On the degree complexity of Hilbert's 17th problem and the Real Nullstellensatz

HABILITATIONSSCHRIFT

zur Erlangung der Lehrbefugnis
für das Fach Mathematik
an der Universität Dortmund

von
Joachim Schmid

Mai 1998

Table of contents

Introduction

Complexity issues concerning polynomial ideals were first considered by Hermann [18] in 1926. If $f, f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ is a system of polynomials over an arbitrary field k such that f vanishes in all common zeroes of the polynomials $f_1, \ldots, f_m$ then, by Hilbert's Nullstellensatz, there are $t \in \mathbb{N}$ and $q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that

$$f^t = \sum_{i=1}^{m} q_i f_i \tag{1}$$

Unfortunately the classical proof of Hilbert's Nullstellensatz gives no further information about the polynomials $q_1, \ldots, q_m$ and their degrees. Using elimination theory Hermann proved that the exponent t and the degrees of the polynomials $q_1, \ldots, q_m$ can be bounded by a double exponential function in n and the degrees of $f, f_1, \ldots, f_m$. Several authors tried to improve her bounds but for more than 60 years only little progress was made. Then using analytic tools Brownawell [8] gave the first single exponential bound in the case $k = \mathbb{C}$, and Kollár [23] proved in 1988 that if d is an upper bound for the degrees of $f_1, \ldots, f_m$ then one always can obtain bounds $t \leq d^n$ and $\deg(q_i f_i) \leq d^n \cdot (1 + \deg f)$, independent of the field k. Furthermore he gave an example which shows that d^n is also a worst-case lower bound for the exponent t.

If k is a formally real field (i.e. -1 is not a sum of squares in k) and $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$, then the set of real zeroes of $f_1, \ldots, f_m$ is

$$\mathrm{V_r}(f_1, \ldots, f_m) := \{(x_1, \ldots, x_n) \in \mathrm{V}(f_1, \ldots, f_m) \mid k(x_1, \ldots, x_n) \text{ is formally real}\}$$

One of the first basic theorems in real algebraic geometry is the so-called "Real Nullstellensatz" which was proven independently by Dubois [15], Krivine [24] and Risler [38]. It states that a polynomial $f \in k[X_1, \ldots, X_n]$ vanishes on $\mathrm{V_r}(f_1, \ldots, f_m)$ iff there is an equation of the form

$$f^{2t} + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} q_i f_i \tag{2}$$

for certain $r, t \in \mathbb{N}, q_1, \ldots, q_m, h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$.

In contrast to the case of Hilbert' Nullstellensatz only little is known about degree bounds for the Real Nullstellensatz. Using the Hörmander tableaux method for the elimination of quantifiers for real closed fields Lombardi [30] proved that if $\mathrm{V_r}(f_1, \ldots, f_m) = \emptyset$ and $\deg f_i \leq d$ then there is an equation

$$1 + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} q_i f_i \tag{3}$$

for certain $r \in \mathbb{N}, h_1, \ldots, h_r, q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that r and the degrees of the polynomials h_i, q_i can be bounded by

$$2^{2^{\cdot^{\cdot^{\cdot^{2^{P(n,d)}}}}}}$$

where P is a polynomial and the tower has length $n + 4$. Recently Lombardi and Roy announced that they are able to reduce the length of this tower to 5, independent of n. However, at this moment their result is not published.

One of the main problems seems to find the relevant parameters which the degrees really depend on. A possible parameter is the dimension of the ideal $(f_1, \ldots, f_m)$. In [41] it is shown that in the case $\dim(f_1, \ldots, f_m) = 0$ one can obtain $\deg(q_i f_i) \leq d^n(d^n + 1)$ in equation (3).

It is one of the aims of this work to extend the results of [41] and to determine the influence of the dimension of the ideal $(f_1, \ldots, f_m)$ on the degree bounds for the Real Nullstellensatz. The source for our degree estimates are degree bounds for another problem from real algebra, namely Hilbert's 17th problem:

Given a polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ which is positive semidefinite, i.e. $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Is f a sum of squares of rational functions ?

This is one of the famous 23 problems which were raised by Hilbert in 1900 at the international congress of mathematicians at Paris. Hilbert already knew that the answer to this problem is yes if $n = 1$ or $n = 2$ (cf. [20]) and that a positive semidefinite polynomial is not necessarily a sum of squares of polynomials unless $n = 1$ (cf. [19]). The most prominent example of such a polynomial is due to Motzkin (cf. [31]):

$$f(X_1, X_2) = 1 + X_1^4 X_2^2 + X_1^2 X_2^4 - 3X_1^2 X_2^2$$

An affirmative answer for arbitrary n was given by Artin in 1927 (cf. [2]). The methods he used were developed in the joint paper [3] with Schreier which together with [1] and [4] form the starting point of what nowadays is called real algebra.

A model theoretic proof for Artin's result goes as follows. Assume that $f \in \mathbb{R}[X_1, \ldots, X_n]$ is positive semidefinite but not a sum of squares in $K := \mathbb{R}(X_1, \ldots, X_n)$. Then by a theorem of Artin and Schreier from [3] there is an ordering $\leq$ of K such that $f < 0$. Hence in the real closure $\overline{(K, \leq)}$ of K w.r.t. $\leq$ holds:

$$\overline{(K, \leq)} \models \exists x_1, \ldots, x_n \; f(x_1, \ldots, x_n) < 0$$

Now model completeness of the theory of real closed fields (cf. [37], Satz 4.7) yields

$$(\mathbb{R}, \leq) \models \exists x_1, \ldots, x_n \; f(x_1, \ldots, x_n) < 0$$

and thus f would not be positive semidefinite.

Although model theory and its tools and methods did not exist at that time, Artin's original proof has some model theoretic flavour. He is working with "properties" and their "specializabilty" rather than with polynomials, and certain authors consider Artin's proof as the beginning of model theory.

Artin just proves that a positive semidefinite polynomial f is positive w.r.t. every ordering of $\mathbb{R}(X_1, \ldots, X_n)$ and thus it is a sum of squares. The proof yields no information how to obtain a representation of the form

$$f = \sum_{i=1}^{r} \left(\frac{g_i}{h_i} \right)^2 \tag{4}$$

for certain $g_1, \ldots, g_r, h_1, \ldots, h_r \in \mathbb{R}[X_1, \ldots, X_n]$, neither it gives bounds for the number r of summands and the degrees of $g_1, \ldots, g_r, h_1, \ldots, h_r$.

In the fifties Kreisel noticed that by means of proof theory, in particular by the use of Hilbert's ε-elimination theorems, it should be possible to "unwind" non-constructive existence proofs in mathematics in order to obtain constructive ones. In the case of Artin's non-constructive solution of Hilbert's 17th problem the details were worked out by Daykin in his thesis [12] in 1961. Daykin proved that for a positive semidefinite polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ a representation of the form (4) can be obtained by a primitive recursive procedure, and as a by-product he obtained an effective bound on the number r. Daykin's thesis was never published but a readable account of Kreisel's unwinding method can be found in [13]. Also certain attempts to obtain bounds on r and the occurring degrees are mentioned there.

The best known bound for r was given by Pfister (cf. [34]) in 1967. By means of quadratic form theory he proved that a rational function $f \in \mathbb{R}(X_1, \ldots, X_n)$ which is a sum of squares in $\mathbb{R}(X_1, \ldots, X_n)$ is already a sum of 2^n squares in $\mathbb{R}(X_1, \ldots, X_n)$. Three years before Cassels [10] had given the worst-case lower bound $n + 1$ for r.

The best known bound for the degrees of the polynomials occurring in (4) is 5-fold exponential in n and the degree of f and arises from the unpublished 5-fold exponential bound for the Real Nullstellensatz which was announced by Lombardi and Roy.

One of the aims of this work is to present degree bounds for a slight generalization of Hilbert's 17th problem. If k is an arbitrary formally real field and $f \in k[X_1, \ldots, X_n]$ a polynomial which is positive semidefinite in each real closure of k, then it is well-known that f is of the form

$$f = \sum_{i=1}^{r} \left(\frac{g_i}{h_i} \right)^2$$

for certain $g_1, \ldots, g_r, h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$. Clearing the denominators we get

$$h^2 \cdot f = \sum_{i=1}^{r} f_i^2$$

for certain $h, f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$. We will give an n-fold exponential bound on the degrees of the polynomials $f_1, \ldots, f_r$. For $n \leq 4$ this improves the bounds of Lombardi and Roy.

Now we give a rough outline of our approach. In a first stage we just present the algebraic machinery and omit all quantitative considerations concerning degree bounds. We will combine some ideas from [12] with methods from quadratic form theory and valuation theory.

We start with a fixed formally real field k and a polynomial $f \in k[X_1, \ldots, X_n]$ which is positive semidefinite in each real closure of k. We may assume that f is squarefree. Now we consider f as a univariate polynomial in the variable X_n over the field $K := k(X_1, \ldots, X_{n-1})$. An easy argument shows that f is positive definite in each real closure of K. Let $A = K[X_n]/(f)$. The symmetric K-bilinear form

$$\begin{aligned} s : A \times A &\longrightarrow K \\ (x, y) &\mapsto \operatorname{tr}_{A/K}(x \cdot y) \end{aligned}$$

induces a non-degenerate quadratic form q and by a classical result of Sylvester and Hermite

$$\operatorname{sign}_P(q) = \# \left\{ z \in \overline{(K, P)} \;\middle|\; f(z) = 0 \right\}$$

for every ordering P of K. Since f is positive definite in each real closure this yields that $\operatorname{sign}_P(q) = 0$ for every ordering P of K. Hence, by a theorem of Pfister, the form q is weakly hyperbolic over K, i.e., there are $s, t \in \mathbb{N}$ such that

$$s \times q \cong_K t \times < 1, -1 > \tag{5}$$

Now we extend an idea of Daykin. We consider all extensions E of K such that f splits over E in the form

$$f = c \cdot \prod_{i=1}^{\ell} (X_n - \alpha_i) \cdot \prod_{i=1}^{m} ((X_n - \beta_i)^2 + {\gamma_i}^2) \tag{6}$$

for certain $c \in K, \alpha_1, \ldots, \alpha_\ell, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m \in E$ and such that E is minimal with this property, i.e. $E = K(\alpha_1, \ldots, \alpha_\ell, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m)$. The numbers ℓ and m may depend on E. Such a field we will call a semi-splitting field of f over K. Over such a semi-splitting field we will obtain

$$q \cong_E \ell\times < 1 > \oplus\, m\times < 1, -1 > \tag{7}$$

Together with (5) this yields

$$t\times < 1, -1 > \ \cong_E s\ell\times < 1 > \oplus\, sm\times < 1, -1 > \tag{8}$$

Comparing the dimension of the forms we get $2t = s\ell + 2sm$ and thus $s\ell$ is even and $N := t - sm = \frac{1}{2}s\ell$. If $\ell > 0$ then Witt's cancellation theorem applied to (8) yields

$$N\times < -1 > \ \cong_E N\times < 1 >$$

and thus -1 is a sum of squares in E. If $\ell = 0$ then one concludes immediately from (6) that f is a sum of squares in $E[X_n]$. Note that c is a sum of squares in K since f is positive definite in each real closure of K. In any case, the quadratic form $< 1, -f >$ is weakly isotropic over $E(X_n)$.

In the final step we now glue together the weak isotropy of the form $< 1, -f >$ over all the fields $E(X_n)$ in order to obtain weak isotropy of $< 1, -f >$ over $K(X_n) = k(X_1, \ldots, X_n)$.

The splitting field F of f over K is a finite Galois extension of K. We choose a 2-Sylow subgroup H of $\mathrm{Gal}(F/K)$ and denote its fixed field by L. Then L/K is a finite separable extension of odd degree and F/L is a 2-extension. Thus L/K is simple, say $L = K(z)$ and there is a tower of successive quadratic extensions

$$K(z) = L \subsetneq L(\sqrt{z_1}) \subsetneq \ldots \subsetneq L(\sqrt{z_1}, \ldots, \sqrt{z_{p-1}}) \subsetneq L(\sqrt{z_1}, \ldots, \sqrt{z_p}) = F \tag{9}$$

with $z_1 \in L, z_2 \in L(\sqrt{z_1}), \ldots, z_p \in L(\sqrt{z_1}, \ldots, \sqrt{z_{p-1}})$. For every p-tuple $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_p) \in \{1, -1\}^p$ we let

$$E_\varepsilon = L(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_p z_p})$$

Then $F = E_\varepsilon$ with $\varepsilon = (1, \ldots, 1)$. Furthermore it will turn out that each of the fields E_ε contains a semi-splitting field E of f over K. To each of the fields E_ε there corresponds also a tower of field extensions, namely

$$L \subset L(\sqrt{\varepsilon_1 z_1}) \subset \ldots \subset L(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_{p-1} z_{p-1}}) \subset L(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_p z_p}) = E_\varepsilon$$

However, this is not necessarily a tower of successive quadratic extensions, e.g. $z_2 \in L(\sqrt{z_1})$ but not necessarily $z_2 \in L(\sqrt{-z_1})$. Then, in general $L(\sqrt{-z_1}, \sqrt{z_2})/L(\sqrt{-z_1})$ will be an extension of degree 4.

Now fix $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_p)$ and suppose that $z_p \in E'_\varepsilon := L(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_{p-1} z_{p-1}})$. Both fields $E'_\varepsilon(\sqrt{z_p})$ and $E'_\varepsilon(\sqrt{-z_p})$ contain a semi-splitting field of f over K. Therefore the quadratic form $< 1, -f >$ is weakly isotropic over the fields $E'_\varepsilon(\sqrt{z_p})(X_n)$ and $E'_\varepsilon(\sqrt{-z_p})(X_n)$ and quadratic form theory yields that $< 1, -f >$ is also weakly isotropic over the field $E'_\varepsilon(X_n)$. If $z_p \notin E'_\varepsilon$ there occur some technical difficulties. For this reason we will introduce the notion of a semi-extension of a field which enables us to treat the problem in a more conceptual way.

Nevertheless we finally obtain that $< 1, -f >$ is weakly isotropic over $L(X_n)$. Since L/K is an extension of odd degree, Springer's Theorem then yields that $< 1, -f >$ is also weakly isotropic over $K(X_n) = k(X_1, \dots, X_n)$. Hence there are $g_1, \dots, g_r, h_1, \dots, h_r \in k(X_1, \dots, X_n)$ such that not all of them are zero and

$$\sum_{i=1}^{r} g_i^2 - f \sum_{i=1}^{r} h_i^2 = 0 \tag{10}$$

After clearing the denominators we may assume that $g_1, \dots, g_r, h_1, \dots, h_r \in k[X_1, \dots, X_n]$. Since k is formally real this immediately implies that $\sum_{i=1}^r g_i^2 \neq 0$ and also $\sum_{i=1}^r h_i^2 \neq 0$. If we let $h := \sum_{i=1}^r h_i^2$ then

$$h^2 f = \sum_{i=1}^{r} \sum_{j=1}^{r} (g_i h_j)^2 \tag{11}$$

and hence f is sum of squares in $k(X_1, \dots, X_n)$.

In order to obtain degree bounds for the polynomials $g_1, \dots, g_r, h_1, \dots, h_r$ occurring in equation (11) the whole construction has to be carried out in an effective or quantitative way, in particular:

A) *The isometry $s \times q \cong_K t \times < 1, -1 >$ from (5) is needed effectively.*

B) *For each semi-splitting field E of f the isometry $q \cong_E \ell \times < 1 > \oplus\, m \times < 1, -1 >$ from (7) and the weak isotropy of $< 1, -f >$ over $E(X_n)$ is needed effectively.*

C) *The weak isotropy of $< 1, -f >$ over $K(X_n)$ has to be obtained in an effective way from the weak isotropy of $< 1, -f >$ over the rational function fields $E(X_n)$ of all the semi-splitting fields of f over K.*

In detail:

ad A) In this case effective means that the isometry has to be expressed in form of a matrix equation over $K = k(X_1, \dots, X_{n-1})$. The occurring degrees in this equation and the numbers s, t have to be bounded. However, this is a problem concerning only $n-1$ variables and it will turn out that one can reduce it to the problem of finding degree bounds for Hilbert's 17th problem in the case of $n-1$ variables.

ad B) For each semi-splitting field E of f the isometry in (7) also can be expressed in form of a matrix equation. However, the entries of the matrices are polynomial expressions in $\alpha_1, \dots, \alpha_\ell, \beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_m$ from (6), and thus the entries are elements from E and not polynomials or rational functions. Thus we need a measure for the size of the elements of the semi-splitting field E or even for the elements of the algebraic closure $\bar{K}$ of K. In the case of a polynomial this measure should coincide with the degree. Valuation theory will provide us with such a measure. By $v(g/h) = \deg h - \deg g$ a valuation $v : k(X_1, \ldots, X_{n-1}) \longrightarrow \mathbb{Z} \cup \{\infty\}$ is defined. Then we extend v to a valuation $v : \bar{K} \longrightarrow \mathbb{Q} \cup \{\infty\}$. The values $v(\alpha_i), v(\beta_i), v(\gamma_i)$ can be bounded by certain data from f. This finally yields bounds for the values of the entries in the matrices describing the isometries (7) and also for the values of the coordinates of the isotropic vectors of a multiple of $< 1, -f >$. However, it is not sufficient to consider only one extension of v to $\bar{K}$, we need all of them. In order to avoid working with infinitely many valuations we will introduce the concept of a degree function.

ad C) In order to carry out this step, for our approach it will be necessary to split the Galois extension F/K in an effective way in a 2-Sylow subfield and a tower of successive quadratic extensions, i.e., we need bounds for the values of the elements $z, z_1, \ldots, z_p$ of (9) under the considered degree function. Since the behaviour of quadratic forms under quadratic extensions and extensions of odd degree is well-known and can be handled by symbolic manipulations, the bounds for the values of the entries of isotropic vectors of multiples of $< 1, -f >$ over the fields $E(X_n)$ then yield bounds for the values of the entries of an isotropic vector over $K(X_n)$ of a multiple of $< 1, -f >$. Therefore we finally obtain equation (10) and bounds for the values of $g_1, \ldots, g_r, h_1, \ldots, h_r \in k(X_1, \ldots, X_n)$ under the degree function.

As the usual degree and the chosen degree function coincide on $k[X_1, \ldots, X_n]$, this would yield the desired degree bounds in the case that $g_1, \ldots, g_r, h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$. In the case that the leading coefficient c of f is an element of k, $\alpha_1, \ldots, \alpha_\ell, \beta_1, \ldots, \beta_m$ and $\gamma_1, \ldots, \gamma_m$ are integral over $k[X_1, \ldots, X_n]$. Our construction then will show that also $g_1, \ldots, g_r, h_1, \ldots, h_r$ are integral over $k[X_1, \ldots, X_n]$, and thus $g_1, \ldots, g_r, h_1, \ldots, h_r$ are polynomials. However, after an affine transformation one always may assume that $c \in k$. Since an affine transformation does not effect degrees, this finally yields our degree bounds.

This work contains 11 chapters. In the first chapter we introduce the basic notations. In particular, we give the definitions for the functions H_k and N_k which describe the degree bounds for Hilbert's 17th problem and the Real Nullstellensatz for a fixed field k, and we prove a first relation between H_k and N_k.

The chapters 2 and 3 are devoted to the study of degree functions and their properties.

The fourth chapter is of preparatory character for the fifth chapter and it is concerned with the so-called Shape Lemma. We will prove bounds w.r.t. degree functions for the coefficients of the polynomials occurring in the Shape Lemma.

In chapter 5 we prove a recursion formula for N_k in which also H_k is involved. Together with the results of chapter 1 this shows that each of the functions H_k and N_k can be expressed in terms of the other one.

In chapter 6 we introduce semi-splitting fields of polynomials and study their properties.

The chapters 7 and 8 contain the crucial part of our approach. We introduce quantitative notions of isotropy of quadratic forms and congruence of matrices over fields with a degree function. It turns out that this is the appropriate abstract setting in order to obtain the weak isotropy of a quadratic form over a certain field from the weak isotropy over all semi-splitting fields of a given polynomial.

In chapter 9 we also treat a quantitative problem concerning quadratic forms. It is a well-know fact that over a field K which is not formally real each quadratic form is weakly hyperbolic. For a given degree function on K we give bounds for values of the entries of the corresponding transformation matrix.

Chapter 10 is concerned with the quantitative diagonalization of Hankel matrices.

In the last chapter 11 we finally give a recursion formula for H_k and as a consequence we obtain an estimate for H_k and N_k.

Acknowledgement

I am grateful to Prof. E. Becker for his kind support and to Dr. R. Berr for several helpful discussions. Further I take the opportunity to thank Deutsche Forschungsgemeinschaft for their financial support.

Chapter 1

Preliminaries

In this chapter we introduce the basic notations which will be used in the sequel and we prove some preliminary results. Throughout this chapter we let k be a formally real field and denote its algebraic closure by $\bar{k}$. If $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ is an ideal we let

$$\mathrm{V}(\mathfrak{a}) := \{x \in \bar{k}^n \mid f(x) = 0 \text{ for all } f \in \mathfrak{a}\ \}$$

be the set of zeroes of $\mathfrak{a}$. A zero $x = (x_1, \ldots, x_n) \in \mathrm{V}(\mathfrak{a})$ of $\mathfrak{a}$ is called a real zero if $k(x_1, \ldots, x_n)$ is a formally real field. The set of all real zeroes of $\mathfrak{a}$ we denote by $\mathrm{V_r}(\mathfrak{a})$. If $\mathfrak{a}$ is generated by the polynomials $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ we also use the notions $\mathrm{V}(f_1, \ldots, f_m)$ and $\mathrm{V_r}(f_1, \ldots, f_m)$.

In full analogy to Hilbert's Nullstellensatz the Real Nullstellensatz characterizes the polynomials $f \in k[X_1, \ldots, X_n]$ vanishing on the set of real zeroes of a system of polynomials $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$.

Theorem 1.1 (Real Nullstellensatz): *Let $f, f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Then f vanishes on $\mathrm{V_r}(f_1, \ldots, f_m)$ iff there are $r, t \in \mathbb{N}$, $h_1, \ldots, h_r, q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that*

$$f^{2t} + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} q_i f_i$$

Proof: If f satisfies an equation of the above type then f obviously vanishes on the set of real zeroes $\mathrm{V_r}(f_1, \ldots, f_m)$. In order to prove the non-trivial direction suppose first that $\mathrm{V_r}(f_1, \ldots, f_m) = \emptyset$, $f = 1$ and let $\mathfrak{a} := (f_1, \ldots, f_m)$. Assume that $\mathfrak{a}$ is a semireal ideal. By [28] Theorem 2.3 there is a real prime ideal $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ which contains $\mathfrak{a}$. Then

$K := \mathrm{Quot}(k[X_1,\dots,X_n]/\mathfrak{p})$ is a formally real field and k is canonically embedded in K. Let P be an ordering of K. Then

$$\overline{(K,P)} \models \exists x_1,\dots,x_n \bigwedge_{i=1}^{m} f_i(x_1,\dots,x_n)=0$$

and by model completeness of the theory of real closed fields we obtain

$$\overline{(k,k\cap P)} \models \exists x_1,\dots,x_n \bigwedge_{i=1}^{m} f_i(x_1,\dots,x_n)=0$$

This yields the contradiction $\mathrm{V_r}(f_1,\dots,f_m)\neq\emptyset$.

Thus $\mathfrak{a}$ is not a semireal ideal and hence -1 is a sum of squares in the residue class ring $k[X_1,\dots,X_n]/\mathfrak{a}$. Therefore there are $r\in\mathbb{N}$ and $h_1,\dots,h_r,q_1,\dots,q_m\in k[X_1,\dots,X_n]$ such that

$$1+\sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} q_i f_i$$

The usual Rabinowitsch trick finally yields the assertion. □

For a polynomial $f\in k[X_1,\dots,X_n]$ and a real closed extension R of k we define as usual:

f is positive definite in R	$:\Longleftrightarrow$	$f(x)>0$	for all $x\in R^n$
f is positive semidefinite in R	$:\Longleftrightarrow$	$f(x)\geq 0$	for all $x\in R^n$
f is negative definite in R	$:\Longleftrightarrow$	$f(x)<0$	for all $x\in R^n$
f is negative semidefinite in R	$:\Longleftrightarrow$	$f(x)\leq 0$	for all $x\in R^n$

f is called definite in R if it is positive definite or negative definite in R and we say that f is semidefinite in R if f is positive semidefinite or semidefinite in R.

If f is positive semidefinite in every real closed extension of k we call f positive semidefinite over k. Similarly we introduce the meaning for a polynomial to be positive definite, negative semidefinite or negative definite over k.

Furthermore, we say that f is definite over k if f is definite in every real closed extension R of k, and we call f semidefinite over k if f is semidefinite in every real closed extension of k.

Remark: Note that it is possible that a polynomial which is semidefinite over k is positive semidefinite in one real closed extension while it is negative semidefinite in another. The field $\mathbb{Q}(\sqrt{2})$ admits two orderings P_1,P_2 according to the two different embeddings of $\mathbb{Q}(\sqrt{2})$ into $\mathbb{R}$ and $\sqrt{2}$ is positive w.r.t. one and negative w.r.t. the other ordering. Say $\sqrt{2}\in P_1$ and $-\sqrt{2}\in P_2$. Thus the polynomial $f(X)=\sqrt{2}X^2\in\mathbb{Q}(\sqrt{2})[X]$ is positive semidefinite in the real closure of $\mathbb{Q}(\sqrt{2})$ w.r.t. P_1 but negative semidefinite in the real closure of $\mathbb{Q}(\sqrt{2})$ w.r.t. P_2. However, by our definition f is semidefinite over $\mathbb{Q}(\sqrt{2})$.

Usually Hilbert's 17th problem is stated for $\mathbb{R}$ or more generally for real closed fields. Also the following version of Artin's result is well-know but not explicitly in the literature. However, it will be the version which our degree bounds refer at. Therefore we state the result explicitly and we give a simple model theoretic proof.

Theorem 1.2: *Let $f \in k[X_1, \dots, X_n]$ be positive semidefinite over k. Then f is a sum of squares in $k(X_1, \dots, X_n)$.*

Proof: Assume that f is not a sum of squares in $K := k(X_1, \dots, X_n)$. Then by a theorem of Artin and Schreier (cf. [36], Cor. 1.9) there is an ordering P of K such that $f < 0$. Thus

$$\overline{(K, P)} \models \exists x_1, \dots, x_n \ f(x_1, \dots, x_n) < 0$$

and by model completeness of the theory of real closed fields we get

$$\overline{(k, k \cap P)} \models \exists x_1, \dots, x_n \ f(x_1, \dots, x_n) < 0$$

and hence f would not be positive semidefinite over k. $\square$

We define $H_k(n,d)$ and $N_k(n,s,d)$ in the following way:

Definition: *$H_k(n,d)$ is the least natural number t such that for every positive semidefinite polynomial $f \in k[X_1, \dots, X_n]$ of degree $\deg f \le d$ there are $r \in \mathbb{N}$ and polynomials $g, g_1, \dots, g_r \in k[X_1, \dots, X_n]$, $g \neq 0$ of degrees $\deg g_i \le t$ such that $g^2 f = \sum_{i=1}^r g_i^2$. If there is no such a number t we let $H_k(n,d) = \infty$.*

Definition: *$N_k(n,s,d)$ is the least natural number t such that for each system of polynomials $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ with $\mathrm{V_r}(f_1, \dots, f_m) = \emptyset$, $\dim(f_1, \dots, f_m) = s$ and $\deg f_i \le d$ $(1 \le i \le m)$ there are $r \in \mathbb{N}$ and $h_1, \dots, h_r, q_1, \dots, q_m \in k[X_1, \dots, X_n]$ such that*

$$1 + \sum_{i=1}^r h_i^2 = \sum_{i=1}^m q_i f_i$$

and $\deg(q_i f_i) \le t$. If there is no such a number t we let $N_k(n,s,d) = \infty$.

Remark:
1) As usual the unit ideal has dimension -1.
2) Since there is no ideal $\mathfrak{a} \subset k[X_1, \dots, X_n]$ with $\dim \mathfrak{a} > n$ we get $N_k(n,s,d) = 0$ if $s > n$.

First let us state some trivial lower bounds for H_k and N_k. For a real number $x \in \mathbb{R}$ we let $[x] := \max\{n \in \mathbb{Z} \mid n \le x\}$

Lemma 1.3: *Let $n, s, d \in \mathbb{N}$, $n \ge 1$. Then*

(a) $H_k(n,d) \ge [\frac{1}{2}d]$

(b) $N_k(n,s,d) \ge d$

Proof: Immediate by the definition $\square$

Lemma 1.4: $N_k(n,-1,d) \le d^n$ *for $n, d \in \mathbb{N}$, $n \ge 1$, $d \ge 3$.*

Proof: Let $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ of degrees $\deg f_i \le d$ such that $1 \in (f_1, \dots, f_m)$. Then by the effective Nullstellensatz there are polynomials $q_1, \dots, q_m \in k[X_1, \dots, X_n]$ such that $\deg(q_i f_i) \le d^n$ and $1 = \sum_{i=1}^m q_i f_i$. This yields the result. $\square$

Lemma 1.5: $H_k(1,d) = [\frac{1}{2}d]$ *for all* $d \in \mathbb{N}$.

Proof: Let $f \in k[X]$ be positive semidefinite over k and suppose that $\deg f \le d$. Then f is a sum of squares in $k(X)$ and by Satz 7 [2] f is even a sum of squares of polynomials, i.e.,

$$f = \sum_{i=1}^{r} g_i^2$$

for certain $g_1, \dots, g_r \in k[X]$. As k is formally real we get

$$2 \cdot \deg g_i \le \deg \left(\sum_{j=1}^{r} g_j^2 \right) = \deg f \le d$$

and thus $\deg g_i \le [\frac{1}{2}d]$. This implies $H_k(1,d) \le [\frac{1}{2}d]$. Since also $H_k(1,d) \ge [\frac{1}{2}d]$ by Lemma 1.3(a) we are done. $\square$

Next we will show that the values of H_k and N_k are finite provided that the second Pythagoras number $\mathrm{P}_2(k)$ of k is finite. By definition $\mathrm{P}_2(k)$ is the least natural number r such that every sum of squares in k is already a sum of r squares. If such a number r does not exist we let $\mathrm{P}_2(k) = \infty$. First we need a simple model theoretic lemma.

Lemma 1.6: *Let φ be a formula in the language of ordered fields and let $r \in \mathbb{N}$. Then there is a formula ψ in the language of fields with the same free variables as φ such that for every formally real field k with $\mathrm{P}_2(k) \le r$ and all $a_1, \dots, a_n \in k$ holds*

$$k \models \psi(a_1, \dots, a_n) \iff \overline{(k,P)} \models \varphi(a_1, \dots, a_n) \quad \text{for all orderings } P \text{ of } k$$

Proof: We first treat the case where φ is of the form $\chi \vee \bigvee_{i=1}^{m} P(t_i)$ for certain terms $t_1, \dots, t_m$ and a disjunction χ of equations and negations of equations. Since φ is quantifier free we get

$$(k,P) \models \varphi(a_1, \dots, a_n) \quad \iff \quad \overline{(k,P)} \models \varphi(a_1, \dots, a_n)$$

and since χ does not contain the symbol P we are restricted to the problem to express the clause

$$\text{"for each ordering } P \text{ of } k: \quad (k,P) \models \bigvee_{i=1}^{m} P(t_i(a_1, \dots, a_n)) \text{"}$$

However, this just means that $-t_1(a_1, \dots, a_n), \dots, -t_m(a_1, \dots, a_n)$ do not generate a preordering. Since $\mathrm{P}_2(k)$ is bounded by r this obviously can be expressed by a first order formula.

Now let φ be an arbitrary formula. Since the theory RCF of real closed fields admits elimination of quantifiers (cf. [37], Satz 4.7) there is a quantifier free formula φ' which has the same free variables as φ such that

$$\mathrm{RCF} \models (\varphi \longleftrightarrow \varphi')$$

Furthermore φ' can be chosen in conjunctive normal form, and since

$$\mathrm{RCF} \models (\neg P(t) \longleftrightarrow (P(-t) \wedge t \neq 0))$$

we may assume that φ' is of the form $\bigwedge_{i=1}^{\ell}(\chi_i \vee \chi_i')$ with each χ_i is a disjunction of equations and negations of equations and each χ_i' is of the form $\bigvee_{i=1}^{m} P(t_i)$.

As we have shown above there are formulas $\psi_1, \dots, \psi_\ell$ in the language of fields such that for each formally real field k such that $\mathrm{P}_2(k) \leq r$ and all $a_1, \dots, a_n \in k$ holds

$$k \models \psi_i(a_1, \dots, a_n) \iff \overline{(k, P)} \models \chi_i'(a_1, \dots, a_n) \quad \text{for all orderings } P \text{ of } k$$

for $1 \leq i \leq \ell$. Since χ_i is a formula in the language of fields $\chi_i(a_1, \dots, a_n)$ either holds in k and all its real closures or in none of these fields. Therefore

$$\psi := \bigwedge_{i=1}^{\ell}(\chi_i \vee \psi_i)$$

has the desired properties. $\square$

Theorem 1.7: *Assume that* $\mathrm{P}_2(k) < \infty$. *Then* $H_k(n, d) < \infty$ *and* $N_k(n, s, d) < \infty$ *for all* $n, s, d \in \mathbb{N}$.

Proof: We proof that $H_k(n, d)$ is finite. The proof for the finiteness of $N_k(n, s, d)$ runs similar. It suffices to show that for given $n, d, r \in \mathbb{N}$ there is a natural number $m \in \mathbb{N}$ such that $H_k(n, d) \leq m$ for all formally real fields k with $\mathrm{P}_2(k) \leq r$. Assume the contrary. Then for every $m \in \mathbb{N}$ there is a formally real field k_m and a polynomial $f_m \in k_m[X_1, \dots, X_n]$ such that $\mathrm{P}_2(k_m) \leq r$, f_m is positive semidefinite over k_m of degree $\deg f_m \leq d$ and for each representation

$$g^2 \cdot f_m = \sum_{i=1}^{N} h_i^2$$

in $k_m[X_1, \dots, X_n]$ with $g \neq 0$ we get $\deg h_i > m$ for at least one i.

By Lemma 1.6 there is a formula ψ in the language of fields such that for every formally real field k such that $\mathrm{P}_2(k) \leq r$ and each $f \in k[X_1, \dots, X_n]$ of degree $\deg f \leq d$ holds

$$k \models \psi(f) \quad \iff \quad f \text{ is positive semidefinite over } k$$

Of course, $\psi(f)$ means the formula which is obtained from ψ by substituting the coefficients from f for the corresponding free variable of ψ.

Let $\mathcal{U}$ be a non-principal ultrafilter on $\mathbb{N}$ and let

$$k := \prod_{m \in \mathbb{N}} k_m / \mathcal{U}$$

be the ultraproduct of the fields $(k_m)_{m \in \mathbb{N}}$ and define $f := \overline{(f_m)_{m \in \mathbb{N}}}$. Then, by Łos' theorem (cf. [37], Satz 2.23) k is a formally real field and $\mathrm{P}_2(k) \leq r$. Since each f_m is positive semidefinite over k_m we get $k_m \models \psi(f_m)$ and thus $k \models \psi(f)$ by Łos' theorem. Hence f is positive semidefinite over k and thus there are $g, h_1, \ldots, h_N \in k[X_1, \ldots, X_n], g \neq 0$ such that

$$g^2 f = \sum_{i=1}^{N} h_i^2$$

Let $t := \max(\deg h_1, \ldots, \deg h_N)$. Again by Łos' theorem there is a set $J \in \mathcal{U}$ such that for each $j \in J$ there is a representation

$$g_j^2 f_j = \sum_{i=1}^{N} h_{ij}^2$$

such that $g_j \neq 0$ and $\deg h_{ij} \leq t$. However, as $\mathcal{U}$ is non-principal J has to be infinite and thus there is a natural number $m > t$ such that $m \in J$. Then

$$g_m^2 f_m = \sum_{i=1}^{N} h_{im}^2$$

and $g_m \neq 0$ and $\deg h_{im} \leq t < m$ in contradiction to the choice of k_m and f_m. This proves the finiteness of $H_k(n, d)$. □

As already mentioned in the introduction Daykin [12] obtained a bound for the number of summands which are required to represent a positive semidefinite polynomial as a sum of squares of rational functions. We are interested in the degrees occurring in such a representation. However, a bound on the degree also yields a bound on the number of summands. This is an immediate consequence of a result of Powers and Wörmann [35]. In that paper the authors gave an algorithm which decides whether a given polynomial $f \in \mathbb{R}[X]$ is a sum of squares of polynomials and which effectively produces a representation $f = \sum_{i=1}^{r} f_i^2$ if there is one. Implicitely they proved the following result for the case $n = 1$.

Theorem 1.8: *Let $f \in k[X_1, \ldots, X_n] \setminus k$ be a sum of squares in $k[X_1, \ldots, X_n]$ and assume that $\deg f \leq d$. Then f is already a sum of $\mathrm{P}_2(k) \cdot d^n$ squares in $k[X_1, \ldots, X_n]$*

Proof: If $\mathrm{P}_2(k) = \infty$ there is nothing to show. So assume that $r = \mathrm{P}_2(k) < \infty$. As f is a sum of squares in $k[X_1, \ldots, X_n]$ its degree is even. Thus $\deg f = 2m \leq d$ for some $m \in \mathbb{N}$. Note that this implies $d \geq 2$ as $f \notin k$. Assume that $f = \sum_{i=1}^{s} g_i^2$. Then $\deg g_i \leq m$ $(1 \leq i \leq s)$. Now let $P_1, \ldots, P_t$ be the terms $\prod_{i=1}^{n} X_i^{t_i}$ of degree $\leq m$. It is well-known that

$$t = \binom{n+m}{n} = \binom{n+\frac{1}{2}d}{n} = \frac{1}{n!} \cdot \prod_{i=1}^{n} (\tfrac{1}{2}d + i) = \prod_{i=1}^{n} \frac{d+2i}{2i} \leq d^n$$

Every g_i admits a representation $g_i = \sum_{i=1}^{t} a_{ij} P_i$ for certain $a_{ij} \in k$. Now let A be the coefficient matrix

$$A := \begin{pmatrix} a_{11} & \ldots & a_{1t} \\ \vdots & & \vdots \\ a_{s1} & \ldots & a_{st} \end{pmatrix}$$

Then

$$\begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1t} \\ \vdots & & \vdots \\ a_{s1} & \dots & a_{st} \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ \vdots \\ P_t \end{pmatrix}$$

The matrix $A^T A$ is a symmetric $(t \times t)$-matrix over k. Hence there is a regular matrix $Q \in \mathrm{GL}(t, k)$ such that

$$Q^T(A^T A)Q = \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_t \end{pmatrix}$$

for certain $b_1, \dots, b_t \in k$. Denote the diagonal matrix on the right hand side of the above equation by B. If $e_1, \dots, e_t$ are the canonical unit vectors we get

$$b_i = e_i^T B e_i = e_i^T A^T A e_i = (Ae_i)^T (Ae_i)$$

and hence $b_1, \dots, b_t$ are sums of squares. Therefore $b_i = \sum_{j=1}^r b_{ij}^2$ $(1 \le i \le t)$ for certain $b_{ij} \in k$. Denote the entries of Q^{-1} by c_{ij} and define $h_i := \sum_{j=1}^t c_{ij} P_j$ $(1 \le i \le t)$. Let further

$$v := \begin{pmatrix} P_1 \\ \vdots \\ P_t \end{pmatrix}$$

Then

$$Q^{-1} v = \begin{pmatrix} h_1 \\ \vdots \\ h_t \end{pmatrix}$$

and thus

$$f = \sum_{i=1}^s g_i^2 = (Av)^T (Av) = (Q^{-1}v)^T B (Q^{-1}v) = \sum_{i=1}^t b_i h_i^2 = \sum_{i=1}^t \sum_{j=1}^r b_{ij}^2 h_i^2$$

This proves the theorem. $\square$

With an idea of Colliot-Thélène [11] we get a first easy relation of H_k and N_k.

Theorem 1.9: $H_k(n, d) \le \frac{1}{2} \cdot (d+2) \cdot N_k(n+1, n, d+2)$

Proof: Let $f \in k[X_1, \dots, X_n] \backslash \{0\}$ be positive semidefinite over k and assume that $\deg f \le d$. We introduce a new variable Y and let $\mathfrak{a}$ be the principal ideal generated by $1 + Y^2 f$ in $k[X_1, \dots, X_n, Y]$. Then $\dim \mathfrak{a} = n$ since $\mathrm{V}(\mathfrak{a})$ is a hypersurface. Obviously $\mathrm{V_r}(\mathfrak{a}) = \emptyset$. Hence

$$1 + \sum_{i=1}^r h_i^2 = q \cdot (1 + Y^2 f) \tag{1}$$

for certain $h_1, \ldots, h_r, q \in k[X_1, \ldots, X_n, Y]$ such that

$$\deg(q(1+Y^2 f)) \leq N_k(n+1, n, d+2) \tag{2}$$

Now let $t := \max(\deg h_1, \ldots, \deg h_r)$. Then (1) and (2) yield

$$2t = \deg\left(1 + \sum_{i=1}^{r} h_i^2\right) \leq N_k(n+1, n, d+2)$$

and thus

$$t \leq \tfrac{1}{2} \cdot N_k(n+1, n, d+2) \tag{3}$$

We choose a natural number m such that $t \leq 2m \leq t+1$ and let $X := (X_1, \ldots, X_n)$. Every h_i we express in the form

$$h_i(X, Y) = \sum_{j=0}^{2m} h_{ij}(X) Y^j$$

for certain $h_{ij} \in k[X_1, \ldots, X_n]$ of degree $\deg h_{ij} \leq 2m - j$. Thus

$$\sqrt{-f}^{2m} h_i(X, \frac{1}{\sqrt{-f}}) = \sum_{j=0}^{2m} h_{ij}(X) \sqrt{-f}^{2m-j} = P_i(X) + \sqrt{-f} \cdot Q_i(X) \tag{4}$$

with $P_i(X) = \sum_{j=0}^{m} h_{i\,2j}(X) \cdot (-f)^{m-j}$ and $Q_i(X) = \sum_{j=1}^{m} h_{i\,2j-1}(X) \cdot (-f)^{m-j}$.
For $1 \leq j \leq m$ we obtain

$$\deg(h_{i\,2j-1}(X) \cdot (-f)^{m-j}) \leq 2m - (2j-1) + (m-j)d \leq 2m - 1 + (m-1)d$$

and thus

$$\deg Q_i \leq t + \tfrac{1}{2}(t-1)d \qquad (1 \leq i \leq r) \tag{5}$$

In equation (1) we first substitute $Y \mapsto \frac{1}{\sqrt{-f}}$ and then we multiply the obtained equation by f^{2m}. By (4) this yields

$$0 = f^{2m} + \sum_{i=1}^{r} (P_i + \sqrt{-f}\, Q_i)^2 = f^{2m} + \sum_{i=1}^{r} P_i^2 - f \sum_{i=1}^{r} Q_i^2 + 2\sqrt{-f} \sum_{i=1}^{r} P_i Q_i$$

Therefore $\sum_{i=1}^{r} P_i Q_i = 0$. Otherwise $-f$ would be a sum of squares in $k(X_1, \ldots, X_n)$ which is impossible since f is positive semidefinite and $f \neq 0$. Hence

$$f \cdot \sum_{i=1}^{r} Q_i^2 = f^{2m} + \sum_{i=1}^{r} P_i^2 \tag{6}$$

The right hand side of the equation is non-zero because $k(X_1,\dots,X_n)$ is formally real and $f\neq 0$. Thus $\sum_{i=1}^{r} Q_i^2 \neq 0$. Now let $h := \sum_{i=1}^{r} Q_i^2$. From (5) we get

$$\deg h = 2\cdot\max(\deg Q_1,\dots,\deg Q_r) \leq 2t + (t-1)d$$

Now (6) yields that $h^2 f$ is a sum of squares in $k[X_1,\dots,X_n]$

$$h^2 f = \sum_{i=1}^{s} g_i^2$$

for certain $s\in\mathbb{N}, g_1,\dots,g_s \in k[X_1,\dots,X_n]$. Then

$$2\cdot\deg g_i \leq \deg\left(\sum_{i=1}^{s} g_i^2\right) = \deg(h^2 f) \leq 4t + 2(t-1)d + d \leq (d+2)2t$$

and therefore $\deg g_i \leq (d+2)\cdot t$. From (3) we obtain the assertion. $\square$

The remaining part of this chapter is devoted to the study of degree bounds for the real Nullstellensatz in the zero-dimensional case. The upper bound for $N_k(n,0,d)$ can implicitly be found in [41].

We again assume that k is a formally real field. By X_k we denote the set of all orderings of k. This set is a compact Hausdorff space w.r.t. the so-called Harrison topology. A basis for the open sets of this topology is given by the sets

$$H(a_1,\dots,a_n) = \{P\in X_k \mid a_1,\dots,a_n \in P\}$$

$(a_1,\dots,a_n \in k, n\in\mathbb{N})$(cf. [36], Chap.6).

Lemma 1.10: *Let $f\in k[X]$ be a univariate polynomial without real zeroes. Then there is some $a\in k^\times$, a natural number $r\leq \mathrm{P}_2(k(X))$ and polynomials $h_1,\dots,h_r\in k[X]$ such that*

$$af = 1 + \sum_{i=1}^{r} h_i^2$$

Proof: Let $c\in k^\times$ be the leading coefficient of f. For $a\in k$ we let

$$U_a := \left\{P\in X_k \mid \overline{(k,P)} \models \forall x\ a^2 c^{-1} f(x) \geq 1\right\}$$

where $\overline{(k,P)}$ is the real closure of (k,P). Since the theory of real closed fields admits elimination of quantifiers in the language of ordered fields the sets U_a are open subsets of the space X_k of orderings of k. We first show that every ordering P of k is contained in such a set U_a.

Let P be an arbitrary ordering of k. As $c^{-1}f$ is monic and has no zero in $\overline{(k,P)}$ it is positive definite and thus there is some $b\in\overline{(k,P)}$, $b\neq 0$ such that $c^{-1}f(x)\geq b$ for all

$x \in \overline{(k,P)}$. As $\overline{(k,P)}$ is an algebraic extension of k the field k is cofinal w.r.t. P in $\overline{(k,P)}$. Hence there is an element $a \in k^\times$ such that $b^{-1} \leq a^2$ and thus $b \geq a^{-2}$. Therefore we obtain $1 \leq a^2 c^{-1} f(x)$ for every $x \in \overline{(k,P)}$. Thus $P \in U_a$.
This shows

$$\bigcup_{a \in k} U_a = X_k$$

Since X_k is compact there are finitely many elements $a_1, \ldots, a_m \in k^\times$ such that

$$\bigcup_{i=1}^{m} U_{a_i} = X_k$$

Now let $a := c^{-1} \sum_{i=1}^m a_i^2$. Then one can easily check that $af - 1$ is positive semidefinite in every real closure of k. Therefore $af - 1$ is a sum of squares of rational functions, i.e.

$$af - 1 = \sum_{i=1}^{r} g_i^2$$

for certain $r \leq \mathrm{P}_2(k(X)), g_1, \ldots, g_r \in k(X)$. By Cassels' theorem ([39], p. 148, Cor. 3.1) there are $h_1, \ldots, h_r \in k[X]$ such that

$$af - 1 = \sum_{i=1}^{r} h_i^2$$

This proves the lemma. $\square$

Theorem 1.11: *Let $\mathfrak{a} = (f_1, \ldots, f_m) \subset k[X_1, \ldots, X_n]$ be a 0-dimensional ideal, $d \in \mathbb{N}$, $d \geq 3$ such that $\deg f_i \leq d$ $(1 \leq i \leq m)$ and assume that $\mathfrak{a}$ has no real zeroes. Let $s := \#\mathrm{V}(\mathfrak{a})$. Then there are $r \in \mathbb{N}$ and polynomials $h_1, \ldots, h_r, q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that*

$$1 + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} q_i f_i$$

and

(a) $r \leq \mathrm{P}_2(k(X))$
(b) $\deg \sum_{i=1}^r h_i^2 \leq d^n s \leq d^{2n}$
(c) $\deg(q_i f_i) \leq d^n \cdot (1+s) \leq d^n(d^n+1) \quad (1 \leq i \leq m)$

Proof: After an affine invertible transformation of the coordinates we may assume that the projection map

$$\pi : \mathrm{V}(\mathfrak{a}) \longrightarrow \bar{k}$$
$$(x_1, \ldots, x_n) \mapsto x_n$$

is injective. This invertible transformation induces an automorphism of the polynomial ring $k[X_1, \ldots, X_n]$ which preserves the total degree. So w.l.o.g. we may assume that π is injective. By the Shape Lemma ([6], p. 281) there are polynomials $g, g_1, \ldots, g_{n-1} \in k[X_n]$ such that

$$\sqrt{\mathfrak{a}} = (g(X_n), X_1 - g_1(X_n), \ldots, X_{n-1} - g_{n-1}(X_n)) \tag{1}$$

and

$$\deg g_i < \deg g = \#\mathrm{V}(\mathfrak{a}) = s$$

As $g \in \sqrt{\mathfrak{a}}$ we obtain by the effective Nullstellensatz ([23], Cor. 1.7)

$$g^t = \sum_{i=1}^{m} q_i f_i \tag{2}$$

for certain $t \in \mathbb{N}$ and $q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that $t \leq d^n$ and $\deg(q_i f_i) \leq d^n(1 + \deg g) = d^n(1 + s)$. From (1) we immediately obtain

$$\mathrm{V}(\mathfrak{a}) = \{(g_1(a), \ldots, g_{n-1}(a), a) |\ a \in \bar{k}, g(a) = 0\}$$

and hence g has no real zeroes. Therefore also g^t has no real zeroes. By Lemma 1.10 there are a natural number $r \leq \mathrm{P}_2(k(X))$, an element $a \in k^\times$ and polynomials $h_1, \ldots, h_r \in k[X_n]$ such that

$$1 + \sum_{i=1}^{r} h_i^2 = a g^t \tag{3}$$

Then

$$\deg \sum_{i=1}^{r} h_i^2 \leq \deg g^t = t \deg g \leq d^n s$$

Now (2) and (3) yield

$$1 + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{m} a q_i f_i$$

From the Bezout inequality ([40], Theorem 3.1) we get $s = \#\mathrm{V}(\mathfrak{a}) \leq d^n$. This proves the theorem. □

Corollary 1.12: *Let $d \geq 3$. Then:* $N_k(n, 0, d) \leq d^n(d^n + 1)$

Proof: The corollary is an immediate consequence of the above theorem. □

In the next proposition we give a lower bound for $N_k(n,0,d)$ of the type $d^{O(n-1)}$. For the proof we extend an example which also occurs in [23].

Proposition 1.13: $N_k(n,0,d) \geq d^{n-2}(d-2)$

Proof: If $d \leq 2$ there is nothing to show. So we assume that $d \geq 3$ and let

$$\mathfrak{a} := \left(X_1^d - X_2, X_2^d - X_3, \ldots, X_{n-2}^d - X_{n-1}, X_{n-1}^{d-2} \cdot (X_{n-1}^2 + 1), X_1 X_n - 1\right)$$

It is easy to see that $\mathrm{V}(\mathfrak{a})$ is finite and non-empty but $\mathrm{V_r}(\mathfrak{a}) = \emptyset$. Thus there is an equation of the type

$$(1) \qquad 1 + \sum_{i=1}^{r} h_i^2 = \sum_{i=1}^{n-2} q_i \cdot \left(X_i^d - X_{i+1}\right) + q_{n-1} \cdot X_{n-1}^{d-2} \cdot (X_{n-1}^2 + 1) + q_n \cdot (X_1 X_n - 1)$$

for certain polynomials $q_1, \ldots, q_n, h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$ such that the maximal degree of all summands occurring on the right hand side of equation (1) is bounded by $N_k(n,0,d)$. Denote this maximal degree by m. Then $\deg q_i \leq m-2$ $(1 \leq i \leq n)$ and

$$2 \cdot \deg h_i \leq \deg\left(1 + \sum_{j=1}^{r} h_j^2\right) \leq m \quad (1 \leq i \leq r)$$

and therefore $\deg h_i \leq t := [\frac{1}{2}m]$. Now we substitute $X_n \mapsto X_1^{-1}$ in equation (1) and multiply the obtained equation by X_1^{2t}. This yields

$$X_1^{2t} + \sum_{i=1}^{r} g_i^2 = \sum_{i=1}^{n-2} p_i \cdot \left(X_i^d - X_{i+1}\right) + p_{n-1} \cdot X_{n-1}^{d-2} \cdot (X_{n-1}^2 + 1)$$

for certain polynomials $p_1, \ldots, p_{n-1}, g_1, \ldots, g_r \in k[X_1, \ldots, X_n]$. Then the substitution $X_i \mapsto X^{d^{i-1}}$ $(1 \leq i \leq n)$ yields the equation

$$X^{2t} + \sum_{i=1}^{r} f_i^2 = p \cdot X^{d^{n-2}(d-2)} \cdot (X^{2d^{n-2}} + 1)$$

for certain $f_1, \ldots, f_r, p \in k[X]$. The valuation $v : k(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$ which corresponds to the valuation ring $k[X]_{(X)}$ is real. Hence by Lemma 3.7 [27] we get

$$\begin{aligned} d^{n-2}(d-2) &\leq v(p \cdot X^{d^{n-2}(d-2)} \cdot (X^{2d^{n-2}} + 1)) = v(X^{2t} + \sum_{i=1}^{r} f_i^2) \\ &= \min\{2t, v(f_1^2), \ldots, v(f_r^2)\} \leq 2t \leq m \end{aligned}$$

and the proposition is proved. $\square$

Chapter 2

Degree functions

This chapter is devoted to a first study of degree functions. A degree function is a generalization of the notion of the usual degree of a polynomial. It will turn out that for our purpose degree functions are the appropriate tool to measure the size of elements of an algebraic extension of a rational function field.

Definition: *Let R be an integral domain. A degree function on R is a map*

$$\delta\colon R \longrightarrow \Gamma \cup \{-\infty\}$$

from R into a totally ordered abelian group Γ together with a distinguished element $-\infty$ such that for all $x, y \in R$ the following conditions hold:

(i) $\delta(x) = -\infty \iff x = 0$

(ii) $\delta(x+y) \leq \max(\delta(x), \delta(y))$

(iii) $\delta(xy) \leq \delta(x) + \delta(y)$

(iv) $\delta(x^n) = n \cdot \delta(x)$ *for all* $n \in \mathbb{N}$

with the conventions $(-\infty) + (-\infty) = \alpha + (-\infty) = (-\infty) + \alpha = -\infty$ and $-\infty < \alpha$ for all elements $\alpha \in \Gamma$.

Examples, remarks:

1) Every integral domain admits the trivial degree function

$$x \mapsto \begin{cases} 0 & \text{if } x \neq 0 \\ -\infty & \text{if } x = 0 \end{cases}$$

2) If R is a domain then $\deg\colon R[X_1, \ldots, X_n] \longrightarrow \mathbb{Z} \cup \{-\infty\}$ is a degree function.

3) If $v\colon K \longrightarrow \Gamma \cup \{\infty\}$ is a valuation of the field K then $\delta = -v$ is obviously a degree function on K.

4) Let $\delta_1, \ldots, \delta_n\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be degree functions on the field K. Then it is easy to see that also $\delta = \max(\delta_1, \ldots, \delta_n)$ is a degree function on K.

5) Let $v_2, v_3\colon \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the 2-adic and 3-adic valuation on the field $\mathbb{Q}$ of rational numbers. According to 3) and 4) the application $\delta(z) = -\min(v_2(z), v_3(z))$ yields a degree function $\delta\colon \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{-\infty\}$. As one can easily see $\delta(2) = \delta(3) = 0$ and $\delta(6) = -1$. This shows that in condition (iii) the strict inequality may occur. Furthermore $\delta(\frac{1}{2}) = 1$. Thus in general $\delta(x^n) \neq n \cdot \delta(x)$ for negative integers n.

6) Let again v_2 be the 2-adic valuation of $\mathbb{Q}$ and let v_0 be the trivial valuation. Then also by $\delta(z) = -\min(v_0(z), v_2(z))$ a degree function is defined. Obviously $\delta(\mathbb{Q}^\times) = \mathbb{N}$. So the image of a field under a degree function is not necessarily a group.

The next proposition combines the examples 2) and 3).

Proposition 2.1: *Assume that k is a field and let n be a natural number. Then there is a degree function $\delta\colon \overline{k(X_1, \ldots, X_n)} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ such that $\delta(f) = \deg f$ for every polynomial $f \in k[X_1, \ldots, X_n]$.*

Proof: Let $K := k(X_1, \ldots, X_n)$ be the field of rational functions in n indeterminates over k. It is well-known that the map

$$\begin{aligned} v_\infty : K &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ f/g &\mapsto \deg g - \deg f \end{aligned}$$

is a valuation on K. We extend v_∞ to a valuation $v : \bar{K} \longrightarrow \mathbb{Q} \cup \{\infty\}$ of the algebraic closure $\bar{K}$ of K and let $\delta := -v$. Then $\delta\colon \bar{K} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ is a degree function on $\bar{K}$ and $\delta(f) = \deg f$ for all polynomials $f \in k[X_1, \ldots, X_n]$. $\square$

After these examples we first state and prove some elementary facts about degree functions.

Lemma 2.2: *Let $\delta\colon R \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the domain R. Then:*

(a) $\delta(1) = 0$
(b) $\delta(\zeta) = 0$ *if $\zeta \in R$ is a root of unity*
(c) $\delta(-x) = \delta(x)$ *for all $x \in R$*

Proof: From $\delta(1) = \delta(1^2) = 2 \cdot \delta(1)$ we get $\delta(1) = 0$. If $\zeta^n = 1$ for some $n \in \mathbb{N}$ we obtain $n \cdot \delta(\zeta) = \delta(\zeta^n) = \delta(1) = 0$, and hence $\delta(\zeta) = 0$. If $x \in R\backslash\{0\}$ then $2 \cdot \delta(-x) = \delta((-x)^2) = \delta(x^2) = 2 \cdot \delta(x)$, and therefore $\delta(-x) = \delta(x)$. $\square$

As in the case of valuations we have:

Lemma 2.3: *Let $\delta\colon R \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the integral domain R and assume that $x, y \in R$. If $\delta(x) \neq \delta(y)$ then $\delta(x + y) = \max(\delta(x), \delta(y))$.*

Proof: We may assume that $\delta(x) < \delta(y)$. The assumption $\delta(x+y) < \max(\delta(x), \delta(y))$ then yields the contradiction

$$\delta(y) = \delta(x+y-x) \leq \max(\delta(x+y), \delta(-x)) < \delta(y)$$

and the lemma is proved. $\square$

Let $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K. An element $a \in K^\times$ is called a δ-unit if $\delta(a) = \delta(a^{-1}) = 0$.

Lemma 2.4: *Let $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K. Then the set of δ-units form a subgroup of $K^\times$.*

Proof: Since the inverse of a δ-unit is again a δ-unit by definition, it suffices to show that the product of two δ-units is again a δ-unit. Let $a, b \in K^\times$ be δ-units. Then one gets $\delta(ab) \leq \delta(a) + \delta(b) = 0$ and $\delta((ab)^{-1}) \leq \delta(a^{-1}) + \delta(b^{-1}) = 0$. Therefore, since

$$0 = \delta(1) = \delta(ab(ab)^{-1}) \leq \delta(ab) + \delta((ab)^{-1}) \leq 0$$

neither $\delta(ab) < 0$ nor $\delta((ab)^{-1}) < 0$ and thus $\delta(ab) = \delta((ab)^{-1}) = 0$. $\square$

We now fix some notations which will be used in the sequel.

If $A = (a_{ij})$ is an $(n \times n)$-matrix over a field K we denote by $\widetilde{A}$ the matrix which has as its entries the cofactors of A, i.e. $\widetilde{A} = (b_{ij})$ with $b_{ij} = (-1)^{i+j} \cdot \det A_{ji}$ and A_{ji} is the $(n-1) \times (n-1)$-matrix which is obtained from A by canceling the j-th row and the i-th column.

If $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K and $x = (x_1, \ldots, x_n) \in K^n$ we let $M_\delta(x) := \max(\delta(x_1), \ldots, \delta(x_n))$. In the same way we define for an $m \times n$ matrix $A = (a_{ij})_{ij}$ over K

$$M_\delta(A) := \max\{\ \delta(a_{ij}) \mid 1 \leq i \leq m,\ 1 \leq j \leq n\ \}$$

With this notations we have:

Lemma 2.5: *Let $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K and assume that A is an $n \times n$ matrix over K with row vectors $v_1, \ldots, v_n \in K^n$ and column vectors $w_1, \ldots, w_n \in K^n$. Then:*

(a) $\delta(\det A) \leq \sum_{i=1}^n M_\delta(v_i)$

(b) $\delta(\det A) \leq \sum_{i=1}^n M_\delta(w_i)$

(c) $\delta(\det A) \leq n \cdot M_\delta(A)$

(d) $M_\delta(\widetilde{A}) \leq (n-1) \cdot M_\delta(A)$

Proof: Let $A = (a_{ij})$. Then $\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$. Since

$$\delta(\prod_{i=1}^{n} a_{i\sigma(i)}) \leq \sum_{i=1}^{n} \delta(a_{i\sigma(i)}) \leq \sum_{i=1}^{n} M_\delta(v_i)$$

we obtain $\delta(\det A) \leq \sum_{i=1}^{n} M_\delta(v_i)$. This proves (a). The second assertion follows from (a) and the fact that $\det A = \det A^T$. The assertions (c) and (d) are also immediate consequences of (a). $\square$

Lemma 2.6: *Let $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on K and let A, B be matrices with entries from K. Then*

(a) $M_\delta(A + B) \leq \max(M_\delta(A), M_\delta(B))$

(b) $M_\delta(AB) \leq M_\delta(A) + M_\delta(B)$

whenever $A + B$ and AB are defined.

Proof: Obvious. $\square$

The next results are concerned with bounds for solutions of linear systems of equations w.r.t. a degree function on a field.

Proposition 2.7: *Let R be an integral domain with $K = \operatorname{Quot}(R)$ and assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further A be non-zero $m \times n$ matrix over R of rank r. Then there are $x_1, \ldots, x_{n-r} \in R^n$ such that*

(a) *$x_1, \ldots, x_{n-r}$ is a K-basis for the linear space of solutions of $Ax = 0$*

(b) $M_\delta(x_i) \leq r \cdot M_\delta(A) \qquad (1 \leq i \leq n - r)$

Proof: Let $A = (a_{ij})_{ij}$. As $\operatorname{rk}(A) = r$ there is a regular $r \times r$-submatrix B of A. W.l.o.g. we may assume that

$$B = \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}$$

Otherwise we change the enumeration of the equations or the indeterminates. Let $b := \det B \in R$. Then $b \neq 0$ since B is regular.

For $1 \leq i \leq r$, $r + 1 \leq j \leq n$ we let B_{ij} be the matrix which is obtained by substituting the i-th column of B by $(-a_{1j}, \ldots, -a_{rj})$. Furthermore we define $b_{ij} := \det B_{ij}$. Then, by Cramer's rule, $(b_{1j}, \ldots, b_{rj})$ is a solution of

$$Bx = \begin{pmatrix} -ba_{1j} \\ \vdots \\ -ba_{rj} \end{pmatrix}$$

For $r + 1 \leq j \leq n$ we let $x_j := (b_{1j}, \ldots, b_{rj}, 0, \ldots, 0, b, 0, \ldots, 0) \in R^n$ with the entry b in the j-th coordinate. By our construction each of the vectors x_j is a solution of the first r equations of the system $Ax = 0$. Since the first r rows of A are linearly independent and $\operatorname{rk}(A) = r$, the vectors $x_{r+1}, \ldots, x_n$ are solutions of the whole system $Ax = 0$. Furthermore $x_{r+1}, \ldots, x_n$ are linearly independent over K since $b \neq 0$. As the linear space of solutions of $Ax = 0$ has dimension $n - r$, $x_{r+1}, \ldots, x_n$ is a basis of this space. By Lemma 2.5 we get $\delta(b), \delta(b_{ij}) \leq rM_\delta(A)$. This yields the result. $\square$

Proposition 2.8: *Let R be an integral domain with $K = \mathrm{Quot}(R)$ and assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further A be non-zero $m \times n$ matrix over R of rank r and let $b \in R^m$. Suppose that the system $Ax = b$ has a solution in K^n. Then there are $z, z_1, \ldots, z_n \in R,\ z \neq 0$ such that*

(a) $(z_1 z^{-1}, \ldots, z_n z^{-1})$ *is a solution of* $Ax = b$

(b) $\delta(z)\ \leq r \cdot M_\delta(A)$

(c) $\delta(z_i) \leq (r-1) \cdot M_\delta(A) + M_\delta(b) \qquad (1 \leq i \leq n)$

Proof: Let $A = (a_{ij})_{ij}$ and $b = (b_1, \ldots, b_m)$. As $\mathrm{rk}(A) = r$ there is a regular $r \times r$-submatrix B of A. W.l.o.g. we may assume that

$$B = \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}$$

Otherwise we change the enumeration of the equations or the indeterminates. Let $z := \det B \in R$. Then $z \neq 0$ since B is regular.

Let B_j be the matrix which is obtained from B by substituting the j-th column of B by $b_1, \ldots, b_r$ and let $z_j := \det B_j\ (1 \leq j \leq r)$. By Cramer's rule we obtain

$$B \cdot \begin{pmatrix} z_1 z^{-1} \\ \vdots \\ z_r z^{-1} \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

If we further let $z_{r+1} = \ldots = z_n = 0$ then $(z_1 z^{-1}, \ldots, z_n z^{-1})$ is a solution of the first r equations of the system $Ax = b$. As the whole system is solvable we get

$$\mathrm{rk} \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix} = \mathrm{rk} \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} = r = \mathrm{rk} \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}$$

and therefore also

$$\mathrm{rk} \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{r1} & \ldots & a_{rn} & b_r \end{pmatrix} = r$$

Thus $(z_1 z^{-1}, \ldots, z_n z^{-1})$ is even a solution of the whole system. From Lemma 2.5(b) we immediately get $\delta(z) \leq r \cdot M_\delta(A)$ and $\delta(z_i) \leq (r-1) \cdot M_\delta(A) + M_\delta(b)$. $\square$

Corollary 2.9: *Let R be a domain with K as its field of quotients and assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further A be non-zero $m \times n$ matrix over R of rank r and let $b \in R^m$. Suppose that $y = (y_1, \ldots, y_n) \in K^n$ is a solution of the system $Ax = b$. Then there are $z, z_1, \ldots, z_n \in R,\ z \neq 0$ such that*

(a) $(z_1 z^{-1}, \ldots, z_n z^{-1})$ *is a solution of* $Ax = b$

(b) $\delta(z)\ \leq r \cdot M_\delta(A)$

(c) $\delta(z_i) \leq (r-1) \cdot M_\delta(A) + M_\delta(b) \qquad (1 \leq i \leq n)$

(d) $\{i |\ y_i = 0\ \} \subset \{i |\ z_i = 0\ \}$

Proof: W.l.o.g. we may assume that $y_1, \ldots, y_k \neq 0$ and $y_{k+1}, \ldots, y_n = 0$. Let

$$B = \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mk} \end{pmatrix}$$

Then $\operatorname{rk}(B) \leq \operatorname{rk}(A) = r$, $M_\delta(B) \leq M_\delta(A)$ and $y' = (y_1, \ldots, y_k)$ is a solution of the system $Bx = b$. By Proposition 2.8 there are $z, z_1, \ldots, z_k \in R,\ z \neq 0$ such that $(z_1 z^{-1}, \ldots, z_k z^{-1})$ is a solution of $Bx = b$ and $\delta(z) \leq r M_\delta(B) \leq r M_\delta(A)$ and $M_\delta(z_i) \leq (r-1) M_\delta(A) + M_\delta(b)$. If we define $z_{k+1}, \ldots, z_n = 0$ then $(z_1 z^{-1}, \ldots, z_n z^{-1})$ is the solution of $Ax = b$ we were looking for. $\square$

Assume that $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K. Then for a polynomial $f = \sum_{i=1}^m a_i \prod_{j=1}^n X_j^{r_{ij}} \in K[X_1, \ldots, X_n]$ we let

$$M_\delta(f) := \max(\delta(a_1), \ldots, \delta(a_m))$$

With this notation we have:

Lemma 2.10: *Let $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on K and assume that $f, g \in K[X_1, \ldots, X_n]$. Then*

(a) $M_\delta(f + g) \leq \max(M_\delta(f), M_\delta(g))$

(b) $M_\delta(fg) \leq M_\delta(f) + M_\delta(g)$

Proof: Obvious. $\square$

For univariate polynomials we also introduce a weighted version of M_δ. This modification will be more appropriate for our purpose.

Definition: *Let $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K. Then for a polynomial $f(X) = \sum_{i=0}^n a_i X^i \in K[X]$, $a_n \neq 0$ we let*

$$\bar{M}_\delta(f) := \max\left(\left\{\frac{1}{n-i}(\delta(a_i) + (n-i-1)\delta(a_n)) \mid 0 \leq i \leq n-1\right\} \cup \{\delta(a_n)\}\right)$$

Furthermore we define $\bar{M}_\delta(0) := -\infty$.

Remark: $\bar{M}_\delta(f)$ is an element of the divisible hull $D(\Gamma)$ of Γ.

The next result yields a comparison of $M_\delta(f)$ and $\bar{M}_\delta(f)$

Proposition 2.11: *Let $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K. Then*

$$\bar{M}_\delta(f) \leq M_\delta(f)$$

for all $f \in K[X]$.

Proof: Let $f(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$. Immediately by the definition of $M_\delta(f)$ we get $\delta(a_n) \leq M_\delta(f)$. For $0 \leq i \leq n-1$ we obtain $\delta(a_i) + (n-i-1)\delta(a_n) \leq (n-i)M_\delta(f)$ and thus

$$\frac{1}{n-i}\left(\delta(a_i) + (n-i-1)\delta(a_n)\right) \leq M_\delta(f)$$

This proves the proposition. □

Let $v_2, v_3 : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the 2-adic and 3-adic valuation on the field $\mathbb{Q}$ of rational numbers. As we have seen before, the application $\delta(z) = -\min(v_2(z), v_3(z))$ yields a degree function $\delta : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{-\infty\}$. We let

$$\begin{aligned} f(X) &:= 6X^2 + X + \tfrac{1}{6} \\ g(X) &:= X^3 + X^2 + X + 1 \end{aligned}$$

Then one can easily see that $\bar{M}_\delta(f) = \bar{M}_\delta(g) = 0$ but $\bar{M}_\delta(f+g) = \frac{1}{3}$. Therefore the inequality $\bar{M}_\delta(f+g) \leq \max(\bar{M}_\delta(f), \bar{M}_\delta(g))$ is not true in general, in contrast to the estimate $M_\delta(f+g) \leq \max(M_\delta(f), M_\delta(g))$ which was stated in Lemma 2.10(a). However, part (b) of Lemma 2.10 remains valid for $\bar{M}_\delta$ as the next result shows.

Proposition 2.12: *Suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K and let $f, g \in K[X]$. Then*

$$\bar{M}_\delta(fg) \leq \bar{M}_\delta(f) + \bar{M}_\delta(g)$$

Proof: In the case $f = 0$ or $g = 0$ the assertion is obvious. Now suppose that $f, g \neq 0$ and let $f(X) = \sum_{i=0}^{n} a_i X^i$ and $g(X) = \sum_{j=0}^{m} b_j X^j$, $a_n, b_m \neq 0$. Let further $fg = \sum_{k=0}^{n+m} c_k X^k$. Then $c_k = \sum_{i+j=k} a_i b_j$. The leading coefficient of fg is $c_{n+m} = a_n b_m$ and thus $\delta(c_{n+m}) \leq \delta(a_n) + \delta(b_m) \leq \bar{M}_\delta(f) + \bar{M}_\delta(g)$. Now let $0 \leq k \leq n+m-1$. Then $\delta(c_k) \leq \delta(a_i b_j)$ for certain i, j such that $i + j = k$. Hence

$$\begin{aligned} \delta(c_k) + (n+m-k-1)\delta(c_{n+m}) &\leq \delta(a_i) + \delta(b_j) + (n+m-i-j-1)\delta(a_n b_m) \\ &\leq \delta(a_i) + (n-i-1)\delta(a_n) + (m-j)\delta(a_n) + \delta(b_j) + (m-j-1)\delta(b_m) + (n-1)\delta(b_m) \\ &\leq (n-i)\bar{M}_\delta(f) + (m-j)\delta(a_n) + (m-j)\bar{M}_\delta(g) + (n-i)\delta(b_m) \\ &\leq (n+m-k) \cdot (\bar{M}_\delta(f) + \bar{M}_\delta(g)) \end{aligned}$$

This yields

$$\frac{1}{n+m-k}(\delta(c_k) + (n+m-k-1)\delta(c_{n+m})) \leq \bar{M}_\delta(f) + \bar{M}_\delta(g)$$

and the proposition is proved. □

Proposition 2.13: *Assume that $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K and let $f, g \in K[X]$. Suppose that g is monic. Then*

$$\bar{M}_\delta(f) \leq \bar{M}_\delta(fg) + \bar{M}_\delta(g)$$

Proof: If $f = 0$ there is nothing to show. So we may assume that $f \neq 0$. Let $f(X) = \sum_{i=0}^{n} a_i X^i, g(X) = \sum_{j=0}^{m} b_j X^j$, $a_n \neq 0$, $b_m = 1$. Then $fg = \sum_{k=0}^{n+m} c_k X^k$ with $c_k = \sum_{i+j=k} a_i b_j$. In particular $c_{n+m} = a_n b_m = a_n$. Note that $\bar{M}_\delta(g) \geq 0$ since g is monic. Now we show by reverse induction on $\nu = n, n-1, \ldots, 1, 0$

$$\delta(a_\nu) + (n - \nu - 1)\delta(a_n) \leq (n - \nu) \cdot (\bar{M}_\delta(fg) + \bar{M}_\delta(g))$$

The case $\nu = n$ is obvious. Now let $\nu < n$. Then $c_{m+\nu} = \sum_{i=0}^{\ell} a_{\nu+i} b_{m-i}$ with $\ell = \min(n - \nu, m)$. As $b_m = 1$ we get

$$a_\nu = c_{m+\nu} - \sum_{i=1}^{\ell} a_{\nu+i} b_{m-i} \tag{1}$$

Immediately by the definition of $\bar{M}_\delta(fg)$ we get

$$\begin{aligned} \delta(c_{m+\nu}) + (n - \nu - 1)\delta(a_n) &= \delta(c_{m+\nu}) + (n + m - (\nu + m) - 1)\delta(c_{n+m}) \\ &\leq (n - \nu)\bar{M}_\delta(fg) \leq (n - \nu) \cdot (\bar{M}_\delta(fg) + \bar{M}_\delta(g)) \end{aligned} \tag{2}$$

Furthermore, for $1 \leq i \leq \ell$ we obtain by the induction hypothesis

$$\begin{aligned} \delta(a_{\nu+i} b_{m-i}) + (n - \nu - 1)\delta(a_n) &\leq \delta(a_{\nu+i}) + \delta(b_{m-i}) + (n - \nu - 1)\delta(a_n) \\ &\leq (n - (\nu + i)) \cdot (\bar{M}_\delta(fg) + \bar{M}_\delta(g)) + i\delta(a_n) + \delta(b_{m-i}) \end{aligned}$$

Since g is monic we get $\delta(b_{m-i}) \leq i\bar{M}_\delta(g)$. Furthermore, a_n is also the leading coefficient of fg and thus $\delta(a_n) \leq \bar{M}_\delta(fg)$. Altogether this yields

$$\delta(a_{\nu+i} b_{m-i}) + (n - \nu - 1)\delta(a_n) \leq (n - \nu) \cdot (\bar{M}_\delta(fg) + \bar{M}_\delta(g)) \tag{3}$$

Now by (1),(2) and (3) we finally get

$$\delta(a_\nu) + (n - \nu - 1)\delta(a_n) \leq (n - \nu) \cdot (\bar{M}_\delta(fg) + \bar{M}_\delta(g))$$

With this induction and the fact

$$\delta(a_n) = \delta(c_{n+m}) \leq \bar{M}_\delta(fg) \leq \bar{M}_\delta(fg) + \bar{M}_\delta(g)$$

the proposition is shown. $\square$

It is a well-known fact that the absolute value of a zero of a polynomial $f \in \mathbb{C}[X]$ can be bounded in terms of the coefficients of f. If $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, $a_n \neq 0$ and $z \in \mathbb{C}$ is a zero of f, then:

$$|z| \leq \frac{1}{|a_n|} \cdot \sum_{i=0}^{n} |a_i|$$

Then next theorem states a similar result for the case of a field with a degree function. This result is the main source for our bounds for H_k.

Theorem 2.14: *Let $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K. Let further $f \in K[X] \setminus K$ with leading coefficient $a \in K$ and assume that $z \in K$ is a zero of f. Then:*

$$\delta(az) \leq \bar{M}_\delta(f)$$

Proof: Let $f(X) = \sum_{i=0}^{n} a_i X^i, a_n \neq 0$. From $f(z) = 0$ we obtain $a_n z^n = -\sum_{i=0}^{n-1} a_i z^i$. Multiplication by a_n^{n-1} yields

$$(a_n z)^n = -\sum_{i=0}^{n-1} a_i a_n^{n-1} z^i$$

Hence

$$n \cdot \delta(a_n z) = \delta((a_n z)^n) = \delta\left(\sum_{i=0}^{n-1} a_i a_n^{n-1} z^i\right) \leq \max\{\delta(a_i a_n^{n-1} z^i) \mid (0 \leq i \leq n-1)\}$$

and therefore $n \cdot \delta(a_n z) \leq \delta\left(a_j a_n^{n-1} z^j\right)$ for some $j \in \{0, \ldots, n-1\}$. Thus we obtain

$$\begin{aligned} n \cdot \delta(a_n z) &\leq \delta(a_j) + \delta(a_n^{n-1-j}) + \delta((a_n z)^j) \\ &= \delta(a_j) + (n-j-1)\delta(a_n) + j \cdot \delta(a_n z) \leq (n-j)\bar{M}_\delta(f) + j \cdot \delta(a_n z) \end{aligned}$$

and hence $(n-j) \cdot \delta(a_n z) \leq (n-j) \cdot \bar{M}_\delta(f)$. Since $j < n$ this immediately yields the assertion $\delta(a_n z) \leq \bar{M}_\delta(f)$. □

Lemma 2.15: *Assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K and let $z_1, \ldots, z_n \in K$ and $f(X) := \prod_{i=1}^{n} (X - z_i)$. Then*

$$\bar{M}_\delta(f) = \max(\delta(z_1), \ldots, \delta(z_n), 0)$$

Proof: Let $\gamma := \max(\delta(z_1), \ldots, \delta(z_n), 0)$ and $f(X) = \sum_{i=0}^{n} a_i X^i$. Then

$$a_i = (-1)^{n-i} s_{n-i}(z_1, \ldots, z_n)$$

with $s_0, \ldots, s_n \in K[X_1, \ldots, X_n]$ the elementary symmetric functions. The leading coefficient of f is $a_n = 1$ and thus $\delta(a_n) = 0 \leq \gamma$. Furthermore

$$\delta(a_i) + (n-i-1)\delta(a_n) = \delta(a_i) = \delta(s_{n-i}(z_1, \ldots, z_n)) \leq (n-i)\gamma$$

Hence $\bar{M}_\delta(f) \leq \gamma$. On the other hand side we get $0 \leq \bar{M}_\delta(f)$ since f is monic and Theorem 2.14 yields $\delta(z_i) \leq \bar{M}_\delta(f)$. Thus also $\gamma \leq \bar{M}_\delta(f)$. This yields the result. □

We end this chapter with a few lemmas which will be needed later.

Lemma 2.16: *Let $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K and suppose that $f \in K[X]$ is of degree d. If the leading coefficient of f has a non-negative value under δ, then*

$$\delta(f(z)) \leq (d+1) \cdot \max(\bar{M}_\delta(f), \delta(z))$$

for each $z \in K$.

Proof: If $f = 0$ there is nothing to show. Let $f(X) = \sum_{i=0}^{d} a_i X^i$, $a_d \neq 0$. Then

$$\delta(a_d z^d) \leq \delta(a_d) + d\delta(z) \leq (d+1) \cdot \max(\bar{M}_\delta(f), \delta(z))$$

From the definition of $\bar{M}_\delta(f)$ and the fact $\delta(a_d) \geq 0$ we get

$$\delta(a_i) \leq (d-i)\bar{M}_\delta(f) - (d-i-1)\delta(a_d) \leq (d-i)\bar{M}_\delta(f)$$

for $0 \leq i \leq d-1$ and thus

$$\delta(a_i z^i) \leq d \cdot \max(\bar{M}_\delta(f), \delta(z)) \leq (d+1) \cdot \max(\bar{M}_\delta(f), \delta(z))$$

For the last estimate note that $\delta(a_d) \geq 0$ implies $\bar{M}_\delta(f) \geq 0$. This proves the lemma. □

Lemma 2.17: *Let $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on the field K and suppose that $f \in K[X_1, \ldots, X_n]$ is of degree d. Let further $z_1, \ldots, z_n \in K$. Then*

$$\delta(f(z_1, \ldots, z_n)) \leq M_\delta(f) + d \cdot \max(\delta(z_1), \ldots, \delta(z_n), 0)$$

Proof: Obvious

Lemma 2.18: *Suppose that $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K. Let $f \in K[X] \setminus \{0\}$ of degree n and assume that $a \in K^\times$ such that $\delta(a) \geq 0$. Let $g(X) := a^n f(a^{-1}X)$. Then:*

$$\bar{M}_\delta(g) \leq \bar{M}_\delta(f) + \delta(a)$$

Proof: Let $f(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$. Then $g(X) = \sum_{i=0}^{n} a_i a^{n-i} X^i$. The leading coefficient of g is a_n. As $\delta(a) \geq 0$ we get $\delta(a_n) \leq \bar{M}_\delta(f) \leq \bar{M}_\delta(f) + \delta(a)$ and for $0 \leq i \leq n-1$ we obtain

$$\begin{aligned}\delta(a_i a^{n-i}) + (n-i-1)\delta(a_n) &\leq \delta(a_i) + (n-i-1)\delta(a_n) + (n-i)\delta(a) \\ &\leq (n-i) \cdot (\bar{M}_\delta(f) + \delta(a))\end{aligned}$$

Hence

$$\frac{1}{n-i}(\delta(a_i a^{n-i}) + (n-i-1)\delta(a_n)) \leq \bar{M}_\delta(f) + \delta(a)$$

and we are done. □

Lemma 2.19: *Let k be a field and suppose that $\delta : k(X_1,\ldots,X_n) \longrightarrow \mathbb{Q} \cup \{-\infty\}$ is a degree function on $k(X_1,\ldots,X_n)$ such that $\delta(f) = \deg_{X_1,\ldots,X_n} f$ for all $f \in k[X_1,\ldots,X_n]$. Then*

$$\bar{M}_\delta(f) \leq \deg_{X_1,\ldots,X_n,X} f - \deg_X f + 1$$

for all $f \in k[X_1,\ldots,X_n,X] \backslash \{0\}$.

Proof: Let $r := \deg_{X_1,\ldots,X_n,X} f$ and $s := \deg_X f$. Then $f = \sum_{i=0}^{s} f_i X^i$, $f_s \neq 0$ and $\delta(f_i) = \deg_{X_1,\ldots,X_n} f_i \leq r - i$. Therefore $\delta(f_s) \leq r - s \leq r - s + 1$ and for $0 \leq i \leq s-1$ holds

$$\begin{aligned} \delta(f_i) + (s-i-1)\delta(f_s) &\leq (r-i) + (s-i-1)\cdot(r-s) \\ &= (r-s+1)\cdot(s-i) \end{aligned}$$

Hence $\bar{M}_\delta(f) \leq r - s + 1$. □

Lemma 2.20: *Let K be a field and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Assume that $\delta' : K(X) \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on $K(X)$ which extends δ and let $f \in K[X]$ be monic of degree $d > 0$. Then*

$$\delta'(f) \leq d \cdot \max(\bar{M}_\delta(f), \delta'(X))$$

Proof: Let $f(X) = \sum_{i=0}^{d} a_i X^i$, $a_d = 1$. By the definition of $\bar{M}_\delta(f)$ and the fact $a_d = 1$ we get

$$\delta(a_i) = \delta(a_i) + (d-i-1)\delta(a_d) \leq (d-i)\bar{M}_\delta(f) \qquad (0 \leq i \leq d-1)$$

A direct inspection shows that the estimate above is also valid for $i = d$. Therefore, for all i we get

$$\delta'(a_i X^i) \leq \delta(a_i) + i\delta'(X) \leq (d-i)\bar{M}_\delta(f) + i\delta'(X) \leq d \cdot \max(\bar{M}_\delta(f), \delta'(X))$$

and hence also $\delta'(f) \leq d \cdot \max(\bar{M}_\delta(f), \delta'(X))$ □

Chapter 3

Stable degree functions

If L/K is a Galois extension and $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ a degree function on L then also $\delta \circ \sigma$ is a degree function for all $\sigma \in \mathrm{Gal}(L/K)$. Thus $\mathrm{Gal}(L/K)$ acts on the set of all degree functions on L. In this chapter we study properties of those degree functions which are fixed under this action.

Let K be a field and denote its algebraic closure by $\bar{K}$. We recall that two elements $x, y \in \bar{K}$ are called conjugate over K if there is a K-automorphism σ of $\bar{K}$ such that $\sigma(x) = y$. It is well-known that two elements $x, y \in \bar{K}$ are conjugate over K iff $\mathrm{Irr}(x, K) = \mathrm{Irr}(y, K)$. Note that if L/K is an algebraic extension and $x, y \in L$ are conjugate over K, then there is not necessarily a K-automorphism σ of L such that $\sigma(x) = y$ unless the extension L/K is normal. The set of K-automorphisms of an extension field L of K we denote by $\mathrm{Gal}(L/K)$, also in the case that L/K is not a Galois extension.

Definition: *Let R be an integral domain and assume that L is an algebraic extension of $K := \mathrm{Quot}(R)$. A degree function $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ on L is called R-stable if:*

(i) $\delta(a) \geq 0$ *for all* $a \in R \setminus \{0\}$

(ii) *If* $x, y \in L$ *are conjugate over* K *then* $\delta(x) = \delta(y)$

Proposition 3.1: *Let L/K be a normal algebraic extension and assume that R is a subring of K such that $K = \mathrm{Quot}(R)$. Furthermore let $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on L such that $\delta(a) \geq 0$ for all $a \in R \setminus \{0\}$. Then there is a degree function $\delta' : L \longrightarrow \Gamma \cup \{-\infty\}$ such that*

(a) δ' *is R-stable*

(b) $\delta(z) \leq \delta'(z)$ *for all* $z \in L$

(c) $\delta'\big|_K = \delta\big|_K$

Proof: For $z \in L$ we define

$$\delta'(z) := \max\{\delta(\sigma(z)) | \ \sigma \in \mathrm{Gal}(L/K)\}$$

Since an element $z \in L$ has only finitely many conjugates the set $\{\sigma(z) | \ \sigma \in \mathrm{Gal}(L/K)\}$ is finite and thus δ' is well-defined. Obviously $\delta'(x) = -\infty$ iff $x = 0$. Now let $x, y \in L$. Then $\delta'(x+y) = \delta(\sigma(x+y))$ for some $\sigma \in \mathrm{Gal}(L/K)$. Thus

$$\delta'(x+y) = \delta(\sigma(x) + \sigma(y)) \leq \max(\delta(\sigma(x)), \delta(\sigma(y))) \leq \max(\delta'(x), \delta'(y))$$

In a similar way one can prove that $\delta'(xy) \leq \delta'(x) + \delta'(y)$. If n is a natural number and $x \in L$ then

$$\delta'(x^n) = \max\{\delta(\sigma(x^n)) | \ \sigma \in \mathrm{Gal}(L/K)\} = n \cdot \max\{\delta(\sigma(x)) | \ \sigma \in \mathrm{Gal}(L/K)\} = n \cdot \delta'(x)$$

Thus $\delta' : L \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on L. Assertion (b) follows immediately from the definition of δ' and since $\mathrm{Gal}(L/K)$ acts trivially on K, δ and δ' coincide on K. In particular we obtain $\delta'(a) \geq 0$ for all $a \in R \backslash \{0\}$. Obviously two conjugate elements have the same value under the degree function δ' and thus δ' is R-stable □

Corollary 3.2: *Assume that k is a field and let n be a natural number. Then there is a $k[X_1, \ldots, X_n]$-stable degree function $\delta : \overline{k(X_1, \ldots, X_n)} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ such that $\delta(f) = \deg f$ for every polynomial $f \in k[X_1, \ldots, X_n]$.*

Proof: By Proposition 2.1 there is a degree function

$$\delta : \overline{k(X_1, \ldots, X_n)} \longrightarrow \mathbb{Q} \cup \{-\infty\}$$

such that $\delta(f) = \deg f$ for every polynomial $f \in k[X_1, \ldots, X_n]$. In particular $\delta(f) \geq 0$ if $f \in k[X_1, \ldots, X_n] \backslash \{0\}$. Now Proposition 3.1 immediately yields the result. □

Proposition 3.3: *Let R be an integral domain which is integrally closed in its field of fractions K and assume that L is a normal algebraic extension of K. Let furthermore $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on L. Then $\delta(z) \geq 0$ for all $z \in L^\times$ which are integral over R.*

Proof: Assume that $z \in L^\times$ is integral over R and let f be its irreducible polynomial over K. As R is integrally closed in K we get $f \in R[X]$. Since L/K is normal f splits into linear factors in $L[X]$, i.e.,

$$f(X) = \prod_{i=1}^{n} (X - z_i)$$

for certain $z_1, \ldots, z_n \in L$, $z_1 = z$. The elements $z_1, \ldots, z_n$ are conjugate over K and therefore $\delta(z_1) = \ldots = \delta(z_n)$. Since $f(0) = (-1)^n \prod_{i=1}^{n} z_i \in R \backslash \{0\}$ we obtain

$$0 \leq \delta(f(0)) = \delta\left(\prod_{i=1}^{n} z_i\right) \leq \sum_{i=1}^{n} \delta(z_i) = n \cdot \delta(z)$$

This finally implies $\delta(z) \geq 0$. □

This result has an important consequence:

Corollary 3.4: *Let R be an integral domain which is integrally closed in its field of fractions K and assume that L is a normal algebraic extension of K. Let further $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on L. Suppose that F is an intermediate field of the extension L/K and let S be the integral closure of R in F. Then δ is S-stable.*

Proof: If $x, y \in L$ are conjugate over F they are also conjugate over K and thus $\delta(x) = \delta(y)$. By Proposition 3.3 we obtain $\delta(a) \geq 0$ for all $a \in S \backslash \{0\}$. Thus δ is S-stable. □

Theorem 3.5: *Let R be an integral domain which is integrally closed in its field of fractions K and assume that L is a normal algebraic extension of K. Let $\vartheta \in L$ be separable over K and assume that it is integral over R. Let $[K(\vartheta) : K] = n$ and denote by d the discriminant of* $\mathrm{Irr}(\vartheta, K)$. *Let further $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on L. Then:*

(a) $d \in R \backslash \{0\}$

(b) $\delta(d) \leq n(n-1)\delta(\vartheta)$

(c) *For every element $z \in K(\vartheta)$ which is integral over R there are $a_0, \ldots, a_{n-1} \in R$ such that $d \cdot z = \sum_{i=0}^{n-1} a_i \vartheta^i$ and $\delta(a_i) \leq n(n-1)\delta(\vartheta) + \delta(z) \quad (0 \leq i \leq n-1)$*

Proof: Let $\sigma_1, \ldots, \sigma_n$ be the different K-embeddings of $K(\vartheta)$ into $\bar{K}$, $\sigma_1 = \mathrm{id}$. We define $\vartheta_i := \sigma_i(\vartheta)$ $(1 \leq i \leq n)$ and let A be the $n \times n$ matrix

$$A := \begin{pmatrix} 1 & \vartheta_1 & \vartheta_1^2 & \ldots & \vartheta_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \vartheta_n & \vartheta_n^2 & \ldots & \vartheta_n^{n-1} \end{pmatrix}$$

It is well-known that $d = (\det A)^2$. The matrix A is a Vandermonde matrix and thus

$$\det A = \prod_{j=2}^{n} \prod_{i=1}^{j-1} (\vartheta_j - \vartheta_i)$$

Since ϑ is separable over K the conjugates $\vartheta_1, \ldots, \vartheta_n$ of ϑ are mutually distinct and thus $\det A \neq 0$. Furthermore $\sigma_1, \ldots, \sigma_n$ permute $\vartheta_1, \ldots, \vartheta_n$. Thus $d = (\det A)^2$ is fixed under $\sigma_1, \ldots, \sigma_n$ and therefore we obtain $d \in K$. As ϑ is integral over R, so are $\vartheta_1, \ldots, \vartheta_n$. Hence d is integral over R, and since R is integrally closed in K we obtain $d \in R$. Now

$$(1) \qquad \delta(\det A) \leq \sum_{j=2}^{n} \sum_{i=1}^{j-1} \delta(\vartheta_j - \vartheta_i) \leq \tfrac{1}{2} n(n-1)\delta(\vartheta)$$

This implies $\delta(d) = 2 \cdot \delta(\det A) \leq n(n-1)\delta(\vartheta)$.

It remains to show (c). Let $z \in K(\vartheta)$ be integral over R. If $z = 0$ let $a_0 = \ldots = a_{n-1} = 0$. Now assume that $z \neq 0$. Since z is integral over R also $z_1 := \sigma_1(z), \ldots, z_n := \sigma_n(z)$ are integral. As $1, \vartheta, \ldots, \vartheta^{n-1}$ is a K-basis for $K(\vartheta)$ there are $b_0, \ldots, b_{n-1} \in K$ such that $z = \sum_{i=0}^{n-1} b_i \vartheta^i$. Apply the embeddings $\sigma_1, \ldots, \sigma_n$ to obtain

$$\begin{aligned} z_1 &= b_0 + b_1\vartheta_1 + \ldots + b_{n-1}\vartheta_1^{n-1} \\ &\vdots \\ z_n &= b_0 + b_1\vartheta_n + \ldots + b_{n-1}\vartheta_n^{n-1} \end{aligned}$$

For $i = 0, \ldots, n-1$ let A_i be the matrix which is obtained from A by replacing the $(i+1)$-th column by $z_1, \ldots, z_n$. Then Cramer's rule yields

$$b_i = \frac{\det A_i}{\det A} = \frac{\det A \cdot \det A_i}{d} \qquad (0 \le i \le n-1)$$

We define $a_i := d \cdot b_i = \det A \cdot \det A_i$ $(0 \le i \le n-1)$. Then $d \cdot z = \sum_{i=0}^{n-1} a_i \vartheta^i$.
Since the entries of the matrices A_i are integral over R, also $a_0, \ldots, a_{n-1}$ are integral over R. On the other hand side $a_i = d \cdot b_i \in K$ $(0 \le i \le n-1)$ and thus $a_i \in R$ $(0 \le i \le n-1)$ since R is integrally closed in K.
Finally we prove the stated bounds for $\delta(a_i)$. From Lemma 2.5(b) we obtain

$$\delta(\det A_i) \le \sum_{\substack{j=0 \\ j \ne i}}^{n-1} j\delta(\vartheta) + \delta(z)$$

and hence $\delta(\det A_i) \le \frac{1}{2}n(n-1)\delta(\vartheta) + \delta(z)$ since $\delta(\vartheta) \ge 0$ by Proposition 3.3. Together with (1) this yields the assertion. □

Theorem 3.6: *Let R be an integral domain which is integrally closed in its field of fractions K and assume that L is a simple normal extension of K. Let $\vartheta \in L$ be a primitive element for the extension L/K and assume that ϑ is integral over R. Let further $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on L and assume that F is an intermediate field of the extension L/K. Then there are $r \in \mathbb{N}$ and elements $z_1, \ldots, z_r \in F$ such that:*

(a) $F = K(z_1, \ldots, z_r)$
(b) $z_1, \ldots, z_r$ *are integral over* R
(c) $2^r \le [F : K]$
(d) $\delta(z_i) \le [L : F] \cdot \delta(\vartheta) \qquad (1 \le i \le r)$

Proof: Let $f(X) = \sum_{i=0}^m a_i X^i, a_m = 1$ be the irreducible polynomial of ϑ over F. By S we denote the integral closure of R in F. Since ϑ is integral over R it is also integral over S. Hence $f \in S[X]$. Now let $E := K(a_0, \ldots, a_{m-1})$. Then $E \subset F$ and $f \in E[X]$. Thus f is also the irreducible polynomial of ϑ over E and therefore

$$[L : E] = \deg f = m = [L : F]$$

As $E \subset F$ this yields $E = F$. Since L/K is normal also L/F is normal. Therefore f splits over L into linear factors:

$$f(X) = \prod_{i=1}^{m}(X - \vartheta_i)$$

The elements $\vartheta_1, \ldots, \vartheta_m$ are conjugate over F and hence over K. Thus $\delta(\vartheta_i) = \delta(\vartheta)$ $(1 \leq i \leq m)$. From $a_i = (-1)^{m-i}s_{m-i}(\vartheta_1, \ldots, \vartheta_m)$ we obtain

$$\delta(a_i) \leq (m-i)\delta(\vartheta) \leq m\delta(\vartheta) = [L : F] \cdot \delta(\vartheta)$$

because $\delta(\vartheta) \geq 0$ by Proposition 3.3.

Finally we choose a minimal subset $\{z_1, \ldots, z_r\}$ of $\{a_0, \ldots, a_m\}$ which still generates F/K. Then all the extensions $K(z_1, \ldots, z_i)/K(z_1, \ldots, z_{i-1})$ are proper and thus

$$[F : K] = \prod_{i=1}^{r}[K(z_1, \ldots, z_i) : K(z_1, \ldots, z_{i-1})] \geq 2^r$$

This proves the theorem. $\square$

Corollary 3.7: *Let R be an integral domain which is integrally closed in its field of fractions K and assume that* $\mathrm{char}(K) \neq 2$. *Let L be a simple normal extension of K with a primitive element $\vartheta \in L$ and suppose that ϑ is integral over R. Let further $\delta : L \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on L and assume that F is an intermediate field of the extension L/K such that $[F : K] = 2$. Then there is an element $z \in R$ such that $F = K(\sqrt{z})$ and $\delta(z) \leq [L : K] \cdot \delta(\vartheta)$.*

Proof: By Theorem 3.6 there is an element $x \in F$ which is integral over R such that $F = K(x)$ and $\delta(x) \leq [L : F] \cdot \delta(\vartheta)$. Let

$$\mathrm{Irr}(x, K) = X^2 + aX + b$$

As R is integrally closed in K we get $\mathrm{Irr}(x, K) \in R[X]$ and thus $a, b \in R$. In $F[X]$ the polynomial $\mathrm{Irr}(x, K)$ splits into $\mathrm{Irr}(x, K) = (X - x)(X - y)$ for some $y \in F$. Since the zeroes x, y are conjugate over K we get $\delta(y) = \delta(x)$. Let $z := a^2 - 4b \in R$. Then $x, y = \frac{1}{2}(-a \pm \sqrt{z})$ yields $F = K(\sqrt{z})$. From $-a = x + y$ and $b = xy$ we immediately obtain

$$\delta(z) \leq 2\delta(x) \leq 2 \cdot [L : F] \cdot \delta(\vartheta) = [L : K] \cdot \delta(\vartheta)$$

and the corollary is proved. $\square$

Remark:
As the following easy example shows, the bound given in Corollary 3.7 is optimal.

Fix a natural number $n \in \mathbb{N}$ and let $R := \mathbb{C}[X]$ and $K := \mathbb{C}(X)$. Choose an element $\vartheta \in \bar{K}$ such that $\vartheta^{2n} = X$ and let $L := K(\vartheta)$ and $F := K(\sqrt{X})$. As $\mathbb{C}$ contains all roots of unity L/K is normal. Let $\delta : \bar{K} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$ such that $\delta(f) = \deg f$ for all $f \in R = \mathbb{C}[X]$ according to Corollary 3.2. Then $\delta(\vartheta) = \frac{1}{2n}$. If $F = K(\sqrt{f})$ for some $f \in R = \mathbb{C}[X]$ then f is not a constant. Hence

$$\delta(f) = \deg f \geq 1 = [L : K] \cdot \delta(\vartheta)$$

Chapter 4

A remark on the Shape Lemma

The Shape Lemma occurred the first time in a paper of Gianni and Mora in 1989 (cf. [16]). It is a generalization of the Primitive Element Theorem and it states that for a zero-dimensional ideal $\mathfrak{a}$ of the polynomial ring $K[X_1, \ldots, X_n]$ over a perfect field K the radical of $\mathfrak{a}$ is of the form

$$\sqrt{\mathfrak{a}} = (g(X_n), X_1 - g_1(X_n), \ldots, X_{n-1} - g_{n-1}(X_n))$$

for certain polynomials $g, g_1, \ldots, g_{n-1} \in K[X_n]$, provided that the set $\mathrm{V}(\mathfrak{a})$ of zeroes of $\mathfrak{a}$ is in general position w.r.t. X_n, i.e., that the projection map

$$\begin{aligned} \pi : \mathrm{V}(\mathfrak{a}) &\longrightarrow \bar{K} \\ (x_1, \ldots, x_n) &\mapsto x_n \end{aligned}$$

is injective. Moreover, the polynomials $g(X_n), X_1 - g_1(X_n), \ldots, X_{n-1} - g_{n-1}(X_n)$ form a Gröbner basis for $\sqrt{\mathfrak{a}}$ w.r.t. the lexicographical term order such that $X_n < \ldots < X_1$.

A simple proof of the Shape Lemma can be found in [6]. From this proof one can easily see that $\deg g_i < \deg g = \#\mathrm{V}(\mathfrak{a})$ $(1 \leq i \leq n-1)$. If d is a bound for the degrees of a set of generators of $\mathfrak{a}$ we have $\#\mathrm{V}(\mathfrak{a}) \leq d^n$ by the affine Bezout inequality and hence also $\deg g \leq d^n$.

In this chapter we are concerned with the coefficients of the polynomials $g, g_1, \ldots, g_{n-1}$. We will present bounds for the values of the coefficients w.r.t. a degree function on the field K. In the next chapter we will need this bounds in order to compare N_k and H_k for a formally real field k.

Theorem 4.1: *Let R be an integral domain and $K := \mathrm{Quot}(R)$ and suppose that $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further $f, f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$, $q_1, \ldots, q_m \in K[X_1, \ldots, X_n]$, $d_1, d_2 \in \mathbb{N}_{\geq 1}$, $\gamma \in \Gamma_{\geq 0}$ such that $\deg f_i \leq d_1$, $\deg q_i \leq d_2$, $M_\delta(f_i) \leq \gamma$ and assume that $f = \sum_{i=1}^m q_i f_i$. Then there are $p_1, \ldots, p_m \in R[X_1, \ldots, X_n]$ and $a \in R \backslash \{0\}$ such that*

(a) $af = \sum_{i=1}^m p_i f_i$

(b) $\deg p_i \leq \deg q_i \qquad (1 \leq i \leq m)$

(c) $\delta(a) \leq 2 \cdot (d_1 + d_2)^n \cdot \gamma$

(d) $M_\delta(p_i) \leq 2 \cdot (d_1 + d_2)^n \cdot \gamma + M_\delta(f)$

Proof: Let be:

$$\begin{array}{llll} P_j & (1 \leq j \leq N_1) & \text{the terms } \prod_{i=1}^n X_i^{r_i} & \text{of degree } \leq d_1 \\ Q_j & (1 \leq j \leq N_2) & \text{the terms } \prod_{i=1}^n X_i^{r_i} & \text{of degree } \leq d_2 \\ R_j & (1 \leq j \leq N_3) & \text{the terms } \prod_{i=1}^n X_i^{r_i} & \text{of degree } \leq d_1 + d_2 \end{array}$$

Then

$$N_3 = \binom{n + d_1 + d_2}{n} \leq 2 \cdot (d_1 + d_2)^n \tag{1}$$

Now write

$$\begin{array}{lllll} f_i & = & \sum_{j=1}^{N_1} a_{ij} P_j & \text{for certain } a_{ij} \in R & (1 \leq i \leq m,\ 1 \leq j \leq N_1) \\ q_i & = & \sum_{j=1}^{N_2} b_{ij} Q_j & \text{for certain } b_{ij} \in K & (1 \leq i \leq m,\ 1 \leq j \leq N_2) \\ f & = & \sum_{j=1}^{N_3} c_j R_j & \text{for certain } c_j \in R & (1 \leq j \leq N_3) \end{array}$$

and let $I_j := \{(\nu, \mu) |\ 1 \leq \nu \leq N_1,\ 1 \leq \mu \leq N_2,\ P_\nu \cdot Q_\mu = R_j\}$ $(1 \leq j \leq N_3)$. Then

$$\begin{aligned} \sum_{j=1}^{N_3} c_j R_j = f = \sum_{i=1}^m q_i f_i &= \sum_{i=1}^m \left(\sum_{\mu=1}^{N_2} b_{i\mu} Q_\mu \right) \cdot \left(\sum_{\nu=1}^{N_1} a_{i\nu} P_\nu \right) \\ &= \sum_{j=1}^{N_3} \left(\sum_{i=1}^m \sum_{(\nu,\mu) \in I_j} a_{i\nu} b_{i\mu} \right) \cdot R_j \end{aligned}$$

Comparing the coefficients we obtain

$$\sum_{i=1}^m \sum_{(\nu,\mu) \in I_j} a_{i\nu} \cdot b_{i\mu} = c_j \quad (1 \leq j \leq N_3) \tag{2}$$

Hence $(b_{i\mu})_{i,\mu}$ is a solution of the system

$$\sum_{i=1}^m \sum_{(\nu,\mu) \in I_j} a_{i\nu} \cdot x_{i\mu} = c_j \qquad (1 \leq j \leq N_3) \tag{3}$$

(3) is a system of N_3 linear equations in the $m \cdot N_2$ indeterminates $x_{i\mu}$. The entries of its coefficient matrix are either zero or of the form $a_{i\nu}$. Note that for given j, μ there is at most one ν such that $(\nu, \mu) \in I_j$.

According to Corollary 2.9 there are $z_{i\mu} \in R$ $(1 \le i \le m,\ 1 \le \mu \le N_2)$ and $a \in R\backslash\{0\}$ such that $(z_{i\mu}a^{-1})_{i,\mu}$ is a solution of (3), $z_{i\mu} = 0$ whenever $b_{i\mu} = 0$ and $\delta(a) \le N_3 \cdot \gamma$ and $\delta(z_{i\mu}) \le N_3 \cdot \gamma + M_\delta(f)$. Now define

$$p_i := \sum_{\mu=1}^{N_2} z_{i\mu} Q_\mu \qquad (1 \le i \le m)$$

In the polynomial p_i only those terms Q_μ occur which also occur in q_i. Thus $\deg p_i \le \deg q_i$. Furthermore

$$M_\delta(p_i) \le \max\{\ \delta(z_{i\mu}) \mid i, \mu\ \} \le N_3 \cdot \gamma + M_\delta(f)$$

Finally, an elementary computation yields $af = \sum_{i=1}^{m} p_i f_i$ and the theorem is proved. □

Corollary 4.2: *Let R be an integral domain and $K := \mathrm{Quot}(R)$ and assume that $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further $f, f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$, $d \in \mathbb{N}$, $d \ge 3$, $\gamma \in \Gamma_{\ge 0}$ such that $\deg f_i \le d$, $M_\delta(f_i) \le \gamma$ and suppose that f vanishes on $\mathrm{V}(f_1, \ldots, f_m)$. Then there are $t \in \mathbb{N}, a \in R\backslash\{0\}$ and $q_1, \ldots, q_m \in R[X_1, \ldots, X_n]$ such that*

(a) $af^t = \sum_{i=1}^{m} q_i f_i$

(b) $t \le d^n$

(c) $\deg(q_i f_i) \le d^n(1 + \deg f)$

(d) $\delta(a) \le 2d^{n^2}(2 + \deg f)^n \gamma$

(e) $M_\delta(q_i) \le 2d^{n^2}(2 + \deg f)^n \gamma + M_\delta(f)$

Proof: By the effective Nullstellensatz we obtain

$$f^t = \sum_{i=1}^{m} p_i f_i$$

for certain $t \in \mathbb{N}, p_1, \ldots, p_m \in K[X_1, \ldots, X_n]$ such that $t \le d^n$ and $\deg(p_i f_i) \le d^n(1 + \deg f)$. An immediate application of Theorem 4.1 yields the result. □

Theorem 4.3: *Let R be an integral domain with $K := \mathrm{Quot}(R)$ and assume that K is perfect. Suppose that $\delta\colon K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K and let $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$, $d \in \mathbb{N}$, $d \ge 3$, $\gamma \in \Gamma_{\ge 0}$ such that $\deg f_i \le d$, $M_\delta(f_i) \le \gamma$. Let further $\mathfrak{a}$ be the ideal generated by $f_1, \ldots, f_m$ in $K[X_1, \ldots, X_n]$ and assume that $\mathfrak{a}$ is zero-dimensional. Then there is a non-zero polynomial $f \in \mathfrak{a} \cap R[X_n]$ such that*

(a) $\deg f \le d^{2n}$

(b) $M_\delta(f) \le 2d^{2n^2} \cdot \gamma$

Proof: Since $\mathfrak{a}$ is zero-dimensional $\mathrm{V}(\mathfrak{a})$ is finite. Let $x_1, \ldots, x_r \in \bar{K}$ be the n-th coordinates of the zeroes of $\mathfrak{a}$ counted without multiplicity. Then the affine Bezout inequality yields $r \leq \#\mathrm{V}(\mathfrak{a}) \leq d^n$. Let $g := \prod_{i=1}^{r}(X_n - x_i)$. The absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K acts on $\mathrm{V}(\mathfrak{a})$ and hence on the set $\{x_1, \ldots, x_r\}$. Therefore the coefficients of g are fixed under all K-automorphisms of $\bar{K}$ and thus $g \in K[X_n]$, because K is assumed to be perfect.

Obviously g vanishes on $\mathrm{V}(\mathfrak{a})$ and thus the effective Nullstellensatz yields

$$g^s = \sum_{i=1}^{m} q_i f_i$$

for certain $s \in \mathbb{N}, q_1, \ldots, q_m \in K[X_1, \ldots, X_n]$ such that $s \leq d^n$ and

$$\deg(q_i f_i) \leq (1 + \deg g) d^n \leq (d^n + 1) d^n$$

Now we proceed in a similar manner as in the proof of Theorem 4.1. Let be:

$$\begin{array}{llll} P_j & (1 \leq j \leq N_1) & \text{the terms } \prod_{i=1}^{n} X_i^{r_i} & \text{of degree } \leq d \\ Q_j & (1 \leq j \leq N_2) & \text{the terms } \prod_{i=1}^{n} X_i^{r_i} & \text{of degree } \leq d^n \cdot (d^n + 1) \\ R_j & (1 \leq j \leq N_3) & \text{the terms } \prod_{i=1}^{n} X_i^{r_i} & \text{of degree } \leq d + d^n \cdot (d^n + 1) \end{array}$$

Then

$$N_3 = \binom{n + d + d^n(d^n + 1)}{n} = \frac{1}{n!} \cdot \prod_{i=1}^{n} (d + d^n(d^n + 1) + i)$$

As $d \geq 3$ we get $d + d^n(d^n + 1) + i \leq 2d^{2n}$ and hence

$$N_3 \leq \frac{2^n}{n!} \cdot d^{2n^2} \leq 2d^{2n^2} \tag{1}$$

Now write

$$\begin{array}{rcllll} f_i & = & \sum_{j=1}^{N_1} a_{ij} P_j & \text{for certain} & a_{ij} \in R & (1 \leq i \leq m,\ 1 \leq j \leq N_1) \\ q_i & = & \sum_{j=1}^{N_2} b_{ij} Q_j & \text{for certain} & b_{ij} \in K & (1 \leq i \leq m,\ 1 \leq j \leq N_2) \\ g^s & = & \sum_{j=1}^{N_3} c_j R_j & \text{for certain} & c_j \in K & (1 \leq j \leq N_3) \end{array}$$

and let $I_j := \{(\nu, \mu) |\ 1 \leq \nu \leq N_1,\ 1 \leq \mu \leq N_2,\ P_\nu \cdot Q_\mu = R_j\}$ $(1 \leq j \leq N_3)$. Then

$$\begin{aligned} \sum_{j=1}^{N_3} c_j R_j = g^s = \sum_{i=1}^{m} q_i f_i &= \sum_{i=1}^{m} \left(\sum_{\mu=1}^{N_2} b_{i\mu} Q_\mu \right) \cdot \left(\sum_{\nu=1}^{N_1} a_{i\nu} P_\nu \right) \\ &= \sum_{j=1}^{N_3} \left(\sum_{i=1}^{m} \sum_{(\nu,\mu) \in I_j} a_{i\nu} b_{i\mu} \right) \cdot R_j \end{aligned}$$

Comparing the coefficients we obtain

$$\sum_{i=1}^{m} \sum_{(\nu,\mu)\in I_j} a_{i\nu} \cdot b_{i\mu} = c_j \quad (1 \leq j \leq N_3) \tag{2}$$

In contrast to the situation in the proof of Theorem 4.1 we do not know the elements c_j. Hence Proposition 2.8 is not applicable now and a more careful inspection of the situation is necessary. We let

$$I := \{\ j \mid 1 \leq j \leq N_3,\ R_j \notin K[X_n] \text{ or } \deg R_j > d^{2n}\ \}$$

Since $\deg g^s = s \cdot \deg g \leq d^{2n}$ and $g \in K[X_n]$ we get $c_j = 0$ whenever $j \in I$. As $g \neq 0$ there is some index ℓ such that $c_\ell \neq 0$.
Now consider the system

$$\begin{aligned} \sum_{i=1}^{m} \sum_{(\nu,\mu)\in I_j} a_{i\nu} \cdot x_{i\mu} &= 0 \qquad (j \in I) \\ \sum_{i=1}^{m} \sum_{(\nu,\mu)\in I_l} a_{i\nu} \cdot x_{i\mu} &= 1 \end{aligned} \tag{3}$$

Immediately from (2) one can see that $(c_\ell^{-1} b_{i\mu})_{i,\mu}$ is a solution of (3). By Proposition 2.8 there are $z_{i\mu} \in R$ $(1 \leq i \leq m,\ 1 \leq \mu \leq N_2)$ and $z \in R \backslash \{0\}$ such that $(z_{i\mu} z^{-1})_{i,\mu}$ is a solution of (3) and $\delta(z_{i\mu}) \leq (N_3 - 1) \cdot \gamma$. Now let

$$w_j := \sum_{i=1}^{m} \sum_{(\nu,\mu)\in I_j} a_{i\nu} \cdot z_{i\mu} \in R \quad (1 \leq j \leq N_3)$$

Then $w_\ell = z \neq 0$ and $w_j = 0$ for $j \in I$. Furthermore $\delta(z_{i\mu}) \leq (N_3 - 1) \cdot \gamma$ yields $\delta(w_j) \leq N_3 \cdot \gamma$. We define

$$f := \sum_{j=1}^{N_3} w_j \cdot R_j = \sum_{j \notin I} w_j \cdot R_j \tag{4}$$

Then $M_\delta(f) \leq N_3 \cdot \gamma \leq 2d^{2n^2} \cdot \gamma$ by (1). From the definition of the set I we obtain $f \in R[X_n]$ and $\deg f \leq d^{2n}$. Furthermore $w_\ell = z \neq 0$ implies $f \neq 0$. If we define

$$p_i := \sum_{\mu=1}^{N_2} z_{i\mu} Q_\mu \qquad (1 \leq i \leq m)$$

then from the construction we obtain $f = \sum_{i=1}^{m} p_i f_i$ and therefore $f \in \mathfrak{a}$. $\square$

The next theorem is the version of the Shape Lemma we were looking for.

Theorem 4.4: *Let R be an integral domain which is integrally closed in $K := \mathrm{Quot}(R)$ and assume that K is perfect. Let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$ and suppose that $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$, $d \in \mathbb{N}$, $\gamma \in \Gamma_{\geq 0}$, $\deg f_i \leq d$, $M_\delta(f_i) \leq \gamma$. Let further $\mathfrak{a}$ be the ideal generated by $f_1, \ldots, f_m$ in $K[X_1, \ldots, X_n]$ and assume that $\mathfrak{a}$ is zero-dimensional and in general position w.r.t. X_n. Then there are $a_1, \ldots, a_{n-1} \in R\backslash\{0\}, g, g_1, \ldots, g_{n-1} \in R[X]$ such that:*

(a) $\sqrt{\mathfrak{a}} = (g(X_n), a_1X_1 - g_1(X_n), \ldots, a_{n-1}X_{n-1} - g_{n-1}(X_n))$

(b) *g has only simple zeroes and the leading coefficient of g is a square*

(c) $\deg g_i < \deg g = \#\mathrm{V}(\mathfrak{a}) \leq d^n$

(d) $M_\delta(g) \leq 2(d^n + 1)d^{2n^2}\gamma$

(e) $M_\delta(g_i) \leq 2d^{2n^2+2n}\gamma$

(f) $\delta(a_i) \leq 2d^{2n^2+2n}\gamma$

Proof: By Theorem 4.3 there are non-zero polynomials $f_i \in \mathfrak{a} \cap R[X_i]$ $(1 \leq i \leq n)$ such that $M_\delta(f_i) \leq 2d^{2n^2}\gamma$. Let $b_1, \ldots, b_n \in R$ be their leading coefficients. Then $\delta(b_i) \leq M_\delta(f_i) \leq 2d^{2n^2}\gamma$.

As $\mathfrak{a}$ is zero-dimensional, $\mathrm{V}(\mathfrak{a})$ is finite. Let $\mathrm{V}(\mathfrak{a}) = \{x_1, \ldots, x_r\} \subset \bar{K}^n$. Then $r \leq d^n$ by the affine Bezout inequality. Denote the n-th coordinates of $x_1, \ldots, x_r$ by $y_1, \ldots, y_r$. Then $y_1, \ldots, y_r$ are mutually distinct, because $\mathrm{V}(\mathfrak{a})$ is in general position w.r.t. X_n by assumption. As $f_n \in \mathfrak{a}$ we get $f_n(y_i) = 0$ $(1 \leq i \leq r)$. Thus $b_ny_1, \ldots, b_ny_r$ are integral over R and furthermore

$$\delta(b_ny_i) \leq \bar{M}_\delta(f_n) \leq M_\delta(f_n) \leq 2d^{2n^2}\gamma \tag{1}$$

by Proposition 2.11 and Theorem 2.14. The absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K acts on $\mathrm{V}(\mathfrak{a})$ and hence on the set $\{y_1, \ldots, y_r\}$ of n-th coordinates of the zeroes of $\mathfrak{a}$. Thus the coefficients of the polynomial

$$h(X_n) := \prod_{i=1}^{r}(X_n - y_i)$$

are fixed under $\mathrm{Gal}(\bar{K}/K)$ and hence $h \in K[X_n]$, since K is perfect. Choose $s \in \mathbb{N}$ such that $r \leq 2s \leq r + 1$. Then the coefficients of the polynomial $g = b_n^{2s} \cdot h \in K[X_n]$ are integral over R and hence $g \in R[X_n]$ as R is integrally closed in K. The leading coefficient of g is b_n^{2s} which is obviously a square. Since g vanishes on $\mathrm{V}(\mathfrak{a})$ by construction, Hilbert's Nullstellensatz yields $g \in \sqrt{\mathfrak{a}}$. Furthermore $M_\delta(g) \leq \delta(b_n) + \sum_{i=1}^{r} M_\delta(b_nX_n - b_ny_i)$ by Lemma 2.10. Note that $\delta(b_n) \geq 0$ since $b_n \in R$. Thus

$$M_\delta(g) \leq 2(d^n + 1)d^{2n^2}\gamma$$

Now fix some index $k \in \{1, \ldots, n-1\}$ and let $z_1, \ldots, z_r \in \bar{K}$ be the k-th coordinates of the zeroes $x_1, \ldots, x_r$ of $\mathfrak{a}$. From $f_k(X_k) \in \mathfrak{a}$ we obtain $f_k(z_i) = 0$ $(1 \leq i \leq r)$. Thus $b_k z_1, \ldots, b_k z_r$ are integral over R and furthermore

$$\delta(b_k z_i) \leq \bar{M}_\delta(f_k) \leq M_\delta(f_k) \leq 2d^{2n^2}\gamma \tag{2}$$

by Proposition 2.11 and Theorem 2.14. By Lagrange interpolation there is a unique polynomial $h_k \in \bar{K}[X]$ of degree $\leq r-1$ such that $h_k(y_i) = z_i$ $(1 \leq i \leq r)$. Let $h_k(X) = \sum_{i=0}^{r-1} c_i X^i$.

For $\sigma \in \mathrm{Gal}(\bar{K}/K)$ we let $h_k^\sigma(X) = \sum_{i=0}^{r-1} \sigma(c_i) X^i$. $\mathrm{Gal}(\bar{K}/K)$ also acts on the set $\{(y_1, z_1), \ldots, (y_r, z_r)\}$. Thus for each i there is an index j such that $\sigma^{-1}(y_i) = y_j$ and $\sigma^{-1}(z_i) = z_j$ hence

$$h_k^\sigma(y_i) = h_k^\sigma(\sigma(y_j)) = \sigma(h_k(y_j)) = \sigma(z_j) = z_i$$

The uniqueness of h_k yields $h_k^\sigma = h_k$. Thus the coefficients of h_k are fixed under all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and therefore $h_k \in K[X]$.

Let

$$A := \begin{pmatrix} 1 & y_1 & \ldots & y_1^{r-1} \\ \vdots & \vdots & & \vdots \\ 1 & y_r & \ldots & y_r^{r-1} \end{pmatrix}$$

The fact $h_k(y_i) = z_i$ $(1 \leq i \leq r)$ yields

$$\begin{aligned} z_1 &= c_0 + y_1 c_1 + \ldots + y_1^{r-1} c_{r-1} \\ &\vdots \\ z_r &= c_0 + y_r c_1 + \ldots + y_r^{r-1} c_{r-1} \end{aligned}$$

As $y_1, \ldots, y_r$ are mutually distinct A is regular and we may apply Cramer's rule to obtain

$$c_i = \frac{\det A_i}{\det A} \tag{3}$$

where A_i $(0 \leq i \leq r-1)$ is the matrix which is obtained from A by substituting the $(i+1)$-th column by $(z_1, \ldots, z_r)$.

An application of an automorphism $\sigma \in \mathrm{Gal}(\bar{K}/K)$ permutes the rows of A. Thus $(\det A)^2$ is fixed under $\mathrm{Gal}(\bar{K}/K)$ and therefore an element of K. Now define

$$B := \begin{pmatrix} 1 & b_n y_1 & \ldots & (b_n y_1)^{r-1} \\ \vdots & \vdots & & \vdots \\ 1 & b_n y_r & \ldots & (b_n y_r)^{r-1} \end{pmatrix}$$

and let B_i be the matrix which is obtained from B by substituting the $(i+1)$-th column by $(b_k z_1, \dots, b_k z_r)$. Then, by linearity of the determinant

$$\det B = b_n^{\frac{1}{2}r(r-1)} \cdot \det A$$

(4)

$$\det B_i = b_k \cdot b_n^{\frac{1}{2}r(r-1)-i} \cdot \det A_i$$

The entries of the matrices $B, B_0, \dots, B_{r-1}$ are integral over R and thus also their determinants are integral over R. But, as $(\det A)^2 \in K$ also $(\det B)^2 \in K$ and therefore $(\det B)^2 \in R$, because R is integrally closed in K. We define $a_k := b_k \cdot (\det B)^2 \in R \setminus \{0\}$ and $g_k(X_k) := a_k \cdot h_k(X_k)$. Then by (3) and (4)

$$a_k \cdot c_i = b_n^i \cdot \det B \cdot \det B_i \qquad (0 \leq i \leq r-1) \tag{5}$$

The right hand side of the above equality is integral over R while the left hand side is an element of K. Since R is integrally closed in K we obtain $a_k c_i \in R$ and thus $g_k(X_k) \in R[X_k]$.

Next we want to find bounds for $\delta(a_k)$ and $M_\delta(g_k)$. By (1), (2) and Lemma 2.5(b) we get

$$\delta(\det B) \leq \sum_{j=1}^{r-1} j M_\delta(f_n) = r(r-1)d^{2n^2}\gamma \tag{6}$$

$$\delta(\det B_i) \leq \sum_{\substack{j=1 \\ j \neq i}}^{r-1} j M_\delta(f_n) + M_\delta(f_k) \leq (\tfrac{1}{2}r(r-1) - i + 1)2d^{2n^2}\gamma \tag{7}$$

Since $\delta(b_k) \leq M_\delta(f_k) \leq 2d^{2n^2}\gamma$ and $r \leq d^n$ we get from (6)

$$\delta(a_k) \leq (r(r-1)+1)2d^{2n^2}\gamma \leq 2d^{2n^2+2n}\gamma$$

and from (5), (6), (7) and $\delta(b_n) \leq M_\delta(f_n) \leq 2d^{2n^2}\gamma$ we obtain

$$\delta(a_k c_i) \leq (r(r-1)+1)2d^{2n^2}\gamma \leq 2d^{2n^2+2n}\gamma$$

Thus also

$$M_\delta(g_k) \leq 2d^{2n^2+2n}\gamma$$

Finally we are left to show that

$$\sqrt{\mathfrak{a}} = (g(X_n), a_1 X_1 - g_1(X_n), \dots, a_{n-1}X_{n-1} - g_{n-1}(X_n))$$

Denote the ideal on the right hand side by $\mathfrak{b}$. Then obviously

$$\mathfrak{b} = (g(X_n), X_1 - h_1(X_n), \dots, X_{n-1} - h_{n-1}(X_n))$$

By construction, the polynomials $g(X_n), X_1 - h_1(X_n), \dots, X_{n-1} - h_{n-1}(X_n)$ vanish on $\mathrm{V}(\mathfrak{a})$ and thus $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$ by Hilbert's Nullstellensatz. To show the converse let $f \in \sqrt{\mathfrak{a}}$. Then f vanishes on $\mathrm{V}(\mathfrak{a})$ and thus the polynomial $f(h_1(X_n), \dots, h_{n-1}(X_n), X_n) \in K[X_n]$ vanishes on the zeroes $y_1, \dots, y_r$ of g. As g has only simple zeroes $f(h_1(X_n), \dots, h_{n-1}(X_n), X_n)$ is a multiple of g and hence $f(h_1(X_n), \dots, h_{n-1}(X_n), X_n) \in \mathfrak{b}$. However, as $X_i \equiv h_i(X_n) \pmod{\mathfrak{b}}$ we get $f \equiv f(h_1(X_n), \dots, h_{n-1}(X_n), X_n) \pmod{\mathfrak{b}}$ and thus $f \in \mathfrak{b}$. This proves the theorem. $\square$

Chapter 5

A comparison of N_k and H_k

The aim of this chapter is to prove a recursion formula for N_k. In this formula also H_k will be involved, and thus with the results of Chapter 1 we obtain a comparison of N_k and H_k. The basic idea is to use the method of localizing, introduced by Gianni, Trager and Zacharias in [17]; a method which was successfully used by Becker and Neuhaus [5] in their algorithm for the computation of the real radical of a polynomial ideal.

The method of Gianni, Trager and Zacharias reduces the general situation of an ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ to the case of a zero-dimensional ideal over a field of rational functions $k(X_1, \ldots, X_s)$, s being the dimension of $\mathfrak{a}$.

Throughout this chapter we again assume that k is a formally real field. We start with an observation which will be important also in later chapters.

Lemma 5.1: *Let $f \in k[X_1, \ldots, X_n]$ be positive semidefinite over k and squarefree. Then f is positive definite as a univariate polynomial over $k(X_1, \ldots, X_{n-1})$.*

Proof: Let $K := k(X_1, \ldots, X_{n-1})$. In $k[X_1, \ldots, X_n]$ we split f into a product of irreducible factors $f = \prod_{i=1}^{m} f_i$. Then each of the polynomials $f_1, \ldots, f_m$ either remains irreducible in $K[X_n]$ or becomes a unit (cf.[29], Ch. V, Theorem 10).

As f is positive semidefinite over k it is a sum of squares in $k(X_1, \ldots, X_n)$ and hence, considered as a univariate polynomial over K, it is also positive semidefinite over K. Suppose that f is not positive definite over K. Then f has a real zero, i.e. there is a real closure R of K and some $x \in R$ such that $f(X_1, \ldots, X_{n-1}, x) = 0$. Since f is positive semidefinite the multiplicity of the root x has to be even. However, as the irreducible factors $f_1, \ldots, f_m$ are separable w.r.t. X_n there are i, j such that $i \neq j$ and $f_i(X_1, \ldots, X_{n-1}, x) = f_j(X_1, \ldots, X_{n-1}, x) = 0$. Since f_i, f_j are irreducible over K they coincide up to a factor

$c \in K^\times$. Thus $q \cdot f_i = p \cdot f_j$ for certain $p, q \in k[X_1, \ldots, X_{n-1}]$. As f_i, f_j are coprime in $k[X_1, \ldots, X_n]$ we obtain that f_i divides p and thus $\deg_{X_n} f_i \leq \deg_{X_n} p = 0$. Therefore $f_i \in K$. This contradicts $f_i(X_1, \ldots, X_{n-1}, x) = 0$. $\square$

Lemma 5.2: *Let $f \in k[X_1, \ldots, X_n] \setminus k$ be squarefree and assume that $g^2 f = \sum_{i=1}^r g_i^2$ for certain $g, g_1, \ldots, g_r \in k[X_1, \ldots, X_n] \setminus \{0\}$. If there is no polynomial $h \in k[X_1, \ldots, X_n] \setminus \{0\}$ of degree $\deg h < \deg g$ such that $h^2 f$ is also a sum of r squares in $k[X_1, \ldots, X_n]$ then f does not divide all the polynomials g_i.*

Proof: Assume the contrary, i.e., $g_i = f \cdot h_i$ for certain $h_1, \ldots, h_m \in k[X_1, \ldots, X_n]$. Then $g^2 f = \sum_{i=1}^r g_i^2$ yields

$$g^2 f = f^2 \cdot \sum_{i=1}^r h_i^2$$

and thus f divides g^2. Since f is squarefree, f also divides g. Thus $g = fh$ for some $h \in k[X_1, \ldots, X_n]$ of degree $\deg h < \deg g$. However, this implies

$$h^2 f = \sum_{i=1}^r h_i^2$$

and we got a contradiction since $\deg h < \deg g$. $\square$

Theorem 5.3: *Let $f \in k[X_1, \ldots, X_n] \setminus k$ be squarefree of degree $\deg f \leq d$ and positive semidefinite over k. Then there are $r \in \mathbb{N}$ and $g, g_1, \ldots, g_r \in k[X_1, \ldots, X_n]$, $g \neq 0$ such that:*

(a) $g^2 f = \sum_{i=1}^r g_i^2$
(b) $\deg g_i \leq H_k(n, d)$
(c) $r \leq 2^n \cdot \mathrm{P}_2(k) \cdot H_k(n, d)^n$
(d) *f does not divide all g_i*

Proof: This is an immediate consequence of Theorem 1.8 and Lemma 5.2. $\square$

Lemma 5.4: *Let $f \in k[X_1, \ldots, X_n]$ be semidefinite over k and squarefree. Then every irreducible factor of f is semidefinite over k.*

Proof: We first assume that k itself is real closed. Let $f = \prod_{i=1}^m f_i$ be the decomposition into irreducible factors. We prove the assertion by induction on the number m of irreducible factors. In the case $m = 1$ there is nothing to show. So let $m > 1$. As f is semidefinite the principal ideal (f) is not real by Lemma 5.2. Hence, by the Changing Sign Criterion ([28], Theorem 6.11) at least one of the polynomials f_i is semidefinite, say f_1. Therefore also $\prod_{i=2}^m f_i$ has to be semidefinite. Now we may apply the induction hypothesis to obtain that also $f_2, \ldots, f_m$ are semidefinite.

To treat the general case let K be a real closure of k. Let further $g \in k[X_1, \ldots, X_n]$ be an irreducible factor of f in $k[X_1, \ldots, X_n]$. The irreducible factors of g in $K[X_1, \ldots, X_n]$ are also irreducible factors of f in $K[X_1, \ldots, X_n]$. As we proved above, all of them are semidefinite in K. Note that f remains squarefree in $K[X_1, \ldots, X_n]$. Thus also g is semidefinite in K. $\square$

It is well-known that for two given univariate polynomials $f, g \in k[X]$ there are $F, G \in k[X]$ of degrees $\deg F \leq \deg g - 1$ and $\deg G \leq \deg f - 1$ such that the resultant of f and g admits a representation of the form $\mathrm{Res}(f,g) = Ff + Gg$. In the multivariate case a similar result is true.

Proposition 5.5: *Let $f, g \in k[X_1, \ldots, X_n]$ and let $R = \mathrm{Res}_{X_n}(f,g)$. Then:*

(a) $\deg R \leq \deg f \cdot \deg g$

(b) *There are $F, G \in k[X_1, \ldots, X_n]$ such that $\deg F \leq \deg f \cdot (\deg g - 1)$, $\deg G \leq \deg g \cdot (\deg f - 1)$ and $R = Ff + Gg$*

Proof: We express f, g in the form $f = \sum_{i=0}^{r} f_i X_n^i$ and $g = \sum_{i=0}^{s} g_i X_n^i$ for certain $f_0, \ldots, f_r, g_0, \ldots, g_s \in k[X_1, \ldots, X_{n-1}]$, $f_r, g_s \neq 0$ and denote the total degree of f and g by d_1 and d_2 respectively. Then

$$\begin{aligned} &\deg f_i \leq d_1 - i \\ &\deg g_i \leq d_2 - i \end{aligned} \tag{1}$$

The resultant of f and g w.r.t. X_n is the determinant of the $(r+s) \times (r+s)$-matrix

$$A := \begin{pmatrix} f_r & \cdots & \cdots & \cdots & f_0 & & \\ & \ddots & & & & \ddots & \\ & & f_r & \cdots & \cdots & \cdots & f_0 \\ g_s & \cdots & \cdots & g_0 & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & g_s & \cdots & \cdots & g_0 \end{pmatrix}$$

i.e. $A = (h_{ij})$ with

$$h_{ij} := \begin{cases} f_{r+i-j} & \text{if } i \leq s \\ g_{i-j} & \text{if } i > s \end{cases}$$

Formally we let $f_i = 0$ if $i > r$ or $i < 0$ and $g_i = 0$ if $i > s$ or $i < 0$. Note that (1) still holds since $\deg 0 = -\infty$. Then

$$R = \det A = \sum_{\sigma \in S_{r+s}} \mathrm{sign}(\sigma) \cdot \prod_{i=1}^{r+s} h_{i\sigma(i)}$$

For each permutation $\sigma \in S_{r+s}$ we get

$$\prod_{i=1}^{r+s} h_{i\sigma(i)} = \prod_{i=1}^{s} f_{r+i-\sigma(i)} \cdot \prod_{i=s+1}^{r+s} g_{i-\sigma(i)}$$

and thus

$$\begin{aligned} \deg \prod_{i=1}^{r+s} h_{i\sigma(i)} &\leq \sum_{i=1}^{s} (d_1 + \sigma(i) - r - i) + \sum_{i=s+1}^{r+s} (d_2 + \sigma(i) - i) \\ &= sd_1 + rd_2 - rs = d_1 d_2 - (d_1 - r)(d_2 - s) \leq d_1 d_2 \end{aligned}$$

This proves (a). In order to prove (b) we multiply the j-th column ($1 \le j \le r+s-1$) of A by X_n^{r+s-j} and add it to the last column. This yields the matrix

$$B = \begin{pmatrix} f_r & \cdots & \cdots & \cdots & f_0 & & X_n^{s-1}f \\ & \ddots & & & & \ddots & \vdots \\ & & f_r & \cdots & \cdots & \cdots & f \\ g_s & \cdots & \cdots & g_0 & & & X_n^{r-1}g \\ & \ddots & & & \ddots & & \vdots \\ & & \ddots & & & \ddots & \vdots \\ & & & g_s & \cdots & \cdots & g \end{pmatrix}$$

The first $r+s-1$ columns of the matrices A and B coincide but the last column of B is $(X_n^{s-1}f, \ldots, X_n f, f, X_n^{r-1}g, \ldots, X_n g, g)$. However, by elementary linear algebra $\det A = \det B$. Thus

$$R = \sum_{j=1}^{s} \sum_{\substack{\sigma \in S_{r+s} \\ \sigma(j)=r+s}} \operatorname{sign}(\sigma) \cdot X_n^{s-j} f \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)} + \sum_{j=s+1}^{r+s} \sum_{\substack{\sigma \in S_{r+s} \\ \sigma(j)=r+s}} \operatorname{sign}(\sigma) \cdot X_n^{r+s-j} g \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)}$$

We let

$$F := \sum_{j=1}^{s} \sum_{\substack{\sigma \in S_{r+s} \\ \sigma(j)=r+s}} \operatorname{sign}(\sigma) \cdot X_n^{s-j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)}$$

and

$$G := \sum_{j=s+1}^{r+s} \sum_{\substack{\sigma \in S_{r+s} \\ \sigma(j)=r+s}} \operatorname{sign}(\sigma) \cdot X_n^{r+s-j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)}$$

Then $R = Ff + Gg$. For $1 \le j \le s$ holds

$$X_n^{s-j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)} = X_n^{s-j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{s} f_{r+i-\sigma(i)} \cdot \prod_{i=s+1}^{r+s} g_{i-\sigma(i)}$$

Taking into account that $\sigma(j) = r+s$ this yields

$$\begin{aligned} \deg\left(X_n^{s-j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{r+s} h_{i\sigma(i)} \right) &\le s - j + \sum_{\substack{i=1 \\ i \neq j}}^{s} (d_1 + \sigma(i) - r - i) + \sum_{i=s+1}^{r+s} (d_2 + \sigma(i) - i) \\ &= (s-1)d_1 + rd_2 - rs = d_1 d_2 - (d_1 - r)(d_2 - s) - d_1 \le d_1(d_2 - 1) \end{aligned}$$

Thus $\deg F \le d_1(d_2 - 1)$. In the same way one can show that $\deg G \le d_2(d_1 - 1)$. □

Remark: Assertion (a) of Proposition 5.5 is a well-know fact. However, the degree bounds of (b) are not explicitly in the literature.

Theorem 5.6: *Let $f \in k[X_1, \ldots, X_n] \setminus \{0\}$ be positive semidefinite over k and square-free. Let $\deg f = d$. Then there are non-zero polynomials $p \in k[X_1, \ldots, X_n]$ and $q \in k[X_1, \ldots, X_{n-1}]$ such that*

(a) $pf - q^2$ *is a sum of squares in* $k[X_1, \ldots, X_n]$

(b) $\deg p \le 2d \cdot H_k(n,d) - d$

(c) $\deg q \le d \cdot H_k(n,d)$

Proof: We first assume that f is irreducible. Then, by Theorem 5.3 there are $r \in \mathbb{N}$ and $g, g_1, \ldots, g_r \in k[X_1, \ldots, X_n] \setminus \{0\}$ such that $\deg g_i \le H_k(n,d)$,

$$g^2 f = \sum_{i=1}^{r} g_i^2 \tag{1}$$

and f does not divide all the polynomials g_i, say $f \not| \; g_1$. Since $2 \cdot \deg g + \deg f = \deg \sum_{i=1}^{r} g_i^2 \le 2H_k(n,d)$ we obtain

$$\deg g \le H_k(n,d) - \tfrac{1}{2} d \tag{2}$$

If the indeterminate X_n does not occur in one of the polynomials g_i we are done. Otherwise let $q := \mathrm{Res}_{X_n}(f, g_1)$. As f is irreducible and $f \not| \; g_1$ the polynomials f and g_1 have no factor in common. Thus $q \in k[X_1, \ldots, X_{n-1}] \setminus \{0\}$ and

$$\deg q \le d \cdot \deg g_1 \le d \cdot H_k(n,d) \tag{3}$$

By Proposition 5.5 there are $F, G \in k[X_1, \ldots, X_n]$ such that $q = Ff + Gg_1$ and

$$\begin{aligned} \deg F &\le \deg f \cdot (\deg g_1 - 1) \le d \cdot (H_k(n,d) - 1) \\ \deg G &\le \deg g_1 \cdot (\deg f - 1) \le (d-1) \cdot H_k(n,d) \end{aligned}$$

Thus by (2) and (3):

$$\deg(Fq) \le 2d \cdot H_k(n,d) - d \tag{4}$$

$$\deg(Gg) \le d \cdot H_k(n,d) - \tfrac{1}{2} d \tag{5}$$

From (1) we obtain

$$G^2 g^2 f = \sum_{i=1}^{r} (Gg_i)^2 = (q - Ff)^2 + \sum_{i=2}^{r} (Gg_i)^2$$

and thus

$$(G^2 g^2 + 2qF) f = q^2 + (Ff)^2 + \sum_{i=2}^{r} (Gg_i)^2 \tag{5}$$

Now let $p = G^2 g^2 + 2qF$. Then (4) and (5) imply $\deg p \le 2d \cdot H_k(n,d) - d$. Since $q \ne 0$ we obtain from (5) that also $p \ne 0$ since k is formally real.

Now let f be arbitrary. We split f into its irreducible factors

$$f = \prod_{i=1}^{m} f_i$$

and denote the degrees of $f_1, \ldots, f_m$ by $d_1, \ldots, d_m$. By Lemma 5.4 $f_1, \ldots, f_m$ are semidefinite in every real closure of k. Let $x \in k^n$ be a non-zero of f and define $a_i = f_i(x)$. Then obviously $a_1 f_1, \ldots, a_m f_m$ are positive semidefinite over k. As the assertion is already proved for irreducible polynomials we obtain $p_1, \ldots, p_m \in k[X_1, \ldots, X_n] \setminus \{0\}$ and $q_1, \ldots, q_m \in k[X_1, \ldots, X_{n-1}] \setminus \{0\}$ such that

$$(5) \qquad p_i a_i f_i = q_i^2 + h_i \quad (1 \leq i \leq m)$$

for certain polynomials $h_1, \ldots, h_m$ which are sums of squares in $k[X_1, \ldots, X_n]$, and

$$\begin{aligned} \deg p_i &\leq 2d_i \cdot H_k(n, d_i) - d_i \\ \deg q_i &\leq d_i \cdot H_k(n, d_i) \end{aligned}$$

If we multiply all the equations in (5) we obtain

$$\prod_{i=1}^{m} a_i p_i \cdot f = \prod_{i=1}^{m} q_i^2 + h$$

with h a sum of squares of polynomials. Now note that $d = \sum_{i=1}^{m} d_i$. Since furthermore $H_k(n, d_i) \leq H_k(n, d)$ we obtain the asserted degree bounds immediately. $\square$

In their attempts to find degree bounds for Hilbert's Nullstellensatz, several authors reduced the problem to the case of an ideal which is generated by a regular sequence (cf. [8], [9], [14]). In the proof of the main result of this chapter we will proceed in a similar manner. For this purpose we need a real version of a standard result.

Lemma 5.7: *Let $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ be an ideal generated by non-zero polynomials $f_1, \ldots, f_m$ of degree $\deg f_i \leq d$ and suppose that $\dim \mathfrak{a} = s$. Then there are $h_1, \ldots, h_{n-s} \in \mathfrak{a}$ such that*

(a) $h_1, \ldots, h_{n-s}$ *is a regular sequence*

(b) $\deg h_1 \leq 2d, \ \deg h_i \leq d \quad (2 \leq i \leq n-s)$

(c) $\mathrm{V_r}(h_1, \ldots, h_{n-s}) = \mathrm{V_r}(\mathfrak{a})$

Proof: We define $h_1, \ldots, h_{n-s}$ in a recursive way. Let $h_1 := \sum_{i=1}^{m} f_i^2$. Assume that we already constructed a regular sequence $h_1, \ldots, h_r \in \mathfrak{a}$ with degrees $\deg h_1 \leq 2d$, $\deg h_i \leq d$ $(2 \leq i \leq r)$ for $r < n - s$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the associated primes of $(h_1, \ldots, h_r)$. Then $\dim \mathfrak{p}_i = \dim(h_1, \ldots, h_r) = n - r > s$ by Macaulay's Unmixedness Theorem. Thus $\mathfrak{a}$ is not contained in any of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Let

$$U_i := \{(a_1, \ldots, a_m) \in k^m \mid \sum_{j=1}^{m} a_j f_j \in \mathfrak{p}_i \}$$

for $1 \leq i \leq t$. Obviously $U_1, \ldots, U_t$ are k-linear subspaces of k^m. Furthermore, all of them are proper subspaces because $\mathfrak{a}$ is not contained in any of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Since k is infinite also

$$\bigcup_{i=1}^{t} U_i \neq k^m$$

Now choose $(a_1, \ldots, a_m) \in k^m \setminus \bigcup_{i=1}^t U_i$ and let $h_{r+1} := \sum_{j=1}^m a_j f_j$. Then $h_{r+1} \notin \bigcup_{i=1}^t \mathfrak{p}_i$ by definition of $U_1, \ldots, U_t$ and thus $h_1, \ldots, h_{r+1}$ is a regular sequence. Since $\deg f_i \leq d$ $(1 \leq i \leq m)$ also $\deg h_{r+1} \leq d$.

If we finally constructed the sequence we get

$$\mathrm{V_r}(\mathfrak{a}) \subset \mathrm{V_r}(h_1, \ldots, h_{n-s}) \subset \mathrm{V_r}(h_1) = \mathrm{V_r}(f_1^2 + \ldots + f_m^2) = \mathrm{V_r}(\mathfrak{a})$$

and thus $\mathrm{V_r}(\mathfrak{a}) = \mathrm{V_r}(h_1, \ldots, h_{n-s})$. $\square$

In order to state the next theorem properly we define

Definition: $N'_k(n, s, d) := \max(N_k(n, s, d), N_k(n, -1, d))$

Theorem 5.8: *Let $0 < s < n$ and $d \geq 3$. Then:*

$$N_k(n, s, d) \leq 5d^n \cdot N'_k(n, s-1, d^{4n^2} \cdot H_k(s+1, d^{4n^2}))$$

Proof: Let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ of degree $\deg f_i \leq d$ generate an ideal $\mathfrak{a}$ of dimension s without any real zero. By Lemma 5.7 there are polynomials $h_1, \ldots, h_{n-s} \in \mathfrak{a}$ which form a regular sequence such that $\deg h_1 \leq 2d$, $\deg h_i \leq d$ $(2 \leq i \leq n-s)$ and $\mathrm{V_r}(h_1, \ldots, h_{n-s}) = \mathrm{V_r}(\mathfrak{a}) = \emptyset$. Let $\mathfrak{b} := (h_1, \ldots, h_{n-s})$. By Noether's Normalization Theorem ([25], Ch. II, Theorem 3.1) there are $t_1, \ldots, t_s \in k[X_1, \ldots, X_n]$ such that their residues modulo $\mathfrak{b}$ are algebraically independent over k and $k[X_1, \ldots, X_n]/\mathfrak{b}$ is integral over $k[\bar{t}_1, \ldots, \bar{t}_s]$. Since k is infinite the elements $t_1, \ldots, t_s$ can be chosen as linear forms in $X_1, \ldots, X_n$. After an affine invertible transformation we can get $t_1 = X_1, \ldots, t_s = X_s$. This affine transformation preserves the total degree and thus we may assume that we are in the situation

(1) $\quad k[X_1, \ldots, X_s] \cap \mathfrak{b} = (0)$

(2) $\quad \varphi : k[X_1, \ldots, X_s] \hookrightarrow k[X_1, \ldots, X_n]/\mathfrak{b}$ is an integral embedding

Now let $K := k(X_1, \ldots, X_s)$ and $R := k[X_1, \ldots, X_s]$ and let $\bar{K}$ the algebraic closure of K. Furthermore let

$$\delta : \bar{K} \longrightarrow \mathbb{Q} \cup \{-\infty\}$$

be an R-stable degree function according to Corollary 3.2, i.e. $\delta(f) = \deg f$ for each $f \in R = k[X_1, \ldots, X_s]$. Then $M_\delta(h_1) = \deg_{X_1, \ldots, X_s} h_1 \leq 2d$ and $M_\delta(h_i) = \deg_{X_1, \ldots, X_s} h_i \leq d$ $(2 \leq i \leq n-s)$.

By $\mathfrak{B}$ we denote the ideal generated by $h_1, \ldots, h_{n-s}$ in $K[X_{s+1}, \ldots, X_n]$. Then (2) immediately implies that $\dim \mathfrak{B} = 0$. The affine Bezout inequality yields

$$\#\mathrm{V}(\mathfrak{B}) \leq \prod_{i=1}^{n-s} \deg_{X_{s+1},\ldots,X_n} h_i \leq 2d^{n-s}$$

After a further affine transformation over k in the variables $X_{s+1}, \ldots, X_n$ we may assume that $\mathrm{V}(\mathfrak{B}) \subset \bar{K}^{n-s}$ is in general position w.r.t. X_n, i.e. the projection map

$$\begin{aligned} \pi : \mathrm{V}(\mathfrak{B}) &\longrightarrow \bar{K} \\ (x_{s+1}, \ldots, x_n) &\mapsto x_n \end{aligned}$$

is injective. Note that $k[X_1, \ldots, X_s]$ is fixed under this transformation and thus (1) and (2) are still valid. By Theorem 4.4 there are $g_{s+1}, \ldots, g_n \in R[X_n] = k[X_1, \ldots, X_s, X_n]$, $a_{s+1}, \ldots, a_n \in R\backslash\{0\} = k[X_1, \ldots, X_s]\backslash\{0\}$ and a polynomial $g \in R[X_n]\backslash\{0\}$ such that

$$\sqrt{\mathfrak{B}} = (g(X_n), a_{s+1}X_{s+1} - g_{s+1}(X_n), \ldots, a_{n-1}X_{n-1} - g_{n-1}(X_n)) \tag{3}$$

and

$$\deg_{X_n} g \leq \#\mathrm{V}(\mathfrak{B}) \leq 2d^{n-s} \tag{4}$$

$$\deg_{X_1,\ldots,X_s} g = M_\delta(g) \leq 2((2d)^{n-s} + 1)(2d)^{2(n-s)^2}(2d) \tag{5}$$

and

- g has only simple zeroes in $\bar{K}$
- the leading coefficient of g is a square

By (4) and (5) we obtain

$$\begin{aligned} d' := \deg g &\leq 2d^{n-s} + 2((2d)^{n-s} + 1)(2d)^{2(n-s)^2+1} \\ &\leq 2d^{n-s} + 2d \cdot (2d)^{n-s} \cdot (2d)^{2(n-s)^2+1} = 2d^{n-s} + (2d)^{2(n-s)^2+n-s+2} \\ &\leq 2 \cdot (2d)^{2(n-s)^2+n-s+2} \leq (2d)^{2(n-s)^2+n-s+3} \leq d^{4(n-s)^2+2n-2s+6} \end{aligned}$$

and thus $0 < s < n$ implies

$$d' \leq d^{4n^2} \tag{6}$$

Now we claim:

Claim 1: The univariate polynomial $g \in K[X_n]$ is positive definite over K

To prove the claim let L be a real closure of K w.r.t. a certain ordering. Suppose that g has a zero in L, say z, and define $z_i := a_i^{-1} g_i(X_1, \ldots, X_s, z) \in L$ $(s+1 \leq i \leq n-1)$.

Then $(z_{s+1},\dots,z_{n-1},z)$ is a real zero of $\mathfrak{B}$ by (3). Since $h_1,\dots,h_{n-s}\in\mathfrak{B}$ we get $h_i(X_1,\dots,X_s,z_{s+1},\dots,z_{n-1},z)=0$ $(1\le i\le n-s)$ and hence

$$(L,L^{\geq 0})\models \exists x_1,\dots,x_n\left(\bigwedge_{i=1}^{n-s} h_i(x_1,\dots,x_n)=0\right)$$

Model completeness of the theory of real closed fields yields

$$\overline{(k,k\cap L^{\geq 0})}\models \exists x_1,\dots,x_n\left(\bigwedge_{i=1}^{n-s} h_i(x_1,\dots,x_n)=0\right)$$

and hence $\mathfrak{b}$ would have a real zero. Thus g has no zero in L. By the intermediate value theorem, g must be definite in L. As the leading coefficient of g is a square, g is positive definite and the claim is proved.

Hence g is a sum of squares in $K(X_n)=k(X_1,\dots,X_s,X_n)$. Therefore, as a polynomial in $k[X_1,\dots,X_s,X_n]$, g is positive semidefinite over k. We split g in $k[X_1,\dots,X_s,X_n]$ into

$$g=F^2\cdot G$$

with G squarefree. Since g has only simple zeroes in $\bar{K}$ it is squarefree in $K[X_n]=k(X_1,\dots,X_s)[X_n]$ and thus F must be a unit in $K[X_n]$. Hence $F\in k[X_1,\dots,X_s]$. As g is positive semidefinite over k so is G. By Theorem 5.6 there are polynomials $p\in k[X_1,\dots,X_s,X_n]\backslash\{0\}$ and $q\in k[X_1,\dots,X_s]\backslash\{0\}$ of degrees

$$\begin{aligned}\deg p &\le 2d'\cdot H_k(s+1,d')-d'\\ \deg q &\le d'\cdot H_k(s+1,d')\end{aligned}$$

such that

(7) $$H=pG-q^2\in\sum k[X_1,\dots,X_s,X_n]^2$$

The degree bounds for p and q yield

(8) $$\deg H\le 2d'\cdot H_k(s+1,d')$$

Next we claim:

Claim 2: $\mathfrak{p} \cap k[X_1, \ldots, X_s] = (0)$ *for every associated prime ideal of* $\mathfrak{b}$

To prove the claim let $\mathfrak{p}$ be an associated prime of $\mathfrak{b}$ an let $\mathfrak{q} = \mathfrak{p} \cap k[X_1, \ldots, X_s]$. Since $\mathfrak{b}$ is generated by a regular sequence all its associated primes are of dimension s by Macaulay's Unmixedness Theorem. Let

$$\psi : k[X_1, \ldots, X_n]/\mathfrak{b} \twoheadrightarrow k[X_1, \ldots, X_n]/\mathfrak{p}$$

be the canonical surjection. Then by (2) we obtain that $k[X_1, \ldots, X_n]/\mathfrak{p}$ is integral over the image of

$$\psi \circ \varphi : k[X_1, \ldots, X_s] \longrightarrow k[X_1, \ldots, X_n]/\mathfrak{p}$$

Obviously $\ker(\psi \circ \varphi) = \mathfrak{q}$ and thus $\psi \circ \varphi$ induces an integral embedding

$$k[X_1, \ldots, X_s]/\mathfrak{q} \hookrightarrow k[X_1, \ldots, X_n]/\mathfrak{p}$$

Therefore $\dim \mathfrak{q} = \dim \mathfrak{p} = s$. Since (0) is the only s-dimensional prime ideal in $k[X_1, \ldots, X_s]$ we get $\mathfrak{q} = (0)$. This proves the claim.

Claim 3: $G \in \sqrt{\mathfrak{a}}$

By construction we get $g \in \sqrt{\mathfrak{B}} \subset K[X_{s+1}, \ldots, X_n]$. Thus $g^t = \sum_{i=1}^{n-s} Q_i h_i$ for some $t \in \mathbb{N}$ and $Q_1, \ldots, Q_{n-s} \in K[X_{s+1}, \ldots, X_n] = k(X_1, \ldots, X_s)[X_{s+1}, \ldots, X_n]$. After multiplication with a certain $h \in k[X_1, \ldots, X_s] \backslash \{0\}$ this yields $hg^t \in \mathfrak{b}$ and thus $hg = hF^2G \in \sqrt{\mathfrak{b}}$. However, since $h, F \in k[X_1, \ldots, X_s]$ none of them is contained in any of the associated primes of $\mathfrak{b}$. Hence $G \in \sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a}}$ and the claim is proved.

Now let $\mathfrak{c} := (h_1, \ldots, h_{n-s}, q)$. As $q \in k[X_1, \ldots, X_s]$ it is not contained in any associated prime of $\mathfrak{b}$ by Claim 2. Thus $h_1, \ldots, h_{n-s}, q$ is a regular sequence and therefore either $\dim \mathfrak{c} = s - 1$ or $1 \in \mathfrak{c}$. Since $\mathfrak{b} \subset \mathfrak{c}$ we obtain $\mathrm{V_r}(\mathfrak{c}) = \emptyset$ and thus

$$1 + P = \sum_{i=1}^{n-s} p_i h_i + p_0 q$$

for certain $p_0, \ldots, p_{n-s} \in k[X_1, \ldots, X_n]$ and $P \in \sum k[X_1, \ldots, X_n]^2$ of degrees

$$\deg(p_i h_i), \deg(p_0 q) \leq N'_k(n, s-1, d' \cdot H_k(s+1, d')) \tag{9}$$

Therefore also $\deg(1 + P) \leq N'_k(n, s-1, d' \cdot H_k(s+1, d'))$ and furthermore

$$1 + P \equiv p_0 q \pmod{\mathfrak{b}}$$

Squaring this equation we get together with (7)

$$(1 + P)^2 + p_0^2 H \equiv p_0^2 p G \pmod{\mathfrak{b}}$$

Since $\mathfrak{b} \subset \mathfrak{a}$ and $G \in \sqrt{\mathfrak{a}}$ by Claim 3 this yields

$$(1 + P)^2 + p_0^2 H \in \sqrt{\mathfrak{a}}$$

From (8) and (9) we get

$$\begin{aligned}\deg(p_0^2 H) &\leq 2N_k'(n, s-1, d' \cdot H_k(s+1, d')) + 2d' \cdot H_k(s+1, d') \\ &\leq 4N_k'(n, s-1, d' \cdot H_k(s+1, d'))\end{aligned}$$

Finally we apply the effective Nullstellensatz to obtain

$$((1+P)^2 + p_0^2 H)^t = \sum_{i=1}^{m} q_i f_i$$

for certain $t \in \mathbb{N}, q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ such that

$$\deg(q_i f_i) \leq d^n \cdot (1 + \deg((1+P)^2 + p_0^2 H)) \leq 5d^n \cdot N_k'(n, s-1, d' \cdot H_k(s+1, d'))$$

Together with (6) this yields the result. $\square$

Chapter 6

Semi-splitting fields and semi-extensions of fields

In this short chapter we introduce the notion of a semi-splitting field of a polynomial and of a semi-extension of fields. Throughout this chapter we assume that K is a field. Its algebraic closure we denote by $\bar{K}$, and we let $i \in \bar{K}$ be a fixed square root of -1.

Definition: *Let $f \in K[X] \setminus K$. An extension field L of K is called a semi-splitting field of f over K if there are $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m \in L$ and $c \in K^\times$ such that:*

(i) *the decomposition of f into irreducible factors in $L[X]$ is of the form*

$$f(X) = c \cdot \prod_{i=1}^{n}(X - \alpha_i) \cdot \prod_{i=1}^{m}((X - \beta_i)^2 + \gamma_i^2)$$

(ii) $L = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m)$

We call (n, m) the type of the semi-splitting field L.

Examples, remarks:

1) The cases $n = 0$ or $m = 0$ are not excluded in the above definition. In particular, a splitting field of a polynomial is also a semi-splitting field.

2) Let $f(X) := X^2 + 1 \in \mathbb{R}[X]$. Then $\mathbb{R}$ is a semi-splitting field of f over $\mathbb{R}$. As $\mathbb{C}$ is the splitting field of f also $\mathbb{C}$ is a semi-splitting field of f over $\mathbb{R}$. Therefore two semi-splitting fields of a given polynomial are not necessarily isomorphic.

3) Let K be a formally real field and let R be the real closure of K w.r.t. a fixed ordering P of K. Then in $R[X]$ every polynomial $f \in K[X] \setminus K$ splits in the form

$$f(X) = c \cdot \prod_{i=1}^{n} (X - \alpha_i) \cdot \prod_{i=1}^{m} ((X - \beta_i)^2 + \gamma_i^2)$$

and thus for every polynomial $f \in K[X]$ the field R contains a semi-splitting field. This shows that there is a certain analogy between splitting fields and semi-splitting fields of polynomials. The algebraic closure $\bar{K}$ of a field K is the direct limit of all splitting fields of polynomials $f \in K[X]$. In the same way one can consider the real closure $\overline{(K, P)}$ of an ordered field (K, P) as the direct limit of ordered semi-splitting fields. Thus, in a certain sense, ordered semi-splitting fields are the real analogue of splitting fields. However, we are interested also in non-real semi-splitting fields. It even will turn out that for our purpose the non-real semi-splitting fields are more important than the real ones.

The following lemma gives a criterion for a polynomial of the form $(X - a)^2 + b^2$ to be reducible.

Lemma 6.1: *Let $a, b \in K$. The following conditions are equivalent:*

(i) *$(X - a)^2 + b^2$ is reducible in $K[X]$*

(ii) *$b = 0$ or -1 is a square in K*

Proof: If $\mathrm{char}(K) = 2$ then $(X - a)^2 + b^2$ is reducible and $-1 = 1$ is a square. So assume that $\mathrm{char}(K) \neq 2$. The zeroes of $(X - a)^2 + b^2$ are $\alpha = a + ib$ and $\beta = a - ib$. If -1 is a square in K or $b = 0$, then $(X - a)^2 + b^2$ splits into linear factors in $K[X]$ and hence it is reducible. Now assume that $(X - a)^2 + b^2$ is reducible in $K[X]$. Then $\alpha, \beta \in K$ and hence $2ib = \alpha - \beta \in K$. Therefore $b = 0$ or -1 is a square in K. $\square$

The following theorem characterizes the semi-splitting fields of a given polynomial completely.

Theorem 6.2: *Let E, F be two field extensions of K which are contained in a common extension. Assume further that F is the splitting field of the polynomial $f \in K[X] \setminus K$ over K. Then the following conditions are equivalent*

(i) *E is a semi-splitting field of f over K*

(ii) *$E = F$ or $E \neq E(i) = F(i)$*

Proof: (i) $\Rightarrow$ (ii): Since E is a semi-splitting field of f over K, the polynomial f splits in $E[X]$ into a product of irreducible factors of the form

$$f(X) = c \cdot \prod_{i=1}^{n} (X - \alpha_i) \cdot \prod_{i=1}^{m} ((X - \beta_i)^2 + \gamma_i^2)$$

for certain $c \in K^\times, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m \in E$ such that

$$E = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m)$$

The zeroes of f are $\alpha_1, \ldots, \alpha_n, \beta_1 \pm i\gamma_1, \ldots, \beta_m \pm i\gamma_m \in \bar{K}$. Hence

$$F = K(\alpha_1, \ldots, \alpha_n, \beta_1 + i\gamma_1, \beta_1 - i\gamma_1, \ldots, \beta_m + i\gamma_m, \beta_m - i\gamma_m)$$

If $m = 0$, then obviously $E = F$. If $m \neq 0$, then -1 is not a square in E by Lemma 6.1. Thus $E \neq E(i)$ and furthermore $\mathrm{char}(K) \neq 2$. Now it is easy to see that $E(i) = F(i)$.

(ii) $\Rightarrow$ (i): If $E = F$ there is nothing to show. Now assume that $E \neq E(i) = F(i)$. Then $E(i)/E$ is a Galois extension of degree 2 with a non-trivial E-automorphism

$$\sigma : E(i) \longrightarrow E(i)$$

with the property $\sigma(i) = -i$. Moreover $\mathrm{char}(K) \neq 2$. We split f in $E[X]$ into a product

$$f(X) = c \cdot \prod_{j=1}^{n} g_j(X)$$

with $c \in K^\times$ and $g_1, \ldots, g_n \in E[X]$ are monic and irreducible. Since $F \subset F(i) = E(i)$ the polynomial f and hence also the factors $g_1, \ldots, g_n$ split into linear factors over $E(i)$. Thus $\deg g_j \leq [E(i) : E] = 2$ $(1 \leq j \leq n)$.

Now let g be one of these irreducible factors and assume that $\deg g = 2$. Let $z \in E(i)$ be a zero of g. Then there are $\beta, \gamma \in E$ such that $z = \beta + i\gamma$. Since g is irreducible of degree 2 we get $z \notin E$. Also $\sigma(z)$ is a zero of g and furthermore $z \neq \sigma(z)$ because E is the fixed field of σ. Thus

$$g(X) = (X - z) \cdot (X - \sigma(z)) = (X - \beta)^2 + \gamma^2$$

Hence the factorization of f into a product of irreducible factors over E is of the form

$$f(X) = c \cdot \prod_{i=1}^{n} (X - \alpha_i) \cdot \prod_{i=1}^{m} ((X - \beta_i)^2 + \gamma_i^2)$$

for certain $c \in K^\times$, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m \in E$. Define

$$L := K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m)$$

It remains to show that $E = L$. Obviously $L \subset E$. However, over $L(i)$ the polynomial f splits into irreducible factors. Thus $F \subset L(i) \subset E(i) = F(i)$ and hence $L(i) = E(i) = F(i)$. Therefore $[E(i) : L] = [L(i) : L] = 2$ and from $[E(i) : E] = 2$ we obtain $L = E$. $\square$

Corollary 6.3: *Let $f \in K[X] \setminus K$ be of degree n and assume that E is a semi-splitting field of f over K. Then*

$$[E : K] \leq n!$$

Proof: Let F be the splitting field of f over K. The estimate $[F : K] \leq n!$ is well-known. If $E = F$, we are done. Otherwise, by Theorem 6.2 we get $E \neq E(i) = F(i)$ and thus

$$2 \cdot [E : K] = [E(i) : K] = [F(i) : K] \leq 2 \cdot [F : K] \leq 2n!$$

Hence $[E : K] \leq n!$ $\square$

Corollary 6.4: *Let L/K be a field extension and assume that $f \in K[X] \setminus K$. Then the following conditions are equivalent:*

(i) *L contains a semi-splitting field E of f over K*

(ii) *There are $c \in K^\times, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_m \in L$ such that*

$$f(X) = c \cdot \prod_{i=1}^{n}(X - \alpha_i) \cdot \prod_{i=1}^{m}((X - \beta_i)^2 + \gamma_i^2)$$

(iii) *Over $L(i)$ the polynomial f splits into a product of linear factors*

Proof: The implications (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) are obvious and it remains to show (iii) $\Rightarrow$ (i). Let F be the splitting field of f over K. Then $F = K(x_1, \ldots, x_r)$ for certain $x_1, \ldots, x_r \in F$. Since f splits over $L(i)$ we obtain $F \subset L(i)$. If already $F \subset L$ we are done. Otherwise $L \neq L(i)$ and thus $\mathrm{char}(K) \neq 2$.

We express the elements $x_1, \ldots, x_r$ in the form $x_k = a_k + ib_k$ $(1 \leq k \leq r)$ for certain $a_1, \ldots, a_r, b_1, \ldots, b_r \in L$ and let $y_k := a_k - ib_k \in L(i)$ $(1 \leq k \leq r)$. The elements x_k, y_k $(1 \leq k \leq r)$ are conjugate over L and hence over K. As F/K is normal $y_1, \ldots, y_r \in F$. Now we define $E := K(a_1, \ldots, a_r, b_1, \ldots, b_r)$. Then $E \subset L$ and $F \subset E(i)$. But since $\mathrm{char}(K) \neq 2$ we also get $E(i) = K(x_1, \ldots, x_r, y_1, \ldots, y_r, i) \subset F(i)$ and therefore $E(i) = F(i)$. Since $L \neq L(i)$ and $E \subset L$ also $E \neq E(i)$. Therefore by Theorem 6.2, E is a semi-splitting field of f over K which is contained in L. $\square$

After the characterization of semi-splitting fields of polynomials we treat the second topic of this chapter. We start with a definition.

Definition: *Let K, L be two fields which are contained in a common extension. L is called a semi-extension of K if $K(i) \subset L(i)$.*

Proposition 6.5: *Let L, F be extensions of the field K and assume that L/K is algebraic. Suppose further that F is a semi-extension of L and let E be the relative algebraic closure of K in F. Then also E is a semi-extension of L.*

Proof: By the definition we get $L \subset F(i)$. We have to prove that $L \subset E(i)$. If $F = F(i)$ we obtain $L \subset E$ by the definition of E. Now assume that $F \neq F(i)$. Then $\mathrm{char}(K) \neq 2$. Let $z \in L \subset F(i)$. Then there are $a, b \in F$ such that $z = a + ib$. We define $y := a - ib$. Since $K \subset F$ also y is a zero of $\mathrm{Irr}(z, K)$ and thus both elements y, z are algebraic over K. Thus also $z \pm y$ are algebraic over K and hence a, b are algebraic over K. Thus $a, b \in E$ and therefore $z \in E(i)$. $\square$

Let E, F be two fields which are contained in a common extension and assume that F is a semi-extension of E. Let further $z \in E$. Then obviously $F(\sqrt{z})$ is a semi-extension of $E(\sqrt{z})$. If z is not a square in E then $E(\sqrt{z})/E$ is a quadratic extension, and as $E \subset F(i)$ we obtain that $[F(\sqrt{z}) : F]$ is either $1, 2$ or 4. One can easily see that all three values are possible and thus $F(\sqrt{z})/F$ is not necessarily a quadratic extension. In the next theorem we prove that there is an extension F' of F such that F' is a semi-extension of $E(\sqrt{z})$ and F' is obtained from F by two successive quadratic extensions.

Theorem 6.6: *Let R be an integral domain which is integrally closed in its field of quotients K and let $\delta\colon \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that E and F are subfields of $\bar{K}$ which contain K and suppose that F is a semi-extension of E. Let further $z \in E$ be integral over R. Then there are elements $a, b \in F$ and $u \in F(\sqrt{a^2+b^2})$ such that:*

(1) *a, b, u are integral over R*

(2) *$F(\sqrt{a^2+b^2}, \sqrt{u})$ and $F(\sqrt{a^2+b^2}, \sqrt{-u})$ are semi-extension of $E(\sqrt{z})$*

(3) *$\delta(a), \delta(b), \delta(u) \leq \delta(z)$*

Proof: We have $z \in E \subset E(i) \subset F(i)$. If $z \in F$ let $a = b = 0$ and $u = z$. Now assume that $z \notin F$. Then $F \neq F(i)$ and $\operatorname{char}(K) \neq 2$. Hence $z = c + id$ for some uniquely determined elements $c, d \in F, d \neq 0$. Let $z' := c - id$. Then z and z' are conjugate over F and hence also over K. As R is integrally closed in K also z' is integral over R, and since δ is R-stable we have $\delta(z) = \delta(z')$.

Now define $a := 2c = z + z'$ and $b := 2d = i(z' - z)$. Then $a, b \in F$ and both elements are integral over R. We get $\delta(a) = \delta(z+z') \leq \max(\delta(z), \delta(z')) = \delta(z)$ and $\delta(b) = \delta(i(z'-z)) \leq \delta(z)$.

We choose an element $w \in \bar{K}$ such that $w^2 = a^2 + b^2$. Then $2 \cdot \delta(w) = \delta(a^2 + b^2) \leq 2 \cdot \max(\delta(a), \delta(b)) \leq 2 \cdot \delta(z)$ and thus $\delta(w) \leq \delta(z)$. Now let $u := w + a$ and $u' := w - a$. Then $u, u' \in F(\sqrt{a^2+b^2})$ and both elements are integral over R. Furthermore $\delta(u) \leq \delta(z)$. We get $u + u' = 2w,\ u - u' = 2a$ and $uu' = b^2 = 4d^2 \neq 0$. Now we choose an element $x \in \bar{K}^{\times}$ such that $x^2 = u$ and let $y := bx^{-1} \in F(\sqrt{a^2+b^2}, \sqrt{u})$. Then $y^2 = u'$. Finally let $v := x + iy \in F(\sqrt{a^2+b^2}, \sqrt{u}, i)$. Then $v^2 = x^2 - y^2 + 2ixy = u - u' + 2ib = 2a + 2ib = 4z$. Thus z is a square in $F(\sqrt{a^2+b^2}, \sqrt{u}, i)$ and hence

$$E(\sqrt{z}, i) \subset F(\sqrt{a^2+b^2}, \sqrt{u}, i) = F(\sqrt{a^2+b^2}, \sqrt{-u}, i)$$

Therefore both fields $F(\sqrt{a^2+b^2}, \sqrt{u})$ and $F(\sqrt{a^2+b^2}, \sqrt{-u})$ are semi-extensions of $E(\sqrt{z})$. This proves the theorem. $\square$

Chapter 7

The size of isotropic vectors

This chapter together with the next one is the crucial part of our approach. We introduce a quantitative notion of isotropy for quadratic forms over fields with a degree function. The main result (Theorem 7.9) of this chapter is a certain local-global-principle for quantitative isotropy of quadratic forms.

We assume that the reader is familiar with the elementary theory of quadratic forms and we just fix some notations. A quadratic form over a field K is a homogeneous polynomial $f \in K[X_1, \ldots, X_n]$ of degree $\deg f = 2$. If f, g are quadratic forms we denote their orthogonal sum and their product by $f \oplus g$ and $f \otimes g$ respectively. The n-fold orthogonal sum $f \oplus \ldots \oplus f$ we denote by $n \times f$ and f^n denotes the n-fold product $f \otimes \ldots \otimes f$. If $a_1, \ldots, a_n \in K$ we denote the diagonal form $\sum_{i=1}^n a_i X_i^2$ by $< a_1, \ldots, a_n >$.

As in the previous chapters we denote the algebraic closure of a field K by $\bar{K}$. If R is a domain, then $\bar{R}$ denotes the integral closure of R in the algebraic closure of $\mathrm{Quot}(R)$. With this notation $K \cap \bar{R}$ is the integral closure of R in K.

Definition: *Let K be a field and suppose that R is a subdomain. Let furthermore $\delta: K \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on K and let $\alpha \in \Gamma_{\geq 0}$. A quadratic form $q \in K[X_1, \ldots, X_n]$ over K is called α-isotropic w.r.t. (R, δ) over K if there is an isotropic vector $x = (x_1, \ldots, x_n) \in (K \cap \bar{R})^n$ of q such that $M_\delta(x) \leq \alpha$.*

Remark: If it is clear from the context which triple (K, R, δ) α-isotropy refers at, we will omit the phrase "w.r.t. (R, δ) over K" or a part of it.

Lemma 7.1: *Let $R \subset S$ be two subdomains of the field K and suppose that S/R is an integral extension. Assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K and let $\alpha \in \Gamma_{\geq 0}$. Then a quadratic form $q \in K[X_1, \ldots, X_n]$ is α-isotropic w.r.t. (R, δ) over K iff q is α-isotropic w.r.t. (S, δ) over K.*

Proof: Immediate by the definition

Lemma 7.2: *Let K be a field and suppose that R is a subdomain. Assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function and let $\alpha \in \Gamma_{\geq 0}$. Let f, g be quadratic forms over K and suppose that $f \oplus g$ and $f \oplus -g$ are α-isotropic w.r.t. (R, δ) over K. Then $2 \times (f \otimes g)$ is 2α-isotropic w.r.t. (R, δ) over K.*

Proof: Let $\dim f = n$ and $\dim g = m$. For $x = (x_1, \ldots, x_n) \in K^n$ and $y = (y_1, \ldots, y_m) \in K^m$ we let $x \otimes y := (x_1 y_1, \ldots, x_1 y_m, \ldots, x_n y_1, \ldots, x_n y_m)$, i.e., we identify $K^n \otimes_K K^m$ and K^{nm} via the canonical isomorphism. Then, with this notation holds

$$(f \otimes g)(x \otimes y) = f(x) \cdot g(y)$$

By assumption there are $x, y \in (K \cap \bar{R})^n$ and $v, w \in (K \cap \bar{R})^m$ such that $M_\delta(x), M_\delta(y), M_\delta(v), M_\delta(w) \leq \alpha$ and $(x, v), (y, w) \in (K \cap \bar{R})^{n+m}$ are isotropic vectors of $f \oplus g$ and $f \oplus -g$ respectively. Then

$$f(x) + g(v) = 0 \tag{1}$$
$$f(y) - g(w) = 0 \tag{2}$$

If $x = 0$ then $v \neq 0$ as (x, v) is an isotropic vector of $f \oplus g$. But $g(v) = -f(0) = 0$. If we let $e_n := (1, \ldots, 1) \in K^n$ then $(f \otimes g)(e_n \otimes v) = f(e_n) \cdot g(v) = 0$ and thus $e_n \otimes v \in (K \cap \bar{R})^{nm}$ is an isotropic vector of $f \otimes g$ and $M_\delta(e_n \otimes v) = M_\delta(v) \leq \alpha$. Hence $f \otimes g$ and therefore also $2 \times (f \otimes g)$ is α-isotropic. But then $2 \times (f \otimes g)$ is also 2α-isotropic over K.

If $w = 0$ then $y \neq 0$ and we can treat this case in a similar way as above. Now suppose that $x, w \neq 0$. We multiply equation (1) by $g(w)$ and equation (2) by $g(v)$. Adding the obtained equations one gets

$$0 = f(x)g(w) + f(y)g(v) = (f \otimes g)(x \otimes w) + (f \otimes g)(y \otimes v)$$

As $x, w \neq 0$ also $x \otimes w \neq 0$ and thus $(x \otimes w, y \otimes v) \in (K \cap \bar{R})^{2nm}$ is an isotropic vector of $2 \times (f \otimes g)$. The estimates $M_\delta(x \otimes w) \leq M_\delta(x) + M_\delta(w) \leq 2\alpha$ and $M_\delta(y \otimes v) \leq M_\delta(y) + M_\delta(v) \leq 2\alpha$ are obvious. $\square$

Now we study the behaviour of our quantitative notion of isotropy of quadratic forms under field extensions. First we treat the case of a quadratic extension.

Lemma 7.3: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let $z \in R \backslash \{0\}, \alpha \in \Gamma_{\geq 0}$ and suppose that q is a quadratic form over K which is α-isotropic over $K(\sqrt{z})$. Then $q \oplus zq$ is $(\alpha + \frac{1}{2}\delta(z))$-isotropic over K.*

Proof: Let $q(X_1,\dots,X_n) = \sum_{i,j} a_{ij}X_iX_j$. By assumption there is an isotropic vector $x = (x_1,\dots,x_n) \in (K(\sqrt{z}) \cap \bar{R})^n$ such that $M_\delta(x) \le \alpha$.

If $K(\sqrt{z}) = K$ then $x \in R^n$ and $(x_1,\dots,x_n,0,\dots,0) \in R^{2n}$ is an isotropic vector of $q \oplus zq$. Thus $q \oplus zq$ is α-isotropic and hence $(\alpha + \frac{1}{2}\delta(z))$-isotropic over K because $\delta(z) \ge 0$.

Now assume that $K(\sqrt{z})/K$ is a proper extension. Every coordinate $x_i \in K(\sqrt{z})$ we express in the form $x_i = b_i + \sqrt{z}c_i$ for certain $b_1,\dots,b_n,c_1,\dots,c_n \in K$. Let $b := (b_1,\dots,b_n)$ and $c := (c_1,\dots,c_n)$. An easy computation shows

$$0 = q(x) = q(b) + zq(c) + \sqrt{z} \cdot \sum_{i,j} a_{ij}(b_ic_j + b_jc_i)$$

By assumption $\sqrt{z} \notin K$ and thus $\sum_{i,j} a_{ij}(b_ic_j + b_jc_i) = 0$. This implies $q(b) + zq(c) = 0$. If we define $y_i := b_i - \sqrt{z}c_i$ $(1 \le i \le n)$, then x_i and y_i are conjugate over K and thus $\delta(y_i) = \delta(x_i) \le \alpha$ $(1 \le i \le n)$.

Furthermore the elements $y_1,\dots,y_n$ are integral over R, because $x_1,\dots,x_n$ are integral over R and R is integrally closed in K. Therefore also $2b_i = x_i + y_i \in \bar{R}$ and $2\sqrt{z}c_i = x_i - y_i \in \bar{R}$ and we have the estimates $\delta(2b_i) \le \max(\delta(x_i),\delta(y_i)) \le \alpha$ and $\delta(2\sqrt{z}c_i) \le \alpha$. As $2b_i \in K$ we obtain $2b_i \in K \cap \bar{R} = R$. Finally, since $z, 2\sqrt{z}c_i \in \bar{R}$ also $2zc_i \in \bar{R} \cap K = R$ and $\delta(2zc_i) \le \alpha + \frac{1}{2}\delta(z)$. Now $q(2zc) + zq(2b) = 4z(q(b) + zq(c)) = 0$ and therefore $(2zc_1,\dots,2zc_n,2b_1,\dots,2b_n) \in R^{2n}$ is an isotropic vector of $q \oplus zq$. This proves the lemma. $\square$

Lemma 7.4: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \ne 2$. Let further $\alpha \in \Gamma_{\ge 0}$ and $z \in R\setminus\{0\}$ and assume that q is a quadratic form over K which is α-isotropic over $K(\sqrt{z})$ and also over $K(\sqrt{-z})$. Then $2 \times (q \otimes q)$ is $(2\alpha + \delta(z))$-isotropic w.r.t. (R,δ) over K.*

Proof: By Lemma 7.3 we get that the quadratic forms $q \oplus zq$ and $q \oplus -zq$ are both $(\alpha + \frac{1}{2}\delta(z))$-isotropic over K. By Lemma 7.2 the form $2 \times (q \otimes zq)$ is $(2\alpha + \delta(z))$-isotropic over K. Now note that an isotropic vector of $2 \times (q \otimes zq)$ is also an isotropic vector of $2 \times (q \otimes q)$ and thus the lemma is proved. $\square$

Lemma 7.5: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \ne 2$. Let $\alpha, \beta \in \Gamma_{\ge 0}$, $a, b \in R$ such that $\delta(a), \delta(b) \le \beta$. Assume that q is a quadratic form over K which is α-isotropic w.r.t. (R,δ) over $K(\sqrt{a^2+b^2})$. Then $3 \times q$ is $(\alpha + 2\beta)$-isotropic w.r.t. (R,δ) over K.*

Proof: Since $\delta(a^2+b^2) \le 2\beta$ we get by Lemma 7.3 that $q \oplus (a^2+b^2)q$ is $(\alpha+\beta)$-isotropic w.r.t. (R,δ) over K. Denote the dimension of q by n and let $x = (x_1,\dots,x_{2n}) \in R^{2n}$ be an isotropic vector of $q \oplus (a^2+b^2)q$ such that $M_\delta(x) \le \alpha + \beta$. Then

$$0 = q(x_1,\dots,x_n) + (a^2+b^2) \cdot q(x_{n+1},\dots,x_{2n})$$

and thus $y = (x_1,\dots,x_n,ax_{n+1},\dots,ax_{2n},bx_{n+1},\dots,bx_{2n}) \in R^{3n}$ is an isotropic vector of $3 \times q$ and $M_\delta(y) \le \alpha + 2\beta$. $\square$

Theorem 7.6: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta: \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let further L be a subfield of $\bar{K}$ which contains K and let $\alpha \in \Gamma_{\geq 0}$. Suppose that $z \in L^{\times}$ is integral over R and assume that q is a quadratic form over L which is α-isotropic over every semi-extension F of $L(\sqrt{z})$ which contains K. Then $6 \times (q \otimes q)$ is $(2\alpha + 3\delta(z))$-isotropic over each semi-extension E of L which contains K.*

Proof: Let E be a semi-extension of L which contains K. By Theorem 6.6 there are $a, b \in \bar{R} \cap E$ and $u \in \bar{R} \cap E(\sqrt{a^2+b^2})$ such that $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$ are semi-extensions of $L(\sqrt{z})$ and $\delta(a), \delta(b), \delta(u) \leq \delta(z)$. By assumption q is α-isotropic w.r.t. (R, δ) over both fields $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$. By Corollary 3.4 , δ is also A-stable where A is the integral closure of R in $E(\sqrt{a^2+b^2})$, and by Lemma 7.1 the form q is also α-isotropic w.r.t. (A, δ) over both fields $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$. Thus we may apply Lemma 7.4 to obtain that $2 \times (q \otimes q)$ is $(2\alpha + \delta(z))$-isotropic over $E(\sqrt{a^2+b^2})$ w.r.t. (A, δ) and therefore also w.r.t. (R, δ).

Now let B be the integral closure of R in E. Then δ is also B-stable and by Lemma 7.5 the form $6 \times (q \otimes q)$ is $(2\alpha + 3\delta(z))$-isotropic over E w.r.t. (B, δ) and hence also w.r.t. (R, δ) by Lemma 7.1. This proves the theorem. $\square$

The next result is a quantitative version of Springer's theorem on odd extensions (cf. [26], Chap. 7, Theorem 2.3). We only consider the case of a separable extension.

Lemma 7.7: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta: \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Let $L = K(z)$ be a separable extension of K of odd degree $n = [L : K]$ and suppose that z is integral over R. Let furthermore $\alpha, \beta \in \Gamma_{\geq 0}$, $a_1, \ldots, a_m \in R \setminus \{0\}$, $\delta(a_i) \leq \beta$ $(1 \leq i \leq r)$ and assume that the quadratic form $q =< a_1, \ldots, a_m >$ is α-isotropic over L. Then q is*

$$2^n n! \cdot (2\alpha + \beta + 2n^2\delta(z)) - \text{isotropic}$$

over K.

Proof: We prove the statement by induction on n. The case $n = 1$ is obvious. Now let $n > 1$. Then

$$g := \mathrm{Irr}(z, K)$$

is a polynomial of degree n with coefficients in R since z is integral over R. By d we denote the discriminant of g. Then $d \in R \setminus \{0\}$ and

$$\delta(d) \leq n(n-1)\delta(z)$$

by Theorem 3.5(a) and (b). By assumption there is an isotropic vector $u = (u_1, \ldots, u_m) \in (L \cap \bar{R})^m$ of q such that $\delta(u_i) \leq \alpha$. W.l.o.g. we may assume that $u_1, \ldots, u_m \neq 0$. Now apply Theorem 3.5(c) to obtain elements $b_{ij} \in R$ such that

$$d \cdot u_i = \sum_{j=0}^{n-1} b_{ij} z^j \qquad (1 \leq i \leq m)$$

(1) $$\delta(b_{ij}) \leq n(n-1)\delta(z) + \alpha$$

and let

$$f_i(X) := \sum_{j=0}^{n-1} b_{ij} X^j \in R[X] \qquad (1 \le i \le m)$$

and

$$f(X) := \sum_{i=1}^{m} a_i f_i(X)^2 \in R[X]$$

From the construction follows $f_i(z) = d \cdot u_i \neq 0$ and thus

$$f(z) = d^2 \cdot \sum_{i=1}^{m} a_i u_i^2 = d^2 \cdot q(u) = 0 \tag{2}$$

Furthermore $f_1, \ldots, f_m \neq 0$. Immediately by (1) we get

$$M_\delta(f_i) \le n(n-1)\delta(z) + \alpha \qquad (1 \le i \le m) \tag{3}$$

and thus

$$M_\delta(f) = M_\delta(\sum_{i=1}^{m} a_i f_i^2) \le 2\alpha + \beta + 2n(n-1)\delta(z) \tag{4}$$

By s_i we denote the degree of f_i and we let s be the maximum of $s_1, \ldots, s_m$. Then $s \le n-1$. By b_i we denote the coefficient of f_i corresponding to X^s. Then not all b_i's are zero and $\delta(b_i) \le n(n-1)\delta(z) + \alpha$ according to (1), since $b_1, \ldots, b_m$ are among the elements b_{ij}. Furthermore $\deg f \le 2s$. Now we distinguish two cases.

Case 1: $\deg f < 2s$

Then $\sum_{i=1}^{m} b_i^2 = 0$ and thus $(b_1, \ldots, b_m) \in R^m$ is an isotropic vector of q. Consequently q is even $(2\alpha + \beta + 2n(n-1)\delta(z))$-isotropic in this case.

Case 2: $\deg f = 2s$

In particular $f \neq 0$. We denote the leading coefficient of f by a. Then $a \in R$ and hence

$$0 \le \delta(a) \le M_\delta(f) \tag{5}$$

Let

$$\begin{aligned} F(X) &:= a^{2s-1} f(a^{-1}X) \\ G(X) &:= a^n g(a^{-1}X) \\ G_i(X) &:= a^{s_i} f_i(a^{-1}X) \quad (1 \le i \le m) \end{aligned}$$

From Lemma 2.18, Proposition 2.11 and (5) we get

$$\bar{M}_\delta(G_i) \le \bar{M}_\delta(f_i) + \delta(a) \le M_\delta(f_i) + M_\delta(f) \tag{6}$$

Immediate by the above definitions we obtain

$$F(X) = a^{-1} \cdot \sum_{i=1}^{m} a_i a^{2(s-s_i)} G_i(X)^2 \tag{7}$$

One can easily see that F and G are monic polynomials with coefficients from R. Also $G_i \in R[X]$. Since g is irreducible in $K[X]$ so is G. Furthermore $\deg F = \deg f = 2s$ and $\deg G = \deg g = n$. Since $G(az) = a^n g(z) = 0$ we obtain that $G = \mathrm{Irr}(az, K)$. From (2) we obtain $F(az) = a^{2s-1} f(z) = 0$, and thus G divides F. Hence $F = G \cdot h$ for some $h \in K[X]$. Since F, G are monic also h is monic and as n is odd also $\deg h = \deg F - \deg G = 2s - n$ is odd. Since $s \leq n-1$, this furthermore yields $\deg h \leq n-2$.

Now we split h in $K[X]$ into a product of monic irreducible polynomials

$$h = \prod_{i=1}^{t} h_i^{\nu_i}$$

Then all the h_i's divide F, and since $F \in R[X]$ is monic we get $h_i \in R[X]$, because R is integrally closed in K. As $\deg h$ is odd there is some i such that $\deg h_i$ and ν_i are odd. W.l.o.g we may assume that $\deg h_1$ and ν_1 are odd. Now let ℓ be the maximal natural number j such that h_1^j divides all the polynomials $G_1, \ldots, G_m$, possibly $\ell = 0$. Then write

$$G_i(X) = h_1(X)^\ell \cdot p_i(X) \quad (1 \leq i \leq m)$$

for certain $p_1, \ldots, p_m \in K[X]$. As $G_i \in R[X]$ and $h_1 \in R[X]$ is monic we get $p_1, \ldots, p_m \in R[X]$. Then by (7)

$$G \cdot \prod_{i=1}^{t} h_i^{\nu_i} = G \cdot h = F = a^{-1} \cdot \sum_{i=1}^{m} a_i a^{2(s-s_i)} G_i^2 = a^{-1} \cdot h_1^{2\ell} \cdot \sum_{i=1}^{m} a_i a^{2(s-s_i)} p_i^2$$

G and h_1 are both monic and irreducible. Since $\deg h_1 \leq \deg h \leq n-2$ but $\deg G = n$ they are different and hence $\nu_1 \geq 2\ell$ by the uniqueness of the factorization. Since ν_1 is odd we even obtain $\nu_1 > 2\ell$. Thus

$$\sum_{i=1}^{m} a_i a^{2(s-s_i)} p_i^2 = a G h_1^{\nu_1 - 2\ell} \cdot \prod_{i=2}^{t} h_i^{\nu_i} = p \cdot h_1 \tag{8}$$

for some $p \in K[X]$. Now we split h_1 in $\bar{K}[X]$ into linear factors

$$h_1(X) = \prod_{i=1}^{k} (X - y_i)$$

As $h_1 \in R[X]$ is monic we get $y_1, \ldots, y_k \in \bar{R}$. As h_1 divides F also $F(y_i) = 0$ and thus $f(a^{-1} y_i) = 0$. Then Theorem 2.14 and Proposition 2.11 imply

$$\delta(y_i) \leq \bar{M}_\delta(f) \leq M_\delta(f) \tag{9}$$

The estimate (9) and Lemma 2.15 applied to h_1^ℓ yield

$$\bar{M}_\delta(h_1^\ell) \le M_\delta(f) \tag{10}$$

Since h_1^ℓ is monic we obtain from Proposition 2.13, (6) and (10)

$$\bar{M}_\delta(p_i) \le \bar{M}_\delta(h_1^\ell p_i) + \bar{M}_\delta(h_1^\ell) = \bar{M}_\delta(G_i) + \bar{M}_\delta(h_1^\ell) \le 2M_\delta(f) + M_\delta(f_i) \tag{11}$$

Let $w_i := a^{s-s_i} p_i(y_1) \in K(y_1) \cap \bar{R}$. Not all w_i's are zero. Otherwise h_1 would divide all the polynomials $p_1, \dots, p_m$, contradicting the maximality of ℓ. From (8) we get

$$\sum_{i=1}^m a_i w_i^2 = \sum_{i=1}^m a_i a^{2(s-s_i)} p_i(y_1)^2 = p(y_1) \cdot h_1(y_1) = 0$$

and hence $w := (w_1, \dots, w_m) \in (\bar{R} \cap K(y_1))^m$ is an isotropic vector of q.
Since $\deg p_i \le \deg G_i = \deg f_i = s_i$ we get from (9), (11) and Lemma 2.16

$$\delta(p_i(y_1)) \le (s_i + 1) \cdot \max(\bar{M}_\delta(p_i), \delta(y_1), 0) \le (s_i + 1) \cdot (2M_\delta(f) + M_\delta(f_i)) \tag{12}$$

Taking into account that $s_i \le s \le n-1$ we obtain from (5) and (12)

$$\delta(w_i) \le (s - s_i)\delta(a) + \delta(p_i(y_1)) \le n \cdot (2M_\delta(f) + M_\delta(f_i))$$

Finally (3) and (4) imply

$$\delta(w_i) \le 5n\alpha + 2n\beta + 5n^2(n-1)\delta(z) =: \alpha' \tag{13}$$

Thus q is α'-isotropic over $K(y_1)$. Since

$$[K(y_1) : K] = \deg h_1 \le \deg h \le n - 2$$

and $\deg h_1$ is odd, we obtain by the induction hypothesis that the quadratic form q is $(2^{n-2}(n-2)!\ (2\alpha' + \beta + 2(n-2)^2\delta(y_1))$- isotropic over K. Since $n \ge 3$ we get by (13), (9) and (4)

$$\begin{aligned} 2\alpha' + \beta + 2(n-2)^2\delta(y_1) &\le 4n^2\alpha + 2n^2\beta + 4n^3(n-1)\delta(z) \\ &\le 2n^2 \cdot (2\alpha + \beta + 2n^2\delta(z)) \end{aligned}$$

Therefore

$$2^{n-2}(n-2)!\ (2\alpha' + \beta + 2(n-2)^2\delta(y_1)) \le 2^n n!\ (2\alpha + \beta + 2n^2\delta(z))$$

since $n \le 2(n-1)$ and we are done. $\square$

Theorem 7.8: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Let $L = K(z_1, \dots, z_r)$ be a separable extension of K of odd degree $n = [L : K]$ and suppose that $z_1, \dots, z_r$ are integral over R and $\delta(z_i) \le \gamma$ $(1 \le i \le r)$. Let furthermore $a_1, \dots, a_m \in R \setminus \{0\}$, $\delta(a_i) \le \beta$ $(1 \le i \le r)$ and assume that the quadratic form $q =< a_1, \dots, a_m >$ is α-isotropic over L. Then q is*

$$2^n n! \cdot (2\alpha + \beta + 2n^2\gamma) - \text{isotropic}$$

over K.

Proof: The proof runs by induction on r. The case $r = 1$ is exactly the statement of Lemma 7.7. Now suppose that $r > 1$ and let $F := K(z_1, \dots, z_{r-1})$. Then $L = F(z_r)$. If $F = K$ the assertion follows immediately from the lemma above. If $L = F$ the induction hypothesis can be applied to obtain the result. So we may assume that $K \neq F \neq L$. Then $k = [F : K] \geq 3$ and also $\ell = [L : F] \geq 3$. Denote the integral closure of R in F by S. Then Corollary 3.4 applied to the extensions $K \subset F \subset \bar{K}$ yields that δ is S-stable. By Lemma 7.7 the form q is $2^\ell \ell! \cdot (2\alpha + \beta + 2\ell^2\gamma)$-isotropic over F w.r.t. (S, δ) and hence also w.r.t. (R, δ) as S/R is integral. Now, by the induction hypothesis q is $2^k k! \cdot (2^{\ell+1}\ell! \cdot (2\alpha + \beta + 2\ell^2\gamma) + \beta + 2k^2\gamma)$-isotropic over K w.r.t. (R, δ). Now

$$\begin{aligned} 2^k k! \cdot (2^{\ell+1}\ell! \cdot (2\alpha + \beta + 2\ell^2\gamma) + \beta + 2k^2\gamma) &\leq 2^k \cdot k! \cdot 2^{\ell+1} \cdot \ell! \cdot (2\alpha + 2\beta + 2(k^2 + \ell^2)\gamma) \\ &\leq 2^{k+\ell+2} \cdot k! \cdot \ell! \cdot (2\alpha + \beta + 2(k^2 + \ell^2)\gamma) \end{aligned}$$

Now $k, \ell \geq 3$ implies $n = k \cdot \ell \geq k + \ell + 2$, $k! \cdot \ell! \leq n!$ and $k^2 + \ell^2 \leq n^2$. This finally yields the result. □

Remark:
Note that Theorem 7.8 is not an immediate consequence of Lemma 7.7. Of course, by a well-known fact from elementary algebra, L/K admits a primitive element z. But, unless $\mathrm{char}(K) = 0$, we do not know a bound for $\delta(z)$ in terms of γ. If $\mathrm{char}(K) = 0$ there are $a_1, \dots, a_r \in \mathbb{N}$ such that $z = \sum_{i=1}^r a_i z_i$ is a primitive element. This element satisfies $\delta(z) \leq \gamma$. If $\mathrm{char}(K) \neq 0$ there is also a primitive element z of the form $z = \sum_{i=1}^r a_i z_i$ for certain $a_1, \dots, a_r \in K$, provided that K is infinite. But there is no information about $\delta(a_1), \dots, \delta(a_r)$ and $\delta(z)$, because $a_1, \dots, a_r$ possibly cannot be chosen from the prime field of K.

Now we are able to prove the main result of this chapter.

Theorem 7.9: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let L/K be a finite Galois extension of degree n with a primitive element ϑ and assume that ϑ is integral over R. Suppose that $\alpha, \beta \in \Gamma_{\geq 0}$. Let furthermore $a_1, \dots, a_m \in R$, $\delta(a_i) \leq \beta$ and assume that the quadratic form $q =< a_1, \dots, a_m >$ is α-isotropic over every semi-extension of L which contains K. Then $6^{n-1} \times q^n$ is $2^n n! \cdot (2\alpha + \beta + 2n^2\delta(\vartheta))$-isotropic over K.*

Proof: Let $[L : K] = n = 2^r \cdot s$ with s odd and choose a 2-Sylow subgroup H of $\mathrm{Gal}(L/K)$. Let F be its fixed field. Then F/K is a separable extension of odd degree s and L/F is a 2-extension of degree $[L : F] = 2^r$. Since H is a 2-group of order 2^r there is an ascending chain of subgroups

$$\{\mathrm{id}\} = H_0 \subsetneqq H_1 \subsetneqq \dots \subsetneqq H_r = H$$

such that $[H_{i+1} : H_i] = 2$ $(0 \leq i \leq r - 1)$. Let F_i be the fixed field of H_i and let R_i be the integral closure of R in F_i. By finite Galois theory

$$F = F_r \subsetneqq F_{r-1} \subsetneqq \dots \subsetneqq F_1 \subsetneqq F_0 = L$$

and $[F_i : F_{i+1}] = 2$ $(0 \leq i \leq r-1)$. Now we show by induction on $i = 0, \ldots, r$ that $6^{2^i-1} \times q^{2^i}$ is $2^i \cdot (\alpha + 3i\delta(\vartheta))$-isotropic w.r.t (R, δ) over every semi-extension of F_i which contains K. The case $i = 0$ follows from our assumptions.

Let $i > 0$. Since δ is also R_{i+1}-stable by Corollary 3.4, we may apply Corollary 3.7 to the situation $F_{i+1} \subset F_i \subset L = K(\vartheta) = F_{i+1}(\vartheta)$ to obtain some $z \in R_{i+1}$ such that $F_i = F_{i+1}(\sqrt{z})$ and

$$\delta(z) \leq [L : F_{i+1}] \cdot \delta(\vartheta) = 2^{i+1} \cdot \delta(\vartheta)$$

By the induction hypothesis $6^{2^i-1} \times q^{2^i}$ is $2^i \cdot (\alpha + 3i\delta(\vartheta))$-isotropic w.r.t (R, δ), and hence also w.r.t. (R_{i+1}, δ), over every semi-extension of F_i which contains K. Then Theorem 7.6 implies that $6 \times (6^{2^i-1} \times q^{2^i})^2$ is $(2 \cdot 2^i(\alpha + 3i\delta(\vartheta)) + 3\delta(z))$-isotropic w.r.t. (R_{i+1}, δ) over every semi-extension of F_{i+1} which contains K. Now the estimate

$$\begin{aligned} 2 \cdot 2^i(\alpha + 3i\delta(\vartheta)) + 3\delta(z) &\leq 2^{i+1}(\alpha + 3i\delta(\vartheta)) + 3 \cdot 2^{i+1} \cdot \delta(\vartheta) \\ &= 2^{i+1} \cdot (\alpha + 3(i+1)\delta(\vartheta)) \end{aligned}$$

yields the induction step.

In particular we obtained that $6^{2^r-1} \times q^{2^r}$ is $2^r \cdot (\alpha + 3r\delta(\vartheta))$-isotropic w.r.t (R, δ) over F. By Theorem 3.6 there are $t \in \mathbb{N}$ and $z_1, \ldots, z_t$, integral over R such that $F = K(z_1, \ldots, z_t)$, $2^t \leq [F : K] = s$ and $\delta(z_i) \leq [L : F]\delta(\vartheta) = 2^r\delta(\vartheta)$. Thus by Theorem 7.8 the quadratic form $6^{2^r-1} \times q^{2^r}$ is $2^s s! \cdot (2 \cdot 2^r(\alpha + 3r\delta(\vartheta)) + \beta + 2s^2 2^r\delta(\vartheta))$-isotropic w.r.t. (R, δ) over K. Since

$$\begin{aligned} 2^s s! \cdot (2 \cdot 2^r(\alpha + 3r\delta(\vartheta)) + \beta + 2s^2 2^r\delta(\vartheta)) &\leq 2^s 2^r s! \cdot (2\alpha + \beta + 2(3r + s^2)\delta(\vartheta)) \\ &\leq 2^n n!(2\alpha + \beta + 2(3r + s^2)\delta(\vartheta)) \end{aligned}$$

and $3r + s^2 \leq 4^r s^2 = n^2$, this yields the assertion and the theorem is proved. $\square$

Chapter 8

The size of congruences

In this chapter we introduce a quantitative notion of the congruence of two quadratic matrices over a field with a degree function. The main result (Theorem 8.18) is a local-global-principle for the quantitative congruence of matrices.

We fix some notations. If R is an arbitrary ring then $M_n(R)$ denotes the set of $n \times n$-matrices with entries from R. If $A \in M_n(R)$ and $B \in M_m(R)$ we let $A \oplus B \in M_{n+m}(R)$ be the block matrix

$$A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in M_{n+m}(R)$$

Obviously $\oplus$ is not commutative but associative. For a natural number $k \in \mathbb{N}$ we let $k \times A$ be the k-fold sum $A \oplus \ldots \oplus A$. For $A = (a_{ij}) \in M_n(R)$ and $B \in M_m(R)$ we let $A \otimes B \in M_{nm}(R)$ be the Kronecker product of A and B, i.e.

$$A \otimes B = \begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \ldots & a_{nn}B \end{pmatrix}$$

An easy but tedious computation shows that $\otimes$ is associative. For a natural number k we let $A^{\otimes k}$ be the k-fold Kronecker product $A \otimes \ldots \otimes A$. If $a_1, \ldots, a_n \in R$ we let $\operatorname{diag}(a_1, \ldots, a_n)$ be the diagonal matrix with the entries $a_1, \ldots, a_n$ in its diagonal.

As in the previous chapters we denote the algebraic closure of a field K by $\bar{K}$, and for a domain R we denote by $\bar{R}$ the integral closure of R in the algebraic closure of $\operatorname{Quot}(R)$.

In the sequel we will make use of the following easy properties which are listed in the following three lemmas.

Lemma 8.1: *Let $A_1, \ldots, A_n, B_1, \ldots, B_n$ be quadratic matrices over the field K and suppose that for each i the matrices A_i and B_i are of the same size. Then*

$$\oplus_{i=1}^{n} A_i \cdot \oplus_{i=1}^{n} B_i = \oplus_{i=1}^{n} (A_i \cdot B_i)$$

Proof: Elementary □

Lemma 8.2: *Let K be a field. Then:*

(a) $(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = A_1 A_2 \otimes B_1 B_2$ *for all* $A_1, A_2 \in M_n(K), B_1, B_2 \in M_m(K)$

(b) $(A \otimes B)^T = A^T \otimes B^T$ *for all* $A \in M_n(K), B \in M_m(K)$

Proof: Elementary computation □

Lemma 8.3: *Suppose that K is a field and let $A_i \in M_{n_i}(K)$ $(1 \leq i \leq r)$, $B \in M_m(K)$. Then*

$$(\oplus_{i=1}^{r} A_i) \otimes B = \oplus_{i=1}^{r} (A_i \otimes B)$$

Proof: Elementary □

Definition: *Let R be a subdomain of the field K. Then we let*

$$M_n^{\times}(K, R) := M_n(K \cap \bar{R}) \cap \mathrm{GL}(n, K)$$

Definition: *Let R be a subdomain of the field K and suppose that that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further $\alpha \in \Gamma_{\geq 0}$. Two matrices $A, B \in M_n(L)$ are called α-congruent over K w.r.t. (R, δ) if there are $P, Q \in M_n^{\times}(K, R)$ and $a, b \in K^{\times} \cap \bar{R}$ such that $M_\delta(P), M_\delta(Q), \delta(a), \delta(b) \leq \alpha$ and*

$$P^T A P = a^2 B$$
$$Q^T B Q = b^2 A$$

Remark: If it is clear from the context which triple (K, R, δ) α-congruence refers at, we will omit the phrase "w.r.t. (R, δ) over K" or parts of it. If A and B are α-congruent we will denote this by $A \equiv_\alpha B$.

Lemma 8.4: *Let $R \subset S$ be two subdomains of the field K and suppose that S/R is an integral extension. Assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K and let $\alpha \in \Gamma_{\geq 0}$. Then two matrices $A, B \in M_n(K)$ are α-congruent w.r.t. (R, δ) over K iff they are α-congruent w.r.t. (S, δ) over K.*

Proof: Immediate by the definition. □

Lemma 8.5: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A, B, C \in M_n(K)$ and $\alpha, \beta \in \Gamma_{\geq 0}$. Then:*

(a) $A \equiv_0 A$

(b) *If* $A \equiv_\alpha B$ *then* $B \equiv_\alpha A$

(c) *If* $A \equiv_\alpha B$ *and* $B \equiv_\beta C$ *then* $A \equiv_{\alpha+\beta} C$

Proof: Elementary □

Lemma 8.6: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A_i \in M_{n_i}(K)$ $(1 \leq i \leq m)$. Then $\oplus_{i=1}^m A_i \equiv_0 \oplus_{i=1}^m A_{\sigma(i)}$ for each permutation $\sigma \in S_m$.*

Proof: Elementary □

Lemma 8.7: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A, B \in M_n(K)$, $\alpha \in \Gamma_{\geq 0}$ and $a \in K^\times$. If $A \equiv_\alpha B$ then also $aA \equiv_\alpha aB$.*

Proof: Elementary □

Lemma 8.8: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A_1, A_2 \in M_n(K)$, $B_1, B_2 \in M_m(K)$ and $\alpha, \beta \in \Gamma_{\geq 0}$. Assume that $A_1 \equiv_\alpha A_2$ and $B_1 \equiv_\beta B_2$. Then $(A_1 \oplus B_1) \equiv_{\alpha+\beta} (A_2 \oplus B_2)$ and $(A_1 \otimes B_1) \equiv_{\alpha+\beta} (A_2 \otimes B_2)$.*

Proof: By assumption there are $P \in M_n^\times(K, R)$, $Q \in M_m^\times(K, R)$ and $a, b \in K^\times \cap \bar{R}$ such that $M_\delta(P), \delta(a) \leq \alpha$, $M_\delta(Q), \delta(b) \leq \beta$ and

$$\begin{aligned} P^T A_1 P &= a^2 A_2 \\ Q^T B_1 Q &= b^2 B_2 \end{aligned}$$

Define $U := bP \oplus aQ$. Then $U \in M_{n+m}^\times(K, R)$ and $M_\delta(U) \leq \alpha + \beta$ and

$$\begin{aligned} U^T (A_1 \oplus B_1) U &= \begin{pmatrix} bP^T & 0 \\ 0 & aQ^T \end{pmatrix} \cdot \begin{pmatrix} A_1 & 0 \\ 0 & B_1 \end{pmatrix} \cdot \begin{pmatrix} bP & 0 \\ 0 & aQ \end{pmatrix} \\ &= \begin{pmatrix} a^2 b^2 A_2 & 0 \\ 0 & a^2 b^2 B_2 \end{pmatrix} = (ab)^2 (A_2 \oplus B_2) \end{aligned}$$

Furthermore by Lemma 8.2 we get

$$(P \otimes Q)^T (A_1 \otimes B_1)(P \otimes Q) = P^T A_1 P \otimes Q^T B_1 Q = a^2 A_2 \otimes b^2 B_2 = (ab)^2 A_2 \otimes B_2$$

and since $(P \otimes Q) \cdot (P^{-1} \otimes Q^{-1}) = PP^{-1} \otimes QQ^{-1} = E_n \otimes E_m = E_{nm}$ the matrix $P \otimes Q$ is regular. Obviously $M_\delta(P \otimes Q) \leq \alpha + \beta$. The same argument with (A_1, B_1) and (A_2, B_2) interchanged yields the result. □

Lemma 8.9: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A, B \in M_n(K)$, $\alpha \in \Gamma_{\geq 0}$ and assume that $A \equiv_\alpha B$. Then also $m \times A \equiv_\alpha m \times B$ for every natural number $m \geq 1$.*

Proof: By assumption there are $P, Q \in M_n^\times(K, R)$ and elements $a, b \in K^\times \cap \bar{R}$ such that $M_\delta(P), M_\delta(Q), \delta(a), \delta(b) \leq \alpha$ and $P^T A P = a^2 B$ and $Q^T B Q = b^2 A$. By Lemma 8.1 we obtain

$$(m \times P)^T \cdot (m \times A) \cdot (m \times P) = a^2 (m \times B)$$
$$(m \times Q)^T \cdot (m \times B) \cdot (m \times Q) = b^2 (m \times A)$$

This proves the lemma. □

The following two propositions are needed in the last chapter. Before we state the results we introduce some notion.

If $A = (a_{ij})$ is a symmetric $(n \times n)$-matrix over a field K we let $q_{_A}$ be the corresponding quadratic form, i.e.,

$$q_{_A}(X_1, \ldots, X_n) := \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} X_i X_j$$

Proposition 8.10: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $A, B \in M_n(K)$ be symmetric and let $\alpha, \beta \in \Gamma_{\geq 0}$. Suppose that $A \equiv_\alpha B$ and $q_{_A}$ is β-isotropic over K. Then $q_{_B}$ is $(\alpha + \beta)$-isotropic over K.*

Proof: By definition there are $P \in M_n^\times(K, R)$ and $a \in K^\times \cap \bar{R}$ such that $M_\delta(P), \delta(a) \leq \alpha$ and $P^T B P = a^2 A$. Furthermore, there is an isotropic vector $x \in (K \cap \bar{R})^n$ of $q_{_A}$ such that $M_\delta(x) \leq \beta$. Then

$$q_{_B}(Px) = (Px)^T B (Px) a^2 x^T A x = a^2 q_{_A}(x) = 0$$

Since P is regular and $x \neq 0$ also $Px \neq 0$. Thus $Px \in (K \cap \bar{R})^n$ is an isotropic vector of $q_{_B}$ and furthermore $M_\delta(Px) \leq \alpha + \beta$. □

Proposition 8.11: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let further $a \in R \backslash \{0\}$. Then*

$$\operatorname{diag}(1, a)^{\otimes n} \equiv_{\max((n-1)\delta(a), 0)} 2^n \times \operatorname{diag}(1, a)$$

for all natural numbers n.

Proof: We prove the assertion by induction on n. The case $n = 1$ is clear. From

$$\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^2 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & a^2 \end{pmatrix} \cdot \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = a^2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

follows immediately $\operatorname{diag}(1, a) \equiv_{\max(\delta(a), 0)} \operatorname{diag}(a, a^2)$. Since

$$\operatorname{diag}(1, a)^{\otimes 2} = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \oplus \begin{pmatrix} a & 0 \\ 0 & a^2 \end{pmatrix}$$

we obtain from Lemma 8.8

$$(1) \qquad \mathrm{diag}(1,a)^{\otimes 2} \equiv_{\max(\delta(a),0)} 2 \times \mathrm{diag}(1,a)$$

which proves the case $n = 2$. Now let $n > 2$. By the induction hypothesis one gets

$$\mathrm{diag}(1,a)^{\otimes(n-1)} \equiv_{\max((n-2)\delta(a),0)} 2^{n-1} \times \mathrm{diag}(1,a)$$

Lemma 8.3 and Lemma 8.8 imply

$$(2) \qquad \mathrm{diag}(1,a)^{\otimes n} \equiv_{\max((n-2)\delta(a),0)} 2^{n-1} \times \mathrm{diag}(1,a)^{\otimes 2}$$

From (1) and Lemma 8.9 follows

$$2^{n-1} \times \mathrm{diag}(1,a)^{\otimes 2} \equiv_{\max(\delta(a),0)} 2^{n} \times \mathrm{diag}(1,a)$$

and together with (2) and Lemma 8.5 this yields the induction step. □

After these first results of preparatory character we now turn to the proof of the main result of this chapter. We proceed in a similar manner as in the last chapter. First we study the case of a quadratic extension.

Lemma 8.12: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that* $\mathrm{char}(K) \neq 2$. *Let $A, B \in \mathrm{GL}(n,K), z \in R\backslash\{0\}, \alpha \in \Gamma_{\geq 0}$ and assume that the matrices A, B are α-congruent over $K(\sqrt{z})$ w.r.t. (R,δ). Then there are $S \in M_{2n}(R) \cap \mathrm{GL}(2n,K)$ and $a \in R\backslash\{0\}$ such that*

(a) $S^T(A \oplus zA)S = a^2z^2(B \oplus zB)$

(b) $M_\delta(S) \leq \frac{3}{2}\delta(z) + 2\alpha$

(c) $\delta(a) \leq 2\alpha$

Proof: By assumption there are $U \in M_n^\times(K(\sqrt{z}), R)$ and $u \in K(\sqrt{z})^\times \cap \bar{R}$ such that

$$U^T A U = u^2 B$$

and $M_\delta(U), \delta(u) \leq \alpha$. If $K(\sqrt{z}) = K$ we let $S := zU \oplus zU$. Then

$$\begin{aligned} S^T(A \oplus zA)S &= \begin{pmatrix} zU^T & 0 \\ 0 & zU^T \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & zA \end{pmatrix} \cdot \begin{pmatrix} zU & 0 \\ 0 & zU \end{pmatrix} \\ &= \begin{pmatrix} z^2U^TAU & 0 \\ 0 & z^3U^TAU \end{pmatrix} = u^2z^2(B \oplus zB) \end{aligned}$$

Now assume that $K(\sqrt{z})/K$ is a proper extension and let $\sqrt{z}$ be a fixed square root of z. We express u in the form $u = b + \sqrt{z}c$ for some uniquely determined $b, c \in K$. Let $u' := b - \sqrt{z}c$. Then u, u' are conjugate over K. Hence u' is also integral over R and $\delta(u') = \delta(u) \leq \alpha$. Now define

$$a := 2uu' = 2(b^2 - zc^2) \in K^\times$$

Since u, u' are integral over R so is a. But as R is integrally closed in K we get $a \in R$. Furthermore $\delta(a) \le \delta(u) + \delta(u') \le 2\alpha$.

Let $u_{ij} \in K(\sqrt{z}) \cap \bar{R}$ be the entries of the matrix U and define $w_{ij} := u' u_{ij}$. The elements w_{ij} are integral over R. Let $W := (w_{ij})$. Then

$$4W^T AW = a^2 B$$

Each w_{ij} we express in the form $w_{ij} = b_{ij} + \sqrt{z} c_{ij}$ for certain $b_{ij}, c_{ij} \in K$ and let $w'_{ij} := b_{ij} - \sqrt{z} c_{ij}$. Then w_{ij}, w'_{ij} are conjugate over K and hence also the elements w'_{ij} are integral over R and $\delta(w'_{ij}) = \delta(w_{ij}) \le \delta(u') + \delta(u_{ij}) \le 2\alpha$.

Furthermore $2b_{ij} = w_{ij} + w'_{ij}$ and $2\sqrt{z} c_{ij} = w_{ij} - w'_{ij}$ are also integral over R and $\delta(2b_{ij}), \delta(2\sqrt{z} c_{ij}) \le 2\alpha$. Since z is integral over R and R is integrally closed in K we obtain that $2b_{ij}, 2zc_{ij} \in R$. Now let $P := (2b_{ij})$ and $Q := (2c_{ij})$. Then $P + \sqrt{z} \cdot Q = 2W$ and thus

$$\begin{aligned} a^2 B = 4W^T AW &= (P^T + \sqrt{z} Q^T) A (P + \sqrt{z} Q) \\ &= P^T AP + zQ^T AQ + \sqrt{z} \cdot (P^T AQ + Q^T AP) \end{aligned}$$

Since $\sqrt{z} \notin K$ we obtain by comparing the entries of the matrices

$$\begin{aligned} P^T AP + zQ^T AQ &= a^2 B \\ P^T AQ + Q^T AP &= 0 \end{aligned}$$

If we define

$$S := \begin{pmatrix} zP & z^2 Q \\ zQ & zP \end{pmatrix}$$

then $S \in M_{2n}(R)$ and

$$\begin{aligned} S^T (A \oplus zA) S &= \begin{pmatrix} zP^T & zQ^T \\ z^2 Q^T & zP^T \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & zA \end{pmatrix} \cdot \begin{pmatrix} zP & z^2 Q \\ zQ & zP \end{pmatrix} \\ &= \begin{pmatrix} z^2 a^2 B & 0 \\ 0 & z^3 a^2 B \end{pmatrix} = a^2 z^2 (B \oplus zB) \end{aligned}$$

and $M_\delta(zP) \le \delta(z) + 2\alpha$, $M_\delta(zQ) \le \delta(\sqrt{z}) + M_\delta(\sqrt{z} Q) \le \frac{1}{2}\delta(z) + 2\alpha$ and $M_\delta(z^2 Q) \le \frac{3}{2}\delta(z) + 2\alpha$. Thus also $M_\delta(S) \le \frac{3}{2}\delta(z) + 2\alpha$ as $\delta(z) \ge 0$. Note that S is regular since B and hence also $B \oplus zB$ is regular. □

Lemma 8.13: *Let R be a subdomain of the field K and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Assume that* $\mathrm{char}(K) \neq 2$. *Let $A \in M_n(K)$ and assume that $z \in R \backslash \{0\}$. Then*

$$(A \oplus -A) \equiv_{\max(\delta(z),0)} (zA \oplus -zA)$$

Proof: Let

$$P := \begin{pmatrix} (z+1)E_n & (z-1)E_n \\ (z-1)E_n & (z+1)E_n \end{pmatrix} \in M_{2n}(R)$$

For an arbitrary matrix $B \in M_n(K)$ holds

$$P^T \begin{pmatrix} B & 0 \\ 0 & -B \end{pmatrix} P = 4 \cdot \begin{pmatrix} zB & 0 \\ 0 & -zB \end{pmatrix}$$

Applying this equation to the case $B = E_n$ one gets after taking determinants

$$(\det P)^2 = (4z)^{2n} \neq 0$$

Thus $P \in \mathrm{GL}(2n, K)$. If we apply the above equation to the cases $B = A$ and $B = zA$ respectively we obtain the assertion. □

Proposition 8.14: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let $A, B \in \mathrm{GL}(n, K)$, $z \in R \backslash \{0\}$, $\alpha \in \Gamma_{\geq 0}$ and assume that A and B are α-congruent w.r.t. (R, δ) over both fields $K(\sqrt{z})$ and $K(\sqrt{-z})$. Then $A \oplus A \oplus A \oplus -A$ and $B \oplus B \oplus B \oplus -B$ are $(\frac{7}{2}\delta(z) + 4\alpha)$-congruent over K w.r.t. (R, δ).*

Proof: By Lemma 8.12 there are matrices $P, Q \in M_{2n}^{\times}(K, R)$ and $a, b \in R \backslash \{0\}$ such that $M_\delta(P), M_\delta(Q) \leq \frac{3}{2}\delta(z) + 2\alpha$, $\delta(a), \delta(b) \leq 2\alpha$ and

$$P^T(A \oplus zA)P = a^2 z^2 (B \oplus zB)$$
$$Q^T(A \oplus -zA)Q = b^2 z^2 (B \oplus -zB)$$

We let $U := bP \oplus aQ \in M_{4n}^{\times}(K, R)$. Then $M_\delta(U) \leq \frac{3}{2}\delta(z) + 4\alpha$ and an elementary computation yields

$$U^T(A \oplus zA \oplus A \oplus -zA)U = (abz)^2 (B \oplus zB \oplus B \oplus -zB)$$

The same argument with A and B interchanged yields that $A \oplus zA \oplus A \oplus -zA$ and $B \oplus zB \oplus B \oplus -zB$ are $(\frac{3}{2}\delta(z) + 4\alpha)$-congruent w.r.t. (R, δ) over K. Then Lemma 8.6, Lemma 8.8 and Lemma 8.13 imply that $3 \times A \oplus -A$ and $3 \times B \oplus -B$ are $(\frac{7}{2}\delta(z) + 4\alpha)$-congruent w.r.t. (R, δ) over K. □

Remark: An easy consequence of Witt's cancellation theorem is that the congruence of the matrices $A \oplus A \oplus A \oplus -A$ and $B \oplus B \oplus B \oplus -B$ implies that also $A \oplus A$ and $B \oplus B$ are congruent. It is possible to prove a quantitative version of Witt's cancellation theorem, and therefore one can obtain a quantitative result on the congruence of $A \oplus A$ and $B \oplus B$. However, if we now would apply this quantitative version of the cancellation theorem, in chapter 11 this finally would yield an $(n+1)$-fold exponential bound for H_k instead of an n-fold one. Therefore we avoid an application of the cancellation theorem, although this causes some inconveniences but finally we obtain a better bound for H_k.

Theorem 8.15: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta\colon \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let $A, B \in \mathrm{GL}(n, K)$, $z_1, \ldots, z_r \in R$, $\alpha, \gamma \in \Gamma_{\geq 0}$, $\delta(z_1), \ldots, \delta(z_r) \leq \gamma$. Suppose that for each r-tuple $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_r) \in \{1, -1\}^r$ the matrices A and B are α-congruent over the field $K(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_r z_r})$. Then $2^{r-1}(2^r + 1) \times A \oplus 2^{r-1}(2^r - 1) \times (-A)$ and $2^{r-1}(2^r + 1) \times B \oplus 2^{r-1}(2^r - 1) \times (-B)$ are $4^r(\alpha + 2\gamma)$-congruent over K.*

Proof: We argue by induction on r. The case $r = 0$ is obvious. Now let $r > 0$. Proposition 8.14 applied to each of the fields $K(\sqrt{\varepsilon_1 z_1}, \ldots, \sqrt{\varepsilon_{r-1} z_{r-1}})$ implies that $3 \times A \oplus (-A)$ and $3 \times B \oplus (-B)$ are $(\frac{7}{2}\gamma + 4\alpha)$-congruent over all these fields. Then, by the induction hypothesis $2^{r-2}(2^{r-1} + 1) \times (3 \times A \oplus (-A)) \oplus 2^{r-2}(2^{r-1} - 1) \times (3 \times (-A) \oplus A)$ and $2^{r-2}(2^{r-1} + 1) \times (3 \times B \oplus (-B)) \oplus 2^{r-2}(2^{r-1} - 1) \times (3 \times (-B) \oplus B)$ are $4^{r-1}(\frac{7}{2}\gamma + 4\alpha + 2\gamma)$-congruent over K. Now some elementary arithmetic yields the induction step. □

Proposition 8.16: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta\colon \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let $A, B \in \mathrm{GL}(n, K)$, $x, y \in R$ and $\alpha, \beta \in \Gamma_{\geq 0}$ such that $\delta(x), \delta(y) \leq \beta$. If A and B are α-congruent over $K(\sqrt{x^2 + y^2})$ w.r.t. (R, δ), then $A \oplus A$ and $B \oplus B$ are $2(\alpha + \beta)$-congruent over K w.r.t. (R, δ).*

Proof: The proof is similar to that one of Lemma 8.12. If $K(\sqrt{x^2 + y^2}) = K$ the assertion follows from Lemma 8.9. Now assume that $K(\sqrt{x^2 + y^2}) \neq K$. By the assumption there are a matrix $U \in M_n^{\times}(K(\sqrt{x^2 + y^2}), R)$ and $u \in K(\sqrt{x^2 + y^2})^{\times} \cap \bar{R}$ such that $M_\delta(U), \delta(u) \leq \alpha$ and

$$U^T A U = u^2 B$$

We express u in the form $u = a + b\sqrt{x^2 + y^2}$ for certain $a, b \in K$ and let $u' := a - b\sqrt{x^2 + y^2}$. Then u and u' are conjugate over K and hence also u' is integral over R and $\delta(u') = \delta(u) \leq \alpha$. Now define

$$c := 2uu' = 2(a^2 - (x^2 + y^2)b^2) \in K^{\times}$$

Since u, u' are integral over R so is c, and hence $c \in R$ as R is integrally closed in K. Furthermore $\delta(c) \leq \delta(u) + \delta(u') \leq 2\alpha$.

Let $u_{ij} \in K(\sqrt{x^2 + y^2}) \cap \bar{R}$ be the entries of the matrix U and define $w_{ij} := u' u_{ij}$. These elements are integral over R. If we let $W := (w_{ij})$ then

$$4W^T A W = c^2 B$$

Each w_{ij} we express in the form $w_{ij} = a_{ij} + b_{ij}\sqrt{x^2 + y^2}$ for certain $a_{ij}, b_{ij} \in K$ and we define $w'_{ij} := a_{ij} - b_{ij}\sqrt{x^2 + y^2}$. Then w_{ij} and w'_{ij} are conjugate over K and hence also the elements w'_{ij} are integral over R and $\delta(w'_{ij}) = \delta(w_{ij}) \leq \delta(u') + \delta(u_{ij}) \leq 2\alpha$.

Furthermore $2a_{ij} = w_{ij} + w'_{ij}$ and $2b_{ij}\sqrt{x^2 + y^2} = w_{ij} - w'_{ij}$ are also integral over R and $\delta(2a_{ij}), \delta(2b_{ij}\sqrt{x^2 + y^2}) \leq 2\alpha$. Since $x, y \in R$ and R is integrally closed in K we obtain that $2a_{ij}, 2b_{ij}(x^2 + y^2) \in R$. Now let $P := (2a_{ij})$ and $Q := (2b_{ij})$. Then $P + \sqrt{x^2 + y^2}Q = 2W$ and thus

$$\begin{aligned} c^2 B = 4W^T A W &= (P^T + \sqrt{x^2 + y^2}Q^T)A(P + \sqrt{x^2 + y^2}Q) \\ &= P^T A P + (x^2 + y^2)Q^T A Q + \sqrt{x^2 + y^2}(P^T A Q + Q^T A P) \end{aligned}$$

Since $\sqrt{x^2+y^2} \notin K$ we obtain

$$\begin{aligned} P^T AP + (x^2+y^2) Q^T AQ &= c^2 B \\ P^T AQ + Q^T AP &= 0 \end{aligned}$$

If we now let

$$V := \begin{pmatrix} P + xQ & yQ \\ yQ & P - xQ \end{pmatrix} \in M_{2n}(K)$$

then

$$\begin{aligned} V^T(A \oplus A)V &= \begin{pmatrix} P^T + xQ^T & yQ^T \\ yQ^T & P^T - xQ^T \end{pmatrix} \cdot \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \cdot \begin{pmatrix} P + xQ & yQ \\ yQ & P - xQ \end{pmatrix} \\ &= \begin{pmatrix} c^2 B & 0 \\ 0 & c^2 B \end{pmatrix} = c^2(B \oplus B) \end{aligned}$$

Finally let $S := (x^2+y^2)V$. Then $S \in M_{2n}(R)$ and $M_\delta(S) \leq 2\alpha + 2\beta$ and

$$S^T(A \oplus A)S = (x^2+y^2)^2 c^2 (B \oplus B)$$

As B is regular so is $B \oplus B$ and hence also S is regular. The same argument, applied to the situation with A and B interchanged, finally yields the assertion. $\square$

Theorem 8.17: *Suppose that R is a domain which is integrally closed in $K :=$ Quot(R) and let $\delta\colon \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that* char$(K) \neq$ *2. Let L be a subfield of $\bar{K}$ which contains K and let $\alpha \in \Gamma_{\geq 0}$. Let further $z \in L^\times$ be integral over R and assume that $A, B \in GL(n, L)$ are α-congruent w.r.t. (R, δ) over every semi-extension F of $L(\sqrt{z})$ which contains K. Then $6 \times A \oplus 2 \times (-A)$ and $6 \times B \oplus 2 \times (-B)$ are $(8\alpha + 9\delta(z))$-congruent w.r.t. (R, δ) over every semi-extension E of L which contains K.*

Proof: Let E be a semi-extension of L which contains K. By Theorem 6.6 there are $a, b \in E \cap \bar{R}$ and $u \in E(\sqrt{a^2+b^2}) \cap \bar{R}$ such that $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$ are both semi-extensions of $L(\sqrt{z})$ and $\delta(a), \delta(b), \delta(u) \leq \delta(z)$. By assumption A, B are α-congruent w.r.t. (R, δ) over both fields $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$. Now let S be the integral closure of R in $E(\sqrt{a^2+b^2})$. By Corollary 3.4 , δ is also S-stable, and by Lemma 8.4 the matrices A and B are also α-congruent w.r.t. (S, δ) over the fields $E(\sqrt{a^2+b^2}, \sqrt{u})$ and $E(\sqrt{a^2+b^2}, \sqrt{-u})$. So we may apply Proposition 8.14 to obtain that $3 \times A \oplus -A$ and $3 \times B \oplus -B$ are $(\frac{7}{2}\delta(z) + 4\alpha)$-congruent w.r.t. (S, δ), and therefore w.r.t. (R, δ), over $E(\sqrt{a^2+b^2})$.

Now let S' be the integral closure of R in E. Then δ is also S'-stable and Proposition 8.16 yields that $2 \times (3 \times A \oplus -A)$ and $2 \times (3 \times B \oplus -B)$ are $(9\delta(z) + 8\alpha)$-congruent w.r.t. (S', δ), and hence w.r.t. (R, δ), over E. Now Lemma 8.6 yields the result. $\square$

Before we state and prove the main result of this chapter we want to remind the reader that a 2-extension of fields is a Galois extension with a 2-group as its Galois group.

Theorem 8.18: *Suppose that R is a domain which is integrally closed in $K := \mathrm{Quot}(R)$ and let $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ be an R-stable degree function on $\bar{K}$. Assume that $\mathrm{char}(K) \neq 2$. Let L/K be a finite 2-extension of degree n with primitive element ϑ and assume that ϑ is integral over R. Suppose that $\alpha \in \Gamma_{\geq 0}$. Let furthermore $A, B \in \mathrm{GL}(m, K)$ and assume that A and B are α-congruent w.r.t. (R, δ) over each semi-extension of L which contains K. Then $\frac{1}{2}n^2(n+1) \times A \oplus \frac{1}{2}n^2(n-1) \times (-A)$ and $\frac{1}{2}n^2(n+1) \times B \oplus \frac{1}{2}n^2(n-1) \times (-B)$ are $n^3(\alpha + 3\delta(\vartheta))$-congruent w.r.t. (R, δ) over K.*

Proof: Let $G := \mathrm{Gal}(L/K)$. Then $\#G = [L : K] = n = 2^r$ for some $r \in \mathbb{N}$. Since G is a 2-group of order 2^r there is an ascending chain of subgroups

$$\{\mathrm{id}\} = G_0 \subsetneqq G_1 \subsetneqq \ldots \subsetneqq G_r = G$$

such that $[G_{i+1} : G_i] = 2$ $(0 \leq i \leq r-1)$. Let F_i be the fixed field of G_i and denote the integral closure of R in F_i by R_i. By finite Galois theory

$$K = F_r \subsetneqq F_{r-1} \subsetneqq \ldots F_1 \subsetneqq F_0 = L$$

and $[F_i : F_{i+1}] = 2$ $(0 \leq i \leq r-1)$. Now let

$$\begin{aligned} \alpha_i &:= 8^i\alpha + 3 \cdot 2^i(4^i - 1)\delta(\vartheta) \\ s_i &:= \tfrac{1}{2}4^i(2^i + 1) \\ t_i &:= \tfrac{1}{2}4^i(2^i - 1) \end{aligned}$$

and define

$$\begin{aligned} A_i &:= s_i \times A \oplus t_i \times (-A) \\ B_i &:= s_i \times B \oplus t_i \times (-B) \end{aligned}$$

An easy computation shows $6s_i + 2t_i = s_{i+1}$ and $6t_i + 2s_i = t_{i+1}$ for $0 \leq i \leq r-1$, and thus Lemma 8.6 yields

$$\begin{aligned} A_{i+1} &\equiv_0 6 \times A_i \oplus 2 \times (-A_i) \\ B_{i+1} &\equiv_0 6 \times B_i \oplus 2 \times (-B_i) \end{aligned}$$

w.r.t. (R, δ) over K.

Now we show by induction on $i = 0, \ldots, r$ that A_i and B_i are α_i-congruent w.r.t. (R_i, δ) over every semi-extension of F_i which contains K. The case $i = 0$ follows from our assumptions.

Let $i > 0$. Since δ is also R_{i+1}-stable by Corollary 3.4 we may apply Corollary 3.7 to the situation $F_{i+1} \subset F_i \subset L = K(\vartheta) = F_{i+1}(\vartheta)$ to obtain an element $z \in R_{i+1}$ such that $F_i = F_{i+1}(\sqrt{z})$ and

$$\delta(z) \leq [L : F_{i+1}] \cdot \delta(\vartheta) = 2^{i+1} \cdot \delta(\vartheta)$$

By the induction hypothesis A_i and B_i are α_i-congruent w.r.t. (R_i, δ), and hence also w.r.t. (R_{i+1}, δ), over every semi-extension of F_i which contains K. Then Theorem 8.17 implies that $6 \times A_i \oplus 2 \times (-A_i)$ and $6 \times B_i \oplus 2 \times (-B_i)$ are $(8\alpha_i + 9\delta(z))$-congruent w.r.t. (R_{i+1}, δ) over every semi-extension of F_{i+1} which contains K. Thus, by Lemma 8.5 , A_{i+1} and B_{i+1} are $(8\alpha_i + 9\delta(z))$-congruent w.r.t. (R_{i+1}, δ) over every semi-extension of F_{i+1} which contains K, and the estimate

$$8\alpha_i + 9\delta(z) \leq 8\alpha_i + 9 \cdot 2^{i+1}\delta(\vartheta) = \alpha_{i+1}$$

yields the induction step. Now the case $i = r$ implies the assertion. $\square$

Chapter 9

Some remarks on hyperbolicity

If K is a field which is not formally real, then, by a theorem of Pfister (cf. [33], Satz 6), every quadratic form is weakly hyperbolic over K, i.e., for every quadratic form f there are $n, m \in \mathbb{N}$ such that

$$n \times f \cong_K m \times < 1, -1 >$$

This isometry can be expressed in terms of congruence of matrices. In this chapter we are concerned with the size of this congruence w.r.t. a degree function on the field K.

Lemma 9.1: *Let R be a domain and suppose that $\delta : R \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on R. Let further $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$, $\alpha \in \Gamma$ and assume that $\delta(a_i), \delta(b_i) \leq \alpha$ $(1 \leq i \leq n)$. Then there are $a, b \in R$ such that $\delta(a), \delta(b) \leq n\alpha$ and*

$$\prod_{i=1}^{n} (a_i^2 + b_i^2) = a^2 + b^2$$

Proof: With the use of the well-known identity

$$(X_1^2 + Y_1^2) \cdot (X_2^2 + Y_2^2) = (X_1 X_2 + Y_1 Y_2)^2 + (X_1 Y_2 - X_2 Y_1)^2$$

the assertion follows by an easy induction on the number n. $\square$

Identities like that one used in the proof above also exist in the case of a product of sums of 4 and 8 squares. Thus, similar results hold in that case but we do not need them in our approach, and they also cannot be generalized to a product of arbitrary sums of squares because Hurwitz (cf. [21], Chap. 7.6) proved that an identity of the form

$$\sum_{i=1}^{n} X_i^2 \cdot \sum_{i=1}^{n} Y_i^2 = \sum_{i=1}^{n} Z_i^2$$

where $Z_1, \ldots, Z_n$ are bilinear forms in $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ only exists if $n \in \{1, 2, 4, 8\}$. However, as was shown by Pfister (cf. [32], Satz 2), a product of two sums of n squares in a field K is again a sum of n squares in K, provided that the number n is a power of 2. We need a quantitative version of this result. The next lemma is a quantitative version of Satz 1 from [34].

Lemma 9.2: *Let R be a domain an let $\delta : R \longrightarrow \Gamma \cup \{-\infty\}$ be a degree function on R. Suppose that $a_1, \ldots, a_{2^n} \in R$, $\alpha \in \Gamma_{\geq 0}$, $\delta(a_i) \leq \alpha$ and let $a := \sum_{i=1}^{2^n} a_i^2$. Then there is a matrix $S \in M_{2^n}(R)$ and an element $b \in R \backslash \{0\}$ such that*

(a) $S^T S = b^2 a \cdot E_{2^n}$

(b) $M_\delta(S) \leq 3^n \alpha$

(c) $\delta(b) \leq (3^n - 1)\alpha$

Proof: We prove the lemma by induction on n. In the case $n = 0$ we choose $S = (a_1)$ and $b = 1$. Now assume $n > 0$. Let $a := \sum_{i=1}^{2^{n+1}} a_i^2$, $v := \sum_{i=1}^{2^n} a_i^2$ and $w := \sum_{i=2^n+1}^{2^{n+1}} a_i^2$. If $v = 0$ or $w = 0$ then a is already a sum of 2^n squares and we may apply the induction hypothesis to obtain $P \in M_{2^n}(R)$ and $b \in R \backslash \{0\}$ such that $P^T P = b^2 a \cdot E_{2^n}$ and $M_\delta(P) \leq 3^n \alpha$, $\delta(b) \leq (3^n - 1)\alpha$. Define $S := P \oplus P$. Then $S^T S = b^2 a \cdot E_{2^{n+1}}$ and we are done.

Now assume that $v, w \neq 0$. Then $\delta(v), \delta(w) \leq 2\alpha$. By the induction hypothesis there are $P, Q \in M_{2^n}(R)$ and $c, d \in R \backslash \{0\}$ such that $M_\delta(P), M_\delta(Q) \leq 3^n \alpha$, $\delta(c), \delta(d) \leq (3^n - 1)\alpha$ and

$$P^T P = c^2 v \cdot E_{2^n} \tag{1}$$

$$Q^T Q = d^2 w \cdot E_{2^n} \tag{2}$$

As $d, w \neq 0$ equation (2) yields that Q is invertible and $Q^T = d^2 w \cdot Q^{-1}$. Thus also

$$QQ^T = d^2 w \cdot E_{2^n} \tag{3}$$

Now let

$$S := \begin{pmatrix} vc^2 Q & vcdP \\ -vcdP & PQ^T P \end{pmatrix}$$

Then

$$\begin{aligned} M_\delta(vc^2 Q) &\leq \delta(v) + 2\delta(c) + M_\delta(Q) \leq 2\alpha + 2(3^n - 1)\alpha + 3^n \alpha = 3^{n+1}\alpha \\ M_\delta(vcdP) &\leq \delta(v) + \delta(c) + \delta(d) + M_\delta(P) \leq 2\alpha + (3^n - 1)\alpha + (3^n - 1)\alpha + 3^n \alpha = 3^{n+1}\alpha \\ M_\delta(PQ^T P) &\leq 2M_\delta(P) + M_\delta(Q) \leq 3^{n+1}\alpha \end{aligned}$$

and thus also $M_\delta(S) \leq 3^{n+1}\alpha$. Using (1),(2),(3) and the fact $a = v + w$ we obtain by an elementary computation

$$S^T S = (c^2 dv)^2 a \cdot E_{2^{n+1}}$$

Let finally $b := c^2 dv$. Then $b \neq 0$ and

$$\delta(b) \leq 2\delta(c) + \delta(d) + \delta(v) \leq 3(3^n - 1)\alpha + 2\alpha = (3^{n+1} - 1)\alpha$$

This yields the induction step and the lemma is proved. $\square$

This lemma has some important consequences. The first one is a quantitative version of Pfister's result mentioned above.

Corollary 9.3: *Let R be an integral domain and assume that $\delta : R \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on R. Let further $a_1, \ldots, a_{2^n}, b_1, \ldots, b_{2^n} \in R, \alpha \in \Gamma_{\geq 0}$, $\delta(a_i), \delta(b_i) \leq \alpha$. Then there are $c, c_1, \ldots, c_{2^n} \in R, c \neq 0$ such that $\delta(c) \leq (3^n - 1)\alpha$, $\delta(c_i) \leq (3^n + 1)\alpha$ and*

$$\sum_{i=1}^{2^n} c_i^2 = c^2 \cdot \sum_{i=1}^{2^n} a_i^2 \cdot \sum_{i=1}^{2^n} b_i^2$$

Proof: Let $a := \sum_{i=1}^{2^n} a_i^2$ and $b := \sum_{i=1}^{2^n} b_i^2$. By Lemma 9.2 there are $S \in M_{2^n}(R)$ and $c \in R \backslash \{0\}$ such that $M_\delta(S) \leq 3^n\alpha$, $\delta(c) \leq (3^n - 1)\alpha$ and $S^T S = c^2 a \cdot E_{2^n}$. Now define

$$v := \begin{pmatrix} b_1 \\ \vdots \\ b_{2^n} \end{pmatrix}$$

and let $w := Sv$. Denote the coordinates of w by $c_1, \ldots, c_{2^n}$. Then $c_1, \ldots, c_{2^n} \in R$ and $\delta(c_i) \leq M_\delta(S) + M_\delta(v) \leq (3^n + 1)\alpha$. Furthermore

$$\sum_{i=1}^{2^n} c_i^2 = w^T w = (Sv)^T (Sv) = v^T S^T S v = c^2 a v^T v = c^2 ab$$

and the corollary is proved. $\square$

Corollary 9.4: *Let R be a domain with $K := \mathrm{Quot}(R)$ and assume that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $a_1, \ldots, a_{2^n} \in R, \alpha \in \Gamma_{\geq 0}$ and suppose that $a := \sum_{i=1}^{2^n} a_i^2 \neq 0$ and $\delta(a_i) \leq \alpha$. Then:*

$$aE_{2^n} \equiv_{(3^n+1)\alpha} E_{2^n}$$

w.r.t. (R, δ) over K.

Proof: By Lemma 9.2 there are $S \in M_{2^n}(R)$ and $b \in R \backslash \{0\}$ such that $M_\delta(S) \leq 3^n\alpha$, $\delta(b) \leq (3^n - 1)\alpha$ and $S^T S = b^2 a E_{2^n}$. Thus $S^T a E_{2^n} S = (ab)^2 \cdot E_{2^n}$. Now the estimate $\delta(ab) \leq (3^n - 1)\alpha + 2\alpha = (3^n + 1)\alpha$ yields the assertion. $\square$

Theorem 9.5: *Let R be a domain with K as its field of quotients and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on K. Let $\alpha, \gamma \in \Gamma_{\geq 0}$, $r, n \in \mathbb{N}$ such that $r \leq 2^n + 1$ and assume that $r \times < 1 >$ is γ-isotropic over K. Let further $a_1, \ldots, a_m \in R \backslash \{0\}$ such that $\delta(a_i) \leq \alpha$. Then*

$$2^{n+1} \times \mathrm{diag}(a_1, \ldots, a_m) \equiv_{m((3^n+2)\gamma+\alpha)} (2^n m) \times \mathrm{diag}(1, -1)$$

Proof: By assumption there are $z_1, \ldots, z_r \in K \cap \bar{R}$ such that $\delta(z_i) \leq \gamma$ and $\sum_{i=1}^r z_i^2 = 0$ and $z_r \neq 0$. Thus $-z_r = \sum_{i=1}^{r-1} z_i^2$ and hence Corollary 9.4 yields that

$$-z_r^2 E_{2^n} \equiv_{(3^n+1)\gamma} E_{2^n}$$

w.r.t. $(K \cap \bar{R}, \delta)$ and hence also w.r.t. (R, δ).
Thus $z_r^2 E_{2^n} \equiv_{(3^n+1)\gamma} -E_{2^n}$ by Lemma 8.7. Immediately by definition we get $z_r^2 E_{2^n} \equiv_\gamma E_{2^n}$, and hence Lemma 8.5 yields

$$E_{2^n} \equiv_{(3^n+2)\gamma} -E_{2^n}$$

By a further application of Lemma 8.7 we get $a_i E_{2^n} \equiv_{(3^n+2)\gamma} -a_i E_{2^n}$ for all $i = 1, \ldots, m$ and hence

$$a_i E_{2^{n+1}} \equiv_{(3^n+2)\gamma} a_i E_{2^n} \oplus -a_i E_{2^n}$$

Since $a_i E_{2^n} \oplus -a_i E_{2^n} \equiv_\alpha E_{2^n} \oplus -E_{2^n}$ by Lemma 8.13 we obtain from Lemma 8.5 and Lemma 8.6

$$a_i E_{2^{n+1}} \equiv_{(3^n+2)\gamma+\alpha} 2^n \times \mathrm{diag}(1, -1)$$

A further application of Lemma 8.8 finally yields the result. $\square$

Chapter 10

Some remarks on Hankel matrices

An $n \times n$-matrix $A = (a_{ij})$ over a field K is called a Hankel matrix if there are elements $a_0, \ldots, a_{2n-2} \in K$ such that $a_{ij} = a_{i+j-2}$. In this chapter we are concerned with the quantitative diagonalization of Hankel matrices over fields with a degree function. We follow an approach of Wörmann (cf. [42]).

Throughout this chapter we assume that R is an integral domain which is integrally closed in $K := \mathrm{Quot}(R)$. Further we suppose that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is an R-stable degree function on the algebraic closure $\bar{K}$ of K and that $\mathrm{char}(K) \neq 2$.
We start with two technical lemmas:

Lemma 10.1: *Suppose $a_1, \ldots, a_n \in R, a_1 \neq 0$ and let A be the lower right triangular matrix*

$$A := \begin{pmatrix} & & & a_1 \\ & & \iddots & a_2 \\ & \iddots & \iddots & \vdots \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

Then there is a diagonal matrix $D \in M_n^{\times}(K, R)$ such that

(a) $M_\delta(D) \leq M_\delta(A)$

(b) *A and D are $\frac{1}{2}n \cdot M_\delta(A)$-congruent w.r.t (R, δ) over K*

Proof: We distinguish two cases. First we assume that n is even, say $n = 2m$. Then A is of the form

$$A = \begin{pmatrix} 0 & B \\ B & C \end{pmatrix}$$

with $B, C \in M_m(R)$ symmetric. Let $d := \det B$. Then $d = (-1)^{\frac{1}{2}m(m-1)} a_1^m \neq 0$. Define $D := E_m \oplus -E_m$ and

$$P := \begin{pmatrix} \widetilde{B}\cdot(4E_m - C) & \widetilde{B}\cdot(4E_m + C) \\ 2dE_m & -2dE_m \end{pmatrix} \in M_{2m}(R)$$

Since B is symmetric, so is $\widetilde{B}$. Thus

$$\begin{aligned} P^T AP &= \begin{pmatrix} (4E_m - C)\cdot\widetilde{B} & 2dE_m \\ (4E_m + C)\cdot\widetilde{B} & -2dE_m \end{pmatrix} \cdot \begin{pmatrix} 0 & B \\ B & C \end{pmatrix} \cdot \begin{pmatrix} \widetilde{B}\cdot(4E_m - C) & \widetilde{B}\cdot(4E_m + C) \\ 2dE_m & -2dE_m \end{pmatrix} \\ &= \begin{pmatrix} 16d^2 E_m & 0 \\ 0 & -16d^2 E_m \end{pmatrix} = (4d)^2 \cdot D \end{aligned}$$

Now define

$$Q := \begin{pmatrix} 2B & C + E_m \\ 2B & C - E_m \end{pmatrix}$$

Then

$$\begin{aligned} Q^T DQ &= \begin{pmatrix} 2B & 2B \\ C + E_m & C - E_m \end{pmatrix} \cdot \begin{pmatrix} E_m & 0 \\ 0 & -E_m \end{pmatrix} \cdot \begin{pmatrix} 2B & C + E_m \\ 2B & C - E_m \end{pmatrix} \\ &= \begin{pmatrix} 0 & 4B \\ 4B & 4C \end{pmatrix} = 4A \end{aligned}$$

The estimate $M_\delta(Q) \leq M_\delta(A)$ is obvious and by Lemma 2.5 and Lemma 2.6 we obtain $M_\delta(P) \leq m \cdot M_\delta(A)$ and $\delta(4d) \leq \delta(d) \leq m \cdot M_\delta(A)$. This proves the lemma in the case that n is even.

Now assume that n is odd and let $n = 2m + 1$. In the case $n = 1$ there is nothing to show. Thus, we may assume that $n \geq 3$ and hence $m \geq 1$. In this case A is of the form

$$A = \begin{pmatrix} 0 & 0 & B \\ 0 & a_1 & v \\ B & v^T & C \end{pmatrix}$$

for certain symmetric $B, C \in M_m(R)$ and some row vector $v \in R^m$. We let $d := \det B$. Then again $d \neq 0$. We define $D := E_m \oplus (a_1) \oplus -E_m$ and

$$P := \begin{pmatrix} \widetilde{B}\cdot(4E_m - C) & -4\widetilde{B}v^T & \widetilde{B}\cdot(4E_m + C) \\ 0 & 4d & 0 \\ 2dE_m & 0 & -2dE_m \end{pmatrix}$$

Then, by an elementary computation

$$P^T AP = (4d)^2 \cdot D$$

Let finally

$$Q := \begin{pmatrix} 2a_1 B & 0 & U + a_1 E_m \\ 0 & 2a_1 & 2v \\ 2a_1 B & 0 & U - a_1 E_m \end{pmatrix}$$

with $U := a_1C - v^Tv \in M_m(R)$. Since U is symmetric we obtain

$$\begin{aligned} Q^TDQ &= \begin{pmatrix} 2a_1B & 0 & 2a_1B \\ 0 & 2a_1 & 0 \\ U+a_1E_m & 2v^T & U-a_1E_m \end{pmatrix} \cdot \begin{pmatrix} E_m & 0 & 0 \\ 0 & a_1 & 0 \\ 0 & 0 & -E_m \end{pmatrix} \cdot \begin{pmatrix} 2a_1B & 0 & U+a_1E_m \\ 0 & 2a_1 & 2v \\ 2a_1B & 0 & U-a_1E_m \end{pmatrix} \\ &= (2a_1)^2 \begin{pmatrix} 0 & 0 & B \\ 0 & a_1 & v \\ B & v^T & C \end{pmatrix} = (2a_1)^2 \cdot A \end{aligned}$$

Again Lemma 2.5 and Lemma 2.6 yield $M_\delta(P) \le m \cdot M_\delta(A)$ and $\delta(4d) \le \delta(d) \le m \cdot M_\delta(A)$. Furthermore $M_\delta(Q) \le 2 \cdot M_\delta(A) \le m \cdot M_\delta(A)$, provided that $m \ge 2$, i.e., $n \ge 5$. However, the case $n = 3$ is settled by the equality

$$\begin{pmatrix} 2a_1 & 0 & 2a_1 \\ 2a_2 & 2 & 2a_2 \\ a_3+1 & 0 & a_3-1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2a_1 & 2a_2 & a_3+1 \\ 0 & 2 & 0 \\ 2a_1 & 2a_2 & a_3-1 \end{pmatrix} = 4 \cdot \begin{pmatrix} 0 & 0 & a_1 \\ 0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \end{pmatrix}$$

and we are done. □

Lemma 10.2: *Suppose that $a_0, \ldots, a_{2n-2} \in R$, $a_0 \neq 0$, $n \ge 2$ and let*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{n-1} \\ a_1 & a_2 & & \iddots & a_n \\ \vdots & & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & & \vdots \\ a_{n-1} & a_n & \cdots & \cdots & a_{2n-2} \end{pmatrix}$$

Assume that $\det A \neq 0$. *Then there are $r \in \{1, \ldots, n-1\}$ and Hankel matrices $B \in M_r(R)$ and $C \in M_{n-r}(R)$ such that*

(a) *A and $B \oplus C$ are $r(n-r)M_\delta(A)$-congruent w.r.t. (R, δ) over K*

(b) *C is a lower right triangular matrix*

(c) *$M_\delta(B) \le M_\delta(A)$*

(d) *$M_\delta(C) \le (2r+1)M_\delta(A)$*

Proof: For $1 \le k \le n$ we let

$$A_k := (a_{i+j-2})_{1 \le i,j \le k} \in M_k(R)$$

and by d_k we denote the determinant of A_k. Then $d_1, \ldots, d_n$ are the principal minors of A and $d_1 = a_0 \neq 0$. Let

$$r := \max\{\ i \mid 1 \le i \le n-1,\ d_i \neq 0\ \}$$

and define $B := A_r$. Then B is regular since $\det B = d_r \neq 0$ and hence $\mathrm{rk}(B) = r$. Obviously, B is a Hankel matrix and $M_\delta(B) \leq M_\delta(A)$. We apply Proposition 2.8 to obtain $z, z_1, \ldots, z_r \in R$, $z \neq 0$ such that $(z_1 z^{-1}, \ldots, z_r z^{-1})$ is a solution of

$$Bx = \begin{pmatrix} a_r \\ \vdots \\ a_{2r-1} \end{pmatrix}$$

and $\delta(z), \delta(z_i) \leq r \cdot M_\delta(A)$. Further, we let $z_{r+1} = -z$ and $z_i = 0$ for $i \leq 0$ and $i \geq r+2$, and we define

$$\begin{aligned}
u_i &:= -\sum_{j=0}^{r} a_{i+j} z_{j+1} && 0 \leq i \leq 2n-r-2 \\
c_i &:= -\sum_{j=0}^{r} u_{i+j} z_{j+1} && 0 \leq i \leq 2n-2r-2 \\
y_{ij} &:= \sum_{\nu=1}^{n} a_{i+\nu-2} z_{r+1+\nu-j} && 1 \leq i \leq n, \quad r+1 \leq j \leq n
\end{aligned}$$

Then $\delta(u_i) \leq (r+1)M_\delta(A)$ and $\delta(c_i) \leq (2r+1)M_\delta(A)$. A reenumeration of the indices yields

$$y_{ij} = \sum_{\mu=r+2-j}^{r+1+n-j} a_{i+j+\mu-r-3} z_\mu = \sum_{\mu=1}^{r+1} a_{i+j+\mu-r-3} z_\mu$$

To obtain the last equality one has to take into account that $r+1 \leq j \leq n$ and $z_\mu = 0$ if $\mu \leq 0$ or $\mu \geq r+2$. Thus

$$y_{ij} = -u_{i+j-r-2}$$

Let us further define

$$w_{ij} := \begin{cases} \delta_{ij} & \text{if } 1 \leq i \leq n \quad 1 \leq j \leq r \\ -z_{r+1+i-j} & \text{if } 1 \leq i \leq n \quad r+1 \leq j \leq n \end{cases}$$

where δ_{ij} is the usual Kronecker symbol. Then $W := (w_{ij})_{ij} \in M_n(R)$ is an upper right triangular matrix with entries $1, \ldots, 1, z, \ldots, z$ in the diagonal. Hence W is regular and $\det W = z^{n-r}$. Let $V := W^T A W$. Then also V is regular with entries from R. Denote its entries by v_{ij} and let furthermore $V_k := (v_{ij})_{1 \leq i,j \leq k}$ and $W_k := (w_{ij})_{1 \leq i,j \leq k}$ $(1 \leq k \leq n)$. As W is an upper triangular matrix and easy argument yields $V_k = W_k^T A_k W_k$ and hence

$$\det V_k = (\det W_k)^2 \cdot d_k$$

Now we compute the entries v_{ij}. Since $V = W^T A W$ we get

$$v_{ij} = \sum_{\nu=1}^{n} \sum_{\mu=1}^{n} a_{\nu+\mu-2} w_{\nu i} w_{\mu j}$$

We distinguish three cases:

Case 1: $1 \le i, j \le r$

$$v_{ij} = \sum_{\nu=1}^{n} \sum_{\mu=1}^{n} a_{\nu+\mu-2} \delta_{\nu i} \delta_{\mu j} = a_{i+j-2}$$

Case 2: $1 \le i \le r, \quad r+1 \le j \le n$

$$\begin{aligned} v_{ij} &= -\sum_{\nu=1}^{n} \sum_{\mu=1}^{n} a_{\nu+\mu-2} \delta_{\nu i} z_{r+1+\mu-j} = -\sum_{\mu=1}^{n} a_{i+\mu-2} z_{r+1+\mu-j} \\ &= -y_{ij} = u_{i+j-r-2} \end{aligned}$$

Case 3: $r+1 \le i, j \le n$

$$\begin{aligned} v_{ij} &= \sum_{\nu=1}^{n} \sum_{\mu=1}^{n} a_{\nu+\mu-2} z_{r+1+\nu-i} z_{r+1+\mu-j} = \sum_{\nu=1}^{n} \left(\sum_{\mu=1}^{n} a_{\nu+\mu-2} z_{r+1+\mu-j} \right) z_{r+1+\nu-i} \\ &= \sum_{\nu=1}^{n} y_{\nu j} z_{r+1+\nu-i} = -\sum_{\nu=1}^{n} u_{\nu+j-r-2} z_{r+1+\nu-i} = -\sum_{k=r+2-i}^{r+1+n-i} u_{i+j+k-2r-3} z_k \\ &= -\sum_{k=1}^{r+1} u_{i+j+k-2r-3} z_k = -\sum_{k=0}^{r} u_{i+j+k-2r-2} z_{k+1} = c_{i+j-2r-2} \end{aligned}$$

Since V is symmetric, this yields that V is of the form

$$V = \begin{pmatrix} B & U \\ U^T & C \end{pmatrix}$$

where U is the $r \times (n-r)$-matrix

$$U := \begin{pmatrix} u_0 & u_1 & \dots & u_{n-r-1} \\ \vdots & & & \vdots \\ u_{r-1} & u_r & \dots & u_{n-2} \end{pmatrix}$$

and C is the Hankel matrix

$$C := \begin{pmatrix} c_0 & \dots & c_{n-r-1} \\ \vdots & \iddots & \vdots \\ c_{n-r-1} & \dots & c_{2(n-r)-2} \end{pmatrix}$$

of size $(n-r) \times (n-r)$. Now we show that $U = 0$ and that C is a lower right triangular matrix. First, by the choice of $z_1, \dots, z_r$ we get

$$B \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = z \begin{pmatrix} a_r \\ \vdots \\ a_{2r-1} \end{pmatrix}$$

and thus $\sum_{j=1}^{r} a_{i+j-2}z_j = z \cdot a_{r+i-1}$. Comparing this equation with the definition of u_{i-1} we get $u_0, \ldots, u_{r-1} = 0$. Therefore, in the case $r = n-1$ we are done. Now assume that $r < n-1$. We prove by induction on $i = 0, \ldots, n-r-2$ that $u_{r+i} = 0$ and $c_i = 0$.

$i = 0:$ Since $u_0, \ldots, u_{r-1} = 0$ we get $V_{r+1} = B \oplus (c_0)$ and therefore

$$c_0 d_r = \det V_{r+1} = (\det W_{r+1})^2 \cdot d_{r+1} = 0$$

since $d_{r+1} = 0$ by the definition of r. As $d_r \neq 0$ we obtain $c_0 = 0$. Thus, by the definition of c_0

$$0 = c_0 = -\sum_{j=0}^{r} u_j z_{j+1} = u_r z - \sum_{j=0}^{r-1} u_j z_{j+1} = u_r z$$

The last equality follows again from the fact $u_0, \ldots, u_{r-1} = 0$. Since $z \neq 0$ we get $u_r = 0$.

$i \Rightarrow i+1:$ If $i+1 \leq n-r-2$ then $r+i+2 < n$. By the induction hypothesis $u_0, \ldots, u_{r+i} = 0$ and $c_0, \ldots, c_i = 0$ we get

$$V_{r+i+2} = \begin{pmatrix} & & & 0 & \ldots & 0 \\ & B & & \vdots & & \vdots \\ & & & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & c_{i+1} \\ \vdots & & \vdots & \vdots & \iddots & \\ 0 & \ldots & 0 & c_{i+1} & & * \end{pmatrix}$$

Thus

$$(-1)^{\frac{1}{2}(i+2)(i+1)} c_{i+1}^{i+2} \cdot d_r = \det V_{r+i+2} = (\det W_{r+i+2})^2 \cdot d_{r+i+2} = 0$$

Hence $c_{i+1} = 0$, because $d_r \neq 0$. Finally, by the definition of c_{i+1} and the induction hypothesis we obtain

$$0 = c_{i+1} = -\sum_{j=0}^{r} u_{i+1+j} z_{j+1} = u_{r+i+1} z - \sum_{j=0}^{r-1} u_{i+1+j} z_{j+1} = u_{r+i+1} z$$

and $z \neq 0$ implies $u_{r+i+1} = 0$. This yields the induction step.

Thus $W^T A W = V = B \oplus C$. The definition of W yields $M_\delta(W) \leq r M_\delta(A)$. Now note that the only entries in the first r columns of W are 0 and 1 and therefore Lemma 2.5(b) implies $M_\delta(\widetilde{W}) \leq (n-r) r M_\delta(A)$. Since $\det W = z^{n-r}$ we get $\widetilde{W}^T V \widetilde{W} = z^{2(n-r)} A$ and thus A and $B \oplus C$ are $r(n-r)M_\delta(A)$-congruent w.r.t. (R, δ) over K. $\square$

As a consequence we obtain the following theorem on the quantitative diagonalization of Hankel matrices over fields with a degree function.

Theorem 10.3: *Suppose that* $a_0, \ldots, a_{2n-2} \in R$, $a_0 \neq 0$ *and let*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{n-1} \\ a_1 & a_2 & & \cdot^{\cdot^{\cdot}} & a_n \\ \vdots & & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \vdots \\ \vdots & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & & \vdots \\ a_{n-1} & a_n & \cdots & \cdots & a_{2n-2} \end{pmatrix}$$

Assume that $\det A \neq 0$. *Then there is a diagonal matrix* $D \in M_n^\times(K, R)$ *such that*

(a) *A and D are $2n^2 M_\delta(A)$-congruent w.r.t. (R, δ) over K.*

(b) $M_\delta(D) \leq (2n-1) M_\delta(A)$

Proof: We prove the theorem by induction on n. The case $n = 1$ is obvious. Now suppose $n > 1$. By Lemma 10.2 there are a natural number $r \in \{1, \ldots, n-1\}$ and Hankel matrices $B \in M_r(R)$ and $C \in M_{n-r}(R)$ such that C is a lower right triangular matrix, $M_\delta(B) \leq M_\delta(A)$, $M_\delta(C) \leq (2r+1) M_\delta(A)$ and A and $B \oplus C$ are $r(n-r)M_\delta(A)$-congruent w.r.t. (R, δ) over K.

By the induction hypothesis there is a diagonal matrix $D_1 \in M_r(R)$ such that B and D_1 are $2r^2 M_\delta(B)$-congruent w.r.t. (R, δ) over K and $M_\delta(D_1) \leq (2r-1)M_\delta(B) \leq (2n-1)M_\delta(A)$. By Lemma 10.1 there is a diagonal matrix D_2 such that C and D_2 are $\frac{1}{2}(n-r)M_\delta(C)$-congruent w.r.t. (R, δ) over K and $M_\delta(D_2) \leq M_\delta(C) \leq (2r+1)M_\delta(A) \leq (2n-1)M_\delta(A)$. An easy computation yields

$$r(n-r)M_\delta(A) + 2r^2 M_\delta(B) + \tfrac{1}{2}(n-r)M_\delta(C) \leq 2n^2 \cdot M_\delta(A)$$

and hence A and $D = D_1 \oplus D_2$ are $2n^2 M_\delta(A)$-congruent w.r.t. (R, δ) over K by Lemma 8.5 and Lemma 8.8. This yields the induction step and the theorem is proved. □

To each separable polynomial we now assign a Hankel matrix.

Definition: *Let $f \in K[X] \setminus K$ of degree $\deg f = d$ and assume that $z_1, \ldots, z_d \in \bar{K}$ are the zeroes of f and suppose that all of them are simple. Then we call the $d \times d$ matrix*

$$\mathrm{H}_f = (t_{i+j-2}(f))_{1 \leq i,j \leq d}$$

with $t_k(f) := \sum_{i=1}^d z_i^k$ the Hankel matrix of f.

Remark:

1) Sometimes H_f is also called the Sylvester matrix of f

2) As one can easily see, the matrix H_f defined above is a Hankel matrix.

3) If $f \in K[X]$ is a polynomial of degree d, then the residue class ring $A := K[X]/(f)$ is a finite dimensional vector space over K, and the map

$$s : A \times A \longrightarrow K$$
$$(x, y) \mapsto \mathrm{tr}_{A/K}(x \cdot y)$$

is a symmetric bilinear form. It is well-known that H_f is the representation matrix for s w.r.t. the basis $1, X, \ldots, X^{d-1}$ (cf. [22], Chap. I, §8).

The following result is well-known.

Proposition 10.4: *Let $f \in K[X] \setminus K$ without multiple zeroes and suppose that* $\deg f = d$. *Then* $\mathrm{H}_f \in M_d(K)$

Proof: Since f has only simple zeroes its splitting field F is a finite Galois extension of K. Obviously all the elements $t_k(f)$ are fixed under $\mathrm{Gal}(F/K)$ and thus $t_k(f) \in K$. □

Proposition 10.5: *Assume that $f \in R[X] \setminus R$ is monic of degree d without multiple zeroes. Then there is a diagonal matrix $D \in M_d(R)$ such that*

(a) $\mathrm{H}_f \equiv_{4d^3 \bar{M}_\delta(f)} D$

(b) $M_\delta(D) \leq 4d^2 \bar{M}_\delta(f)$

Proof: Let $z_1, \ldots, z_d \in \bar{K}$ be the zeroes of f. As f is monic $z_1, \ldots, z_d \in \bar{R}$. Thus $t_k(f) \in K \cap \bar{R} = R$ and hence H_f has entries from R. By Theorem 2.14 we get $\delta(z_i) \leq \bar{M}_\delta(f)$ and thus $\delta(t_k(f)) \leq k\bar{M}_\delta(f)$. Consequently $M_\delta(\mathrm{H}_f) \leq (2d-2)\bar{M}_\delta(f) \leq 2d\bar{M}_\delta(f)$. By Theorem 10.3 there is a diagonal matrix $D \in M_d^\times(K, R)$ such that $M_\delta(D) \leq (2d-1)M_\delta(\mathrm{H}_f) \leq 4d^2\bar{M}_\delta(f)$ and $\mathrm{H}_f \equiv_{2d^2 M_\delta(\mathrm{H}_f)} D$. This proves the proposition. □

Theorem 10.6: *Suppose that $f \in R[X]$ is monic of degree d without multiple zeroes, and let L be a semi-splitting field of f over K of type (n, m). Then H_f and $(n+m) \times (1) \oplus m \times (-1)$ are $\frac{1}{2}d(d-1)\bar{M}_\delta(f)$-congruent over L.*

Proof: In $L[X]$ the polynomial f splits in the form

$$f(X) = \prod_{j=1}^{n}(X - z_j) \cdot \prod_{j=1}^{m}((X - x_j)^2 + {y_j}^2)$$

Let $v_j := x_j + iy_j,\ w_j := x_j - iy_j\ (1 \leq j \leq m)$. Then $z_1, \ldots, z_n, v_1, \ldots, v_m, w_1, \ldots, w_{2m}$ are exactly the zeroes of f and hence these elements are integral over R. For $1 \leq j \leq m$ and $1 \leq k \leq d$ we define

$$\begin{aligned} a_{jk} &:= v_j^{k-1} + w_j^{k-1} \\ b_{jk} &:= i(v_j^{k-1} - w_j^{k-1}) \end{aligned}$$

An easy computation shows

$$a_{\nu j}a_{\nu k} - b_{\nu j}b_{\nu k} = 2 \cdot \left(v_\nu^{j+k-2} + w_\nu^{j+k-2}\right) \tag{1}$$

Now we define the matrix $P := (c_{\nu\mu})_{\nu\mu}$ by

$$c_{\nu\mu} := \begin{cases} 2z_\nu^{\mu-1} & \text{if} \quad 1 \leq \nu \leq n \\ a_{\nu-n\ \mu} & \text{if} \quad n+1 \leq \nu \leq n+m \\ b_{\nu-n-m\ \mu} & \text{if} \quad n+m+1 \leq \nu \leq n+2m = d \end{cases}$$

i.e.

$$P = \begin{pmatrix} 2 & 2z_1 & 2z_1^2 & \dots & 2z_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 2 & 2z_n & 2z_n^2 & \dots & 2z_n^{d-1} \\ a_{11} & a_{12} & a_{13} & \dots & a_{1d} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{md} \\ b_{11} & b_{12} & b_{13} & \dots & b_{1d} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & b_{m3} & \dots & b_{md} \end{pmatrix}$$

An easy Galois theoretic argument shows $P \in M_d(L)$. Now let

$$U := n \times (1) \oplus m \times (2) \oplus m \times (-2)$$

Lemma 8.13 and Lemma 8.8 yield

$$U \equiv_0 (n+m) \times (1) \oplus m \times (-1) \tag{2}$$

Using equation (1) an elementary computation shows

$$P^T U P = 4 \cdot \mathrm{H}_f \tag{3}$$

In order to show that P is regular we compute $\det P$ by use of some linear algebra. Since $a_{jk} - ib_{jk} = 2v_j^{k-1}$ we get

$$\det P = \det \begin{pmatrix} 2 & 2z_1 & 2z_1^2 & \dots & 2z_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 2 & 2z_n & 2z_n^2 & \dots & 2z_n^{d-1} \\ 2 & 2v_1 & 2v_1^2 & \dots & 2v_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 2 & 2v_m & 2v_m^2 & \dots & 2v_m^{d-1} \\ b_{11} & b_{12} & b_{13} & \dots & b_{1d} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & b_{m3} & \dots & b_{md} \end{pmatrix}$$

and $b_{jk} - i \cdot v_j^{k-1} = -i \cdot w_j^{k-1}$ implies

$$\det P = \det \begin{pmatrix} 2 & 2z_1 & 2z_1^2 & \dots & 2z_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 2 & 2z_n & 2z_n^2 & \dots & 2z_n^{d-1} \\ 2 & 2v_1 & 2v_1^2 & \dots & 2v_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 2 & 2v_m & 2v_m^2 & \dots & 2v_m^{d-1} \\ -i & -iw_1 & -iw_1^2 & \dots & -iw_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ -i & -iw_m & -iw_m^2 & \dots & -iw_m^{d-1} \end{pmatrix}$$

Altogether this yields

$$\det P = 2^{n+m}(-i)^m \det V$$

where V is the Vandermonde matrix

$$V = \begin{pmatrix} 1 & z_1 & \dots & z_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & w_m & \dots & w_m^{d-1} \end{pmatrix}$$

Since we assumed that f has only simple zeroes, the matrix V is regular. Thus also P is regular.
By Theorem 2.14 we get $\delta(z_j), \delta(v_j), \delta(w_j) \leq \bar{M}_\delta(f)$. If we denote the column vectors of P by $x_1, \dots, x_d$ this yields $M_\delta(x_i) \leq (i-1)\bar{M}_\delta(f)$ and thus

$$\delta(\det P), M_\delta(\widetilde{P}) \leq \tfrac{1}{2}d(d-1) \cdot \bar{M}_\delta(f)$$

by Lemma 2.5(b). From (3) we get

$$(2\widetilde{P})^T \mathrm{H}_f (2\widetilde{P}) = (\det P)^2 \cdot U$$

and thus H_f and U are $\frac{1}{2}d(d-1)\bar{M}_\delta(f)$-congruent. Now (2) and Lemma 8.5 yield the result. $\square$

Chapter 11

Bounds for H_k and N_k

In this final chapter we prove a recursion formula for H_k. As a consequence we obtain a bound for H_k and together with the results from the first chapter this finally yields a bound for N_k.

In order to obtain the recursion formula for H_k we proceed in two steps. We start with a polynomial $f \in k[X_1, \ldots, X_n]$ and consider it as a univariate polynomial over $k(X_1, \ldots, X_{n-1})$. Furthermore we choose a $k[X_1, \ldots, X_{n-1}]$-stable degree function

$$\delta : \overline{k(X_1, \ldots, X_{n-1})} \longrightarrow \mathbb{Q} \cup \{-\infty\}$$

according to Corollary 3.2, i.e., $\delta(g) = \deg g$ for all $g \in k[X_1, \ldots, X_{n-1}]$. Then, roughly speaking we proceed as follows:

In the first step we show that from a congruence

$$\ell \times \mathrm{H}_f \oplus m \times -H_f \equiv_\alpha r \times \mathrm{diag}(1, -1)$$

one can obtain a representation of f as a sum of squares in $k(X_1, \ldots, X_n)$ in an effective way, i.e., we get bounds for the degrees of the numerators and denominators in terms of ℓ, m, r and α.

In the second step we show how to obtain such a congruence as above from the fact that f is positive semidefinite over k.

Lemma 11.1: *Let R be an integral domain and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on $K := \mathrm{Quot}(R)$. Let further $\ell, n, m \in \mathbb{N}, \ell > m$, $\alpha \in \Gamma_{\geq 0}$ and assume that $\ell \times (1) \oplus\ m \times (-1) \equiv_\alpha n \times \mathrm{diag}(1,-1)$ over K. Then $(2n+1) \times < 1 >$ is $2n\alpha$-isotropic.*

Proof: Let $A := \ell \times (1) \oplus\ m \times (-1)$ and $B := n \times \mathrm{diag}(1,-1)$ and let $e_1, \ldots, e_{2n}$ be the canonical unit vectors in K^{2n}. The assumption $A \equiv_\alpha B$ implies $\ell + m = 2n$. As $\ell > m$ this yields $\ell \geq n+1$. Hence

$$\begin{aligned} e_i^T A e_j &= \delta_{ij} && 1 \leq i, j \leq n+1 \\ e_i^T B e_j &= -\delta_{ij} && n+1 \leq i, j \leq 2n \end{aligned}$$

Since $A \equiv_\alpha B$ there are $P \in M_{2n}^\times(K, R)$ and $a \in K^\times \cap \bar{R}$ such that $M_\delta(P), \delta(a) \leq \alpha$ and $P^T A P = a^2 B$.

The $2n+1$ vectors $ae_1, \ldots, ae_{n+1}$, $Pe_{n+1}, \ldots, Pe_{2n} \in K^{2n}$ are linearly dependent over K and thus, by Proposition 2.7, there is a non trivial linear combination

$$\sum_{i=1}^{n+1} a_i a e_i + \sum_{i=n+1}^{2n} b_i P e_i = 0$$

for certain $a_1, \ldots, a_{n+1}, b_{n+1}, \ldots, b_{2n} \in K \cap \bar{R}$ such that $\delta(a_i), \delta(b_i) \leq 2n\alpha$. Then

$$v := a \cdot \sum_{i=1}^{n+1} a_i e_i = - \sum_{i=n+1}^{2n} b_i P e_i$$

Thus

$$v^T A v = a^2 \cdot \left(\sum_{i=1}^{n+1} a_i e_i^T \right) A \left(\sum_{j=1}^{n+1} a_j e_j \right) = a^2 \cdot \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} a_i a_j e_i^T A e_j = a^2 \cdot \sum_{i=1}^{n+1} a_i^2$$

and also

$$\begin{aligned} v^T A v &= \left(\sum_{i=n+1}^{2n} b_i e_i^T P^T \right) A \left(\sum_{j=n+1}^{2n} b_j P e_j \right) = \sum_{i=n+1}^{2n} \sum_{j=n+1}^{2n} b_i b_j e_i^T (P^T A P) e_j \\ &= a^2 \cdot \sum_{i=n+1}^{2n} \sum_{j=n+1}^{2n} b_i b_j e_i^T B e_j = -a^2 \cdot \sum_{i=n+1}^{2n} b_i^2 \end{aligned}$$

This yields

$$\sum_{i=1}^{n+1} a_i^2 + \sum_{i=n+1}^{2n} b_i^2 = 0$$

and thus $(2n+1) \times < 1 >$ is $2n\alpha$-isotropic over K. $\square$

Lemma 11.2: *Let R be an integral domain which is integrally closed in $K := \mathrm{Quot}(R)$ and suppose that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is an R-stable degree function. Let furthermore $f \in R[X]\backslash\{0\}$ be monic of degree d, $\alpha \in \Gamma_{\geq 0}$ and assume that $\ell, m, n \in \mathbb{N}$, $\ell > m$ such that*

$$\ell \times \mathrm{H}_f \oplus m \times (-\mathrm{H}_f) \equiv_\alpha n \times \mathrm{diag}(1, -1)$$

over K. Then $(2n+1)\times < 1 >$ is $2n(\alpha + d(d-1)\bar{M}_\delta(f))$-isotropic over each semi-splitting field E of f which contains a zero of f.

Proof: Let (r, s) be the type of E. Then $r \neq 0$ because E contains a zero of f. Theorem 10.6 yields that H_f and $(r+s)\times(1) \oplus s\times(-1)$ are $\frac{1}{2}d(d-1)\bar{M}_\delta(f)$-congruent w.r.t. (R, δ) over E. Hence, by Lemma 8.9 and Lemma 8.7

$$\ell \times \mathrm{H}_f \equiv_{\frac{1}{2}d(d-1)\bar{M}_\delta(f)} (\ell r + \ell s) \times (1) \oplus \ell s \times (-1)$$
$$m \times (-\mathrm{H}_f) \equiv_{\frac{1}{2}d(d-1)\bar{M}_\delta(f)} (mr + ms) \times (-1) \oplus ms \times (1)$$

Now Lemma 8.6 and Lemma 8.8 yield

$$\ell \times \mathrm{H}_f \oplus m \times (-\mathrm{H}_f) \equiv_{d(d-1)\bar{M}_\delta(f)} (\ell r + \ell s + ms) \times (1) \oplus \ (mr + ms + \ell s) \times (-1)$$

By Lemma 8.5 and the assumption $\ell \times \mathrm{H}_f \oplus m \times (-\mathrm{H}_f) \equiv_\alpha n \times \mathrm{diag}(1, -1)$ we obtain

$$(\ell r + \ell s + ms) \times (1) \oplus \ (mr + ms + \ell s) \times (-1) \equiv_{\alpha + d(d-1)\bar{M}_\delta(f)} n \times \mathrm{diag}(1, -1)$$

As $\ell > m$ and $r \neq 0$ we get $\ell r + \ell s + ms > mr + ms + \ell s$. Now Lemma 11.1 yields the result. $\square$

Lemma 11.3: *Let R be an integral domain and suppose that $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on $K := \mathrm{Quot}(R)$. Let furthermore $\gamma \in \Gamma_{\geq 0}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$, $\delta(a_i), \delta(b_i) \leq \gamma$ $(1 \leq i \leq n)$ and let $f(X) := \prod_{i=1}^n ((X - a_i)^2 + b_i^2)$. Then there are monic polynomials $g, h \in R[X]$ such that*

(a) $2 \cdot f = g^2 + h^2$

(b) $\deg g = \deg h = n$

(c) $\bar{M}_\delta(g), \bar{M}_\delta(h) \leq \gamma$

Proof: Using the well-known identity $(a^2 + b^2) \cdot (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$ it is easy to see that there are polynomials $G, H \in \mathbb{Z}[X, Y_1, \ldots, Y_n, Z_1, \ldots, Z_n]$, homogeneous of degree n such that G is monic in X, $\deg_X G = n$, $\deg_X H < n$ and

$$\prod_{i=1}^n ((X - Y_i)^2 + Z_i^2) = G^2 + H^2$$

Now define

$$g(X) := G(X, a_1, \ldots, a_n, b_1, \ldots, b_n) + H(X, a_1, \ldots, a_n, b_1, \ldots, b_n)$$
$$h(X) := G(X, a_1, \ldots, a_n, b_1, \ldots, b_n) - H(X, a_1, \ldots, a_n, b_1, \ldots, b_n)$$

Then $g, h \in R[X]$ are both monic of degree n and $g^2 + h^2 = 2 \cdot f$. Now it remains to prove assertion (c).

The polynomials $G+H, G-H \in \mathbb{Z}[X, Y_1, \ldots, Y_n, Z_1, \ldots, Z_n]$ are both monic in X and of total degree n. We express $G+H$ in the form $G+H = \sum_{i=0}^n p_i X^i$ for certain $p_0, \ldots, p_n \in \mathbb{Z}[Y_1, \ldots, Y_n, Z_1, \ldots, Z_n]$, $p_n = 1$. Then $\deg p_i \leq n - i$. Furthermore $g(X) = \sum_{i=0}^n c_i X^i$ with $c_i = p_i(a_1, \ldots, a_n, b_1, \ldots, b_n)$. Since p_i has integer coefficients we obtain $\bar{M}_\delta(p_i) \leq 0$ and thus $\delta(c_i) \leq (n-i)\gamma$ by Lemma 2.17. As $c_n = 1$ this yields $\bar{M}_\delta(g) \leq \gamma$. In the same way one proves $\bar{M}_\delta(h) \leq \gamma$. □

Corollary 11.4: *Let R be an integral domain with K as its field of fractions and suppose that $2 \in R^\times$. Let further $f \in R[X] \setminus \{0\}$ be monic of degree $d = 2m$ and let E be a semi-splitting field of f over K of type $(0, m)$. Denote the integral closure of R in E by S and assume that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on $\bar{K}$ such that $\delta(\frac{1}{2}) = 0$. Then there are monic polynomials $g, h \in S[X]$ such that:*

(a) $2 \cdot f = g^2 + h^2$

(b) $\deg g = \deg h = m$

(c) $\bar{M}_\delta(g), \bar{M}_\delta(h) \leq \bar{M}_\delta(f)$

Proof: In $E[X]$ the polynomial f splits in the form

$$f(X) = \prod_{j=1}^{m} ((X - a_j)^2 + b_j^2)$$

for certain $a_1, \ldots, a_m, b_1, \ldots, b_m \in E$. The zeroes of f are $a_j \pm i b_j$ $(1 \leq j \leq m)$. Thus $a_j \pm i b_j$ are integral over R and therefore $a_1, \ldots, a_m, b_1, \ldots, b_m \in S$ since $2 \in R^\times$. Moreover $\delta(a_j \pm i b_j) \leq \bar{M}_\delta(f)$ by Theorem 2.14. Thus

$$\delta(a_j) \leq \delta(2a_j) + \delta(\tfrac{1}{2}) = \delta(2a_j) \leq \max(\delta(a_j + ib_j), \delta(a_j - ib_j)) \leq \bar{M}_\delta(f)$$

Similarly we get $\delta(ib_j) \leq \bar{M}_\delta(f)$ and thus $\delta(b_j) \leq \delta(ib_j) + \delta(-i) = \delta(ib_j) \leq \bar{M}_\delta(f)$ since $\delta(-i) = 0$ by Lemma 2.2(b). Now Lemma 11.3 applied to S yields the result. □

Theorem 11.5: *Let R be an integral domain which is integrally closed in $K := \mathrm{Quot}(R)$ and assume that $\mathrm{char}(K) = 0$ and $2 \in R^\times$. Suppose that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is an R-stable degree function on $\bar{K}$ with $\delta(\frac{1}{2}) = 0$ and let $\delta' : \overline{K(X)} \longrightarrow \Gamma \cup \{-\infty\}$ be an $R[X]$-stable extension of δ to $\overline{K(X)}$. Let furthermore $f \in R[X] \setminus \{0\}$ be monic of degree $d \geq 2$ without multiple zeroes and assume that $\ell, m, n \in \mathbb{N}$, $\alpha \in \Gamma_{\geq 0}$ such that $\ell > m$, $\bar{M}_\delta(f), \delta'(X) \leq \alpha$ and*

$$\ell \times \mathrm{H}_f \oplus m \times (-\mathrm{H}_f) \equiv_\alpha n \times \mathrm{diag}(1, -1)$$

w.r.t. (R, δ) over K. Then there is a natural number t such that

(a) $t \times < 1, -f >$ *is $(2^{2^{d^2}} \cdot n \cdot \alpha)$-isotropic w.r.t. $(R[X], \delta')$ over $K(X)$*

(b) $t \leq (24n + 12)^{2^{d^2}}$

Proof: Let E be an arbitrary semi-splitting field of f over K. We first claim that the form $(2n+1)\times < 1, -f >$ is $2n(d^2-d+1)\alpha$-isotropic w.r.t. $(R[X], \delta')$ over $E(X)$. We distinguish two cases.

Case 1: f has a zero in E

By Lemma 11.2 the form $(2n+1)\times < 1 >$ is $2n(\alpha + d(d-1)\bar{M}_\delta(f))$-isotropic w.r.t. (R, δ) over E and thus also w.r.t. $(R[X], \delta')$ over $E(X)$. Since $\alpha + d(d-1)\bar{M}_\delta(f) \leq (d^2-d+1)\alpha$ the claim is proved in this case.

Case 2: f has no zero in E

In this case E is a semi-splitting field of f of type $(0, \frac{1}{2}d)$. We let S be the integral closure of R in E. Then, by Corollary 11.4 there are monic polynomials $g, h \in S[X]$ of degree $\frac{1}{2}d$ such that $2f = g^2 + h^2$ and $\bar{M}_\delta(g), \bar{M}_\delta(h) \leq \bar{M}_\delta(f)$. Lemma 2.20 then yields $\delta'(g), \delta'(h) \leq \frac{1}{2}d\alpha$. Since $S[X]$ is an integral extension of $R[X]$ this yields that $2\times < 1, -f >$ is $\frac{1}{2}d\alpha$-isotropic w.r.t. $(R[X], \delta')$ over $E(X)$. Obviously $\frac{1}{2}d\alpha \leq 2n(d^2-d+1)\alpha$. This proves the claim in the second case.

Now let $F \subset \bar{K}$ be the splitting field of f over K and denote the zeroes of f by $\vartheta_1, \ldots, \vartheta_d$. As f is monic, $\vartheta_1, \ldots, \vartheta_d$ are integral over R and $\delta(\vartheta_i) \leq \bar{M}_\delta(f) \leq \alpha$ by Theorem 2.14. Since $\mathrm{char}(K) = 0$ there is a $\mathbb{Z}$-linear combination ϑ of $\vartheta_1, \ldots, \vartheta_d$ such that ϑ is a primitive element for the extension F/K. Then also ϑ is integral over R and $\delta(\vartheta) \leq \alpha$. Furthermore $F(X)/K(X)$ is a finite Galois extension, and ϑ is also a primitive element for $F(X)/K(X)$.

Next we want to show that the form $(2n+1)\times < 1, -f >$ is $2n(d^2-d+1)\alpha$-isotropic w.r.t. $(R[X], \delta')$ over each semi-extension of $F(X)$ which contains $K(X)$. Let F' be such a semi-extension of $F(X)$. Then F' is also a semi-extension of F and by Proposition 6.5 the relative algebraic closure E' of K in F' is also a semi-extension of F. Therefore $F \subset E'(i)$ and thus f splits into linear factors in $E'(i)[X]$. Hence E' contains a semi-splitting field E of f by Corollary 6.4.

As we have seen above the form $(2n+1)\times < 1, -f >$ is $2n(d^2-d+1)\alpha$-isotropic w.r.t. $(R[X], \delta')$ over $E(X)$ and hence also over F', because $E(X) \subset F'$.

As $R[X]$ is integrally closed in $K[X]$ (cf. [7], Chap. V, §1, Prop.13) and $K[X]$ is integrally closed in $K(X)$ also $R[X]$ is integrally closed in $K(X)$. Since $\delta'(f) \leq d\alpha$ by Lemma 2.20 and $\delta(\vartheta) \leq \alpha$ we obtain from Theorem 7.9 that $6^{s-1} \cdot (2n+1)^s \times < 1, -f >^s$ is $2^s s!(4n(d^2-d+1)\alpha + d\alpha + 2s^2\alpha)$-isotropic w.r.t. $(R[X], \delta')$ over $K(X)$ with

$$(1) \qquad s := [F(X) : K(X)] = [F : K] \leq d! \leq d^d \leq 2^{d^2}$$

Proposition 8.11 yields

$$\mathrm{diag}(1, -f)^{\otimes s} \equiv_{(s-1)d\alpha} 2^s \times \mathrm{diag}(1, -f)$$

and therefore

$$6^{s-1} \cdot (2n+1)^s \times \mathrm{diag}(1, -f)^{\otimes s} \equiv_{(s-1)d\alpha} 6^{s-1} \cdot (2n+1)^s \cdot 2^s \times \mathrm{diag}(1, -f)$$

by Lemma 8.9. Now Proposition 8.10 implies that $6^{s-1} \cdot (2n+1)^s \cdot 2^s \times < 1, -f >$ is $((s-1)d\alpha + (2^s s!(4n(d^2-d+1)+d+2s^2)\alpha))$-isotropic over $K(X)$.
As $d \geq 2$ we obtain

$$\begin{aligned}(s-1)d + 2^s s!(4n(d^2-d+1)+d+2s^2) &\leq 2^s s! \cdot (4n(d^2-d+1)+2d+2s^2)\\ &\leq 2^s s! \cdot (4nd^2+2s^2)\\ &\leq 8nd^2s^2 \cdot 2^s s!\end{aligned}$$

We claim that

$$8d^2s^2 \cdot 2^s s! \leq 2^{2^{d^2}} \tag{2}$$

If $d=2$ we get $s \leq 2$ and a direct computation shows that the estimate above holds. Now let $d \geq 3$. From (1) follows $\log_2 s \leq d \cdot \log_2 d \leq d^2$ and hence

$$\log_2(s!) \leq \log_2(s^s) = s \cdot \log_2 s \leq sd^2$$

Therefore

$$\log_2(8d^2s^2 \cdot 2^s s!) \leq 3 + 2 \cdot \log_2 d + 2 \cdot \log_2 s + s + sd^2 \leq 5sd^2 \leq 5d^2 \cdot d!$$

Now by an easy induction one can show that $5d^2 \cdot d! \leq 2^{d^2}$ for $d \geq 3$. This proves (2).
Therefore $t \times < 1, -f >$ is $(2^{2^{d^2}} \cdot n \cdot \alpha)$-isotropic w.r.t. $(R[X], \delta')$ over $K(X)$ with $t := 6^{s-1} \cdot (2n+1)^s \cdot 2^s \leq (24n+12)^{2^{d^2}}$. This proves the theorem. $\square$

The next lemma is of combinatorial nature. Before we state it we introduce a notation. If A is a subset of a field K we denote by $A - A$ the set

$$A - A := \{a - b \mid a, b \in A\}$$

Lemma 11.6: *Let $A \neq \emptyset$ be a finite subset of the field K and suppose that $B \subset A - A$ has the property that for all $a, b \in A$, $a \neq b$ we have $a - b \in B$ or $b - a \in B$. Assume that the field $K(\sqrt{x} \mid x \in B)$ is not formally real. Then there is a set $C \subset B$ such that*

(a) *$K(\sqrt{x} \mid x \in C)$ is not formally real*

(b) *$\#C \leq \#A$*

Proof: We define a binary relation on A by

$$a \leq b \;:\Longleftrightarrow\; b - a \in B \cup \{0\}$$

Obviously $\leq$ is reflexive. We distinguish three cases.

Case 1: $\leq$ is not antisymmetric

Then there are $a, b \in A$ such that $a \leq b$, $b \leq a$ but $a \neq b$. Hence $b - a, a - b \in B \backslash \{0\}$ and we may choose $C := \{a - b, b - a\}$. Note that in this case $\#A \geq 2$ as $a \neq b$.

Case 2: $\leq$ *is not transitive*

In this case there are $a, b, c \in A$ such that $a \leq b$, $b \leq c$ but $a \not\leq c$. It is easy to see that these three conditions together with the reflexivity of $\leq$ yield that a, b, c are pairwise distinct. Thus $\#A \geq 3$. Moreover, we get $b - a, c - b \in B$ but $c - a \notin B \cup \{0\}$ and thus the assumption on B yields $a - c \in B$. Now let $C := \{b - a, c - b, a - c\}$. Then $C \subset B$, $\#C \leq \#A$ and it is easy to see that $K\left(\sqrt{x} \mid x \in C\right)$ is not formally real.

Case 3: $\leq$ *is antisymmetric and transitive*

As $\leq$ is also reflexive it is a partial order on A, and by the assumption on B it is even a total order. Let $A = \{a_1, \ldots, a_n\}$ and assume w.l.o.g. that $a_1 \leq \ldots \leq a_n$. Furthermore, let

$$C' := \{a_2 - a_1, a_3 - a_2, \ldots, a_n - a_{n-1}\}$$

Then $C' \subset B$ and $\#C' \leq n - 1 < \#A$. If $L := K\left(\sqrt{x} \mid x \in C'\right)$ is not formally real we are done. Otherwise L admits an ordering P. Since $K\left(\sqrt{x} \mid x \in B\right)$ is not formally real there is some $x \in B$ such that $x \notin P$ (cf. [36], Theorem 1.26). Since $B \subset A - A$ there are i, j such that $x = a_i - a_j$.

The assumption $i \geq j$ would yield that $x = a_i - a_j$ is a sum of squares in L and thus $x \in P$. Therefore $i < j$.

Now let $C := C' \cup \{a_i - a_j\}$. Then $C \subset B$ and $\#C \leq n = \#A$ and

$$\sqrt{a_i - a_j}^{\,2} + \sum_{k=i}^{j-1} \sqrt{a_{k+1} - a_k}^{\,2} = 0$$

is a non-trivial representation of 0 as a sum of squares in $K\left(\sqrt{x} \mid x \in C\right)$. Hence this field is not formally real. $\square$

In order to state the next result properly we need a technical definition. The second condition in the following definition is only of technical nature. It will avoid an inconvenient case distinction in the next result.

Definition: *Let R be an integral domain with K as its field of quotients and suppose that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on $\bar{K}$. By $\mathcal{H}(K, R, \delta)$ we denote the set of all pairs (h_1, h_2) of functions $h_1 : \mathbb{N}_{\geq 2} \times \Gamma_{\geq 0} \longrightarrow \mathbb{N}$, $h_2 : \mathbb{N}_{\geq 2} \times \Gamma_{\geq 0} \longrightarrow \Gamma_{\geq 0}$ which satisfy*

(i) *For each $\vartheta \in \bar{R}$ with $K(\vartheta)$ not formally real, $[K(\vartheta) : K] \leq d$ and $\delta(\vartheta) \leq \gamma$ the form $h_1(d, \gamma) \times < 1 >$ is $h_2(d, \gamma)$-isotropic w.r.t. (R, δ) over $K(\vartheta)$*

(ii) $h_2(d, \gamma) \geq [\log_2 d] \cdot \gamma$ *for all $d \in \mathbb{N}_{\geq 2}, \gamma \in \Gamma_{\geq 0}$*

Remark: Note that if (h_1, h_2) is such a pair of functions as in the above definition, then $h_1(d, \gamma) \geq 2$ for all $d \in \mathbb{N}_{\geq 2}$, $\gamma \in \Gamma_{\geq 0}$, because the 1-dimensional form $< 1 >$ is not isotropic over any field.

We recall that if $\delta : K \longrightarrow \Gamma \cup \{-\infty\}$ is a degree function on the field K an element $a \in K^\times$ is called a δ-unit if $\delta(a) = \delta(a^{-1}) = 0$.

The next theorem is a quantitative version of a result of Pfister which states that a quadratic form q over a formally real field K is weakly hyperbolic iff $\mathrm{sign}_P q = 0$ for every ordering P of K.

Theorem 11.7: *Let R be an integral domain which is integrally closed in $K = \mathrm{Quot}(R)$ and assume that K is formally real and $2 \in R^\times$. Suppose that $\delta : \bar{K} \longrightarrow \Gamma \cup \{-\infty\}$ is an R-stable degree function on $\bar{K}$ with $\delta(\frac{1}{2}) = 0$ and let $\delta' : \overline{K(X)} \longrightarrow \Gamma \cup \{-\infty\}$ be an $R[X]$-stable extension of δ to $\overline{K(X)}$. Assume that $(h_1, h_2) \in \mathcal{H}(K, R, \delta)$. Let $f_1, \ldots, f_{2m} \in R[X] \backslash \{0\}$ of degrees $\deg f_i \leq d$, $d \geq 2$ and assume that their leading coefficients are units in R and δ-units. Let $\gamma \in \Gamma_{\geq 0}$ and suppose that $\delta'(X) \leq \gamma$ and also $\bar{M}_\delta(f_i) \leq \gamma$ $(1 \leq i \leq 2m)$. Suppose that $\mathrm{sign}_P(< f_1, \ldots, f_{2m} >) = 0$ for every ordering P of $K(X)$. Then there are $k, \ell, n \in \mathbb{N}$, $\alpha \in \Gamma_{\geq 0}$ such that*

(a) $k \times \mathrm{diag}(f_1, \ldots, f_{2m}) \oplus \ell \times \mathrm{diag}(-f_1, \ldots, -f_{2m}) \equiv_\alpha n \times \mathrm{diag}(1, -1)$ *w.r.t. $(R[X], \delta')$ over $E(X)$ for every semi-splitting field E of $\prod_{i=1}^{2m} f_i$ over K.*

(b) $k > \ell$ *and* $n \leq 2^{6m^2d^2+2} \cdot m \cdot h_1((2^{d+1}d!)^{2m}, \gamma)$

(c) $\alpha \leq 5m \cdot 2^{6m^2d^2} \cdot h_1((2^{d+1}d!)^{2m}, \gamma)^2 \cdot h_2((2^{d+1}d!)^{2m}, \gamma)$

Proof: Denote the degrees of $f_1, \ldots, f_{2m}$ by $d_1, \ldots, d_{2m}$ and let $a_1, \ldots, a_{2m}$ be the leading coefficients of these polynomials. Let furthermore $a := \prod_{i=1}^{2m} a_i$ and $f := \prod_{i=1}^{2m} f_i$. Fix (r, s) and let E be a semi-splitting field of f of type (r, s). Then f splits in the form

$$f = a \cdot \prod_{j=1}^{r} (X - x_j) \cdot \prod_{j=1}^{s} ((X - y_j)^2 + {z_j}^2)$$

for certain $x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s \in E$ such that

$$E = K(x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s)$$

and

$$r \leq \deg f = \sum_{i=1}^{2m} d_i \leq 2md \tag{1}$$

The elements $x_1, \ldots, x_r, y_1 \pm iz_1, \ldots, y_s \pm iz_s \in \bar{K}$ are the zeroes of f and since $f = \prod_{i=1}^{2m} f_i$ all of them are zeroes of some f_i. Thus $x_1, \ldots, x_r, y_1 \pm iz_1, \ldots, y_s \pm iz_s$ are integral over R since $a_1, \ldots, a_{2m} \in R^\times$. As $2 \in R^\times$ also $y_1, \ldots, y_s$ and $z_1, \ldots, z_s$ are integral over R. Since $a_1, \ldots, a_{2m}$ are δ-units we obtain from Theorem 2.14 that $\delta(x_j), \delta(y_j \pm iz_j) \leq \gamma$, and $\delta(\frac{1}{2}) = 0$ finally implies $\delta(y_j), \delta(z_j) \leq \gamma$.

In $E[X]$ the polynomials $f_1, \ldots, f_{2m}$ split in the form

$$f_i = a_i \cdot \prod_{j \in I_i} (X - x_j) \cdot \prod_{j \in J_i} ((X - y_j)^2 + z_j^2) \qquad (1 \leq i \leq 2m)$$

for certain $I_i \subset \{1, \ldots, r\}$, $J_i \subset \{1, \ldots, s\}$. Let $k_i := \#I_i$ and $\ell_i := \#J_i$ and define

$$E_i := K(\{x_j | \ j \in I_i\} \cup \{y_j, z_j | \ j \in J_i\})$$

Then E_i is a semi-splitting field of f_i over K and E is the composite of $E_1, \ldots, E_{2m}$. Thus $[E_i : K] \leq d_i! \leq d!$ by Corollary 6.3 and hence

$$[E : K] \leq \prod_{i=1}^{2m} [E_i : K] \leq d!^{2m} \tag{2}$$

Now fix

$$\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{2m}, (\varepsilon_{ij})_{1 \leq i < j \leq r}, \varepsilon'_1, \ldots, \varepsilon'_r) \in \{1, -1\}^{2m + \frac{1}{2}r(r-1)+r}$$

and let

$$F_\varepsilon := E(\sqrt{\varepsilon_1 a_1}, \ldots, \sqrt{\varepsilon_{2m} a_{2m}}, \left\{\sqrt{\varepsilon_{ij}(x_i - x_j)} \middle| 1 \leq i < j \leq 2m\right\})$$

and

$$E_\varepsilon := F_\varepsilon(\sqrt{\varepsilon'_1(X - x_1)}, \ldots, \sqrt{\varepsilon'_r(X - x_r)})$$

Then F_ε is an algebraic extension of E and E_ε is an algebraic extension of $E(X)$. Furthermore, let

$$\eta_i := \varepsilon_i \cdot \prod_{j \in I_i} \varepsilon'_j \in \{1, -1\} \qquad (1 \leq i \leq 2m)$$

and

$$\begin{aligned} N_\varepsilon^+ &:= \#\{i \mid \eta_i = 1\} \\ N_\varepsilon^- &:= \#\{i \mid \eta_i = -1\} \end{aligned}$$

By Lemma 9.1 there are elements $u'_i, v'_i \in E[X]$ which are integral over $R[X]$ such that

$$\prod_{j \in J_i} ((X - y_j)^2 + z_j^2) = {u'_i}^2 + {v'_i}^2$$

and $\delta'(u'_i), \delta'(v'_i) \leq \ell_i \gamma$. If we define

$$\begin{aligned} u_i &:= u'_i \cdot \sqrt{\varepsilon_i a_i} \cdot \prod_{j \in I_i} \sqrt{\varepsilon'_j(X - x_j)} \qquad (1 \leq i \leq 2m) \\ v_i &:= v'_i \cdot \sqrt{\varepsilon_i a_i} \cdot \prod_{j \in I_i} \sqrt{\varepsilon'_j(X - x_j)} \qquad (1 \leq i \leq 2m) \end{aligned}$$

then also $u_1, \ldots, u_{2m}, v_1, \ldots, v_{2m} \in E_\varepsilon$ are integral over $R[X]$ and

$$\delta'(u_i), \delta'(v_i) \leq \ell_i \gamma + \tfrac{1}{2} k_i \gamma = \tfrac{1}{2} \cdot (k_i + 2\ell_i)\gamma = \tfrac{1}{2} d_i \gamma \leq \tfrac{1}{2} d\gamma$$

An easy computation shows

$$f_i = \eta_i \cdot (u_i^2 + v_i^2) \qquad (1 \leq i \leq 2m)$$

and thus $\delta'(f_i) \leq d \cdot \gamma$. Now define

$$W_i := \begin{pmatrix} u_i & v_i \\ -v_i & u_i \end{pmatrix} \qquad (1 \leq i \leq 2m)$$

The matrices W_i are regular since $\det W_i = u_i^2 + v_i^2 = \eta_i f_i \neq 0$ and an easy computation shows

$$W_i^T \begin{pmatrix} \eta_i & 0 \\ 0 & \eta_i \end{pmatrix} W_i = \begin{pmatrix} f_i & 0 \\ 0 & f_i \end{pmatrix} \quad \text{and} \quad W_i^T \begin{pmatrix} f_i & 0 \\ 0 & f_i \end{pmatrix} W_i = f_i^2 \cdot \begin{pmatrix} \eta_i & 0 \\ 0 & \eta_i \end{pmatrix}$$

Since $\delta'(u_i), \delta'(v_i) \leq \frac{1}{2} d\gamma$ and $\delta'(f_i) \leq d\gamma$ this yields $2 \times (f_i) \equiv_{d\gamma} 2 \times (\eta_i)$ and therefore Lemma 8.6 and Lemma 8.8 yield

$$(3) \qquad 2 \times D \equiv_{2md\gamma} 2 \times \operatorname{diag}(\eta_1, \ldots, \eta_{2m}) \qquad \text{w.r.t. } (R[X], \delta') \text{ over } E_\varepsilon$$

with $D := \operatorname{diag}(f_1, \ldots, f_{2m})$. Now we distinguish two cases.

Case 1: F_ε is formally real

We fix an ordering P of F_ε and distinguish two subcases

Subcase 1.1: There are i, j such that $\varepsilon_i' = -1,\ \varepsilon_j' = 1,\ x_i \leq_P x_j$

Then $\sqrt{x_i - X}, \sqrt{X - x_j} \in E_\varepsilon$. Furthermore $\sqrt{x_i - x_j} \in F_\varepsilon$ or $\sqrt{x_j - x_i} \in F_\varepsilon$ by the construction of F_ε. Since F_ε is formally real and $x_i \leq_P x_j$ we necessarily obtain $\sqrt{x_j - x_i} \in F_\varepsilon$. Hence

$$\sqrt{x_i - X}^2 + \sqrt{X - x_j}^2 + \sqrt{x_j - x_i}^2 = 0$$

is a non-trivial representation of 0 as a sum of squares in E_ε, and all summands are integral over $R[X]$. The δ'-values of all the roots are bounded by $\frac{1}{2}\gamma$. Thus $3 \times < 1 >$ is $\frac{1}{2}\gamma$-isotropic over E_ε. Therefore

$$4 \times D \equiv_{2m(d + \frac{5}{2})\gamma} 4m \times \operatorname{diag}(1, -1) \quad \text{w.r.t. } (R[X], \delta') \text{ over } E_\varepsilon$$

by Theorem 9.5.

Subcase 1.2: For all i, j such that $\varepsilon_i' = -1,\ \varepsilon_j' = 1$ holds $x_j <_P x_i$

In this case the ordering P of F_ε extends to an ordering P' of $F_\varepsilon(X)$ such that $x_j < X$ if $\varepsilon_j' = 1$ and $X < x_i$ if $\varepsilon_i' = -1$ (cf. [22], Ch. I, §1). Thus $\varepsilon_i'(X - x_i) \in P'$ $(1 \leq i \leq r)$ and therefore P' extends to an ordering P'' of E_ε (cf. [36], Theorem 1.26). We further let $Q := P'' \cap K(X)$. Then by assumption

$$0 = \operatorname{sign}_Q < f_1, \ldots, f_{2m} >= \operatorname{sign}_{P''} < \eta_1(u_1^2 + v_1^2), \ldots, \eta_{2m}(u_{2m}^2 + v_{2m}^2) > = N_\varepsilon^+ - N_\varepsilon^-$$

and thus $N_\varepsilon^+ = N_\varepsilon^-$. Therefore

$$\operatorname{diag}(\eta_1, \ldots, \eta_{2m}) \equiv_0 m \times \operatorname{diag}(1, -1)$$

by Lemma 8.6 and thus

$$2 \times D \equiv_{2md\gamma} 2m \times \operatorname{diag}(1, -1) \qquad \text{over } E_\varepsilon$$

by (3), Lemma 8.5 and Lemma 8.9.

Case 2: F_ε *is not formally real*

We apply Lemma 11.6 to the field $E(\sqrt{\varepsilon_1 a_1},\ldots,\sqrt{\varepsilon_{2m}a_{2m}})$ and obtain a subset $I \subset \{(i,j)|\ 1 \le i < j \le r\}$ of cardinality $\#I \le r$ such that

$$L := E(\sqrt{\varepsilon_1 a_1},\ldots,\sqrt{\varepsilon_{2m}a_{2m}}, \left\{\sqrt{\varepsilon_{ij}(x_i - x_j)}\middle|(i,j)\in I\right\})$$

is not formally real. Obviously $[L:E] \le 2^{2m+r}$ and thus we get from (1) and (2)

$$[L:K] = [L:E]\cdot[E:K] \le 2^{2m+r}\cdot d!^{2m} \le 2^{2m+2md}\cdot d!^{2m} = (2^{d+1}\cdot d!)^{2m} =: d'$$

Since $\mathrm{char}(K) = 0$ there is a $\mathbb{Z}$-linear combination ϑ of $x_1,\ldots,x_r,y_1,\ldots,y_s,z_1,\ldots,z_s$, $\sqrt{\varepsilon_1 a_1},\ldots,\sqrt{\varepsilon_{2m}a_{2m}}$ and $\sqrt{\varepsilon_{ij}(x_i-x_j)}$ $\quad((i,j)\in I)$ such that ϑ is a primitive element for the extension L/K. By construction ϑ is integral over R and $\delta(\vartheta) \le \gamma$. Thus the form $h_1(d',\gamma)\times <1>$ is $h_2(d',\gamma)$-isotropic over $K(\vartheta) = L$ and hence over E_ε.

Now let $t \in \mathbb{N}_{\ge 1}$ be minimal such that $h_1(d',\gamma) \le 2^t + 1$. Then the definition of t yields $2^{t-1} \le h_1(d',\gamma)$, provided that $t \ne 1$. However, if $t = 1$ this estimate is obviously true since $h_1(d',\gamma) \ge 2$. By Theorem 9.5 we get

$$2^{t+1}\times D \equiv_{2m((3^t+2)h_2(d',\gamma)+d\gamma)} 2^{t+1}m\times \mathrm{diag}(1,-1) \quad \text{over } E_\varepsilon$$

Thus we proved that for any choice of $\varepsilon \in \{-1,1\}^p$ with $p := 2m + \frac{1}{2}r(r+1)$ we obtained that

$$2^{t+1}\times D \equiv_\beta 2^{t+1}m\times \mathrm{diag}(1,-1)$$

w.r.t. $(R[X],\delta')$ over E_ε with

$$\beta := \max(2m(d+\tfrac{5}{2})\gamma, 2m((3^t+2)h_2(d',\gamma)+d\gamma))$$

Now we may apply Theorem 8.15 and obtain that

$$k'\times D \oplus \ell'\times(-D) \equiv_{\alpha'} k'm\times\mathrm{diag}(1,-1)\oplus \ell'm\times\mathrm{diag}(-1,1)$$

w.r.t. $(R[X],\delta')$ over $E(X)$, with

$$\begin{aligned} k' &:= 2^{p-1}(2^p+1)2^{t+1} \\ \ell' &:= 2^{p-1}(2^p-1)2^{t+1} \\ \alpha' &:= 4^p(\beta+2\gamma) \end{aligned}$$

Note that $k' > \ell'$. If we further let $n' := (k'+\ell')m = 2^{2p+t+1}m$ then Lemma 8.6 yields

$$k'\times D\oplus \ell'\times(-D) \equiv_{\alpha'} n'\times \mathrm{diag}(1,-1) \tag{4}$$

Since $h_2(d',\gamma) = h_2((2^{d+1}d!)^{2m},\gamma) \ge [\log_2(2^{d+1}d!)]\cdot\gamma \ge d\gamma$ one can easily see that

$$\beta + 2\gamma \le 2m(3^t+3)\cdot h_2(d',\gamma) \tag{5}$$

We now claim that

$$\beta + 2\gamma \leq 5m \cdot h_1(d',\gamma)^2 \cdot h_2(d',\gamma) \tag{6}$$

If $t = 1$ the claim follows immediately from (5) and the fact $h_1(d',\gamma) \geq 2$. If $t \neq 1$ then $2^{t-1} + 1 \leq h_1(d',\gamma)$ by the definition of t. Thus

$$h_1(d',\gamma)^2 \geq (2^{t-1}+1)^2 = 4^{t-1} + 2^t + 1 \geq \tfrac{4}{3}(3^{t-1}+1) = \tfrac{4}{9}(3^t+3)$$

and (5) implies the assertion of the claim.
The integers p, k', ℓ' and n' still depend on the type (r,s) of the semi-splitting field E of f. Therefore we define

$$q := 2m + \tfrac{1}{2}\deg f(\deg f + 1)$$

and

$$\begin{aligned} k &:= 2^{q-1}(2^q+1)2^{t+1} \\ \ell &:= 2^{q-1}(2^q-1)2^{t+1} \\ n &:= (k+\ell)m = 2^{2q+t+1}m \\ \alpha &:= 4^q(\beta+2\gamma) \end{aligned}$$

Then p, k, ℓ, n and α do not depend on r. The definition of p and (1) yield

$$2p \leq 2q \leq 4m + 2md(2md+1) \leq 6m^2d^2 \tag{7}$$

Furthermore $k > \ell$ and by (6),(7) and $2^{t-1} \leq h_1(d',\gamma)$ we obtain the estimates

$$\begin{aligned} n &\leq 2^{6m^2d^2+2} \cdot m \cdot h_1(d',\gamma) \\ \alpha &\leq 5m \cdot 2^{6m^2d^2} \cdot h_1(d',\gamma)^2 \cdot h_2(d',\gamma) \end{aligned}$$

We finally will prove that

$$k \times D \oplus \ell \times (-D) \equiv_\alpha n \times \operatorname{diag}(1,-1) \qquad \text{w.r.t. } (R[X],\delta') \text{ over } E(X)$$

If $r = \deg f$ then $p = q$ and we are done. So assume that $r < \deg f$ and hence $p < q$. Some elementary computations show

$$\begin{aligned} k - \ell &= 2^{q+t+1} \\ k' - \ell' &= 2^{p+t+1} \\ \ell - 2^{q-p}\ell' &= 2^{q+t}(2^q - 2^p) > 0 \end{aligned}$$

and hence $k = \ell + 2^{q-p}(k'-\ell')$. From (4) and Lemma 8.6 we get

$$2^{q-p}k' \times D \oplus 2^{q-p}\ell' \times -D \equiv_{\alpha'} 2^{q-p}n' \times \operatorname{diag}(1,-1) \tag{8}$$

As $\delta'(f_i) \le d\gamma$ we obtain from Lemma 8.13

$$\operatorname{diag}(f_i, -f_i) \equiv_{d\gamma} \operatorname{diag}(1, -1) \quad (1 \le i \le 2m)$$

and thus

$$D \oplus -D \equiv_{2md\gamma} 2m \times \operatorname{diag}(1, -1)$$

by Lemma 8.6 and Lemma 8.8. Now Lemma 8.9 implies

$$(\ell - 2^{q-p}\ell') \times (D \oplus -D) \equiv_{2md\gamma} 2m(\ell - 2^{q-p}\ell') \times \operatorname{diag}(1, -1) \tag{9}$$

Taking into account that $2^{q-p}n' + 2m(\ell - 2^{q-p}\ell') = n$ and $k = \ell + 2^{q-p}(k' - \ell')$ we obtain from (8), (9), Lemma 8.6, Lemma 8.8 and Lemma 8.5

$$k \times D \oplus \ell \times -D \equiv_{\alpha' + 2md\gamma} n \times \operatorname{diag}(1, -1)$$

Finally, the definition of α' and β imply $\alpha' + 2md\gamma \le 2\alpha' \le 4^{q-p}\alpha' = \alpha$ and the theorem is proved. $\square$

Definition: *Let k be a formally real field with finite second Pythagoras number $\mathrm{P}_2(k)$. For $n, d \in \mathbb{N}$, $n \ge 1$, $d \ge 2$ and $s \in \mathbb{Q}_{\ge 0}$ we let*

$$H_k^{1,n}(d, s) := 2^{n+1} \cdot \mathrm{P}_2(k) \cdot H_k(n+1, \max(d, [ds]))^{n+1}$$
$$H_k^{2,n}(d, s) := H_k(n+1, \max(d, [ds])) \cdot \max(1, s)$$

Proposition 11.8: *Let k be a formally real field with finite second Pythagoras number $\mathrm{P}_2(k)$ and suppose that $\delta\colon \overline{k(X_1, \ldots, X_n)} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ is a $k[X_1, \ldots, X_n]$-stable degree function such that $\delta(f) = \deg f$ for all $f \in k[X_1, \ldots, X_n]$. Then*

$$(H_k^{1,n}, H_k^{2,n}) \in \mathcal{H}(k(X_1, \ldots, X_n), k[X_1, \ldots, X_n], \delta)$$

Proof: Define $K := k(X_1, \ldots, X_n)$ and $R := k[X_1, \ldots, X_n]$ and let $\vartheta \in \bar{K}$ be integral over $k[X_1, \ldots, X_n]$, $[K(\vartheta) : K] \le d$, $d \ge 2$, $\delta(\vartheta) \le s$ and suppose that $K(\vartheta)$ is not formally real. Let

$$f := \operatorname{Irr}(\vartheta, K)$$

Then

$$\bar{M}_\delta(f) = \delta(\vartheta) \le s$$

by Lemma 2.15 and Proposition 3.3. As ϑ is integral over $R = k[X_1, \ldots, X_n]$ we obtain $f \in R[X]$. Thus f is a polynomial in $n+1$ indeterminates over k. Let $m := \deg_X f = [K(\vartheta) : K] \le d$ and express f in the form

$$f = \sum_{i=0}^{m} f_i X^i$$

for certain $f_0, \ldots, f_m \in k[X_1, \ldots, X_n]$, $f_m = 1$. As f is monic in X we get $\deg f_i = \delta(f_i) \leq (m-i)\bar{M}_\delta(f) \leq (m-i)s$ and therefore $\deg(f_i X^i) \leq (m-i)s+i \leq m{\cdot}\max(1,s) \leq d{\cdot}\max(1,s)$ Thus

$$\deg f \leq \max(d, [ds]) =: \ell$$

By Theorem 5.3 there are a natural number $r \leq 2^{n+1} \cdot P_2(k) \cdot H_k(n+1, \ell)^{n+1} = H_k^{1,n}(d,s)$ and polynomials $g, g_1, \ldots, g_r \in k[X_1, \ldots, X_n]$, $g \neq 0$ such that $g^2 f = \sum_{i=1}^r g_i^2$, $\deg g_i \leq H_k(n+1, \ell)$ and f does not divide all polynomials $g_1, \ldots, g_r$. Since f is monic in X also in $K[X]$ it does not divide all g_i's and consequently $w_i := g_i(X_1, \ldots, X_n, \vartheta) \neq 0$ for at least one i. Furthermore $w_1, \ldots, w_r$ are integral over $R = k[X_1, \ldots, X_n]$ and

$$\sum_{i=1}^r w_i^2 = g(\vartheta)^2 f(\vartheta) = 0$$

is a non-trivial representation of 0 as a sum of squares in $K(\vartheta)$.

Let $d_i := \deg_X g_i$ and express g_i in the form $\sum_{j=0}^{d_i} g_{ij} X^j$. Then $\deg g_{ij} \leq d_i - j$ and hence $\delta(g_{ij}\vartheta^j) \leq d_i - j + js \leq d_i \cdot \max(1,s)$. This yields $\delta(w_i) \leq H_k(n+1, \ell) \cdot \max(1,s) = H_k^{2,n}(d,s)$ and therefore $r \times < 1 >$ is $H_k^{2,n}(d,s)$-isotropic over K. Finally, the technical condition (ii) in the definition of $\mathcal{H}(K, R, \delta)$ is also satisfied since

$$H_k^{2,n}(d,s) = H_k(n+1, \ell) \cdot \max(1,s) \geq [\tfrac{1}{2}\ell] \cdot s \geq [\tfrac{1}{2}d] \cdot s \geq [\log_2 d] \cdot s$$

by Lemma 1.3. $\square$

The next lemma is a well-known result. For the convenience of the reader we give a proof.

Lemma 11.9: *Let k be an infinite field and assume that $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Then there is a k-algebra automorphism σ of $k[X_1, \ldots, X_n]$ such that*

(a) $\sigma(X_n) = X_n$

(b) $\deg f = \deg \sigma(f)$ *for all* $f \in k[X_1, \ldots, X_n]$

(c) $\deg_{X_n} \sigma(f_i) = \deg \sigma(f_i) \qquad (1 \leq i \leq m)$

Proof: As k is infinite there are $a_1, \ldots, a_{n-1} \in k$ such that $(a_1, \ldots, a_{n-1}, 1)$ is not a zero of any of the homogeneous components of highest degree of the polynomials $f_1, \ldots, f_m$. We define

$$\sigma : k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n]$$

by $\sigma(f) := f(X_1 + a_1 X_n, \ldots, X_{n-1} + a_{n-1} X_n, X_n)$. Obviously σ is a k-algebra automorphism with $\sigma^{-1}(f) = f(X_1 - a_1 X_n, \ldots, X_{n-1} - a_{n-1} X_n, X_n)$. The assertions (a) and (b) are obvious. If $f = \sum_{i=0}^d f^{(i)}$ is the decomposition of f into homogeneous components then

$$\sigma(f) = f^{(d)}(a_1, \ldots, a_{n-1}, 1) X_n^d + g$$

for some $g \in k[X_1, \ldots, X_n]$ with $\deg_{X_n} g < d$. This proves (c). $\square$

Corollary 11.10: *Let k be an infinite field and assume that $f \in k[X_1, \ldots, X_n] \backslash \{0\}$. Then there are $a \in k^\times$, $g, h \in k[X_1, \ldots, X_n]$ and a k-algebra automorphism σ of $k[X_1, \ldots, X_n]$ which preserves the total degree such that*

(a) $\sigma(f) = a \cdot h^2 \cdot g$

(b) *g is squarefree and monic in X_n*

(c) $\deg_{X_n} g = \deg g$

Proof: We split f in the form $f = p^2 \cdot q$ with q squarefree. By Lemma 11.9 there is a k-algebra automorphism σ of $k[X_1, \ldots, X_n]$ which preserves the total degree and

$$\begin{aligned} \deg_{X_n} \sigma(f) &= \deg \sigma(f) \\ \deg_{X_n} \sigma(p) &= \deg \sigma(p) \\ \deg_{X_n} \sigma(q) &= \deg \sigma(q) \end{aligned}$$

Then $\sigma(q) = a \cdot g$ for certain $a \in k^\times$, $g \in k[X_1, \ldots, X_n]$ such that g is monic in X_n and $\deg_{X_n} g = \deg g$.

As q is squarefree so is $\sigma(q)$ and hence also g is squarefree. If we define $h := \sigma(p)$ then $\sigma(f) = a \cdot h^2 \cdot g$ and the corollary is proved. $\square$

Now we are able to prove the following recursion formula for H_k.

Theorem 11.11: *Let k be a formally real field with finite second Pythagoras number $\mathrm{P}_2(k)$ and suppose that $n, d \in \mathbb{N}$, $n \geq 1, d \geq 2$. Then:*

$$H_k(n, d) \leq 2^{2^{9d^4}} \cdot 2^{3n} \cdot \mathrm{P}_2(k)^3 \cdot H_k(n-1, 2^{8d^4})^{3n-2}$$

Proof: Let $f \in k[X_1, \ldots, X_n]$ be positive semidefinite over k and suppose that $\deg f \leq d$. By Corollary 11.10 there is a k-algebra automorphism τ of $k[X_1, \ldots, X_n]$ which preserves the total degree and $\tau(f) = a \cdot h^2 \cdot g$ for certain $a \in k^\times$, $g, h \in k[X_1, \ldots, X_n]$ with g squarefree and monic in X_n and $\deg g = \deg_{X_n} g$.

Since f is positive semidefinite over k so is $\tau(f)$ and hence also ag is positive semidefinite. As g is monic in X_n also g is positive semidefinite and a is a sum of squares in k. Since g is positive semidefinite $\deg g$ is even, i.e.,

$$2m = \deg g = \deg_{X_n} g \leq \deg \tau(f) = \deg f \leq d$$

for some $m \in \mathbb{N}$.

Now we introduce some notation. We let $R := k[X_1, \ldots, X_n]$, $R' := k[X_1, \ldots, X_{n-1}]$ and $R'' := k[X_1, \ldots, X_{n-2}]$. Their fields of quotients we denote by K, K' and K''. Finally we let $\delta : \bar{K} \longrightarrow \mathbb{Q} \cup \{-\infty\}$ be an R-stable degree function on $\bar{K} = \overline{k(X_1, \ldots, X_n)}$ such that $\delta(f) = \deg f$ for all $f \in R = k[X_1, \ldots, X_n]$. The restrictions of δ to the algebraic closures of K' and K'' we denote by δ' and δ''. It is easy to see that δ', δ'' are R'-stable respectively R''-stable.

By Lemma 5.1 g is positive definite over K' as a univariate polynomial in the indeterminate X_n. Furthermore g remains squarefree in the polynomial ring $K'[X_n]$ and thus it has only simple zeroes.

Lemma 2.19 yields $\bar{M}_{\delta'}(g) \leq 1$. Thus we may apply Proposition 10.5 to obtain a diagonal matrix $D = \operatorname{diag}(p_1, \ldots, p_{2m}) \in M_{2m}(R')$ such that $M_{\delta'}(D) \leq 4d^2$ and $\mathrm{H}_g \equiv_{4d^3} D$. In particular $p_1, \ldots, p_{2m} \in R' = k[X_1, \ldots, X_{n-1}]$ and $\deg p_i = \delta'(p_i) \leq 4d^2$.

By Lemma 11.9 there is a k-algebra automorphism $\sigma : R' \longrightarrow R'$ which preserves the total degree such that $\deg \sigma(p_i) = \deg_{X_{n-1}} \sigma(p_i) \quad (1 \leq i \leq 2m)$. Now we define $q_i := \sigma(p_i)$ $(1 \leq i \leq 2m)$ and consider these elements as polynomials in X_{n-1} over R''. Since $\deg q_i = \deg_{X_{n-1}} q_i \quad (1 \leq i \leq 2m)$ the leading coefficients of $q_1, \ldots, q_{2m}$ are elements from $k^\times$ and thus δ''-units. Moreover $\delta'(q_i) = \deg q_i = \deg p_i \leq 4d^2$ and $\bar{M}_{\delta''}(q_i) \leq 1$ by Lemma 2.19.

For a matrix $A = (a_{ij})$ over R' we let $A^\sigma := (\sigma(a_{ij}))$ and for a polynomial $p = \sum_i a_i X_n^i \in R'[X_n] = R$ we define $p^\sigma := \sum_i \sigma(a_i) X_n^i$. Note that $\deg p^\sigma = \deg p$.

The congruence $\mathrm{H}_g \equiv_{4d^3} D$ can be expressed in the form of two matrix equations over $R' = k[X_1, \ldots, X_{n-1}]$. Since σ is a degree preserving automorphism we get $\mathrm{H}_g^\sigma \equiv_{4d^3} D^\sigma$, and as σ extends to an automorphism of the algebraic closure of K' it follows that $\mathrm{H}_g^\sigma = \mathrm{H}_{g^\sigma}$ Therefore

$$\mathrm{H}_{g^\sigma} \equiv_{4d^3} D^\sigma = \operatorname{diag}(q_1, \ldots, q_{2m}) \tag{1}$$

w.r.t. (R', δ') over K'.

As g is positive definite over K' so is g^σ and therefore

$$\operatorname{sign}_P < q_1, \ldots, q_{2m} >= \operatorname{sign}_P(H_{g^\sigma}) = 0$$

for every ordering P of $K' = K''(X_{n-1})$ (cf. [36], Theorem 3.7). Thus by Theorem 11.7 and Proposition 11.8 we obtain natural numbers N_1, N_2, N_3 and $\alpha \in \mathbb{Q}_{\geq 0}$ such that

$$A := N_1 \times D^\sigma \oplus N_2 \times -D^\sigma \equiv_\alpha N_3 \times \operatorname{diag}(1, -1)$$

w.r.t. (R', δ') over $E(X_{n-1})$ for every semi-splitting field E of $q := \prod_{i=1}^{2m} q_i$ over K'' and $N_1 > N_2$ and

$$\begin{aligned} N_3 &\leq 2^{6m^2(4d^2)^2+2} \cdot m \cdot H_k^{1,n-2}(d', 1) \\ &\leq 2d \cdot 2^{24d^6} \cdot H_k^{1,n-2}(d', 1) \end{aligned}$$

$$\begin{aligned} \alpha &\leq 5m \cdot 2^{6m^2(4d^2)^2} \cdot H_k^{1,n-2}(d', 1)^2 \cdot H_k^{2,n-2}(d', 1) \\ &\leq \tfrac{5}{2} d \cdot 2^{24d^6} \cdot H_k^{1,n-2}(d', 1)^2 \cdot H_k^{2,n-2}(d', 1) \end{aligned}$$

with $d' := (2^{4d^2+1} \cdot (4d^2)!)^{2m}$. We get

$$\begin{aligned} \log_2 d' &= 2m \cdot (4d^2 + 1 + \log_2((4d^2)!)) \leq d \cdot (4d^2 + 1 + 4d^2 \cdot \log_2(4d^2)) \\ &= d \cdot (4d^2 + 1 + 8d^2 \cdot \log_2(2d)) \leq 8d^3 \cdot (1 + \log_2(2d)) \\ &\leq 8d^3 \cdot \log_2(4d) \leq 8d^4 \end{aligned}$$

if $d \geq 4$. This yields

$$d' \leq 2^{8d^4} \tag{2}$$

in the case $d \geq 4$. However, a direct computation of d' shows that the above inequality also holds for $d = 2, 3$.
With the definitions of $H_k^{1,n-2}$ and $H_k^{2,n-2}$ this yields the bounds

$$N_3 \leq 2^n \cdot d \cdot 2^{24d^6} \cdot \mathrm{P}_2(k) \cdot H_k(n-1, 2^{8d^4})^{n-1} \tag{3}$$

$$\alpha \leq 5d \cdot 2^{2n-3} \cdot 2^{24d^6} \cdot \mathrm{P}_2(k)^2 \cdot H_k(n-1, 2^{8d^4})^{2n-1} =: \gamma \tag{4}$$

Now let $F_1, \ldots, F_{2m}$ be the splitting fields of $q_1, \ldots, q_{2m}$ over K'' and let F be the composite of $F_1, \ldots, F_{2m}$. Then F is the splitting field of q over K'' and

$$\ell := [F : K''] \leq \prod_{i=1}^{2m} [F_i : K''] \leq \prod_{i=1}^{2m} (\deg_{X_{n-1}} q_i)! \leq (4d^2)!^{2m} \leq d' \tag{5}$$

F is obtained by adjoining all zeroes of all q_i's to K''. Since the leading coefficients of $q_1, \ldots, q_{2m}$ are elements from $k^\times$ these zeroes are integral over R'' and their δ''-values are bounded by 1 by Theorem 2.14. A certain $\mathbb{Z}$-linear combination ϑ of the zeroes of $q_1, \ldots, q_{2m}$ is a generating element for F/K''. By the construction ϑ is integral over R'' and $\delta''(\vartheta) \leq 1$.
F/K'' is a finite Galois extension. Let $[F : K''] = 2^s \cdot t$, t odd and choose a 2-Sylow subfield L of the extension F/K''. Then F/L is a 2-extension of degree $[F : L] = 2^s$ and $[L : K''] = t$ and also $F(X_{n-1})/L(X_{n-1})$ is a 2-extension of degree $[F(X_{n-1}) : L(X_{n-1})] = 2^s$ with ϑ as a generating element.
Now we show that $A \equiv_\alpha N_3 \times \mathrm{diag}(1, -1)$ w.r.t. (R', δ') over F' for every semi-extension F' of $F(X_{n-1})$ which contains $L(X_{n-1})$.
If F' is such a semi-extension of $F(X_{n-1})$ then it is also a semi-extension of F. Let E' be the relative algebraic closure of L in F'. By Proposition 6.5 E' is a semi-extension of F. Thus $F \subset E'(i)$ and therefore q splits into linear factors over $E'(i)$. By Corollary 6.4 E' contains a semi-splitting field E of q over K''. Obviously $E(X_{n-1}) \subset F'$. Since $A \equiv_\alpha N_3 \times \mathrm{diag}(1, -1)$ w.r.t. (R', δ') over $E(X_{n-1})$ we are done.
Now we may apply Theorem 8.18 and obtain that $\frac{1}{2} 2^{2s}(2^s + 1) \times A \oplus \frac{1}{2} 2^{2s}(2^s - 1) \times (-A)$ and $\frac{1}{2} 2^{2s}(2^s + 1) \times \mathrm{diag}(1, -1) \oplus \frac{1}{2} 2^{2s}(2^s - 1) \times \mathrm{diag}(-1, 1)$ are $2^{3s}(\alpha + 3)$-congruent w.r.t. (R', δ') over $L(X_{n-1})$. Thus

$$N_1' \times D^\sigma \oplus N_2' \times -D^\sigma \equiv_{2^{3s}(\alpha+3)} 2^{3s} N_3 \times \mathrm{diag}(1, -1) \tag{6}$$

w.r.t. (R', δ') over $L(X_{n-1})$ for certain $N_1', N_2' \in \mathbb{N}$ by Lemma 8.6 and Lemma 8.5. By (1) and Lemma 8.9 we get

$$N_1' \times H_{g^\sigma} \equiv_{4d^3} N_1' \times D^\sigma$$
$$N_2' \times -H_{g^\sigma} \equiv_{4d^3} N_2' \times -D^\sigma$$

over K' and hence over $L(X_{n-1})$. Thus

$$N_1' \times H_{g^\sigma} \oplus N_2' \times -H_{g^\sigma} \equiv_{8d^3} N_1' \times D^\sigma \oplus N_2' \times -D^\sigma$$

by Lemma 8.8 and hence by (6) and Lemma 8.5

$$N_1' \times H_{g^\sigma} \oplus N_2' \times -H_{g^\sigma} \equiv_\beta 2^{3s} N_3 \times \operatorname{diag}(1, -1)$$

w.r.t. (R', δ') over $L(X_{n-1})$ with $\beta := 2^{3s}(\alpha + 3) + 8d^3$. Since $2^s \leq [F : K''] = \ell$ we get

$$\beta \leq \ell^3(\alpha + 3) + 8d^3 \leq 2\ell^3\gamma \tag{7}$$

Then by Theorem 11.5 there is a natural number N such that the form $N\times < 1, -g^\sigma >$ is $(2^{3s} \cdot N_3 \cdot 2^{2^{d^2}} \cdot \beta)$-isotropic w.r.t. (R, δ) over $L(X_{n-1}, X_n)$.
L was chosen as a 2-Sylow subfield of F/K''. By Theorem 3.6 there are $z_1, \ldots, z_r \in L$, integral over R'' such that $L = K''(z_1, \ldots, z_r)$ and

$$\delta''(z_i) \leq [F : L] \cdot \delta''(\vartheta) \leq [F : L] = 2^s$$

Obviously

$$L(X_{n-1}, X_n) = K''(X_{n-1}, X_n)(z_1, \ldots, z_r) = K(z_1, \ldots, z_r)$$

and furthermore $[L(X_{n-1}, X_n) : K] = [L : K''] = t$ is odd. Now Theorem 7.8 implies that $N\times < 1, -g^\sigma >$ is $2^t \cdot t! \cdot (2N_3 \cdot 2^{3s} \cdot 2^{2^{d^2}} \cdot \beta + d + 2t^2 \cdot 2^s)$-isotropic w.r.t. (R, δ) over K.
By definition there are $g_1, \ldots, g_N, h_1, \ldots, h_N \in R = k[X_1, \ldots, X_n]$ such that not all of them are zero and

$$\sum_{i=1}^{N} h_i^2 - g^\sigma \sum_{i=1}^{N} g_i^2 = 0$$

and

$$\delta(g_i), \delta(h_i) \leq 2^t \cdot t! \cdot (2N_3 \cdot 2^{3s} \cdot 2^{2^{d^2}} \cdot \beta + d + 2t^2 \cdot 2^s)$$

We define $G := \sum_{i=1}^N g_i^2$. Then $G \neq 0$. Otherwise also $\sum_{i=1}^N h_i^2 = g^\sigma G = 0$ and hence $g_1, \ldots, g_N, h_1, \ldots, h_N = 0$ since $k(X_1, \ldots, X_n)$ is formally real. Since $\tau(f) = ah^2 g$ we obtain

$$G^2 \cdot \tau(f) = ah^2 G^2 g = a \cdot \sum_{i=1}^{N} \sum_{j=1}^{N} (g_i^{\sigma^{-1}} h_j^{\sigma^{-1}} h)^2 = a \cdot \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij}^2$$

with $f_{ij} := g_i^{\sigma^{-1}} h_j^{\sigma^{-1}} h$. Since $\deg p^\sigma = \deg p$ for all $p \in k[X_1, \ldots, X_n]$ we get

$$\begin{aligned}
\deg f_{ij} = \deg(g_i^{\sigma^{-1}} h_j^{\sigma^{-1}} h) &= \deg g_i + \deg h_j + \deg h \leq \delta(g_i) + \delta(h_j) + d \\
&\leq 2 \cdot 2^t \cdot t! \cdot (2N_3 \cdot 2^{3s} \cdot 2^{2^{d^2}} \cdot \beta + d + 2t^2 \cdot 2^s) + d \\
&\leq 2^{3s+1} \cdot 2^{2^{d^2}} \cdot 2^t \cdot t! \cdot (2N_3 \cdot \beta + d + t^2)
\end{aligned}$$

Since $2^s \cdot t = \ell$ and $d \leq \gamma$ we get from (7)

$$2N_3\beta + d + t^2 \leq 4N_3\ell^3\gamma + d + \ell^2 \leq 6N_3\ell^3\gamma$$

and furthermore

$$2^{3s+1} \cdot 2^t \cdot t! \leq 2^{2s+1} \cdot 2^t \cdot (2^s t)! \leq 2\ell^2 \cdot 2^\ell \cdot \ell!$$

Together with the bounds (3),(4) for N_3 and γ this yields

$$\begin{aligned}\deg f_{ij} &\leq 60d^2 \cdot 2^{48d^6} \cdot \ell^5 \cdot 2^\ell \cdot \ell! \cdot 2^{2^{d^2}} \cdot 2^{3n-3} \cdot \mathrm{P}_2(k)^3 \cdot H_k(n-1, 2^{8d^4})^{3n-2} \\ &\leq 8d^2 \cdot 2^{48d^6} \cdot \ell^5 \cdot 2^\ell \cdot \ell! \cdot 2^{2^{d^2}} \cdot 2^{3n} \cdot \mathrm{P}_2(k)^3 \cdot H_k(n-1, 2^{8d^4})^{3n-2}\end{aligned}$$

By (2) and (5) we get $\ell \leq d' \leq 2^{8d^4}$ and thus

$$\log_2(\ell!) \leq \log_2(\ell^\ell) = \ell \cdot \log_2 \ell \leq 2^{8d^4} \cdot \ell$$

Hence

$$\begin{aligned}\log_2(8d^2 \cdot 2^{48d^6} \cdot \ell^5 \cdot 2^\ell \cdot \ell! \cdot 2^{2^{d^2}}) &\leq \log_2(8d^2) + 48d^6 + 5 \cdot 8d^4 + \ell + 8d^4 \cdot \ell + 2^{2^{d^2}} \\ &\leq 6 \cdot 8d^4 \cdot 2^{8d^4} \leq 2^{9d^4}\end{aligned}$$

The last estimate follows from the fact that $48d^6 \leq 2^{d^4}$ for $d \geq 2$. This can easily be shown by induction. Finally this yields the bound

$$\deg f_{ij} \leq 2^{2^{9d^4}} \cdot 2^{3n} \cdot \mathrm{P}_2(k)^3 \cdot H_k(n-1, 2^{8d^4})^{3n-2}$$

Since τ preserves the total degree and a is a sum of squares in k we are done. $\square$

This recursion formula enables us to give bounds for the functions N_k and H_k. First we introduce some notation. We let

$$\begin{aligned}\exp_2 :\ \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto 2^x\end{aligned}$$

and by $\exp_2^n$ we denote the n-fold composition of $\exp_2$. Next we state and prove two easy lemmas concerning the function $\exp_2$.

Lemma 11.12: *Let $x, y \in \mathbb{R}$, $n, m \in \mathbb{N}\backslash\{0\}$ and suppose that $x \leq y$ and $n \leq m$. Then:*

(a) $\exp_2^n(x) \leq \exp_2^n(y)$

(b) $\exp_2^n(x) \leq \exp_2^m(x)$

Proof: (a) can be shown by an easy induction on n and (b) follows from the fact that $x \leq 2^x$ for $x \in \mathbb{R}$. $\square$

Lemma 11.13: *Let $x, y \in \mathbb{R}_{\geq 1}$, $n \in \mathbb{N}\setminus\{0\}$. Then:*

$$\exp_2^n(x) \cdot \exp_2^n(y) \leq \exp_2^n(x+y)$$

Proof: The proof runs by induction on n. The case $n = 1$ follows immediately from

$$\exp_2(x) \cdot \exp_2(y) = 2^x \cdot 2^y = 2^{x+y} = \exp_2(x+y)$$

Now let $n > 1$. The induction hypothesis yields

$$\exp_2^n(x) \cdot \exp_2^n(y) = \exp_2^{n-1}(2^x) \cdot \exp_2^{n-1}(2^y) \leq \exp_2^{n-1}(2^x + 2^y)$$

Since $x, y \geq 1$ we get $1 \leq (2^x - 1) \cdot (2^y - 1) = 2^{x+y} - 2^x - 2^y + 1$ and thus $2^x + 2^y \leq 2^{x+y}$. Now Lemma 11.12(a) implies

$$\exp_2^{n-1}(2^x + 2^y) \leq \exp_2^{n-1}(2^{x+y}) = \exp_2^n(x+y)$$

This yields the assertion. $\square$

The next theorem gives a bound for $H_k(n, d)$. In the case $n \leq 4$ this bound improves the known bounds of Lombardi and Roy.

Theorem 11.14: *Let k be a formally real field with finite second Pythagoras number $\mathrm{P}_2(k)$. Then there is a real number $C \leq \max(6, \mathrm{P}_2(k))$ such that*

$$H_k(n, d) \leq \exp_2^n(C \cdot n \cdot d^4)$$

for all $n, d \in \mathbb{N}$, $n \geq 1$, $d \geq 2$.

Proof: Let $C := \max(6, \mathrm{P}_2(k))$. We prove the theorem by induction on n. The case $n = 1$ is obvious since $H_k(1, d) = [\frac{1}{2}d] \leq \frac{1}{2}d$ by Lemma 1.5. In the case $n = 2$ our recursion formula from Theorem 11.11 yields

$$H_k(2, d) \leq 2^{2^{9d^4}} \cdot 2^6 \cdot \mathrm{P}_2(k)^3 \cdot (\tfrac{1}{2} \cdot 2^{8d^4})^4 = 2^{2^{9d^4}} \cdot 2^{32d^4+2} \cdot \mathrm{P}_2(k)^3$$

Since $32d^4 + 2 \leq 33d^4 \leq 2^{d^4}$ and $\mathrm{P}_2(k)^3 \leq 2^{2^{\mathrm{P}_2(k)}}$ we get from Lemma 11.13

$$H_k(2, d) \leq \exp_2^2(10d^4 + \mathrm{P}_2(k))$$

As $d \geq 2$ and $C \geq 6$ we obtain $10d^4 \leq 6(2d^4 - 1) \leq C(2d^4 - 1)$ and thus $10d^4 + \mathrm{P}_2(k) \leq C \cdot 2d^4$. This yields the case $n = 2$.

Now let $n \geq 3$. By Theorem 11.11 and the induction hypothesis we get

$$H_k(n, d) \leq 2^{2^{9d^4}} \cdot 2^{3n} \cdot \mathrm{P}_2(k)^3 \cdot \exp_2^{n-1}(C \cdot (n-1) \cdot 2^{8d^4})^{3n-2}$$

As $n \geq 3$ and $\mathrm{P}_2(k)^3 \leq 2^{2^{\mathrm{P}_2(k)}}$ we get from Lemma 11.12 and Lemma 11.13

$$\begin{aligned} H_k(n, d) &\leq \exp_2^{n-1}(9d^4 + 3n + \mathrm{P}_2(k) + (3n-2)C(n-1) \cdot 2^{8d^4}) \\ &\leq \exp_2^{n-1}(3n^2 C \cdot 2^{8d^4}) \end{aligned}$$

$d \geq 2$ and $C \geq 6$ yield

$$\begin{aligned} \log_2(3n^2 C) &\leq \log_2(4n^2 C^2) = 2 \cdot \log_2(2nC) \leq 4nC \leq \tfrac{1}{2} C n d^4 \\ 8d^4 &\leq \tfrac{1}{2} C n d^4 \end{aligned}$$

and thus $3n^2 C \cdot 2^{8d^4} \leq 2^{Cnd^4}$. Hence

$$H_k(n, d) \leq \exp_2^{n-1}(2^{Cnd^4}) = \exp_2^n(Cnd^4)$$

This yields the induction step and the theorem is proved. $\square$

Finally we also give a bound for $N_k(n,s,d)$. However, only in the case $s=1$ this bound will improve known results.

Theorem 11.15: *Let k be a formally real field with finite second Pythagoras number $\mathrm{P}_2(k)$. Then there is a real number $C \le \max(24, \mathrm{P}_2(k))$ such that*

$$N_k(n,s,d) \le \exp_2^{\nu(s)}(C\cdot n^2\cdot\max(1,s)\cdot\log_2 d)$$

for all $n,s,d\in\mathbb{N}$, $n\ge 1$, $d\ge 3$, with $\nu(s) := \frac{1}{2}(s+1)(s+2)$.

Proof: Let $C := \max(24, \mathrm{P}_2(k))$. We prove the theorem by induction on s. By Corollary 1.12 we have

$$N_k(n,0,d) \le d^n(d^n+1) \le 2d^{2n} \le 2^{Cn^2\cdot\log_2 d}$$

As $\nu(0)=1$ this yields the case $s=0$.

Now assume that $s\ge 1$. By Theorem 5.8 we obtain

$$N_k(n,s,d) \le 5d^n\cdot N'_k(n,s-1,\ell) \tag{1}$$

with $\ell := d^{4n^2}\cdot H_k(s+1,d^{4n^2})$. The induction hypothesis and Lemma 1.4 yield

$$\begin{aligned} N'_k(n,s-1,\ell) &= \max(N_k(n,s-1,\ell), N_k(n,-1,\ell)) \\ &\le \max(\exp_2^{\nu(s-1)}(Cn^2s\cdot\log_2\ell), \ell^n) = \exp_2^{\nu(s-1)}(Cn^2s\cdot\log_2\ell) \end{aligned} \tag{2}$$

since $\nu(s-1)\ge 1$. Theorem 11.14 implies

$$H_k(s+1,d^{4n^2}) \le \exp_2^{s+1}(C(s+1)d^{16n^2})$$

and thus

$$\begin{aligned} \ell = d^{4n^2}\cdot H_k(s+1,d^{4n^2}) &\le \exp_2(\log_2(d^{4n^2}))\cdot\exp_2^{s+1}(C(s+1)d^{16n^2}) \\ &\le \exp_2^{s+1}(\log_2(d^{4n^2}) + C(s+1)d^{16n^2}) \end{aligned}$$

by Lemma 11.13. Hence

$$\log_2\ell \le \exp_2^s(\log_2(d^{4n^2}) + C(s+1)d^{16n^2})$$

and Lemma 11.13 yields

$$\begin{aligned} Cn^2s\cdot\log_2\ell &\le Cn^2s\cdot\exp_2^s(\log_2(d^{4n^2}) + C(s+1)d^{16n^2}) \\ &= \exp_2(\log_2(Cn^2s))\cdot\exp_2^s(\log_2(d^{4n^2}) + C(s+1)d^{16n^2}) \\ &\le \exp_2^s(\log_2(Cn^2sd^{4n^2}) + C(s+1)d^{16n^2}) \end{aligned}$$

Therefore (2) implies

$$N'_k(n,s-1,\ell) \le \exp_2^{\nu(s-1)+s}(\log_2(Cn^2sd^{4n^2}) + C(s+1)d^{16n^2})$$

and a further application of Lemma 11.13 together with (1) yields

$$N_k(n,s,d) \le \exp_2^{\nu(s-1)+s}(\log_2(5d^n) + \log_2(Cn^2sd^{4n^2}) + C(s+1)d^{16n^2}) \tag{3}$$

Now

$$\log_2(5d^n) + \log_2(Cn^2sd^{4n^2}) = \log_2(5Cn^2sd^n \cdot d^{4n^2}) \le 5Cn^2sd^n \cdot d^{4n^2} \le Cs \cdot d^{16n^2}$$

and hence

$$\log_2(5d^n) + \log_2(Cn^2sd^{4n^2}) + C(s+1)d^{16n^2} \le C(2s+1)d^{16n^2} \le 3Csd^{16n^2} \tag{4}$$

Since $\nu(s) = \nu(s-1) + s + 1$ we obtain from (3) and (4)

$$N_k(n,s,d) \le \exp_2^{\nu(s)}(\log_2(3Cs) + 16n^2 \cdot \log_2 d) \tag{5}$$

As the map $x \mapsto x^{-1} \cdot \log_2 x$ is decreasing for $x \ge 3$ we get

$$\frac{\log_2(3Cs)}{3Cs} \le \frac{\log_2 72}{72} \le \frac{7}{72} \le \frac{1}{10}$$

and therefore

$$\log_2(3Cs) \le \tfrac{3}{10}Cs \le \tfrac{1}{3}Cn^2s \cdot \log_2 d$$

Since

$$16n^2 \cdot \log_2 d \le \tfrac{2}{3}Cn^2s \cdot \log_2 d$$

we get from (5)

$$N_k(n,s,d) \le \exp_2^{\nu(s)}(Cn^2s \cdot \log_2 d)$$

This yields the induction step and the theorem is proved. $\square$

Remark: Since $\nu(1) = 3$ the above theorem yields a 3-fold exponential bound for $N_k(n,1,d)$. This improves the result of Lombardi and Roy in the case of a one-dimensional ideal.

References

[1] ARTIN, E.: *Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abh. Math. Sem. Univ. Hamburg 3 (1924), 319-323*

[2] ARTIN, E.: *Über die Zerlegung definiter Funktionen in Quadrate, Abh. Math. Sem. Univ. Hamburg 5 (1927), 100-115*

[3] ARTIN, E., SCHREIER, O.: *Algebraische Konstruktion reeller Körper, Abh. Math. Sem. Univ. Hamburg 5 (1927), 85-99*

[4] ARTIN, E, SCHREIER, O.: *Eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg 5 (1927), 225-231*

[5] BECKER, E., NEUHAUS, R.: *Computation of real radicals of polynomial ideals, in: Computational Algebraic Geometry, Progress in Math., Vol. 109, Birkhäuser 1993, 1-20*

[6] BECKER, E., WÖRMANN, T.: *On the trace formula for quadratic forms, in: Proc. RAGSQUAD Berkeley, Contemp. Math., Vol. 155, American Mathematical Society 1994, 271-291*

[7] BOURBAKI, N.: *Commutative Algebra, Paris 1972*

[8] BROWNAWELL, W.D.: *Bounds for the degrees in the Nullstellensatz, Ann. Math. 126 (1987), 577-592*

[9] CANIGLIA, L., GALLIGO, A., HEINTZ, J.: *Some new effectivity bounds in computational geometry, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proc. 6th Intern. Conf. AAECC-6, Lecture Notes in Computer Science 357, Springer 1989, 131-151*

[10] CASSELS, J.W.S.: *On the representation of rational functions as sums of squares, Acta Arithm. 9 (1964), 79-82*

[11] COLLIOT-THÉLÈNE, J.-L.: *Variantes du Nullstellensatz réel et anneaux formellement réels, in: Géométrie Algébrique Réelle et Formes Quadratiques, Lecture Notes in Math. 959, Springer 1982, 98-108*

[12] DAYKIN, D. E.: *Hilbert's 17th and other problems, Thesis, University of Reading (1961), unpublished*

[13] DELZELL, C. N.: *Kreisel's Unwinding of Artin's Proof, in: Kreiseliana, about and around Georg Kreisel, A.K. Peters, Wellesley, 1996*

[14] DUBÉ, T.W.: *A combinatorial proof of the effective Nullstellensatz, J. Symb. Comput. 15 (1993), 277-296*

[15] DUBOIS, D.W.: *A nullstellensatz for ordered fields, Arkiv för Mat. 8 (1969), 111-114*

[16] GIANNI, P., MORA, T.: *Algebraic solution of systems of polynomial equation using Gröbner bases, Proc. AAECC 5, Lecture Notes in Computer Science 356, Springer 1989, 247-257*

[17] GIANNI, P., TRAGER, B., ZACHARIAS, G.: *Gröbner bases and primary decomposition of polynomial ideals, in: Computational aspects of commutative algebra, Academic press, 15-33*

[18] HERMANN, G.: *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95 (1926), 736-788*

[19] HILBERT, D.: *Über die Darstellung definiter Formen als Summe von Formenquadrate, Math. Ann. 32 (1888), 342-350*

[20] HILBERT, D.: *Über ternäre definite Formen, Acta Math. 17 (1893), 169-197*

[21] JACOBSON, N.: *Basic Algebra I, W.H. Freeman 1974*

[22] KNEBUSCH, M., SCHEIDERER, C.: *Einführung in die reelle Algebra, Vieweg 1989*

[23] KOLLÁR, J.: *Sharp effective Nullstellensatz, Journal Amer. Math. Soc. 1 (1988), 963-975*

[24] KRIVINE, J.L.: *Anneaux préordonnés, Journal d'analyse mathématique 12 (1964), 307-326*

[25] KUNZ, E.: *Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg 1980*

[26] LAM, T.Y.: *The algebraic theory of quadratic forms, Reading, 1973*

[27] LAM, T.Y.: *Orderings, valuations and quadratic forms, Regional conference series in mathematics 52, American Mathematical Society, 1983*

[28] LAM, T.Y.: *An introduction to real algebra, Rocky Mountain J. Math. 14 (1984), 767-814*

[29] LANG, S.: *Algebra, Addison-Wesley 1965*

[30] LOMBARDI, H.: *Une borne sur les degrés pour le théorème des zéros réels effectif, in: Real Algebraic Geometry, Lecture Notes in Math. 1524, Springer 1992, 323-345*

[31] MOTZKIN, T.S.: *The arithmetic-geometric inequality, in: Inequalities, Academic Press, New York 1967, 205-224*

[32] PFISTER, A.: *Zur Darstellung von* -1 *als Summe von Quadraten in einem Körper, Journal London Math. Soc. 40 (1965), 159-165*

[33] PFISTER, A.: *Multiplikative quadratische Formen, Arch. Math. 16 (1965), 363-370*

[34] PFISTER, A.: *Zur Darstellung definiter Funktionen als Summe von Quadraten, Inv. Math. 4 (1967), 229-237*

[35] POWERS, V., WÖRMANN, T.: *An algorithm for sums of squares of polynomials, to appear in: J. Pure Appl. Algebra*

[36] PRESTEL, A.: *Lectures on formally real fields, Lecture Notes in Math. 1093, Springer 1984*

[37] PRESTEL, A.: *Einführung in die Mathematische Logik und Modelltheorie, Vieweg 1986*

[38] RISLER, J.J.: *Une caractérisation des variétés algébriques réelles, C.R.A.S. Paris 271 (1970), 1171-1173*

[39] SCHARLAU, W.: *Quadratic and Hermitean Forms, Grundlehren der math. Wissenschaften 270, Springer 1985*

[40] SCHMID, J.: *On the affine Bezout inequality, manuscripta math. 88 (1995), 225-232*

[41] SCHMID, J.: *On the complexity of the real Nullstellensatz in the 0-dimensional case, to appear in: J. Pure Appl. Algebra*

[42] WÖRMANN, T.: *Spurformen und reelle Nullstellen, Diplomarbeit, Dortmund 1991*

List of symbols

$\widetilde{A}$	adjoint matrix of the matrix A
$D(\Gamma)$	divisible hull of the abelian group Γ
$\mathrm{diag}(a_1, \ldots, a_n)$	diagonal matrix with entries $a_1, \ldots, a_n$
E_n	unit matrix of size $n \times n$
$\exp_2$	exponential function w.r.t. the base 2
$\mathrm{Gal}(L/K)$	group of K-automorphisms of L
$\Gamma_{\geq 0}$	non-negative elements of the ordered abelian group $(\Gamma, \leq)$
$\mathrm{Irr}(z, K)$	irreducible polynomial of z w.r.t. the field K
$\bar{K}$	algebraic closure of the field K
$\log_2$	logarithm w.r.t. the base 2
$\mathrm{P}_2(k)$	second Pythagoras number of the field k
q_A	quadratic form associated to the symmetric matrix A
$\mathrm{Quot}(R)$	field of quotients of the domain R
$\bar{R}$	integral closure of the domain R in the algebraic closure of $\mathrm{Quot}(R)$
$R^{\times}$	group of units of the ring R
$\sum R^2$	set of sums of squares of the ring R
X_K	space of orderings of the field K
$[x]$	greatest integer n such that $n \leq x$
$< a_1, \ldots, a_n >$	diagonal quadratic form
$\equiv_{\alpha}$	α-congruence
$\#A$	cardinality of the set A