Het pythagorasgetal van enkele commutatieve ringen

Nicolas Daans

Bachelorproef in de fundamentele wiskunde vervaardigd
onder begeleiding van prof. Karim Johannes Becher

Voorgelegd aan de UA in mei 2016
Gecorrigeerde versie van augustus 2016

Inhoudsopgave

Inleiding

In 1772 bewees Lagrange zijn vierkwadratenstelling, die stelt dat elk natuurlijk getal geschreven kan worden als een som van vier kwadraten van natuurlijke getallen. We kunnen dit opvatten als een eigenschap van de commutatieve ring $\mathbb{Z}$. Dit is de idee achter de definitie van het *pythagorasgetal* van een commutatieve ring A als het kleinste natuurlijke getal k met de eigenschap dat elke som van kwadraten in A geschreven kan worden als een som van k kwadraten - als zo een getal niet bestaat, zeggen we dat het pythagorasgetal ∞ is. De vierkwadratenstelling van Lagrange zegt dan precies dat vier het pythagorasgetal van $\mathbb{Z}$ is.

Het doel van dit artikel is om een idee te geven welke resultaten er over het pythagorasgetal van commutatieve ringen bestaan en hoe deze bewezen worden. Hiernaast is er ook nog veel bekend over het pythagorasgetal van lichamen, maar die resultaten zijn grotendeels gefundeerd op de theorie van de kwadratische vormen, waar we in dit artikel niet te diep op in wilden gaan. *Introduction to Quadratic Forms over Fields* [7] van T. Y. Lam is een goed vertrekpunt voor wie hier meer over wilt weten. Wij zullen in dit artikel enkel uitgaan van een basiskennis commutatieve algebra.

In het eerste hoofdstuk worden, naast enkele basiseigenschappen, vooral veel voorbeelden gegeven. Zo kijken we naar het bewijs van de vierkwadratenstelling en bespreken we kort waarom hieruit volgt dat ook $\mathbb{Q}$ pythagorasgetal vier heeft. Wegens de analogie in de manier van bewijzen, tonen we ook aan welke natuurlijke getallen als som van twee kwadraten geschreven kunnen worden. We introduceren het nauw verwante concept van *het level* van een commutatieve ring en gebruiken dit om het pythagorasgetal van $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}[X]$ te berekenen voor algemene $n \in \mathbb{N}$. Verder bewijzen we dat het pythagorasgetal van ieder eindig lichaam met van twee verschillende karakteristiek twee is.

Hierna, in het tweede hoofdstuk, bekijken we voor enkele klassen van ringen welke bovengrenzen we kunnen vinden voor het pythagorasgetal. We bekijken in het bijzonder wat we kunnen zeggen over eindigdimensionale k-algebra's (voor eender welk lichaam k) en over $\mathbb{R}$-algebra's met transcendentiegraad 1 over $\mathbb{R}$. Tussendoor tonen we aan dat, voor ieder natuurlijk getal $n \in \mathbb{N}_+$, de ring $\mathbb{R}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^3$ pythagorasgetal n heeft en dat dus elk natuurlijk getal bereikt kan worden als het pythagorasgetal van een zekere commutatieve ring.

Ten slotte bekijken we in het derde hoofdstuk enkele voorbeelden van ringen

met oneindig pythagorasgetal. Een commutatieve ring A heeft oneindig pythagorasgetal indien er geen $k \in \mathbb{N}$ bestaat zodanig dat elke som van kwadraten in A een som van k kwadraten is. Via een verrassend algemene constructie zullen we onder andere kunnen aantonen dat $\mathbb{Z}[X]$, $\mathbb{Q}[X, Y]$ en $\mathbb{R}[X, Y]$ oneindig pythagorasgetal hebben. In de laatste sectie van dat hoofdstuk bespreken we enkele voorbeelden van ringen met oneindig pythagorasgetal die toch 'dicht bij' (een) ring(en) met eindig pythagorasgetal liggen.

Vele van de eenvoudige resultaten uit het eerste hoofdstuk heb ik zelf of met de hulp van prof. Becher bewezen, de stellingen in het tweede en derde hoofdstuk komen grotendeels uit de voornaamste inspiratiebron voor dit werkje: het artikel *The Pythagoras number of some affine algebras and local algebras* van M.D. Choi, Z.D. Dai, T.Y. Lam en B. Reznick uit 1981. [3] Ik bedank mijn begeleider prof. Karim Johannes Becher, zowel voor zijn ideeën voor de invulling van dit werk als voor het kritisch nalezen van eerdere versies. Met zijn tips heb ik enkele definities, stellingen en bewijzen substantieel kunnen vereenvoudigen, verduidelijken en veralgemenen. Tot slot bedank ik ook mijn klasgenoot Arne Mertens voor zijn vele tips en verbeteringen, alsook prof. David Leep voor de interessante gesprekken over dit onderwerp.

Hoofdstuk 1

Het pythagorasgetal

1.1 Definities en eerste observaties

Zij $(A, +, \cdot, 0, 1)$ altijd een commutatieve ring. We noteren $\mathbb{N}$ voor de verzameling van natuurlijke getallen (inclusief 0) en $\mathbb{N}_+$ voor $\mathbb{N} \setminus \{0\}$. Verder noteren we $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ en $\mathbb{C}$ voor de verzamelingen der gehele, rationale, reële en complexe getallen respectievelijk.

Definitie 1.1.1. (1) Neem $n \in \mathbb{N}_+$. Definieer de verzamelingen

$$\Sigma_n A^2 = \{\sum_{i=1}^{n} a_i^2 \mid a_1, ..., a_n \in A\}$$
$$\Sigma A^2 = \bigcup_{m=1}^{\infty} \Sigma_m A^2.$$

De elementen van $\Sigma_n A^2$ noemen we de *sommen van n kwadraten*, de elementen van ΣA^2 simpelweg de *sommen van kwadraten* in A.

(2) Voor $a \in A$ definiëren we de *lengte* van a in A als

$$l_A(a) = \inf\{n \in \mathbb{N}_+ \mid a \in \Sigma_n A^2\}.$$

Indien er geen verwarring kan ontstaan, schrijven we $l(a)$ in plaats van $l_A(a)$. Het is het kleinste natuurlijk getal n zodat a als een som van n kwadraten geschreven kan worden, of ∞ als a niet als som van kwadraten geschreven kan worden.

(3) Het *pythagorasgetal* van A is

$$P(A) = \sup\{l(a) \mid a \in \Sigma A^2\} \in \mathbb{N}_+ \cup \{\infty\}$$

of equivalent

$$P(A) = \inf\{n \in \mathbb{N}_+ \mid \Sigma_n A^2 = \Sigma A^2\}.$$

Volgens bovenstaande definitie is $l(0) = 1$ in iedere ring en dus ook $P(A) = 1$ als A de nulring is. Men zou ook kunnen stellen dat 0 het enige element is van lengte 0, maar wij zullen deze conventie niet volgen. In ieder geval zal het niet veel uitmaken in dit paper en dikwijls zullen we impliciet onderstellen dat de ringen die we gebruiken niet de nulring zijn.

Merk op dat een eindig pythagorasgetal zeker niet impliceert dat elke $a \in A$ een som van kwadraten is (denk bijvoorbeeld aan $A = \mathbb{R}$), enkel dat die elementen in A die sommen van kwadraten zijn, geschreven kunnen worden als sommen van hoogstens $P(A)$ kwadraten. Er geldt $P(A) = \infty$ wanneer elementen van willekeurig hoge, eindige lengte kunnen worden gevonden. Voorbeelden van ringen met oneindig pythagorasgetal volgen in hoofdstuk 3.

Schrijf $\text{char}(A)$ voor de kleinste $k \in \mathbb{N}_+$ zodanig dat $k = 0$ in A of stel $\text{char}(A) = 0$ indien zo een getal niet bestaat. We noemen $\text{char}(A)$ de karakteristiek van A.

Voorbeelden 1.1.2. (1) In $\mathbb{R}$ zijn sommen van kwadraten altijd positieve getallen en van positieve getallen kan men wortels trekken, zodat elke som van kwadraten zelf een kwadraat is. Dit toont dat $\Sigma\mathbb{R}^2 = [0, \infty[$ en $P(\mathbb{R}) = 1$. In $\mathbb{C}$ heeft de vergelijking $X^2 - a = 0$ een oplossing voor elk getal $a \in \mathbb{C}$, dus is elk getal een kwadraat. We hebben dat $\Sigma\mathbb{C}^2 = \mathbb{C}$ en $P(\mathbb{C}) = 1$.

(2) Zij A een commutatieve ring met $\text{char}(A) = 2$. Dan is $2 = 0$ en hebben we voor $n \in \mathbb{N}_+, x_1, \ldots, x_n \in A$ dat $x_1^2 + \ldots + x_n^2 = (x_1 + \ldots + x_n)^2$, zodat elke som van kwadraten vanzelf een kwadraat is. Bijgevolg is $P(A) = 1$.

(3) We tonen dat $\Sigma\mathbb{Z}^2 = \mathbb{N}$ en $\Sigma\mathbb{Q}^2 = \mathbb{Q} \cap [0, \infty[$. Uit (1) en het feit dat $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ volgt meteen dat $\Sigma\mathbb{Z}^2 \subseteq \mathbb{N}$ en dat $\Sigma\mathbb{Q}^2 \subseteq [0, \infty[$. Omgekeerd: het is duidelijk dat $0 \in \Sigma\mathbb{Q}^2 \cap \Sigma\mathbb{Z}^2$. Verder kan elk element van $\mathbb{Q} \cap]0, \infty[$ geschreven worden als $\frac{a}{b}$ voor zekere $a, b \in \mathbb{N}_+$, zodat

$$\frac{a}{b} = \frac{ab}{b^2} = \sum_{i=1}^{ab} \left(\frac{1}{b}\right)^2 \in \Sigma\mathbb{Q}^2$$

en dus $\mathbb{Q} \cap [0, \infty[\subseteq \Sigma\mathbb{Q}^2$. Door voor een willekeurige $a \in \mathbb{N}_+$ bovenstaande gelijkheden te beschouwen voor $b = 1$, vinden we bovendien $\mathbb{N} \subseteq \Sigma\mathbb{Z}^2$.

We noteren A_S voor de lokalisatie van een ring A aan een multiplicatief gesloten deel S en $\text{Frac}(A)$ voor het breukenlichaam van een domein A. Voor een deelverzameling $C \subseteq A$ en $a \in A$ noteren we aC voor de verzameling $\{ac \mid c \in C\}$.

Propositie 1.1.3. *Zij A en B commutatieve ringen.*

(1) Zij $f : A \to B$ een ringmorfisme. Dan geldt $l(f(a)) \leq l(a)$ voor iedere $a \in A$. Als f surjectief is, dan is voor iedere $n \in \mathbb{N}_+$ $\Sigma_n B^2 = f(\Sigma_n A^2)$ en bijgevolg $P(B) \leq P(A)$. In het bijzonder is $P(A/I) \leq P(A)$ voor elk ideaal I van A.

(2) Zij S een multiplicatief deel van A. Dan geldt voor $a \in A, b \in S$ en $n \in \mathbb{N}_+$

$$\frac{a}{b} \in \Sigma_n A_S^2 \Leftrightarrow \exists s \in S : as^2 \in b\Sigma_n A^2.$$

In het bijzonder is $l(\frac{a}{1}) \leq l(a)$ voor iedere $a \in A$ en geldt $P(A_S) \leq P(A)$.

(3) Zij $n \in \mathbb{N}_+$ en $(A_i)_{i\in I}$ een collectie commutatieve ringen. Dan geldt

$$\Sigma_n \left(\prod_{i\in I} A_i \right)^2 = \prod_{i\in I} \left(\Sigma_n A_i^2 \right).$$

Bijgevolg is $P\left(\prod_{i\in I} A_i\right) = \sup_{i\in I} P(A_i)$.

Bewijs. Stel dat $f : A \to B$ een ringmorfisme is, neem $a \in A$. Als $l(a) = \infty$, is $l(f(a)) \leq l(a)$ triviaal. Stel $l(a) = n < \infty$. Dan bestaan er $a_1, \ldots, a_n \in A$ zodanig dat

$$a = \sum_{i=1}^{n} a_i^2.$$

Er volgt dat

$$f(a) = f\left(\sum_{i=1}^{n} a_i^2 \right) = \sum_{i=1}^{n} f(a_i)^2 \in \Sigma_n B^2,$$

zodat $l(f(a)) \leq n = l(a)$. Als $f : A \to B$ een surjectief ringmorfisme is, dan is $\Sigma_n B^2 = \Sigma_n f(A)^2 = f(\Sigma_n A^2)$ voor iedere $n \in \mathbb{N}_+$, zodat $P(B) \leq P(A)$.
Voor het tweede deel, neem $a \in A, b \in S$ en $n \in \mathbb{N}_+$ zodat $\frac{a}{b} \in \Sigma_n A_S^2$. Dan bestaan er $a_1, ..., a_n \in A, c \in S$ met

$$\frac{a}{b} = \sum_{i=1}^{m} \left(\frac{a_i}{c} \right)^2.$$

Er bestaat dan een $s \in S$ zodanig dat achtereenvolgens

$$ac^2 s = bs \sum_{i=1}^{n} a_i^2$$

$$a(cs)^2 = b \sum_{i=1}^{n} (sa_i)^2$$

en dus $a(cs)^2 \in b\Sigma_n A^2$. Omgekeerd, stel $s \in S$ zodanig dat $as^2 \in b\Sigma_n A^2$. Dan bestaan er $a_1, \ldots, a_n \in A$ met achtereenvolgens

$$as^2 = b \sum_{i=1}^{n} a_i^2$$

$$\frac{a}{b} = \sum_{i=1}^{n} \left(\frac{a_i}{s} \right)^2$$

zodat $\frac{a}{b} \in \Sigma_n A_S^2$. Dit toont de equivalentie in het tweede deel aan. $l(\frac{a}{1}) \leq l(a)$ voor $a \in A$ volgt door $s = b = 1$ te stellen in het rechterlid van de equivalentie. $P(A_S) \leq P(A)$ volgt ook aangezien voor alle $a \in A, b \in S, n \in \mathbb{N}_+$ en $m = P(A)$

$$\frac{a}{b} \in \Sigma_n A_S^2 \Rightarrow \exists s \in S : as^2 \in b\Sigma_n A^2$$
$$\Rightarrow \exists s \in S : as^2 \in b\Sigma_m A^2 \Rightarrow \frac{a}{b} \in \Sigma_m A_S^2.$$

waar we $P(A) < \infty$ onderstelden, aangezien de ongelijkheid anders triviaal geldig is. Voor het laatste deel tenslotte, neem $(a_i)_{i\in I} \in \prod_{i\in I} A_i$. Onderstel dat $(a_i)_{i\in I} \in \prod_{i\in I} \left(\Sigma_n A_i^2\right)$, dan bestaat er per definitie een collectie elementen $(a_{ij})_{i\in I, 1\leq j\leq n}$ (met $a_{ij} \in A_i$) zodanig dat

$$a_i = \sum_{j=1}^{n} a_{ij}^2 \quad \forall i \in I.$$

Dit is equivalent met

$$(a_i)_{i\in I} = \left(\sum_{j=1}^{n} a_{ij}^2\right)_{i\in I} = \sum_{j=1}^{n} (a_{ij})_{i\in I}^2,$$

hetgeen betekent dat $(a_i)_{i\in I} \in \Sigma_n \left(\prod_{i\in I} A_i\right)^2$. □

1.2 Compositieformules

Propositie 1.2.1. *Stel $a, b \in \Sigma A^2$. Er gelden:*

- $a + b \in \Sigma A^2$ *en* $l(a + b) \leq l(a) + l(b)$
- $ab \in \Sigma A^2$ *en* $l(ab) \leq l(a)l(b)$

Bewijs. Duidelijk. □

De volgende formules laten toe om, voor bepaalde waarden van $l(a)$ en $l(b)$, een sterkere afschatting te vinden voor $l(ab)$. Ze staan bekend als *compositieformules* voor sommen van kwadraten.

Stelling 1.2.2 (Compositieformules)**.** *Zij $k \in \{1, 2, 4, 8\}$. Voor iedere $a_1, \ldots, a_k$, $b_1, \ldots, b_k \in A$ bestaan er $c_1, \ldots, c_k \in A$ zodanig dat*

$$\left(\sum_{i=1}^{k} a_i^2\right) \cdot \left(\sum_{i=1}^{k} b_i^2\right) = \sum_{i=1}^{k} c_i^2.$$

Deze $c_1, \ldots, c_k$ kunnen als volgt gekozen worden:

$$\begin{aligned}
c_1 &= a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7 - a_8b_8 \\
c_2 &= a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3 + a_5b_6 - a_6b_5 - a_7b_8 + a_8b_7 \\
c_3 &= a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2 + a_5b_7 + a_6b_8 - a_7b_5 - a_8b_6 \\
c_4 &= a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1 + a_5b_8 - a_6b_7 + a_7b_6 - a_8b_5 \\
c_5 &= a_1b_5 - a_2b_6 - a_3b_7 - a_4b_8 + a_5b_1 + a_6b_2 + a_7b_3 + a_8b_4 \\
c_6 &= a_1b_6 + a_2b_5 - a_3b_8 + a_4b_7 - a_5b_2 + a_6b_1 - a_7b_4 + a_8b_3 \\
c_7 &= a_1b_7 + a_2b_8 + a_3b_6 - a_4b_6 - a_5b_3 + a_6b_4 + a_7b_1 - a_8b_2 \\
c_8 &= a_1b_8 - a_2b_7 + a_3b_5 + a_4b_5 - a_5b_4 - a_6b_3 + a_7b_2 + a_8b_1
\end{aligned}$$

waarbij we $a_i = b_i = 0$ stellen voor $k < i \leq 8$ in het geval $k \in \{1, 2, 4\}$.

Bewijs. Elk van deze formules kan nagegaan worden door beide leden uit te werken. □

Gevolg 1.2.3. *Zij $k \in \{1, 2, 4, 8\}$, dan geldt voor $a, b \in \Sigma_k A^2$ dat $ab \in \Sigma_k A^2$.*

Voor een commutatieve ring A, noteer $A^\times$ voor de inverteerbare elementen in A. Analoog noteren we $(\Sigma_k A^2)^\times$ voor $\Sigma_k A^2 \cap A^\times$. Als F een lichaam is, is $F^\times = F \setminus \{0\}$ per definitie.

Gevolg 1.2.4. *Zij $k \in \{1, 2, 4, 8\}$ en F een lichaam. Dan is $(\Sigma_k F^2)^\times$ een deelgroep van $(F^\times, \cdot, 1)$.*

Bewijs. $1 = 1^2 \in F^{\times 2} \subseteq (\Sigma_k F^2)^\times$ en wegens het voorgaande gevolg is $(\Sigma_k F^2)^\times$ gesloten onder vermenigvuldiging. Verder, als $a \in (\Sigma_k F^2)^\times$, dan

$$\frac{1}{a} = \left(\frac{1}{a}\right)^2 a \in (\Sigma_k F^2)^\times.$$

□

Gevolg 1.2.3 betekent onder andere dat, als er een deel $S \subseteq \Sigma A^2$ bestaat zodanig dat elk element van ΣA^2 een product van elementen uit S is, we uit $S \subseteq \Sigma_k A^2$ mogen concluderen dat $\Sigma A^2 = \Sigma_k A^2$ voor $k \in \{1, 2, 4, 8\}$. Dit laat ons bijvoorbeeld toe om ons in het bewijs van de Vierkwadratenstelling te beperken tot priemgetallen, zie Stelling 1.5.4.

We kunnen elke ring A op een unieke manier opvatten als een $\mathbb{Z}$-algebra. Dit laat ons toe om het bestaan van compositieformules voor $k \in \{1, 2, 4, 8\}$ anders te formuleren: voor $k \in \{1, 2, 4, 8\}$ geldt dat $(X_1^2 + \ldots + X_k^2)(Y_1^2 + \ldots + Y_k^2)$ een som van k kwadraten is in $A_k = \mathbb{Z}[X_1, \ldots, X_k, Y_1, \ldots, Y_k]$. Hurwitz bewees in 1898 het omgekeerde, i.e. als voor zekere $k \in \mathbb{N}_+$ geldt dat $(X_1^2 + \ldots + X_k^2)(Y_1^2 + \ldots Y_k^2)$ een som van k kwadraten is in A_k, dan is $k \in \{1, 2, 4, 8\}$. We kunnen dus niet hopen om voor andere waarden van k een compositieformule te vinden. [11, p. 2]

Rond 1965 breidde Pfister de kennis hierover uit. $\Sigma_k F^2 \setminus \{0\}$ vormt een deelgroep met de vermenigvuldiging voor elk lichaam F als en slechts als $k = 2^l, l \in \mathbb{N}$. [11, p. 4] In het bijzonder betekent dit dat $(X_1^2+\ldots+X_k^2)(Y_1^2+\ldots+Y_k^2)$ voor iedere $k = 2^l, l \in \mathbb{N}$ een som van k kwadraten is in $\mathbb{Q}(X_1, \ldots, X_k, Y_1, \ldots, Y_k)$. Voor een uitgebreide bespreking van compositieformules voor sommen van kwadraten (en algemener, kwadratische vormen), zie [11].

1.3 Level van een commutatieve ring

In deze sectie bespreken we kort een verband tussen het pythagorasgetal van een ring en een andere invariant, het level. Zij A steeds een commutatieve ring.

Definitie 1.3.1. We definiëren het *level* van A als

$$S(A) = l_A(-1)$$

Het level van een commutatieve ring is oneindig als en slechts als -1 niet geschreven kan worden als som van kwadraten. Uit Propositie 1.1.3 halen we meteen de volgende eenvoudige eigenschappen:

Propositie 1.3.2. *(1) Zij $f : A \to B$ een ringmorfisme in een commutatieve ring B. Dan geldt $S(B) \leq S(A)$. In het bijzonder is $S(A/I) \leq S(A)$ voor elk ideaal I van A.*

(2) Zij S een multiplicatief deel van A, dan is $S(A_S) \leq S(A)$. In het bijzonder is $S(\mathrm{Frac}(A)) \leq S(A)$ voor een domein A.

(3) Zij $n \in \mathbb{N}_+$ en $(A_i)_{i\in I}$ een collectie commutatieve ringen. Dan geldt dat $S\left(\prod_{i\in I} A_i\right) = \sup_{i\in I} S(A_i)$.

Bewijs. De drie uitspraken volgen direct uit de overeenkomstige uitspraken in Propositie 1.1.3 (bij de eerste gebruikend dat $f(-1) = -f(1) = -1$). □

Voorbeelden 1.3.3. (1) $S(\mathbb{R}) = S(\mathbb{Q}) = S(\mathbb{Z}) = \infty$

(2) $S(\mathbb{C}) = 1$

(3) Als A een commutatieve ring is met $k = \mathrm{char}(A) \neq 0$, dan is

$$0 = \underbrace{1+\ldots+1}_{k \text{ keer}} \quad \text{en dus} \quad -1 = \underbrace{1+\ldots+1}_{k-1 \text{ keer}}.$$

Bijgevolg is $-1 \in \Sigma_{k-1}A^2$, zodat $S(A) \leq k-1 < \infty$.

Als het level oneindig is, geeft dit geen informatie over het pythagorasgetal (bijvoorbeeld $\mathbb{R}$ en $\mathbb{Q}$ hebben hetzelfde level, maar een ander pythagorasgetal). Dit wordt nog verder gesterkt in Gevolg 2.2.10, waar we tonen dat ieder natuurlijk getal bekomen kan worden als pythagorasgetal van een ring met oneindig level. In het geval het level van een ring eindig is, biedt het echter zowel een onder- als bovengrens voor het pythagorasgetal. Het bewijs van volgende stelling is voor een groot deel overgenomen uit [10, hoofdstuk 7].

Stelling 1.3.4 (Joly-Peters)**.** *Zij A een commutatieve ring met $S = S(A) < \infty$. Dan gelden*

(1) $S \leq P(A) \leq S + 2$.

(2) Als S even is, dan $S \leq P(A) \leq S + 1$.

(3) $4A \subseteq \Sigma_{S+1}A^2$. *Bijgevolg, als* $2 \in A^\times$, *dan is* $A = \Sigma A^2$ *en* $S \leq P(A) \leq S + 1$.

Bewijs. Omdat $S < \infty$, is $-1 \in \Sigma A^2$ en is dus $S = l(-1) \leq P(A)$. Neem $z_1, \ldots, z_S \in A$ zodanig dat $-1 = \sum_{i=1}^{S} z_i^2$. We hebben alvast voor een willekeurig element $a \in A$

$$4a = (a+1)^2 - (a-1)^2 = (a+1)^2 + \sum_{i=1}^{S} (z_i(a-1))^2$$

zodat inderdaad elk element van $4A$ geschreven kan worden als een som van hoogstens $S + 1$ kwadraten. Als dan $2 \in A^\times$, is $4A = A$ en dit bewijst (3).

In het algemene geval, neem $a \in \Sigma A$, stel $a = \sum_{i=1}^{n} a_i^2$ voor zekere $n \in \mathbb{N}_+$, $a_i \in A$. Laat $c = 1 + \sum_{i=1}^{n} a_i$, dan is $c^2 = 1 + a + 2b$ voor zekere $b \in A$ zodat

$$a = c^2 - 1 - 2b = c^2 + b^2 - (1+b)^2 = c^2 + b^2 + \sum_{i=1}^{S} (z_i(1+b))^2 .$$

a is dus te schrijven als som van $S + 2$ kwadraten en we hebben $P(A) \leq S + 2$. Dit toont (1) aan.

Stel tenslotte dat S even is, neem $a \in \Sigma A^2$. Dan ook $-a \in \Sigma A^2$ (wegens $-1 \in \Sigma A^2$) zodat, gezien de berekening in het vorige deel van het bewijs, er c en b in A bestaan zodanig dat $-a = c^2 + b^2 - (1+b)^2$. We hebben

$$\begin{aligned} a &= (c^2+b^2)(-1) + (1+b)^2 = (1+b)^2 + (c^2+b^2)\left(\sum_{i=1}^{S} z_i^2\right) \\ &= (1+b)^2 + (c^2+b^2)\left(\sum_{i=1}^{S/2} (z_{2i-1}^2 + z_{2i}^2)\right) \\ &= (1+b)^2 + \sum_{i=1}^{S/2} (c^2+b^2)(z_{2i-1}^2 + z_{2i}^2) \end{aligned}$$

Nu weten we uit de compositieformule voor twee kwadraten (Stelling 1.2.2) dat er y_i bestaan voor $i \in \{1, \ldots, S\}$ met $(c^2+b^2)(z_{2i-1}^2 + z_{2i}^2) = y_{2i-1}^2 + y_{2i}^2$. Vorige berekening verderzetten geeft dan:

$$a = (1+b)^2 + \sum_{i=1}^{S/2} (y_{2i-1}^2 + y_{2i}^2) = (1+b)^2 + \sum_{i=1}^{S} y_i^2 \in \Sigma_{S+1}A^2$$

en we hebben inderdaad $P(A) \leq S + 1$, wat we moesten bewijzen voor (2). $\square$

Propositie 1.3.5. *Zij A een commutatieve ring. Dan is $S(A) = S(A[X])$. Als $S = S(A) < \infty$, $\mathrm{char}(A) \neq 2$ in A en A een eindig product van lokale ringen is, is*

$$S + 1 \leq l_{A[X]}(2X) \leq P(A[X]) \leq S + 2$$

Bewijs. Aangezien er een inbedding $A \to A[X]$ bestaat en een A-algebramorfisme $A[X] \to A$ (bijvoorbeeld bepaald door $X \mapsto 0$) volgt $S = S(A[X])$ uit het eerste deel van Propositie 1.3.2. $P(A[X]) \leq S + 2$ volgt uit Stelling 1.3.4.

Stel $A = A_1 \times \ldots \times A_n$ voor zekere $n \in \mathbb{N}$ en lokale ringen $A_1, \ldots, A_n$. Het is gemakkelijk na te gaan dat het A-algebramorfisme

$$\phi : A[X] \to A_1[X] \times \ldots \times A_n[X]$$

bepaald door $\phi(X) = (X, \ldots, X)$ een isomorfisme definieert, zodat het wegens het derde deel van Propositie 1.1.3 voldoende is de bewering te bewijzen voor een lokale ring A. Stel dus zonder velies van algemeenheid dat A lokaal is met uniek maximaal ideaal M.

We hebben $2X = (X + 1)^2 + (-1)X^2 + (-1) \in \Sigma A[X]^2$ omdat $S < \infty$. Onderstel uit het ongerijmde dat $2X \in \Sigma_S A[X]^2$, neem $F_1, \ldots, F_S \in A[X]$ met

$$2X = \sum_{i=1}^{S} F_i^2. \tag{1.1}$$

Voor $1 \leq i \leq S, j \in \mathbb{N}$, noteer $F_i^{(j)}$ voor de j-degraadscoëfficiënt van F_i. Vergelijken we in (1.1) de coëfficiënten van eerste graad, dan vinden we

$$2 = 2\left(\sum_{i=1}^{S} F_i^{(0)} F_i^{(1)}\right)$$

zodat

$$\sum_{i=1}^{S} F_i^{(0)} F_i^{(1)} - 1 \in \{a \in A \mid 2a = 0\}.$$

Omdat $\mathrm{char}(A) \neq 2$, is $\{a \in A \mid 2a = 0\}$ een echt ideaal van A, dus bevat in het maximale ideaal M. We vinden aldus

$$\sum_{i=1}^{S} F_i^{(0)} F_i^{(1)} \notin M$$

hetgeen impliceert dat er minstens één van de $F_i^{(0)}$ niet in M zit. Stel zonder verlies van algemeenheid dat $F_1^{(0)} \in A \setminus M = A^\times$. Bekijken we dan in (1.1) de constante cöfficiënten, dan vinden we achtereenvolgens

$$0 = \sum_{i=1}^{S} (F_i^{(0)})^2$$

$$-1 = \sum_{i=2}^{S} \left(\frac{F_i^{(0)}}{F_1^{(0)}}\right)^2 \in \Sigma_{S-1} A^2$$

hetgeen in strijd is met $S = S(A)$. □

1.4 Eindige lichamen

Het doel van deze sectie is om level en pythagorasgetal van alle eindige lichamen te bepalen. De resultaten uit deze sectie zijn gevonden met behulp van tips van prof. Becher. Noteer $\mathbb{F}_p$ voor het lichaam $\mathbb{Z}/p\mathbb{Z}$, waar $p \in \mathbb{N}$ een priemgetal is. We vermelden ter herinnering volgend resultaat:

Propositie 1.4.1. *Zij F een eindig lichaam, stel $p = \mathrm{char}(F)$. Dan is p een priemgetal en is $|F| = p^n$ voor een zekere $n \in \mathbb{N}_+$. Bovendien is $(F^\times, \cdot, 1)$ een cyclische groep.*

Bewijs. [6, Stelling 5.1-5.3, p246] □

Propositie 1.4.2. *Zij k een lichaam. Dan is $k^{\times 2}$ een deelgroep van $(k^\times, \cdot, 1)$ en de afbeelding*

$$f : k^\times \to k^{\times 2} : x \mapsto x^2$$

is een surjectief groepsmorfisme met $\mathrm{Ker}\, f = \{1, -1\}$. Het is een isomorfisme als en slechts als $\mathrm{char}(k) = 2$.

Bewijs. Dat $k^{\times 2}$ een deelgroep is van $k^\times$ werd bewezen in Gevolg 1.2.4 en dat f een surjectief groepsmorfisme is, is duidelijk. Stel $a \in \mathrm{Ker}\, f$, dan $a^2 = 1$, of nog, $0 = a^2 - 1 = (a-1)(a+1)$. Aangezien k een lichaam (en dus een domein) is, impliceert dit dat $a = 1$ of $a = -1$ en dus dat $\mathrm{Ker}\, f = \{1, -1\}$. f is injectief indien $\mathrm{Ker}\, f = \{1\}$, dus wanneer $1 = -1$, of equivalent, $\mathrm{char}(k) = 2$. □

Stelling 1.4.3. *Stel F een eindig lichaam met $p = \mathrm{char}(F)$. Er geldt $\Sigma F^2 = F$ en*

$$P(F) = |F^\times / F^{\times 2}| = \begin{cases} 1 & \text{als } p = 2 \\ 2 & \text{als } p \neq 2 \end{cases} .$$

Bewijs. Als $p = 2$, dan is de afbeelding f uit vorige propositie een isomorfisme en is dus $F = F^2$. Stel $p \neq 2$. Uit de Stelling van Lagrange en de Eerste Isomorfiestelling toegepast op de afbeelding f uit vorige propositie, volgt $|F^\times / F^{\times 2}| = |\,\mathrm{Ker}\, f| = |\{-1, 1\}|$, hetgeen de tweede gelijkheid bewijst.

Neem nu $a \in F$, laat $q = |F|$. De verzamelingen F^2 en $a - F^2 = \{a - x^2 \mid x \in F\}$ bevatten beide $\frac{q+1}{2}$ elementen. Ze kunnen bijgevolg niet disjunct zijn; anders zou hun unie een deelverzameling van F zijn die $q+1$ elementen bevat. Er bestaan dus $x, y \in F$ zodanig dat $x^2 = a - y^2$, of nog, $a = x^2 + y^2$. Vanwege de algemeenheid van a toont dit dat $F = \Sigma_2 F^2$ en dus $P(A) \leq 2$. $P(A) \geq 2$ omdat de afbeelding f geen isomorfisme is. □

Stelling 1.4.4. *Stel F een eindig lichaam met $q = |F|$. Er geldt:*

$$S(F) = \begin{cases} 2 & \text{als } q \equiv 3 \bmod 4 \\ 1 & \text{als } q \not\equiv 3 \bmod 4 \end{cases}$$

Bewijs. Laat $p = \mathrm{char}(F)$. Als $p = 2$ is, weten we dat $(\Sigma F^2)^\times = F^{\times 2}$ en dus $S(F) = P(F) = 1$. Stel vanaf nu $p \neq 2$. Wegens de vorige stelling en het feit dat $S(F) \leq p - 1 < \infty$ is $S(F) \leq P(F) = 2$, dus het is voldoende te tonen dat $-1 \in F^{\times 2}$ als en slechts als $q \equiv 1 \bmod 4$.

Stel $-1 \in F^{\times 2}$. Dan bestaat er een $x \in F$ met $x^2 = -1$. Gebruikend dat $q = p^n$ oneven is, vinden we

$$1 = x^{q-1} = \left(x^2\right)^{\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}},$$

hetgeen enkel kan als $\frac{q-1}{2}$ even is. Dit impliceert dat $q \equiv 1 \bmod 4$.

Omgekeerd, stel $q \equiv 1 \bmod 4$. Dan is $\frac{q-1}{2}$ even. Neem een voortbrenger x van $F^\times$. Omdat $x^{\frac{q-1}{2}}$ een wortel is van de veelterm $X^2 - 1$ over F, maar x multiplicatieve orde $q - 1$ heeft, is

$$-1 = x^{\frac{q-1}{2}} = \left(x^{\frac{q-1}{4}}\right)^2 \in F^{\times 2}.$$

□

1.5 Twee- en vierkwadratenstelling

We beginnen nu aan de voorbereiding van het bewijs van de vier- en tweekwadratenstellingen. In dit artikel steunen beide resultaten op een soort lokaal-globaalresultaat in de ring $\mathbb{Z}$, Lemma 1.5.3, en op de eerdere resultaten voor eindige lichamen. We zullen in wat komt de vier- en tweekwadratenstellingen simultaan bewijzen, aangezien de gebruikte technieken grotendeels dezelfde zijn.

Lemma 1.5.1. *Zij $k \in \{2, 4\}$. Als $n \in \mathbb{N}$ even en een som van k kwadraten in $\mathbb{N}$ is, dan is ook $\frac{n}{2}$ een som van k kwadraten in $\mathbb{N}$.*

Bewijs. Als $n = a^2 + b^2 + c^2 + d^2$ voor zekere $a, b, c, d \in \mathbb{N}$ dan moet het aantal oneven termen in die uitdrukking even zijn. Zonder verlies van algemeenheid kunnen we stellen dat a en b aan de ene kant en c en d aan de andere kant dezelfde pariteit hebben. Dan is

$$\frac{n}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

en alle optredende breuken zijn natuurlijke getallen. Als $k = 2$, dan kunnen we in bovenstaand bewijs $c = d = 0$ kiezen en vinden we dat $\frac{n}{2}$ een som van twee kwadraten is. □

Voorbeeld 1.5.2. Lemma 1.5.1 geldt niet in algemene commutatieve ringen: in het euclidische domein $\mathbb{Z}[i]$ is $2i = (1 + i)^2$, maar i is geen som van kwadraten in $\mathbb{Z}[i]$.

Lemma 1.5.3. *Zij $k \in \{2, 4\}$, stel $p \in \mathbb{N}_+$ een priemgetal zodanig dat $S(\mathbb{Z}/p\mathbb{Z}) < k$. Dan is $p \in \Sigma_k \mathbb{Z}^2$.*

Bewijs. We weten dat $1, 2 \in \Sigma_2\mathbb{Z}^2$, dus mogen in het vervolg $p > 2$ onderstellen. Omdat $S(\mathbb{Z}/p\mathbb{Z}) < k$, bestaan er $a_1, \ldots, a_{k-1} \in \mathbb{Z}$ zodanig dat $a_1^2 + \ldots + a_{k-1}^2 + 1 \equiv 0 \bmod p$ en dus bestaat er een $m \in \mathbb{N}_+$ zodanig dat

$$a_1^2 + \ldots + a_{k-1}^2 + 1 = mp.$$

Bovendien kunnen we $|a_i| \leq \frac{p-1}{2}$ kiezen, zodat $mp \leq (k-1)\left(\frac{p-1}{2}\right)^2 + 1 < p^2$ en dus $m < p$. Kies dan $z \in \mathbb{N}_+$ minimaal met betrekking tot de eigenschap dat er $b_1, \ldots, b_k \in \mathbb{N}$ bestaan zodanig dat

$$b_1^2 + \ldots + b_k^2 = zp.$$

Zo een z bestaat en is kleiner dan p wegens het voorgaande en is noodzakelijk oneven wegens Lemma 1.5.1. Als $z = 1$, hebben we dat p geschreven kan worden als een som van k kwadraten. Stel uit het ongerijmde dat $z > 1$.

Als $k = 2$, stel dan $b_3 = b_4 = 0$. Omdat z even is, kunnen we $w_1, \ldots, w_4 \in \mathbb{Z}$ kiezen met $|w_i| \leq \frac{z-1}{2}$ voor iedere $i \in \{1, \ldots, 4\}$ en met de eigenschap dat $w_1 \equiv b_1 \bmod z$ en $w_i \equiv -b_i \bmod z$ voor $i \in \{2, 3, 4\}$. Merk op dat, als $k = 2$, dan $w_3 = w_4 = 0$. Verder zien we dat niet alle w_i nul kunnen zijn, anders zouden alle b_i deelbaar zijn door z, wat zou impliceren dat $\frac{p}{z}$ een som van vier kwadraten van gehele getallen is. Maar p is een priemgetal en $z < p$, dus $\frac{p}{z}$ kan zelf geen geheel getal zijn.

Omdat $w_1^2 + \ldots + w_4^2 \equiv b_1^2 + \ldots + b_4^2 \equiv 0 \bmod z$, bestaat er een $n \in \mathbb{N}_+$ met

$$0 < zn = w_1^2 + \ldots + w_k^2.$$

Nu is

$$w_1^2 + \ldots + w_k^2 \leq 4\left(\frac{z-1}{2}\right)^2 = (z-1)^2$$

zodat $0 < n < z$. Definieer nu

$$\begin{aligned}
\beta_1 &= b_1w_1 - b_2w_2 - b_3w_3 - b_4w_4 \\
\beta_2 &= b_1w_2 + b_2w_1 + b_3w_4 - b_4w_3 \\
\beta_3 &= b_1w_3 + b_3w_1 + b_4w_2 - b_2w_4 \\
\beta_4 &= b_1w_4 + b_4w_1 + b_2w_3 - b_3w_2
\end{aligned}$$

en merk op dat $\beta_3 = \beta_4 = 0$ indien $k = 2$, want dan is $b_3 = w_3 = b_4 = w_4$. Er geldt wegens de compositieformule voor vier kwadraten uit Stelling 1.2.2 dat

$$\beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2 = (w_1^2 + w_2^2 + w_3^2 + w_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = z^2np.$$

Echter, we vinden ook dat

$$\begin{aligned}
\beta_1 &\equiv b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv 0 \bmod z \\
\beta_2 &\equiv -b_1b_2 + b_1b_2 - b_3b_4 + b_4b_3 \equiv 0 \bmod z \\
\beta_3 &\equiv -b_1b_3 + b_1b_3 - b_4b_2 + b_4b_2 \equiv 0 \bmod z \\
\beta_4 &\equiv -b_1b_4 + b_1b_4 - b_2b_3 + b_3b_2 \equiv 0 \bmod z
\end{aligned}$$

zodat elke β_i deelbaar is door z; schrijf $z\gamma_i = \beta_i$ voor zekere $\gamma_i \in \mathbb{N}$ en merk opnieuw op dat $\gamma_3 = \gamma_4 = 0$ als $k = 2$. We vinden dat

$$\gamma_1^2 + \ldots + \gamma_4^2 = \gamma_1^2 + \ldots + \gamma_k^2 = np,$$

hetgeen wegens $n < z$ in strijd is met de minimale keuze van z. We besluiten dat $z = 1$ moet gelden. □

Stelling 1.5.4 (Lagrange, Vierkwadratenstelling)**.** *Elk natuurlijk getal kan geschreven worden als een som van vier kwadraten van natuurlijke getallen. Er geldt $P(\mathbb{Z}) = 4$.*

Bewijs. Wegens Gevolg 1.2.3 volstaat het te tonen dat p een som van vier kwadraten is voor elk priemgetal $p \in \mathbb{N}$. Als p een priemgetal is, is $\mathbb{Z}/p\mathbb{Z}$ een eindig lichaam en is $S(\mathbb{Z}/p\mathbb{Z}) \leq 2 < 4$ wegens Stelling 1.4.4. Dan is p een som van vier kwadraten wegens Lemma 1.5.3.

Enkel natuurlijke getallen zijn sommen van kwadraten in $\mathbb{Z}$ en het is duidelijk dat $l_{\mathbb{Z}}(7) = 4$. Dit toont samen met het voorgaande dat $P(\mathbb{Z}) = 4$. □

Uit Stelling 1.4.4 weten we ook dat $S(\mathbb{Z}/p\mathbb{Z}) = 1$ als $p = 2$ of als p een priemgetal is met $p \equiv 1 \bmod 4$. Wegens Lemma 1.5.3 weten we dan dat deze priemgetallen een som van twee kwadraten zijn. Om te kunnen tonen welke natuurlijke getallen precies sommen van twee kwadraten zijn, moeten we nog wat meer werk doen. Het loont om eerst even te kijken naar de consequenties van Lemma 1.5.3 voor de ring $\mathbb{Z}[i]$.

We herhalen nog even dat $\mathbb{Z}[i]$ een domein is en dat ieder element van de vorm $a + bi$ is met $a, b \in \mathbb{Z}$. De functie

$$N : \mathbb{Z}[i] \to \mathbb{N} : a + bi \mapsto a^2 + b^2$$

maakt van $\mathbb{Z}[i]$ een euclidisch domein. In het bijzonder is het dus een factoriëel domein. Verder voldoet N aan de multiplicatieve eigenschap $N(xy) = N(x)N(y)$ voor alle $x, y \in \mathbb{Z}[i]$ en gelden

$$N^{-1}(1) = \mathbb{Z}[i]^\times = \{1, -1, i, -i\} \quad \text{en} \quad N^{-1}(0) = \{0\}.$$

Ten slotte hebben we een $\mathbb{Z}$-algebra-automorfisme

$$\bar{\cdot} : \mathbb{Z}[i] \to \mathbb{Z}[i] : a + bi \mapsto a - bi$$

en geldt er dat $N(z) = z\overline{z}$ voor iedere $z \in \mathbb{Z}[i]$, alsook $N(z) = N(\overline{z})$. Al deze eigenschappen zijn welbekend en kunnen gemakkelijk nagegaan worden. Lemma 1.5.3 toegepast met $k = 2$ is nodig voor volgend resultaat:

Propositie 1.5.5. *De priemelementen van $\mathbb{Z}[i]$ zijn juist, op vermenigvuldiging met een element uit $\mathbb{Z}[i]^\times$ na,*

1. *De elementen $a + bi$ waarbij $a, b \in \mathbb{N}$ zodanig zijn dat $N(a + bi) = a^2 + b^2$ een priemgetal is.*

2. De priemgetallen $p \in \mathbb{N}$ met $p \equiv 3 \bmod 4$.

Bewijs. Als $N(a+bi) = a^2+b^2$ een priemgetal is, dan moet $a+bi$ zelf een priemelement zijn van $\mathbb{Z}[i]$ wegens de multiplicatieve eigenschap van N.

Als $p \in \mathbb{N}$ een priemgetal is met $p \equiv 3 \bmod 4$, dan is p geen som van twee kwadraten in $\mathbb{Z}$, omdat men makkelijk nagaat dat

$$l_{\mathbb{Z}/4\mathbb{Z}}(p+4\mathbb{Z}) = l_{\mathbb{Z}/4\mathbb{Z}}(3+4\mathbb{Z}) = 3$$

en het eerste deel van Propositie 1.1.3 van toepassing is. Bijgevolg is $N(z) \neq p$ voor iedere $z \in \mathbb{Z}[i]$. Stel dat $p = xy$ voor zekere $x, y \in \mathbb{Z}[i]$, dan moet $p^2 = N(p) = N(x)N(y)$, zodat ofwel $N(x) = 1$ ofwel $N(y) = 1$, omdat het niet mogelijk is dat $N(x) = p$ of $N(y) = p$. Bijgevolg is $x \in \mathbb{Z}[i]^\times$ of $y \in \mathbb{Z}[i]^\times$. Dit toont dat p een priemelement is van $\mathbb{Z}[i]$.

We bewijzen nu dat dit de enige priemelementen van $\mathbb{Z}[i]$ zijn. Omdat $\mathbb{Z}[i]$ factorieel is, volstaat het te tonen dat elk niet-inverteerbaar, niet-nul element van $\mathbb{Z}[i]$ door een van de eerder vernoemde priemelementen deelbaar is. Neem $z \in \mathbb{Z}[i] \setminus (\mathbb{Z}[i]^\times \cup \{0\})$. Dan is $N(z) > 1$ en bestaat er dus een priemgetal $p \in \mathbb{N}$ met $p \mid N(z)$. Als $p = 2$ of $p \equiv 1 \bmod 4$, dan is $p = a^2+b^2$ voor zekere $a, b \in \mathbb{N}$. Stel $\pi = a+bi$; dit is een priemelement van $\mathbb{Z}[i]$ met $\pi \mid N(z)$. Als $p \equiv 3 \bmod 4$, dan is $\pi = p$ een priemelement in $\mathbb{Z}[i]$ dat $N(z)$ deelt.

In ieder geval hebben we dus een priemelement π van $\mathbb{Z}[i]$ dat $N(z) = z\overline{z}$ deelt. Dan moet ofwel $\pi \mid z$ ofwel $\pi \mid \overline{z}$ en in het tweede geval volgt dat $\overline{\pi} \mid z$. Als $\pi \in \mathbb{Z}$, is $\pi = \overline{\pi}$. Als $\pi \notin \mathbb{Z}$, is $\pi = a+bi$ met $a, b \in \mathbb{N}$ en $N(\pi) = p$ priem. Als dan $\overline{\pi} \mid z$, dan is $\pi' = i\overline{\pi} = b+ai$ een priemgetal van de eerste vorm dat z deelt. Hoe dan ook is z aldus deelbaar door een van de eerder besproken priemgetallen. □

Stelling 1.5.6 (Euler, Tweekwadratenstelling)**.** *Zij $n \in \mathbb{N}$, $n \geq 2$. Dan is $n \in \Sigma_2\mathbb{Z}^2$ als en slechts als*

$$n = p_1 p_2 \dots p_l q^2$$

met $q \in \mathbb{N}$ en voor zekere priemgetallen $p_1, \dots, p_l$ met $p_i = 2$ of $p_i \equiv 1 \bmod 4$ voor iedere $i \in \{1, \dots, l\}$.

Bewijs. We beargumenteerden al dat p een som van twee kwadraten is als $p = 2$ of $p \equiv 1 \bmod 4$ voor een priemgetal p. Als $n \in \mathbb{N}$ in bovenstaande vorm staat, dan is ze dus een som van twee kwadraten wegens de compositieformule voor $k = 2$ in Stelling 1.2.2.

Omgekeerd, onderstel dat $n = a^2+b^2$ voor zekere $a, b \in \mathbb{Z}$. Dan is $n = N(z)$ voor $z = a+bi$. Schrijf $z = q_1 \dots q_m$ voor zekere priemelementen $q_1, \dots, q_m \in \mathbb{Z}[i]$. Dan is $n = N(z) = N(q_1) \dots N(q_m)$ en voor iedere $i \in \{1, \dots, m\}$ geldt $N(q_i) = 2$, $N(q_i) = p^2$ voor zeker priemgetal $p \in \mathbb{N}$ of $N(q_i) = p \equiv 1 \bmod 4$ voor zeker priemgetal $p \in \mathbb{N}$ wegens Propositie 1.5.5. □

Historisch gezien was het waarschijnlijk Albert Girard die als eerste de tweekwadratenstelling als veronderstelling formuleerde in 1625. Tegenwoordig wordt

de stelling vaak toegeschreven aan Fermat, maar het eerste bewijs (en enkel voor priemgetallen) dat werd overgeleverd, komt van Euler uit 1749. Ook de vierkwadratenstelling was al veel eerder een vermoeden dan dat ze bewezen was. Het eerste bewijs wordt toegeschreven aan Lagrange, die de stelling in 1772 bewees.

De nog overblijvende vraag is welke getallen geschreven kunnen worden als een som van drie kwadraten. Het ontbreken van een compositieformule voor sommen van drie kwadraten maakt dat dit een moeilijker probleem is. Fermat formuleerde het vermoeden dat enkel de getallen van de form $4^k(8l+7)$ voor $k, l \in \mathbb{N}$ *niet* geschreven kunnen worden als een som van drie kwadraten; dit werd voor het eerst bewezen door Legendre in 1798. [4, voorwoord, p. i-x] Wij bewijzen enkel de eenvoudige implicatie.

Propositie 1.5.7. *Zij $k, c \in \mathbb{N}$ zodanig dat $c \equiv 7 \bmod 8$. Dan is $4^k c \notin \Sigma_3\mathbb{Q}^2$.*

Bewijs. Onderstel uit het ongerijmde dat er $a_1, a_2, a_3, b \in \mathbb{Z}$ bestaan met $b \neq 0$ zodanig dat $4^k c = \frac{a_1^2}{b^2} + \frac{a_2^2}{b^2} + \frac{a_3^2}{b^2}$, of equivalent:

$$4^k c b^2 = a_1^2 + a_2^2 + a_3^2. \tag{1.2}$$

We bekijken deze vergelijking modulo 4. c is altijd oneven. Als b even is of $k \geq 1$, dan bekomen we

$$0 \equiv a_1^2 + a_2^2 + a_3^2 \bmod 4$$

Aangezien 0 en 1 de enige kwadraten modulo 4 zijn, kan dit enkel indien $a_1^2 \equiv a_2^2 \equiv a_3^2 \equiv 0 \bmod 4$, of nog, indien a_1, a_2 en a_3 alledrie even zijn. We kunnen dan beide kanten van de gelijkheid (1.2) door 2 delen om ofwel

$$4^k c \left(\frac{b}{2}\right)^2 = \left(\frac{a_1}{2}\right)^2 + \left(\frac{a_2}{2}\right)^2 + \left(\frac{a_3}{2}\right)^2$$

te bekomen indien b even is, ofwel

$$4^{k-1} c b^2 = \left(\frac{a_1}{2}\right)^2 + \left(\frac{a_2}{2}\right)^2 + \left(\frac{a_3}{2}\right)^2$$

in het geval $k \geq 1$.

Door bovenstaand procedé voldoende vaak te herhalen, bekomen we uiteindelijk $a_1', a_2', a_3', b' \in \mathbb{N}$ met

$$c b'^2 = a_1'^2 + a_2'^2 + a_3'^2 \tag{1.3}$$

en b' een oneven getal. Weer gebruikend dat 1 en 0 de enige kwadraten modulo 4 zijn, hebben we dat $c \equiv -1$ en $b'^2 \equiv 1 \mod 4$; dit geeft

$$-1 \equiv a_1'^2 + a_2'^2 + a_3'^2 \bmod 4,$$

hetgeen dus enkel kan indien $a_1'^2 \equiv a_2'^2 \equiv a_3'^2 \equiv 1 \bmod 4$, of nog, a_1', a_2' en a_3' alledrie oneven zijn.

Tenslotte willen we (1.3) bekijken modulo 8. We weten dat $1 \equiv 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \bmod 8$, zodat $1 \equiv b'^2 \equiv a_1'^2 \equiv a_2'^2 \equiv a_3'^2$. Maar dit geeft een contradictie met (1.3):

$$-1 \equiv cb'^2 \equiv a_1'^2 + a_2'^2 + a_3'^2 \equiv 1 + 1 + 1 \equiv 3 \bmod 8.$$

We besluiten dat de onderstelling $4^k c \in \Sigma_3\mathbb{Q}^2$ verkeerd was, wat we moesten bewijzen. □

Gevolg 1.5.8. *We hebben* $P(\mathbb{Q}) = 4$.

Bewijs. $P(\mathbb{Z}) = 4$ wegens Stelling 1.5.4 (de Vierkwadratenstelling), $P(\mathbb{Q}) \leq P(\mathbb{Z})$ wegens het tweede deel van Propositie 1.1.3 en $4 \leq P(\mathbb{Q})$ omdat $l_{\mathbb{Q}}(7) = 4$ wegens Propositie 1.5.7. □

De aanpak van de twee- en vierkwadratenstelling uit deze sectie is een eigen poging om deze stellingen zo compact mogelijk te bewijzen met behulp van de reeds gekende theorie over level en pythagorasgetal. Het idee om met de ring $\mathbb{Z}[i]$ te werken is aan Carl Friedrich Gauss te danken.

1.6 Quotiënten van de ring der gehele getallen

In de laatste sectie van dit hoofdstuk bepalen we voor $n \in \mathbb{N}, n \geq 2$ de getallen $S(\mathbb{Z}/n\mathbb{Z})$ en $P(\mathbb{Z}/n\mathbb{Z})$. Het zal blijken dat we deze getallen gemakkelijk kunnen bepalen als we de priemontbinding van n kennen. Het bewijs splitsen we op in kleine proposities waarin het innige verband tussen level en pythagorasgetal meermaals zal worden gebruikt. Uiteindelijk besluiten we met een manier om level en pythagorasgetal van $\mathbb{Z}/n\mathbb{Z}$ te bepalen uit de priemontbinding van n. De resultaten uit dit hoofdstuk heb ik grotendeels zelfstandig afgeleid.

Propositie 1.6.1. $\Sigma_4(\mathbb{Z}/n\mathbb{Z})^2 = \mathbb{Z}/n\mathbb{Z}$ *voor iedere* $n \in \mathbb{N}$.

Bewijs. Ieder element van $\mathbb{Z}/n\mathbb{Z}$ kan geschreven worden als $m + n\mathbb{Z}$ voor zekere $m \in \mathbb{N}$. Wegens Stelling 1.5.4 kan m als een som van vier kwadraten geschreven worden in $\mathbb{Z}$ en dit wordt overgedragen naar $\mathbb{Z}/n\mathbb{Z}$ zoals beschreven in het eerste deel van Propositie 1.1.3. □

Propositie 1.6.2. *Als* $n, m \in \mathbb{Z}$ *met* $n \mid m$, *dan* $P(\mathbb{Z}/n\mathbb{Z}) \leq P(\mathbb{Z}/m\mathbb{Z})$ *en* $S(\mathbb{Z}/n\mathbb{Z}) \leq S(\mathbb{Z}/m\mathbb{Z})$.

Bewijs. Als $n \mid m$, dan is $m\mathbb{Z} \subseteq n\mathbb{Z}$ en bestaat er een natuurlijk surjectief morfisme $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Het resultaat volgt uit het eerste deel van Propositie 1.1.3 en 1.3.2. □

Propositie 1.6.3. *Er geldt*

$$S(\mathbb{Z}/2^k\mathbb{Z}) = P(\mathbb{Z}/2^k\mathbb{Z}) = \begin{cases} 1 & \text{als } k = 1 \\ 3 & \text{als } k = 2 \\ 4 & \text{als } k \geq 3 \end{cases}$$

Bewijs. Voor $k \leq 3$ kan de bewering door een eindig aantal berekeningen geverifieerd worden. Aangezien voor $k \in \mathbb{N}, k \geq 3$ geldt dat $8 \mid 2^k \mid 0$, geldt (gezien Propositie 1.6.2)

$$4 = P(\mathbb{Z}) = P(\mathbb{Z}/0\mathbb{Z}) \geq P(\mathbb{Z}/2^k\mathbb{Z}) \geq P(\mathbb{Z}/8\mathbb{Z}) = 4.$$

Een gelijkaardige redenering doet men voor $S(\mathbb{Z}/2^k\mathbb{Z})$. □

Propositie 1.6.4. *Als p een priemgetal is met $p > 2$, dan is $\left|(\mathbb{Z}/p\mathbb{Z})^2\right| = \frac{p+1}{2}$ en $P(\mathbb{Z}/p\mathbb{Z}) = 2$.*

Bewijs. Dit volgt uit Propositie 1.4.2 en Stelling 1.4.3. □

Propositie 1.6.5. *Stel p een priemgetal $p > 2$, $n \in \mathbb{N}_+$. Dan geldt*

$$S(\mathbb{Z}/p^n\mathbb{Z}) = \begin{cases} 1 \text{ als } p \equiv 1 \bmod 4 \\ 2 \text{ als } p \equiv 3 \bmod 4 \end{cases}$$

Bewijs. Voor $n = 1$ bewezen we het gestelde reeds in Stelling 1.4.4. In het bijzonder kunnen we $x, y \in \mathbb{Z}$ kiezen met $x^2 + y^2 + 1 \in p\mathbb{Z}$, waarbij $y = 0$ in het geval $p \equiv 1 \bmod 4$. Er geldt dan voor iedere $l \in \mathbb{Z}$ dat $(x + lp)^2 + y^2 + 1 \in p\mathbb{Z}$. Beschouw de afbeelding

$$f : \{0, 1, \ldots, p^{n-1} - 1\} \to p\mathbb{Z}/p^n\mathbb{Z} : l \mapsto (x + lp)^2 + y^2 + 1.$$

We tonen dat deze afbeelding injectief is. Onderstel dat voor zekere $l, m \in \{0, 1, \ldots, p^{n-1} - 1\}$ geldt

$$(x + lp)^2 + y^2 + 1 \equiv (x + mp)^2 + y^2 + 1 \bmod p^n.$$

Dit uitwerken levert achtereenvolgens

$$\begin{aligned} (x + lp)^2 - (x + mp)^2 &\equiv 0 \bmod p^n \\ p(l - m)(2x + lp + mp) &\equiv 0 \bmod p^n. \end{aligned}$$

Aangezien $2x + lp + mp \equiv 2x \not\equiv 0 \bmod p$, betekent dit dat $l - m \equiv 0 \bmod p^{n-1}$, wat enkel kan als $l = m$. Dit toont de injectiviteit van f aan.

Omdat f een injectieve afbeelding tussen eindige verzameling van dezelfde grootte is, is ze surjectief, en bestaat er een $l \in \mathbb{Z}$ zodanig dat $(x+lp)^2+y^2+1 \equiv 0 \bmod p^n$. Dit toont dat $S(\mathbb{Z}/p^n\mathbb{Z}) \leq 2$ in het algemeen en dat $S(\mathbb{Z}/p^n\mathbb{Z}) = 1$ als $p \equiv 1 \bmod 4$, want dan was $y = 0$. Hiermee kunnen we het bewijs besluiten, want $S(\mathbb{Z}/p^n\mathbb{Z}) \geq 2$ volgt uit $S(\mathbb{Z}/p\mathbb{Z}) = 2$ voor $p \equiv 3 \bmod 4$ wegens Propositie 1.6.2. □

Gevolg 1.6.6. *Neem een priemgetal $p > 2$, $n \in \mathbb{N}, n \geq 2$. Dan geldt*

$$P(\mathbb{Z}/p^n\mathbb{Z}) = \begin{cases} 2 \text{ als } p \equiv 1 \bmod 4 \\ 3 \text{ als } p \equiv 3 \bmod 4. \end{cases}$$

Als $p \equiv 3 \bmod 4$, is $l(p + p^n\mathbb{Z}) = 3$ in $\mathbb{Z}/p^n\mathbb{Z}$.

Bewijs. Omdat p oneven is, is $2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, aangezien $2 \cdot \left(\frac{1-p^n}{2}\right) \equiv 1 \bmod p^n$. Wegens het derde deel van Stelling 1.3.4 en voorgaande propositie hebben we

$$P(\mathbb{Z}/p^n\mathbb{Z}) \leq S(\mathbb{Z}/p^n\mathbb{Z}) + 1 = \begin{cases} 2 \text{ als } p \equiv 1 \bmod 4 \\ 3 \text{ als } p \equiv 3 \bmod 4. \end{cases}$$

Anderzijds volgt uit Propositie 1.6.2 en 1.6.4 dat $P(\mathbb{Z}/p^n\mathbb{Z}) \geq 2$. Als we nu nog tonen dat $p + p^n\mathbb{Z}$ een element van lengte 3 in $\mathbb{Z}/p^n\mathbb{Z}$ is als $p \equiv 3 \bmod 4$, dan zijn we klaar. $l(p + p^n\mathbb{Z}) \leq 3$ weten we al. Onderstel uit het ongerijmde dat er $a, b \in \mathbb{Z}$ bestaan zodanig dat

$$p \equiv a^2 + b^2 \bmod p^n.$$

Dan kunnen a en b niet beide deelbaar zijn door p, aangezien in dat geval $\overline{a}^2, \overline{b}^2 \in p^2\mathbb{Z}/p^n\mathbb{Z}$, in strijd met $p \equiv a^2 + b^2 \bmod p^n$. Anderzijds geldt wel dat

$$a^2 + b^2 \equiv 0 \bmod p. \tag{1.4}$$

Stel zonder verlies van algemeenheid $b \not\equiv 0 \bmod p$. Omdat $\mathbb{Z}/p\mathbb{Z}$ een lichaam is, bestaat er dus een $c \in \mathbb{Z}$ met $bc \equiv 1 \bmod p$. We vinden uit (1.4) door met c^2 te vermenigvuldigen

$$(ac)^2 + 1 \equiv 0 \bmod p,$$

hetgeen een contradictie levert met $S(\mathbb{Z}/p\mathbb{Z}) = 2$. □

Merk op dat we nu $P(\mathbb{Z}/n\mathbb{Z})$ en $S(\mathbb{Z}/n\mathbb{Z})$ kunnen vinden als n van de vorm p^k is voor een $k \in \mathbb{N}$ en een priemgetal p. De volgende propositie toont aan dat we hiermee de oorspronkelijke vraag hebben beantwoord:

Propositie 1.6.7. *Zij n en $m \in \mathbb{N}_+$ copriem. Dan gelden*

$$P(\mathbb{Z}/mn\mathbb{Z}) = \max\{P(\mathbb{Z}/m\mathbb{Z}), P(\mathbb{Z}/n\mathbb{Z})\}$$
$$S(\mathbb{Z}/mn\mathbb{Z}) = \max\{S(\mathbb{Z}/m\mathbb{Z}), S(\mathbb{Z}/n\mathbb{Z})\}$$

Bewijs. Als n en m copriem zijn, zijn de idealen $n\mathbb{Z}$ en $m\mathbb{Z}$ copriem. Uit de Chinese Reststelling volgt dat

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

en het resultaat volgt door toepassing van het derde deel van Propositie 1.1.3 en Propositie 1.3.2. □

We vatten alle bewezen resultaten van dit deelhoofdstuk samen in volgende stelling.

Stelling 1.6.8. *Zij $n \in \mathbb{N}$, $n \geq 2$. Laat $P = P(\mathbb{Z}/n\mathbb{Z})$ en $S = S(\mathbb{Z}/n\mathbb{Z})$. Dan geldt:*

$$S = \begin{cases} 4 & \text{als } 8 \mid n, \\ 3 & \text{als } 4 \mid n \text{ en } 8 \nmid n, \\ 2 & \text{als } 4 \nmid n \text{ en } p \mid n \text{ voor een zeker priemgetal } p \equiv 3 \bmod 4, \\ 1 & \text{anders}, \end{cases}$$

$$P = \begin{cases} 3 & \text{als } 8 \nmid n \text{ en } p^2 \mid n \text{ voor een priemgetal } p \equiv 3 \bmod 4, \\ 2 & \text{als } n \neq 2, 4 \nmid n \text{ en } p \not\equiv 3 \bmod 4 \text{ voor ieder priemgetal } p \mid n, \\ S & \text{anders.} \end{cases}$$

Bewijs. Het geval $n = 2$ is evident, zie Propositie 1.6.3. Stel vanaf nu $n > 2$. Schrijf

$$n = \prod_{i=1}^{m} p_i^{k_i}$$

voor zekere $m \in \mathbb{N}_+$, paarsgewijs verschillende priemgetallen p_i en zekere $k_i \in \mathbb{N}_+$. Er geldt wegens Propositie 1.6.7 dat

$$S = \max\{S(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) \mid i \in \{1, \ldots, m\}\},$$
$$P = \max\{P(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) \mid i \in \{1, \ldots, m\}\}.$$

en voor iedere $i \in \{1, \ldots, m\}$ geldt

$$S(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) = \begin{cases} 4 & \text{als } p_i = 2, k_i \geq 3, \\ 3 & \text{als } p_i = 2, k_i = 2, \\ 2 & \text{als } p_i \equiv 3 \bmod 4, \\ 1 & \text{anders}, \end{cases}$$

$$P(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) = \begin{cases} S(\mathbb{Z}/p_i^{k_i}\mathbb{Z}) & \text{als } p_i = 2, \\ 3 & \text{als } p_i \equiv 3 \bmod 4, k_i \geq 2, \\ 2 & \text{anders.} \end{cases}$$

wegens voorgaande resultaten. De stelling volgt door te observeren voor welke $i \in \{1, \ldots, m\}$ de getallen $S(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$ en $P(\mathbb{Z}/p_i^{k_i}\mathbb{Z}))$ hun maximale waarden aannemen. □

Propositie 1.6.9. *Zij $n \in \mathbb{N}, n \geq 2$. Dan gelden*

$$S(\mathbb{Z}/n\mathbb{Z}[X]) = S(\mathbb{Z}/n\mathbb{Z}) \quad \text{en} \quad P(\mathbb{Z}/n\mathbb{Z}[X]) = \begin{cases} 1 & \text{als } n = 2, \\ 5 & \text{als } 4 \mid n, \\ S(\mathbb{Z}/n\mathbb{Z}) + 1 & \text{anders.} \end{cases}$$

Bewijs. Voor $n = 2$ is het resultaat wederom triviaal; stel $n > 2$. De gelijkheid van de levels, alsook het feit dat $P(\mathbb{Z}/n\mathbb{Z}[X]) \geq S(\mathbb{Z}/n\mathbb{Z}) + 1$, werden bewezen

in Propositie 1.3.5. Bovendien is voorgaande ongelijkheid een gelijkheid indien n oneven is: in dat geval is immers $2 \in \mathbb{Z}/n\mathbb{Z}[X]^\times$ en kunnen we het derde deel van Stelling 1.3.4 toepassen. Verder hebben we sowieso dat $P(\mathbb{Z}/n\mathbb{Z}) \leq 5$, daar $S(\mathbb{Z}/n\mathbb{Z}) \leq 4$ en we het tweede deel van Stelling 1.3.4 mogen toepassen.

We bewijzen de bewering nu voor $n = 4$. Wegens Propositie 1.3.5 is $4 \leq l_{\mathbb{Z}/4\mathbb{Z}[X]}(2X) \leq 5$; we zullen tonen dat $l_{\mathbb{Z}/4\mathbb{Z}[X]}(2X) = 5$. Onderstel uit het ongerijmde dat er $F_1, F_2, F_3, F_4 \in \mathbb{Z}/4\mathbb{Z}[X]$ bestaan met $2X = F_1^2 + \ldots + F_4^2$. We noteren $F_i^{(j)}$ voor de j-degraadscoëfficiënt van F_i. De constante coëfficiënten vergelijken levert

$$0 = (F_1^{(0)})^2 + \ldots + (F_4^{(0)})^2$$

wat enkel kan als alle $(F_i^{(0)})^2 = 1$ (i.e. $F_i^{(0)} \in \{1, 3\}$) of alle $(F_i^{(0)})^2 = 0$ (i.e. $F_i^{(0)} \in \{0, 2\}$). Door vergelijken van de eerstegraadscoëfficiënten vinden we

$$2 = 2\left((F_1^{(0)})(F_1^{(1)}) + \ldots + (F_4^{(0)})(F_4^{(1)})\right)$$

en is het dus onmogelijk dat alle $F_i^{(0)} \in \{0, 2\}$. We hebben aldus dat $F_i^{(0)} \in \{1, 3\}$ voor $i \in \{1, 2, 3, 4\}$. Dan moet een oneven aantal van de $(F_i^{(1)}) \in \{1, 3\}$, anders zou $(F_1^{(0)})(F_1^{(1)}) + \ldots + (F_4^{(0)})(F_4^{(1)}) \in \{0, 2\}$. Bijgevolg is $(F_1^{(1)})^2 + \ldots + (F_4^{(1)})^2 \in \{1, 3\}$. Tot slot kijken we naar de tweedegraadscoëfficiënten in de uitdrukking $2X = F_1^2 + \ldots + F_4^2$:

$$0 = 2\left((F_1^{(0)})(F_1^{(2)}) + \ldots + (F_4^{(0)})(F_4^{(2)})\right) + (F_1^{(1)})^2 + \ldots + (F_4^{(1)})^2.$$

Maar dit kan niet, aangezien een oneven aantal van de termen in het rechterlid in $\{1, 3\}$ zit. We vinden dat $l_{\mathbb{Z}/4\mathbb{Z}[X]}(2X) = 5$ en dus $P(\mathbb{Z}/4\mathbb{Z}[X]) = 5$. Uiteraard geldt dan ook $P(\mathbb{Z}/2^k\mathbb{Z}[X]) = 5$ voor iedere $k \in \mathbb{N}$ met $k \geq 2$, aangezien in dat geval $\mathbb{Z}/4\mathbb{Z}[X]$ uit $\mathbb{Z}/2^k\mathbb{Z}[X]$ als quotiëntring bekomen kan worden.

In het algemene geval kunnen we n schrijven als $2^k m$ voor zekere $k \in \mathbb{N}$ en $m \in \mathbb{N}$ even. Wegens de Chinese Reststelling is

$$\mathbb{Z}/n\mathbb{Z}[X] \cong \mathbb{Z}/2^k\mathbb{Z}[X] \times \mathbb{Z}/m\mathbb{Z}[X]$$

zodat het algemene resultaat volgt uit het voorgaande en het derde deel van Propositie 1.1.3. □

Voorbeeld 1.6.10. Dat $S(\mathbb{Z}/4\mathbb{Z}[X]) = 3$ en $P(\mathbb{Z}/4\mathbb{Z}[X]) = 5$, toont dat de ongelijkheid in het eerste deel van Stelling 1.3.4 strikt kan zijn. Het bewijs dat $P(\mathbb{Z}/4\mathbb{Z}[X]) = 5$ is grotendeels overgenomen uit [8].

De laatste stelling van dit hoofdstuk toont aan dat voor $n \in \mathbb{N}_+$, de ring $\mathbb{Z}/n\mathbb{Z}[X]$ maximaal Pythagorasgetal heeft binnen de klasse van commutatieve ringen met karakteristiek n. Dit wordt uitgebreid naar het geval $n = 0$ in hoofdstuk 3, waar we tonen dat $P(\mathbb{Z}[X]) = \infty$.

Stelling 1.6.11. *Zij A een commutatieve ring met $n = \mathrm{char}(A) \neq 0$. Dan gelden*

$$S(A) \leq S(\mathbb{Z}/n\mathbb{Z}) \qquad P(A) \leq P(\mathbb{Z}/n\mathbb{Z}[X])$$

Bewijs. Zij $n \in \mathbb{N}_+$ en A een commutatieve ring met $n = \text{char}(A)$. Er bestaat dan een uniek ringmorfisme $\mathbb{Z}/n\mathbb{Z} \to A$, zodat alvast $S(A) \leq S(\mathbb{Z}/n\mathbb{Z})$. Het tweede deel van Stelling 1.3.4 levert verder dat $P(A) \leq 5$ omdat $S(A) \leq S(\mathbb{Z}/n\mathbb{Z}) \leq 4$.

Schrijf $n = 2^k m$ met $k, m \in \mathbb{N}$ en m oneven. De Chinese Reststelling zegt ons dan dat

$$A \cong A/2^k A \times A/mA$$

zodat het volstaat de stelling te tonen voor $n = 2^k$ en $n = m$ wegens het derde deel van Propositie 1.1.3. Als n oneven is, dan is $2 \in \mathbb{Z}/n\mathbb{Z}^\times$ en dus ook $2 \in A^\times$, zodat $P(A) \leq S(A)+1 \leq S(\mathbb{Z}/n\mathbb{Z})+1$ wegens het derde deel van Stelling 1.3.4. In het geval $n = 1$ is er niets te bewijzen en voor $n = 2$ weten we reeds dat $P(A) = 1$. Als $n = 2^k$ met $k \geq 2$, geldt $4 \mid n$ en moeten we ook niets meer bewijzen. Dit toont de tweede ongelijkheid in het algemeen aan. □

Opmerking 1.6.12. Een naïeve aanpak om de tweede ongelijkheid in voorgaande stelling te bewijzen, zou zijn om voor $a \in A$ willekeurig te kijken naar het unieke ringmorfisme $\mathbb{Z}/n\mathbb{Z}[X] \to A$ dat X naar a stuurt. Als X dan een som van $P(\mathbb{Z}/n\mathbb{Z}[X])$ kwadraten is, dan a ook. Deze aanpak werkt als n oneven is, maar gaat voorbij aan het feit dat X geen som van kwadraten is in $\mathbb{Z}/n\mathbb{Z}[X]$ als n even is.

Hoofdstuk 2

Ringen met eindig pythagorasgetal

2.1 Reële commutatieve ringen

Belangrijk in het vervolg van dit artikel is het concept van een reële commutatieve ring, dat een bepaalde eigenschap met betrekking tot sommen van kwadraten in bijvoorbeeld $\mathbb{Z}, \mathbb{Q}$ en $\mathbb{R}$ veralgemeent.

Definitie 2.1.1. Een commutatieve ring A heet *reëel* indien voor elke $n \in \mathbb{N}_+, a_1, \ldots, a_n \in A \setminus \{0\}$ geldt dat:

$$\sum_{i=1}^{n} a_i^2 \neq 0.$$

Een ideaal I van A heet reëel indien de quotiënting A/I reëel is.

Opmerking 2.1.2. In de literatuur spreekt men ook van formeel reële ringen.

Propositie 2.1.3. *Zij k een reële commutatieve ring. Dan is $S(k) = \infty$ en* $\mathrm{char}(A) = 0$. *Als k een lichaam is, dan zijn volgende uitspraken equivalent:*

1. *k is reëel.*
2. *$S(k) = \infty$.*
3. $\mathrm{char}(k) \neq 2$ *en* $k \neq \Sigma k^2$

Bewijs. We bewijzen eerst het eerste deel. Als $m = \mathrm{char}(k) \neq 0$, dan is $\sum_{i=1}^{m} 1^2 = \sum_{i=1}^{m} 1 = 0$, zodat k niet reëel is. Als elk element van k een som van kwadraten is, dan is in het bijzonder -1 een som van kwadraten, dus $-1 = \sum_{i=1}^{n} a_i^2$ voor zekere $n \in \mathbb{N}_+$, $a_i \in k$. Dus is $0 = 1^2 + \sum_{i=1}^{n} a_i^2$ zodat k niet reëel is. Dit toont de implicaties (1) $\Rightarrow$ (3) en (1) $\Rightarrow$ (2) en dat $\mathrm{char}\, k = 0$ en voor dit alles hadden we niet nodig dat k een lichaam is.

Stel vanaf nu dat k een lichaam is. Voor de implicatie (3) $\Rightarrow$ (2), onderstel dat (2) niet geldt, dus $S(k) = n < \infty$. We willen tonen dat (3) niet geldt. Als $\text{char}(k) = 2$ zijn we klaar, in het andere geval is $2 \in k^\times$ en volgt uit het derde deel van Stelling 1.3.4 dat $k = \Sigma k^2$ en dus dat (3) niet geldt.

Stel tenslotte dat (1) niet geldt, dat wil zeggen: er bestaan $n \in \mathbb{N}_+$, $a_1, \ldots, a_n \in k \setminus \{0\}$ zodanig dat $0 = \sum_{i=1}^n a_i^2$. Dan is a_n inverteerbaar in k, zodat

$$0 = \sum_{i=1}^{n} \left(\frac{a_i}{a_n}\right)^2 = 1 + \sum_{i=1}^{n-1} \left(\frac{a_i}{a_n}\right)^2$$

en dus $-1 = \sum_{i=1}^{n-1} \left(\frac{a_i}{a_n}\right)^2$ zodat $S(k) \leq n-1 < \infty$. Dit toont dat (2) niet geldt en bijgevolg via contrapositie dat (2) $\Rightarrow$ (1). $\square$

Opmerking 2.1.4. In de ringen $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ hebben we een 'natuurlijke' totale orde die compatibel is met optelling en vermenigvuldiging. De sommen van kwadraten zijn in deze ringen juist de positieve getallen. Artin en Schreier bewezen dat een lichaam k reëel is als en slechts als er zo een orde op k bestaat, i.e. een totale orde die compatibel is met de bewerkingen $+$ en $\cdot$. Voor formele definities en bewijzen hieromtrent, zie [10, hoofdstuk 6, deel 1].

We geven nog enkele constructies van reële ringen.

Propositie 2.1.5. *Zij A een reële commutatieve ring. Dan gelden:*

(1) $A[X]$ is reëel.

(2) Voor elk multiplicatief deel $S \subseteq A$ is de lokalisatie A_S reëel.

Bewijs. We beginnen met de eerste uitspraak. Neem $n \in \mathbb{N}_+$, $F_i \in A[X]$ voor $i \in \{1, \ldots, n\}$ zodanig dat $0 = \sum_{i=1}^n F_i^2$. Onderstel uit het ongerijmde dat niet alle F_i nul zijn, dan bestaat er een $d \in \mathbb{N}$ maximaal zodanig dat X^d iedere F_i deelt. Schrijf dan $F_i = X^d F_i'$ voor zekere $F_i' \in A[X]$, dan vinden we achtereenvolgens

$$0 = \sum_{i=1}^{n} F_i^2 = \sum_{i=1}^{n} X^{2d} F_i'^2 = X^{2d} \sum_{i=1}^{n} F_i'^2$$

en dus

$$0 = \sum_{i=1}^{n} F_i'^2.$$

Door de keuze van d, is tenminste één van de $F_i'(0)$ verschillend van nul, maar door in bovenstaande vergelijking de constante term links en rechts te vergelijken, vinden we

$$0 = \sum_{i=1}^{n} F_i'(0)^2,$$

hetgeen in strijd is met de onderstelling dat A reëel is. We besluiten dat $F_i = 0$ voor alle $i \in \{1, \ldots, n\}$. Alles tezamen hebben we dat $A[X]$ reëel is.

Voor de tweede uitspraak, neem $n \in \mathbb{N}_+, a_1, \ldots, a_n \in A, s \in S$. Onderstel dat

$$0 = \sum_{i=1}^{n} \left(\frac{a_i}{s}\right)^2 = \frac{\sum_{i=1}^{n} a_i^2}{s^2},$$

dan volgt dat er een $t \in S$ bestaat met $0 = t \sum_{i=1}^{n} a_i^2$. Dan is ook

$$0 = \sum_{i=1}^{n} (ta_i)^2$$

en omdat A reëel is, impliceert dit dat $ta_i = 0$ voor iedere i. We vinden dan voor iedere $i \in \{1, \ldots, n\}$

$$\frac{a_i}{s} = \frac{a_i t}{st} = \frac{0}{st} = 0.$$

Dit toont aan dat A_S reëel is. □

2.2 Eindigdimensionale algebra's

We noteren $k[\underline{X}]$ voor $k[X_1, \ldots, X_n]$ en $\underline{X}$ voor de rijvector $(X_1, \ldots, X_n) \in k[\underline{X}]^n$, indien geen verwarring kan bestaan over de waarde van n.

Definitie 2.2.1. Zij k een commutatieve ring, $n \in \mathbb{N}_+$. Als $f \in k[X_1, \ldots, X_n]$ een homogene veelterm van graad 2 is, noemen we f een *kwadratische vorm* in n veranderlijken, of een n-aire kwadratische vorm (over k). Als f een homogene veelterm van graad 1 is, spreken we over een n-aire *lineaire vorm*.

Kwadratische vormen spelen een belangrijke rol in de theorie van level en pythagorasgetal van lichamen. Zie hiervoor bijvoorbeeld [10, hoofdstuk 3 en 7].

Wij zullen enkel een belangrijke eigenschap van kwadratische vormen over lichamen nodig hebben, de diagonalisatiestelling genaamd. We herhalen eerst een definitie (en voeren notatie in) voor een lineaire transformatie.

Definitie 2.2.2. Zij k een lichaam, $n \in \mathbb{N}_+$. Een *lineaire transformatie* (van $k[X_1, \ldots, X_n]$ naar $k[X_1, \ldots, X_n]$) is een k-algebra-isomorfisme

$$T : k[\underline{X}] \to k[\underline{X}]$$

zodanig dat $T(X_i)$ een lineaire veelterm is voor $i \in \{1, \ldots, n\}$. De afbeelding T wordt uniek bepaald door de waarden $T(X_1), \ldots, T(X_n)$, of equivalent, door een inverteerbare $n \times n$ matrix $A = [a_{ij}]_{i=1,j=1}^{n}$ over k met $T(X_i) = \sum_{j=1}^{n} a_{ij} X_j$.

Voor een veelterm $F \in k[\underline{X}]$ noteren we ook F_A of $F(A \cdot \underline{X})$ voor de veelterm $T(F)$.

Merk op dat een samenstelling van lineaire transformaties opnieuw een lineaire transformatie is.

Propositie 2.2.3 (Diagonalisatiestelling)**.** *Zij k een lichaam met* $\mathrm{char}(k) \neq 2$ *en f een kwadratische vorm in n veranderlijken over k. Dan bestaat er een lineaire transformatie T zodanig dat*

$$f = \sum_{i=1}^{n} \beta_i T(X_i)^2$$

voor zekere $\beta_1, \ldots, \beta_n \in k$.

Bewijs. We bewijzen de stelling via inductie op n. Als $n = 1$, dan is $f = \beta_1 X_1^2$ per definitie van een kwadratische vorm, dus kies $T(X_1) = X_1$.

Onderstel dan $n > 1$. Schrijf f als

$$f = \beta_n X_n^2 + X_n L(X_1, \ldots, X_{n-1}) + H(X_1, \ldots, X_{n-1}) \tag{2.1}$$

waar $\beta_n \in k$, $L = L(X_1, \ldots, X_{n-1})$ een lineaire vorm is en $H = H(X_1, \ldots, X_{n-1})$ een kwadratische vorm. Laten we ook eerst onderstellen dat $\beta_n \neq 0$, later zullen we tonen waarom dit (na een lineaire transformatie) altijd het geval is. We kunnen dan schrijven

$$f = \beta_n \left(X_n + \frac{1}{2\beta_n} L \right)^2 - \frac{1}{4\beta_n^2} L^2 + H.$$

Nu is

$$-\frac{1}{4\beta_n^2} L(X_1, \ldots, X_{n-1})^2 + H(X_1, \ldots, X_{n-1})$$

een kwadratische vorm in $n-1$ veranderlijken, zodat er wegens de inductiehypothese een lineaire transformatie $T : k[X_1, \ldots, X_{n-1}] \to k[X_1, \ldots, X_{n-1}]$ bestaat en er $\beta_1, \ldots, \beta_{n-1} \in k$ bestaan zodanig dat

$$-\frac{1}{4\beta_n^2} L^2 + H = \sum_{i=1}^{n-1} \beta_i T(X_i)^2$$

$$f = \beta_n \left(X_n + \frac{1}{2\beta_n} L \right)^2 + \sum_{i=1}^{n-1} \beta_i T(X_i)^2.$$

Stellen we dan

$$T(X_n) = X_n + \frac{1}{2\beta_n} L$$

dan is het duidelijk dat dit de gewenste lineaire transformatie oplevert.

Rest ons nog te tonen waarom we $\beta_n \neq 0$ altijd kunnen bekomen. Herinner dat we in het geval $\beta_n = 0$ hebben dat

$$f = X_n L + H.$$

en schrijf

$$L = \sum_{i=1}^{n-1} a_i X_i$$

voor zekere $a_i \in k$. Als alle $a_i = 0$, dan $L = 0$ en in dat geval is $f \in k[X_1, \ldots, X_{n-1}]$, zodat we de inductiehypothese direct mogen toepassen op $f = H$ en vervolgens $T(X_n) = X_n$ stellen.. Stel dat niet alle $a_i = 0$, dan is zonder verlies van algemeenheid $a_{n-1} \neq 0$. Definieer dan

$$\begin{aligned} R(X_i) &= X_i \qquad i \leq n-2 \\ R(X_{n-1}) &= \frac{X_n + L}{2} \\ R(X_n) &= \frac{X_n - L}{2} \end{aligned}$$

hetgeen een lineaire transformatie is, aangezien haar inverse gegeven wordt door

$$\begin{aligned} R^{-1}(X_i) &= X_i \qquad i \leq n-2 \\ R^{-1}(X_{n-1}) &= \frac{1}{a_{n-1}} \left(X_{n-1} - X_n - \sum_{i=1}^{n-2} a_i X_i \right) \\ R^{-1}(X_n) &= X_n + X_{n-1}. \end{aligned}$$

We vinden

$$\begin{aligned} f &= X_n L + H = \frac{1}{4}(X_n + L)^2 - \frac{1}{4}(X_n - L)^2 + H \\ &= R(X_n)^2 - R(X_{n-1})^2 \\ &+ H\left(R(X_1), \ldots, R(X_{n-2}), \frac{1}{a_{n-1}} \left(R(X_{n-1}) - R(X_n) - \sum_{i=1}^{n-2} a_i R(X_i) \right) \right). \end{aligned}$$

Merk op dat het mogelijk is dat een term uit H met de term $R(X_n)^2$ annihileert, maar dan kan niet gelijktijdig de term $-R(X_{n-1})^2$ wegvallen; eventueel moeten $R(X_n)$ en $R(X_{n-1})$ nog door een lineaire transformatie verwisseld worden. Hiermee hebben we getoond dat, na een lineaire transformatie, we er altijd voor kunnen zorgen dat f een coëfficiënt bij X_n^2 heeft, wat we moesten bewijzen. □

Voor een commutatieve ring A en $n \in \mathbb{N}_+$, noteer $g_A(n)$ voor het kleinste natuurlijke getal g zodanig dat iedere som van kwadraten van n-aire lineaire vormen over A geschreven kan worden als een som van g kwadraten van n-aire lineaire vormen. Indien zo een g niet bestaat, stellen we $g_A(n) = \infty$. Met behulp van vorige propositie vinden we het volgende.

Propositie 2.2.4. *Zij k een lichaam. Dan is*

$$g_k(n) \leq nP(k)$$

Bewijs. Als $\text{char}(k) = 2$ is iedere som van kwadraten zelf een kwadraat en is $g_k(n) = 1$; onderstel vanaf nu $\text{char}(k) \neq 2$. We mogen ook $P = P(k) < \infty$ onderstellen. Beschouw $m \in \mathbb{N}_+$ willekeurig en willekeurige n-aire lineaire vormen $L_1, \ldots, L_m \in k[X_1, \ldots, X_n]$ en laat

$$G = \sum_{i=1}^{m} L_i^2.$$

Wegens Propositie 2.2.3 bestaat er een lineaire transformaties T zodanig dat

$$G = \sum_{i=1}^{n} \beta_i T(X_i)^2$$
$$G_{T^{-1}} = \sum_{i=1}^{n} \beta_i X_i^2$$

Evalueren we $G_{T^{-1}}$ in $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ (een 1 op plaats j), dan bekomen we

$$\beta_j = G_{T^{-1}}(e_j) = \sum_{i=1}^{m} L_i(T^{-1}(e_j), \ldots, T^{-1}(e_j))^2 \in \Sigma k^2.$$

Iedere β_j is dus een som van P kwadraten, zeg maar $\beta_j = \sum_{r=1}^{P} \beta_{j,r}^2$ en we hebben

$$G = \sum_{j=1}^{n} \sum_{r=1}^{P} (\beta_{j,r} T(X_j))^2 \in \Sigma_{nP} k[X_1, \ldots, X_n]^2$$

hetgeen we moesten bewijzen. □

We komen bij de belangrijkste stelling van deze sectie. Samen met vorige propositie werd ze het eerst bewezen in [3, p49-50].

Stelling 2.2.5. *Zij k een commutatieve ring, A een k-algebra. Als A als k-moduul voortgebracht is door $n \in \mathbb{N}_+$ elementen, dan is*

$$P(A) \leq g_k(n).$$

Bewijs. Onderstel dat $g_k(n) < \infty$, anders valt er niets te bewijzen. Zij $y_1, \ldots, y_n \in A$ een stel voortbrengers voor A als k-moduul. Neem een $a \in \Sigma A^2$. Dan bestaan er $N \in \mathbb{N}_+, a_1, \ldots, a_N \in A$ zodanig dat $a = \sum_{i=1}^{N} a_i^2$. Er bestaan $a_{ij} \in k$ voor $1 \leq i \leq N, 1 \leq j \leq n$ zodanig dat $a_i = \sum_{j=1}^{n} a_{ij} y_j$. Beschouw de kwadratische vorm

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{N} (a_{i1} X_1 + \ldots + a_{in} X_n)^2.$$

Deze is te schrijven als een som van $g_k(n)$ kwadraten. Anderzijds, door deze te evalueren in $(y_1, \ldots, y_n)$, vinden we dat a een som van $g_k(n)$ kwadraten is, wat we moesten bewijzen. □

Gevolg 2.2.6. *Indien k een lichaam is en A een k-algebra, dan is*

$$P(A) \leq \dim_k(A) P(k)$$

Bewijs. Volgt door combinatie van Propositie 2.2.4 en Stelling 2.2.5. □

Opmerking 2.2.7. De bovengrens $g_k(n) \leq nP(k)$ is over het algemeen vrij zwak en kan voor bepaalde lichamen verbeterd worden. Zo vond L. Mordell bijvoorbeeld al $g_{\mathbb{Q}}(n) = n + 3$ voor iedere $n \in \mathbb{N}$. [3, p51] Het getal $g_k(n)$ is echter nog maar voor weinig lichamen (laat staan commutatieve ringen) bekend. Enkele recente ontwikkelingen zijn te vinden in [2] en [9].

Propositie 2.2.8. *Zij k een reëel lichaam, beschouw het ideaal $I = (X_1, \ldots X_n)^3$ van $k[X_1, \ldots, X_n]$. Voor de k-algebra $A = k[X_1, \ldots, X_n]/I$ geldt dan $P(A) = g_k(n)$.*

Bewijs. Elk element f van A heeft een (unieke) voorstelling van de vorm

$$f = a + L(\overline{X}) + Q(\overline{X})$$

met $a \in k$, $\overline{X} = (\overline{X_1}, \ldots, \overline{X_n})$, L een lineaire en Q een kwadratische vorm over k. Onderstel $f \in \Sigma A^2$. Dan is $a \in \Sigma k^2$ en $l_k(a) \leq l_A(F)$. Bijgevolg, als $P = P(k) = \infty$, dan ook $P(A) = \infty = g_k(n)$; onderstel in het vervolg dat $P < \infty$.

Stel eerst $a \neq 0$, schrijf $a = \sum_{i=1}^{P} a_i^2$ voor zekere $a_i \in k$. We mogen zonder verlies van algemeenheid $a_1 \neq 0$ onderstellen. Definieer dan

$$f_1 = a_1 + \frac{L(\overline{X})}{2a_1} + R(\overline{X})$$

waarbij R een nog later te bepalen kwadratische vorm is. Deze uitdrukking kwadrateren levert, rekening houdend met het feit dat termen van graad 3 en 4 wegvallen per definitie van de ring A,

$$f_1^2 = a_1^2 + L(\overline{X}) + \frac{L(\overline{X})^2}{4a_1^2} + 2a_1 R(\overline{X}).$$

Als we dan $R = \frac{1}{2a_1}\left(Q - \frac{L^2}{4a_1}\right)$ stellen, dan is

$$f_1^2 = a_1^2 + L(\overline{X}) + Q(\overline{X})$$

zodat

$$f = f_1^2 + a_2^2 + \ldots + a_P^2 \in \Sigma_P A^2 \subseteq \Sigma_{g_k(n)} A^2$$

aangezien $P \leq g_k(n)$.

Stel dan $a = 0$. Omdat $f \in \Sigma A^2$, bestaan er $N \in \mathbb{N}_+, a_1, \ldots, a_N \in k$, lineaire vormen $L_1, \ldots, L_N$ en kwadratische vormen $Q_1, \ldots, Q_N$ zodanig dat

$$f = \sum_{i=1}^{N} (a_i + L_i(\overline{X}) + Q_i(\overline{X}))^2.$$

De constante term in beide leden vergelijkend levert dan

$$0 = a = \sum_{i=1}^{N} a_i^2,$$

hetgeen impliceert dat $a_i = 0$ voor alle i, aangezien k reëel is. Rekening houdend met het feit dat termen van graad 3 en hoger wegvallen, vinden we

$$Q(\overline{X}) = f = \sum_{i=1}^{N} L_i(\overline{X})^2$$

hetgeen enkel kan indien

$$Q = \sum_{i=1}^{N} L_i^2$$

in $k[X_1, \ldots, X_n]$. We vinden hieruit dat $P(A) \leq g_k(n)$. Omgekeerd, stel dat Q een som van kwadraten van lineaire vormen in $k[X_1, \ldots, X_n]$ is. Bekijken we Q modulo I, dan bestaan er wegens het voorgaande lineaire polynomen $L_1, \ldots, L_N$ met $N \leq P(A)$ zodanig dat

$$\sum_{i=1}^{N} L_i^2 - Q \in I.$$

Alle elementen van $I \setminus \{0\}$ zijn echter polynomen van graad minstens 3, zodat het bovenstaande enkel kan indien

$$Q = \sum_{i=1}^{N} L_i^2$$

en we besluiten dat $g_k(n) = P(A)$. □

Het laatste resultaat van dit hoofdstuk toont aan dat elk natuurlijk getal bereikt kan worden als het pythagorasgetal van een commutatieve ring, zelfs van een eindigdimensionale $\mathbb{R}$-algebra, door $k = \mathbb{R}$ te nemen.

Lemma 2.2.9. *Zij k een lichaam, $n \in \mathbb{N}$ zodanig dat $n \leq S(k)$. Dan is $X_1^2 + \ldots + X_n^2$ geen som van $n-1$ kwadraten in $k[X_1, \ldots, X_m]$ voor iedere $m \geq n$.*

Bewijs. Het is voldoende de bewering te bewijzen voor $m = n$. Onderstel dat er $F_1, \ldots, F_{n-1} \in k[X_1, \ldots, X_n]$ bestaan zodanig dat

$$X_1^2 + \ldots + X_n^2 = F_1^2 + \ldots + F_{n-1}^2.$$

Iedere F_i, $i \in \{1, \ldots, n-1\}$ is dan noodzakelijk linear, zodat we een lineaire afbeelding bekomen

$$F : k^n \to k^{n-1} : \underline{x} \to (F_1(\underline{x}), F_2(\underline{x}), \ldots, F_{n-1}(\underline{x})).$$

Deze afbeelding heeft een niet-triviale kern, dus er bestaat een $\underline{x} = (x_1, \ldots, x_n) \in k^n \setminus \{0\}$ zodanig dat $(F_1(\underline{x}), \ldots, F_{n-1}(\underline{x})) = (0, \ldots, 0)$. Maar dan is

$$x_1^2 + \ldots + x_n^2 = F_1(\underline{x})^2 + \ldots + F_{n-1}(\underline{x})^2 = 0$$

en dit is in tegenspraak met de onderstelling dat $S(k) \geq n$: als bijvoorbeeld $x_1 \neq 0$, dan hebben we uit het bovenstaande dat

$$-1 = \sum_{i=2}^{n} \left(\frac{x_i}{x_1} \right)^2.$$

□

Gevolg 2.2.10. *Neem $n \in \mathbb{N}_+$, zij k een reëel lichaam met $P(k) = 1$. Dan is $g_k(n) = n$. Bovendien geldt $P(A) = n$ met*

$$A = k[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^3.$$

Bewijs. $g_k(n) \leq n$ volgt uit het tweede deel van Propositie 2.2.4 en $g_k(n) \geq n$ volgt uit het lemma. Dat $P(A) = n$, volgt dan weer uit voorgaande propositie. □

Opmerking 2.2.11. De bovenstaande ring A is lokaal, artins en een eindigdimensionale k-algebra, maar geen domein [3, p. 50-51]. Hoffmann toonde aan dat het ook mogelijk is om (reële) lichamen te construeren met eender welk pythagorasgetal. [5, Stelling 1]

2.3 Eindig voortgebrachte reële algebra's

In de vorige sectie zagen we hoe we een bovengrens kunnen vinden voor het pythagorasgetal van een eindigdimensionale k-algebra, met k een lichaam. We verbreden onze blik nu naar eindig voortgebrachte (maar niet noodzakelijk eindigdimensionale) k-algebra's. Als k niet reëel is, kan er alvast niet veel gebeuren.

Propositie 2.3.1. *Zij k een lichaam met* $\mathrm{char}(k) \neq 2$ *en $S(k) = S < \infty$, zij A een k-algebra. Dan is $\Sigma A^2 = A$ en $P(A) \leq S+1$. Verder is $P(k[X_1, \ldots, X_n]) = S + 1$ voor iedere $n \in \mathbb{N}_+$.*

Bewijs. $\Sigma A^2 = A$ en $P(A) \leq S+1$ volgen meteen uit het derde deel van Stelling 1.3.4. $P(k[X_1, \ldots, X_n]) \leq S+1$ vinden we hier als speciaal geval uit. De andere ongelijkheid volgt door Propositie 1.3.5 toe te passen op $A = k$ en te gebruiken dat men $k[X_1, \ldots, X_n]$ surjectief kan afbeelden op $k[X]$ voor iedere $n \in \mathbb{N}_+$. □

We zijn voor de rest van de sectie geïnteresseerd in reële grondlichamen k. In Stelling 3.1.9 zullen we zien dat $P(k[X_1, \ldots, X_n]) = \infty$ zodra $n \geq 2$. In het geval $n = 1$ hebben we een resultaat wanneer $k = \mathbb{R}$; onze focus zal dan ook liggen op algebra's met grondlichaam $\mathbb{R}$.

Propositie 2.3.2. *De sommen van kwadraten in $\mathbb{R}[T]$ zijn juist die veeltermen die geen negatieve waarden kunnen aannemen door ze in $\mathbb{R}$ te evalueren. Verder is $P(\mathbb{R}[T]) = 2$.*

Bewijs. Het is duidelijk dat, als $F \in \mathbb{R}[T]$ een som van kwadraten is, dat $F(a)$ voor iedere $a \in \mathbb{R}$ ook een som van kwadraten, en dus positief, is. Verder hebben we dat $T^2 + 1$ een som van (twee) kwadraten is, maar onmogelijk zelf een kwadraat kan zijn: als het wel het kwadraat van een (noodzakelijk) lineair polynoom in $\mathbb{R}[T]$ was, dan moest het een nulpunt in $\mathbb{R}$ hebben.

Rest ons nog te tonen dat elk polynoom $F \in \mathbb{R}[T]$, dat enkel positieve waarden aanneemt, geschreven kan worden als een som van twee kwadraten. Neem dus zo een F. We mogen F kwadraatvrij onderstellen en kunnen F dan ontbinden als

$$F = c \prod_{i=1}^{n} Q_i(T) \prod_{i=1}^{m} L_i(T)$$

waarbij $m, n \in \mathbb{N}, c \in \mathbb{R}$, $L_1, \ldots, L_m$ paarsgewijs verschillende, monische lineaire polynomen en $Q_1, \ldots, Q_n$ paarsgewijs verschillende, monische kwadratische polynomen zonder reële nulpunten zijn. Iedere L_i heeft een nulpunt $\alpha_i \in \mathbb{R}$ van multipliciteit 1 in F, zodat F in α_i van teken wisselt. Maar dat is in strijd met de onderstelling dat F enkel positieve waarden aanneemt! We besluiten dat $m = 0$. Verder is het duidelijk dat ook $c \geq 0$ moet gelden, en dat c dus een kwadraat is.

Wegens Gevolg 1.2.3 is het nu voldoende te tonen dat ieder monisch kwadratisch polynoom zonder reële nulpunten $Q \in \mathbb{R}[T]$ een som van twee kwadraten is. Schrijf $Q = T^2 + bT + a$, dan is

$$Q = T^2 + bT + a = \left(T + \frac{b}{2}\right)^2 + a - \frac{b^2}{4}$$

en omdat Q geen reële nulpunten heeft, is $a - \frac{b^2}{4} \geq 0$ en dus een kwadraat in $\mathbb{R}$. □

Opmerking 2.3.3. Het is duidelijk dat het bewijs voor $P(\mathbb{R}[T]) = 2$ niet naar andere reële lichamen veralgemeend kan worden. Er bestaat echter wel een klasse van reële lichamen, *reëel gesloten lichamen* genaamd, die vele eigenschappen met $\mathbb{R}$ delen. In de meeste van de stellingen in deze sectie kan $\mathbb{R}$ door een willekeurig reëel gesloten lichamen worden vervangen, maar we zullen dit hier niet doen. Zie [7, hoofdstuk 8] voor meer informatie over reëel gesloten lichamen.

Stelling 2.3.4. *Voor $n \in \mathbb{N}$ geldt*

$$g_{\mathbb{R}[T]}(n) = n + 1.$$

Bewijs. Zie [9, Stelling 7.1, p. 14]. □

Als een eindig voortgebrachte $\mathbb{R}$-algebra integraal is over $\mathbb{R}$, dan is ze eindigdimensionaal als $\mathbb{R}$-algebra (zie bijvoorbeeld [6, Propositie 1.2, p 335]) en heeft ze wegens Stelling 2.2.5 eindig pythagorasgetal. De volgende stelling uit [3, p 52] laat toe dit uit te breiden.

Stelling 2.3.5. *(1) Zij A een $\mathbb{R}[T]$-algebra, als $\mathbb{R}[T]$-moduul voortgebracht door $d < \infty$ elementen, dan is $P(A) \leq d + 1$.*

(2) Zij A een $\mathbb{R}$-algebra met $d = \dim_{\mathbb{R}}(A) < \infty$. Dan is $P(A[T]) \leq d + 1$.

(3) Zij A een eindig voortgebrachte $\mathbb{R}$-algebra van transcendentiegraad 1. Dan is $P(A) < \infty$.

Bewijs. De eerste uitspraak volgt door Stelling 2.2.5 toe te passen op $k = \mathbb{R}[T]$, waarbij we gebruiken dat $g_k(n) = n + 1$ wegens Stelling 2.3.4.

Voor de tweede uitspraak, gebruik dat een basis voor A als $\mathbb{R}$-vectorruimte een stel voortbrengers wordt voor $A[T]$ als $\mathbb{R}[T]$-moduul; pas dan het eerste deel toe.

We bewijzen tenslotte de derde uitspraak. Wegens het Noether Normalizatielemma (zie bijvoorbeeld [1, Oefening 16, p 69]) bestaat er een element $t \in A$, zelf transcendent over $\mathbb{R}$, zodanig dat A een integrale uitbreiding is van $\mathbb{R}[t]$. Aangezien A eindig voortgebracht is als $\mathbb{R}$-algebra, is A eindig voortgebracht als $\mathbb{R}[t]$-moduul (gebruik weer [6, Propositie 1.2, p 335]). Pas dan weer het eerste deel van de stelling toe. □

Opmerking 2.3.6. Het derde deel van vorige stelling vereist enkel dat $g_{\mathbb{R}[T]}(n) < +\infty$ voor iedere $n \in \mathbb{N}$, een veel zwakker resultaat dan Stelling 2.3.4 dat ook al eerder bekend was. De twee eerste delen werden aanvankelijk in een zwakkere vorm geformuleerd, gebaseerd op de toen bekende bovengrens $g_{\mathbb{R}[T]}(n) \leq 2n$. [3, p52]

Voorbeeld 2.3.7. $\{1, X\}$ is een stel voortbrengers (van minimale grootte) van $A = \mathbb{R}[X, Y]/(X^2 + Y^2)$ als $\mathbb{R}[Y]$-moduul, zodat $P(A) \leq 3$ wegens het eerste deel van Stelling 2.3.5. Hier wordt echter al duidelijk dat deze afschatting niet optimaal is; in [3, p 54-55] wordt bewezen dat $P(\mathbb{R}[X, Y]/(F)) = 2$ voor ieder tweedegraadspolynoom F.

Voorbeeld 2.3.8. Zij $A = \mathbb{R}[X_1, \ldots, X_n]/I$, waar I het ideaal is voortgebracht door $\{X_i X_j \mid i \neq j\}$. Stellen we $t = \overline{X_1 + \ldots + X_n}$, dan is A als $\mathbb{R}[t]$-moduul voortgebracht door $\{\overline{X_1}, \ldots, \overline{X_n}\}$ ($\overline{X_i}^d = t^{d-1}\overline{X_i}$ voor iedere $d \in \mathbb{N}_+$) zodat we $P(A) \leq n + 1$ vinden door Stelling 2.3.5. In feite geldt er $P(A) = 2$. [3, p 52]

Bewijs. Neem $f(\overline{X}_1, \ldots, \overline{X}_n) \in \Sigma A^2$. f heeft een representatie van de vorm

$$f(\overline{X}_1, \ldots, \overline{X}_n) = a + \sum_{i=1}^{n} \overline{X}_i g_i(\overline{X}_i)$$

voor zekere $a \in \mathbb{R}$, $g_i \in \mathbb{R}[\overline{X}_i]$. Zij $T_i : \mathbb{R}[X_1, \ldots, X_n] \to \mathbb{R}[X_i]$ het $\mathbb{R}$-algebramorfisme bepaald door $T_i(X_j) = \delta_{i,j} X_i$. Aangezien $\operatorname{Ker} T_i \supseteq I$, induceert T_i een $\mathbb{R}$-algebramorfisme $\tilde{T}_i : A \to \mathbb{R}[X_i]$. We hebben $\tilde{T}_i(f) = a + X_i g_i(X_i) \in \Sigma\mathbb{R}[X_i]^2$, zodat $a + X_i g_i(X_i)$ (en dus ook $a + \overline{X_i} g_i(\overline{X_i})$) een som van twee kwadraten is wegens Propositie 2.3.2. In het bijzonder is $a \geq 0$.

Als $a > 0$, dan is

$$f = \frac{1}{a^{n-1}} \prod_{i=1}^{n} (a + \overline{X_i} g_i(\overline{X_i}))$$

en aangezien alle factoren van dit product sommen van twee kwadraten zijn, is f een som van twee kwadraten wegens Gevolg 1.2.3.

Stel tenslotte dat $a = 0$. Schrijf $X_i g_i(X_i) = h_i(X_i)^2 + k_i(X_i)^2$ voor zekere $h_i, k_i \in \mathbb{R}[X_i]$. Dan zijn h_i en k_i deelbaar door X_i (gebruikt dat $\mathbb{R}$ reëel is!) zodat $h_i(\overline{X_i})h_j(\overline{X_j}) = 0 = k_i(\overline{X_i})k_j(\overline{X_j})$ als $i \neq j$. We vinden

$$f = \sum_{i=1}^{n} h_i(\overline{X_i})^2 + \sum_{i=1}^{n} k_i(\overline{X_i})^2 = \left(\sum_{i=1}^{n} h_i(\overline{X_i}) \right)^2 + \left(\sum_{i=1}^{n} k_i(\overline{X_i}) \right)^2$$

zodat $f \in \Sigma_2 A^2$. We hebben getoond dat $P(A) \leq 2$. Aangezien $1 + \overline{X_i}^2$ geen kwadraat is ($T_i(1 + \overline{X_i}^2) = 1 + X_i^2$ is geen kwadraat in $\mathbb{R}[X_i]$), is $P(A) = 2$. □

Tenslotte willen we nog aantonen dat het derde deel van Stelling 2.3.5 niet omgekeerd kan worden; het is niet omdat een eindig voortgebrachte $\mathbb{R}$-algebra A een transcendentiegraad van 2 of hoger heeft, dat $P(A) = \infty$. Volgend lemma en gevolg zijn in iets andere vorm terug te vinden in [3, p. 48-49 en p. 56].

Lemma 2.3.9. *Zij I een ideaal van een commutatieve ring A, voortgebracht door $a_1, \ldots, a_n$. Onderstel dat $2 \in A^\times$ en dat $a_1, \ldots, a_n, -a_1, \ldots, -a_n \in \Sigma_r A^2$ voor zekere $r \in \mathbb{N}_+$. Voor iedere $c \in A$ is dan $l_{A/I}(\overline{c}) \leq l_A(c) \leq l_{A/I}(\overline{c}) + 2rn$. Bijgevolg is $P(A/I) \leq P(A) \leq P(A/I) + 2rn$ en in het bijzonder geldt er $P(A) < \infty$ als en slechts als $P(A/I) < \infty$.*

Bewijs. Zij $B = A/I$. $l_B(\overline{c}) \leq l_A(c)$ voor alle $c \in A$ weten we uit Propositie 1.1.3. Omgekeerd, neem $c \in A$ willekeurig, onderstel $p = l_B(\overline{c}) < \infty$ (anders valt er niets te bewijzen). Dan bestaan er $c_1, \ldots, c_p \in A$ zodanig dat $\overline{c} = \sum_{i=1}^{p} \overline{c_i}^2$. Voor zekere $b_1, \ldots, b_n \in A$ geldt dan

$$c = \sum_{i=1}^{p} c_i^2 + \sum_{i=1}^{n} b_i a_i.$$

We hebben $b_i = d_i^2 - e_i^2$ met $d_i = \frac{b_i + 1}{2}$ en $e_i = \frac{b_i - 1}{2}$. Dit geeft

$$c = \sum_{i=1}^{p} c_i^2 + \sum_{i=1}^{n} a_i d_i^2 + \sum_{i=1}^{n} (-a_i) e_i^2$$

zodat c een som van $p + 2rn$ kwadraten is, wat we moesten bewijzen. □

Opmerking 2.3.10. De bovengrens $l_A(c) \leq l_{A/I}(\overline{c}) + 2rn$ zou nog verscherpt kunnen worden door $l(a_i)$ en $l(-a_i)$ apart te bekijken voor iedere i. We krijgen dan

$$l_A(c) \leq l_{A/I}(\overline{c}) + \sum_{i=1}^{n} (l_A(a_i) + l_A(-a_i)).$$

In het vervolg hebben we echter enkel nodig dat $P(A)$ eindig is.

Gevolg 2.3.11. *Zij R een ring met $2 \in R^\times$, zij $b_1, \ldots, b_n \in R$. Dan is $P(R/(b_1^2 + \ldots + b_n^2)) < \infty$ als en slechts als $P(R/(b_1^2, \ldots, b_n^2)) < \infty$.*

Bewijs. Stel $A = R/(b_1^2 + \ldots + b_n^2)$ en $a_i = \overline{b_i}^2 \in \Sigma_{n-1}A^2$, dan is $-a_i = \sum_{j=1, j\neq i}^n \overline{b_i}^2 \in \Sigma_{n-1}A^2$, zodat we vorig lemma kunnen toepassen met $I = (a_1, \ldots, a_n)$, gebruikend dat A/I isomorf is met $R/(b_1^2, \ldots, b_n^2)$. □

Propositie 2.3.12. *Stel dat $\mathbb{R}[X_1, \ldots, X_n]/(F_1^2, \ldots, F_r^2)$ transcendentiegraad hoogstens 1 heeft over $\mathbb{R}$ voor zekere $F_1, \ldots, F_r \in \mathbb{R}[X_1, \ldots, X_n]$. Dan is $P(A) < \infty$ met $A = \mathbb{R}[X_1, \ldots, X_n]/(F_1^2 + \ldots + F_r^2)$.*

Bewijs. Dit volgt uit vorig gevolg en het derde deel van Stelling 2.3.5. □

Voorbeeld 2.3.13. Voorbeelden van $\mathbb{R}$-algebra's met transcendentiegraad $n-1$ over $\mathbb{R}$, maar eindig pythagorasgetal, zijn $\mathbb{R}[X_1, \ldots, X_n]/(X_1^2 + \ldots + X_n^2)$ en $\mathbb{R}[X_1, \ldots, X_n]/(X_1^2 + \ldots + X_{n-1}^2)$.

Hoofdstuk 3

Ringen met oneindig pythagorasgetal

3.1 Veeltermenringen

Zoals eerder vermeld bestaan er ringen met oneindig Pythagorasgetal, wat erop neerkomt dat er elementen bestaan van willekeurig hoge, eindige lengte. Het doel van deze sectie is om een paar voldoende voorwaarden te formuleren, zodanig dat $P(A[X]) = \infty$ zodra A aan deze voorwaarden voldoet. Het bewijs is grotendeels overgenomen uit [3, hoofdstuk 4], maar wat verder uitgewerkt.

Voor een commutatieve ring A en een natuurlijk getal n, noteer

$$U_n(A) = \{(a_1, \ldots, a_n) \in A^n \mid a_1^2 + \ldots + a_n^2 = 1\}$$

voor de eenheidsvectoren over A. We zullen U_n schrijven in plaats van $U_n(A)$ indien geen verwarring mogelijk is. Noteer verder

$$O_n(A) = \{M \in \mathbb{M}_n(A) \mid M^T M = I_n\}$$

voor de verzameling van de orthogonale $n \times n$ matrices over A. Opnieuw zullen we O_n in plaats van $O_n(A)$ noteren.

Propositie 3.1.1. *O_n vormt een deelgroep van GL_n (de inverteerbare $n \times n$ matrices) met de matrixvermenigvuldiging en*

$$O_n \times U_n \to U_n : (M, v) \mapsto M \cdot v$$

bepaalt een groepsactie van O_n op U_n.

Bewijs. Dat O_n een deelgroep is van GL_n, is duidelijk uit de identiteit $(MN)^T = N^T M^T$ voor alle $M, N \in \mathbb{M}_n$ en uit het feit dat $M^T = M^{-1}$ voor iedere $M \in O_n$. Verder wordt U_n ook beschreven door de verzameling van alle kolomvectoren v in A^n waarvoor $v^T v = 1$, zodat voor iedere $M \in O_n$ geldt dat $Mv \in U_n$, aangezien $(Mv)^T Mv = v^T M^T Mv = v^T v = 1$. □

Propositie 3.1.2. *Zij k een reëel lichaam met* $\mathrm{char}(k) \neq 2$. *Dan is er voor iedere $W \in k^n \setminus \{0\}$ een unieke matrix $M_W \in O_n(k)$ met voor alle $V \in k^n$*

$$M_W V = V - \frac{2V^T W}{W^T W} W.$$

Bovendien geldt voor $V \neq W \in U_n(k)$ dat $M_{W-V}V = W$, in het bijzonder werkt O_n transitief op U_n.

Bewijs. Dat er een unieke matrix $M_W \in \mathbb{M}_n(k)$ bestaat die aan bovenstaande formule voldoet, is duidelijk: de afbeelding

$$\tau_W : k^n \to k^n : V \mapsto V - \frac{2V^T W}{W^T W} W$$

is k-lineair, zodat de i-de kolom ($1 \leq i \leq n$) van M_W juist het beeld onder τ_W is van de i-de kanonieke basisvector $e_i = [\delta_{i,j}]_{j=1}^n$. Verder rekenen we gemakkelijk na voor $V_1, V_2 \in k^n$ dat

$$(M_W V_1)^T (M_W V_2) = \left(V_1^T - \frac{2V_1^T W}{W^T W} W^T\right)\left(V_2 - \frac{2V_2^T W}{W^T W} W\right) = V_1^T V_2.$$

Hieruit volgt dat $M_W^T M_W$ de eenheidsmatrix is, aangezien het element op plaats (i,j) ($1 \leq i,j \leq n$) van $M_W^T M_W$ gegeven wordt door

$$e_i^T M_W^T M_W e_j = (M_W e_i)^T (M_W e_j) = e_i^T e_j = \delta_{i,j}.$$

De gelijkheid $M_{W-V}V = W$ kan je gemakkelijk uitrekenen voor $V, W \in U_n(k)$, gebruikend dat $V^T V = W^T W = 1$. □

Voor een commutatieve ring A en een natuurlijk getal $n \in \mathbb{N}_+$, noteer

$$\mathcal{D}_n(A) = \{\alpha \in A \setminus \{0\} \mid \forall (a_1, \ldots, a_n) \in U_n(A) \forall i \in \{1, \ldots, n\} : \alpha \nmid a_i \text{ of } a_i = 0\}$$

en formuleer volgende twee criteria:

$(1)_n$ De groepsactie van O_n op U_n is transitief.

$(2)_n$ $\mathcal{D}_n(A) \neq \emptyset$

Lemma 3.1.3. *Als A een domein is met* $\mathrm{char}(A) \neq 2$ *dat aan $(2)_n$ voldoet, dan bevat $\mathcal{D}_n(A)$ oneindig veel elementen die 2 niet delen.*

Bewijs. Fix een $\alpha \in \mathcal{D}_n(A)$. Dan is α niet inverteerbaar, anders zou $\alpha \mid 1$, in tegenspraak met $(1, 0, \ldots, 0) \in U_n$. We mogen α door 2α vervangen, want als $2\alpha \mid a$ voor zekere $a \in A$, dan $\alpha \mid a$. Aldus mogen we $\alpha \nmid 2$ onderstellen.

Omdat α niet inverteerbaar is, is A geen lichaam en is A dus oneindig. Dan is ook $A\alpha$ oneindig (de afbeelding $f : A \to A\alpha : x \mapsto \alpha x$ is injectief) en $A\alpha \setminus \{0\} \subseteq \mathcal{D}_n(A)$. □

Stelling 3.1.4. *Zij A een reëel domein, $n \in \mathbb{N}_+$, onderstel dat A voldoet aan $(1)_n$ en $(2)_n$. Onderstel dat $f(X) \in A[X]$ een polynoom is met $l_{A[X]}(f(X)) = n$ en zij $r \in \mathbb{N}_+$ zodanig dat $\deg f < 2r$. Stel $\alpha_1 = 0$ en $\{\alpha_j \in \mathcal{D}_n(A) \mid 2 \leq j \leq r\}$ verschillende elementen met $\alpha_j \nmid 2$. Dan is $F(X) = \Delta_r(X)^2 f(X) + 1$ een polynoom van lengte $n+1$, waar $\Delta_r(X) = (X - \alpha_1) \dots (X - \alpha_r)$.*

Bewijs. We hebben zeker $F \in \Sigma_{n+1} A[X]^2$, dus het volstaat te tonen dat $F \notin \Sigma_n A[X]^2$. Stel uit het ongerijmde dat $F(X) = \sum_{i=1}^n \psi_i(X)^2$ voor zekere $\psi_i \in A[X], 1 \leq i \leq n$. We hebben $\deg(F(X)) = 2\deg(\Delta_r(X)) + \deg(f(X)) < 4r$, zodat $\deg(\psi_i(X)) < 2r$ voor $1 \leq i \leq n$, waar we gebruikt hebben dat A reëel is.

Evalueren we F in 0, dan bekomen we

$$1 = \Delta_r(0)^2 f(0) + 1 = F(0) = \sum_{i=1}^n \psi_i(0)^2$$

aangezien $\alpha_1 = 0$. Stellen we $V(X) = (\psi_1(X), \dots, \psi_n(X))^T \in A[X]^n$, dan is $V(0) \in U_n(A)$, zodat er wegens $(1)_n$ een $M = [m_{ij}]_{i=1,j=1}^n \in O_n(A)$ bestaat met $MV(0) = (1, 0, \dots, 0)^T$. Verder is $F = V(X)^T V(X) = (MV(X))^T MV(X) = \sum_{i=1}^n \varphi_i(X)^2$ met $\varphi_i(X) = \sum_{j=1}^n m_{ij}\psi_j(X)$ $(1 \leq i \leq n)$, $\varphi_1(0) = 1$ en $\varphi_i(0) = 0$ voor $i \geq 2$.

Schrijf $\varphi_1(X) = 1 + X\phi_1(X)$, $\varphi_i(X) = X\phi_i(X)$ $(i \geq 2)$ voor zekere $\phi_1, \dots, \phi_n \in A[X]$. Evalueren we F in $\alpha \in \{\alpha_2, \dots, \alpha_r\}$, dan is

$$1 = \Delta_r(\alpha)^2 f(\alpha) + 1 = F(\alpha) = \sum_{i=1}^n \varphi_i(\alpha)^2 = (1 + \alpha\phi_1(\alpha))^2 + \sum_{i=2}^n \alpha^2 \phi_i(\alpha)^2$$

zodat $\phi_2(\alpha) = \dots = \phi_n(\alpha) = 0$ aangezien $\alpha \in \mathcal{D}_n(A)$. Er geldt bijgevolg dat iedere φ_i voor $2 \leq i \leq r$ deelbaar is door $\Delta_r(X)$. Schrijven we $\varphi_i(X) = \Delta_r(X)\varphi_i'(X)$, dan vinden we achtereenvolgens

$$\begin{aligned}
\Delta_r(X)^2 \left(f(X) - \sum_{i=2}^n \varphi_i'(X)^2 \right) &= \Delta_r(X)^2 f(X) - \sum_{i=2}^n \left(\Delta_r(X)\varphi_i'(X)\right)^2 \\
&= F(X) - 1 - \sum_{i=2}^n \varphi_i(X)^2 = \varphi_1(X)^2 - 1 \\
&= (\varphi_1(X) - 1)(\varphi_1(X) + 1) \\
&= (\varphi_1(X) - 1)(2 + X\phi_1(X)). \qquad (3.1)
\end{aligned}$$

Geen van de $\alpha_2, \dots, \alpha_r$ deelt 2, zodat $\Delta_r(X)^2 \mid (\varphi_1(X) - 1)$. Maar $\deg(\Delta_r(X)^2) = 2r$ terwijl $\deg(\varphi_1(X)) \leq \max_{i=1}^n \deg(\psi_i(X)) < 2r$, zodat $\varphi_1(X) = 1$ moet gelden. Het rechterlid in (3.1) wordt dan 0, zodat $f(X) = \sum_{i=2}^n \varphi_i'(X)^2$ omdat A een domein is. Dit is in tegenspraak met de onderstelling dat $l(f) = n$. □

Gevolg 3.1.5. *Als A een reëel domein is dat aan $(1)_n$ en $(2)_n$ voldoet voor alle $n \in \mathbb{N}_+$, dan $P(A[X]) = \infty$.*

Bewijs. Dit volgt uit de stelling door bijvoorbeeld $f_1(X) = 1$ te stellen en recursief een element van lengte n te vinden, $f_n(X)$, door de stelling toe te passen op het element van lengte $n-1$, $f_{n-1}(X)$. □

Opmerking 3.1.6. De constructie uit Stelling 3.1.4 en haar gevolg geeft een rij polynomen $(f_n)_n$ waarbij de graad van f_n meer dan het dubbel is van die van f_{n-1}, de graad neemt dus exponentieel toe met de lengte. Voor bepaalde ringen A is het mogelijk een algoritme te vinden voor een rij polynomen $(g_n)_n$ met stijgende lengte, maar waarbij de graad lineair toeneemt met n. In [3, hoofdstuk 4bis] worden er zo enkele voorbeelden uitgewerkt.

Het volgende gevolg laat onder andere zien dat $\mathbb{Z}[X]$ oneindig pythagorasgetal heeft.

Gevolg 3.1.7. *Zij A een reëel domein dat geen lichaam is. Onderstel dat, voor alle $n \in \mathbb{N}$, als $a_1^2 + \ldots + a_n^2 = 1$ in A, slechts één van de a_i verschilt van 0. Dan $P(A[X]) = \infty$.*

Bewijs. Per definitie bestaat $U_n(A)$ in dit geval uitsluitend uit de permutaties van $(1, 0, \ldots, 0)$ en $(-1, 0, \ldots, 0)$. Voor $(2)_n$ kunnen we dus een willekeurig niet-inverteerbaar element als α nemen. Voor $(1)_n$, merk op dat de orthogonale matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix}$$

de vector met een 1 op plaats k omzet naar de vector met een 1 op plaats $k-1 \pmod n$ en dat de orthogonale matrix $-I_n$ (met I_n de eenheidsmatrix) het teken van de vector wisselt. Tezamen brengen zij alle mogelijke permutaties voort, zodat aan $(1)_n$ voldaan is en Stelling 3.1.4 kan worden toegepast. □

Gevolg 3.1.8. *Zij A een reëel domein, maar geen lichaam. Stel dat A een lichaam k bevat zodanig dat $U_n(A) = U_n(k)$. Dan $P(A[X]) = \infty$.*

Bewijs. Voor $(2)_n$, neem net als in vorig gevolg een willekeurig niet-inverteerbaar element als α. $(1)_n$ volgt direct uit Propositie 3.1.2. □

Stelling 3.1.9. *Zij k een reëel lichaam, A een k-deelalgebra van $k[X_1, \ldots, X_r]$ die van k verschilt. Dan is $P(A[X]) = \infty$. In het bijzonder is voor ieder reëel lichaam k en $r \geq 2$, $P(k[X_1, X_2, \ldots, X_r]) = \infty$.*

Bewijs. Dit volgt vrij direct uit vorig gevolg: onderstel $a_1^2 + \ldots + a_n^2 = 1$, $a_i \in A$. Na permutatie van de a_i's mogen we onderstellen dat a_1 de hoogste graad heeft (beschouwd als polynoom over k), laat $d = \deg a_1$ en onderstel uit het ongerijmde dat $d \neq 0$ (als $d = 0$, dan is $a_i \in k$ voor alle $i \in \{1, \ldots, n\}$).

Neem een willekeurig monoom $X_1^{d_1}X_2^{d_2}\cdots X_r^{d_r}$ van graad d (dat wil zeggen zodanig dat $d = d_1 + \ldots + d_r$) en laat c_i de hierbij horende coëfficiënt zijn in a_i. Door de keuze van d als hoogste graad, krijgen we bij het vergelijken van de coëfficiënten horend bij $X_1^{2d_1}X_2^{2d_2}\cdots X_r^{2d_r}$ in de vergelijking $a_1^2 + \ldots + a_n^2 = 1$, $c_1^2 + \ldots + c_n^2 = 0$, wat (wegens k reëel) impliceert dat alle $c_i = 0$. Maar dit geldt voor elk monoom van graad d, in tegenspraak met $d = \deg a_1$. □

3.2 Hoofdideaalringen

Stelling 3.1.9 en andere uit voorgaande sectie laten toe een aantal voorbeelden te geven van constructies die de eindigheid van het pythagorasgetal niet behouden. De meeste van deze voorbeelden zijn in gelijkaardige vorm te vinden in [3, p. 56-58]

Om te beginnen is $\mathbb{R}[X]$ een hoofdideaalring met $P(\mathbb{R}[X]) = 2$, maar is $P(\mathbb{R}[X][Y]) = \infty$. Bovendien is $\mathbb{Z}$ een euclidisch domein met $P(\mathbb{Z}) = 4$, maar is $P(\mathbb{Z}[X]) = \infty$. Dit toont dat eindigheid van het pythagorasgetal van een ring niet wordt overgedragen op de veeltermenring, zelfs niet voor hoofdideaalringen.

Verder kunnen ook niet-reële $\mathbb{R}$-algebra's oneindig pythagorasgetal hebben. De algebra $A = \mathbb{R}[W, X, Y, Z]/(Y^2 + Z^2)$ is niet reëel omdat $\overline{Y}^2 + \overline{Z}^2 = 0$, maar heeft een oneindig pythagorasgetal: het surjectief $\mathbb{R}$-algebramorfisme $T : \mathbb{R}[W, X, Y, Z] \to \mathbb{R}[W, X]$ bepaald door $T(W) = W, T(X) = X$ en $T(Y) = T(Z) = 0$ voldoet aan $\operatorname{Ker} T \supseteq (Y^2 + Z^2)$, zodat het een surjectief $\mathbb{R}$-algebramorfisme $\tilde{T} : A \to \mathbb{R}[X, Y]$ induceert. $P(A) = \infty$ volgt dan uit het eerste deel van Propositie 1.1.3.

Ook twee lokaal-globaal resultaten ontbreken. Hoewel $\mathbb{R}[X, Y]$ oneindig pythagorasgetal heeft, hebben alle quotiënten van $\mathbb{R}[X, Y]$ transcendentiegraad ≤ 1 over $\mathbb{R}$ en dus eindig pythagorasgetal wegens Stelling 2.3.5. Men kan ook bewijzen dat $P(\mathbb{R}[X, Y]_{\mathfrak{p}}) = 4$ voor iedere priemideaal $\mathfrak{p}$ van $\mathbb{R}[X, Y]$; het bewijs hiervan steunt op de theorie van kwadratische vormen en werken we niet uit, zie bijvoorbeeld [3, p. 57] voor een bewijs.

Als laatste voorbeeld willen we nog tonen dat het breukenlichaam van een hoofdideaalring met oneindig pythagorasgetal zelf eindig pythagorasgetal kan hebben. Hiervoor zullen we beroep doen op een van de belangrijkste stellingen uit de theorie van het pythagorasgetal van lichamen, dat we zonder bewijs vermelden. Opnieuw mag $\mathbb{R}$ vervangen worden door eender welk reëel gesloten lichaam, zie Opmerking 2.3.3.

Stelling 3.2.1 (Pfister)**.** *Zij k een lichaam van transcendentiegraad $n \in \mathbb{N}$ over $\mathbb{R}$. Dan is $P(k) \leq 2^n$. In het bijzonder geldt dit voor $k = \mathbb{R}(X_1, \ldots, X_n)$.*

Bewijs. Zie [10, p. 92]. □

Lemma 3.2.2 (Wadsworth A.)**.** *Zij S een multiplicatieve verzameling ($0 \notin S$) in een domein A, voortgebracht door een verzameling S_0 waarvan ieder element een reëel hoofdideaal voortbrengt. Voor iedere $a \in A$ is dan $l_A(a) = l_{A_S}(a)$. In het bijzonder is $P(A) = P(A_S)$.*

Bewijs. Neem $a \in A$. $l_A(a) \geq l_{A_S}(a)$ volgt direct uit Propositie 1.1.3. Onderstel nu dat $a \in \sum_r A_S^2$ voor zekere $r \in \mathbb{N}$. Dan bestaan er $s \in S, a_1, \ldots, a_r \in A$ zodanig dat

$$as^2 = \sum_{i=1}^{r} a_i^2. \tag{3.2}$$

Stel om te beginnen dat $s \in S_0$. Bovenstaande vergelijking modulo s bekijken levert dan $0 = \sum_{i=1}^{r} \overline{a_i}^2$, hetgeen impliceert dat $\overline{a_i} = 0$ voor $1 \leq i \leq r$ (aangezien $A/(s)$ reëel is), of nog, $a_i = sb_i$ voor zekere $b_1, \ldots, b_r \in A$. Dit invullen in (3.2) geeft achtereenvolgens

$$as^2 = \sum_{i=1}^{r} (sb_i)^2$$
$$a = \sum_{i=1}^{r} b_i^2 \in \Sigma_r A^2$$

zodat we het gestelde getoond hebben voor $s \in S_0$. Het algemene geval volgt door op te merken dat iedere $s \in S$ geschreven kan worden als een product van elementen uit S_0 en dan bovenstaande procedure recursief toe te passen. □

Propositie 3.2.3. *Zij $n \in \mathbb{N}$, $n \geq 2$. Ieder maximaal ideaal van $\mathbb{R}[X_1, \ldots, X_n]$ bevat een lineair polynoom.*

Bewijs. Onderstel dat M een maximaal ideaal van $\mathbb{R}[X_1, \ldots, X_n]$ is. Stel $k = \mathbb{R}[X_1, \ldots, X_n]/M$. Dan is k een lichaamsuitbreiding van $\mathbb{R}$ en omdat k eindig voortgebracht is als $\mathbb{R}$-algebra, is k een algebraïsche uitbreiding van $\mathbb{R}$ wegens het Lemma van Zariski [1, Oefening 18, p. 70]. k kan dan ingebed worden in $\mathbb{C}$ (zie [6, Stelling 2.8, p. 233]), in het bijzonder is $\dim_{\mathbb{R}}(k) \leq 2$.

De $n+1 > 2$ elementen $1, \overline{X_1}, \ldots, \overline{X_n} \in k$ vormen dus een $\mathbb{R}$-lineair afhankelijke collectie. Er bestaan aldus $a, a_1, \ldots, a_n \in \mathbb{R}$ zodanig dat $a + a_1\overline{X_1} + \ldots + a_n\overline{X_n} = \overline{0}$, of nog,

$$a + a_1X_1 + \ldots + a_nX_n \in M$$

□

Propositie 3.2.4. *Zij S_0 de verzameling lineaire polynomen in $\mathbb{R}[X, Y]$ en S het hierdoor voortgebrachte multiplicatieve deel van $\mathbb{R}[X, Y]$. Laat $R = \mathbb{R}[X, Y]_S$. Dan is R een hoofdideaalring met $P(R) = \infty$ en het breukenlichaam van R is $\mathbb{R}(X, Y)$.*

Bewijs. R is een lokalisatie van de factoriële ring $\mathbb{R}[X, Y]$, dus zelf factorieel. [6, Oefening 5, p. 115] Als we kunnen tonen dat de Krulldimensie van R één is, dan weten we dat R een hoofdideaalring is. $\mathbb{R}[X, Y]$ heeft Krulldimensie twee en de priemidealen van R corresponderen met de priemidealen van $\mathbb{R}[X, Y]$ die een lege doorsnede hebben met S. Wegens Propositie 3.2.3 zijn dit enkel priemidealen van $\mathbb{R}[X, Y]$ van hoogte hoogstens 1, zodat elk priemideaal van hoogte 1 in R maximaal is, hetgeen we moesten bewijzen.

Dat $\mathbb{R}(X,Y)$ het breukenlichaam is van R, is duidelijk. We willen tonen dat $P(R) = P(\mathbb{R}[X,Y]) = \infty$ door gebruik te maken van Lemma 3.2.2. Hiervoor moeten we tonen dat elk lineair polynoom $aX + bY + c \in \mathbb{R}[X,Y]$ ($a, b, c \in \mathbb{R}$ met a en b niet beide 0) een reëel hoofdideaal voortbrengt. Stel zonder verlies van algemeenheid dat $b \neq 0$, beschouw dan het unieke $\mathbb{R}$-algebramorfisme $f : \mathbb{R}[X,Y] \to \mathbb{R}[Z]$ met de eigenschap dat $f(X) = Z$ en $f(Y) = \frac{-a}{b}Z - \frac{c}{b}$. Men gaat gemakkelijk na dat dit surjectief is en dat ker $f = (aX + bY + c)$. Bijgevolg is

$$\frac{\mathbb{R}[X,Y]}{(aX + bY + c)} \cong \mathbb{R}[Z],$$

wat een reële ring is wegens Propositie 2.1.5. □

Tot slot willen we nog opmerken dat de constructie uit Stelling 3.1.4 de basis vormt voor veel meer stellingen over ringen met oneindig pythagorasgetal die geen veeltermring zijn over een bepaalde ring. In [3, p. 74 e.v.] wordt zo bijvoorbeeld bewezen dat elke reële algebra (over eender welk grondlichaam) met Krulldimensie ≥ 3, oneindig pythagorasgetal heeft.

Bibliografie

[1] Atiyah M. F. en Macdonald I. G. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[2] Becher K. J. en Leep D. B. *The length and other invariants of a real field.* Springer-Verlag, 2010.

[3] Choi M.D., Dai Z.D., Lam, T.Y. en Reznick B. *The Pythagoras number of some affine algebras and local algebras.* 1981.

[4] Dickson L. E., *History of the Theory of Numbers, Vol. II.* Verenigde Staten van Amerika: Carnegie Institution of Washington, 1919.

[5] Hoffmann D. W. Pythagoras number of fields. *Journal of the American Mathematical Society.* 1999, 12(3): p. 839-848.

[6] Lang S. *Algebra.* 3de uitgave. Verenigde Staten van Amerika: Addison-Wesley Publishing Company, 1999.

[7] Lam, T.Y. *Introduction to Quadratic Forms over Fields.* Providence, Rhode Island: American Mathematical Society, 2005.

[8] Leep, D. B. en Hoffmann, D.W. *Sums of squares in nonreal commutative rings.* Lexington: University of Kentucky, Department of Mathematics, 2010. (Ongepubliceerd paper)

[9] Leep, D. B. *Sums of squares of polynomials and the invariant $g_n(R)$.* Lexington: University of Kentucky, Department of Mathematics, 2006.

[10] Pfister A. *Quadratic forms with applications to geometry and topology.* Cambridge: University Press, 1995.

[11] Shapiro D. B. *Compositions of Quadratic Forms.* Berlijn: Walter de Gruyter, 2000.