z}$ (kleinste gemeenschappelijk veelvoud)
- $14\mathbb{Z} \cdot 6\mathbb{Z} = 84\mathbb{Z}$ ()

Voorbeeld 4.1.1. Er geldt voor twee idealen I, J:

$$(I + J)(I \cap J) \subset (IJ) + (JI)$$

Bekijk de linker kant. Dit zijn elementen in de vorm $(x + y)z$ waar $x \in I, y \in J, z \in I \cap J$.

$$(x + y)z = xz + yz \mid xz \in IJ, yz \in JI$$

Voorbeeld 4.1.2. Bekijk nu $R = \mathbb{Z}$. De idealen in $\mathbb{Z}$ zijn hoofdidealen, dus $I = a\mathbb{Z}, J = b\mathbb{Z}$

$$(a\mathbb{Z} + b\mathbb{Z})(a\mathbb{Z} \cap b\mathbb{Z}) \subset (a\mathbb{Z}b\mathbb{Z}) + (b\mathbb{Z}a\mathbb{Z})$$

Uit het voorbeeld hierboven volgt:

$$(\mathrm{ggd}\,(a, b)\mathbb{Z})(\mathrm{kgv}(a, b)\mathbb{Z}) \subset ab\mathbb{Z} + ab\mathbb{Z}$$

$$ab\mathbb{Z} = ab\mathbb{Z}$$

4.2 Vervolg evaluatieafbeelding

Bewijs. Dat Φ_α een ringhomorfisme is, is eenvoudig na te rekenen; merk op dat we nodig hebben dat R commutatief is!

Duidelijk is verder dat Φ_α surjectief is, want een element $a \in R$ is het beeld onder Φ_α van het constante polynoom a.

We bewijzen nu dat $\ker(\Phi_\alpha) = (X - \alpha)$.

Voor '$\supset$': Er geldt $\Phi_\alpha(X-\alpha) = \alpha - \alpha = 0$, dus $X - \alpha \in \ker(\Phi_\alpha)$, en omdat $\ker(\Phi_\alpha)$ een ideaal is geldt dan ook $R[X](X-\alpha) \subset \ker(\Phi_\alpha)$. Voor '$\subset$; Stel dat $f = \sum a_i X^i \in \ker(\Phi_\alpha)$, dan geldt $\sum a_i \alpha^i = 0$, dus

$$f = \sum a_i X^i = \sum a_i X^i - \sum a_i \alpha^i = \sum a_i (X^i - \alpha^i) = \sum a_i b(X - \alpha)$$

Hiermee is 2.13 bewezen. □

Voorbeeld 4.2.1. We behandelen enkele voorbeelden.

1. $\Phi_0 : \mathbb{R}[X] \to \mathbb{R} : f \to f(0)$. Dit geeft $\ker \Phi_0 = \{\sum a_i X^i \mid a_0 = 0\} = \{X \sum a_i X^{i-1} \mid a_0 = 0\} = \{Xg \mid g \in \mathbb{R}[x]\} = (X) = (X - 0)$ zoals de stelling ons vertelde.

2. Bekijk $\mathbb{R}[X,Y] = (\mathbb{R}[X])[Y]$. Nu is er voor elke coefficient uit $\mathbb{R}[X]$ ook een evaluatieafbeelding.
$$\Phi_f : R[X,Y] \to R[X] : F_{X,Y} \mapsto F_{X,f(x)}.$$
Wegens de stelling:
$$\ker(\Phi_f) = (Y - f(x)) \subset \mathbb{R}[X,Y]$$

4.3 Stellingen uit Algbra 1

Stelling 4.3.1 (Homomorfiestelling voor ringen)**.** Zij $f : R_1 \to R_2$ een ringhomomorfisme, $I \subset R$ een ideaal met $I \subset \ker(f)$ en $\Phi : R_1 \to R_1/I$ het kanonieke ringhomomorfisme. Dan is er precies één ringhomomorfisme $g : R_1/I \to R_2$ zodat $g \circ \Phi = f$. Bovendien geldt $\ker g = \phi(\ker(f))$

Bewijs. Uit Algebra 1 weten we dat er een uniek groepshomomorfisme is $g : (R_1/I)^+ \to R_2^+$ met $g \circ \Phi = f$ en $\ker(g) = \phi(\ker(f))$. Nu gaan we aantonen dat g een ringhomomorfisme is. Voor $a \in R_1$ schrijven we $\overline{a} = \phi(a) \in R_1/I$

$$g(\overline{1}) = g(\phi(1)) = f(1) = 1$$

en dan

$$g(\overline{a} \cdot \overline{b}) = g(\overline{ab}) = g(\phi(\overline{a})) = f(\overline{ab}) = f(a)f(b) = g(\phi(a))g(\phi(b)) = g(\overline{a}) \cdot g(\overline{b})).$$

□

Stelling 4.3.2 (Eerste isomorfiestelling voor ringen)**.** Zij $f : R_1 \to R_2$ een ringhomomorfisme. Dan is er een isomorfisme van ringen

$$R_1/\ker(f) \to f(R_2) : \overline{a} = a + \ker(f) \to f(a)$$

In het bijzonder geldt er als f surjectief is, dat

$$R_1/\ker(f) \cong R_2$$

Bewijs. Gebruik de homomorfiestelling met $\ker(f) = I$ en $\phi R_1 \to R_1/\ker(f)$. Dus er is een ringhomomorfisme zodat

$$g : R_1/\ker(f) \to R_2$$

met $f = \phi \circ g$ en $\ker(g) = \phi(\ker(f)) = \{\overline{0}\}$. Dus is g injectief.

Omdat ϕ surjectief is, geldt $g(R_1/\ker(f)) = g(\phi(R_1)) = f(R_1)$. Nu geldt dat

$$g : R_1/\ker(f) \to f(R_1)$$

een bijectief ringhomomorfisme is. □

Voorbeeld 4.3.3. Definieer

$$\phi : R[X] \to \mathbb{C} : f \mapsto f(i).$$

We beweren dat ϕ surjectief is: als $z = a+bi \in \mathbb{C}$, dan is er een $f = a+bX$ zodat $\phi(f) = z$. Uit opgave 37 weten we dat $\ker\phi = (X^2+1)$. We passen de eerste isomorfiestelling toe.

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

Voorbeeld 4.3.4. Bekijk

$$f : \mathbb{Z}[i] \to \mathbb{F}_2 : a + bi \mapsto \overline{a} + \overline{b}$$

met kern $(2, i+1) = (i+1)$ (zie opgave 2.10). We passen de eerste isomorfiestelling toe.

$$\mathbb{Z}[i]/(i+1) \cong \mathbb{F}_2$$

Voorbeeld 4.3.5 (Evalutaieafbeelding)**.** Neem $a \in R$, dan geldt $R[X]/(X-a) \cong \mathbb{R}.$˙

Voorbeeld 4.3.6. Idealen voorgebracht door constanten. Neem het ideaal I van de commutatieve ring R. Dan $\mathbb{R}[X] \supset \mathbb{R}[X] \cdot I$ met $I[X] := \{\sum a_iX^i \in \mathbb{R}[X] \mid a_i \in I\}$. De claim is dat $R[X]/I[X] \cong (R/I)[X]$.

Bewijs. Definieer de afbeelding $\mathbb{R}[X] \to (R/I)[X] : \sum a_iX^i \mapsto \sum \overline{a_i}X^i$. Dit is zeker surjectief, en ook is het makkelijk te zine dat het een surjectief ringhomomorfisme is. De kern is $I[X]$. Nu zijn we met de eerste isomorfiestelling klaar.

Stelling 4.3.7 (derde isomofiestelling voor ringen)**.** *Zij R een ring met ideaal I en zij $\phi : R \to R/I$. Dan*

(i) *Als J ook een ideaal is met $I \subset J$, dan is $J/I = \phi(J)$ een ideaal van R/I. Bovendien is elk ideaal van R/I van deze vorm.*

(ii) *Er geldt $(R/I)/(J/I) \cong R/J$.*

Bewijs. Bewijs zoals bij Algebra 1. □

Voorbeeld 4.3.8. Zij I een hoofdideaal voortgebracht door (a) en zij J het ideaal voortgebracht door (a,b). Dan geldt dat $I \subset J$. Noem $\overline{R} = R/(a)$ en $\overline{b} = b + (a)$ het beeld van b in $\overline{R}$.

Beijk $\overline{R} \supset J/I = (a,b)/(a) = (\overline{b})$ en per derde isomofiestelling $\overline{R}/(\overline{b}) = R/(a,b)$.

Opmerking 4.3.9. Neem $a, b, c \in R$. Bekijk (a,b). Dan is dit hezelfde als $(a, b+ca)$.

Voorbeeld 4.3.10. Gegeven $I = (X+Y, X^2+X+Y+1) \subset \mathbb{R}[X,Y]$. Wat is $\mathbb{R}[X,Y]/I$?

Er geldt: $(X+Y, X^2+X+Y+1) = (X+Y, X^2+1)$. Dus $\mathbb{R}[X,Y]/I = \mathbb{R}[X,Y]/(X+Y, X^2+1) \cong (\mathbb{R}[X,Y]/(X+Y))/(\overline{X^2+1})$. We weten uit 2.30 dat $(\mathbb{R}[X])[Y]/(Y-(-X) \cong \mathbb{R}[X]$. Dus $(\mathbb{R}[X,Y]/(X+Y))/(\overline{X^2+1}) \cong \mathbb{R}[X]/(\overline{X^2+1}) \cong \mathbb{C}$.

Stelling 4.3.11 (Chineese reststelling voor ringen)**.** Zij R een commutatieve ring. Neem I, J onderling ondeelbare idealen; ofwel $I + J = R$. Dan geldt

(i) $I \cap J = I \cdot J$

(ii) $R/I \cdot J \cong R/I \cdot R/J$

Bewijs. (i) $I \cap J = I \cdot J$ bewijzen we met twee inclusies. $I \cdot J \subset I \cap J$ is altijd waar. We tonen nog aan $I \cdot J \supset I \cap J$: neem $x \in I, y \in J$ z.d.d $x + y = 1$. Dit kan, want $I \cdot J = R$. Neem $z \in I \cap J$. Dan $z = z * 1 = z(x+y) = zx + zy \in (I \cdot J)$

(ii) Voor $R/I \cdot J \cong R/I \cdot R/J$ gebruiken we de 1e isomorfiestelling. Neem $\xi : R \to R/I$ en $\psi : R \to R/J$. Laat vervolgens $\phi R \to R/I \times R/J : x \mapsto (\xi(x), \psi(x))$ een ringhomomorfisme zijn. Claim ϕ is surjectief met kern $I \cdot J$. Nu volgt de stelling met de 1e isomorfiestelling.

$\square$

Gevolg 4.3.12. Zij $m, n \in \mathbb{Z}$ zodat $\gcd(m,n) = 1$. Dan geldt dat $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Er is een ringisomorfisem $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Voorbeeld 4.3.13. Neem $R = \mathbb{Q}[X], I = (X-1), J = (X+1)$. Er geldt dat $1 \in I + J$, want $1 = -\frac{1}{2}(X-1) + \frac{1}{2}(X+1) \in I + J$. Daarnee zijn I, J onderling ondeelbaar.

$I \cdot J = (X-1)(X+1) = ((X-1)(X+1))$ wegegens voorbeeld 2.35. Met de Chineese reststelling hebben we dat

$$\mathbb{Q}[X]/IJ \cong \mathbb{Q}[X]/I \times \mathbb{Q}[X]/J \cong \mathbb{Q} \times \mathbb{Q}$$

Voorbeeld 4.3.14. We weten dat

$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q} \times \mathbb{Q}.$$

Geldt het dat

$$\mathbb{Q}[X]/(X^p+1) \cong \mathbb{Q}^p?$$

Nee, bekijk

$$\mathbb{Q}[X]/(X^4+1) \cong \mathbb{Q}[X]/(X^2-1) \times \mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i]$$

Deel II

Algebra 2

Hoorcollege 5

Nulpunten van polynomen

5.1 Delen met rest over polynomen

Stelling 5.1.1. Zij R een ring, en $f, g \in R[X]$. Neem aan dat $g \neq 0$ en dat de kopcoëfficiënt van g een eenheid van R is. Dan bestaan er unieke $q, r \in R[X]$ zodanig dat

$$f = qg + r \text{ en } r = 0 \text{ of } gr(r) < gr(g)$$

Men noemt q en r het quotiënt en de rest bij de deling door g. Indien we de conventie aanhouden dat het nulpolynoom graad $-\infty$ heeft, dan hoeven we de mogelijk dat $r = 0$ niet apart te vermelden.

Bewijs. We gaan eerst de existentie van q en r bewijzen. Laat $n = gr(f)$ en $m = gr(g) \geq 0$. We voeren het bewijs, bij vaste g, met inductie naar n.

Als $n < m$ dan kunnen we $q = 0$ en $r = f$ nemen; dit geval is het begin van de inductie.

Laat nu $n \geq m$. Zij a de kopcoëfficiënt van f, en b de kopcoëfficiënt van g. Er is gegeven dat b een eenheid is, dus er is een $c \in R$ zodat $cb = bc = 1$. Het polynoom $acX^{n-m} \cdot g$ heeft dan graad n en kopcoëfficiënt $a \cdot cb = a$. Hieruit volgt dat $f_1 = f - acX^{n-m} \cdot g$ een graad heeft die kleiner dan n is; de n-de graads termen vallen immers tegen elkaar weg. We kunnen op f_1 nu de inductiehypothese toepassen (de stelling geld voor polynomen graad kleiner dan n), en we vinden dat er $q_1, r_1 \in R[X]$ bestaan met: $f_1 = q_1 g + r_1$ en $r_1 = 0$ of $gr(r_1) < gr(g)$. Er geldt dus:

$$f = f1 + acX^{n-m}g = acX^{n-m} + q1 \cdot g + r1.$$

Laat nu $q = acX^{n-m} + q_1$ en $r = r_1$, dan hebben we: $f = qg + r$, $r = 0$ of $gr(r) < gr(g)$, zoals verlangd.

Nu bewijzen we de uniciteit van q en r. Stel dat ook $f = q_0 g + r_0$ en dat $r_0 = 0$ of $gr(r_0) < gr(g)$. Dan hebben we: $(q - q_0)g = r_0 - r$. De graad van het rechterlid is kleiner dan $gr(g)$. Zou nu $q \neq q_0$, dan was de graad van de linkerkant groter dan of gelijk aan $gr(g)$, aangezien de kopcoëfficient van g een eenheid is. Dit levert een tegenspraak, dus moet wel $q = q_0$, en dan ook $r_0 - r = 0$ dus $r = r_0$.

Hiermee is de stelling bewezen. $\square$

Voorbeeld 5.1.2. Zij R een domein en laat $\phi : \mathbb{R}[X, Y] \to R[T] : f \mapsto f(T^3, T^7)$. Dit is een ringhomomorfisme. We willen de $\ker(\phi)$ vinden. We weten zeker $X^7 - Y^3 \in \ker(\phi)$[1]. We claimen dat $\ker(\phi) = (X^7 - Y^3)$.

[1] $\phi(X^7 - Y^3) = T^{7^3} - T^{7^3} = T^{21} - T^{21} = 0$.

Bewijs. Zij $f \in \ker(\phi) \subset (R[X])[Y]$. Laat $g : Y^7 - Y^3$. De kopcoëfficient van g als element van $(R[X])[Y]$ is $-1 \in R[X]^*$. Wegens Stelling 5.1.1 geldt dat er $q, r \in (R[X])[Y]$ zodanig dat $f = qg + r$, en $r = 0$ of $gr_y(r) < gr_y(g) = 3$. Dus $r = f_0 + f_1 Y + f_2 Y^2$ voor zeker $f_0, f_1, f_2 \in R[X]$.

We bekijken nogmaals $0 = \phi(f) = \phi(q)\phi(g) + \phi(r) = \phi(q)0 + \phi(r) = \phi(r) = f_0(T^3) + f_1(T^3)T^7 + f_2(T^3)T^14$. Hieruit volgt dat alle coeffeicienten nul zijn. Merk op dat $f_0(T^3)$ een som van termen $a_iT^i, i \equiv 0 \mod 3$, $f_1(T^3)T^7$ een som van termen $a_iT^i, i \equiv 10 \equiv 1 \mod 3$ en zo ook $f_2(T^3)T^14$ een som van termen $a_iT^i, i \equiv 17 \equiv 2 \mod 3$. Hierdoor kunnen deze termen niet tegen elkaar wegvallen, en moeten ze allemaal gelijk zijn aan 0.

Er volgt: $r = 0$, dus $f = qg$ en daarmee $f \in (Y^7 - Y^3)$. □

Gevolg 5.1.3. Als K een lichaam is, dan is ieder ideaal van $K[X]$ een hoofdideaal.

Bewijs. Zij K een lichaam en $I \subset K[X]$ een ideaal. We zoeken een $x \in K[X]$ zodat $I = (x)$. Als $I = \{0\}$, dan $x = 0$. Als $I = K[X]$, dan $x = 1$. In andere gevallen nemen we we een element $0 \neq x \in I$ van minimale graad. Nu is het zo dat x het ideaal voortbrengt:

- $K[X] \cdot g \subset I$ is altijd waar per definitie van een ideaal.
- Voor $K[X] \cdot g \supset I$ nemen we een willekeurig element $f \in I$. Gezien K een lichaam is, is de kopcoëfficiënt een eenheid. Dus weten we per Stelling 5.1.1 dat $\exists! q, r \in K[X]$ zodat $f = qg + r$ en $r = 0$ of $gr(r) < gr(g)$. We willen laten zien dat dit laatste niet kan.

  We weten dat $r = f - gh \in I$, dus $gr(r) \geq gr(g)$, waarmee $r = 0$ en $f = qg$. Dan $f \in (g)$.

□

Stelling 5.1.4. Zij R een commutatieve ring, $\alpha \in R$ en $f \in R[X]$. Dan is er een $q \in R[X]$ zodat

$$f = q(X - \alpha) + f(\alpha).$$

Bewijs. Gebruik Stelling 5.1.1 met $g = X - \alpha$ en merk op dat $gr(r) < 1$ impliceert dar $r \in \{0, 1\} \subset R[X]$. □

Definitie 5.1.5. Zij R een ring, $f = \sum_{i=1}^n a_i X^i \in R[X]$. Dan noemen we α een *nulpunt* van f als $f(\alpha) = 0$.

Stelling 5.1.6. Zij R een domein, $f \in R[X]$ en $\alpha_1, \alpha_2, \dots \alpha_n \in R$ n nulpunten van f zijn. Dan is er een $q \in R[X]$ zodat $f = q(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$

Bewijs. We gaan inductie doen naar n. Als $n = 1$, volgt dit uit Stelling 5.1.1.

Als n 1. dam os er wegens Stelling 5.1.1 een $f_1 \in R[X]$ zodat

$$f = f_1(x - \alpha_n). \tag{5.1}$$

Als we nu voor $i = 1, \dots, n-1$ de subsitutie van α_i in Vergelijking 5.1 doen, dan geldt

$$0 = f(\alpha_i) = f_1(\alpha_i)(\alpha_i - \alpha_n).$$

Gezien $\alpha_i - \alpha_n \neq 0$, volgt dat $f_1(\alpha_i) = 0$.

Wegens de inductiehypothese is er een q zodat $f_1 = q(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{n-1})$ en daarmee

$$f = q(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{n-1})(x - \alpha_n)$$

□

Stelling 5.1.7. Zij R een domein, en $f \in R[X]$ een polynoom ongelijk aan nul. Dan is het aantal onderling verschillende nulpunten van f in R ten hoogste gelijk aan $gr(f)$.

Bewijs. Dit volgt uit Stelling 5.1.6, want als $\alpha_1, ..., \alpha_n$ verschillende nulpunten zijn van f dan is $f = q \cdot (X - \alpha 1)...(X - \alpha_n)$. Dit geeft $gr(f) = gr(q) + n$, dus $gr(f) \geq n$. □

Opmerking 5.1.8. De eis in Stelling 5.1.7 dat R een domein is, is essentieel. Het polynoom $X^2 - 1$ in $(\mathbb{Z}/8\mathbb{Z})[X]$ van graad 2 heeft 4 nulpunten in $Z/8Z$ en $X^2 + 1 \in H[X]$ heeft zelfs oneindig veel nulpunten in H. De ringen $\mathbb{Z}/8\mathbb{Z}$ en H zijn dan ook geen domeinen: $\mathbb{Z}/8\mathbb{Z}$ heeft nuldelers en H is niet commutatief.

5.2 Dubbele nulpunten en afgeleides

Opmerking 5.2.1. Het is ook gemakkelijk in te zien dat er polynomen waarbij er minder dan n nulpunten zijn. Bekijk $(X - \alpha)^d$, $X^2 + 1 \in R[X]$.

Definitie 5.2.2. Zij R een domein, $f \in R[X] \setminus \{0\}, \alpha \in R$ een nulpunt. We noemen α een *meervoudig nulpunt* als in de schrijfwijze $f = q(X - \alpha)$ geldt $q(\alpha) = 0$.

Definitie 5.2.3. Zij R een domein, $f \in R[X]$. De *afgeleide* van $f = \sum_{i=1}^{n} a_i X^i$ is

$$f' = \sum_{i=1}^{n} i a_i X^{i-1}$$

Lemma 5.2.4. *Zij R een commutatieve ring. Dan geldt*

(i) $(f + g)' = f' + g'$;

(ii) $(cf)' = cf'$;

(iii) $(fg)' = fg' + gf'$.

Stelling 5.2.5. Zij R een commutatieve ring, $f \in R[X]$. Dan is α een dubbel nulpunt van $f \iff \alpha$ is een nulpunt van f'.

Bewijs. Zij $f = q(X - \alpha)$. Dan geldt

$$f' = (q(X - \alpha)' = q(X - \alpha)' + q'(X - \alpha) = q + q'(X - \alpha) \implies f'(\alpha) = q(\alpha).$$

We hebben dan dat

$$f'(\alpha) = 0 \iff q(\alpha) = 0 \iff \alpha \text{ is een dubbel nulpunt van } f$$

□

Stelling 5.2.6. Zij p priem. In $\mathbb{F}_p[X]$ geldt

$$\prod_{a \in \mathbb{F}_p} (X - a) = X^p - X$$

Bewijs. Voor alle $a \in \mathbb{F}_p$ geldt dat $a^P = a$ wegens de kleine stelling van Fermat. Dan zijn alle p elementen van $\mathbb{F}_p$ nulpunten van$X^p - X$. Daarnaast is $\mathbb{F}_p$ een domein; daarmee zijn er niet meer nulpunten dan dit.

Nu geeft Stelling 5.1.6 ons dat

$$X^p - X = q \prod_{a \in \mathbb{F}_p} (X - a)$$

Met het vergelijk van graden vinden we dat q constant is. Als we de kopcoefficienten vergelijken kan je concluderen dat $q = 1$. □

Gevolg 5.2.7. Zij p priem. Dan geldt $(p-1)! \equiv -1 \mod p$

Bewijs. Bekijk Stelling 5.2.6 die zegt dat

$$\prod_{a \in \mathbb{F}_p} (X - a) = X^p - X.$$

Nu geldt ook

$$X \prod_{a \in \mathbb{F}_p \setminus \{0\}} (X - a) = x(X^{p-1} - 1)$$

Er volgt

$$\prod_{a \in \mathbb{F}_p \setminus \{0\}} (X - a) = (X^{p-1} - 1)$$

Neem $X = 0$. Dan

$$(-1)^{p-1} \prod_{a \in \mathbb{F}_p \setminus \{0\}} (a) = (-1)$$

wat gelijk is aan

$$(p-1)! \equiv (-1)$$

mod 3. □

Lemma 5.2.8. *Zij n het element van maximale orde in een eindige abels groep G met orde m. Dan voldoet elke $y \in G$ aan $y^m = 1$*

Stelling 5.2.9. Zij R een domein en $G \subset R$ een eindig ondergroep. Dan is G cyclisch.

Bewijs. Omdat R een domein is, is G abels. Zij $x \in G$ een element van maximale order m. Dit element bestaat wegens de eindigheid van de groep.

Dan brengt x de groep G voort: Stelling 5.2.8 geeft ons dat elke $b \in G$ een nulpunt is van $X^m - 1 \in R[X]$. Dit geeft dat $\#G \leq m$ wegens Stelling 5.1.7. G bevat de ondergroep $< a >$, die m element heeft. Dus moet $G =< a >$ □

Gevolg 5.2.10. Zij p priem. Dan is $\mathbb{F}_p[X]$ cyclisch van orde $p - 1$.

Definitie 5.2.11. Elk element van eindig orde in R^* heten *eenheidswortels*.