

QUADRATIC MODULES IN $R[[X]]$

DORIS AUGUSTIN AND MANFRED KNEBUSCH

(Communicated by Bernd Ulrich)

ABSTRACT. We give a complete list of all quadratic modules and inclusions between them in the ring $R[[X]]$ of formal power series in one variable X over a euclidean field R .

1. INTRODUCTION

A *quadratic module* in a commutative ring A (always with unit element) is a subset Q of A containing the unit element 1, which is closed under addition and under multiplication with squares. In short, $1 \in Q, Q + Q \subseteq Q$, and $A^2Q \subseteq Q$ with $A^2 = \{x^2 \mid x \in A\}$. Such a set Q is called a *preordering* of A if, in addition, Q is closed under multiplication, $Q \cdot Q \subseteq Q$, in other words, if Q is a subsemiring of A containing A^2 . We do not exclude the case $-1 \in Q$ (“improper quadratic modules”), in contrast to much of the existing literature.

The ring A contains a smallest quadratic module, namely, the set ΣA^2 consisting of all sums of squares of elements of A . It is a preordering. On the other hand A itself is the biggest quadratic module in A .

If elements $g_1, \dots, g_r \in A$ are given, we denote the quadratic module generated by g_1, \dots, g_r , i.e. the unique smallest quadratic module containing these elements, by $QM(g_1, \dots, g_r)$. It consists of the elements $f = \sigma_0 + \sigma_1 g_1 + \dots + \sigma_r g_r$ with $\sigma_i \in \Sigma A^2$ for $0 \leq i \leq r$. There also exists a unique smallest preordering of A containing the elements g_i ($1 \leq i \leq r$). We denote it by $PO(g_1, \dots, g_r)$. It consists of the elements $h = \sum \sigma_\epsilon g_\epsilon$, where ϵ runs through the set $\{0, 1\}^r$, $\epsilon = (\epsilon_1, \dots, \epsilon_r)$, and $g_\epsilon = \prod_{i=1}^r g_i^{\epsilon_i}$, $\sigma_\epsilon \in \Sigma A^2$. In this notation we have $QM(1) = PO(1) = \Sigma A^2$.

If 2 is a unit in A , then $QM(-1) = PO(-1) = A$, since every $x \in A$ can be written as $x = \left(\frac{x+1}{2}\right)^2 + (-1)\left(\frac{x-1}{2}\right)^2$. Notice that more generally we have for any $g \in A$ that $QM(g) = PO(g)$. We call these quadratic modules *monogenic*.

Quadratic modules, and in particular preorderings, play a ubiquitous role in present day real algebra, cf. the books [PD], [M] and standard texts on real algebra from the eighties and nineties ([BCR], [KS], [L],...). We also mention a recent survey article by C. Scheiderer [S].

For many problems in real algebra and real algebraic geometry it seems to be crucial to have a good grasp of finitely generated preorderings, or even quadratic

Received by the editors July 15, 2008, and, in revised form, May 5, 2009.

2000 *Mathematics Subject Classification*. Primary 13J05, 13J30; Secondary 06F25.

Key words and phrases. Quadratic modules, preorderings, formal power series rings.

©2009 American Mathematical Society
Reverts to public domain 28 years from publication

modules, and to understand their relation to other preorderings or quadratic modules which are perhaps not finitely generated. For example, if $A = \mathbb{R}[X_1, \dots, X_n]$, the polynomial ring in n variables over the reals, and polynomials g_1, \dots, g_r are given, one wants to understand the relations between $PO(g_1, \dots, g_r)$, $QM(g_1, \dots, g_r)$ and the bigger preordering consisting of all polynomials which have nonnegative values on the semialgebraic set $\{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \dots, g_r(x) \geq 0\}$.

In this light, a classification of all finitely generated preorderings or even quadratic modules in $\mathbb{R}[X_1, \dots, X_n]$ is a very desirable goal. One of the present authors has obtained this for $n = 1$ in her recent thesis [A], building on much previous work of others. If $n \geq 2$, striving for a classification in a strong sense may well be elusive.

But there are even simpler cases which nevertheless deserve our interest. Let us first look at fields. A field R is called *euclidean* if R is formally real and for every $x \in R$ either x or $-x$ is a square. Now, such a field is too simple for our goals: $\{0\}$, R^2 , R are the only quadratic modules in R . On the other hand, in some sense the ring $R[X]$ in one variable X over a euclidean field R is already too difficult, since we cannot use Tarski's principle here. It works only if R is a real closed field.

But we have a good chance to classify all finitely generated quadratic modules in the ring $R[[X]]$ of formal power series in one variable X over a euclidean field R . This will be done in the present paper. (A less detailed description of these quadratic modules already appears in Chapter 9 of [M].)

The ring $R[[X]]$ for $R = \mathbb{R}$, or more generally R a real closed field, seems to be the simplest ring of interest in real algebra which is not a field. It is legitimate to look here for a classification of quadratic modules as explicit as possible, since $R[[X]]$ appears as an auxiliary ring in many real algebraic problems.

That we can admit a euclidean field R instead of a real closed field serves as a witness that methods from model theory, in particular Tarski's principle, are not yet needed. Everything will be completely elementary.

We thank the referee for a very careful reading of the manuscript.

2. MONOGENIC QUADRATIC MODULES

Let R be a euclidean field. R has a unique (total) ordering. Thus for every $x \in R$, $x \neq 0$, either $x > 0$ or $-x > 0$, and $x > 0$ if and only if x is a square. We consider the formal power series ring $A = R[[X]]$ in one variable X and study now the monogenic quadratic modules in A .

Notice that the R -algebra A admits an involution $\iota : A \rightarrow A$ which leaves the elements of R fixed and takes X to $-X$.

$R[[X]]$ is a local ring with maximal ideal $XR[[X]]$. For every $q \in XR[[X]]$ the element $1 + q$ is a unit and a square in $R[[X]]$, as the geometric series for $(1 + q)^{-1}$ and the binomial series for $(1 + q)^{\frac{1}{2}}$ show.

Remark 2.1. Every element $f = \sum_{i=0}^{\infty} c_i X^i \in R[[X]]$ different from zero can be written in the form $f = c_d X^d (1 + q)$ for some uniquely determined $d \in \mathbb{N}_0$, $c_d \neq 0$ and $q \in XR[[X]]$. Just let d be the minimal index $i \in \mathbb{N}_0$ for which $c_i \neq 0$. Then $f = c_d X^d \underbrace{\left(1 + \frac{c_{d+1}}{c_d} X + \dots\right)}_{=: 1+q}$.

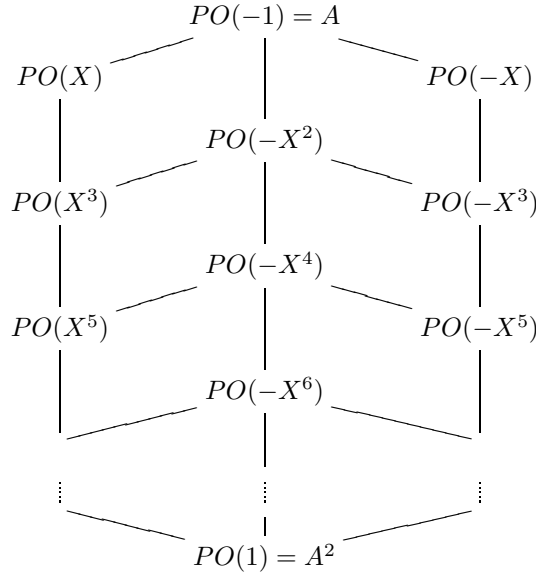
We denote the sign of c_d by $\epsilon(f)$. The number d itself is nothing else but the order of f , $d = \text{ord}(f)$.

Proposition 2.2. *Let $f \in A = R[[X]]$ be given, $f \neq 0$. The following are equivalent:*

- a) $f \in A^2$.
- b) $f \in \sum A^2$; i.e. f is a sum of squares in A .
- c) $\text{ord}(f)$ is even and $\epsilon(f) = 1$.

The proof is straightforward. Verify $a) \Rightarrow b) \Rightarrow c) \Rightarrow a)$. The main fact to be used is that every element in $1 + XA$ is a square.

Theorem 2.3. *The partially ordered set (via inclusion) of all monogenic quadratic modules in $A = R[[X]]$ has the following diagram (cf. first paragraph of Remark 2.6 below for explanations).*



Proof. Let $g \in R[[X]]$. By Remark 2.1 we have $g = cX^d(1+q)$ for some $d \in \mathbb{N}_0, c \neq 0$ in R , and $q \in XR[[X]]$. This implies that $PO(g) = PO(cX^d)$ because $1+q$ is a square and a unit in $R[[X]]$. This shows that all quadratic modules generated by one polynomial in $R[[X]]$ are of the form $PO(\pm 1 \cdot X^d)$ for some $d \in \mathbb{N}_0$.

As said in Section 1 the quadratic module generated by -1 is equal to $R[[X]]$.

The quadratic modules of the form $PO(X^{2k})$ for some $k \in \mathbb{N}_0$ are clearly equal to $\sum R[[X]]^2$, which by Proposition 2.2 is equal to $R[[X]]^2$.

For any $k \in \mathbb{N}_0$ it is easily verified that $X^{2k+1} \notin PO(X^{2k+3})$. Thus we have a chain of strict inclusions

$$PO(X) \supset PO(X^3) \supset PO(X^5) \supset \dots$$

Applying the involution ι we obtain a chain of strict inclusions

$$PO(-X) \supset PO(-X^3) \supset PO(-X^5) \supset \dots$$

For the study of the preorderings $PO(-X^{2k})$ we quote an easy general lemma which we will prove at the end of this section.

Lemma 2.4. *Let A be a commutative ring with $\frac{1}{2} \in A$ and $\sum A^2 = A^2$. Then for every $f \in A$*

$$PO(f) + PO(-f) = A^2 + Af$$

and

$$PO(-f^2) = A^2 + Af^2.$$

Returning to $A = R[[X]]$, we obtain by this lemma

$$(*) \quad PO(-X^{2k}) = A^2 + AX^{2k}.$$

It is now evident for $k \geq 1$ that $-X^{2k-2} \notin PO(-X^{2k})$, because every element $f \in PO(-X^{2k})$ with $\text{ord}(f) < 2k$ must have a positive leading coefficient. Thus we obtain the following chain of strict inclusions

$$A = PO(-1) \supset PO(-X^2) \supset PO(-X^4) \supset \dots$$

Terminology 2.5. We call these chains of preorderings the *left*, *central* and *right columns* of the diagram displayed above. We call $PO(-1)$ the *top* and $PO(1)$ the *bottom* of the diagram. Notice that the bottom is not a member of any column.

We continue with the proof of Theorem 2.3. The involution ι interchanges the left and the right columns, mapping $PO(X^{2k+1})$ to $PO(-X^{2k+1})$, and it fixes every member of the central column.

We examine the possible inclusions between members of the left and the right columns.

For arbitrary $k, l \in \mathbb{N}_0$ we have $X^{2k+1} \notin PO(-X^{2l+1})$. This will be proved by contradiction. Suppose that $X^{2k+1} = \sigma_0 + \sigma_1(-X^{2l+1})$ for some $\sigma_0, \sigma_1 \in R[[X]]^2$. Then by Remark 2.1 and Proposition 2.2, $\sigma_i = c_i X^{2k_i}(1+q_i)$ for some $k_i \in \mathbb{N}_0, c_i > 0$ and $q_i \in XR[[X]]$ ($i = 0, 1$). Thus

$$X^{2k+1} = c_0 X^{2k_0}(1+q_0) + (c_1 X^{2k_1}(1+q_1))(-X^{2l+1}).$$

The term of lowest degree on the right hand side has either even degree or odd degree, but then with negative coefficient, whereas the term on the left hand side has odd degree with positive coefficient 1. This is the desired contradiction.

Thus

$$PO(X^{2k+1}) \not\subseteq PO(-X^{2l+1})$$

for every $k, l \in \mathbb{N}_0$. Applying ι we see also that

$$PO(-X^{2k+1}) \not\subseteq PO(X^{2l+1}).$$

Regarding the inclusions between the left and the central columns we note that $X^{2k+1} \notin PO(-X^{2l})$ if $2k+1 < 2l$, due to the description (*) of $PO(-X^{2l})$ above.

However, if $2k+1 > 2l$, then $X^{2k+1} \in PO(-X^{2l})$ by Lemma 2.4; hence we have $PO(X^{2k+1}) \subseteq PO(-X^{2l})$. For the same reason $PO(-X^{2k+1}) \subseteq PO(-X^{2l})$.

No member Q of the central column can be contained in a member P of the left column, since, as we have just proved, Q contains members of the right column, but no member of the right column is contained in any member of the left column. Thus all inclusions from members of the left column in members of the central column are strict.

Due to the involution ι we now also know which inclusions hold between members of the right and the central columns. \square

Remark 2.6. The diagram in Theorem 2.3 gives complete information about all inclusion relations between the monogenic quadratic modules. Omitting the bottom A^2 , it should be viewed as a directed graph. Every edge is oriented “from south to north”. This is unambiguous, since no edge is horizontal. Given two different vertices P and Q we have $P \subseteq Q$ if and only if there exists a path from P to Q , always going north, and then $P \subset Q$.

In particular, if such a path meets the central column it will stay in this column up to its end. Thus a quadratic module in this column is not contained in a member of another column. On the other hand, a member of the left or right column does only contain members of the same column.

Proof of Lemma 2.4. We first verify that for every $f \in A$

$$PO(f) + PO(-f) = A^2 + Af.$$

For the inclusion \subseteq we note that the set on the right hand side is a preordering which contains f and $-f$. The inclusion \supseteq follows from

$$\left(\frac{u+v}{2}\right)^2 f + \left(\frac{u-v}{2}\right)^2 (-f) = uvf$$

for arbitrary $u, v \in A$.

Applying this to f^2 we obtain $PO(-f^2) = A^2 + Af^2$, since $PO(f^2) = A^2$ is contained in $PO(-f^2)$. \square

3. THE OTHER QUADRATIC MODULES

Let Q be a quadratic module in $A = R[[X]]$ with R a euclidean field, as before.

Definition 3.1. If Q contains a monogenic quadratic module from the left column in the diagram of Theorem 2.3, we denote the union of all these submodules by Q_l (read “ Q -left”). Otherwise we put $Q_l := A^2$. We call Q_l the *left component* of the quadratic module Q . In the same way we define the *central component* Q_c and the *right component* Q_r of Q .

Since in each column only finitely many members exist which contain a given quadratic module of the column and these form a chain, it is clear that Q_l is the unique maximal monogenic quadratic module from the left column contained in Q , provided $Q_l \neq A^2$. The same holds for Q_c and Q_r . The following is now evident.

Proposition 3.2.

- a) $Q = Q_l \cup Q_c \cup Q_r = Q_l + Q_c + Q_r$. In particular, every quadratic module in $R[[X]]$ is finitely generated, more precisely generated by at most three elements.
- b) If Q' is a second quadratic module in $R[[X]]$, then $Q \subset Q'$ if and only if $Q_l \subseteq Q'_l, Q_c \subseteq Q'_c, Q_r \subseteq Q'_r$, and at least one of these inclusions is strict.

Remark 3.3. The components of Q can also be described in the following numerical way. Let

$$\begin{aligned} k(Q) &:= \min\{\text{ord}(f) \mid f \in Q, \text{ord}(f) \text{ even}, \epsilon(f) = -1\}, \\ k^+(Q) &:= \min\{\text{ord}(f) \mid f \in Q, \text{ord}(f) \text{ odd}, \epsilon(f) = 1\}, \\ k^-(Q) &:= \min\{\text{ord}(f) \mid f \in Q, \text{ord}(f) \text{ odd}, \epsilon(f) = -1\}. \end{aligned}$$

If one of the sets on the right hand side is empty, read ∞ for the minimum.

Then

$$\begin{aligned} Q_c &= PO(-X^{k(Q)}), \\ Q_l &= PO(X^{k^+(Q)}), \\ Q_r &= PO(-X^{k^-(Q)}), \end{aligned}$$

provided $k(Q) \neq \infty, k^+(Q) \neq \infty, k^-(Q) \neq \infty$, respectively. If one of these numbers is ∞ , the corresponding component is A^2 .

Before we continue with quadratic modules that are not monogenic, we briefly look at the components in the monogenic case.

Scholium 3.4. Due to Theorem 2.3 we have the following list of components of the monogenic quadratic modules $\neq A^2$:

- 1) $Q = PO(X^{2l+1}) : Q_l = Q, \quad Q_c = A^2, \quad Q_r = A^2.$
- 2) $Q = PO(-X^{2l+1}) : Q_l = A^2, \quad Q_c = A^2, \quad Q_r = Q.$
- 3) $Q = PO(-X^{2n}) : Q_l = PO(X^{2n+1}), \quad Q_c = Q, \quad Q_r = PO(-X^{2n+1}).$

Theorem 3.5. *Every quadratic module Q in $R[[X]]$ is the sum of at most two monogenic submodules.*

Proof. We start with

$$Q = Q_l + Q_c + Q_r.$$

If $Q_r \subset Q_c$, we have $Q = Q_l + Q_c$. If $Q_l \subset Q_c$, we have $Q = Q_r + Q_c$.

Assume now that $Q_r \not\subset Q_c$ and $Q_l \not\subset Q_c$. The quadratic modules $\iota(Q_l)$ and Q_r are both in the right column, hence comparable.

Assume then that $\iota(Q_l) \supseteq Q_r$. By Theorem 2.3

$$Q_l = PO(X^{2p+1}), \quad Q_r = PO(-X^{2q+1}), \quad Q_c = PO(-X^{2n})$$

with $p \leq q$ and $2q + 1 < 2n$, i.e. $n > q$. Invoking Lemma 2.4 we see that

$$Q_l + Q_r \supseteq PO(X^{2q+1}) + PO(-X^{2q+1}) = A^2 + AX^{2q+1}.$$

Thus $-X^{2n} \in Q_l + Q_r$; hence $Q = Q_l + Q_r$.

The proof of the other case, i.e. $\iota(Q_r) \supseteq Q_l$, is analogous. \square

From these considerations the following is now obvious.

Corollary 3.6. *Every quadratic module Q in $R[[X]]$ which is not monogenic is one of the following three types:*

- (1) $Q^{LC}(l, n) := PO(X^{2l+1}) + PO(-X^{2n})$ with $l, n \in \mathbb{N}_0, l < n.$
- (2) $Q^{RC}(l, n) := PO(-X^{2l+1}) + PO(-X^{2n})$ with $l, n \in \mathbb{N}_0, l < n.$
- (3) $Q^{LR}(l, m) := PO(X^{2l+1}) + PO(-X^{2m+1})$ with $l, m \in \mathbb{N}_0.$

We refer to the three types in Corollary 3.6 as the *left-central*, the *right-central* and the *left-right types*.

In all three cases we want to determine the components of Q . We start with the left-right type.

Theorem 3.7. *Assume that $Q = PO(X^{2l+1}) + PO(-X^{2m+1})$ with $l, m \in \mathbb{N}_0$. Let $n := \max(l, m) + 1$. Then*

$$\begin{aligned} Q_l &= PO(X^{2l+1}), \\ Q_r &= PO(-X^{2m+1}), \\ Q_c &= PO(-X^{2n}). \end{aligned}$$

In particular the numbers l and m are uniquely determined by Q , namely,

$$2l + 1 = k^+(Q), \quad 2m + 1 = k^-(Q).$$

Q is not the union of two monogenic quadratic modules.

Proof. Due to the automorphism $\iota : X \mapsto -X$ we assume without loss of generality that $l \leq m$. Then we have $n = m + 1$. Of course, $PO(X^{2l+1}) \subseteq Q_l$ and $PO(-X^{2m+1}) \subseteq Q_r$. By Lemma 2.4 the module

$$A^2 + AX^{2m+1} = PO(X^{2m+1}) + PO(-X^{2m+1})$$

is contained in Q , and thus

$$PO(-X^{2n}) = PO(-X^{2m+2}) \subseteq Q_c.$$

We have to verify that $X^{2l-1} \notin Q$, $-X^{2m-1} \notin Q$, $-X^{2m} \notin Q$.

a) The case $l = m$.

Now $Q = A^2 + AX^{2l+1}$.

Suppose that $X^{2l-1} \in Q$, in particular $l \geq 1$. Then $X^{2l-1} = s_0^2 + aX^{2l+1}$ for some $s_0, a \in A$, and therefore

$$s_0^2 = X^{2l-1} - aX^{2l+1}.$$

But this is impossible since the right hand side has the odd order $2l - 1$. Thus $X^{2l-1} \notin Q$. Applying the automorphism ι we obtain also $-X^{2l-1} \notin Q$.

Suppose that $-X^{2l} \in Q$. Then $-X^{2l} = s_0^2 + aX^{2l+1}$ for some $s_0, a \in A$, and therefore

$$s_0^2 + X^{2l} = -aX^{2l+1}.$$

This is a contradiction because the order of the left hand side is $\leq 2l$, whereas the order of the right hand side is greater than or equal to $2l + 1$. Thus $-X^{2l} \notin Q$.

b) The case $l < m$.

Suppose $X^{2l-1} \in Q$, in particular $l \geq 1$. Then $X^{2l-1} = s_0^2 + s_1^2 X^{2l+1} + aX^{2m+1}$ for some $s_0, s_1, a \in A$; hence

$$s_0^2 = X^{2l-1} - s_1^2 X^{2l+1} - aX^{2m+1}.$$

This is impossible because the order of the right hand side is $2l - 1$ and the order of the left hand side is even. Thus $X^{2l-1} \notin Q$.

Suppose that $-X^{2m-1} \in Q$. Then $-X^{2m-1} = s_0^2 + s_1^2 X^{2l+1} + aX^{2m+1}$ for some $s_0, s_1, a \in A$. Thus

$$-s_0^2 = (X^{2m-1} + aX^{2m+1}) + s_1^2 X^{2l+1}.$$

The order of the right hand side is the minimum of $2l + 1 + 2 \text{ord}(s_1)$ and $2m - 1$, hence is an odd number, while the order of the left hand side is even, a contradiction. We conclude that $-X^{2m-1} \notin Q$.

Finally suppose that $-X^{2m} \in Q$. Then $-X^{2m} = s_0^2 + s_1^2 X^{2l+1} + aX^{2m+1}$; hence

$$-(X^{2m} + s_0^2) = s_1^2 X^{2l+1} + aX^{2m+1}$$

for some $s_0, s_1, a \in A$. In this expression the order of the left hand side is equal to the even number $2 \min(m, \text{ord}(s_0))$.

If $\text{ord}(s_1^2 X^{2l+1}) < 2m + 1$, then the order of the right hand side is odd, a contradiction.

If $\text{ord}(s_1^2 X^{2l+1}) \geq 2m + 1$, then the order of the right hand side is greater than or equal to $2m + 1$, while the order of the left hand side is at most $2m$, again a contradiction. Hence $-X^{2m} \notin Q$.

It is now clear from Theorem 2.3 that Q is not the union of two monogenic quadratic modules. \square

We now deal with the left-central type.

Theorem 3.8. *Let $Q = PO(X^{2l+1}) + PO(-X^{2n})$ for some $l, n \in \mathbb{N}_0$ with $l < n$. Then*

$$\begin{aligned} Q_l &= PO(X^{2l+1}), \\ Q_c &= PO(-X^{2n}), \\ Q_r &= PO(-X^{2n+1}). \end{aligned}$$

In particular, the numbers l and n are uniquely determined by Q , namely,

$$2l + 1 = k^+(Q), \quad 2n = k(Q).$$

Notice also that $Q_r \subset Q_c$; hence $Q = Q_l \cup Q_c$.

Proof. Of course $PO(X^{2l+1}) \subseteq Q_l$ and $PO(-X^{2n}) \subseteq Q_c$. By Theorem 2.3 we know that

$$PO(-X^{2n+1}) \subset PO(-X^{2n}) \subseteq Q.$$

Thus $PO(-X^{2n+1}) \subseteq Q_r$. We are done if we have verified the following:

- (1) $X^{2l-1} \notin Q$ if $l \geq 1$,
- (2) $-X^{2n-1} \notin Q$,
- (3) $-X^{2n-2} \notin Q$.

The diagram in Theorem 2.3 tells us that $PO(-X^{2n-1}) \subset PO(-X^{2n-2})$. Thus it suffices to verify (1) and (2).

By Lemma 2.4 we have $PO(-X^{2n}) = A^2 + AX^{2n}$; hence

$$Q = PO(X^{2l+1}) + AX^{2n}.$$

(1): Suppose that

$$X^{2l-1} = s_0^2 + s_1^2 X^{2l+1} + aX^{2n}$$

for some $s_0, s_1, a \in A$. Then it follows that the order of $s_0^2 + s_1^2 X^{2l+1}$ is equal to $2l - 1$; hence $\text{ord}(s_0^2) = 2l - 1$, a contradiction. This proves that $X^{2l-1} \notin Q$.

(2): Suppose that $-X^{2n-1} = s_0^2 + s_1^2 X^{2l+1} + aX^{2n}$, i.e.

$$-X^{2n-1} - s_1^2 X^{2l+1} = s_0^2 + aX^{2n}$$

for some $s_0, s_1, a \in A$. Both terms on the left hand side have a negative leading coefficient. Hence the order of the left hand side is equal to $\min(2n-1, 2l+1) = 2l+1$ because $2l+1 < 2n$. Thus $\text{ord}(s_0^2) = 2l+1$, which is a contradiction.

We conclude that $-X^{2n-1} \notin Q$, and the theorem is proved. \square

Applying the automorphism $\iota : X \mapsto -X$ we obtain

Corollary 3.9. *Let $Q = PO(-X^{2l+1}) + PO(-X^{2n})$ for some $l, n \in \mathbb{N}_0$ with $l < n$. Then*

$$\begin{aligned} Q_l &= PO(X^{2n+1}), \\ Q_c &= PO(-X^{2n}), \\ Q_r &= PO(-X^{2l+1}). \end{aligned}$$

In particular, the numbers l and n are uniquely determined by Q , namely,

$$2l + 1 = k^-(Q), \quad 2n = k(Q).$$

Also $Q = Q_c \cup Q_r$.

From Scholium 3.4, Theorems 3.7 and 3.8, and Corollary 3.9 we read off that all the quadratic modules in the list in Corollary 3.6 are different and not monogenic.

4. SOME CONSEQUENCES

Theorem 4.1. *Every quadratic module Q of $A = R[[X]]$ is a preordering.*

Proof. Also see [M], 9.3.2. If Q is generated by one polynomial, then Q is clearly multiplicatively closed. Because of Corollary 3.6 and the automorphism $X \mapsto -X$ of A we just have to consider the following two cases.

Case 1. $Q = PO(X^{2l+1}) + PO(-X^{2m+1})$ for some $l, m \in \mathbb{N}_0$, where without loss of generality $l \leq m$. Then

$$X^{2l+1} \cdot (-X^{2m+1}) \in A^2 + AX^{2m+1} \stackrel{2.4}{=} PO(X^{2m+1}) + PO(-X^{2m+1}) \subseteq Q.$$

Case 2. $Q = PO(X^{2l+1}) + PO(-X^{2n})$ for some $l, n \in \mathbb{N}_0$ with $l < n$. Then

$$X^{2l+1} \cdot (-X^{2n}) \in A^2 + AX^{2n} \stackrel{2.4}{=} PO(-X^{2n}) \subseteq Q. \quad \square$$

If Q_1 and Q_2 are quadratic modules in a ring A , let $\sum Q_1 Q_2$ denote the set of finite sums of elements ab with $a \in Q_1, b \in Q_2$. This is the smallest quadratic module in A containing Q_1 and Q_2 .

Corollary 4.2. *If Q_1, Q_2 are quadratic modules of $A = R[[X]]$, then*

$$\sum Q_1 Q_2 = Q_1 + Q_2.$$

Proof. We always have $Q_1 + Q_2 \subseteq \sum Q_1 Q_2$. Now $Q_1 + Q_2$ is already a quadratic module containing Q_1 and Q_2 . Thus $Q_1 + Q_2 = \sum Q_1 Q_2$. \square

Theorem 4.3. *If Q_1 and Q_2 are two monogenic quadratic modules of $A = R[[X]]$, then $Q_1 \cap Q_2$ is again a monogenic quadratic module.*

Proof. There is nothing to prove if Q_1 or Q_2 is the bottom or the top of the list of quadratic modules in Theorem 2.3. Clearly the claim is also true if Q_1 and Q_2 are both in the same column in Theorem 2.3. Taking into account the automorphism $\iota : X \mapsto -X$, we find that only two cases remain.

Case 1. $Q_1 = PO(X^{2l+1}), Q_2 = PO(-X^{2m+1})$ for some $l, m \in \mathbb{N}_0$.

Let Q be a monogenic quadratic module which is a subset of $Q_1 \cap Q_2$. According to Theorem 2.3 Q cannot be one of the quadratic modules from the central column. It also cannot be one of the quadratic modules from the left or the right column. Thus $Q = A^2$. It follows that $Q_1 \cap Q_2 = A^2$.

Case 2. $Q_1 = PO(X^{2l+1}), Q_2 = PO(-X^{2n})$ for some $l \in \mathbb{N}_0$ and $n \in \mathbb{N}$.

Let $N := \max(l, n)$. Then $X^{2N+1} \in Q_1 \cap Q_2$. Let Q be a maximal monogenic quadratic module contained in $Q_1 \cap Q_2$. Q has to be one of the quadratic modules of the left column from Theorem 2.3. By Theorem 2.3 it is clear that $Q_1 \cap Q_2 = PO(X^{2N+1})$. \square

We finally mention that Section 3 implies a solution of the *Membership Problem for quadratic modules* in $A = R[[X]]$. By this we mean the following. Given $f, g_1, \dots, g_r \in A$, decide by an algorithm whether f is an element of the quadratic module $Q := QM(g_1, \dots, g_r)$ or not.

We indicate how this can be done with the considerations from the preceding sections. The membership of f is determined by the numbers $k(Q), k^+(Q)$ and

$k^-(Q)$. Indeed, if $\text{ord}(f)$ is odd and $\epsilon(f) = 1$, then $f \in Q$ if and only if $\text{ord}(f) \geq k^+(Q)$, etc.

Thus we only have to determine these numbers, i.e. the components of Q . First we replace each g_i by an element $\pm X^{n_i}$ using Remark 2.1 and Proposition 2.2. If g_i is a square, we omit g_i . Otherwise $PO(g_i)$ belongs to one of the three columns in Theorem 2.3. Retaining only the elements g_i with $PO(g_i)$ maximal in the set $\{PO(g_1), \dots, PO(g_r)\}$, we have $Q = A^2$, or $Q = Q_1$, or $Q = Q_1 + Q_2$, or $Q = Q_1 + Q_2 + Q_3$, with the Q_i monogenic and in different columns.

The first two cases are trivial. In the third case we get the components directly from Theorems 3.7 and 3.8 and Corollary 3.9. In the last case we have, up to numeration, $Q_i = PO(h_i)$ with $h_1 = X^{2l+1}, h_2 = -X^{2n}, h_3 = -X^{2m+1}$. If $l \geq n$, then we can omit h_1 , and if $m \geq n$, then we can omit h_3 , and so arrive at the third case. Now suppose that $l < n$ and $m < n$. By Theorem 3.8 we know that $Q_1 + Q_2 = Q_1 \cup Q_2$; hence $Q = (Q_1 + Q_3) \cup (Q_2 + Q_3)$. Using Theorems 3.7 and 3.8 we write $Q_1 + Q_3$ as a union of three and $Q_2 + Q_3$ as a union of two monogenic quadratic modules. Then we can read off the components of Q , i.e. the numbers $k(Q), k^+(Q)$ and $k^-(Q)$.

REFERENCES

- [A] D. Augustin, *The membership problem for quadratic modules with focus on the one dimensional case*, Doctoral Dissertation, Universität Regensburg, 2008.
- [BCR] J. Bochnak, M. Coste and M.-F. Roy, *Real algebraic geometry*, Springer, Berlin, 1998. MR1659509 (2000a:14067)
- [KS] M. Knebusch and C. Scheiderer, *Einführung in die reelle Algebra*, Vieweg, Braunschweig, 1989. MR1029278 (90m:12005)
- [L] T. Y. Lam, *An introduction to real algebra*, Rocky Mtn. J. Math. 14 (1984) 767-814. MR773114 (86g:12013)
- [M] M. Marshall, *Positive polynomials and sums of squares*, Math. Surveys and Monographs, 146, Amer. Math. Soc., Providence, RI, 2008. MR2383959 (2009a:13044)
- [PD] A. Prestel and C. N. Delzell, *Positive polynomials - from Hilbert's 17th problem to real algebra*, Springer-Verlag, Berlin, 2001. MR1829790 (2002k:13044)
- [S] C. Scheiderer, *Positivity and sums of squares: A guide to recent results*, in: *Emerging Applications of Algebraic Geometry* (M. Putinar, S. Sullivant, eds.), IMA Volumes Math. Appl., 149, Springer, 2009, pp. 271-324.

UNIVERSITÄT REGENSBURG, NWF I - MATHEMATIK, D-93040 REGENSBURG, GERMANY
E-mail address: `doris.augustin@mathematik.uni-regensburg.de`

UNIVERSITÄT REGENSBURG, NWF I - MATHEMATIK, D-93040 REGENSBURG, GERMANY
E-mail address: `manfred.knebusch@mathematik.uni-regensburg.de`