Annihilating Polynomials for Quadratic Forms

Klaas-Tido Rühl

doctoral thesis – final version
version from April 11, 2010

thesis supervisor: Prof. Eva Bayer-Fluckiger

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Ecole Polytechnique Fédérale de Lausanne
Institut de Mathématiques B
Chaire de Structures Algébriques et Géométriques
Doctoral Program in Mathematics

Abstract

Let K be a field with $\mathrm{char}(K) \neq 2$. The *Witt-Grothendieck* ring $\widehat{W}(K)$ and the *Witt ring* $W(K)$ of K are both quotients of the group ring $\mathbb{Z}[\mathcal{G}(K)]$, where $\mathcal{G}(K) := {}^{K^*}\!/_{(K^*)^2}$ is the square class group of K. Since $\mathbb{Z}[\mathcal{G}(K)]$ is *integral*, the same holds for $\widehat{W}(K)$ and $W(K)$. The subject of this thesis is the study of *annihilating polynomials* for quadratic forms. More specifically, for a given quadratic form φ over K, we study polynomials $P \in \mathbb{Z}[X]$ such that $P([\varphi]) = 0$ or $P(\{\varphi\}) = 0$. Here $[\varphi] \in \widehat{W}(K)$ denotes the isometry class and $\{\varphi\} \in W(K)$ denotes the equivalence class of φ. The subset of $\mathbb{Z}[X]$ consisting of all annihilating polynomials for $[\varphi]$, respectively $\{\varphi\}$, is an ideal, which we call the *annihilating ideal* of $[\varphi]$, respectively $\{\varphi\}$.

Chapter 1 is dedicated to the algebraic foundations for the study of annihilating polynomials for quadratic forms. First we study the general structure of ideals in $\mathbb{Z}[X]$, which later on allows us to efficiently determine complete sets of generators for annihilating ideals. Then we introduce a more natural setting for the study of annihilating polynomials for quadratic forms, i.e. we *define Witt rings for groups of exponent* 2. Both $\widehat{W}(K)$ and $W(K)$ are Witt rings for the square class group $\mathcal{G}(K)$. Studying annihilating polynomials in this more general setting relieves us to a certain extent from having to distinguish between isometry and equivalence classes of quadratic forms.

In Section 1.1 we study the structure of ideals in $R[X]$, where R is a principal ideal domain. For an ideal $I \subset R[X]$ there exist sets of generators, which can be obtained in a natural way by considering the leading coefficients of elements in I. These sets of generators are called *convenient*. By discarding superfluous elements we obtain *modest* sets of generators, which under certain assumptions are minimal sets of generators for I.

Let G be a group of exponent 2. In Section 1.2 we study annihilating polynomials for elements of $\mathbb{Z}[G]$. With the help of the ring homomorphisms $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ it is possible to completely classify annihilating polynomials for elements of $\mathbb{Z}[G]$. Note that an annihilating polynomial for an element $f \in \mathbb{Z}[G]$ also annihilates the image of f in any quotient of $\mathbb{Z}[G]$. In particular, Witt rings for G are quotients of $\mathbb{Z}[G]$. In Section 1.3 we use the ring homomorphisms $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ to describe the prime spectrum of $\mathbb{Z}[G]$. The obtained results can then be employed for the characterisation of the prime spectrum of a Witt ring R for G. Section 1.4 is dedicated to proving the *structure theorems* for Witt rings. More precisely, we generalise the structure theorems for Witt rings of fields to the general setting of Witt rings for groups of exponent 2. Section 1.5 serves to summarise Chapter 1. If R is a Witt ring for G, then we use the structure theorems to determine, for an element $x \in R$, the specific shape of convenient and modest sets of generators for the annihilating ideal of x.

In Chapter 2 we study annihilating polynomials for quadratic forms over fields. More specifically, we first consider fields K, over which quadratic forms can be classified with the help of the classical invariants. Calculations involving these invariants allow us to classify annihilating ideals for isometry and equivalence classes of quadratic forms over K. Then we apply methods from the theory of generic splitting to study annihilating polynomials for excellent quadratic forms. Throughout Chapter 2 we make heavy usage of the results obtained in Chapter 1.

Let K be a field with $\mathrm{char}(K) \neq 2$. Section 2.1 constitutes an introduction to the algebraic theory of quadratic forms over fields. We introduce the Witt-Grothendieck ring $\widehat{W}(K)$ and the Witt ring $W(K)$, and we show that these are indeed Witt rings for $\mathcal{G}(K)$. In addition we adapt the structure theorems to the specific setting of quadratic forms. In Section 2.2 we introduce Brauer groups and quaternion algebras, and in Section 2.3 we define the first three cohomological invariants of quadratic forms. In particular we use quaternion algebras to define the Clifford invariant.

In Section 2.4 we begin our actual study of annihilating polynomials for quadratic forms. Henceforth it becomes necessary to distinguish between isometry and equivalence classes of quadratic forms. We start by classifying annihilating ideals for quadratic forms over fields K, for which $\widehat{W}(K)$ and $W(K)$ have a particularly simple structure. Subsequently we use calculations involving the first three cohomological invariants to determine annihilating ideals for quadratic forms over a field K such that $I^3(K) = \{0\}$, where $I(K) \subset W(K)$ is the fundamental ideal. Local fields, which are a special class of such fields, are studied in Section 2.5. By applying the Hasse-Minkowski Theorem we can then determine annihilating ideals of quadratic forms over global fields.

Section 2.6 serves as an introduction to the elementary theory of generic splitting. In particular we introduce Pfister neighbours and excellent quadratic forms, which are the subjects of study in Section 2.7. We use methods from generic splitting to study annihilating polynomials for Pfister neighbours. The obtained result can be applied inductively to obtain annihilating polynomials for excellent quadratic forms. We conclude the section by giving an alternative, elementary approach to the study of annihilating polynomials for excellent forms, which makes use of the fact that $\widehat{W}(K)$ and $W(K)$ are quotients of $\mathbb{Z}[\mathcal{G}(K)]$.

Keywords

quadratic forms, annihilating polynomials, integral rings, Witt rings

Zusammenfassung

Sei K ein Körper mit $\operatorname{char}(K) \neq 2$. Der *Witt-Grothendieck-Ring* $\widehat{W}(K)$ und der Wittring $W(K)$ von K sind beide Quotienten des Gruppenrings $\mathbb{Z}[\mathcal{G}(K)]$, wobei $\mathcal{G}(K) := {}^{K^*}\!/_{(K^*)^2}$ die Quadratklassengruppe von K sei. Da $\mathbb{Z}[\mathcal{G}(K)]$ ein ganzer Ring ist, gilt dasselbe für $\widehat{W}(K)$ und $W(K)$. Das Thema dieser Doktorarbeit ist das Studium von *Annihilierungspolynomen* für quadratische Formen. Genauer gesagt untersuchen wir für eine quadratische Form φ über K Polynome $P \in \mathbb{Z}[X]$, so dass $P([\varphi]) = 0$ oder $P(\{\varphi\}) = 0$. Mit $[\varphi] \in \widehat{W}(K)$ bezeichnen wir die Isometrieklasse und mit $\{\varphi\} \in W(K)$ die Äquivalenzklasse von φ. Die Teilmenge von $\mathbb{Z}[X]$, die aus allen Annihilierungspolynomen für $[\varphi]$, beziehungsweise $\{\varphi\}$, besteht, nennen wir *Annihilierungsideal* von $[\varphi]$, beziehungsweise $\{\varphi\}$.

Kapitel 1 ist den algebraischen Grundlagen des Studiums von Annihilierungspolynomen für quadratische Formen gewidmet. Zunächst untersuchen wir die Struktur von Idealen in $\mathbb{Z}[X]$. Dies erlaubt uns später die effiziente Bestimmung von Erzeugendensystemen für Annihilierungsideale für quadratische Formen. Anschließend führen wir Wittringe für Gruppen mit Exponent 2 ein. Diese stellen eine Verallgemeinerung von Witt-Grothendieck-Ringen und Wittringen dar. Indem wir Annihilierungspolynome in dieser allgemeineren Situation betrachten, befreien wir uns in einem gewissen Maße von der Notwendigkeit, unentwegt zwischen Isometrie- und Äquivalenzklassen von quadratischen Formen unterscheiden zu müssen.

In Abschnitt 1.1 untersuchen wir die Struktur von Idealen in $R[X]$, wobei R ein Hauptidealring sei. Ist $I \subset R[X]$ ein Ideal, so existiert für I ein Erzeugendensystem, dass man auf natürliche Weise erhält, indem man die Leitkoeffizienten von Elementen aus I betrachtet. Diese Erzeugendensysteme nennen wir *vorteilhaft*. Durch das Streichen von überflüssigen Elementen erhalten wir *genügsame* Erzeugendensysteme. Diese sind unter bestimmten Voraussetzungen minimale Erzeugendensysteme für I.

Sei G eine Gruppe mit Exponent 2. In Abschnitt 1.2 untersuchen wir Annihilierungspolynome für Elemente aus $\mathbb{Z}[G]$. Mit Hilfe der Ringhomomorphismen $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ ist es möglich, Annihilierungspolynome für Elemente aus $\mathbb{Z}[G]$ vollständig zu klassifizieren. Man beachte, dass ein Annihilierungspolynom für $f \in \mathbb{Z}[G]$ auch alle Bilder von f in Quotienten von $\mathbb{Z}[G]$ annihiliert. Insbesondere Wittringe für G sind Quotienten von $\mathbb{Z}[G]$. In Abschnitt 1.3 verwenden wir die Ringhomomorphismen $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, um das Primspektrum von $\mathbb{Z}[G]$ zu beschreiben. Die so erhaltenden Resultate können dann angewendet werden, um das Primspektrum eines Wittrings R für G zu charakterisieren. Die Strukturtheoreme für Wittringe beweisen wir in Abschnitt 1.4. Genauer gesagt verallgemeinern wir die Strukturtheoreme für Wittringe von Körpern, so dass wir sie auf Wittringe für Gruppen mit Ex-

ponent 2 anwenden können. In Abschnitt 1.5 ziehen wir das Fazit aus Kapitel 1. Wir nutzen die Strukturtheoreme, um für einen Wittring R für G und ein Element $x \in R$ die genaue Form von vorteilhaften und genügsamen Erzeugendensystemen für das Annihilierungsideals für x zu bestimmen.

In Kapitel 2 wenden wir uns dem Studium von Annihilierungspolynomen für quadratische Formen über Körpern zu. Zunächst betrachten wir Körper K, über welchen quadratische Formen mit Hilfe der klassischen Invarianten klassifiziert werden können. Berechnungen mit diesen Invarianten erlauben uns, Annihilierungsideale für Isometrie- und Äquivalenzklassen von quadratischen Formen über K zu bestimmen. Anschließend verwenden wir Methoden aus der Theorie der generischen Zerfällung, um Annihilierungspolynome für Pfisternachbarn und exzellente quadratische Formen zu untersuchen. Die Resultate aus Kapitel 1 werden in Kapitel 2 eine intensive Verwendung finden.

Sei K ein Körper mit $\mathrm{char}(K) \neq 2$. Abschnitt 2.1 dient als Einführung in die algebraische Theorie quadratischer Formen. Wir führen den Witt-Grothendieck-Ring $\widehat{W}(K)$ und den Wittring $W(K)$ von K ein, und wir zeigen, dass diese beiden Ringe tatsächliche Wittringe für $\mathcal{G}(K)$ sind. Daraufhin formulieren wir spezifische Fassungen der Strukturtheoreme für Wittringe von Körpern. In Abschnitt 2.2 führen wir Brauergruppen und Quaternionenalgebren ein, und in Abschnitt 2.3 betrachten wir die ersten drei kohomologischen Invarianten von quadratischen Formen. Insbesondere verwenden wir Quaternionenalgebren, um die Cliffordinvariante zu definieren.

In Abschnitt 2.4 beginnen wir unser eigentliches Studium von Annihilierungspolynomen für quadratische Formen. Von nun an ist es notwendig, zwischen Isometrie- und Äquivalenzklassen von quadratischen Formen zu unterscheiden. Wir beginnen mit der Klassifizierung von Annihilierungsidealen für quadratische Formen über Körpern K, für die $\widehat{W}(K)$ und $W(K)$ eine besonders einfache Struktur haben. Anschließend verwenden wir Berechnungen mit den ersten drei kohomologischen Invarianten, um Annihilierungsideale für quadratische Formen über Körpern K, für welche die dritte Potenz $I^3(K)$ des Fundamentalideals $I(K)$ verschwindet, zu bestimmen. Eine spezielle Klasse solcher Körper sind lokale Körper, welche wir in Abschnitt 2.5 betrachten. Daraufhin, indem wir das Hasse-Minkowski-Theorem anwenden, können wir Annihilierungsideale für quadratische Formen über globalen Körpern klassifizieren.

Abschnitt 2.6 dient als Einführung in die elementare Theorie der generischen Zerfällung. Insbesondere definieren wir Pfisternachbarn und exzellente quadratische Formen. Diese sind in Abschnitt 2.7 Gegenstand unserer Untersuchungen. Mit Hilfe von Methoden aus der Theorie der generischen Zerfällung ermitteln wir Annihilierungspolynome für Pfisternachbarn. Das so erhaltene Resultat könne wir daraufhin induktiv anwenden, um Annihilierungspolynome für exzellente quadratische Formen zu erhalten. Zum Abschluss des Abschnitts präsentieren wir eine alternative, elementarere Vorgehensweise, um Annihilierungspolynomen für exzellente Formen zu untersuchen. Diese Vorgehensweise bedient sich der Tatsache, dass $\widehat{W}(K)$ und $W(K)$ Quotienten von $\mathbb{Z}[\mathcal{G}(K)]$ sind,

Schlüsselworte

quadratische Formen, Annihilierungspolynome, ganze Ringe, Wittringe

Contents

Acknowledgements

First of all I would like to thank my Ph.D. supervisor, Eva Bayer-Fluckiger, for allowing me a wonderful amount of freedom and independence in the pursuit of my research, for giving me the opportunity to visit a great number of interesting conferences and workshops, for constantly endeavouring to widen my mathematical horizon, and for many helpful tips. Many thanks also for entrusting me to such an extent with responsibilities in teaching and organisational matters. I would like to thank my colleagues for creating such an accommodating work environment, and for always trying to be helpful with any question I might have had. In particular I would like to thank Mathieu Florence for his many helpful insights and creative suggestions, for being such a wonderful office mate, and for his general encouragement. Thanks also to Jean Fasel, whom I could always count on to help me with the more difficult questions concerning my subject. Many thanks to Monique Kiener for so often helping me with difficult administrational and organisational matters.

Thanks to Detlev Hoffmann for always helping me with my questions. In particular I would like to thank him for thoroughly reading some of my work and thus finding errors that everybody else had overlooked. Many thanks also to Grégory Berhuy for giving much honest and invaluable advice, and for freely and generously offering his help.

I would like to thank the Swiss National Science Foundation[1] and the Marie Curie Actions program[2] for their financial support.

Finally I would like to express my overwhelming gratitude to my family, who always supported me in my endeavours and thus made this thesis possible in the first place. To my mother for always being there, when I needed to talk about my worries and problems, and for showing an unshakeable belief in my abilities. To my father for giving me great confidence, for being an inexhaustible source of calm, and for being the most obliging person I know. To my brother for not holding back with his opinions, and for being a truly great friend.

An dieser Stelle möchte ich ins Deutsche wechseln, um auch meiner Familie meine überwältigende Dankbarkeit vermitteln zu können. Dafür, dass sie mich grundsätzlich und auf jede erdenkliche Art und Weise unterstützt hat und es mir dadurch erst ermöglicht hat, diese Arbeit zu schreiben. Meiner Mutter möchte ich dafür danken, dass Sie immer

[1] grant no. 200020-109174/1, project leader: E. Bayer-Fluckiger

[2] GTEM (Galois Theory and Explicit Methods) Research and Training Network, Marie Curie Actions, Sixth Framework Programme of the European Union, contract no. MRTN-CT-2006-035495 (partner 6: Lausanne, scientist in charge: E. Bayer-Fluckiger)

ein offenes Ohr für mich hat, wenn ich über meine Sorgen und Probleme sprechen möchte, und dass sie schon immer einen unerschütterlichen Glauben an meine Fähigkeiten hatte. Meinem Vater möchte ich für die große Zuversicht danken, die er mir gibt. Dafür, dass er eine unerschöpfliche Quelle der Gelassenheit und Ruhe ist, und dafür, dass er die hilfsbereiteste Person ist, die ich kenne. Meinem Bruder möchte ich dafür danken, dass er mir grundsätzlich die Meinung sagt und mir ein wahrhaft großartiger Freund ist.

Chapter 0

Introduction

Let K be a field of characteristic unequal to 2. Already E. Witt remarked that the Witt ring $W(K)$ of K is integral, i.e. that for every quadratic form φ over K there exists a monic polynomial $P \in \mathbb{Z}[X]$ such that P annihilates the equivalence class $\{\varphi\} \in W(K)$ of φ. This can be deduced from the fact that $W(K)$ is additively generated by the equivalence classes of 1-dimensional quadratic forms $\langle a \rangle$ with $a \in K^*$. The polynomial $X^2 - 1 \in \mathbb{Z}[X]$ annihilates these equivalence classes. Hence $W(K)$ is additively generated by integral elements and therefore integral. By employing an analogous argument we can show that the Witt-Grothendieck ring $\widehat{W}(K)$ of K is integral as well. In this thesis we study *annihilating polynomials* for elements of $\widehat{W}(K)$ and $W(K)$. In particular we study the ideal $\mathrm{Ann}_{[\varphi]} \subset \mathbb{Z}[X]$, respectively $\mathrm{Ann}_{\{\varphi\}} \subset \mathbb{Z}[X]$, consisting of all annihilating polynomials for the isometry class $[\varphi]$, respectively equivalence class $\{\varphi\}$, of a given quadratic form φ over K. It is our aim to achieve a general understanding of the structure of these *annihilating ideals*, and to develop methods that allow us to determine annihilating ideals for isometry and equivalence classes of quadratic forms over a given field.

The study of annihilating polynomials for quadratic forms falls mostly in the field of algebra. While the general study of quadratic forms has both an algebraic and a geometric aspect, it seems as though only few of the geometric properties are useful in the study of annihilating polynomials for quadratic forms. Throughout this thesis our observations about annihilating polynomials for elements of the Witt-Grothendieck ring and the Witt ring of a field are based upon results about principally two algebraic objects: ideals of the polynomial ring $\mathbb{Z}[X]$, and quotients of the group ring $\mathbb{Z}[G]$ for a group G of exponent 2. Chapter 1 is dedicated to the study of these objects.

In general it is easy to invoke an annihilating polynomial for any given quadratic form φ over a field K. If we are given the dimension n of φ, then D. Lewis observed in [Lew87], that the polynomial $P_n = (X-n)(X-n+2)\cdots(X+n)$ annihilates both the isometry and the equivalence class of φ. This already reveals information about the arithmetic structure of the Witt-Grothendieck, respectively the Witt ring, of K. In addition, if we consider the class of n-dimensional quadratic forms over arbitrary fields, the polynomial P_n is in a certain sense optimal. But there are many examples of fields K and quadratic forms φ over K such that there exist annihilating polynomials for φ of significantly lower degree than $\deg(P_n) = n+1$. Since for example, in the case where $\{\varphi\}$ is invertible in $W(K)$, annihilating polynomials for $\{\varphi\}$ can be used to calculate the inverse of $\{\varphi\}$, and since calculations involving annihilating polynomials for quadratic forms quickly become extremely complex with increasing degree, the knowledge of annihilating polynomials with low degree can be very useful. Furthermore, the more detailed our insight into the structure of annihilating polynomials for equivalence classes of quadratic forms over a given field K is, the more precise statements we can make concerning the relations that hold in $W(K)$. Accordingly we study annihilating ideals for equivalence classes of quadratic forms, which as noted above are ideals in $\mathbb{Z}[X]$.

In Section 1.1 we study the structure of ideals in the polynomial ring $R[X]$, where R is a principal ideal domain. For every ideal $I \subset R[X]$ there exist certain sets of generators, which can be obtained in a natural way by considering the leading coefficients of polynomials in I. These sets of generators are called *convenient*. We will see that convenient sets of generators have very useful properties. In particular they will help us, once we study annihilating polynomials for quadratic forms, to efficiently determine complete sets of generators for those ideals. If we are given a convenient set of generators $\mathcal{B}$ for an ideal $I \subset R[X]$, then it is possible to discard certain superfluous elements from $\mathcal{B}$. Thus we obtain a *modest* set of generators $\mathcal{M}$ for I. Our results concerning the structure of elements of $\mathcal{B}$ allow us to identify conditions, under which $\mathcal{M}$ is in fact a minimal set of generators for I.

When studying annihilating polynomials for quadratic forms over a field K, there are two rings to consider: the Witt-Grothendieck ring $\widehat{W}(K)$ of formal differences of isometry classes of quadratic forms, and the Witt ring $W(K)$ of equivalence classes of quadratic forms. Let φ be a quadratic form over K. While $W(K)$ is easy to describe as a quotient of $\widehat{W}(K)$, it is usually not a straightforward matter to obtain the annihilating ideal for the equivalence class $\{\varphi\}$ from the annihilating ideal for the isometry class $[\varphi]$. In addition it might become necessary to separately prove results about annihilating polynomials for each of the two rings. Therefore we consider a more natural setting for the study of annihilating polynomials for quadratic forms. Both the Witt-Grothendieck ring and the Witt ring are quotients of the group ring $\mathbb{Z}[\mathcal{G}(K)]$, where $\mathcal{G}(K)$ is the square class group of K. In [KRW72] M. Knebusch, A. Rosenberg and R. Ware studied certain quotients of the group ring $\mathbb{Z}[G]$ for a group G of prime exponent. They identified conditions on an ideal $J \subset \mathbb{Z}[G]$, under which the quotient $\mathbb{Z}[G]/_J$ has properties similar to those of $\widehat{W}(K)$ and $W(K)$. Those quotients are called *Witt rings for G*. For a field K both $\widehat{W}(K)$ and $W(K)$ are Witt rings for the square class group $\mathcal{G}(K)$. By studying annihilating polynomials for elements of Witt rings for groups of exponent 2, we thus obtain results that can be applied to elements of both the Witt-Grothendieck ring and the Witt ring of a field.

A natural approach to the study of annihilating polynomials for elements of a Witt ring for a group G of exponent 2 is to first study annihilating polynomials for elements of $\mathbb{Z}[G]$. In [Hur89] J. Hurrelbrink showed how to construct annihilating polynomials for elements of $\mathbb{Z}[G]$ by considering the ring homomorphisms $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. More specifically, for any $f \in \mathbb{Z}[G]$ the unique product of linear factors in $\mathbb{Z}[X]$, whose roots are exactly the values $\chi(f) \in \mathbb{Z}$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, generates the annihilating ideal of f. In Section 1.2 we study Hurrelbrink's approach. We generalise the definition of Pfister forms, an exceedingly important class of quadratic forms, to the setting of group rings for groups of exponent 2. In this setting it is possible to use annihilating polynomials to characterise Pfister elements. It will become apparent in Chapter 2 that this does not hold for Pfister quadratic forms.

To be able to comprehensively study annihilating polynomials for elements of a Witt ring $R = {}^{Z[G]}/_{J}$ for a group G of exponent 2, it is necessary that we establish a set of results, which in the setting of quadratic forms are known as the structure theorems. Indeed it is possible to generalise all of these theorems to the more general setting of Witt rings for groups of exponent 2. To this end we study the spectrum of $\mathbb{Z}[G]$ in Section 1.3. We again make use of the ring homomorphisms $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, this time to give a complete list of prime ideals of $\mathbb{Z}[G]$. Since R is a quotient of $\mathbb{Z}[G]$, we can use this list and the assumptions on the ideal J to give a complete and easy to describe list of prime ideals of R. In Section 1.4 we employ our knowledge about the spectrum of R and our previous observations about annihilating polynomials for elements in $\mathbb{Z}[G]$ to formulate and prove the structure theorems for R. These are the crucial ingredients that, in Section 1.5, allow us to adapt our observations about convenient and modest sets of generators for ideals in $\mathbb{Z}[X]$ to the setting of annihilating ideals for elements of the Witt ring R. The specific shape of those annihilating ideals forms the basis for our study of annihilating ideals for quadratic forms in the following chapter. Once again the ring homomorphisms $\operatorname{Hom}(R, \mathbb{Z})$ play a crucial role. Unlike in the setting of group rings, they do not immediately provide us with annihilating polynomials. But for an element $x \in R$ the unique product of linear factors $P_x \in \mathbb{Z}[X]$, whose roots are exactly the values $\chi(x) \in \mathbb{Z}$ for all $\chi \in \operatorname{Hom}(R, \mathbb{Z})$, is the monic greatest common divisor of all annihilating polynomials for x. We call P_x the *signature polynomial.*

Chapter 2 is dedicated to the study of annihilating polynomials for quadratic forms. More specifically, we study annihilating polynomials for isometry and equivalence classes of quadratic forms over fields. The insights about annihilating polynomials for elements of Witt rings for groups of exponent 2, that we have gathered in Chapter 1 and in particular in Section 1.5, form a useful theoretical basis for our approach to the setting of quadratic forms. Knowing the structure of convenient and modest sets of generators allows us to efficiently identify complete and, under certain conditions, even minimal sets of generators for annihilating ideals. Furthermore, our observations about the connection between the ring homomorphisms $\operatorname{Hom}(\widehat{W}(K), \mathbb{Z})$, respectively $\operatorname{Hom}(W(K), \mathbb{Z})$, and the greatest common divisor of all elements of $\operatorname{Ann}_{[\varphi]}$, respectively $\operatorname{Ann}_{\{\varphi\}}$, for a given quadratic form φ over K, provide us with a natural approach to showing that, for a given class of quadratic forms over arbitrary fields, certain annihilating polynomials are optimal.

The first three sections of Chapter 2 serve as a comprehensive introduction to the algebraic theory of quadratic forms. We leave out most of the proofs but instead give exact references for the interested reader. In Section 2.1 we define quadratic spaces and give an overview over the relations between quadratic spaces, symmetric matrices and quadratic forms. Each of these objects highlights different algebraic and geometric aspects of quadratic forms. We continue by considering the algebraic properties of quadratic forms, which form the basis for the definition of the Witt-Grothendieck ring $\widehat{W}(K)$ and the Witt ring $W(K)$

of a field K. After showing that these two rings are indeed Witt rings for the square class group $\mathcal{G}(K)$ of K, we can then translate the structure theorems for Witt rings for groups to the specific setting of Witt rings of fields. We include in Section 2.1 a short introduction to Pfister forms. As was already hinted at previously and will become apparent in the following sections, this class of quadratic forms represents an exceedingly useful tool in basically all fields of study concerning quadratic forms.

Section 2.2 constitutes an introduction to Brauer groups. In this context we also cover quaternion algebras, whose study is closely related to the study of quadratic forms. In particular we will use quaternion algebras in the following section to construct the Hasse invariant and the Clifford invariant. More generally, in Section 2.3 we study the first three cohomological invariants of quadratic forms. These are the dimension index, the discriminant, and the Clifford invariant. Calculations concerning the dimension index and the discriminant are usually not very challenging. But we need a number of formulas which facilitate calculations involving the Clifford invariant.

At the beginning of Section 2.4 we establish the exact relation between $\mathrm{Hom}(\widehat{W}(K), \mathbb{Z})$ and $\mathrm{Hom}(W(K), \mathbb{Z})$. Thus, for a quadratic form φ over K, we can describe the relation between the signature polynomials $P_{[\varphi]}$ and $P_{\{\varphi\}}$. We continue by considering fields K for which the third power of the fundamental $I(K)$ vanishes. Over such a field K quadratic forms can be classified with the help of the dimension index, the discriminant and the Clifford invariant. We use the first three cohomological invariants to determine annihilating ideals for isometry and equivalence classes of quadratic forms over K. These observations then serve to study polynomials, which annihilate the whole Witt ring $W(K)$. In addition we can use the gathered knowledge to easily calculate the inverses of units in $W(K)$. Local fields, which are covered in Section 2.5, are a special example of fields, for which the third power of $I(K)$ vanishes. We specialise our observations from the previous section to the specific setting of local fields. Then we use the Hasse-Minkowski Theorem to classify annihilating ideals for quadratic forms over global fields.

In Section 2.6 we give an introduction to the elementary theory of generic splitting of quadratic forms. This theory was introduced by M. Knebusch in his three articles [Kne73], [Kne76] and [Kne77] and has since proven to be a powerful tool for the study of quadratic forms. We define generic splitting towers and quote some of the most important results on generic splitting. In particular we introduce Pfister neighbours and excellent quadratic forms, which will be the subjects of study in the following section. These two classes of quadratic forms are of particular significance to us, since they have very useful properties and can be characterised in the context of generic splitting. In Section 2.7 we use these characterisations and methods from generic splitting to construct specific annihilating polynomials for Pfister neighbours and excellent forms. In the case of excellent forms, it is also possible to obtain annihilating polynomials through more elementary methods. We give another characterisation of excellent forms which invokes certain elements in $\mathbb{Z}[\mathcal{G}(K)]$. An annihilating polynomial for one of these elements $f \in \mathbb{Z}[\mathcal{G}(K)]$ also annihilates the excellent form associated to f. In particular the polynomials obtained in this way are the same as the ones, that we have obtained through methods from generic splitting.

Chapter 1

Witt Rings for Groups of Exponent 2

In this chapter we construct the theoretical basis for the study of annihilating polynomials for quadratic forms in Chapter 2. The set of annihilating polynomials for the isometry, respectively equivalence class, of a given quadratic form over a field K forms an ideal in $\mathbb{Z}[X]$. In Section 1.1 we undertake a general study of ideals in $\mathbb{Z}[X]$. For an ideal $I \subset \mathbb{Z}[X]$ we introduce canonical sets of generators, which can be obtained by considering the leading coefficients of elements in I. Those sets of generators are called *convenient*. By disposing of certain elements we obtain from a convenient set of generators $\mathcal{B}$ for I a *modest* set of generators $\mathcal{M}$. Under certain conditions on the coefficients of the elements of $\mathcal{B}$, the set of generators $\mathcal{M}$ of I is minimal.

The Witt-Grothendieck ring and the Witt ring of a field K are quotients of $\mathbb{Z}[\mathcal{G}(K)]$, where $\mathcal{G}(K)$ is the square class group of K. Accordingly it is possible to obtain annihilating polynomials for quadratic forms, by considering appropriate elements in $\mathbb{Z}[\mathcal{G}(K)]$. In Section 1.2 we study annihilating polynomials for elements of $\mathbb{Z}[G]$, where G is a group of exponent 2. In this case annihilating polynomials can be obtained in a canonical way by considering the ring homomorphisms $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$.

In Section 1.3 we introduce Witt rings for groups G of exponent 2. These rings have properties that mimic the properties of Witt rings of fields. Both the Witt-Grothendieck ring and the Witt ring of a field K are Witt rings for the square class group of K. In order to establish the set of results, which in the context of quadratic forms is known as the structure theorems, we first study the prime spectrum of Witt rings for groups of exponent 2. If R is such a ring, then the prime ideals of R can be easily described by using the ring homomorphisms $\mathrm{Hom}(R, \mathbb{Z})$. In Section 1.4 we apply this result together with our observations about annihilating polynomials for elements of $\mathbb{Z}[G]$ to prove the structure theorems for Witt rings. The results of the previous sections will then be used in Section 1.5 to translate our results concerning ideals in $\mathbb{Z}[X]$ to the specific setting of annihilating ideals for elements of Witt rings for groups of exponent 2.

1.1 Ideals in polynomial rings over principal ideal domains

We denote by $\mathbb{N}$ the natural numbers $\{1, 2, 3, \dots\}$. In those cases where we need to include 0 we use the notation $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Throughout this section R will denote a principal ideal domain. The purpose of this section is to prove a result by G. Szekeres about generators for an ideal $I \subset R[X]$. In [Sze52] Szekeres constructs for a given $I \subset R[X]$ a certain canonical set of generators. If we impose a number of conditions on the coefficients this set of generators is uniquely determined by I. In his article Szekeres gives the proofs only for the case $R = \mathbb{Z}$, and in this case it is easy to describe the conditions on the coefficients by simple inequalities invoking the usual ordering of $\mathbb{Z}$. In the general case the conditions on the coefficients become significantly more complex to formulate. This is done in detail by L. Rédei in [Réd67]. In this section we first follow Szerekes' approach to introduce these canonical sets of generators, which we call *convenient*. We then eliminate certain elements from a *convenient* set of generators to obtain a so-called *modest* set of generators. In addition we identify conditions on the coefficients of the generators under which a *modest* set of generators is minimal. We conclude by using the specific shape of convenient sets of generators for certain ideals $I \subset R[X]$ to describe the R-module structure of $R[X]/I$.

For the rest of this section $I \subset R[X]$, $I \neq (0)$, denotes an arbitrary ideal.

1.1.1 Definition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal. The polynomial*

$$Q_I \ := \ \gcd(I),$$

where $\gcd(I)$ *denotes any greatest common divisor of all elements of I, is called an* embracing polynomial *of I.*

1.1.2 Remark. The name "embracing polynomial" stems from the fact that we have $I \subset (Q_I)$, and (Q_I) is the unique minimal principal ideal containing I. In this sense the principal ideal generated by Q_I "embraces" the ideal I. Moreover I is principal if and only if $I = (Q_I)$.

Clearly in general the embracing polynomial of an ideal $(0) \neq I \subset R[X]$ is only unique up to multiplication with elements in R^*. But in the case where the leading coefficient of Q_I is a unit, we can assume without loss of generality that Q_I is monic, i.e. that Q_I has leading coefficient 1. Therefore in this case Q_I is uniquely determined. △

For $P \in R[X]$ consider the ideal

$$(I : (P)) \ = \ \{T \in R[X] \mid TP \in I\}.$$

Obviously $I \subset (I : (P))$ for all $P \in R[X]$.

1.1.3 Definition. *For any non-zero ideal $I \subset R[X]$ and any $P \in R[X]$ we call the elements of $(I : (P))$* complements *of P with respect to I.*

1.1.4 Observation. Denote by K the quotient field of R. Since R is a principal ideal domain, $R[X]$ is Noetherian. Suppose that $P_1, \dots, P_n \in R[X]$ generate I, $n \in \mathbb{N}$. Since $K[X]$

is a principal ideal domain there exist $\lambda_1, \dots, \lambda_n \in K[X]$ such that $Q_I = \lambda_1 P_1 + \cdots + \lambda_n P_n$. By multiplying with an appropriate element of R we obtain $\lambda'_1, \dots, \lambda'_n \in R[X]$ and an $m \in R$, $m \neq 0$, such that

$$mQ_I \;=\; \lambda'_1 P_1 + \cdots + \lambda'_n P_n \;\in\; I.$$

In other words a non-zero scalar multiple of Q_I must lie in I or equivalently $(I : (Q_I))$ contains a non-zero element of R. △

For $P = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ with $a_n \neq 0$ denote by $\mathrm{lc}(P) := a_n$ the *leading coefficient* of P. Set

$$C_d^{(I)} \;:=\; \{a \in R \mid a = \mathrm{lc}(P),\, P \in (I : (Q_I)),\, \deg(P) = d\} \;\cup\; \{0\}$$

for $d \in \mathbb{N}_0$. It is clear that $C_d^{(I)} \subset R$ is an ideal and that $C_d^{(I)} \subset C_{d+1}^{(I)}$ for all $d \in \mathbb{N}_0$.

1.1.5 Definition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal. A complement $P \in (I : (Q_I))$, $P \neq 0$, with $d = \deg(P)$ is called* minimal *if the leading coefficient* $\mathrm{lc}(P)$ *generates $C_d^{(I)}$.*

For $d \in \mathbb{N}_0$ let $m_d \in R$ such that $C_d^{(I)} = (m_d)$. Observation 1.1.4 implies that $m_0 \neq 0$. Then $C_d^{(I)} \subset C_{d+1}^{(I)}$ implies that $m_{d+1} \neq 0$ and that m_{d+1} divides m_d for $d \in \mathbb{N}_0$. Choose $P_d \in (I : (Q_I))$ such that $\deg(P_d) = d$ and $\mathrm{lc}(P_d) = m_d$. Set $I_d := (P_0 Q_I, \dots, P_d Q_I)$.

1.1.6 Proposition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal, and for $d \in \mathbb{N}_0$ let $P_d \in (I : (Q_I))$ be minimal with* $\deg(P_d) = d$. *Then, for any $P \in I$ there exist unique $b_d \in R$ such that*

$$P \;=\; \left(\sum_{d \in \mathbb{N}_0} b_d P_d \right) Q_I.$$

Proof. For $d \in \mathbb{N}_0$ let $\mathrm{lc}(P_d) = m_d$. We can write $P = TQ_I$ with $T \in (I : (Q_I))$. Let $r = \deg(T)$. We proceed by induction on r.

If $r = 0$, then $T = c_0 \in C_0^{(I)}$ and $P_0 = m_0$. There exists a $b_0 \in R$ such that $c_0 = b_0 m_0$ and $T = b_0 P_0$.

Now assume that $r > 0$. By definition of $C_r^{(I)}$ we have $\mathrm{lc}(T) \in C_r^{(I)}$. This implies that there exists a $b_r \in R$ such that $T - b_r P_r \in (I : (Q_I))$ has a strictly smaller degree than r. Since $\mathrm{lc}(P) = b_r m_r$ and as R is a unique factorisation domain it follows that b_r is uniquely determined by P, P_r and Q_I. By the induction hypothesis there exist unique $b_0, \dots, b_{r-1} \in R$ such that $T - b_r P_r = b_0 P_0 + \cdots + b_{r-1} P_{r-1}$ or equivalently $T = b_0 P_0 + \cdots + b_r P_r$. □

Since $R[X]$ is Noetherian, there exists a minimal $s \in \mathbb{N}_0$ such that $I_d = I_s$ for all $d \geq s$. By the previous proposition we must have $I = I_s$. In particular s is independent from the choices of the m_d and P_d. Set $s(I) := s$.

1.1.7 Proposition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal. If $P = a_d X^d + \cdots + a_1 X + a_0 \in (I : (Q_I))$ is a complement of Q_I with* $\deg(P) = d$, *then $a_0, \dots, a_d$ lie in $C_d^{(I)}$.*

Proof. We adopt the notation from the paragraph preceding Proposition 1.1.6 and proceed by induction on d.

If $d = 0$, then we have $I_0 = (P_0 Q_I) = C_0^{(I)}(Q_I)$. Thus the claim is trivial in this case.

Now let $d > 0$. We have to distinguish between the cases $P = P_d$ and $P \neq P_d$. Assume first that $P = P_d$. Then there exists a $b \in R$ such that $m_{d-1} = bm_d$, and $T := bP_d - XP_{d-1} \in (I : (Q_I))$ has a degree strictly smaller than d. By induction the coefficients of T and P_{d-1} lie in $C_{d-1}^{(I)}$. Hence the coefficients of bP_d lie in $C_{d-1}^{(I)} = (bm_d)$. Since R is a unique factorisation domain the coefficients of P_d must lie in $(m_d) = C_d^{(I)}$.

Finally assume that $P \neq P_d$. By definition of m_d there exists a $b \in R$ such that $T := P - bP_d \in (I : (Q_I))$ has degree strictly smaller than d. By the above case the coefficients of bP_d lie in $C_d^{(I)}$, and by induction the coefficients of T lie in $C_{d-1}^{(I)} \subset C_d^{(I)}$. Therefore the coefficients of P also lie in $C_d^{(I)}$. □

The previous proposition can also be deduced by using results from [Sze52]. But the proof given here is significantly less technical while also working in the general case.

1.1.8 Corollary. *If $I \subset R[X]$ is a non-zero ideal, and if $P \in (I : (Q_I))$ is a minimal complement with leading coefficient m, then there exists a monic $Q \in R[X]$ such that $P = mQ$.*

1.1.9 Corollary. *If $I \subset R[X]$, $I \neq (0)$, is an ideal, then $(I : (Q_I))$ contains both an element of R and a monic polynomial.*

Proof. The fact that $(I : (Q_I))$ contains an element of R follows from Observation 1.1.4.

We use the notation introduced in the paragraph before Proposition 1.1.7 to show that $(I : (Q_I))$ contains a monic polynomial. Since m_s for $s = s(I)$ divides $m_0, \dots, m_{s-1}$ it follows from Proposition 1.1.7 that m_s divides all elements of $(I : (Q_I))$, i.e. m_s divides the embracing polynomial $Q_{(I:(Q_I))} = 1$. This implies that P_s is monic. □

We can now summarise our observations as follows.

1.1.10 Theorem. *Let $I \subset R[X]$, $I \neq (0)$, be an arbitrary ideal, and let $Q_I = \gcd(I)$. Then there exist a unique $s \in \mathbb{N}_0$, monic polynomials $Q_0, \dots, Q_s \in R[X]$, and elements $0 \neq m_0, \dots, m_s \in R$ such that*

(a) $\deg(Q_d) = d$ for $d = 0, \dots, s$, and $Q_0 = 1$,

(b) $m_d | m_{d-1}$ for $d = 1, \dots, s$, and $m_{s-1} \notin R^*$, $m_s = 1$,

(c) $m_d Q_d \in (I : (Q_I))$ is a minimal complement for $d = 0, \dots, s$, and

(d) $(I : (Q_I)) = (m_0, m_1 Q_1, \dots, m_{s-1} Q_{s-1}, Q_s)$.

In particular

$$I = (m_0 Q_I, m_1 Q_1 Q_I, \dots, m_{s-1} Q_{s-1} Q_I, Q_s Q_I).$$

1.1.11 Definition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal. Then a full set of generators for I as given in Theorem 1.1.10 is called* convenient.

1.1.12 Remark. Recall that two elements $a, b \in R$ are *associated* if there exists a $c \in R^*$ such that $a = bc$. This defines an equivalence relation on the elements of R. Let $\mathfrak{R}$ denote a system of representatives for the classes of associated elements of R. Obviously $0 \in \mathfrak{R}$, and without loss of generality $1 \in \mathfrak{R}$. Now, if we start by choosing representatives for the classes of elements associated to prime elements, then we can choose $\mathfrak{R}$ such that $\mathfrak{R} \setminus \{0\}$ constitutes a free commutative semi-group. We furthermore choose for every $a \in \mathfrak{R}$ a system of representatives $\mathfrak{R}(a)$ for the classes of associated elements of $R/(a)$ such that $0 \in \mathfrak{R}(a)$. In particular $\mathfrak{R}(1) = \{0\}$.

Choose an $s \in \mathbb{N}$, elements $a_1, \ldots, a_s \in \mathfrak{R}$ with $a_s \neq 1$, and elements $b_{1,d}, \ldots, b_{d,d} \in \mathfrak{R}(a_d)$ for $d = 1, \ldots, s$. Then from

$$P_0 := a_1 \cdots a_s \quad \text{and} \quad a_d P_d := X P_{d-1} + \sum_{i=1}^{d} b_{i,d} P_{i-1},\ d = 1, \ldots, s,$$

we obtain polynomials $P_0, \ldots, P_s \in R[X]$. Set

$$I \ = \ (P_0 Q_I, \ldots, P_s Q_I).$$

Szekeres's Theorem [Réd67, Theorem 285, §120] states that every ideal $I \subset R[X]$ can be obtained like this, and furthermore I uniquely determines s, the $a_d \in \mathfrak{R}$, and the $b_{i,d} \in \mathfrak{R}(a_d)$ for $i = 1, \ldots, d$ and $d = 1, \ldots, s$.

The proof of [Réd67, Theorem 285, §120] (also compare [Sze52, (11)] and the subsequent observations) yields that $s = s(I)$. Furthermore with $m_i = a_{i+1} \cdots a_s$ we have $P_i = m_i Q_i$ with a monic $Q_i \in R[X]$ for $i = 0, \ldots, s$. Thus we obtain a convenient set of generators, i.e.

$$I \ = \ (m_0 Q_I, m_1 Q_1 Q_I, \ldots, m_{s-1} Q_{s-1} Q_I, Q_s Q_I),$$

exactly as described in Theorem 1.1.10. △

Minimal modest sets of generators

For certain ideals $I \in R[X]$ it is possible to obtain a minimal set of generators from any convenient set of generators for I. More precisely this is achieved by discarding a number of superfluous elements from a given convenient set of generators. The degrees of the remaining polynomials form a sequence of natural numbers which is independent from the choice of the convenient set of generators.

Let $I \subset R[X]$ be an arbitrary ideal, and let $\mathcal{B} = \{m_d Q_d Q_i \mid d = 0, \ldots, s\}$ be a convenient set of generators for I, $s = s(I)$. We define a set of indices $N(I) \subset \{0, \ldots, s\}$ by

$$d \in N(I) \quad \Longleftrightarrow \quad d = 0 \quad \text{or} \quad (m_d) \neq (m_{d-1}).$$

It follows immediately from the definition of a minimal complement that $N(I)$ is independent from the choice of $\mathcal{B}$.

Let $N(I) = \{d_0, \ldots, d_r\}$ with $d_{i-1} < d_i$ for $i = 1, \ldots, r$. Set $r(I) := r$. Consider an arbitrary $d \in \{0, \ldots, s\}$, and let $i \in \{0, \ldots, r\}$ be maximal with $d_i \leq d$. Then, by definition of $N(I)$, we have $(m_{d_i}) = (m_d)$. Set $\widetilde{Q}_d := X^{d-d_i} Q_{d_i}$. It is clear that $m_d \widetilde{Q}_d Q_I$ is minimal in

I, and thus we obtain another convenient set of generators $\mathcal{B}' = \left\{ m_d\widetilde{Q}_dQ_I \mid d = 0.\dots, s \right\}$. It follows that

$$I \;=\; (m_0Q_I,\; m_{d_1}Q_{d_1}Q_I,\; \dots,\; m_{d_{r-1}}Q_{d_{r-1}}Q_I,\; Q_sQ_i).$$

For $i = 0, \dots, r$ set $P_i := Q_{d_i}$ and $n_i = m_{d_i}$. It follows that

$$\mathcal{M} \;:=\; \{n_iP_iQ_I \mid i = 0, \dots, r(I)\}$$

is a set of generators for I.

1.1.13 Proposition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal, and let Q_I be an embracing polynomial of I. Then there exist a unique $r \in \mathbb{N}_0$, monic polynomials $P_0, \dots, P_r \in R[X]$, and elements $0 \neq n_0, \dots, n_r \in R$ such that*

(a) $\deg(P_{i-1}) < \deg(P_i)$ for $i = 1, \dots, r$, and $Q_0 = 1$,

(b) $n_i|n_{i-1}$ and $(n_i) \neq (n_{i-1})$ for $i = 1, \dots, r$, and $n_r = 1$,

(c) $n_iP_i \in (I : (Q_I))$ is a minimal complement for $i = 0, \dots, r$, and

(d) $I = (n_0Q_I, n_1P_1Q_I, \dots, n_{r-1}P_{r-1}Q_I, P_rQ_I)$.

1.1.14 Definition. *Let $I \subset R[X]$ be an ideal. A full set of generators for I that satisfies the conditions in the previous proposition is called* modest.

We want to investigate the question under which conditions a modest set of generators for an ideal $I \subset R[X]$ is minimal.

1.1.15 Lemma. *Consider a sequence of polynomials $\{P_d \in R[X] \mid d \in \mathbb{N}_0, \deg(P_d) = d\}$. Set $m_d := \mathrm{lc}(P_d)$ and $I = (P_d \mid d \in \mathbb{N}_0)$. Assume that $\gcd(I) = 1$. The polynomials $P_0, P_1, P_2, \dots$ are minimal in $I = (I : (Q_I))$ if and only if for all $d \in \mathbb{N}$ the following conditions are satisfied:*

(a) $m_d|m_{d-1}$,

(b) $P_d = m_dQ_d$ for some monic $Q_d \in \mathbb{Z}[X]$, and

(c) $XP_{d-1} = m_{d-1}Q_d + \sum_{i=0}^{d-1} b_i^{(d)}P_i$ for some $b_i^{(d)} \in R$.

Proof. Note that the assumption that $\deg(P_d) = d$ for all $d \in \mathbb{N}_0$ implies that $P_d \neq 0$.

Assume that the polynomials $P_0, P_1, P_2, \dots$ are minimal in I. Then we have $C_d^{(I)} = (m_d)$ for $d \in \mathbb{N}_0$. Hence by our observations regarding the $C_d^{(I)}$ point (a) follows. We obtain point (b) as a consequence of Proposition 1.1.7. By Proposition 1.1.6 there exist unique $b_0^{(d)}, \dots, b_d^{(d)} \in \mathbb{Z}$ with $XP_{d-1} = \sum_{i=0}^{d} b_i^{(d)}P_d$. Since $\mathrm{lc}(XP_{d-1}) = m_{d-1}$ it follows that $b_d^{(d)}m_dQ_d = m_{d-1}Q_d$. Hence condition (c) is satisfied as well.

Now assume that $P_0, P_1, P_2, \dots$ satisfy the points (a), (b) and (c). Denote by M the set of polynomials $f \in I$ that can be written as

$$f \;=\; \sum_{j\in\mathbb{N}_0} a_jP_j, \quad a_j \in R. \tag{1.1}$$

It is clear that for $f, g \in M$ we have $f + g \in M$, and if $z \in R$ we have $zf \in M$. Furthermore by point (c)

$$Xf \;=\; \sum_{j\in\mathbb{N}_0} a_j X P_j \;=\; \sum_{j\in\mathbb{N}_0} a_j \sum_{i=0}^{j+1} b_i^{(j+1)} P_i \;=\; \sum_{i\in\mathbb{N}_0} \left(\sum_{j=i-1}^{\infty} a_j b_i^{(j+1)} \right) P_i$$

with $a_{-1} := b_0^{(0)} := 0$ and $b_d^{(d)} := \frac{m_{d-1}}{m_d}$ for $d \in \mathbb{N}$, which shows that $Xf \in M$. It follows that $M \subset I$ is an ideal in R. Since all the generators P_d of I lie in M we must have $M = I$. Thus every elements of I can be written as in (1.1).

Let $f \in I$ be an arbitrary element of degree $d \in \mathbb{N}_0$. Write

$$f \;=\; \sum_{j=0}^{d} a_j P_j.$$

Then we see that $\mathrm{lc}(f) = a_d m_d$, i.e. the leading coefficient of f is divisible by the leading coefficient of P_d. It follows that $C_d^{(I)} = (m_d)$. In other words, P_d is minimal in I. □

1.1.16 Example. Consider the set of polynomials

$$\mathcal{B} \;:=\; \{4, 2X, X^2 + 2\} \;\subset\; \mathbb{Z}[X],$$

and let I be the ideal generated by $\mathcal{B}$. The elements of $\mathcal{B}$ clearly satisfy the conditions (a) and (b) from the previous lemma. If we set $m_0 = 4$, $m_1 = 2$, $m_2 = 1$, and $Q_0 = 1$, $Q_1 = X$, $Q_2 = X^2 + 2$, then we furthermore have $X \cdot (m_0 Q_0) = m_0 Q_1$ and $X \cdot (m_1 Q_1) = m_1 Q_2 + (-1) \cdot (m_0 Q_0)$, which shows that the polynomials 4, $2X$ and $X^2 + 2$ also satisfy condition (c). Thus $\mathcal{B}$ is a convenient set of generators for I. We immediately see that $\mathcal{B}$ is even modest. But we have $m_0 Q_0 = 2 \cdot (m_2 Q_2) - X \cdot (m_1 Q_1)$. Thus $\mathcal{B}$ is not minimal. △

1.1.17 Proposition. *Consider an ideal $I \subset R[X]$. Let $\mathcal{B} = \{m_d Q_d Q_I \mid d = 0, \dots, s\}$ be a convenient set of generators for I, let $\mathcal{M} \subset \mathcal{B}$ be the associated modest set of generators, and let $N(I)$ be the set of all indices $d \in \{0, \dots, s\}$ such that $m_d Q_d Q_I \in \mathcal{M}$. For $d = 1, \dots, s$ write*

$$X(m_{d-1} Q_{d-1}) \;=\; m_{d-1} Q_d + \sum_{i=0}^{d-1} b_i^{(d)} m_i Q_i, \qquad b_i^{(d)} \in R. \tag{1.2}$$

If for all $k \in N(I)$ such that $k \le s - 2$ there exists an element $c_k \in R \setminus \{0\}$ with $c_k \notin R^*$ such that c_k divides $b_k^{(d)}$ for all $d = k + 2, \dots, s$, and such that c_k divides $\frac{m_{k-1}}{m_k}$ in the case where $k > 0$, then $\mathcal{M}$ is a minimal set of generators for I.

Proof. The proof is trivial if $s < 2$. So throughout the proof we assume that $s \ge 2$. Furthermore we can without loss of generality assume that $Q_I = 1$.

For $j \in \mathbb{N}$ set $Q_{s+j} := X^j Q_s$, and complete $\mathcal{B}$ to the set of generators $\overline{\mathcal{B}} := \mathcal{B} \cup \{Q_{j+s} \mid j \in \mathbb{N}\}$. We note that, if we set $b_i^{(d)} := 0$ for all $d > s$ and $i = 0, \dots, d-1$, equality (1.2) and the assumptions below the equality hold for all $d \in \mathbb{N}$.

For any $k \in N(I)$ set

$$\mathcal{C} \;:=\; (\overline{\mathcal{B}} \setminus \{m_k Q_k\}) \cup \{c_k m_k Q_k\},$$

and let $J \subset R[X]$ be the ideal generated by $\mathcal{C}$. Since $m_k \notin (c_k m_k)$ it follows that $\mathcal{C} \neq \overline{\mathcal{B}}$. We want to show that the polynomials in $\mathcal{C}$ are minimal in J. For $d \in \mathbb{N}_0$ denote the leading coefficient of the unique polynomial in $\mathcal{C}$ of degree d with a_d.

We have $a_k = c_k m_k$. If we suppose that $k > 0$, then c_k divides $\frac{m_{k-1}}{m_k}$, and it follows that a_k divides $a_{k-1} = m_{k-1}$. Hence in this case condition (a) from Lemma 1.1.15 is satisfied. If $k = 0$, then condition (a) is trivially satisfied. Clearly condition (b) is satisfied for arbitrary k as well. Furthermore by the construction of $\overline{\mathcal{B}}$ condition (c) is satisfied for all $d \in \mathbb{N}$ with $d \leq k$. Consider the case $d = k+1$. We obtain

$$\begin{aligned} X(a_k Q_k) &= c_k(X m_k Q_k) = c_k \left(m_k Q_{k+1} + \sum_{i=0}^{k} b_i^{(k+1)} m_i Q_i \right) \\ &= a_k Q_{k+1} + b_k^{(k+1)} a_k Q_k + \sum_{i=1}^{k-1} (c_k b_i^{(k+1)}) a_i Q_i, \end{aligned}$$

which shows that condition (c) is also satisfied in this case. Finally, consider the case $d > k+1$. Since c_k divides $b_k^{(d)}$, i.e. $b_k^{(d)} = b' c_k$ for some $b' \in R$, we obtain $b_k^{(d)} m_k = b' a_k$ and hence

$$\begin{aligned} X(a_{d-1} Q_{d-1}) &= X(m_{d-1} Q_{d-1}) = m_{d-1} Q_d + \sum_{i=0}^{d-1} b_i^{(d)} m_i Q_i \\ &= a_{d-1} Q_d + \left(\sum_{i=0}^{k-1} b_i^{(d)} a_i Q_i \right) + b' a_k Q_k + \left(\sum_{i=k+1}^{d-1} b_i^{(d)} a_i Q_i \right). \end{aligned}$$

Thus condition (c) holds for all $d \in \mathbb{N}$.

We conclude that the elements of $\mathcal{C}$ are minimal in J. In particular we have $m_k Q_k \notin J$ since $(m_k) \neq (m_{k-1})$ for $k > 0$ and $(m_0) \neq (c_0 m_0)$. Thus $\mathcal{B} \setminus \{m_k Q_k\}$ does not generate I. This holds if we exclude any element of $\mathcal{M}$ from $\mathcal{B}$. It follows that $\mathcal{M}$ is a minimal set of generators for I. □

The following corollary is specifically tailored to match our results about annihilating ideals for elements of Witt rings in Section 2.4 and Section 2.5.

1.1.18 Corollary. *Let $I \subset R[X]$ be an ideal. If $\mathcal{B} = \{m_d Q_d Q_I \mid d = 0, \ldots, s\}$ is a convenient set of generators with $Q_{d-1} | Q_d$ for $d = 1, \ldots, s$, then the associated modest set of generators $\mathcal{M} \subset \mathcal{B}$ is a minimal set of generators for I.*

Proof. For $d = 1, \ldots, s$ we have $Q_d = Q_{d-1} \cdot (X - a_d)$ for some $a_d \in R$. Therefore

$$X m_{d-1} Q_{d-1} = m_{d-1} Q_d + a_d m_{d-1} Q_{d-1}.$$

In particular we have $b_k^{(d)} = 0$ for all $k \in N(I)$, $k \leq s-2$, and for all $d = k+2, \ldots, s$. If $k = 0$, then any element of $R \setminus \{0\}$ divides $b_0^{(2)}, \ldots, b_0^{(s)}$. If $k > 1$, then $\frac{m_{k-1}}{m_k} | b_k^{(d)}$ for all $d = k+2, \ldots, s$. Therefore we can apply Proposition 1.1.17. □

The R-module structure of quotients of $R[X]$

Since, in what follows, we will often deal with quotient groups we agree on the following convention: For any group G, any normal subgroup $N \subset G$, and any $x \in {}^{G}\!/_{N}$ by definition there exists a $g \in G$ such that $x = gN$. We use the notation $\overline{g} := gN$. In particular if $G = S$ is a commutative ring and $N = J \subset S$ is an ideal, then any element of ${}^{S}\!/_{J}$ can be written as $\overline{a} = a + J$ with $a \in S$.

In general, for an ideal $I \subset R[X]$, it is very difficult to describe the ring structure of ${}^{R[X]}\!/_{I}$, but with the help of Theorem 1.1.10 we can at least give a simple description of its R-module structure in the case where $Q_I = mP_I$ with $m \in R$ and a monic $P_I \in R[X]$. Indeed, in this case, it is possible to generalise the structure theorem for finitely generated R-modules (compare [Bou90, §4.4, Chapter VII] or [Lan02, §7, Chapter III]) to R-modules of the form ${}^{R[X]}\!/_{I}$. We can decompose ${}^{R[X]}\!/_{I}$ as the direct sum of a torsion and a free component. The free component is always finitely generated, whereas the torsion component is finitely generated if and only if the embracing polynomial Q_I is primitive.

Here an element $x \neq 0$ of an R-module M is called *torsion* if there exists a non-zero $a \in R$ such that $ax = 0$. The R-submodule of M, consisting of all torsion elements, will be denoted by M_{tor}.

1.1.19 Proposition. *Let $I \subset R[X]$ be a non-zero ideal, and let $Q_I \in R[X]$ be an embracing polynomial of I. Choose $m \in R$ and a primitive $P_I \in R[X]$ such that $Q_I = mP_I$. Then*

$$\left({}^{R[X]}\!/_{I}\right)_{\mathrm{tor}} = {}^{(P_I)}\!/_{I}.$$

If P_I is monic, then there exists an R-module isomorphism

$${}^{R[X]}\!/_{I} \cong {}^{(P_I)}\!/_{I} \oplus {}^{R[X]}\!/_{(P_I)}.$$

In particular ${}^{R[X]}\!/_{(P_I)} \cong R^r$ is free as an R-module, where $r = \deg(P_I)$.

Proof. First we show that $\overline{P} \in {}^{R[X]}\!/_{I}$ is torsion if and only if $P \in (P_I)$. Assume that $\overline{P} \in {}^{R[X]}\!/_{I}$ is torsion. Then there exists a non-zero $a \in R$ such that $aP \in I$. This implies that P_I divides aP. As P_I is primitive and $R[X]$ is a unique factorisation domain we can deduce that P_I divides P, i.e. $P \in (P_I)$. If on the other we hand we assume that $P \in (P_I)$, then $mP \in (Q_I)$. There exists a non-zero $m_0 \in R$ such that $m_0 Q_I \in I$. It follows that $m_0 mP \in I$ which is equivalent to saying that $\overline{P}$ is a torsion element of ${}^{R[X]}\!/_{I}$. Thus $({}^{R[X]}\!/_{I})_{\mathrm{tor}} = {}^{(P_I)}\!/_{I}$.

It is easy to show that $\left({}^{R[X]}\!/_{I}\right)\!/_{\left({}^{(P_I)}\!/_{I}\right)} \cong {}^{R[X]}\!/_{(P_I)}$ is torsion free. In fact the first paragraph of the proof of [Lan02, Theorem 7.3, Chapter III] holds even for modules that are not finitely generated.

Now assume that P_I is monic. Then ${}^{R[X]}\!/_{(P_I)}$ is torsion free and finitely generated as an R-module. Indeed it is generated by $\overline{1}, \overline{X}, \ldots, \overline{X^{r-1}}$. Thus ${}^{R[X]}\!/_{(P_I)}$ is free and hence isomorphic as an R-module to $R^{r'}$ for some $r' \in \mathbb{N}_0$ by [Bou90, Corollary 2, Chapter VII, §4.4]. If K is the quotient field of R we have K-vector space isomorphisms

$$K^r \cong {}^{K[X]}\!/_{(P_I)} \cong {}^{R[X]}\!/_{(P_I)} \otimes_R K \cong R^{r'} \otimes_R K \cong K^{r'}.$$

Hence $r' = r$ and ${}^{R[X]}\!/\!{}_{(P_I)} \cong R^r$.

Finally by [Lan02, Lemma 7.4, Chapter III] we have a decomposition

$$R[X]/I \;=\; \big(R[X]/I\big)_{\mathrm{tor}} \oplus F,$$

where F is a free R-module isomorphic to $R[X]/(P_I)$. □

Now we can use Theorem 1.1.10 to obtain a complete description of the R-module structure of $(R[X]/I)_{\mathrm{tor}} = (P_I)/I$.

1.1.20 Proposition. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal, and let*

$$\{m_0 Q_I, m_1 Q_1 Q_I, \dots, m_{s-1} Q_{s-1} Q_I, Q_s Q_I\}$$

be a convenient set of generators for I with $s = s(I)$, monic $Q_1, \dots, Q_s \in R[X]$ with $\deg(Q_d) = d$ for $d = 1, \dots, s$, and $0 \neq m_0, \dots, m_{s-1} \in R$ with $m_d | m_{d-1}$ for $d = 1, \dots, s$. Let $Q_I = mP_I$ with $m \in R$ and $P_I \in R[X]$ primitive. Then there exists an R-module isomorphism

$$R/(mm_0) \times \cdots \times R/(mm_{s-1}) \times R/(m)[X] \;\xrightarrow{\cong}\; (P_I)/I$$

defined by

$$\left(\overline{a_0}, \dots, \overline{a_{s-1}}, \sum_{i \in \mathbb{N}_0} \overline{f_i} X^i\right) \;\longmapsto\; \left(a_0 + a_1 Q_1 + \cdots + a_{s-1} Q_{s-1} + \left(\sum_{i \in \mathbb{N}_0} f_i X^i\right) Q_s\right) P_I + I.$$

Proof. Consider the homomorphism of R-modules

$$\Phi : \quad R^s \times R[X] \;\longrightarrow\; (P_I)/I$$

defined by

$$(a_0, \dots, a_{s-1}, P) \;\longmapsto\; (a_0 + a_1 Q_1 + \cdots + a_{s-1} Q_{s-1} + P Q_s) P_I + I.$$

It is clearly surjective since $Q_1, \dots, Q_s$ are monic.

Now let $(a_0, \dots, a_{s-1}, P) \in \ker(\Phi)$ with $P = \sum_{i \in \mathbb{N}_0} f_i X^i \in R[X]$. In other words

$$T \;:=\; \left(a_0 + a_1 Q_1 + \cdots + a_{s-1} Q_{s-1} + \left(\sum_{i \in \mathbb{N}_0} f_i X^i\right) Q_s\right) P_I \;\in\; I.$$

This implies that $Q_I = mP_I$ divides T. Hence there exist $b_0, \dots, b_{s-1} \in R$ with $a_d = mb_d$ for $d = 0, \dots, s-1$ and $g_i \in R$ with $f_i = mg_i$ for $i \in \mathbb{N}_0$. We obtain

$$T \;=\; \left(b_0 + b_1 Q_1 + \cdots + b_{s-1} Q_{s-1} + \left(\sum_{i \in \mathbb{N}_0} g_i X^i\right) Q_s\right) Q_I \;\in\; I.$$

By using Proposition 1.1.7 we can show that $b_d \in C_d^{(I)}$ for $d = 0, \dots, s-1$. Hence there exist $c_0, \dots, c_{s-1} \in R$ such that $b_d = m_d c_d$ for $d = 0, \dots, s-1$. Altogether we obtain $a_d = mm_d c_d \in (mm_d)$ for $d = 0, \dots, s-1$ and $g_i = mf_i \in (m)$ for $i \in \mathbb{N}_0$. Therefore

$$(a_0, \dots, a_{s-1}, P) \;\in\; (mm_0) \times \cdots \times (mm_{s-1}) \times mR[X].$$

Furthermore $m_d m Q_d P_I = (m_d Q_d) Q_I \in I$ for $d = 0, \dots, s-1$, and $mPQ_sP_I = PQ_sQ_I \in I$ for all $P \in R[X]$. Thus

$$\ker(\Phi) \; = \; (mm_0) \times \cdots \times (mm_{s-1}) \times mR[X].$$

The claim follows since there exists a canonical R-module isomorphism ${}^{R[X]}\!/_{mR[X]} \cong {}^{R}\!/_{(m)}[X]$ defined by

$$\left(\sum_{i \in \mathbb{N}_0} f_i X^i \right) + mR[X] \longmapsto \sum_{i \in \mathbb{N}_0} \overline{f_i} X^i. \qquad \square$$

1.1.21 Corollary. *We adopt the notation introduced in Proposition 1.1.20. There exists an R-module isomorphism*

$$(Q_I)/I \; \cong \; {}^{R}\!/_{(m_0)} \times \cdots \times {}^{R}\!/_{(m_{s-1})}.$$

Proof. We have canonical R-module isomorphisms $m\big({}^{R}\!/_{(mm_j)}\big) \cong {}^{R}\!/_{(m_j)}$ for $j = 0, \dots, s-1$. Furthermore $m\big({}^{R}\!/_{(m)}[X]\big) = 0$, and $m(P_I) = (Q_I) \subset R[X]$. Hence the claim follows. □

We summarise our observations as follows:

1.1.22 Theorem. *Let $I \subset R[X]$, $I \neq (0)$, be an ideal. Consider an embracing polynomial $Q_I \in R[X]$ of I. Choose $m \in R$ and a primitive $P_I \in R[X]$ with $Q_I = mP_I$. Set $r = \deg(P_I)$. Let $C_d^{(I)} = (m_d)$ with $m_d \in R$ for $d = 0, \dots, s-1$, where $s = s(I)$. If P_I is monic, then there exists an R-module isomorphism*

$$R[X]/I \; \cong \; R^r \times {}^{R}\!/_{(mm_0)} \times \cdots \times {}^{R}\!/_{(mm_{s-1})} \times {}^{R}\!/_{(m)}[X].$$

In particular if $Q_I = P_I$ is monic, then ${}^{R[X]}\!/_{I}$ is finitely generated as an R-module and we have

$$R[X]/I \; \cong \; R^r \times {}^{R}\!/_{(m_0)} \times \cdots \times {}^{R}\!/_{(m_{s-1})}.$$

1.2 Annihilating polynomials for group ring elements

Let G be a group of exponent 2. Consider the group ring $\mathbb{Z}[G]$. Since $g^2 = 1$ for all $g \in G$ we see that $\mathbb{Z}[G]$ is additively generated by integral elements, and therefore $\mathbb{Z}[G]$ is integral itself.

In this section we follow an approach introduced by J. Hurrelbrink in [Hur89] to construct and study annihilating polynomials for elements of $\mathbb{Z}[G]$. The methods introduced here form the basis for our study of annihilating polynomials for elements of Witt rings in Section 1.5 and all of Chapter 2.

Denote by $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ the dual of $\mathbb{Z}[G]$, i.e. the set of ring homomorphisms $\mathbb{Z}[G] \to \mathbb{Z}$. Since $G \subset (\mathbb{Z}[G])^*$, and since a ring homomorphism $\mathbb{Z}[G] \to \mathbb{Z}$ maps units to units, it follows that $\chi(g) = \pm 1$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ and for all $g \in G$.

1.2.1 Definition. *Denote by* $\dim : \mathbb{Z}[G] \to \mathbb{Z}$ *the element of* $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ *that sends every element of G to 1. We call* $\dim(x)$ *the* dimension *of an element $x \in \mathbb{Z}[G]$.*

1.2.2 Definition. *An element $x \in \mathbb{Z}[G]$ is called a* preform *if we can write $x = g_1 + \cdots + g_n$ with $g_i \in G$ for $i = 1, \ldots, n$.*

1.2.3 Lemma. *If $x \in \mathbb{Z}[G]$ is a preform of dimension n such that $\chi(x) = n$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, then $x = n$.*

Proof. Assume that $x = g + y$ such that $1 \neq g \in G$ and y is a preform of dimension $n - 1$. Choose a basis $\mathcal{B}$ for the $\mathbb{F}_2$-vector space G such that $g \in \mathcal{B}$. By mapping $g \mapsto -1$ and $h \mapsto 1$ for all $h \in \mathcal{B}$ with $h \neq g$, we can define a ring homomorphism $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ with $\chi(g) = -1$. Then $\chi(x) = -1 + \chi(y) < n$, which contradicts our assumption. Hence $x = n$. □

The following proposition constitutes the basis for all our observations about annihilating polynomials for group ring elements. It is simply a special case of [Hur89, Lemma 1.1], but in our specific situation it is possible to give a significantly more elementary proof.

1.2.4 Proposition. *If G is a group of exponent 2, then*

$$\bigcap_{\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})} \ker(\chi) \;=\; \{0\}.$$

Proof. Let $x \in \mathbb{Z}[G]$ with $\chi(x) = 0$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. We can write $x = a - b$ with preforms $a = g_1 + \cdots + g_n$ and $b = h_1 + \cdots + h_m$, $g_i, h_j \in G$. Since $\chi(x) = 0$ it follows that $\chi(a) = \chi(b)$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. In particular $\dim(x) = 0$, and therefore we must have $n = \dim(a) = \dim(b) = m$. First assume that $a = n$. Then $\chi(b) = \chi(a) = n$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, and the previous lemma implies $b = n$ and hence $x = 0$.

Next we assume that $g_1 \neq 1$. Let $V \subset G$ be the $\mathbb{F}_2$-subvector space generated by $g_1, \ldots, g_n$ and $h_1, \ldots, h_n$. Clearly V has finite dimension $r \in \mathbb{N}$ over $\mathbb{F}_2$. We can consider $\mathbb{Z}[V]$ as a subring of $\mathbb{Z}[G]$ with $x \in \mathbb{Z}[V]$. Then the restriction map $\operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z}) \to \operatorname{Hom}(\mathbb{Z}[V], \mathbb{Z})$ is surjective, which implies that $\sigma(x) = 0$ and therefore $\sigma(a) = \sigma(b)$ for all $\sigma \in \operatorname{Hom}(\mathbb{Z}[V], \mathbb{Z})$. We proceed by induction on r to show that $a = b$.

If $r = 1$, then $V = \{1, g_1\}$. Hence $a = r + (n - r)g_1$ and $b = s + (n - s)g_1$ with $r, s \in \mathbb{N}$, $0 \leq r, s \leq n$. Let χ be the unique element of $\operatorname{Hom}(\mathbb{Z}[V], \mathbb{Z})$ with $\chi(g_1) = -1$. Then $\chi(a) = 2r - n = 2s - n = \chi(b)$. It follows that $r = s$, and therefore $a = b$.

Now assume that $r > 1$. Choose a basis $\mathcal{B} := \{e_1, \ldots, e_r\}$ of the $\mathbb{F}_2$-vector space V such that $e_1 = g_1$. Denote by U the $\mathbb{F}_2$-subvector space of V generated by $e_2, \ldots, e_r$. For any $\rho \in \operatorname{Hom}(\mathbb{Z}[U], \mathbb{Z})$ there exist exactly two elements in $\operatorname{Hom}(\mathbb{Z}[V], \mathbb{Z})$ that extend ρ. More specifically those two extensions are $\rho_+, \rho_- \in \operatorname{Hom}(\mathbb{Z}[V], \mathbb{Z})$ with $\rho_+(g_1) = 1$ and $\rho_-(g_1) = -1$. We can write $a = a_1 + g_1 a_2$ and $b = b_1 + g_1 b_2$ with preforms $a_1, a_2, b_1, b_2 \in \mathbb{Z}[U]$. In particular we have $\rho_+(a_i) = \rho_-(a_i)$ and $\rho_+(b_i) = \rho_-(b_i)$ for all $\rho \in \operatorname{Hom}(\mathbb{Z}[U], \mathbb{Z})$ and $i = 1, 2$. It follows from $\chi(a) = \chi(b)$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ that

$$\begin{aligned} \rho_+(a) &= \rho(a_1) + \rho(a_2) &= \rho(b_1) + \rho(b_2) &= \rho_+(b), \qquad \text{and} \\ \rho_-(a) &= \rho(a_1) - \rho(a_2) &= \rho(b_1) - \rho(b_2) &= \rho_-(b), \end{aligned}$$

and thus

$$\rho(a_1) \;=\; \rho(b_1) \qquad \text{and} \qquad \rho(a_2) \;=\; \rho(b_2)$$

for all $\rho \in \operatorname{Hom}(\mathbb{Z}[U], \mathbb{Z})$. By induction we must have $a_1 = b_1$ and $a_2 = b_2$. It follows that $a = a_1 + g_1 a_2 = b_1 + g_1 b_2 = b$. Therefore $x = 0$. □

For $x \in \mathbb{Z}[G]$ define the *signature set*

$$S_x \;:=\; \{\chi(x) \mid \chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})\}\,.$$

Write

$$x \;=\; \sum_{g \in G} z_g g, \quad z_g \in \mathbb{Z}.$$

Define the *norm* of x as

$$|x| \;:=\; \sum_{g \in G} |z_g| \;\in\; \mathbb{Z},$$

where $|z_g|$ denotes the usual absolute value of the integer z_g. Then $|\chi(x)| \leq |x|$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. This implies that S_x is finite. Hence we can define the *signature polynomial*

$$P_x \;:=\; \prod_{\chi(x) \in S_x} (X - \chi(x)) \;\in\; \mathbb{Z}[X]. \tag{1.3}$$

1.2.5 Definition. *Let R be a commutative ring, and let $\iota : \mathbb{Z} \to R$ be the canonical homomorphism defined by $\iota(1) = 1_R$. A polynomial $P = z_n X^n + \cdots + z_1 X + z_0 \in \mathbb{Z}[X]$ is called* annihilating polynomial *of an element $x \in R$ if*

$$P(x) \;:=\; \iota(z_n)x^n + \cdots + \iota(z_1)x + \iota(z_0) \;=\; 0 \;\in\; R.$$

Usually we will omit the ι and simply write $mx := \iota(m)x$ for $m \in \mathbb{Z}$ and $x \in R$.

1.2.6 Theorem. *Let $x \in \mathbb{Z}[G]$. Then the signature polynomial P_x as defined in* (1.3) *is an annihilating polynomial of x.*

Proof. We have

$$\sigma(P_x(x)) \;=\; \prod_{\chi(x) \in S_x} (\sigma(x) - \chi(x)) \;=\; 0$$

for all $\sigma \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Thus Proposition 1.2.4 implies $P_x(x) = 0$. □

It is easy to see that in fact every annihilating polynomial of $x \in \mathbb{Z}[G]$ is divisible by P_x.

1.2.7 Definition. *Let R be a commutative ring, and let $x \in R$. We define*

$$\operatorname{Ann}_x \;:=\; \{P \in \mathbb{Z}[X] \mid P(x) = 0\}$$

and call this ideal the annihilating ideal *of x.*

1.2.8 Proposition. *For $x \in \mathbb{Z}[G]$ we have $\operatorname{Ann}_x = (P_x)$.*

Proof. Let $P \in \operatorname{Ann}_x$. Then $P(\chi(x)) = \chi(P(x)) = 0$ for any $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Since $\mathbb{Z}[X]$ is a unique factorisation domain and $\chi(x)$ is a root of P, it follows that $(X - \chi(x))$ divides P. Hence P_x divides P. □

1.2.9 Corollary. *For $n \in \mathbb{N}$ the polynomial*

$$P_n := (X-n)(X-n+2)\cdots(X+n-2)(X+n) \in \mathbb{Z}[X]$$

annihilates any $x \in \mathbb{Z}[G]$ with $|x| = n$.

Proof. Consider any $x \in \mathbb{Z}[G]$ with $|x| = n$. Write $x = \varepsilon_1 g_1 + \cdots + \varepsilon_n g_n$, where $|x| = n$, $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$, and $g_1, \ldots, g_n \in G$. Then clearly $\chi(x) \equiv n \pmod 2$ and $|\chi(x)| \leq n$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Hence P_x divides P_n. □

1.2.10 Remark. In the context of annihilating polynomials the polynomials P_n, $n \in \mathbb{N}_0$, are first mentioned in [Lew87]. In this article D. W. Lewis shows that P_n annihilates the isometry class of every n-dimensional quadratic form over any field K. Therefore the polynomials P_n, $n \in \mathbb{N}_0$, are often called the *Lewis polynomials*. Shortly afterwards, in [Hur89], J. Hurrelbrink shows that the Lewis polynomials are in fact annihilating polynomials for elements of the group ring $\mathbb{Z}[G]$, where $G = {}^{K^*}/_{(K^*)^2}$ is the square class group of a field K. As such they naturally occur as annihilating polynomials for isometry and equivalence classes of quadratic forms over K, since, as we will see in Section 2.1, both the Witt-Grothendieck ring and the Witt ring of K are quotients of $\mathbb{Z}[G]$. △

Pfister elements

We close this section with a few definitions and results that we will need to prove the structure theorems for certain quotients of $\mathbb{Z}[G]$ in Section 1.4. More precisely we will generalise the quadratic-form-theoretic concept of Pfister forms. In the context of group rings it is possible to characterise Pfister elements with the help of annihilating polynomials. Unfortunately this does not hold any more once we consider quotients of $\mathbb{Z}[G]$ and in particular Witt rings of fields.

1.2.11 Definition. *Let $x \in \mathbb{Z}[G]$ and $k \in \mathbb{N}_0$.*

(1) The element x is called k-fold Pfister*, if there exist $g_1, \ldots, g_k \in G$ and $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$ such that $x = (1 + \varepsilon_1 g_1) \cdots (1 + \varepsilon_k g_k)$.*

(2) We say that x is k-fold quasi-Pfister*, if it is an odd multiple of a k-fold Pfister element, i.e. if there exists a k-fold Pfister element $y \in \mathbb{Z}[G]$ and an odd $m \in \mathbb{N}$ such that $x = my$.*

1.2.12 Definition. *Two elements $x, y \in \mathbb{Z}[G]$ are* similar *if there exists a $g \in \mathbb{Z}[G]$ such that $x = \pm gy$.*

1.2.13 Proposition. *Let $x \in \mathbb{Z}[G]$ and $n = |x| > 0$. The element x is similar to a quasi-Pfister element if and only if $(X - n)X(X + n) \in \mathbb{Z}[X]$ annihilates x.*

Proof. *"$\Longrightarrow$":* Write $x = \pm mh(1 + \varepsilon_1 g_1) \cdots (1 + \varepsilon_k g_k)$ with $m \in \mathbb{N}$ odd, $h, g_i \in G$ and $\varepsilon_i \in \{-1, 1\}$. For any $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ we have $\chi(m) = m$, $\chi(h) = \pm 1$, and $\chi(1 + \varepsilon_i g_i) \in \{0, 2\}$. Hence $\chi(x) = 0$ or $\chi(x) = \pm m 2^k = \pm n$, i.e. $S_x \subset \{-n, 0, n\}$. This implies that P_x divides $(X - n)X(X + n)$, which shows that $(X - n)X(X + n)$ annihilates x.

"$\Longleftarrow$": Write

$$x = \pm h(1 + \varepsilon_1 g_1 + \cdots + \varepsilon_{n-1} g_{n-1})$$

with $h, g_i \in G$ and $\varepsilon_i \in \{-1, 1\}$. Without loss of generality we can assume that $g_1, \ldots, g_k$ for some $k \in \mathbb{N}_0$ form a basis of the $\mathbb{F}_2$-vector space generated by $g_1, \ldots, g_{n-1}$. Set $y := 1 + \varepsilon_1 g_1 + \cdots + \varepsilon_{n-1} g_{n-1}$. Since $\chi(y) > -n$ for all $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$, and since by our assumption $S_x \subset \{-n, 0, n\}$, we must have $S_y \subset \{0, n\}$. By induction on $k \geq 0$ we show that 2^k divides n, and that $y = \frac{n}{2^k}(1 + \varepsilon_1 g_1) \cdots (1 + \varepsilon_k g_k)$.

If $k = 0$, then $g_i = 1$ for $i = 1, \ldots, n-1$. In other words $y = 1 + \varepsilon_1 + \cdots + \varepsilon_{n-1}$. Now $|x| = n$ implies $\varepsilon_i = 1$ for all i. Hence $y = n$, and trivially $x = \pm hn$ is similar to the quasi-Pfister element n.

Let $k > 0$. We assumed that $|x| = n > 0$. Thus there must exist a $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ with $\chi(y) = n$. Furthermore, if $\chi(y) = n$ for all $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$, then by Proposition 1.2.4 we have $y = n$, which contradicts our assumption that $k > 0$. Hence $g_1 \neq 1$. It follows that $S_y = \{0, n\}$.

Consider the $\mathbb{F}_2$-subvector space $V \subset G$ generated by $g_1, \ldots, g_k$. We have $\dim_{\mathbb{F}_2}(V) = k$. Let $U \subset V$ be the $\mathbb{F}_2$-subvector space generated by $g_2, \ldots, g_k$. As in the proof of Proposition 1.2.4 we consider $\mathbb{Z}[U] \subset \mathbb{Z}[V] \subset \mathbb{Z}[G]$ as subrings. Hence $\sigma(y) \in \{0, n\}$ for all $\sigma \in \mathrm{Hom}(\mathbb{Z}[V], \mathbb{Z})$, and for every $\rho \in \mathrm{Hom}(\mathbb{Z}[U], \mathbb{Z})$ there exist exactly two $\rho_+, \rho_- \in \mathrm{Hom}(\mathbb{Z}[V], \mathbb{Z})$ with $\rho_+|_{\mathbb{Z}[U]} = \rho_-|_{\mathbb{Z}[U]} = \rho$ and $\rho_+(g_1) = 1$, $\rho_-(g_1) = -1$. Write $y = a + \varepsilon_1 g_1 b$ with $a = 1 + a'$, $b = 1 + b'$, and $a', b' \in \mathbb{Z}[U]$. We can choose a' and b' such that $|a| + |b| = n$.

Consider any $\rho \in \mathrm{Hom}(\mathbb{Z}[U], \mathbb{Z})$. If $\rho(a) = 0$, and if $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ with $\chi|_{\mathbb{Z}[U]} = \rho$, then $0 \leq \chi(y) < n$ implies $\rho(b) = \rho(a) = 0$. Analogously $\rho(b) = 0$ implies $\rho(a) = \rho(b) = 0$. Hence, if $\rho(a) \neq 0$, then we must also have $\rho(b) \neq 0$. By our observations above such a $\rho \in \mathrm{Hom}(\mathbb{Z}[U], \mathbb{Z})$ with $\rho(a) \neq 0$ must exist. In this case, if $\rho_+(y) = \rho(a) + \varepsilon_1 \rho(b) = 0$, then we obtain $\rho_-(y) = \rho(a) - \varepsilon_1 \rho(b) = n$. Similarly, if $\rho_+(y) = n$, then $\rho_-(y) = 0$. This implies that $\rho_+(y) + \rho_-(y) = 2\rho(a) = n$, and hence $\rho(a) = \frac{n}{2}$. In particular it follows that $|a| \geq \frac{n}{2}$. Furthermore $\rho_+(y) - \rho_-(y) = 2\varepsilon_1 \rho(b) = n$ implies $|\rho(b)| = \frac{n}{2}$ and $|b| \geq \frac{n}{2}$. Accordingly, since we assumed that $|a| + |b| = n$, we must have $|a| = |b| = \frac{n}{2}$. As $b = 1 + b'$, we obtain $\rho(b) > -\frac{n}{2}$. Thus $\rho(b) = \frac{n}{2} = \rho(a)$. Altogether we see that $\rho(a) = \rho(b)$ for all $\rho \in \mathrm{Hom}(\mathbb{Z}[U], \mathbb{Z})$, which by Proposition 1.2.4 implies $a = b$. It follows that $y = (1 + \varepsilon_1 g_1)a$.

Write $a = 1 + \delta_1 h_1 + \cdots + \delta_{\frac{n}{2}-1} h_{\frac{n}{2}-1}$ with $\delta_i \in \{-1, 1\}$ and $h_i \in U$. Since $a \in \mathbb{Z}[U]$, it follows that all the summands of $\varepsilon_1 g_1 a = \varepsilon_1 g_1 + \varepsilon_1 \delta_1 g_1 h_1 + \cdots + \varepsilon_1 \delta_{\frac{n}{2}-1} g_1 h_{\frac{n}{2}-1}$ do not lie in $\mathbb{Z}[U]$. Thus all the summands of $y = 1 + \varepsilon_1 g_1 + \cdots + \varepsilon_{n-1} g_{n-1}$ which lie in $\mathbb{Z}[U]$ must be summands of a. We obtain $a = 1 + \varepsilon_2 g_2 + \cdots + \varepsilon_k g_k + a''$ with some $a'' \in \mathbb{Z}[U]$. Now $g_2, \ldots, g_k$ form a basis of the $\mathbb{F}_2$-vector space U. In addition we have seen that $S_a \subset \{0, \frac{n}{2}\}$. Therefore by induction 2^{k-1} divides $\frac{n}{2}$ and $a = \frac{n}{2} \cdot \frac{1}{2^{k-1}} \cdot (1 + \varepsilon_2 g_2) \cdots (1 + \varepsilon_k g_k)$. We conclude that $y = \frac{n}{2^k}(1 + \varepsilon_1 g_1) \cdots (1 + \varepsilon_k g_k)$. □

The proof of the previous proposition also contains the proofs for the following two corollaries.

1.2.14 Corollary. *An element $x \in \mathbb{Z}[G]$ with $n = |x| > 0$ is quasi-Pfister if and only if it is annihilated by $X(X - n) \in \mathbb{Z}[X]$.*

1.2.15 Corollary. *Let $x = 1 + \varepsilon_1 g_1 + \cdots + \varepsilon_{n-1} g_{n-1} \in \mathbb{Z}[G]$ with $n \in \mathbb{N}$, $\varepsilon_i \in \{-1, 1\}$, and $g_i \in G$. Suppose that $X(X-n) \in \mathbb{Z}[X]$ annihilates x. If $g_1, \ldots, g_k$ form a basis of the $\mathbb{F}_2$-vector space generated by $g_1, \ldots, g_{n-1}$, then 2^k divides n and*

$$x \;=\; \frac{n}{2^k}(1 + \varepsilon_1 g_1) \cdots (1 + \varepsilon_k g_k).$$

The results in this section demonstrate how well elements of $\mathbb{Z}[G]$ behave in many respects. Once we pass to quotients of $\mathbb{Z}[G]$ the situation will deteriorate significantly.

1.3 The spectrum of a Witt ring

We again consider a group G of exponent 2. As announced in Section 1.2 we want to consider quotients of the group ring $\mathbb{Z}[G]$. During all of this section $J \subset \mathbb{Z}[G]$, $J \neq \mathbb{Z}[G]$, will denote an ideal, and we set $R := \mathbb{Z}[G]/_J$.

1.3.1 Definition. *The ring R is called a* Witt ring for G *if for every $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ we have $\chi(J) = (0)$ or $\chi(J) = (2^k)$ for some $k \in \mathbb{N}$.*

1.3.2 Examples. Let G be a group of exponent 2.

(1) The simplest example of a Witt ring for G is just $R = \mathbb{Z}[G]$, i.e. $J = (0)$.

(2) Let K be a field with $\operatorname{char}(K) \neq 2$, and let $G = K^*/(K^*)^2$ be the square class group of K. Consider the Witt-Grothendieck ring $\widehat{W}(K)$ of K. Then $\widehat{W}(K) \cong Z[G]/_{J_1}$ with

$$J_1 \;=\; \big(\overline{a} + \overline{b} - \overline{c} - \overline{d} \mid a, b, c, d \in K^*,\ \langle a, b\rangle \cong \langle c, d\rangle\big)$$

by [Sch85, Theorem 9.1, Chapter 2], and it is clear that $\chi(\overline{a}+\overline{b}-\overline{c}-\overline{d}) \in \{-4, -2, 0, 2, 4\}$ for all $a, b, c, d \in K^*$ and $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Thus $\widehat{W}(K)$ is a Witt ring for the square class group G.

(3) Again let K be a field with $\operatorname{char}(K) \neq 2$ and square class group $G = K^*/(K^*)^2$. This time consider the Witt ring $W(K)$ of K. It is well known that $W(K) \cong \mathbb{Z}[G]/_{J_2}$ with

$$J_2 \;=\; J_1 + (\overline{1} + \overline{(-1)})$$

(see [Sch85, Corollary 9.4, Chapter 2]). Since we have $\chi(\overline{1} + \overline{(-1)}) \in \{-2, 0, 2\}$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$, it follows that $W(K)$ is a Witt ring for the square class group G as well. △

1.3.3 Remark. The notion of Witt rings for groups was introduced in [KRW72] by M. Knebusch, A. Rosenberg and R. Ware. In fact they managed to prove, in a more general setting, many of the results we will prove in this and the following section. However, in our special case there exists a shorter and more elementary approach, which in many cases yields notably more specific results. More specifically we generalise the methods demonstrated by D. Lewis in [Lew89]. But while D. Lewis restricts himself to considering Witt rings of fields and besides annihilating polynomials also uses some well-known results about quadratic forms, we will only need a few basic facts from commutative algebra and our observations about annihilating polynomials. This is particularly interesting, since we will obtain the structure theorems for Witt rings of fields as a mere special case. In other words, apart from the basic properties needed to obtain the ideals J_1 and J_2 from the Examples 1.3.2, none of the distinct geometric properties of quadratic forms are needed. △

From commutative algebra we will only need the following results:

1.3.4 Theorem. *Let R be a commutative ring, and let $I \subset R$ be an ideal. Then the radical of I is equal to the intersection of all the prime ideals containing I.*

[Mat86, Chapter 1, §1, p. 3]

1.3.5 Corollary. *The nilradical of a commutative ring R is the intersection of its minimal prime ideals.*

[Mat86, Chapter 1, §1, p. 3]

1.3.6 Theorem ("lying over")**.** *Let $R \subset S$ be commutative rings such that S is an integral extension of R. For every prime ideal $\mathfrak{p} \subset R$ there exists a prime ideal $\mathfrak{q} \subset S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.*

[Eis95, Proposition 4.15, Chapter 4]

1.3.7 Theorem. *Let $R \subset S$ be an integral extension of commutative rings. Then R and S have the same dimension.*

[Kap94, Theorem 48, Chapter 1]

Since $\mathbb{Z}[G]$ is integral, the same holds for any quotient of $\mathbb{Z}[G]$. In particular Witt rings for G are integral. Furthermore, since $\mathbb{Z}$ has dimension 1, it follows from the previous theorem, that $\mathbb{Z}[G]$ has dimension 1 as well. As the prime ideals of $R = \mathbb{Z}[G]/_J$ are in one-to-one correspondence with the prime ideals of $\mathbb{Z}[G]$ containing J, we see that Witt rings for G are of dimension 0 or 1.

In the following we study the prime ideals of $\mathbb{Z}[G]$. It is possible to give a complete list of prime ideals of $\mathbb{Z}[G]$, and for each prime ideal $\mathfrak{p}$ we can give an easy to describe set of generators which not only generate $\mathfrak{p}$ as an ideal but also as a group. We are particularly interested in the minimal prime ideals of $\mathbb{Z}[G]$, since those will later on provide us with the ring homomorphisms $R \to \mathbb{Z}$ for any given Witt ring R for G.

1.3.8 Proposition. *Let G be a group of exponent 2. For any $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ the set*

$$H_\chi \;:=\; \{g \in G \mid \chi(g) = 1\}$$

is a subgroup of G of index at most 2. Conversely every subgroup $H \subset G$ of index at most 2 defines a ring homomorphism $\chi_H : \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$g \longmapsto \begin{cases} 1 & \text{if } g \in H, \\ -1 & \text{otherwise,} \end{cases} \qquad g \in G.$$

We thus get a one-to-one correspondence between subgroups of G of index at most 2 and the ring homomorphisms $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$.

Proof. Let $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$. Since χ is a ring homomorphism, it induces a group homomorphism on the units $\chi : (\mathbb{Z}[G])^* \to \mathbb{Z}^* = \{1, -1\}$. Now $G \subset (\mathbb{Z}[G])^*$, which implies that we can restrict χ to obtain a group homomorphism $\rho : G \to \{1, -1\}$. Therefore $H_\chi = \ker(\rho)$ is a subgroup of G. If $\chi = \dim$, then we have $H = G$, and G is a subgroup of index 1 in G. So we can assume that $\chi \neq \dim$. Then there exist $f, g \in G \setminus H_\chi$. We have $\chi(fg) = \chi(f)\chi(g) = (-1)^2 = 1$, i.e. $fg \in H_\chi$. This implies that $\overline{f} = \overline{g^{-1}} = \overline{g} \in {}^{G}\!/\!_{H_\chi}$. Hence ${}^{G}\!/\!_{H_\chi}$ has exactly 2 elements, and H_χ has index 2 in G.

Now let $H \subset G$ be a subgroup of index at most 2. We have to show that the map χ_H is well-defined and a ring homomorphism. But this is the case if for all $f, g \in G$ we have $\chi(fg) = \chi(f)\chi(g)$. By definition of χ_H this clearly holds if at most one of f and g does not lie in H. This is always the case if $H = G$. Then $\chi_G = \dim$. So we assume that $H \neq G$. If $f, g \notin H$, then the fact that H has index 2 in G implies $fg \in H$. In other words $\chi(fg) = 1 = (-1)^2 = \chi(f)\chi(g)$.

It is easy to see that for $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ we have $\chi_{H_\chi} = \chi$. And for any subgroup $H \subset G$ of index at most 2 we clearly obtain $H_{\chi_H} = H$. □

To a subgroup $H \subset G$ we associate the ideal

$$\mathfrak{p}_H \;:=\; (1 - g \mid g \in H) + (1 + g \mid g \in G \setminus H).$$

1.3.9 Lemma. *Let G be a group of exponent 2, and let $H \subset G$ be a subgroup of index at most 2, then $\ker(\chi_H) = \mathfrak{p}_H$.*

Proof. By definition of $\mathfrak{p}_H$ and χ_H it is clear that $\mathfrak{p}_H \subset \ker(\chi_H)$. Now let $x \in \ker(\chi_H)$. We can write

$$x = \sum_{g \in H} a_g(1 - g) + \sum_{g \in G \setminus H} a_g(1 + g) + z$$

with $a_g, z \in \mathbb{Z}$, $g \in G$. Then $\chi_H(x) = \chi_H(z) = 0$. Since $\chi_H(1) = 1$, we must have $z = 0$. Thus $\ker(\chi_H) = \mathfrak{p}_H$. □

We introduce the following notation: Let R be a ring, let S be an R-algebra via $\iota : R \to S$, and let M be an S-module. For a set $\{m_\nu\}_{\nu \in N} \subset M$, where N is an index set, we write

$$< m_\nu \mid \nu \in N >_R \;:=\; \left\{ \sum_{\nu \in N} \iota(\lambda_\nu) m_\nu \;\middle|\; \lambda_\nu \in R,\ \lambda_\nu = 0 \text{ for almost all } \nu \in N \right\} \subset M$$

for the R-submodule of M generated by $\{m_\nu\}_{\nu \in N}$.

The proof of the previous lemma yields additional information about the elements of $x \in \mathfrak{p}_H$ for a subgroup $H \subset G$ of index at most 2. Indeed the elements $1 - g$ for $g \in H$ and $1 + g$ for $g \notin H$ already generate $\mathfrak{p}_H$ as a group.

1.3.10 Corollary. *For a group G of exponent 2 and a subgroup $H \subset G$ of index at most 2 we have*

$$\mathfrak{p}_H \;= <1 - g \mid g \in H>_{\mathbb{Z}} + <1 + g \mid g \in G \setminus H>_{\mathbb{Z}}.$$

In addition, if $H \subset G$ is a subgroup of index at most 2, then $\mathfrak{p}_H$ is the preimage of the prime ideal $(0) \subset \mathbb{Z}$ via the ring homomorphism $\chi_H : \mathbb{Z}[G] \to \mathbb{Z}$. Accordingly $\mathfrak{p}_H \subset \mathbb{Z}[G]$ is a prime ideal.

1.3.11 Corollary. *If G is a group of exponent 2 and $H \subset G$ a subgroup of index at most 2, then $\mathfrak{p}_H$ is a prime ideal in $\mathbb{Z}[G]$.*

1.3.12 Theorem. *Let G be a group of exponent 2. The following is a complete list of the prime ideals of $\mathbb{Z}[G]$:*

(a) the minimal prime ideals $\mathfrak{p}_H$, where H varies over those subgroups of G with index at most 2,

(b) the maximal prime ideals $\mathfrak{p}_{H,p} := \mathfrak{p}_H + (p)$, where H varies over the subgroups of G of index at most 2, and p varies over the odd prime numbers,

(c) the maximal prime ideal $I(G) := \mathfrak{p}_G + (2)$.

The prime ideals listed above are all pairwise distinct.

Proof. Since $\mathbb{Z}[G]$ has dimension 1, any prime ideal of $\mathbb{Z}[G]$ is minimal or maximal. It is clear that for any subgroup $H \subset G$ of index at most 2 the prime ideal $\mathfrak{p}_H$ is minimal. Indeed this follows directly from the fact that $\mathfrak{p}_H = \ker(\chi)$ for some $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. As $\mathbb{Z}[G]/\mathfrak{p}_H \cong \mathbb{Z}$ is not a field, $\mathfrak{p}_H$ is not maximal and must hence be minimal.

By an argument analogous to the one we employed in the proof of Lemma 1.3.9 it follows that $\chi_H^{-1}((p)) = \mathfrak{p}_H + (p)$, where $H \subset G$ is a subgroup of index at most 2 and p is an arbitrary prime. Since $\mathbb{Z}[G]/\mathfrak{p}_{H,p} \cong \mathbb{Z}/(p)$ is a field, we see that $\mathfrak{p}_H + (p)$ is maximal.

We consider the case $p = 2$. Let $H \subset G$ be a subgroup of index at most 2. Now, if $1 - g \in \mathfrak{p}_H$, then $2 - (1 - g) = 1 + g \in \mathfrak{p}_H + (2)$. Conversely $1 + g \in \mathfrak{p}_H$ implies $1 - g \in \mathfrak{p}_H + (2)$. In other words $\mathfrak{p}_H + (2) = (1 - g \mid g \in G) + (1 + g \mid g \in G)$, and in particular $\mathfrak{p}_H + (2) = \mathfrak{p}_G + (2) = I(G)$.

Now let $\mathfrak{q} \subset \mathbb{Z}[G]$ be any prime ideal. Then $(1-g)(1+g) = 0 \in \mathfrak{q}$ for all $g \in G$. Therefore $(1 - g) \in \mathfrak{q}$ or $(1 + g) \in \mathfrak{q}$. Set

$$A \ := \ \{g \in G \mid (1 - g) \in \mathfrak{q}\}.$$

Obviously $1 \in A$, and if $g, h \in A$, then

$$(1 - g) + g(1 - h) \ = \ 1 - gh \in \mathfrak{q}$$

or equivalently $gh \in A$. As G has exponent 2, it follows that A is a subgroup of A. Assume that $g, h \in G \setminus A$, then $1 + g, 1 + h \in \mathfrak{q}$ and

$$(1 + g) - g(1 + h) \ = \ 1 - gh \in \mathfrak{q}.$$

Hence $gh \in A$. By employing the same argument as in the proof of Proposition 1.3.8 we see that A has index at most two in G. Thus $\mathfrak{p}_A \subset \mathfrak{q}$. The ring homomorphism $\chi_A \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$ induces an isomorphism $\mathbb{Z}[G]/\mathfrak{p}_A \cong \mathbb{Z}$, which maps the prime ideal $\mathfrak{q}/\mathfrak{p}_A$ to a prime ideal $(m) \subset \mathbb{Z}$. If $m = 0$, then $\mathfrak{q} = \mathfrak{p}_A$. Otherwise $m = p$ is prime and $\mathfrak{q} = \chi_A^{-1}((p)) = \mathfrak{p}_A + (p)$. Therefore the list of prime ideals given in the theorem is complete.

It remains to show that the prime ideals mentioned in the theorem are pairwise distinct. Proposition 1.3.8 implies that the minimal prime ideals $\mathfrak{p}_H$, where H varies over all subgroups of G of index at most 2, are distinct. Above we have seen that $\mathfrak{p}_H + (2) = I(G)$ for all subgroups $H \subset G$ of index at most 2. Hence we only have to consider the maximal ideals $\mathfrak{p}_{H,p} = \mathfrak{p}_H + (p)$, where p is an odd prime. Let $H, H' \subset G$ be subgroups of index at most 2, and let $p, p' \in \mathbb{Z}$ be odd primes. Assume that $\mathfrak{p}_H + (p) = \mathfrak{p}_{H'} + (p')$. As $\mathfrak{p}_{H,p}$ is prime, it follows immediately that $p' = p$. Indeed $p, p' \in \mathfrak{p}_{H,p}$ implies $\gcd(p, p') \in \mathfrak{p}_{H,p}$. Now let $g \in H$. Then we must also have $g \in H'$, since otherwise $1 + g \in \mathfrak{p}_{H'}$. This would imply $(1 - g) + (1 + g) = 2 \in \mathfrak{p}_{H,p}$, which is not possible. Therefore $H \subset H'$ and by symmetry $H = H'$. Thus all the $\mathfrak{p}_{H,p}$ are pairwise distinct as well. □

We continue to study the spectrum of an arbitrary Witt Ring $R = \mathbb{Z}[G]/J$ for a group G of exponent 2.

1.3.13 Lemma. *Let $R = \mathbb{Z}[G]/J$ be a Witt ring for a group G of exponent 2. If $J \subset \mathfrak{p}_H + (p)$ for some subgroup $H \subset G$ of index at most 2 and some odd prime p, then $J \subset \mathfrak{p}_H$.*

Proof. Let $x \in J$. We can write

$$x = \sum_{g \in H} a_g(1 - g) + \sum_{g \in G \setminus H} a_g(1 + g) + bp$$

with $a_g, b \in \mathbb{Z}$, $g \in G$. Since $1 - g \in \ker(\chi_H)$ for all $g \in H$, and since $1 + g \in \ker(\chi_H)$ for all $g \in G \setminus H$, it follows that $\chi_H(x) = \chi_H(bp) = bp$. By definition $\chi_H(J) = (0)$ or $\chi_H(J) = (2^k)$ for some $k \in \mathbb{N}$. Since p is an odd prime, this implies that $b = 0$. Therefore $x \in \mathfrak{p}_H$. □

Consider a Witt ring $R = \mathbb{Z}[G]/J$ for a group G of exponent 2. If J is contained in the minimal prime ideal $\mathfrak{p}_G$ associated to the dimension homomorphism $\dim : \mathbb{Z}[G] \to \mathbb{Z}$, then dim induces a ring homomorphism $\overline{\dim} : R \to \mathbb{Z}$. Let $\mathfrak{m}$ be any maximal ideal with $J \subset \mathfrak{m}$. We know that $\mathfrak{m} = \mathfrak{p}_H + (p)$ for some subgroup $H \subset G$ of index at most 2 and some prime number $p \in \mathbb{Z}$. If $p = 2$, then $\mathfrak{m} = I(G)$. If p is odd, then by the previous lemma we must have $J \subset \mathfrak{p}_H$. In the proof of Theorem 1.3.12 we have seen that $\mathfrak{p}_H + (2) = I(G)$. Hence also in this case $J \subset I(G)$. Since $I(G) = \dim^{-1}(2\mathbb{Z})$, it follows that dim induces a ring homomorphism $R \to \mathbb{Z}/2\mathbb{Z}$.

1.3.14 Definition. *Let $R = \mathbb{Z}[G]/J$ be a Witt ring for a group G of exponent 2. The* dimension homomorphism $\dim : \mathbb{Z}[G] \to \mathbb{Z}$ *induces a ring homomorphism $e_0 : R \to \mathbb{Z}/2\mathbb{Z}$, which we call* dimension index. *The kernel of e_0 is called the* fundamental ideal *of R. We write $I(R) := \ker(e_0)$. In the case where $R = \mathbb{Z}[G]$ we have already used the notation $I(G) = I(R)$ in Theorem 1.3.12.*

1.3.15 Theorem. *Let $R = \mathbb{Z}[G]/J$ be a Witt ring for a group G of exponent 2. The following is a complete list of the prime ideals of R:*

(a) the minimal prime ideals $\ker(\overline{\chi})$, where $\overline{\chi}$ varies over the elements of $\mathrm{Hom}(R, \mathbb{Z})$,

(b) the maximal prime ideals $\ker(\overline{\chi}) + (\overline{p})$, where $\overline{\chi}$ varies over the ring homomorphisms $\mathrm{Hom}(R, \mathbb{Z})$, and p varies over the odd primes,

(c) the maximal prime ideal $I(R) = \ker(e_0)$.

The prime ideals listed above are all pairwise distinct.

Proof. From the definition of e_0 it follows that $I(R) = \ker(e_0)$ is a maximal ideal of R. The prime ideals of R are in one-to-one correspondence with the prime ideals of $\mathbb{Z}[G]$ that contain J. It is clear that the preimage of $\ker(e_0)$ via the projection $\mathbb{Z}[G] \to R$ is just the maximal ideal $I(G) = \mathfrak{p}_G + (2)$.

Now let $\chi \in \operatorname{Hom}(\mathbb{Z}[G], \mathbb{Z})$. If $J \subset \ker(\chi)$ then obviously also $J \subset \ker(\chi) + (p)$ for any odd prime p. In this case χ induces a ring homomorphism $\overline{\chi} \in \operatorname{Hom}(R, \mathbb{Z})$, and R contains the minimal prime ideal $\ker(\overline{\chi})$ and the maximal ideals $\ker(\overline{\chi}) + (\overline{p})$ for all odd primes p. If $J \not\subset \ker(\chi)$, then by Lemma 1.3.13 none of the maximal ideals $\ker(\chi) + (p)$, where p varies over all odd primes, can contain J. □

1.3.16 Proposition. *Let* $R = {}^{\mathbb{Z}[G]}\!/_{J}$ *be a Witt ring for a group* G *of exponent* 2*. Then* R *has characteristic* 0 *if and only if* $\operatorname{Hom}(R, \mathbb{Z}) \neq \varnothing$*. Otherwise* $\operatorname{char}(R) = 2^k$ *for some* $k \in \mathbb{N}$*.*

Proof. If there exists a $\overline{\chi} \in \operatorname{Hom}(R, \mathbb{Z})$, and if $\iota : \mathbb{Z} \to R$ is the canonical ring homomorphism, then $\overline{\chi} \circ \iota$ is the identity on $\mathbb{Z}$. Hence ι must be injective, which implies that R has characteristic 0.

Assume that $\operatorname{Hom}(R, \mathbb{Z}) = \varnothing$. By Theorem 1.3.15 this means that R is a local ring with unique prime ideal $I(R)$. In particular $I(G) \subset \mathbb{Z}[G]$ is the unique prime ideal that contains J. Hence $I(G)$ is the radical of J by Theorem 1.3.4. This implies that there exists some minimal $k \in \mathbb{N}$ such that $2^k \in J$. We obtain that $\overline{2^k} = 0 \in R$. In particular $\operatorname{char}(R) \neq 0$. Now let $\operatorname{char}(R) = m$, then m divides 2^k. Therefore m is a power of 2. As k is minimal it follows that $m = 2^k$. □

The proof of the previous proposition also contains the following result:

1.3.17 Corollary. *Let* R *be a Witt ring for a group of exponent* 2*. If* $\operatorname{char}(R) \neq 0$*, then* R *is a local ring with unique prime ideal* $I(R)$*.*

Combining the previous corollary together with Theorem 1.3.15 we obtain the following corollary.

1.3.18 Corollary. *A Witt ring* R *for a group of exponent* 2 *has dimension* 1 *if* R *has characteristic* 0*. Otherwise* R *has dimension* 0*.*

1.4 The structure theorems for Witt rings

We use the notation of the previous section: G is a group of exponent 2, and $J \subset \mathbb{Z}[G]$ is an ideal such that $R := {}^{Z[G]}\!/_{J}$ is a Witt ring for G.

In this section we emulate Lewis' approach in [Lew89] to prove important theorems about Witt rings for groups of exponent 2. More specifically we will use annihilating polynomials to prove generalisations of those results which, in the setting of quadratic forms, are generally known as the structure theorems for Witt rings.

We need to fix some notation and establish a few equalities. Let $x \in \mathbb{Z}[G]$ with $|x| = n \in \mathbb{N}$. Write $x = \varepsilon_1 g_1 + \cdots + \varepsilon_n g_n$ with $\varepsilon_i \in \{-1, 1\}$ and $g_i \in G$. For any vector

$\delta = (\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$ set

$$y_\delta \ := \ \delta_1 + \cdots + \delta_n \qquad \text{and} \qquad \pi_{x,\delta} \ := \ \prod_{i=1}^{n}(1 + \delta_i \varepsilon_i g_i).$$

1.4.1 Lemma. *For any $x \in \mathbb{Z}[G]$ with $|x| = n > 0$ the following equalities hold:*

(1) $x\pi_{\delta,x} = y_\delta \pi_{\delta,x}$ *for any* $\delta = (\delta_1, \ldots, \delta_n) \in \{-1, 1\}^n$*,*

(2) $\displaystyle\sum_{\delta\in\{-1,1\}^n} \pi_{\delta,x} \ = \ 2^n$*,*

(3) $\displaystyle\sum_{\delta\in\{-1,1\}^n} y_\delta \pi_{\delta,x} \ = \ 2^n x$*.*

Proof. (1): We have

$$\begin{aligned} x\pi_{\delta,x} \ &= \ \sum_{j=1}^{n}\left[\varepsilon_j g_j(1 + \delta_j \varepsilon_j g_j)\prod_{i\neq j}(1 + \delta_i \varepsilon_i g_i)\right] \\ &= \ \sum_{j=1}^{n}\left[\delta_j(\delta_j \varepsilon_j g_j + 1)\prod_{i\neq j}(1 + \delta_i \varepsilon_i g_i)\right] \\ &= \ \sum_{j=1}^{n}\delta_j \pi_{\delta,x} \ = \ y_\delta \pi_{\delta,x}. \end{aligned}$$

(2): We proceed by induction on n. For $n = 1$ we have

$$(1 + \varepsilon_1 g_1) + (1 - \varepsilon_1 g_1) \ = \ 2 \ = \ 2^1.$$

Now let $n > 1$, and set $x' = \varepsilon_2 g_2 + \cdots + \varepsilon_n g_n$ and $\delta' = (\delta_2, \ldots, \delta_n)$. Then

$$\begin{aligned} \sum_{\delta\in\{-1,1\}^n} \pi_{\delta,x} \ &= \ \sum_{\delta'\in\{-1,1\}^{n-1}}\left[(1 + \varepsilon_1 g_1)\pi_{\delta',x'} + (1 - \varepsilon_1 g_1)\pi_{\delta',x'}\right] \\ &= \ 2\sum_{\delta'\in\{-1,1\}^{n-1}} \pi_{\delta',x'} \ = \ 2 \cdot 2^{n-1} \ = \ 2^n. \end{aligned}$$

(3): Again we proceed by induction on n. If $n = 1$, then

$$\sum_{\delta\in\{-1,1\}^n} y_\delta \pi_{\delta,x} \ = \ 1 \cdot (1 + \varepsilon_1 g_1) - 1 \cdot (1 - \varepsilon_1 g_1) \ = \ 2\varepsilon_1 g_1 \ = \ 2x.$$

Let $n > 1$. We use the same notation as in the proof of part (2). Then

$$\begin{aligned} \sum_{\delta\in\{-1,1\}^n} y_\delta \pi_{\delta,x} \ &= \ \sum_{\delta'\in\{-1,1\}^{n-1}}\left[(1 + y_{\delta'})(1 + \varepsilon_1 g_1)\pi_{\delta',x'} + (-1 + y_{\delta'})(1 - \varepsilon_1 g_1)\pi_{\delta',x'}\right] \\ &= \ \sum_{\delta'\in\{-1,1\}^{n-1}} (2y_{\delta'}\pi_{\delta',x'} + 2\varepsilon_1 g_1 \pi_{\delta',x'}) \\ &= \ 2 \cdot 2^{n-1}x' + 2 \cdot 2^{n-1}\varepsilon_1 g_1 \ = \ 2^n(\varepsilon_1 g_1 + x') \ = \ 2^n x \end{aligned}$$

by induction and part (2). □

1.4.2 Convention. *Let $R = \mathbb{Z}[G]/J$ be a Witt ring for some group G of exponent 2. Consider the canonical projection $\pi : \mathbb{Z}[G] \to R$. When studying properties of an element $a \in R$ it is often useful to consider one of its preimages via π in $\mathbb{Z}[G]$. Accordingly we will call any element $x \in \mathbb{Z}[G]$ such that $\pi(x) = a$ simply a* preimage *of a.*

For any ring R denote by $\mathrm{zd}(R)$ the set of zero-divisors of R, and denote by $\mathrm{Nil}(R)$ the nilradical of R, i.e. the set of nilpotent elements of R. Here we say that an element $a \in R$ is *torsion*, if there exists some $m \in \mathbb{Z}$ such that $ma = 0$. The torsion subgroup of R will be denoted by R_{tor}.

1.4.3 Lemma. *If R is a Witt ring for a group of exponent 2 with $\mathrm{char}(R) = 0$, then $R_{\mathrm{tor}} \subset \mathrm{Nil}(R)$.*

Proof. Let $a \in R_{\mathrm{tor}}$, $a \neq 0$. Then there exists some $m \in \mathbb{N}$, $m > 1$, such that $ma = 0$. Since $\mathrm{char}(R) = 0$ we know by Corollary 1.3.16 that $\mathrm{Hom}(R, \mathbb{Z}) \neq \varnothing$. Then Theorem 1.3.15 implies that $\overline{m}$ does not lie in any minimal prime ideal $\mathfrak{p}$ of R. Hence $a \in \mathfrak{p}$ for all minimal prime ideals. It follows from Corollary 1.3.5 that $a \in \mathrm{Nil}(R)$. □

1.4.4 Definition. *An element $a \in R$ is called k-fold* Pfister *(respectively k-fold* quasi-Pfister*) if there exists a k-fold Pfister (respectively k-fold quasi-Pfister) element $x \in \mathbb{Z}[G]$ such that x is a preimage of a.*

1.4.5 Proposition. *If $R = \mathbb{Z}[G]/J$ is a Witt ring for a group G of exponent 2, then R has no odd torsion.*

Proof. If $\mathrm{char}(R) \neq 0$, then $\overline{2^l} = 0$ in R for some $l \in \mathbb{N}$. Hence $2^l a = 0$ for all $a \in R$, and R has only 2-torsion.

Next assume that $\mathrm{char}(R) = 0$. Let $a \in R$, $a \neq 0$, be a torsion element, and let $m \in \mathbb{N}$ such that $ma = 0$. By Lemma 1.4.3 we know that $a \in \mathrm{Nil}(R)$. Now let $x = \varepsilon_1 g_1 + \cdots + \varepsilon_n g_n \in \mathbb{Z}[G]$ be a preimage of a with $|x| = n > 0$, $\varepsilon_i \in \{-1, 1\}$, and $g_i \in G$. For any $\delta \in \{-1,1\}^n$ we have $x\pi_{\delta,x} = y_\delta \pi_{\delta,x}$ by Lemma 1.4.1.(1) with $y_\delta = \dim(y_\delta) \in \mathbb{Z}$. Since $\overline{x} = a$ is torsion, the same must be true for $\overline{\pi_{\delta,x}}$. It follows that $\overline{\pi_{\delta,x}}$ is nilpotent. Since $\{-1,1\}^n$ is finite, we can define

$$k \;:=\; \min\left\{ t \in \mathbb{N} \;\middle|\; \overline{\pi_{\delta,x}}^{\,t} = 0 \; \forall\, \delta \in \{1,-1\}^2 \right\}.$$

For all $\delta \in \{-1,1\}^n$ we have $\overline{\pi_{\delta,x}}^{\,k} = 0$. Since $\pi_{\delta,x}$ is Pfister, Corollary 1.2.14 implies that $\pi_{\delta,x}^2 = 2^n \pi_{\delta,x}$. Applying the last equality repeatedly we obtain $2^{(k-1)n}\overline{\pi_{\delta,x}} = 0$. As $2^{kn}x = 2^{(k-1)n} \sum_{\delta \in \{-1,1\}^n} y_\delta \pi_{\delta,x}$ by Lemma 1.4.1.(3), it follows that

$$2^{kn} a \;=\; \sum_{\delta \in \{-1,1\}^n} \overline{y_\delta} \cdot 2^{(k-1)n} \cdot \overline{\pi_{\delta,x}} \;=\; 0,$$

i.e. a has 2-torsion. □

1.4.6 Proposition. *If $R = \mathbb{Z}[G]/J$ is a Witt ring for a group G of exponent 2, then $\mathrm{zd}(R) \subset I(R)$. If $R_{\mathrm{tor}} \neq \{0\}$, then we even have $\mathrm{zd}(R) = I(R)$.*

Proof. Let $a \in R$ such that $a \notin I(R)$. If $x \in \mathbb{Z}[G]$ is a preimage of a, then $n := |x|$ must be odd. By Corollary 1.2.9 the polynomial P_n annihilates x. Hence P_n annihilates a. Assume there exists a $b \in R$ such that $ab = 0$. Note that we must have $a \neq 0$ since $a \notin I(R)$. Of course $P_n(a)b = 0$, where $P_n = (X^2 - 1)(X^2 - 3^2) \cdots (X^2 - n^2)$. Therefore

$$P_n(a)b \;=\; (\underbrace{1 \cdot 3^2 \cdots n^2}_{\text{odd}})b \;=\; 0.$$

The previous proposition implies $b = 0$.

Now assume that $R_{\text{tor}} \neq \{0\}$, then there exists some $b \in R$, $b \neq 0$, such that $2b = 0$. Let $a \in I(R)$. By an analogous reasoning as the one we employed earlier in this proof, there exists some even $n \in \mathbb{N}_0$ such that $P_n = X(X^2 - 2^2) \cdots (X^2 - n^2)$ annihilates a. We have $bP_n(a) = ba^{n+1} = 0$, which shows that a is a zero-divisor. □

We will now have to distinguish between the cases $\text{char}(R) = 0$ and $\text{char}(R) = 2^k$ for some $k \in \mathbb{N}$.

1.4.7 Lemma. *Let R be a Witt ring for a group of exponent 2, and let $a \in I(R)$, then there exists some $b \in R$ such that $a^2 = 2b$.*

Proof. As $a \in I(R)$, there exists an $x \in \mathbb{Z}[G]$ with $n = |x|$ even such that a is the image of x. Write $x = \varepsilon_1 g_1 + \cdots + \varepsilon_n g_n$ with $\varepsilon_i \in \{-1, 1\}$ and $g_i \in G$ for $i = 1, \ldots, n$. Then

$$x^2 \;=\; n + 2\sum_{i<j} \varepsilon_i \varepsilon_j g_i g_j \;=\; 2\underbrace{\left(\frac{n}{2} + \sum_{i<j} \varepsilon_i \varepsilon_j g_i g_j\right)}_{=:y}.$$

If $b \in R$ is the image of y, then $a^2 = 2b$. □

1.4.8 Theorem. *Let R be a Witt ring for a group of exponent 2. Assume that $\text{char}(R) = 2^k$ for some $k \in \mathbb{N}$. Then*

(1) $R^* \;=\; R \setminus I(R)$,

(2) $R_{\text{tor}} \;=\; R$,

(3) $\text{Nil}(R) \;=\; \text{zd}(R) \;=\; I(R)$.

Proof. Since $\text{char}(R) \neq 0$ we know by Corollary 1.3.17 that R is local with maximal ideal $I(R)$. Hence $R^* = R \setminus I(R)$. As $\overline{2^k} = 0$ in R, it follows that $2^k x = 0$ for all $x \in R$. Accordingly $R_{\text{tor}} = R$. By the previous Proposition 1.4.6 this implies that $\text{zd}(R) = I(R)$. Now we obviously have $\text{Nil}(R) \subset \text{zd}(R)$. Let $a \in I(R)$. Then by the previous lemma $a^{2k} = 2^k b^k = 0$ for some $b \in R$. Thus $a \in \text{Nil}(R)$ and $\text{Nil}(R) = \text{zd}(R) = I(R)$. □

1.4.9 Proposition. *Let R be a Witt ring for a group of exponent 2 with $\text{char}(R) = 2^k$ for some $k \in \mathbb{N}$. If $a \in R^*$, then there exists an odd polynomial $P \in \mathbb{Z}[X]$ such that $a^{-1} = P(a)$.*

Proof. As $a \in R^*$, there exists an $x \in \mathbb{Z}[G]$ with $n = |x|$ odd such that a is the image of x. We have $P_n(x) = 0$ with $P_n = (X^2 - 1^2) \cdots (X^n - n^2) \in \mathbb{Z}[X]$. This provides us with elements $z_0, z_2, \cdots, z_{n-1} \in \mathbb{Z}$ such that $P_n = X^{n+1} + z_{n-1}X^{n-1} + \cdots + z_2X^2 + z_0$. Hence $a(a^n + z_{n-1}a^{n-2} + \cdots + z_2a) = -z_0$. Now $z_0 = 1 \cdot 3^2 \cdots n^2$ is odd. Therefore there exists some $m \in \mathbb{Z}$ such that $mz_0 \equiv -1 \pmod{2^k}$. Set

$$P \ := \ m(X^n + z_{n-1}X^{n-2} + \cdots + z_2X).$$

Then $P(a) = a^{-1}$. □

1.4.10 Theorem. *Let R be a Witt ring for a group of exponent* 2*. Assume that* $\mathrm{char}(R) = 0$*. Then*

(1) $R^* \ = \ \{a \in R \mid \chi(a) = \pm 1 \ \forall \, \chi \in \mathrm{Hom}(R, \mathbb{Z})\}$,

(2) $R_{\mathrm{tor}} \ = \ \mathrm{Nil}(R) \ = \ \bigcap_{\chi \in \mathrm{Hom}(R,\mathbb{Z})} \ker(\chi)$.

Proof. (2): By Lemma 1.4.3 we already know that $R_{\mathrm{tor}} \subset \mathrm{Nil}(R)$. Now let $a \in \mathrm{Nil}(R)$, $a \neq 0$. By Proposition 1.4.6 any zero-divisor in R lies in $I(R)$. Thus there exists some even $n \in \mathbb{N}$ such that $P_n = X(X^2 - 2^2) \cdots (X^2 - n^2)$ annihilates a. This implies the existence of integers $z_1, z_3, \ldots, z_{n-1} \in \mathbb{Z}$, $z_1 \neq 0$, such that

$$a^{n+1} + z_{n-1}a^{n-1} + \cdots + z_3a^3 + z_1a \ = \ 0. \tag{1.4}$$

Assume that $a^k = 0$ but $a^{k-1} \neq 0$ for some $k \geq 2$. Multiplying the above equality (1.4) by a^{k-2} results in $z_1a^{k-1} = 0$. If $k \geq 3$ we continue by multiplying equality (1.4) by z_1a^{k-3} to obtain $z_1^2a^{k-2} = 0$. For $k \geq 4$ we multiply equality (1.4) by $z_1^2a^{k-4}$ to obtain $z_1^3a^{k-3} = 0$. If necessary we continue in this fashion. We conclude that there exists some $r \in \mathbb{N}$ with $z_1^ra = 0$. Thus $a \in R_{\mathrm{tor}}$.

We now know that $R_{\mathrm{tor}} = \mathrm{Nil}(R)$, and by Corollary 1.3.5 $\mathrm{Nil}(R)$ equals the intersection of all minimal prime ideals of R. Therefore by Theorem 1.3.15 we have $\mathrm{Nil}(R) = \bigcap_{\chi \in \mathrm{Hom}(R,\mathbb{Z})}$.

(1): Let $a \in R^*$. Then $\chi(aa^{-1}) = 1$ for all $\chi \in \mathrm{Hom}(R, \mathbb{Z})$. Thus we must have $\chi(a) = \pm 1$.

Now let $a \in R$ with $\chi(a) = \pm 1$ for all $\chi \in \mathrm{Hom}(R, \mathbb{Z})$. Then we know by the proof of part (2) that for $P = (X - 1)(X + 1) = (X^2 - 1) \in \mathbb{Z}[X]$ the element $P(a)$ is nilpotent. Hence there exists some $k \in \mathbb{N}$ such that $(a^2 - 1)^k = 0$. In particular there exist elements $z_2, z_4, \ldots, z_{2k-2} \in \mathbb{Z}$ such that

$$(-1)^k \ = \ a^{2k} + z_{2k-2}a^{2k-2} + \cdots + z_2a^2 \ = \ a(a^{2k-1} + z_{2k-2}a^{2k-3} + \cdots + z_2a).$$

Multiplying this equation by $(-1)^k$, we see that there exists an odd polynomial $P \in \mathbb{Z}[X]$ such that $1 = aP(a)$. Thus a is a unit. □

The previous proof contains the proof of the following corollary.

1.4.11 Corollary. *Let R be a Witt ring for a group of exponent* 2 *with* $\mathrm{char}(R) = 0$*, and let $a \in R^*$. Then there exists an odd polynomial $P \in \mathbb{Z}[X]$ such that $a^{-1} = P(a)$.*

1.5 Annihilating polynomials for elements of Witt rings

Let G be a group of exponent 2, and let $J \subset \mathbb{Z}[G]$ be an ideal such that $R := \mathbb{Z}[G]/_J$ is a Witt ring for G. In Section 1.2 we have seen that the annihilating ideal of any element $f \in \mathbb{Z}[G]$ is a principal ideal generated by the signature polynomial P_f as defined in (1.3). As is to be expected the situation in the more general case of Witt rings for G is not quite as simple. We will have to make use of our results about generators for ideals in $\mathbb{Z}[X]$ from Section 1.1 and the structure theorems from the previous Section 1.4 to make specific statements about the structure of annihilating ideals for elements of R.

For any $f \in \mathbb{Z}[G]$ the embracing polynomial Q_{Ann_f} is just the signature polynomial P_f. In the case of an arbitrary Witt ring R for G, the annihilating ideal Ann_x of an element $x \in R$ has more than one generator. We now study the shape of the embracing polynomial Q_{Ann_x} in this general case.

1.5.1 Definition. *Let R be a Witt ring for a group of exponent 2, and let $x \in R$. Analogously to our definition in Section 1.2 we define the* signature set

$$S_x \;:=\; \{\chi(x) \mid \chi \in \mathrm{Hom}(R, \mathbb{Z})\}$$

and the signature polynomial

$$P_x \;:=\; \prod_{\chi(x) \in S_x} (X - \chi(x)).$$

Let $f \in \mathbb{Z}[G]$ be any preimage of an element $x \in R$. Then $S_x \subset S_f$ and S_f is finite. Hence S_x is finite as well, and the signature polynomial P_x in the above definition is well-defined.

While in the general case the signature polynomial will not annihilate an element $x \in R$, it is still possible to generalise the fact that for $f \in \mathbb{Z}[G]$ we have $Q_{\mathrm{Ann}_f} = P_f$. In fact the same equality holds in the more general setting of Witt rings.

1.5.2 Proposition. *Let R be a Witt ring for a group G of exponent 2, and let $x \in R$. Then $Q_{\mathrm{Ann}_x} = P_x$, and there exists some $k \in \mathbb{N}_0$ such that $2^k P_x \in \mathrm{Ann}_x$.*

Proof. By Corollary 1.1.9 there exists some $m \in \mathbb{N}$ such that $mQ_{\mathrm{Ann}_x} \in \mathrm{Ann}_x$. This implies that $Q_{\mathrm{Ann}_x}(x)$ is torsion. By Proposition 1.4.5 there exists some $k \in \mathbb{N}_0$ such that $2^k Q_{\mathrm{Ann}_x} \in \mathrm{Ann}_x$. Let $f \in \mathbb{Z}[G]$ be a preimage of x. Then $P_f \in \mathrm{Ann}_x$. In particular it follows that Q_{Ann_x} divides P_f. Now P_f is monic and a product of linear factors, it follows that Q_{Ann_x} is monic and a product of linear factors as well.

Now consider the signature polynomial P_x. If $\mathrm{char}(R) \neq 0$, then by Proposition 1.3.16 we have $\mathrm{Hom}(R, \mathbb{Z}) = \varnothing$. In this case $2^l \in \mathrm{Ann}_x$ for some $l \in \mathbb{N}$. Since Q_{Ann_x} is monic, it follows that $Q_{\mathrm{Ann}_x} = 1$. As $\mathrm{Hom}(R, \mathbb{Z}) = \varnothing$, and since by definition the empty product is 1, we obtain $P_x = 1 = Q_{\mathrm{Ann}_x}$.

Next assume that $\mathrm{char}(R) = 0$. By definition we have $\chi(P_x(x)) = P_x(\chi(x)) = 0$ for all $\chi \in \mathrm{Hom}(R, \mathbb{Z})$. Theorem 1.4.10 states that $R_{\mathrm{tor}} = \bigcap_{\chi \in \mathrm{Hom}(R,\mathbb{Z})} \ker(\chi)$. This implies that $P_x(x)$ is torsion. Thus there exists some $l \in \mathbb{N}_0$ such that $2^l P_x \in \mathrm{Ann}_x$. Now the monic polynomial Q_{Ann_x} divides $2^l P_x$. Hence Q_{Ann_x} must divide P_x. Since $Q_{\mathrm{Ann}_x}(x) \in R_{\mathrm{tor}}$, we must also have $Q_{\mathrm{Ann}_x}(\chi(x)) = \chi(Q_{\mathrm{Ann}_x}(x)) = 0$ for all $\chi \in \mathrm{Hom}(R, \mathbb{Z})$. We deduce that $X - \chi(x)$ divides Q_{Ann_x} for all $\chi \in \mathrm{Hom}(R, \mathbb{Z})$. Thus P_x divides Q_{Ann_x}, and we obtain $P_x = Q_{\mathrm{Ann}_x}$. □

The previous result, together with the fact that a Witt ring R for a group of exponent 2 only has 2-torsion, gives us the following description of convenient sets of generators for annihilating ideals of elements of R.

1.5.3 Theorem. *Let R be a Witt ring for a group of exponent 2, and let $x \in R$. There exists a unique $s \in \mathbb{N}_0$, monic polynomials $Q_0, \dots, Q_s \in \mathbb{Z}[X]$, and a sequence of natural numbers $k_0, k_1, \dots, k_{s-1}, k_s \in \mathbb{N}$ such that*

(a) $\deg(Q_d) = d$ *for* $d = 0, \dots, s$, *and* $Q_0 = 1$,

(b) $k_0 \geq k_1 \geq \cdots \geq k_{s-1} > k_s = 0$, *and*

(c) $\left\{2^{k_d} Q_d P_x \mid d = 0, \dots, s\right\}$ *is a convenient set of generators for* Ann_x.

In particular

$$\mathrm{Ann}_x \;=\; (2^{k_0} P_x, 2^{k_1} Q_1 P_x, \dots, 2^{k_{s-1}} Q_{s-1} P_x, Q_s P_x).$$

1.5.4 Corollary. *Let R be a Witt ring for a group of exponent 2. Assume that R is torsion-free. If $x \in R$, then*

$$\mathrm{Ann}_x \;=\; (P_x).$$

Naturally we are also interested in a simple description of modest sets of generators for annihilating ideals of elements of R. Consider an element $x \in R$, a polynomial $P \in \mathbb{Z}[X]$, and a minimal $k \in \mathbb{N}_0$ such that $2^k P \in \mathrm{Ann}_x$. Assume that $k > 0$. A consequence of Lemma 1.4.7 is that there exists an $l \in \mathbb{N}_0$ with $l < k$ such that $2^l X^2 P \in \mathrm{Ann}_x$ if $x \in I(R)$ and $2^l (X-1)^2 P \in \mathrm{Ann}_x$ if $x \in R \setminus I(R)$. Taking into account this observation and Corollary 1.1.18 we obtain the following special case of Proposition 1.1.13.

1.5.5 Theorem. *Let R be a Witt ring for a group of exponent 2, and let $x \in R$. There exists a unique $r \in \mathbb{N}_0$, monic polynomials $P_0, \dots, P_r \in \mathbb{Z}[X]$, and a sequence of natural numbers $l_0, \dots, l_r \in \mathbb{N}$ such that*

(1) $\deg(P_i) - \deg(P_{i-1}) \in \{1, 2\}$ *for* $i = 1, \dots, r$, *and* $P_0 = 1$,

(2) $l_0 > l_1 > \cdots > l_{r-1} > l_r = 0$, *and*

(3) $\mathcal{M} := \left\{2^{l_i} P_i P_x \mid i = 0, \dots, r\right\}$ *is a modest set of generators for* Ann_x.

In particular, if in addition we assume for $i = 1, \dots, r$ that $P_i = F_i P_{i-1}$ with some product of linear factors $F_i \in \mathbb{Z}[X]$, then $\mathcal{M}$ is a minimal set of generators for I.

Chapter 2

Annihilating Polynomials for Quadratic Forms

This chapter is dedicated to the study of annihilating polynomials for quadratic forms. More specifically we study the annihilating ideal, i.e. the ideal in $\mathbb{Z}[X]$ consisting of all annihilating polynomials, for the isometry class and the equivalence class of a given quadratic form over a field K. We will make heavy use of the observations made in Chapter 1.

The first three sections serve as an introduction to the algebraic theory of quadratic forms. We introduce the definitions and quote, mostly without proof, the results that will be needed in the later sections. In Section 2.1 we introduce quadratic forms over fields and their algebraic properties. We define the Witt-Grothendieck ring and the Witt ring of a field K, and we show that these rings are Witt rings for the square class group of K. The study of quadratic forms is closely related to the theory of quaternion algebras. Therefore, in Section 2.2, we introduce the Brauer group and important results about quaternion algebras. Section 2.3 covers the first three cohomological invariants of quadratic forms, i.e. the dimension index, the discriminant, and the Clifford invariant. In particular we define the Clifford invariant exclusively by using quaternion algebras.

In Section 2.4 we first adapt our observations about annihilating ideals for elements of Witt rings for groups of exponent 2 from Section 1.5 to the setting of quadratic forms. We continue by applying the obtained results to the special case of fields K, for which the third power of the fundamental ideal $I(K)$ vanishes. Over such a field K quadratic forms can be classified with the help of the first three cohomological invariants. Calculations involving those invariants can then be used to classify annihilating ideals for quadratic forms over K. In particular this holds over local fields, which are considered in Section 2.5. By applying the Hasse-Minkowski Theorem we can then classify annihilating ideals for quadratic forms over global fields.

Section 2.6 contains an introduction to the elementary theory of generic splitting of quadratic forms. We define generic splitting towers and quote important results on generic splitting. In particular we introduce Pfister neighbours and excellent forms, which can be characterised using generic splitting. Those two classes of quadratic forms will be the subjects of study in Section 2.7. By using methods from generic splitting we construct certain annihilating polynomials for Pfister neighbours and excellent forms. We conclude the section by using elementary methods to give an alternative approach to the construction of annihilating polynomials for excellent forms.

2.1 Quadratic forms

From now on we will assume that K is a field of characteristic unequal to 2.

In this section we introduce the algebraic theory of quadratic forms. We define quadratic spaces over a field K, and we show how the study of quadratic spaces is closely related to the study of

(a) symmetric K-bilinear forms,

(b) symmetric matrices with coefficients in K,

(c) quadratic forms, i.e. homogeneous polynomials of degree 2 with coefficients in K.

Knowing the relations between those classes of objects helps understanding different properties of quadratic forms and quadratic spaces. First we focus on the geometric properties of quadratic forms. We introduce a number of necessary notions and important results. In particular we quote Witt's cancellation theorem and Witt's decomposition theorem. These two theorems form the basis for the algebraic theory of quadratic forms. They make possible the introduction of the Witt-Grothendieck ring and the Witt ring, which are both Witt rings for the square class group of K. Accordingly we can translate our results from Section 1.4 to the specific setting of quadratic forms.

2.1.1 Definition. *Let V be a finite-dimensional K-vector space. A* quadratic map *over K is a map*

$$\varphi : \quad V \longrightarrow K,$$

such that

$$b_\varphi : \quad V \times V \longrightarrow K, \quad (v,w) \longmapsto \frac{1}{2}(\varphi(v+w) - \varphi(v) - \varphi(w))$$

is a symmetric K-bilinear form. The tuple (V,φ) is called a quadratic space. *We define the* dimension *of (V,φ) as $\dim(V,\varphi) := \dim_K(V) = n$. Usually we just write $\dim(\varphi) := n$.*

There exists a unique 0-dimensional quadratic space over K. It is given by $(\{0\}, 0)$, where $0 : \{0\} \to K$ is just the zero map.

Let V be a finite-dimensional K-vector space, and let $b : V \times V \to K$ be a symmetric K-bilinear form. Then clearly

$$\varphi_b : \quad V \longrightarrow K, \quad v \longmapsto b(v,v),$$

is a quadratic map, and we have $b_{\varphi_b} = b$. If on the other hand $\varphi : V \to K$ is a quadratic map over K, then $\varphi_{b_\varphi} = \varphi$. Thus we see that over fields of characteristic unequal to 2 quadratic maps and symmetric bilinear forms are in one-to-one correspondence. Over fields of characteristic 2 this does not hold any more. It becomes clear from the definition of a quadratic map, that over fields with characteristic 2 is is necessary to define quadratic maps differently and then study quadratic maps and symmetric bilinear forms separately. For more details see for example [Pfi95, §4, Chapter 1].

2.1.2 Definition. *Two quadratic spaces* (V,φ) *and* (W,ψ) *over* K *are* isometric *if there exists a* K*-vector space isomorphism* $T : V \to W$ *such that*

$$\varphi(v) \;=\; \psi(Tv) \qquad \textit{for all } v \in V.$$

The isomorphism T *is called an* isometry. *We write* $(V,\varphi) \cong (W,\psi)$ *or simply* $\varphi \cong \psi$.

2.1.3 Remark. Let (V,φ) and (W,ψ) be quadratic spaces over K, and let $T : V \to W$ be K-vector space isomorphism. From the definition of b_φ and b_ψ it follows immediately, that T is an isometry if and only if $b_\varphi(v,w) = b_\psi(Tv,Tw)$ for all $v,w \in V$. △

Let V be a K-vector space with $n = \dim_K(V)$, and let $\mathcal{B} = \{v_1,\ldots,v_n\}$ be a K-basis of V. If $\varphi : V \to K$ is a quadratic map, then we can associate to φ a symmetric matrix

$$A_{\varphi,\mathcal{B}} \;:=\; (b_\varphi(v_i,v_j))_{i,j=1,\ldots,n} \;\in\; \mathbb{M}_n(K).$$

If it is clear from the context which basis of V we consider, we will simply write $A_\varphi := A_{\varphi,\mathcal{B}}$.

Denote by $\{e_1,\ldots,e_n\}$ the standard basis of the K-vector space K^n. We can define a K-vector space isomorphism $T : V \to K^n$ by $v_i \mapsto e_i$. Then $(V,\varphi) \cong (K^n,\psi)$, where $\psi(x) = x^t A_{\varphi,\mathcal{B}} x$ for all $x \in K^n$. In particular this shows that in most situations it suffices to consider quadratic maps on vector spaces of the form K^n.

If we are given a symmetric matrix $A \in \mathbb{M}_n(K)$, then A defines a quadratic map

$$\varphi_A : \quad K^n \longrightarrow K, \quad x \longmapsto x^t A x.$$

Clearly $b_{\varphi_A}(x,y) = x^t A y$. Furthermore A induces a quadratic map $\rho : V \to K$ defined by $v_i \mapsto \varphi_A(Tv_i)$. In this situation $A_{\rho,\mathcal{B}} = A$. Thus we see that we can easily fall back on considering symmetric matrices while studying quadratic spaces.

Traditionally a *quadratic form* over K of dimension $n \in \mathbb{N}_0$ is a homogeneous polynomial $\sum_{i,j=1}^n a_{i,j}X_iX_j \in K[X_1,\ldots,X_n]$ of degree 2. Note that the dimension is an integral part of the definition of a quadratic form. For example $X_1^2 \in K[X_1,X_2,X_3]$ is a quadratic form of dimension 3. The reason for this will become apparent immediately. If $P \in K[X_1,\ldots,X_n]$ is a quadratic form of dimension n, then P induces a quadratic map

$$\varphi_P : \quad K^n \longrightarrow K, \quad x = (x_1,\ldots,x_n)^t \longmapsto P(x) = \sum_{i,j=1}^n a_{i,j}x_ix_j.$$

We notice that the polynomial P does not uniquely determine the coefficients $a_{i,j}$. But if we set $b_{i,j} := \frac{1}{2}(a_{i,j}+a_{j,i})$ and $P' := \sum_{i,j=1} b_{i,j}X_iX_j \in K[X_1,\ldots,X_n]$, then $P' = P$ and the matrix $B := (b_{i,j})_{i,j=1,\ldots,n} \in \mathbb{M}_n(K)$ is symmetric. In fact, every symmetric matrix $C = (c_{i,j})_{i,j=1,\ldots,n} \in \mathbb{M}_n(K)$ such that $\sum_{i,j}^n c_{i,j}X_iX_j = P$ must be equal to B. Thus the matrix

$$A_P \;:=\; \left(\frac{1}{2}(a_{i,j}+a_{j,i})\right)_{i,j=1,\ldots,n} \;\in\; \mathbb{M}_n(K)$$

is uniquely determined by P.

Now let (V,φ) be a quadratic space of dimension n over K, and let $\mathcal{B}=\{v_1,\dots,v_n\}$ be a K-basis of V. Then φ defines a quadratic form

$$P_{\varphi,\mathcal{B}} \;:=\; \sum_{i,j=1}^{n} a_{i,j}X_iX_j \;\in\; K[X_1,\dots,X_n], \qquad \text{with } A_{\varphi,\mathcal{B}}=(a_{i,j})_{i,j=1,\dots,n}.$$

Again, when there can be no doubt about the K-basis of V, we simply write $P_\varphi := P_{\varphi,\mathcal{B}}$. It follows that $P_{\varphi_P,\mathcal{S}}=P$, where $\mathcal{S}$ is the standard basis of the K-vector space K^n. We see that the inclusion of the dimension in the definition of a quadratic form makes it possible to construct the above correspondence between quadratic forms and quadratic spaces. Hence, to study quadratic forms, it suffices to study quadratic spaces. In fact many of the important results about quadratic forms can be proven without ever considering polynomials.

2.1.4 Convention. *Henceforth, when we use the term* quadratic form*, we usually understand it to be a quadratic space.*

2.1.5 Definition. *Let (V,φ) be a quadratic form over K.*

(1) Two vectors $v,w\in V$ are called orthogonal *if $b_\varphi(v,w)=0$. We write $v\perp w$.*

(2) Let $U\subset V$ be a K-subvector space. The orthogonal complement *of $U\subset V$ is defined as*

$$U^\perp \;:=\; \{v\in V \mid v\perp u \;\forall\, u\in U\}.$$

(3) A K-subvector space $U\subset V$ is called orthogonal summand *of V if there exists a K-subvector space $W\subset V$ such that $V=U\oplus W$ and $u\perp w$ for all $u\in U$ and $w\in W$. In this case we use the notation*

$$V \;=\; U\perp W \;:=\; U\oplus W.$$

We call $U\perp W$ the orthogonal sum *of U and W.*

Let (V,φ) be a quadratic form over K, and let $V=U\perp W$ with K-subvector spaces $U,W\subset V$. Let $\varphi|_U$ (respectively $\varphi|_W$) be the quadratic form φ restricted to U (respectively W). Since $u\perp w$ for all $u\in U$ and $w\in W$ we have

$$b_\varphi(u_1+w_1,u_2+w_2) \;=\; b_\varphi(u_1,u_2)+b_\varphi(w_1,w_2) \qquad \forall\, u_1,u_2\in U,\ w_1,w_2\in W.$$

In particular $\varphi(u+w)=\varphi|_U(u)+\varphi|_W(w)$ for all $u\in U$ and $w\in W$. Thus we can write $\varphi=\varphi|_U+\varphi|_W$. This shows: A decomposition of V as an orthogonal sum implies the decomposition of φ as a sum of quadratic maps.

2.1.6 Definition. *Let (V,φ) be a quadratic form over K.*

(1) We say that φ represents *an element $a\in K$, if there exists some $v\in V$, $v\neq 0$, such that $\varphi(v)=a$.*

(2) Define the set

$$D_K(\varphi) \;:=\; \{a\in K \mid a=\varphi(v),\ v\in V,\ v\neq 0\}$$

of all elements represented by φ over K. Set $D_K^*(\varphi):=D_K(\varphi)\setminus\{0\}$.

(3) The quadratic map φ is called universal *if $D_K^*(\varphi) = K^*$.*

2.1.7 Definition. *Let (V, φ) be a quadratic form over K. A K-basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V is called an* orthogonal basis *of (V, φ) if we have*

$$b_\varphi(v_i, v_j) \; = \; 0 \qquad \forall\, i, j \in \{1, \dots, n\} \textit{ with } i \neq j.$$

2.1.8 Proposition. *For every n-dimensional quadratic form (V, φ) over K there exists an orthogonal basis $\{v_1, \dots, v_n\}$. In particular, if there exists some $a \in D_K^*(\varphi)$, then $v_1 \in V$ can be chosen such that $\varphi(v_1) = a$.*
[Sch85, Theorem 3.5, Chapter 1]

2.1.9 Notation. *Let $a_1, \dots, a_n \in K$, and let $A := \operatorname{diag}(a_1, \dots, a_n) \in \mathbb{M}_n(K)$ be the diagonal matrix with entries $a_1, \dots, a_n$. We define the notation*

$$\langle a_1, \dots, a_n \rangle \; := \; (K^n, \varphi_A),$$

and we call $\langle a_1, \dots, a_n \rangle$ a diagonal form.

2.1.10 Corollary. *If (V, φ) is an n-dimensional quadratic form over K, then there exist $a_1, \dots, a_n \in K$ such that*

$$(V, \varphi) \; \cong \; \langle a_1, \dots, a_n \rangle.$$

In particular, if there exists some $a \in D_K(\varphi)^*$, then we can choose $a_1 = a$.

In the notation that we have just introduced we do not exclude the case that $a_i = 0$ for some $i \in \{0, \dots, n\}$. In the following we further investigate this case.

2.1.11 Definition. *Let (V, φ) be a quadratic form over K.*

(1) The subvector space

$$\operatorname{Rad}(\varphi) \; := \; V^\perp \; = \; \{v \in V \mid v \perp w \; \forall\, w \in V\} \; \subset \; V$$

is called the radical *of φ.*

(2) The quadratic form (V, φ) is called regular *if $\operatorname{Rad}(\varphi) = \{0\}$.*

2.1.12 Proposition. *Let (V, φ) be a quadratic form over K. Then we can write $V = U \perp \operatorname{Rad}(\varphi)$ and $\varphi = \varphi|_U + \varphi|_{\operatorname{Rad}(\varphi)}$, where $(U, \varphi|_U)$ is regular and $\varphi|_{\operatorname{Rad}(\varphi)} = 0$. The K-sub vector space $U \subset V$ is unique up to isometry, i.e. if $V = W \perp \operatorname{Rad}(\varphi)$ then $(U, \varphi|_U) \cong (W, \varphi|_W)$.*
[Sch85, Theorem 3.8, Chapter 1]

Let (V, φ) be an n-dimensional quadratic form over K, and let $V = U \perp \operatorname{Rad}(\varphi)$ for some K-subvector space $U \subset V$. Consider a diagonal basis $\{v_1, \dots, v_r\}$ of $(U, \varphi|_U)$. Then for all $i \in \{1, \dots, r\}$ we must have $\varphi(a_i) \in K^*$, since otherwise $b_{\varphi|_U}(v_i, v_j) = 0$ for all $j \in \{1, \dots, r\}$. This would mean that $(U, \varphi|_U)$ was not regular, which by the previous proposition is impossible. Now any basis $\{w_1, \ldots, w_s\}$ of $\mathrm{Rad}(\varphi)$ is an orthogonal basis of $(\mathrm{Rad}(\varphi), \varphi|_{\mathrm{Rad}(\varphi)})$ with $\varphi(w_i) = 0$ for $i = 1, \ldots, s$. We conclude that

$$(V, \varphi) \;\cong\; \langle a_1, \ldots, a_r, \underbrace{0, \ldots, 0}_{s\text{-times}} \rangle.$$

In particular a diagonal form $\langle b_1, \ldots, b_m \rangle$ over K is regular if and only if $b_1, \ldots, b_m \in K^*$.

2.1.13 Definition. *Let (V, φ) and (W, ψ) be quadratic forms over K. We define the* orthogonal sum *of (V, φ) and (W, ψ) by*

$$(V, \varphi)\perp(W, \psi) \;:=\; (V \times W, \varphi\perp\psi)$$

with $(\varphi\perp\psi)(v, w) = \varphi(v) + \psi(w)$ for all $v \in V$ and $w \in W$.

Let (V, φ) be a quadratic form over K, and let $U, W \subset V$ be K-subvector spaces such that $V = U\perp W$. Then we have seen that $(V, \varphi) \cong (U, \varphi|_U)\perp(W, \varphi|_W)$. In particular, if $(V, \varphi) = \langle a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in K$, then

$$\langle a_1, \ldots, a_n \rangle \cong \langle a_1 \rangle\perp \ldots \perp\langle a_n \rangle.$$

By definition of the radical we know that φ restricted to $\mathrm{Rad}(\varphi)$ is identically 0. Since we can write V as the orthogonal sum of $\mathrm{Rad}(\varphi)$ and a K-subvector space $U \subset V$ such that $(U, \varphi|_U)$ is regular and unique up to isometry, we see that $\mathrm{Rad}(\varphi)$ does not carry any significant geometric information about φ. On the other hand any quadratic form over K is isometric to the orthogonal sum of a regular quadratic form over K and a quadratic form $(W, 0)$, where W is a K-vector space. Thus it suffices to study regular quadratic forms.

2.1.14 Convention. *Henceforth we only consider regular quadratic forms. Thus when we use the term* quadratic form *we understand it to be a regular quadratic form. Furthermore, if (V, φ) is a quadratic form, then we will often omit the vector space V.*

2.1.15 Definition. *A quadratic form (V, φ) over K is called* isotropic *if $0 \in D_K(\varphi)$, i.e. if there exists a vector $v \in V$, $v \neq 0$, such that $\varphi(v) = 0$. Otherwise (V, φ) is called* anisotropic.

2.1.16 Proposition. *Up to isometry there exists exactly one isotropic quadratic form of dimension 2 over K, i.e. (K^2, φ) with $\varphi((x_1, x_2)^t) = x_1x_2$ for $x_1, x_2 \in K$. Furthermore*

$$(K^2, \varphi) \;\cong\; \langle 1, -1 \rangle \;\cong\; \langle a, -a \rangle \qquad \forall\, a \in K^*.$$

[Lam05, Theorem 3.2, Chapter 1]

2.1.17 Definition. *Any isotropic, 2-dimensional quadratic form over K is called a* hyperbolic plane. *We use the notation $\mathbb{H} := \langle 1, -1 \rangle$.*

2.1.18 Proposition. *If (V, φ) is an n-dimensional, isotropic quadratic form over K, then there exists an $(n-2)$-dimensional quadratic form (W, ψ) over K such that*

$$(V, \varphi) \;\cong\; \mathbb{H}\perp(W, \psi).$$

[Pfi95, Proposition 1.11, Chapter 1]

2.1.19 Corollary. *Every isotropic quadratic form over K is universal.*

We need to fix the following notation: For a quadratic form φ over K and any $n \in \mathbb{N}_0$ set

$$n \times \varphi \ := \ \underbrace{\varphi \perp \ldots \perp \varphi}_{n\text{-times}}.$$

Naturally, for $n = 0$, the form $0 \times \varphi$ is simply the 0-dimensional quadratic form.

2.1.20 Definition. *A quadratic form φ over K is* hyperbolic *if there exists some $m \in \mathbb{N}_0$ such that $\varphi \cong m \times \mathbb{H}$.*

The following two theorems form the basis for the algebraic theory of quadratic forms. The first is Witt's cancellation theorem, which states that cancellation holds for the orthogonal sum.

2.1.21 Theorem (Witt's cancellation theorem)**.** *Let φ, ψ_1, ψ_2 be quadratic forms over K. If $\varphi \perp \psi_1 \cong \varphi \perp \psi_2$, then $\psi_1 \cong \psi_2$.*
[Lam05, Theorem 4.1, Chapter 1]

By repeatedly applying Proposition 2.1.18 and then using Witt cancellation, we obtain Witt decomposition.

2.1.22 Theorem (Witt's decomposition theorem)**.** *Let φ be a quadratic form over K. Then there exists an $i(\varphi) \in \mathbb{N}_0$ and an anisotropic quadratic form φ_{an} over K such that*

$$\varphi \ \cong \ \varphi_{\text{an}} \perp (i(\varphi) \times \mathbb{H}).$$

The natural number $i(\varphi)$ is unique, and the quadratic form φ_{an} is unique up to isometry.
[Lam05, Theorem 4.1, Chapter 1]

2.1.23 Definition. *Let φ be a quadratic form over K, and let $\varphi \cong \varphi_{\text{an}} \perp (i(\varphi) \times \mathbb{H})$ be the decomposition from the previous theorem. Then φ_{an} is called the* anisotropic kernel *of φ, and $i(\varphi)$ is called the* Witt index *of φ.*

The Witt ring of a field

It is clear that isometry of quadratic forms is an equivalence relation. For a quadratic form φ over K, denote by $[\varphi]$ its isometry class. Denote by

$$\widehat{W}^+(K) \ := \ \{[\varphi] \mid \varphi \text{ is a quadratic form over } K\}$$

the set of isometry classes of quadratic forms over K. It is clear that the orthogonal sum of quadratic forms induces an addition on $\widehat{W}^+(K)$ by

$$[\varphi] + [\psi] \ := \ [\varphi \perp \psi] \, .$$

The neutral element with respect to this addition is the isometry class $[0]$ of the 0-dimensional quadratic form.

2.1.24 Definition. *Let (V,φ) and (W,ψ) be quadratic forms over K. We define the* tensor product *$(V\otimes_K W, \varphi\otimes\psi)$ of (V,φ) and (W,ψ) by setting*

$$b_{\varphi\otimes\psi}(v_1\otimes w_1, v_2\otimes w_2) \;:=\; b_\varphi(v_1,v_2)b_\psi(w_1,w_2) \qquad \forall\, v_1,v_2\in V,\, w_1,w_2\in W.$$

Then $(\varphi\otimes\psi)(v\otimes w)=\varphi(v)\psi(w)$ for all $v\in V$ and $w\in W$.

What does the tensor product look like for diagonal forms? Let $\varphi=\langle a_1,\dots,a_n\rangle$ and $\psi=\langle b_1,\dots,b_m\rangle$ with $n,m\in\mathbb{N}_0$ and $a_i,b_j\in K^*$. Denote by $\{e_1,\dots,e_n\}$ (respectively $\{f_1,\dots,f_m\}$) the standard basis of K^n (respectively K^m). We have

$$\begin{aligned} b_{\varphi\otimes\psi}(e_{i_1}\otimes f_{j_1}, e_{i_2}\otimes f_{j_2}) &= b_\varphi(e_{i_1},e_{i_2})b_\psi(f_{j_1},f_{j_2}) \\ &= \begin{cases} \varphi(e_{i_1})\psi(f_{j_1}) & \text{if } i_2=i_1 \text{ and } j_2=j_1, \\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

This shows that $\{e_i\otimes f_j \mid i=1,\dots,n,\ j=1,\dots,m\}$ is an orthogonal basis of the tensor product $(K^n\otimes_K K^m, \varphi\otimes\psi)$, and

$$\varphi\otimes\psi \;\cong\; \langle a_1b_1,\dots,a_1b_m,a_2b_1,\dots,a_nb_m\rangle.$$

From the properties of the usual tensor product we deduce that the tensor product of quadratic forms defines a multiplication

$$[\varphi]\cdot[\psi] \;:=\; [\varphi\otimes\psi]$$

on $\widehat{W}^+(K)$, which is associative, commutative, and distributes over the addition in $\widehat{W}^+(K)$. The neutral element with respect to this multiplication is the isometry class of the quadratic form $(K,\langle 1\rangle)$.

2.1.25 Definition. *By applying the Grothendieck construction to the semi-ring $\widehat{W}^+(K)$ we obtain the* Witt-Grothendieck ring *$\widehat{W}(K)$ of K.*

The elements of $\widehat{W}(K)$ are formal differences $[\varphi]-[\psi]$ with $[\varphi],[\psi]\in\widehat{W}^+(K)$. It follows from Witt's decomposition theorem that for every $[\varphi]-[\psi]\in\widehat{W}(K)$ there exists a unique $m\in\mathbb{Z}$ and an up to isometry unique anisotropic quadratic form χ over K such that

$$[\varphi]-[\psi] \;=\; [\chi]+m\,[\mathbb{H}]\,. \tag{2.1}$$

It can be shown that for any quadratic form φ over K we have $\varphi\otimes\mathbb{H}\cong\dim(\varphi)\times\mathbb{H}$. In particular, if ψ is a hyperbolic quadratic form over K, then $\varphi\otimes\psi$ is hyperbolic. This shows that the isometry classes of hyperbolic quadratic forms over K form an ideal in $\widehat{W}(K)$. More specifically, this ideal is the principal ideal generated by $[\mathbb{H}]$.

2.1.26 Definition. *The quotient ring*

$$W(K) \;:=\; \widehat{W}(K)/([\mathbb{H}]),$$

where $([\mathbb{H}])$ denotes the principal ideal generated by the isometry class of the hyperbolic plane $\mathbb{H}$, is called the Witt ring *of K. For a quadratic form φ over K, we denote by $\{\varphi\}$ its class in $W(K)$. If ψ is a quadratic form over K with $\{\varphi\}=\{\psi\}$ then φ and ψ are called* equivalent, *and we write $\varphi\sim\psi$.*

If follows from (2.1) that every equivalence class $\{\varphi\} \in W(K)$ contains up to isometry exactly one anisotropic quadratic form over K. Thus $W(K)$ classifies anisotropic quadratic forms over K.

Before we treat a few examples, we note that for $a_1, \ldots, a_n \in K^*$ and $b_1, \ldots, b_n \in K^*$ we have

$$\langle a_1, \ldots, a_n\rangle \;\cong\; \langle b_1^2 a_1, \ldots, b_n^2 a_n\rangle.$$

In other words, the entries of a diagonal form only matter up to squares. Let $\mathcal{G}(K) := K^*/(K^*)^2$ be the *square class group* of K. For $a \in K^*$ denote by $\overline{a}$ its image in $\mathcal{G}(K)$. By our observations, in situations where we are interested in quadratic forms only up to isometry, we can allow the notation

$$\langle \overline{a_1}, \ldots, \overline{a_n}\rangle.$$

Now consider two n-dimensional quadratic forms $(V, \varphi) \cong (W, \psi)$ over K. Assume that $A_{\varphi,\mathcal{B}}, A_{\psi,\mathcal{C}} \in \mathbb{M}_n(K)$ are the matrices associated to φ and ψ with respect to a basis $\mathcal{B}$ of V and a basis $\mathcal{C}$ of W. Since φ and ψ are isometric there exists a matrix $T \in \mathbb{M}_n(K)$ such that $A_{\varphi,\mathcal{B}} = T^t A_{\psi,\mathcal{B}} T$. In other words the matrices associated to φ and ψ are congruent. This implies that $\det(A_{\varphi,\mathcal{B}}) = \det(A_{\psi,\mathcal{C}})\lambda^2$ for some $\lambda \in K^*$.

For an n-dimensional quadratic form φ over K we define the *determinant*

$$\det(\varphi) \;:=\; \overline{\det(A_{\varphi,\mathcal{B}})} \;\in\; \mathcal{G}(K).$$

In particular, if $\varphi \cong \langle a_1, \ldots, a_n\rangle$ with $a_1, \ldots, a_n \in K^*$, then $\det(\varphi) = \overline{a_1 \cdots a_n}$. By our observations the determinant is well-defined and invariant under isometry. Furthermore, if ψ is another quadratic form over K, then, by using diagonal forms, we can easily check that $\det(\varphi \perp \psi) = \det(\varphi)\det(\psi)$.

2.1.27 Lemma. *Let φ be an n-dimensional quadratic form over K with $n > 0$. If ψ is a quadratic form of dimension $n-1$ over K such that there exists a $d \in K^*$ with $\psi \perp \langle d\rangle \cong \varphi$, then $\overline{d} = \det(\psi)\det(\varphi)$.*

Proof. Since the determinant is invariant under isometry, it follows that $\det(\varphi) = \det(\psi) \cdot \overline{d}$. As $\mathcal{G}(K)$ has exponent 2 we obtain $\overline{d} = \det(\varphi)\det(\psi)$. □

2.1.28 Examples.

(1) Let $K = \mathbb{R}$. The square class group of $\mathbb{R}$ is $\{\overline{1}, \overline{-1}\}$. Hence any quadratic form φ over $\mathbb{R}$ is isometric to $(r \times \langle 1\rangle) \perp (s \times \langle -1\rangle)$ for some $r, s \in \mathbb{N}_0$. It follows that $1 = [\langle 1\rangle]$ and $[\langle -1\rangle]$ generate $\widehat{W}(\mathbb{R})$ as a group. As $[\langle -1\rangle]^2 = 1$, it follows that $\widehat{W}(\mathbb{R}) \cong \mathbb{Z}[\mathcal{G}(\mathbb{R})]$. Furthermore we note that φ is anisotropic if and only if $r = 0$ or $s = 0$. Since $W(\mathbb{R})$ classifies the anisotropic quadratic forms over $\mathbb{R}$, and since $\{\langle 1\rangle\} + \{\langle -1\rangle\} = 0$, we obtain $W(\mathbb{R}) \cong \mathbb{Z}$.

(2) Consider the field $K = \mathbb{C}$. The square class group of $\mathbb{C}$ is trivial, which implies that any quadratic form φ over $\mathbb{C}$ is isometric to $n \times \langle 1\rangle$, where $n = \dim(\varphi)$. For the Witt-Grothendieck ring we thus obtain $\widehat{W}(\mathbb{C}) \cong \mathbb{Z}$. Now, up to isometry, there exist exactly

2 anisotropic quadratic forms over $\mathbb{C}$, i.e. the 0-dimensional quadratic form and $\langle 1\rangle$. As $\{\langle 1\rangle\} + \{\langle 1\rangle\} = \{\langle 1, -1\rangle\} = 0$, it follows that $W(\mathbb{C}) \cong \mathbb{Z}/2\mathbb{Z}$.

Note that the above observations hold if more generally K is an algebraically closed field.

(3) Let $K = \mathbb{F}_q$ be a finite field, where q is an odd prime power. It is well-known that $\mathcal{G}(\mathbb{F}_q) = \{\overline{1}, \overline{s}\}$, where $s \in \mathbb{F}_q^*$ is not a square. We have to distinguish two cases.

(a) Assume first that $q \equiv 1 \pmod 4$. Then -1 is a square in $\mathbb{F}_q$. In particular $\langle 1, 1\rangle \sim 0$ over $\mathbb{F}_q$. It follows that $\langle a, a\rangle \sim 0$ for all $a \in \mathbb{F}_q^*$. Hence every 3-dimensional quadratic form over $\mathbb{F}_q$ is isotropic. Since s is not a square, it follows that $\langle 1, s\rangle$ is up to isometry the unique 2-dimensional, anisotropic quadratic form over $\mathbb{F}_q$. Thus $0, \langle 1\rangle, \langle s\rangle, \langle 1, s\rangle$ is a complete list of the anisotropic quadratic forms over $\mathbb{F}_q$. Since $\{\langle s\rangle\}^2 = \{\langle 1\rangle\}$ we obtain an isomorphism of rings

$$W(\mathbb{F}_q) \;\cong\; \mathbb{Z}/2\mathbb{Z}[\mathcal{G}(\mathbb{F}_q)] \;\cong\; \mathbb{F}_2[X]/(X^2).$$

(b) Now let $q \equiv 3 \pmod 4$. Then -1 is not a square in $\mathbb{F}_q$ and we can choose $s = -1$. Therefore $\langle 1, 1\rangle$ is anisotropic over $\mathbb{F}_q$. But every element of $\mathbb{F}_q$ can be written as a sum of two squares. Hence $\langle 1, 1, 1\rangle$ is isotropic. It follows from Lemma 2.1.27 that $\langle 1, 1, 1\rangle \cong \langle 1, -1, -1\rangle$. This implies $\langle 1, 1, 1, 1\rangle \cong 2 \times \mathbb{H} \sim 0$. We deduce that $\langle -1, -1\rangle \cong \langle 1, 1\rangle$ and $\langle -1\rangle \sim \langle 1, 1, 1\rangle$. Since -1 is the representative of the non-trivial square class, it follows that every 3-dimensional quadratic form over K is isotropic. Thus $0, \langle 1\rangle, \langle -1\rangle, \langle 1, 1\rangle$ is a list of the anisotropic quadratic forms over $\mathbb{F}_q$. Since $\{\langle -1\rangle\} = \{\langle 1, 1, 1\rangle\}$, we can conclude that

$$W(\mathbb{F}_q) \;\cong\; \mathbb{Z}/4\mathbb{Z}. \qquad \triangle$$

Next we show that both the Witt-Grothendieck ring and the Witt ring of a field K are Witt rings for the square class group $\mathcal{G}(K)$. Consider the map

$$\pi_1 : \quad \mathbb{Z}[\mathcal{G}(K)] \longrightarrow \widehat{W}(K)$$

defined by

$$\overline{a_1} + \cdots + \overline{a_n} \longmapsto [\langle \overline{a_1}, \ldots, \overline{a_n}\rangle]\,.$$

By our previous observations π_1 is well-defined. In fact it can easily be checked that π_1 is a ring homomorphism. As already stated in Example 1.3.2.(2) we have

$$J_1 \;:=\; \ker(\pi_1) \;=\; \big(\overline{a} + \overline{b} - \overline{c} - \overline{d} \mid a, b, c, d \in K^*,\ \langle a, b\rangle \cong \langle c, d\rangle\big) \tag{2.2}$$

by [Sch85, Theorem 9.1, Chapter 2]. For any $\chi \in \mathrm{Hom}(\mathbb{Z}[\mathcal{G}(K)], \mathbb{Z})$ we obtain

$$\chi(\overline{a} + \overline{b} - \overline{c} - \overline{d}) \;\in\; \{-4, -2, 0, 2, 4\}.$$

This gives us the possibilities $\chi(J_1) \in \{(0), (2), (4)\}$. By definition $\widehat{W}(K) \cong \mathbb{Z}[\mathcal{G}(K)]/J_1$ is a Witt ring for $\mathcal{G}(K)$.

Now consider the projection

$$\pi : \quad \widehat{W}(K) \longrightarrow W(K), \quad [\varphi] \longmapsto \{\varphi\}\,.$$

By concatenation we obtain the projection

$$\pi_2 = \pi \circ \pi_1 : \quad \mathbb{Z}[\mathcal{G}(K)] \longrightarrow W(K).$$

By definition of $W(K)$ it follows that

$$J_2 \;:=\; \ker(\pi_2) \;=\; J_1 + (\overline{a} + \overline{-a} \mid a \in K^*\,) \tag{2.3}$$

(see also [Sch85, Corollary 9.4, Chapter 2]). Since also $\chi(\overline{a} + \overline{-a}) \in \{-2, 0, 2\}$ for all $\chi \in \operatorname{Hom}(\mathbb{Z}[\mathcal{G}(K)], \mathbb{Z})$, it follows that $W(K)$ is a Witt ring for $\mathcal{G}(K)$ as well.

Pfister forms

Let (V, φ) be a quadratic form over K. For $a \in K^*$ we define the quadratic form $(V, a\varphi)$ by

$$a\varphi : \quad V \longrightarrow K, \quad v \longmapsto a\varphi(v).$$

2.1.29 Definition. *Let φ be a quadratic form over K.*

(1) Let ψ be another quadratic form over K. Then φ and ψ are similar *if there exists some $a \in K^*$ such that $\varphi \cong a\psi$.*

(2) An element $a \in K^*$ is called a similarity factor *of φ if $\varphi \cong a\varphi$.*

(3) We define the set of similarity factors

$$G_K(\varphi) \;:=\; \{a \in K^* \mid \varphi \cong a\varphi\}\,.$$

It is clear that we always have $(K^*)^2 \subset G_K(\varphi)$. Furthermore it is easy to see that $G_K(\varphi)$ is a subgroup of K^*. Finally, if $1 \in D_K(\varphi)$, then we have $G_K(\varphi) \subset D_K(\varphi)$.

We now introduce an exceedingly important class of quadratic forms, the *Pfister forms.* Introduced by A. Pfister in [Pfi65] under the name of strongly multiplicative forms, they have proven to be useful in nearly every field of study concerning quadratic forms. We have already stated a more general definition in the setting of Witt rings for groups of exponent 2 (see Definitions 1.2.11 and 1.4.4). There we have only made use of their arithmetic properties. In what follows we note some of the geometric properties of Pfister quadratic forms.

2.1.30 Definition. *A quadratic form φ over K is a k-fold* Pfister form*, $k \in \mathbb{N}_0$, if there exist $b_1, \ldots, b_k \in K^*$ such that*

$$\varphi \;\cong\; \langle 1, b_1\rangle \otimes \cdots \otimes \langle 1, b_k\rangle.$$

If $k = 0$, the above notation means that $\varphi \cong \langle 1\rangle$.

2.1.31 Notation. *For $k \in \mathbb{N}$ and $b_1, \dots, b_k \in K^*$ we write*

$$\langle\langle b_1, \dots, b_k \rangle\rangle \ := \ \langle 1, b_1 \rangle \otimes \cdots \otimes \langle 1, b_k \rangle.$$

If (V, φ) is a quadratic form over K, and if L is a field extension of K, then (V, φ) induces a quadratic form $(V \otimes_K L, \varphi_L)$ by

$$\varphi_L : \quad V \otimes_K L \longrightarrow L, \quad v \otimes \lambda \longmapsto \varphi(v)\lambda^2.$$

2.1.32 Proposition. *An anisotropic quadratic form φ over K is a Pfister form if and only if $D^*_L(\varphi_L)$ is a subgroup of L^* for every field extension L of K.*
[Pfi95, Lemma 3.1, Chapter 2]

2.1.33 Proposition. *A Pfister form over K is either anisotropic or hyperbolic.*
[Pfi95, Theorem 3.2, Chapter 2]

2.1.34 Proposition. *If φ is a Pfister form over K, then $G_K(\varphi) = D^*_K(\varphi)$.*
[Lam05, Theorem 1.8, Chapter X]

The structure theorems for Witt rings of fields

2.1.35 Definition. *Let K be a field.*

(1) The level *of K is defined as the minimal number $s \in \mathbb{N}$ such that -1 can be written as a sum of s squares in K. We write $s(K) := s$. In case -1 cannot be written as a sum of squares in K we set $s(K) := \infty$.*

(2) The field K is called formally real *if $s(K) = \infty$.*

2.1.36 Examples. We use the observations we made while studying the Examples 2.1.28 to determine the level of $\mathbb{R}$, algebraically closed fields and finite fields.

(1) Since squares and sums of squares in $\mathbb{R}$ are positive, it follows that -1 cannot be written as a sum of squares in $\mathbb{R}$. Accordingly $s(\mathbb{R}) = \infty$.

(2) Let K be an algebraically closed field. Then -1 is a square in K and $s(K) = 1$.

(3) Consider a finite field $\mathbb{F}_q$, where q is an odd prime power. If $q \equiv 1 \pmod 4$, then -1 is a square in $\mathbb{F}_q$ and $s(\mathbb{F}_q) = 1$. If $q \equiv 3 \pmod 4$, then -1 is not a square in $\mathbb{F}_q$. But we have seen that $\langle 1, 1, 1 \rangle$ is isotropic, which is equivalent to saying that -1 is a sum of two squares. Hence we must have $s(\mathbb{F}_q) = 2$. △

If K is not formally real, then the level of K is the minimal $s \in \mathbb{N}$ such that $-1 \in D_K(s \times \langle 1 \rangle)$. Let $k \in \mathbb{N}_0$ with $2^k \leq s(K) < s^{k+1}$. Then $2^{k+1} \times \langle 1 \rangle$ is an isotropic Pfister form and therefore hyperbolic. It follows that $2^k \times \langle 1 \rangle \cong 2^k \times \langle -1 \rangle$. In particular -1 can be written as a sum of 2^k squares. We obtain $s(K) \leq 2^k$ and hence $s(K) = 2^k$.

2.1.37 Theorem. *The level of a field is either ∞ or a power of* 2.

In the case where $s(K) = 2^k$ with $k \in \mathbb{N}_0$, we have $\left\{2^{k+1} \times \langle 1 \rangle\right\} = 0$ in $W(K)$. By the minimality of $s(K)$ it follows that $\mathrm{char}(W(K)) = 2^{k+1}$. If $s(K) = \infty$, then the definition of the level and our observations imply that $\mathrm{char}(W(K)) = 0$.

2.1.38 Proposition. *Let K be a field. We have*

$$\mathrm{char}(W(K)) \;=\; \begin{cases} 2^{s(K)+1} & \textit{if } s(K) < \infty, \\ 0 & \textit{otherwise.} \end{cases}$$

Now we can reformulate the results from Section 1.4 to obtain the structure theorems for Witt rings of fields.

2.1.39 Definition. *Let K be a field.*

(1) We can extend the dimension *to $\widehat{W}(K)$ by setting*

$$\dim : \quad \widehat{W}(K) \longrightarrow \mathbb{Z}, \quad [\varphi] - [\psi] \longmapsto \dim(\varphi) - \dim(\psi).$$

(2) The dimension index *is defined as*

$$e_0 : \quad W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}, \quad \{\varphi\} \longmapsto \overline{\dim(\varphi)}.$$

(3) We define the fundamental ideal *of K as*

$$I(K) \;:=\; \ker(e_0) \;=\; \{\{\varphi\} \in W(K) \mid \dim(\varphi) \textit{ is even}\}\,.$$

The dimension index and the fundamental ideal as defined in the previous Definition 2.1.39 are just the dimension index and the fundamental ideal as defined in Definition 1.3.14.

2.1.40 Proposition. *Let K be a field. Then $W(K)$ only has 2-torsion, and every zero-divisor in $W(K)$ has even dimension.*

2.1.41 Theorem. *Let K be a formally real field. Then* $\mathrm{Hom}(W(K), \mathbb{Z}) \neq \varnothing$*.*

(1) An element $\{\varphi\} \in W(K)$ is torsion if and only if $\chi(\{\varphi\}) = 0$ for all $\chi \in$ $\mathrm{Hom}(W(K), \mathbb{Z})$*.*

(2) A class $\{\varphi\} \in W(K)$ is a unit if and only if $\chi(\{\varphi\}) = \pm 1$ for all $\chi \in$ $\mathrm{Hom}(W(K), \mathbb{Z})$*.*

2.1.42 Theorem. *Let K be a field with $s(K) < \infty$. Then* $\mathrm{Hom}(W(K), \mathbb{Z}) = \varnothing$*, and R is a torsion ring. Furthermore R is a local ring with maximal ideal $I(K)$, and in particular the equivalence class of every odd-dimensional quadratic form over K is invertible in $W(K)$.*

Ordered fields

We close this section with a few observations about formally real fields.

2.1.43 Definition. *Let K be a field. A subset $P \subset K^*$ is called an* ordering *of K if*

(a) $P \cap -P = \varnothing$ and $P \cup \{0\} \cup -P = K$,

(b) $P + P \subset P$ *and* $P \cdot P \subset P$.

The elements of P *are called* positive*, and the elements of* $-P$ *are called* negative*.*

Let K be a field, and suppose there exists an ordering $P \subset K^*$. Then we can define a total order on K by setting, for $a, b \in K$,

$$a < b \quad :\Longleftrightarrow \quad b - a \in P.$$

Accordingly we write $a \leq b$ if $a < b$ or $a = b$.

If $P \subset K^*$ is an ordering, then it follows from the definition that $1 \in P$ and $(K^*)^2 \subset P$. Hence if $a \in P$, then its square class $\overline{a} \in \mathcal{G}(K)$ is a subset of P. If $H \subset \mathcal{G}(K)$ is the subset of all $\overline{a}$ with $a \in P$, then it can easily be checked that H is a subgroup of G. Since $\overline{(-a)} \cdot \overline{(-b)} \subset P$ for $a, b \in P$, it follows that $xy \in H$ for all $x, y \in \mathcal{G}(K) \setminus H$. This implies that H has index 2 in G. Hence by Theorem 1.3.12 we can define a ring homomorphism

$$\widehat{\chi}: \quad \mathbb{Z}[\mathcal{G}(K)] \longrightarrow \mathbb{Z}, \quad \overline{a} \longmapsto \begin{cases} 1 & \text{if } a \in P, \\ -1 & \text{otherwise.} \end{cases}$$

If $a_1, \dots, a_n \in P$, then it follows from Definition 2.1.43 that $\langle a_1, \dots, a_n \rangle$ is anisotropic. This implies that $\widehat{\chi}$ induces a ring homomorphism $\chi \in \mathrm{Hom}(W(K), \mathbb{Z})$. The homomorphism χ is usually called the *signature homomorphism* associated to the ordering P.

If on the other hand $\chi \in \mathrm{Hom}(W(K), \mathbb{Z})$, then χ induces a ring homomorphism $\widehat{\chi}$: $\mathbb{Z}[\mathcal{G}(K)] \to \mathbb{Z}$. By Proposition 1.3.8 the set $H := \{g \in G \mid \chi(g) = 1\} \subset G$ is a subgroup of index at most 2. Since $\{\langle 1, -1 \rangle\} = 0$ and $\dim(\langle 1, -1 \rangle) = 2$, it follows that the dimension homomorphism $\dim : \mathbb{Z}[\mathcal{G}(K)] \to \mathbb{Z}$ does not induce a ring homomorphism $W(K) \to \mathbb{Z}$. Hence we must have $H \neq G$, and H must have index 2 in G. It is then straightforward to show that the union of all $\overline{a} \in H$ is an ordering $P \subset K^*$.

2.1.44 Proposition. *The ring homomorphisms* $\mathrm{Hom}(W(K), \mathbb{Z})$ *are in one-to-one correspondence with the orderings* $P \subset K^*$*.*

[Sch85, Lemma 7.4, Chapter 2]

2.1.45 Corollary. *The field* K *is formally real if and only if there exists an ordering* $P \subset K^*$*.*

2.2 The Brauer group

In this section we interrupt the study of quadratic forms to give a short introduction to Brauer groups and quaternion algebras. In particular the study of quaternion algebras is heavily linked with the study of quadratic forms. The Hasse invariant and the Clifford invariant of a quadratic form, which we will introduce in the following section, can both be defined and studied by exclusively using quaternion algebras and their properties.

For reasons of coherence, we assume that the base field K always has a characteristic different from 2. But it should be noted that, apart from the definition of quaternion algebras and the results concerning those, everything else considered in this chapter holds over fields with arbitrary characteristic.

2.2.1 Definition. *A ring R is called* simple *if R does not have any non-zero proper two-sided ideal. In other words if $I \subset R$ is a two-sided ideal, then either $I = (0)$ or $I = R$.*

2.2.2 Examples.

(1) Obviously every field K is simple.

(2) Similarly a skew field D is always simple.

(3) It can be shown with the help of elementary matrix operations that $\mathbb{M}_n(D)$ is simple for every skew field D and every $n \in \mathbb{N}$ (see [Ker90, Beispiele 2.2, Kapitel I]). △

2.2.3 Definition. *Let A be a K-algebra.*

(1) The set

$$\mathcal{Z}(A) \ := \ \{a \in A \mid ab = ba \; \forall \, b \in A\}$$

is called the center *of A.*

(2) We say that A is K-central *if $\mathcal{Z}(A) = K$.*

It is straight forward to show that $\mathcal{Z}(A)$ is a subfield of A containing K.

2.2.4 Examples.

(1) The field K is the trivial example of a K-central algebra.

(2) The Hamilton quaternions $\mathbb{H}$ form an $\mathbb{R}$-central skew field.

(3) Again, with the help of elementary matrix operations, it can be shown that for a K-central skew field D the matrix algebra $\mathbb{M}_n(D)$ is also K-central for all $n \in \mathbb{N}$ (see [Ker90, Satz 5.3, Kapitel I]). △

2.2.5 Definition. *A K-algebra A is called a* central simple algebra *over K if A is finite-dimensional as a K-vector space, K-central, and simple.*

2.2.6 Example. If D is a finite-dimensional, K-central skew field, it follows from the previous examples that $\mathbb{M}_n(D)$ is a central simple algebra for all $n \in \mathbb{N}$. It will become apparent that this example is quintessential for the study of central simple algebras. △

The objects that we want to classify are exactly the central simple algebras over K. The following theorem constitutes the foundation for the introduction of the Brauer group.

2.2.7 Theorem (Wedderburn's theorem)**.** *Let A be a finite-dimensional, simple K-algebra. Then there exists a skew field D over K and an $n \in \mathbb{N}$ such that $A \cong \mathbb{M}_n(D)$ as K-algebras. Furthermore n is unique, and D is unique up to K-isomorphism. More specifically if $\mathbb{M}_n(D) \cong \mathbb{M}_m(E)$ with $m, n \in \mathbb{N}$ and skew fields D and E over K, then $n = m$ and $D \cong E$ as K-algebras.*

[GS06, Theorem 2.1.3, Chapter 2]

We need a number of results and formulas about the tensor product.

The following lemma is an immediate consequence of [Lan02, Corollary 2.4, Chapter XVI].

2.2.8 Lemma. *Let A be a K-algebra, and let $n, m \in \mathbb{N}$. Then there exists a K-algebra isomorphism*

$$M_n(A) \otimes_K \mathbb{M}_m(K) \;\cong\; M_{nm}(A).$$

2.2.9 Proposition. *If A and B are K-algebras, then there exists an isomorphism of K-algebras*

$$\mathcal{Z}(A \otimes_K B) \;\cong\; \mathcal{Z}(A) \otimes_K \mathcal{Z}(B).$$

In particular, if A and B are K-central, then $A \otimes_K B$ is K-central as well.
[Ker90, Satz 5.8, Kapitel I]

Let A be a central simple algebra over K, and let $n \in \mathbb{N}$ and D be a skew field over K such that $A \cong \mathbb{M}_n(D)$. By Lemma 2.2.8 we have $\mathbb{M}_n(D) \cong D \otimes_K \mathbb{M}_n(K)$, and by the previous proposition we can now conclude that D is K-central. Hence D is a central simple algebra, too. If on the other hand we assume that D is K-central, then we have seen further up that $\mathbb{M}_n(D)$ is a central simple algebra for all $n \in \mathbb{N}$.

2.2.10 Proposition. *Let A and B be simple K-algebras. If A is also K-central, then $A \otimes_K B$ is simple.*
[Ker90, Satz 5.9, Kapitel I]

2.2.11 Corollary. *The tensor product of two central simple algebras over K is again a central simple algebra over K.*

We can now define an equivalence relation on central simple algebras as follows: Let A and B be central simple algebras, then

$$A \sim B \quad :\Longleftrightarrow \quad \exists\, m, n \in \mathbb{N} \quad \text{such that} \quad A \otimes_K \mathbb{M}_n(K) \cong B \otimes_K \mathbb{M}_m(K).$$

It is easy to check that this indeed defines an equivalence relation. Denote by $[A]$ the equivalence class of A, and let $\mathrm{Br}(K)$ be the set of equivalence classes of central simple algebras over K.

Consider two central simple algebras A and B over K. There exist $r, s \in \mathbb{N}$ and K-central skew fields D and E over K such that $A \cong \mathbb{M}_r(D)$ and $B \cong \mathbb{M}_s(E)$. By Lemma 2.2.8 and the Wedderburn theorem

$$\begin{aligned} A \sim B \quad &\Longleftrightarrow \quad \mathbb{M}_r(D) \otimes_K \mathbb{M}_n(K) \cong \mathbb{M}_s(E) \otimes_K \mathbb{M}_m(K) \\ &\Longleftrightarrow \quad \mathbb{M}_{rn}(D) \cong \mathbb{M}_{sm}(E) \\ &\Longleftrightarrow \quad D \cong E. \end{aligned}$$

In other words two central simple K-algebras $A \cong \mathbb{M}_r(D)$ and $B \cong \mathbb{M}_s(E)$ are equivalent if and only if $D \cong E$. This implies that the equivalence class of a central simple algebra A over K contains up to K-isomorphism exactly one K-central skew field.

The tensor product induces a well-defined multiplication in $\mathrm{Br}(K)$ by

$$[A] \cdot [B] \;:=\; [A \otimes_K B]$$

for central simple algebras A and B over K. We can use the properties of the tensor product to deduce that this multiplication is associative and commutative. The neutral element with respect to this multiplication is the class $[K] = [\mathbb{M}_n(K)]$, $n \in \mathbb{N}$. So, in order for the set of equivalence classes to form a group, it remains to find for a class $[A]$ its inverse class in $\mathrm{Br}(K)$.

2.2.12 Definition. *Let A be a K-algebra. The* opposite algebra A^{op} *of A is defined such that $(A^{\mathrm{op}}, +) := (A, +)$, and the multiplication in A^{op} is given by*

$$a \cdot_{\mathrm{op}} b \;:=\; b \cdot a, \qquad a, b \in A,$$

where $b \cdot a$ is the usual multiplication in A.

2.2.13 Proposition. *If A is a central simple K-algebra, then there exist K-algebra isomorphisms*

$$A \otimes_K A^{\mathrm{op}} \;\cong\; \mathrm{End}_K(A) \;\cong\; \mathbb{M}_n(K),$$

where $n = \dim_K(A)$.

[Ker90, Satz 6.4, Kapitel I]

Thus for a K-algebra A the inverse of $[A]$ in $\mathrm{Br}(K)$ is given by $[A^{\mathrm{op}}]$.

2.2.14 Theorem. *The set* $\mathrm{Br}(K)$ *of equivalence classes of central simple algebras endowed with the multiplication induced by the tensor product forms a commutative group. The neutral element of* $\mathrm{Br}(K)$ *is the class $[K]$, and for every class $[A] \in \mathrm{Br}(K)$ its inverse is given by $[A^{\mathrm{op}}]$.*

2.2.15 Definition. *The group* $\mathrm{Br}(K)$ *is called the* Brauer group *of K.*

2.2.16 Example. Suppose that K is an algebraically closed field. Consider a finite-dimensional, K-central skew field D. It follows that for any $x \in D$ we obtain a subfield $K(x) \subset D$ which is algebraic over K. As K is algebraically closed we must have $K(x) = K$ and hence $x \in K$. This implies that $D = K$. Thus up to isometry K is the unique K-central skew field over K. We obtain $\mathrm{Br}(K) = \{1\}$. △

Consider a field extension L of K. Then, for a K-algebra A, the tensor product $A \otimes_K L$ is an L-algebra. If $\dim_K(A) < \infty$, then $\dim_L(A \otimes_K L) = \dim_K(A)$. We write

$$A_L \;:=\; A \otimes_K L.$$

2.2.17 Proposition. *Let L be a field extension of K, and let A be a K-algebra.*

(1) The algebra A is simple if and only if A_L is simple.

(2) The algebra A is K-central if and only if A_L is L-central.

(3) In particular A is a central simple algebra over K if and only if A_L is a central simple algebra over L.

[Ker90, Satz 5.10, Kapitel I]

The following lemma is a consequence of [Bou89a, Proposition 8, Chapter II, §3.8].

2.2.18 Lemma. *Let L be a field extension of K, let A, B be K-algebras, and let C be an L-algebra. Then there exist L-algebra isomorphisms*

(1) $(A \otimes_K L) \otimes_L C \;\cong\; A \otimes_K C$,

(2) $(A \otimes_K L) \otimes_L (B \otimes_K L) \;\cong\; (A \otimes_K B) \otimes_K L$.

Thus, for a field extension L of K, we can define the *restriction map*

$$r_{L/K}: \quad \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L), \quad [A] \longmapsto [A_L]\,.$$

We use Lemma 2.2.18 to show that $r_{L/K}$ is well-defined, and that for field extensions $K \subset L \subset M$ we have

$$r_{M/L} \circ r_{L/K} \;=\; r_{M/K}.$$

2.2.19 Theorem. *Let A be a finite-dimensional K-algebra. The following are equivalent:*

(i) The algebra A is central simple over K.

(ii) There exists a K-central skew field D and an $m \in \mathbb{N}$ such that $A \cong \mathbb{M}_m(D)$.

(iii) There exists a K-algebra isomorphism

$$A \otimes_K A^{\mathrm{op}} \longrightarrow \mathrm{End}_K(A), \quad a \otimes b \longmapsto (x \mapsto axb).$$

(iv) There exists a $\overline{K}$-algebra isomorphism $A \otimes_K \overline{K} \cong \mathbb{M}_n(\overline{K})$ for some $n \in \mathbb{N}$, where $\overline{K}$ is an algebraic closure of K.

(v) There exists a field extension L of K such that $A \otimes_K L \cong \mathbb{M}_n(L)$ for some $n \in \mathbb{N}$.

[Ker90, Satz 6.4 & Korollar 6.6, Kapitel 1]

2.2.20 Corollary. *The dimension of a central simple algebra over K is a square.*

Thus we can define two invariants of central simple algebras. Let A be a central simple algebra over K. Then

$$\deg_K(A) \;:=\; \sqrt{\dim_K(A)}$$

is called the *degree* of A. Let D be a K-central skew field and let $n \in \mathbb{N}$ such that $A \cong \mathbb{M}_n(D)$. Then we define the *index* of A by

$$\mathrm{ind}_K(A) \;:=\; \sqrt{\dim_K(D)}.$$

We see immediately that $\mathrm{ind}_K(A)$ divides $\deg_K(A)$. Furthermore it follows from our observations that the index is invariant under equivalence of central simple algebras.

Quaternion algebras

We now continue to study a special class of central simple algebras over K, the quaternion algebras. From now on the restriction $\mathrm{char}(K) \neq 2$ is essential.

2.2.21 Definition. *A* quaternion algebra *Q over K is a K-algebra generated by two elements $u, v \in Q$ such that there exist $a, b \in K^*$ with*

$$u^2 = a, \qquad v^2 = b, \qquad uv = -vu.$$

Let Q be a quaternion algebra over K, and let $u, v \in Q$ be generators of Q with $u^2 = a, v^2 = b \in K^*$. It follows from the definition that the elements of K can be written as K-linear combinations of the elements $1, u, v, uv$. In fact it can be shown that $\{1, u, v, uv\}$ is a K-basis of Q (see [Lam05, Proposition 1.0, Chapter III]). Thus Q has dimension 4 over K.

2.2.22 Proposition. *Quaternion algebras over K are central simple algebras over K.*
[Lam05, Proposition 1.1, Chapter III]

2.2.23 Definition. *Let Q be a quaternion algebra over K. Any K-basis $\{1, u, v, w\}$ such that $u^2, v^2 \in K^*$ and $w = uv = -vu$ is called a* standard basis *of Q.*

Let Q and Q' be quaternion algebras over K. Consider a standard basis $\{1, u, v, uv\}$ (respectively $\{1, u', v', u'v'\}$) of Q (respectively Q'). If $u^2 = u'^2 = a$ and $v^2 = v'^2 = b$ with $a, b \in K^*$, then clearly $u \mapsto u'$ and $v \mapsto v'$ defines a K-algebra isomorphism $Q \cong Q'$. Henceforth we consider quaternion algebras over K only up to K-algebra isomorphism. This allows us to introduce the following notation.

2.2.24 Notation. *If Q is a quaternion algebra over K with a standard basis $\{1, u, v, uv\}$, and if $a, b \in K^*$ with $u^2 = a$ and $v^2 = b$, then we write*

$$(a, b)_K := Q.$$

Quaternion algebras are of particular interest in the context of quadratic forms, since they serve, as has already been mentioned, to define invariants of quadratic forms. But the connection is even more immediate, as quaternion algebras are in fact canonically endowed with the structure of a quadratic space.

2.2.25 Lemma. *Let Q be a quaternion algebra over K with a standard basis $\{1, u, v, uv\}$. Then we have*

$$uK + vK + uvK = \left\{ x \in Q \;\middle|\; x^2 \in K,\ x \notin K^* \right\}.$$

In particular the subspace $uK + vK + uvK$ is independent from the choice of standard basis.
[Lam05, Proposition 1.3, Chapter III]

Consider a quaternion algebra $Q = (a, b)_K$, $a, b \in \mathbb{K}^*$. Let $\{1, u, v, uv\}$ be a standard basis of Q such that $u^2 = a$ and $v^2 = b$. By the previous lemma we can define the K-subvector space of *pure quaternions*

$$Q_0 := uK + vK + uvK \subset Q.$$

There exists a direct sum decomposition

$$Q \;=\; 1\cdot K \oplus Q_0.$$

This allows us to define the *canonical involution* of Q by

$$Q \longrightarrow Q,\quad x = x_0 + x_1 \longmapsto \overline{x} \;:=\; x_0 - x_1, \qquad x_0 \in 1\cdot K,\; x_1 \in Q_0.$$

By Lemma 2.2.25 we immediately see that for all $x \in Q$ we have $x\overline{x} \in K$. Now consider the map

$$N:\quad Q \longrightarrow K,\quad x \longmapsto x\overline{x}.$$

It is a quadratic map and we call it the *norm form* of Q. For $x, y \in Q$ we obtain

$$N(xy) \;=\; xy\overline{y}\,\overline{x} \;=\; x\overline{x}y\overline{y} \;=\; N(x)N(y),$$

since $y\overline{y}$ lies in K and K is the center of Q. Now a quick calculation shows that the standard basis $\{1, u, v, uv\}$ of Q is an orthogonal basis of the quadratic space $\big(Q, N\big)$. Since $u^2 = a$ and $v^2 = b$ we obtain

$$\big((a,b)_K\,, N\big) \;\cong\; \big(K^4, \langle 1, -a, -b, ab\rangle\big)\big).$$

It is now possible to use the norm form to show many useful properties of quaternion algebras. Assume for example that N is anisotropic. Then for $x \in (a,b)_K$ with $x \neq 0$ we obtain $x(\overline{x}\frac{1}{N(x)}) = 1$, i.e. $\overline{x}\frac{1}{N(x)}$ is the inverse of x in $(a,b)_K$. It follows that $(a,b)_K$ is a skew field. If on the other hand there exists an $x \in (a,b)_K$, $x \neq 0$, such that $N(x) = x\overline{x} = 0$, then $(a,b)_K$ contains zero-divisors and cannot be a skew field. Since the dimension of a K-central skew field is a square, we obtain the following proposition.

2.2.26 Proposition. *A quaternion algebra over K is a skew field if and only if its norm form is anisotropic.*

With the help of the norm form we can classify quaternion algebras over K.

2.2.27 Theorem. *Let $a, b, c, d \in K^*$. The following are equivalent:*

(i) $(a,b)_K \;\cong\; (c,d)_K$,

(ii) $\langle\langle -a, -b\rangle\rangle \;\cong\; \langle\langle -c, -d\rangle\rangle$,

(iii) $\langle -a, -b, ab\rangle \;\cong\; \langle -c, -d, cd\rangle$.

[Sch85, Theorem 11.9, Chapter 2]

2.2.28 Corollary. *Let $a, b \in K^*$. Then the following are equivalent:*

(i) $(a,b)_K \;\cong\; \mathbb{M}_2(K)$,

(ii) $(a,b)_K \;\cong\; (1,1)_K$,

(iii) $\langle\langle -a, -b\rangle\rangle$ *is hyperbolic,*

(iv) $\langle -a, -b, ab\rangle$ *is isotropic.*

To be able to efficiently work with quaternion algebras we need to recall the following relations.

2.2.29 Corollary. *For $a, b, c, d, e \in K^*$ we have*

(1) $(a,b)_K \;\cong\; \left(ad^2, be^2\right)_K$,

(2) $(a,b)_K \;\cong\; (b,a)_K$,

(3) $\mathbb{M}_2(K) \;\cong\; (1,1)_K \;\cong\; (1,a)_K \;\cong\; (b,-b)_K \;\cong\; (c,1-c)_K, \quad c \neq 0,1,$ *and*

(4) $(a,a)_K \;\cong\; (a,-1)_K$.

[Sch85, Corollary 11.13, Chapter 2]

Statement (1) from the previous corollary states that multiplying the entries $a, b \in K^*$ in $(a,b)_K$ with arbitrary non-zero squares results in a quaternion algebra that lies in the same equivalence class as $(a,b)_K$. Thus we can allow the notation

$$\left[\left(\overline{a}, \overline{b}\right)_K\right] \qquad \text{with} \quad \overline{a}, \overline{b} \;\in\; \mathcal{G}(K).$$

Finally we need to establish that quaternion algebras behave bi-multiplicatively in the Brauer group.

2.2.30 Lemma. *For $a, b, c \in K^*$ we have*

$$[(a,b)_K]\,[(a,c)_K] \;=\; [(a,bc)_K] \qquad \textit{and} \qquad [(a,c)_K]\,[(b,c)_K] \;=\; [(ab,c)_K]\,.$$

[Lam05, Theorem 2.11, Chapter III]

Denote by $\mathrm{Quat}(K) \subset \mathrm{Br}(K)$ the subgroup generated by the equivalence classes of all quaternion algebras over K. Since we have

$$[(a,b)_K]\,[(a,b)_K] \;=\; [(a,1)_K] \;=\; 1$$

It follows that the elements of $\mathrm{Quat}(K)$ have order at most 2. In other words we have $\mathrm{Quat}(K) \subset {}_2\mathrm{Br}(K)$, where ${}_2\mathrm{Br}(K)$ denotes the subgroup of $\mathrm{Br}(K)$ consisting of all elements of order at most 2.

2.3 Cohomological invariants

In Section 2.1 we have already seen the 0-*th cohomological* invariant, the dimension index

$$e_0 : \quad W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}, \quad \{\varphi\} \longmapsto \overline{\dim(\varphi)}.$$

The kernel of e_0 is the fundamental ideal of K, which is the ideal generated by the equivalence classes of all even-dimensional quadratic forms over K. Since e_0 is clearly surjective we obtain

$$W(K)/I(K) \;\cong\; \mathbb{Z}/2\mathbb{Z}.$$

We have seen in Section 2.1 that the determinant $\det(\varphi)$ of a quadratic form φ over K is invariant under isometry. Thus the determinant induces a map

$$\det: \quad \widehat{W}(K) \longrightarrow \mathcal{G}(K), \quad [\varphi] \longmapsto \overline{\det(\varphi)}.$$

If ψ is another quadratic form over K, then $\det(\varphi \perp \psi) = \det(\varphi)\det(\psi)$. Thus $\det : \widehat{W}(K) \to \mathcal{G}(K)$ is in fact a group homomorphism.

But the determinant is not invariant under equivalence, as for example $\det(\varphi \perp \mathbb{H}) = -\det(\varphi)$. Therefore we define the *discriminant* of φ by

$$d(\varphi) \;:=\; (-1)^{\frac{n(n-1)}{2}} \det(\varphi) \;\in\; \mathcal{G}(K).$$

A simple calculation shows that the discriminant is invariant under equivalence of quadratic forms. It thus induces a map

$$e_1: \quad W(K) \longrightarrow \mathcal{G}(K), \quad \{\varphi\} \longmapsto d(\varphi).$$

The map e_1 is also called the *first cohomological invariant*. However, if we consider the equalities $d(\langle 1\rangle) = 1$ and $d(\langle 1,1\rangle) = -1$, we see that the discriminant is not a group homomorphism. But it can be easily checked that $e_1 : I(K) \longrightarrow \mathcal{G}(K)$ is a group homomorphism. Now what is the kernel of e_1? Before we answer this question we have to make a few observations about the powers of the fundamental ideal $I(K)$.

For $k \in \mathbb{N}$, write

$$I^k(K) \;:=\; \big(I(K)\big)^k$$

for the k-th power of the fundamental ideal. For $k = 0$ we set $I^0(K) := W(K)$. Every even dimensional quadratic form can be written as the orthogonal sum of binary forms $\langle a, b\rangle$ with $a, b \in K^*$. We have the equivalence

$$\langle a, b\rangle \;\sim\; \langle 1, a\rangle \perp -\langle 1, -b\rangle.$$

This shows that the 1-fold Pfister forms over K additively generate $I(K)$. We deduce that $I^k(K)$ is additively generated by the k-fold Pfister forms over K.

Now

$$d(\langle\langle a, b\rangle\rangle) \;=\; (-1)^{\frac{4\cdot 3}{2}} \det(\langle 1, a, b, ab\rangle) \;=\; 1$$

for all $a, b \in K^*$. Hence the equivalence classes of 2-fold Pfister forms lie in the kernel of the discriminant e_1. By our observations about the powers of the fundamental ideal it follows that $I^2(K) \subset \ker(e_1)$. In fact one can show that equality holds.

2.3.1 Proposition. *Let K be a field. We have* $\ker(e_1) = I^2(K)$.
[Pfi95, Proposition 3.6, Chapter 2]

By the previous proposition

$$I(K)/I^2(K) \;\cong\; \mathcal{G}(K).$$

Next we would like to define an invariant, which is defined on all of $W(K)$ but a group homomorphism only on $I^2(K)$. Analogously as for the dimension index and the discriminant, we would like the kernel of this invariant to be $I^3(K)$.

For an n-dimensional quadratic form $\varphi \cong \langle a_1, \ldots, a_n \rangle$ over K with $a_1, \ldots, a_n \in K^*$ we define the *Hasse invariant*

$$s(\varphi) \;:=\; \prod_{1 \leq i < j \leq n} \left[(a_i, a_j)_K\right] \;\in\; \mathrm{Br}(K).$$

It is rather technical but not difficult to show that the definition of the Hasse invariant does not depend on the chosen diagonal representation of φ (see [Lam05, Propositon 3.18, Chapter V]). In particular s is invariant under isometry and hence defines a map

$$s: \quad \widehat{W}(K) \longrightarrow \mathrm{Br}(K), \quad [\varphi] \longmapsto s(\varphi).$$

2.3.2 Examples. Let $a, b \in K^*$.

(1) Clearly $s(\langle a, b \rangle) = [(a, b)_K]$. In particular $s(\mathbb{H}) = 1$.

(2) We calculate

$$\begin{aligned} s(\langle\langle -a, -b \rangle\rangle) &= [(-a, -b)_K]\,[(-a, ab)_K]\,[(-b, ab)_K] \\ &= [(-a, -b)_K]\,[(ab, ab)_K] \\ &= [(-a, -b)_K]\,[(ab, -1)_K] \end{aligned}$$

for the 2-fold Pfister form $\langle\langle -a, -b \rangle\rangle$. △

In the following section we will have to undertake a number of calculations involving the Clifford invariant, whose definition is based on the definition of the Hasse invariant. By straight-forward calculations we can establish the following formulas.

2.3.3 Lemma. *For quadratic forms φ and ψ over K we have*

$$s(\varphi \perp \psi) \;=\; s(\varphi)s(\psi)\,[(\det(\varphi), \det(\psi))_K]\,.$$

[Sch85, Lemma 12.6, Chapter 2]

2.3.4 Lemma. *Let φ be an n-dimensional quadratic form over K, and let $b \in \mathbb{K}^*$.*

$$s(b\varphi) \;=\; \begin{cases} s(\varphi)\left[\left(b, (-1)^{\frac{n(n-1)}{2}}\right)_K\right] & \textit{if } n \textit{ is odd,} \\ s(\varphi)\,[(b, d(\varphi))_K] & \textit{if } n \textit{ is even.} \end{cases}$$

Proof. Let $\varphi \cong \langle a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in K^*$. Then

$$\begin{aligned} s(b\varphi) &= \prod_{i<j} \left[(ba_i, ba_j)_K\right] \\ &= s(\varphi) \cdot \left(\prod_{i=1}^{n} [(b, a_i)_K]^{n-1} \right) \cdot [(b, -1)_K]^{\frac{n(n-1)}{2}} \\ &= s(\varphi) \cdot [(b, \det(\varphi))_K]^{n-1} \cdot \left[\left(b, (-1)^{\frac{n(n-1)}{2}}\right)_K\right]. \end{aligned}$$

If we now take into account the parity of n, the claim follows. □

It is possible to define the Clifford invariant by using the theory of Clifford algebras and their classification. While our approach, which only employs quaternion algebras, is not as elegant, it yields additional insight into the arithmetic of the Clifford invariant. This is useful, since we need the Clifford invariant exclusively for calculations.

For an n-dimensional quadratic form φ we define the *Clifford invariant*

$$c(\varphi) := \begin{cases} s(\varphi) & \text{for } n \equiv 1,2 \pmod 8, \\ s(\varphi)\,[(-1,-\det(\varphi))_K] & \text{for } n \equiv 3,4 \pmod 8, \\ s(\varphi)\,[(-1,-1)_K] & \text{for } n \equiv 5,6 \pmod 8, \\ s(\varphi)\,[(-1,\det(\varphi))_K] & \text{for } n \equiv 7,8 \pmod 8. \end{cases}$$

It is clear that c is well-defined and invariant under isometry.

2.3.5 Remark. The invariant c as defined above is introduced under various different names in the literature. While we choose the name *Clifford invariant*, the name probably most commonly used is *Witt invariant* (see for example [Lam05, §3, Chapter V], and [Sch85, §12, Chapter 2]). △

2.3.6 Examples. Let $a, b \in K^*$.

(1) By definition and Example 2.3.2.(1) we have $c(\langle a,b\rangle) = s(\langle a,b\rangle) = [(a,b)_K]$. It follows that $c(\mathbb{H}) = 1$.

(2) Consider the 2-fold Pfister form $\tau := \langle\langle -a,-b\rangle\rangle$. By definition $c(\tau) = s(\tau)\,[(-1,-1)_K]$, and by Example 2.3.2.(2)

$$\begin{aligned} c(\tau) &= [(-a,-b)_K]\,[(ab,-1)_K]\,[(-1,-1)_K] \\ &= [(-a,-b)_K]\,[(-ab,-1)_K] \\ &= [(-a,-b)_K]\,[(-a,-1)_K]\,[(b,-1)_K] \\ &= [(-a,b)_K]\,[(-1,b)_K] \\ &= [(a,b)_K]\,. \end{aligned}$$

This shows that the norm form of $c(\tau)$ is just τ. △

From the Lemmas 2.3.3 and 2.3.4 we deduce the following formulas for the Witt invariant.

2.3.7 Lemma. *Let φ and ψ be quadratic forms over K. Then*

$$c(\varphi\perp\psi) = \begin{cases} c(\varphi)c(\psi)\,[(d(\varphi),d(\psi))_K] & \textit{if } \dim(\varphi) \textit{ and } \dim(\psi) \textit{ are both even or odd,} \\ c(\varphi)c(\psi)\,[(-d(\varphi),d(\psi))_K] & \textit{if } \dim(\varphi) \textit{ is odd and } \dim(\psi) \textit{ is even.} \end{cases}$$

[Lam05, (3.15), Chapter V]

2.3.8 Lemma. *If φ is a quadratic form over K, and if $b \in K^*$, then*

$$c(b\varphi) = \begin{cases} c(\varphi) & \textit{if } \dim(\varphi) \textit{ is odd,} \\ c(\varphi)\,[(b,d(\varphi))_K] & \textit{if } \dim(\varphi) \textit{ is even.} \end{cases}$$

[Lam05, (3.16), Chapter V]

Let φ and ψ be quadratic forms over K. By combining the previous two lemmas we obtain

$$c(\varphi \perp \psi) \;=\; \begin{cases} c(\varphi)c(d(\varphi)\psi) & \text{if } \dim(\varphi) \text{ and } \dim(\psi) \text{ are even,} \\ c(\varphi)c(-d(\varphi)\psi) & \text{if } \dim(\varphi) \text{ is odd and } \dim(\psi) \text{ is even.} \end{cases}$$

In particular

$$c(\varphi \perp \mathbb{H}) \;=\; c(\varphi)c(\pm d(\varphi)\mathbb{H}) \;=\; c(\varphi)c(\mathbb{H}) \;=\; c(\varphi),$$

which implies that c is invariant under equivalence of quadratic forms. Hence c defines a map

$$e_2 : \quad W(K) \longrightarrow \mathrm{Br}(K), \quad \{\varphi\} \longmapsto c(\varphi)$$

which is also called the *second cohomological invariant*.

Lemma 2.3.7 shows that e_2 is not a group homomorphism on $W(K)$. But if we restrict e_2 to $I^2(K)$, then it follows from the fact that the discriminant vanishes on $I^2(K)$, that $e_2 : I^2(K) \to \mathrm{Br}(K)$ is a group homomorphism. Now consider a 3-fold Pfister form $\tau := \langle\langle -a, -b, -c \rangle\rangle$ over K, $a, b, c \in K^*$. Then

$$c(\tau) \;=\; c(\langle\langle -a, -b \rangle\rangle \perp (-c)\langle\langle -a, -b \rangle\rangle) \;=\; c(\langle\langle -a, -b \rangle\rangle)c(\langle\langle -a, -b \rangle\rangle) \;=\; 1.$$

This shows that $I^3(K) \subset \ker(e_3)$. As for the discriminant it is possible to show that equality holds. While this result had been conjectured for quite a long time, it was only in 1981 that A. Merkurjev published a proof for it. Whereas the proof for the discriminant only uses elementary methods, the proof for the Clifford invariant is significantly more difficult and uses advanced methods.

2.3.9 Theorem. *The Clifford invariant induces an isomorphism*

$$I^2(K)/I^3(K) \xrightarrow{\cong} {}_2\mathrm{Br}(K).$$

[Mer81a]

For once this result obviously implies that $\ker(e_2) = I^3(K)$. But since the image of e_2 lies in $\mathrm{Quat}(K)$, and since by our observations $\mathrm{Quat}(K) \subset {}_2\mathrm{Br}(K)$, we can also deduce that $\mathrm{Quat}(K) = {}_2\mathrm{Br}(K)$.

Consider a separable closure K_s of K, and denote by $\Gamma_K := \mathrm{Gal}(K_s/K)$ the absolute Galois group of K. We write $H^k(K) := H^k(\Gamma_K, \mathbb{Z}/2\mathbb{Z})$ for the k-th cohomology group of K with coefficients in $\mathbb{Z}/2\mathbb{Z}$. Now $H^1(K) \cong \mathcal{G}(K)$ is the square class group of K (see [Ser02, Corollary, Chapter I, §1.2]). We use the additive notation for $H^1(K)$. Denote by $(a) \in H^1(K)$ the square class of $a \in K^*$.

The invariants e_0, e_1 and e_2 are called cohomological invariants since $H^0(K) \cong \mathbb{Z}/2\mathbb{Z}$ (see [Ser02, §2.3, Chapter I & §1.1, Chapter II]), $H^1(K) \cong \mathcal{G}(K)$, and $H^2(K) \cong {}_2\mathrm{Br}(K)$ (see [Ser95, Proposition 9, Chapter X, §5] and [Ser02, §1.2, Chapter II]). In other words the invariants take values in the according cohomology groups of K with coefficients in $\mathbb{Z}/2\mathbb{Z}$. In particular the homomorphism $e_1 : I(K) \to H^1(K)$ is defined by $\{\langle\langle -a \rangle\rangle\} \mapsto (a)$ for $a \in K^*$, and $e_2 : I^2(K) \to H^2(K)$ is defined by $\{\langle\langle -a, -b \rangle\rangle\} \mapsto (a) \cup (b)$ for $a, b \in K^*$, where $\cup$ denotes the cup product in the cohomology ring $H^*(K)$.

Now it would be nice if for any $k \in \mathbb{N}_0$ there existed an invariant e_k such that

(a) e_k defines a map $e_k : W(K) \to H^k(K)$,

(b) e_k restricted to $I^k(K)$ is a group homomorphism which is defined by

$$\langle\langle -a_1, \dots, -a_k \rangle\rangle \longmapsto (a_1) \cup \cdots \cup (a_k)$$

for $a_1, \dots, a_k \in K^*$, and

(c) e_k induces an isomorphism $I^k(K)/I^{k+1}(K) \xrightarrow{\cong} H^k(K)$.

This would in particular help us tremendously with the study of annihilating polynomials for quadratic forms in the next section. But in fact invariants that satisfy all of the above conditions do only exist for $k = 0, 1, 2$. For general k there exist invariants that satisfy the conditions (b) and (c), but those invariants are not defined on all of $W(K)$. In his article [Ara75a] J. K. Arason constructs the invariant e_3, which is only defined on $I^3(K)$. But in addition he shows that for $k > 2$ any invariant that satisfies the conditions (b) and (c) can in fact not be defined on all of $W(K)$. In [Mil70] J. W. Milnor introduces what is now generally called the Milnor K-theory, and he uses this K-theory to define for arbitrary $k \in \mathbb{N}_0$ an invariant that satisfies condition (b). However he did not manage to prove that his invariants also satisfy condition (c). The conjecture, that the invariants defined by Milnor satisfy condition (c), is known as the *Milnor conjecture* and was proven by V. Voevodsky (see [Voe03] and [OVV07]).

2.4 Annihilating polynomials for quadratic forms

Throughout this section we will frequently make use of the following notation:

2.4.1 Notation. *Consider an $r \in \mathbb{Z}$. We simply write r for its image in both $\widehat{W}(K)$ and $W(K)$. If $r \geq 0$, then*

$$r = r \cdot [\langle 1 \rangle] = [r \times \langle 1 \rangle] \in \widehat{W}(K) \qquad \textit{and} \qquad r = \{r \times \langle 1 \rangle\} \in W(K).$$

If $r < 0$, then

$$r = r \cdot [\langle 1 \rangle] = -[(-r) \times \langle 1 \rangle] \in \widehat{W}(K)$$
$$\textit{and} \qquad r = r \cdot \{\langle 1 \rangle\} = \{-r \times \langle -1 \rangle\} \in W(K).$$

We have seen in Section 2.1 that both the Witt-Grothendieck ring $\widehat{W}(K)$ and the Witt ring $W(K)$ of a field K are Witt rings for the square class group $\mathcal{G}(K)$. With the help of the structure theorems we can now deduce specific statements about the embracing polynomial for isometry and equivalence classes of quadratic forms. We begin by studying the ring homomorphisms $\operatorname{Hom}(\widehat{W}(K), \mathbb{Z})$ and $\operatorname{Hom}(W(K), \mathbb{Z})$.

By Theorem 1.3.15 the ring homomorphisms $\operatorname{Hom}(\widehat{W}(K), \mathbb{Z})$ correspond to the non-maximal prime ideals of $\widehat{W}(K)$. Now $W(K) = \widehat{W}(K)/([\mathbb{H}])$, which implies that the elements of $\operatorname{Hom}(W(K), \mathbb{Z})$ are in one-to-one correspondence with those $\chi \in \operatorname{Hom}(\widehat{W}(K), \mathbb{Z})$ such that $([\mathbb{H}]) \subset \ker(\chi)$. Now let $\chi \in \operatorname{Hom}(\widehat{W}(K), \mathbb{Z})$ such that $([\mathbb{H}]) \not\subset \ker(\chi)$. This means that

$\chi([\langle 1,-1\rangle]) \neq 0$. Since $\chi([\langle 1\rangle]) = 1$, we must have $\chi([\langle 1,-1\rangle]) = 2$. By Proposition 2.1.16 we have $\langle 1,-1\rangle \cong \langle a,-a\rangle$ for all $a \in K^*$. In particular we must have $\chi([\langle a\rangle]) = 1$ for all $a \in K^*$. This shows that $\chi = \dim$.

2.4.2 Proposition. *Let $\pi : \widehat{W}(K) \to W(K)$ be the canonical projection. There exists a bijective map*

$$\operatorname{Hom}(W(K),\mathbb{Z}) \longrightarrow \operatorname{Hom}(\widehat{W}(K),\mathbb{Z}) \setminus \{\dim\}, \quad \overline{\chi} \longmapsto \overline{\chi} \circ \pi.$$

2.4.3 Corollary. *Let φ be an n-dimensional quadratic form over K. Then the signature set of $\{\varphi\}$ is $S_{[\varphi]} = S_{\{\varphi\}} \cup \{n\}$, and for the signature polynomial we obtain*

$$\mathbb{Z}[X] \ \ni\ P_{[\varphi]} \ =\ \begin{cases} P_{\{\varphi\}} & \text{if } n \in S_{\{\varphi\}}, \\ (X-n)P_{\{\varphi\}} & \text{otherwise.} \end{cases}$$

If the field K is not formally real, then by Theorem 2.1.42 we have $\operatorname{Hom}(W(K),\mathbb{Z}) = \varnothing$.

2.4.4 Corollary. *If K is not formally real, and if φ is a quadratic form over K, then*

$$P_{\{\varphi\}} \ =\ 1 \qquad \text{and} \qquad P_{[\varphi]} \ =\ X-n.$$

A field K is called *Pythagorean* if any sum of two squares in K is again a square. Thus, if K is Pythagorean, it follows that any sum of squares is again a square. By [Sch85, Theorem 4.10, Chapter 2] the Witt-Grothendieck ring $\widehat{W}(K)$ is torsion free if and only if K is Pythagorean, and $W(K)$ is torsion free if and only if K is formally real and Pythagorean.

2.4.5 Corollary. *Let K be a Pythagorean field. Then for any quadratic form φ over K we have*

$$\operatorname{Ann}_{[\varphi]} \ =\ (P_{[\varphi]}).$$

If in addition K is formally real, then also

$$\operatorname{Ann}_{\{\varphi\}} \ =\ (P_{\{\varphi\}}).$$

It follows from Corollary 1.2.9 that for $n \in \mathbb{N}_0$ the polynomial

$$P_n \ :=\ (X-n)(X-n+2)\cdots(X+n-2)(X+n) \ \in\ \mathbb{Z}[X] \tag{2.4}$$

annihilates the isometry and equivalence classes of all n-dimensional quadratic forms over K. As already mentioned in Remark 1.2.10 this was first proven by D. W. Lewis in [Lew87]. Lewis furthermore shows that his polynomials are in a certain sense optimal. More specifically there exists a field K and an n-dimensional quadratic form φ over K such that $\operatorname{Ann}_{[\varphi]} = \operatorname{Ann}_{\{\varphi\}} = (P_n)$. We can now give an easy and intuitive proof of this statement with the help of Corollary 2.4.5.

2.4.6 Examples.

(1) A field K is called *Euclidean* if K is formally real and $(K^*)^2 \subset K^*$ is the unique ordering of K. This implies that $K^* = (K^*)^2 \cup -(K^*)^2$, and hence $\mathcal{G}(K) = \{\overline{1}, \overline{-1}\}$. As in Example 2.1.28.(1) we show that $W(K) \cong \mathbb{Z}$. In particular there exists a unique ring homomorphism $W(K) \to \mathbb{Z}$.

(2) Let K be a field, and let t be transcendental over K. Consider the field of formal Laurent series $L := K((t))$ over K. If φ is a quadratic form over L, then there exist two quadratic forms φ_1 and φ_2 over K such that $\varphi \cong \varphi_1 \perp t\varphi_2$. Up to isometry φ_1 and φ_2 are uniquely determined by φ (see [Lam05, Corollary 1.6, Chapter VI]). Furthermore φ is isotropic if and only if φ_1 or φ_2 is isotropic (see [Lam05, Proposition 1.9, Chapter VI]). We obtain two group homomorphisms $\delta_1, \delta_2 : W(L) \to W(K)$, where δ_1 sends $\{\varphi\}$ to $\{\varphi_1\}$ and δ_2 sends $\{\varphi\}$ to $\{\varphi_2\}$. By [Lam05, Corollary 1.7, Chapter VI] δ_1 and δ_2 induce a ring isomorphism $W(L) \cong W(K)[\{\overline{1}, \overline{t}\}]$, where $\{\overline{1}, \overline{t}\}$ is the subgroup of $\mathcal{G}(L)$ generated by $\overline{t}$.

If K is formally real, then it follows that L is formally real as well. More specifically, if $\chi \in \operatorname{Hom}(W(K), \mathbb{Z})$, then there exist exactly two extensions $\chi_1, \chi_2 \in \operatorname{Hom}(W(L), \mathbb{Z})$ of χ such that $\chi_1(\overline{t}) = -\chi_2(\overline{t})$ (see [Lam05, Proposition 4.11, Chapter VIII]). Furthermore, if K is Pythagorean, then L is Pythagorean as well. △

2.4.7 Proposition. *For $n \in \mathbb{N}_0$ there exists a field K and a quadratic form φ over K such that* $\operatorname{Ann}_{[\varphi]} = \operatorname{Ann}_{\{\varphi\}} = (P_n)$.

Proof. Let F be a Euclidean field, and for $n \in \mathbb{N}_0$ set $K := F((t_1))\cdots((t_n))$, where t_i is transcendental over $F((t_1))\cdots((t_{i-1}))$ for $i = 1, \dots, n$. Then by the Examples 2.4.6.(1) and (2) the field L is Pythagorean. In addition we have $|\operatorname{Hom}(W(K), \mathbb{Z})| = 2^n$. More specifically for every subset $N \subset \{1, \dots, n\}$ there exists a unique $\chi \in \operatorname{Hom}(W(K), \mathbb{Z})$ such that $\chi(t_i) = 1$ for all $i \in N$ and $\chi(t_i) = -1$ for all $i \in \{1, \dots, n\} \setminus N$. Now consider the quadratic form $\varphi = \langle t_1, \dots, t_n \rangle$ over K. We see immediately that

$$S_{[\varphi]} = S_{\{\varphi\}} = \{-n, -n+2, \dots, n-2, n\}.$$

By Corollary 2.4.5 it follows that

$$\operatorname{Ann}_{[\varphi]} = \operatorname{Ann}_{\{\varphi\}} = (P_n). \qquad \square$$

We continue by studying annihilating ideals of arbitrary quadratic forms. There exist a number of fields K, where the structure of the Witt ring is completely known. We now use Theorem 1.5.5 to determine minimal sets of generators for $\operatorname{Ann}_{[\varphi]}$ and $\operatorname{Ann}_{\{\varphi\}}$, where φ is an arbitrary quadratic form over such a field K.

2.4.8 Examples. We start with those fields K, which we have already examined in the Examples 2.1.28.(1) and (2).

(1) Let $K = \mathbb{R}$. Then $\mathcal{G}(\mathbb{R}) = \{\overline{1}, \overline{-1}\}$, and it is clear that there exist two ring homomorphism $\widehat{W}(\mathbb{R}) \to \mathbb{Z}$, namely the dimension dim with and $\dim([\langle 1\rangle]) = \dim([\langle -1\rangle]) = 1$ and the signature sign with $\operatorname{sign}([\langle 1\rangle]) = 1$ and $\operatorname{sign}([\langle -1\rangle]) = -1$. For every quadratic form φ of dimension n over $\mathbb{R}$ there exist $r, s \in \mathbb{N}$ such that $\varphi \cong (r \times \langle 1\rangle) \perp (s \times \langle -1\rangle)$. Then $\dim([\varphi]) = r + s = n$ and $\operatorname{sign}([\varphi]) = r - s$. Since $\widehat{W}(\mathbb{R})$ is torsion free it follows from Corollary 1.5.4 that

$$\operatorname{Ann}_{[\varphi]} = \begin{cases} (X - n) & \text{if } s = 0, \\ ((X - (r - s))(X - n)) & \text{otherwise.} \end{cases}$$

Now by Proposition 2.4.2 the only element of $\mathrm{Hom}(W(K),\mathbb{Z})$ is the induced homomorphism $\overline{\mathrm{sign}}$. The Witt ring $W(K)$ is also torsion free, whence

$$\mathrm{Ann}_{\{\varphi\}} \;=\; (X-(r-s)).$$

(2) Consider any algebraically closed field K. Then the square class group of K is trivial, and any quadratic form φ of dimension n is isomorphic to $n\times\langle 1\rangle$. By Example 2.1.28.(2) we know that $\widehat{W}(K)\cong\mathbb{Z}$ is torsion free. We obtain

$$\mathrm{Ann}_{[\varphi]} \;=\; (X-n).$$

For the Witt ring we know that $W(K)\cong{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. It follows that $P_{\{\varphi\}}=1$. Furthermore $2=0$ in $W(K)$. Thus by Theorem 1.5.5

$$\mathrm{Ann}_{\{\varphi\}} \;=\; (2,X-n). \qquad\triangle$$

We could just as well have studied annihilating ideals of quadratic forms over finite fields, but there exists a more general approach, which makes use of the fact that finite fields have a low level and that the third power of their fundamental ideal vanishes.

Consider a field K with $s(K)=1$. This implies that $2=0$ in $W(K)$. Let $x\in\widehat{W}(K)$ be arbitrary with $\dim(x)$ even, and let $\overline{x}$ be its image in $W(K)$. By Lemma 1.4.7 we know that 2 divides x^2 and $\overline{x}^2$. In particular $\overline{x}^2=0$. Since an element of $\widehat{W}(K)$ is 0 if and only if it has dimension 0 and its image in $W(K)$ vanishes, it follows that $x^2=0$ if and only if $\dim(x)=0$. We thus obtain the following proposition.

2.4.9 Proposition. *Let K be a field with $s(K)=1$, and let φ be an arbitrary quadratic form over K. If* $\dim(\varphi)=n$*, then*

$$\mathrm{Ann}_{[\varphi]} \;=\; \begin{cases}(X-n) & \text{if } \varphi\cong n\times\langle 1\rangle,\\ (2(X-n),(X-n)^2) & \text{otherwise,}\end{cases}$$

and

$$\mathrm{Ann}_{\{\varphi\}} \;=\; \begin{cases}(2,X-n) & \text{if } \varphi\cong n\times\langle 1\rangle,\\ (2,(X-n)^2) & \text{otherwise.}\end{cases}$$

Proof. The statement about $\mathrm{Ann}_{[\varphi]}$ follows from Corollary 2.4.4. For the statement about $\mathrm{Ann}_{\{\varphi\}}$ assume that $\{\varphi\}=m$ for some $m\in\mathbb{Z}$. Then we must have $m\equiv n \pmod 2$, and since $2=0$ in $W(K)$, it follows that $\varphi\cong n\times\langle 1\rangle$. In this case $X-n$ is clearly an annihilating polynomial of $\{\varphi\}$. If on the other hand $X-m$ annihilates $\{\varphi\}$ for some $m\in\mathbb{Z}$, then it follows that $\{\varphi\}=m=n$ in $W(K)$. Therefore $\mathrm{Ann}_{\{\varphi\}}=(2,X-m)=(2,X-n)$. □

The case of fields with level 2 is notably more complicated, since by [OG97, Table 1 & Table 2] there exists a field K with $s(K)=2$ and a quadratic form φ over K such that $\mathrm{Ann}_\varphi=\{4,2X,X^4\}$. By Theorem 1.5.5 and Lemma 1.4.7 this is in a sense the worst case when it comes to the degree of annihilating polynomials. As will become apparent later, we cannot use the first three cohomological invariants to classify annihilating ideals of quadratic forms over such a field K. In the following we choose a different approach to study annihilating polynomials of quadratic forms over at least certain classes of fields with level 2. In addition our approach will include a number of fields with level 4. More specifically we study fields K such that $I^k(K) = \{0\}$ for some $k \in \mathbb{N}$ with $k \leq 3$.

If $k = 1$, then every even-dimensional quadratic form over K is hyperbolic. This implies that $\langle 1, -a\rangle \sim 0$ for all $a \in K^*$. In other words every element in K^* is a square. Hence if φ is an n-dimensional quadratic form over K, then $\varphi \cong n$. In particular $s(K) = 1$.

2.4.10 Proposition. *Let K be a field with $I(K) = \{0\}$, and let φ be an arbitrary quadratic form over K. If $\dim(\varphi) = n$, then*

$$\mathrm{Ann}_{[\varphi]} \;=\; (X - n) \qquad \textit{and} \qquad \mathrm{Ann}_{\{\varphi\}} \;=\; (2, X - n).$$

Next assume that $I(K) \neq \{0\}$ and $I^2(K) = \{0\}$. Then $4 = 2^2 = 0$ in $W(K)$ and $s(K) \leq 2$. If $s(K) = 1$, then we can apply Proposition 2.4.9. So assume that $s(K) = 2$. We consider the dimension index $e_0 : W(K) \to \mathbb{Z}/2\mathbb{Z}$ and the discriminant $e_1 : W(K) \to \mathcal{G}(K)$. If φ is a quadratic form over K with $e_0(\{\varphi\}) = 0$, then $\{\varphi\}$ lies in $I(K)$. If in addition $e_1(\{\varphi\}) = 0$, then $\{\varphi\}$ lies in $I^2(K)$ and must therefore be 0. This shows that equivalence classes of quadratic forms over K can be classified with the help of the dimension index and the discriminant. In particular a polynomial $P \in \mathbb{Z}[X]$ is an annihilating polynomial of $\{\varphi\}$ if $e_0(P(\{\varphi\})) = 0$ and $e_1(P(\{\varphi\})) = 0$. If $\dim(\varphi) = n$, then $\{\varphi\} - n \in I(K)$, and it follows that

$$2(\{\varphi\} - n) \;=\; 0 \qquad \text{and} \qquad (\{\varphi\} - n)^2 \;=\; 0.$$

Since an element $x \in \widehat{W}(K)$ is 0 if and only if $\dim(x) = 0$ and the image of x in $W(K)$ is 0, we obtain the following proposition.

2.4.11 Proposition. *Let K be a field with $I(K) \neq \{0\}$, $I^2(K) = \{0\}$, and let φ be an arbitrary, n-dimensional quadratic form over K.*

(1) If $s(K) = 1$, then see Proposition 2.4.9.

(2) If $s(K) = 2$, then

$$\mathrm{Ann}_{[\varphi]} \;=\; \begin{cases} (X - n) & \textit{if } \varphi \cong n \times \langle 1\rangle, \\ (2(X - n), (X - n)^2) & \textit{otherwise,} \end{cases}$$

and

$$\mathrm{Ann}_{\{\varphi\}} \;=\; \begin{cases} (4, X - m) & \textit{if } \{\varphi\} = m \textit{ for some } m \in \mathbb{Z}, \\ (4, 2(X - n), (X - n)^2) & \textit{otherwise.} \end{cases}$$

Now let $K = \mathbb{F}_q$ be a finite field, where q is an odd prime power. In Example 2.1.28.(3) we have seen that $I(\mathbb{F}_q) \neq \{0\}$ and $I^2(K) = \{0\}$. If $q \equiv 1 \pmod 4$ then $s(K) = 1$, and if $q \equiv 3 \pmod 4$ then $s(K) = 2$. We can thus use the previous results, to classify annihilating ideals of quadratic forms over $\mathbb{F}_q$.

2.4.12 Corollary. *Let $\mathbb{F}_q$ be a finite field with odd characteristic, and let φ be an arbitrary quadratic form over $\mathbb{F}_q$ of dimension n. Then*

$$\mathrm{Ann}_{[\varphi]} = \begin{cases} (X-n) & \textit{if } \det(\varphi)=1, \\ (2(X-n),(X-n)^2) & \textit{otherwise,} \end{cases}$$

and

(1) if $q \equiv 1 \pmod 4$, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2, X-n) & \textit{if } \det(\varphi)=1, \\ (2,(X-n)^2) & \textit{otherwise.} \end{cases}$$

(2) if $q \equiv 3 \pmod 4$, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (4, X-n) & \textit{if } \det(\varphi)=1, \\ (4, X-n+2) & \textit{otherwise.} \end{cases}$$

Proof. We deduce from Example 2.1.28.(3) that for arbitrary q either $\varphi \cong n \times \langle 1\rangle$ or $\varphi \cong ((n-1)\times\langle 1\rangle)\perp\langle s\rangle$, where $s \in \mathbb{F}_q^*$ is not a square. The first case occurs if and only if $\det(\varphi)=1$, and then $X-n$ annihilates $[\varphi]$ and $\{\varphi\}$. In the other case $\varphi \ncong n$, hence $X-n$ is not an annihilating polynomial of $[\varphi]$. Furthermore, if $q \equiv 1 \pmod 4$, then $s \neq -1$ and it follows that $\{\varphi\} \neq m$ for all $m \in \mathbb{Z}$. This implies that there does not exist a monic linear factor which annihilates $\{\varphi\}$. If $q \equiv 3 \pmod 4$, then $s=-1$ and $\{\varphi\} = n-2$, which shows that $X-n+2$ annihilates $\{\varphi\}$. □

Let K be a field with $I^3(K)=\{0\}$ and $I^2(K)\neq\{0\}$. In this case $2^3=0$ in $W(K)$, which implies that $s(K)\leq 3$. As in the previous case we see that now the dimension index e_0, the discriminant e_1 and the Clifford invariant $e_2 : W(K) \to \mathrm{Br}(K)$ classify equivalence classes of quadratic forms over K. But compared to the calculations concerning the determinant and the discriminant, the calculations involving the Clifford invariant are notably more complicated. The complete and detailed calculations needed can be found in Appendix A.1.

2.4.13 Notation. *For the rest of this section we allow the following notation:*

(1) Let $r \in \mathbb{Z}$. If $r \geq 0$, then we simply write r for $r \times \langle 1\rangle$. If $r < 0$, then we write r for $(-r)\times\langle -1\rangle$. Note, that in the case $r<0$ the image of $r \in \widehat{W}(K)$ is equal to $-[(-r)\times\langle 1\rangle] \neq [(-r)\times\langle -1\rangle]$ (compare Notation 2.4.1).

(2) Let $a,b \in K^*$. We simply write $(a,b)_K$ for its equivalence class $[(a,b)_K]$ in the Brauer group $\mathrm{Br}(K)$.

Let φ be an n-dimensional quadratic form over K. We start with a few observations on $\mathrm{Ann}_{[\varphi]}$. Since K is not formally real, we have seen that $Q_{[\varphi]} = X-n$. If $\varphi \cong n$, then of course $\mathrm{Ann}_{[\varphi]} = (X-n)$. In the other case we will show that there exists a linear factor $X-r \in \mathbb{Z}[X]$ such that $(X-r)(X-n) \in \mathrm{Ann}_{[\varphi]}$. Now we apply Theorem 1.5.5. Since the level $s(K)$ of the field K is either 1, 2 or 4, and since the equivalence class of $4 \times (\varphi \perp -n)$ lies in $I^3(K)$, it remains to check whether $2(X-n) \in \mathrm{Ann}_{[\varphi]}$ or not. We obtain

$$\mathrm{Ann}_{[\varphi]} = (2(X-n), (X-r)(X-n)) \qquad \text{or} \qquad \mathrm{Ann}_{[\varphi]} = (4(X-n), (X-r)(X-n)).$$

To find a full set of generators for $\mathrm{Ann}_{\{\varphi\}}$ is more complicated, since we have $Q_{\{\varphi\}} = 1$. First we exclude the trivial case $\varphi \sim r$ for some $r \in \mathbb{Z}$, since in that case $\mathrm{Ann}_{\{\varphi\}} = (2s(K), X-r)$. In the other cases we consider the following lemma.

2.4.14 Lemma. *For any $x \in I(K)$ we have $x(x+2) \in 2I^2(K)$.*
[OG97, Lemma 3.4]

Proof. Let φ be a quadratic form over K with $\{\varphi\} = x$. Since $I(K)$ is generated by 1-fold Pfister forms we can write $\varphi \sim \sum_{i=1}^r a_i\tau_i$ with $a_i \in K^*$, 1-fold Pfister forms τ_i, and some $r \in \mathbb{N}_0$. Say $\tau_i = \langle 1, b_i\rangle$ for some $b_i \in K^*$, then we see immediately that $\tau_i \otimes \tau_i \cong 2 \times \tau_i$. Hence

$$\begin{aligned}
\varphi \otimes \varphi \perp 2 \times \varphi \quad &\sim \quad \left(\sum_{i=1}^r a_i\tau_i\right)^2 \perp 2 \times \sum_{i=1}^r a_i\tau_i \\
&\cong \quad \left(\sum_{i=1}^r a_i^2(\tau_i \otimes \tau_i)\right) \perp \left(\sum_{i\neq j} a_ia_j(\tau_i \otimes \tau_j)\right) \perp 2 \times \sum_{i=1}^r a_i\tau_i \\
&\cong \quad 2 \times \left(\sum_{i<j} a_ia_j(\tau_i \otimes \tau_j)\right) \perp 2 \times \sum_{i=1}^r \langle 1, a_i\rangle \otimes \tau_i.
\end{aligned}$$

Accordingly $x(x+2) = x^2 + 2x \in 2I^2(K)$. □

The previous lemma implies that $X(X+2) \in \mathbb{Z}[X]$ is an annihilating polynomial for every equivalence class of even-dimensional quadratic forms over K. This fact is also a consequence of the calculations concerning the Clifford invariant that we will undertake below. It follows that $(X+1)(X+3)$ is an annihilating polynomial for every equivalence class of odd-dimensional quadratic forms. Now if $s(K) = 1$, then $2 = 0 \in W(K)$, and we can conclude that

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2, X(X+2)) = (2, X^2) & \text{for } \dim(\varphi) \text{ even,} \\ (2, (X+1)(X+3)) = (2, (X+1)^2) & \text{for } \dim(\varphi) \text{ odd.} \end{cases}$$

If $s(K) = 2$ and $\dim(\varphi)$ is even, then we only need to check whether the polynomial $2X$ lies in $\mathrm{Ann}_{\{\varphi\}}$, since $2X \in \mathrm{Ann}_{\{\varphi\}}$ if and only if $2(X+2) \in \mathrm{Ann}_{\{\varphi\}}$. So

$$\mathrm{Ann}_{\{\varphi\}} = (4, 2X, X(X+2)) = (4, 2X, X^2) \qquad \text{or} \qquad \mathrm{Ann}_{\{\varphi\}} = (4, X(X+2)).$$

For the odd-dimensional case it follows that

$$\mathrm{Ann}_{\{\varphi\}} = (4, 2(X+1), (X+1)^2) \qquad \text{or} \qquad \mathrm{Ann}_{\{\varphi\}} = (4, (X+1)(X+3)).$$

Finally, in the case where $s(K) = 4$ and $\dim(\varphi)$ is even, it suffices to consider the polynomials $2X$, $2(X+2)$, and $4X$. The case $2X, 2(X+2) \in \mathrm{Ann}_{\{\varphi\}}$ would imply $4 \in \mathrm{Ann}_{\{\varphi\}}$, which is impossible since $s(K) > 2$. Since φ is even-dimensional, the equivalence class of $4 \times \varphi$ lies in $I^3(K)$. Hence in any case $4X$ lies in $\mathrm{Ann}_{\{\varphi\}}$. Since $X(X+2) = X^2+2X = (X+2)^2-2(X+2)$ we obtain exactly the three cases

$$\begin{array}{rcll}
\mathrm{Ann}_{\{\varphi\}} & = & (8, 2X, X^2), & \\
\mathrm{Ann}_{\{\varphi\}} & = & (8, 2(X+2), (X+2)^2) & \text{or} \\
\mathrm{Ann}_{\{\varphi\}} & = & (8, 4X, X(X+2)). &
\end{array}$$

For the case where φ is odd-dimensional we obtain

$$\begin{array}{rcll}
\mathrm{Ann}_{\{\varphi\}} & = & (8, 2(X+1), (X+1)^2), & \\
\mathrm{Ann}_{\{\varphi\}} & = & (8, 2(X+3), (X+3)^2) & \text{or} \\
\mathrm{Ann}_{\{\varphi\}} & = & (8, 4(X+1), (X+1)(X+3)). &
\end{array}$$

We will now begin our actual calculations. As we have noted before, for an element $\{\varphi\}$ of $W(K)$ to be 0, φ must have even dimension, trivial discriminant, and trivial Clifford invariant. An element $x \in \widehat{W}(K)$ is 0, if it has dimension 0 and its image in $W(K)$ vanishes. The calculations concerning the dimension are all trivial, and since the discriminant vanishes on the second power of the fundamental ideal, we will only need it below for our calculations concerning the Clifford invariant.

It is necessary that we establish certain formulas for the Clifford invariant. Let φ and ψ be quadratic forms over K. Then, by using Corollary 2.2.29 and Lemma 2.2.30, we obtain

$$c(\varphi \otimes \psi) \;=\; (d(\varphi), d(\psi))_K \qquad \text{for } \varphi \text{ and } \psi \text{ even-dimensional} \tag{2.5}$$

(see Calculation A.1.2). By definition of the discriminant $d(r \times \langle 1 \rangle) = (-1)^{\frac{r(r-1)}{2}}$, and it can easily be checked that $d(r \times \langle -1 \rangle) = (-1)^{\frac{r(r+1)}{2}} = (-1)^{\frac{-r(-r-1)}{2}}$ for all $r \in \mathbb{N}_0$. To put it more shortly:

$$d(r) \;=\; (-1)^{\frac{r(r-1)}{2}} \qquad \forall\, r \in \mathbb{Z}$$

(see Calculation A.1.4). It is clear that $d(\varphi \perp \psi) = d(\varphi)d(\psi)$ for even-dimensional φ and ψ. If φ and ψ have odd dimension, then we have $d(\varphi \perp \psi) = -d(\varphi)d(\psi)$. Let $n = \dim(\varphi)$ and $a, b \in \mathbb{Z}$ with $n \equiv a \equiv b \pmod 2$. If we combine (2.5) with our considerations about the discriminant we obtain

$$c((\varphi \perp a) \otimes (\varphi \perp b)) \;=\; ((-1)^n d(\varphi), -1)_K^{1+\frac{a(a-1)}{2}+\frac{b(b-1)}{2}} \, (-1,-1)_K^{\frac{a(a-1)}{2}\frac{b(b-1)}{2}} \tag{2.6}$$

and

$$c(2 \times (\varphi \perp a)) \;=\; ((-1)^n d(\varphi), -1)_K \, (-1,-1)_K^{\frac{a(a-1)}{2}} \tag{2.7}$$

(see Calculations A.1.5 and A.1.10).

2.4.15 Examples. We now consider the formulas (2.6) and (2.7) in a number of special cases that are of particular interest to us. Let φ be an n-dimensional quadratic form over K.

(1) Assume that $b \equiv a \pmod 4$ with $a \equiv n \pmod 2$. Then the table

n a	even	odd
$\equiv 0, 1 \pmod 4$	$(d(\varphi), -1)_K$	$(-d(\varphi), -1)_K$
$\equiv 2, 3 \pmod 4$	$(-d(\varphi), -1)_K$	$(d(\varphi), -1)_K$

shows the possible values of both $c((\varphi \perp a) \otimes (\varphi \perp b))$ and $c(2 \times (\varphi \perp a))$ depending on n and a (see Calculations A.1.7 and A.1.11).

(2) Set $a = -r$ and $b = -s$ with $r \equiv s \equiv n \pmod 2$. This will be the case we have to consider in the next section in the context of signatures. Then we obtain the table

r s	$\equiv 0, 1 \pmod 4$	$\equiv 2, 3 \pmod 4$
$\equiv 0, 1 \pmod 4$	$(d(\varphi), -1)_K$	1
$\equiv 2, 3 \pmod 4$	1	$(-d(\varphi), -1)_K$

for $c((\varphi \perp -r) \otimes (\varphi \perp -s))$ with n arbitrary. In particular

$$c((\varphi \perp -r) \otimes (\varphi \perp -s)) \;=\; \left((-1)^{\frac{r(r-1)}{2}} d(\varphi), -1\right)_K$$

for $r \equiv s \pmod 4$. Furthermore

$$c(2 \times (\varphi \perp -r)) \;=\; \left((-1)^{\frac{r(r-1)}{2}} d(\varphi), -1\right)_K \tag{2.8}$$

(see Calculations A.1.8 and A.1.12).

(3) Consider the case $a = -n$ and $b = -r$ with $r \equiv n \pmod 2$. This case will come up in the context of isometry classes of quadratic forms. We obtain the surprisingly simple table

n r	$\equiv 0, 1 \pmod 4$	$\equiv 2, 3 \pmod 4$
$\equiv 0, 1 \pmod 4$	$(\det(\varphi), -1)_K$	1
$\equiv 2, 3 \pmod 4$	1	$(\det(\varphi), -1)_K$

for $c((\varphi \perp -n) \otimes (\varphi \perp -r))$. In addition we have

$$c(2 \times (\varphi \perp -n)) \;=\; (\det(\varphi), -1)_K$$

as a special case of equation (2.8) (see Corollaries A.1.9 and A.1.13). △

Let $a \in K^*$. By Corollary 2.2.28 we know that $\big(a,-1\big)_K = 1 \in \mathrm{Br}(K)$ if and only if $\langle 1,1,-a\rangle$ is isotropic if and only if a is a sum of two squares in K. Using this we can now translate the above tables into the following theorem.

2.4.16 Theorem. *Let K be a field with $I^3(K) = \{0\}$ and $I^2(K) \neq \{0\}$, and let φ be a quadratic form over K with $\dim(\varphi) = n \in \mathbb{N}_0$.*

(1) If $\varphi \cong n \times \langle 1\rangle$, then $\mathrm{Ann}_{[\varphi]} = (X-n) \subset \mathbb{Z}[X]$.

(2) If $\varphi \not\cong n \times \langle 1\rangle$, and

(a) if $s(K) = 1$, then $\mathrm{Ann}_{[\varphi]} = (2(X-n),(X-n)^2)$.

(b) if $s(K) = 2, 4$, then

$$\mathrm{Ann}_{[\varphi]} = \begin{cases} (2(X-n),(X-n)^2) & \text{if } \det(\varphi) \text{ is a sum of two squares in } K, \\ (4(X-n),(X-n+2)(X-n)) & \text{otherwise.} \end{cases}$$

Next we formulate an analogous result for $\mathrm{Ann}_{\{\varphi\}}$. For the case $s(K) < 4$ we note that $4\times\langle a\rangle \sim 0$ for any $a \in K^*$. This implies $\langle\langle 1,-a\rangle\rangle \cong \langle\langle 1,a\rangle\rangle$. Therefore $(-a,-1)_K = (a,-1)_K$ and $(-1,-1)_K = 1$ in $\mathrm{Br}(K)$.

2.4.17 Theorem. *Let K be a field with $I^3(K) = \{0\}$ and $I^2(K) \neq \{0\}$, and let φ be a quadratic form over K with $\dim(\varphi) = n \in \mathbb{N}_0$.*

(1) If $\varphi \sim r$ with $r \in \mathbb{Z}$, then $\mathrm{Ann}_{\{\varphi\}} = (2s(K), X-r) \subset \mathbb{Z}[X]$.

(2) If $\varphi \not\sim r$ for all $r \in \mathbb{Z}$, and

(a) if $s(K) = 1$, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2,X^2) & \text{if } n \text{ is even,} \\ (2,(X+1)^2) & \text{if } n \text{ is odd.} \end{cases}$$

(b) if $s(K) = 2$, and

(i) if n is even, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (4,2X,X^2) & \text{if } d(\varphi) \text{ is a sum of two squares in } K, \\ (4,X(X+2)) & \text{otherwise.} \end{cases}$$

(ii) if n is odd, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (4,2(X+1),(X+1)^2) & \text{if } d(\varphi) \text{ is a sum of two squares in } K, \\ (4,(X-1)(X+1)) & \text{otherwise.} \end{cases}$$

(c) if $s(K) = 4$, and

(i) if n is even, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (8, 2X, X^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+2), (X+2)^2) & \textit{if } -d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 4X, X(X+2)) & \textit{otherwise.} \end{cases}$$

(ii) if n is odd, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (8, 2(X-1), (X-1)^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+1), (X+1)^2) & \textit{if } -d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 4(X+1), (X-1)(X+1)) & \textit{otherwise.} \end{cases}$$

Instead of considering annihilating polynomials for a given quadratic form over a field K, one can also study the polynomials that annihilate all elements of the Witt ring $W(K)$. The existence of the dimension homomorphism $\dim : \widehat{W}(K) \to \mathbb{Z}$ implies that there do not exist polynomials that annihilate all of $\widehat{W}(K)$.

2.4.18 Definition. *Let K be a field. We set*

$$\begin{aligned} \mathrm{Ann}^{(e)}_{W(K)} &:= \{P \in \mathbb{Z}[X] \mid P(\{\varphi\}) = 0 \ \forall \ \{\varphi\} \in I(K)\}, \\ \mathrm{Ann}^{(o)}_{W(K)} &:= \{P \in \mathbb{Z}[X] \mid P(\{\varphi\}) = 0 \ \forall \ \{\varphi\} \in W(K) \setminus I(K)\}, \\ \mathrm{Ann}_{W(K)} &:= \mathrm{Ann}^{(e)}_{W(K)} \cap \mathrm{Ann}^{(o)}_{W(K)}. \end{aligned}$$

We can now use the above results to give a complete classification of $\mathrm{Ann}^{(e)}_{W(K)}$ for all fields K with $I^3(K) = \{0\}$.

2.4.19 Corollary. *Let K be a field with $I^3(K) = \{0\}$. Then the table*

$\mathrm{Ann}^{(e)}_{W(K)}$	$I(K) = \{0\}$	$I^2(K) = \{0\}, I(K) \neq \{0\}$	$I^3(K) = \{0\}, I^2(K) \neq \{0\}$
$s(K) = 1$	$(2, X)$	$(2, X^2)$	$(2, X^2)$
$s(K) = 2$		$(4, 2X, X^2)$	$\begin{cases} (4, 2X, X^2) & \textit{if } 2I(K) = \{0\} \\ (4, X(X+2)) & \textit{if } 2I(K) \neq \{0\} \end{cases}$
$s(K) = 4$			$(8, 4X, X(X+2))$

describes all possible values of $\mathrm{Ann}^{(e)}_{W(K)}$.

Proof. If $s(K) = 1$, then the claim follows from the Propositions 2.4.9 and 2.4.10. The case $s(K) = 2$ and $I^2(K) = \{0\}$, $I(K) \neq \{0\}$, follows immediately from the observation that $X, X+2 \notin \mathrm{Ann}^{(e)}_{W(K)}$.

Now assume that $s(K) = 2$ and $I^3(K) = \{0\}$, $I^2(K) \neq \{0\}$. If $2I(K) = \{0\}$, then $2X \in \mathrm{Ann}^{(e)}_{W(K)}$. Since $X(X+2) = X^2 + 2X$, we obtain $\mathrm{Ann}^{(e)}_{W(K)} = (4, 2X, X^2)$. If $2I(K) \neq \{0\}$, then there exists some $x \in I(K)$ such that $2x \neq 0$. As $4 = 0$ in $W(K)$, it follows that $2(x+2) \neq 0$. Since $x(x+2) = 0$, we must have $x^2 \neq 0$ and $(x+2)^2 \neq 0$. This implies $2X, 2(X+2), X^2, (X+2)^2 \notin \mathrm{Ann}^{(e)}_{W(K)}$, and therefore $\mathrm{Ann}^{(e)}_{W(K)} = (4, X(X+2))$.

Finally, suppose that $s(K) = 4$ and $I^3(K) = \{0\}$, $I^2(K) \neq \{0\}$. Since $0, 2 \in I(K)$, and since $s(K) = 4$, it follows that $2X, 2(X+2) \notin \mathrm{Ann}^{(e)}_{W(K)}$. As above we obtain $X^2, (X+2)^2 \notin \mathrm{Ann}^{(e)}_{W(K)}$. Thus we must have $\mathrm{Ann}^{(e)}_{W(K)} = \{8, 4X, X(X+2)\}$. □

It is easy to formulate an analogous result for $\mathrm{Ann}^{(o)}_{W(K)}$. The corresponding result for $\mathrm{Ann}_{W(K)}$ is then an immediate consequence.

2.4.20 Remark. In [OG97, Table 1] J. van Geel and V. Ongenae give a full list of all possible $\mathrm{Ann}^{(e)}_{W(K)}$ for fields K with $s(K) \leq 4$. For those cases that we have considered further up, the results by van Geel and Ongenae coincide with our observations. Whereas we have made use of our results about annihilating polynomials for single quadratic forms, van Geel and Ongenae take the approach of specifically excluding coefficients of possible annihilating polynomials with the help of relations in $W(K)$. △

Let K be a field, and let R be either $\widehat{W}(K)$ or $W(K)$. Consider a unit $x \in R^*$. By Proposition 1.4.9 and Corollary 1.4.11 we know that the inverse of x is a polynomial in x with integer coefficients. We want to use the results obtained previously in this section to give specific and particularly simple formulas for calculating inverses in those cases, where K is a field with $s(K) = 1$ or $I^3(K) = 0$.

If $R = \widehat{W}(K)$ with K an arbitrary field, then $\dim \in \mathrm{Hom}(\widehat{W}(K), \mathbb{Z})$, which implies that $\mathrm{char}(R) = 0$. If φ is a quadratic form over K such that $[\varphi] \in (\widehat{W}(K))^*$, then by Theorem 1.4.10 we must have $\dim(\varphi) = 1$. Since $\langle a \rangle \otimes \langle a \rangle \cong \langle 1 \rangle$, it follows that the isometry class of a quadratic form is invertible in $\widehat{W}(K)$ if and only if it has dimension 1. Thus we can focus on calculating inverses in the Witt ring $W(K)$.

2.4.21 Proposition. *If K is a field with with $s(K) = 1$ or $I^3(K) = 0$ then $(W(K))^*$ has exponent 2. More specifically, if φ is a quadratic form over K with odd dimension, then $\{\varphi\}$ is invertible and $\{\varphi\}^{-1} = \{\varphi\}$.*

Proof. If $s(K) = 1$ or $I^3(K) = 0$, then in particular $s(K) \neq \infty$. By Theorem 2.1.42 the ring $W(K)$ is local with $(W(K))^* = W(K) \setminus I(K)$. Consider any odd-dimensional quadratic form φ over K.

If $s(K) = 1$, then by Lemma 1.4.7 the polynomial $(X+1)^2$ annihilates $\{\varphi\}$. Since $X^2 - 1 = (X+1)^2 - 2(X-1)$, and since $2 = 0 \in W(K)$, it follows that $X^2 - 1$ annihilates $W(K)$ as well. In other words $\{\varphi\}^2 = 1$.

In the case where $I^3(K) = 0$, it follows from Example 2.4.15.(2) that $(X+1)(X-1) = X^2 - 1$ is an annihilating polynomial for $\{\varphi\}$. Therefore also in this case $\{\varphi\}^2 = 1$. □

2.5 Local and global fields

In this section we will first consider local fields K that have a finite residue field. These are fields which are complete with respect to a discrete valuation. With the help of this valuation it is then possible to completely classify quadratic forms over K. To learn more about quadratic forms over local fields see [Lam05, Chapter VI]. The only properties we will need here are the following (see [Lam05, Corollary 2.15, Chapter 2]):

(i) For a local field K we have $I^3(K) = \{0\}$ and $I^2(K) \neq \{0\}$.

(ii) From the previous property it follows that $s(K) = 1, 2, 4$.

(iii) Up to isometry there exists exactly one anisotropic quadratic form of dimension 4 over K.

Let φ be a quadratic form over K. When considering the annihilating ideal $\mathrm{Ann}_{[\varphi]}$ it is not necessary to make any changes to Theorem 2.4.16. When considering $\mathrm{Ann}_{\{\varphi\}}$ it is however possible to simplify Theorem 2.4.17 for the case where K is a local field. If $s(K) < 4$, then it follows from our observations just before Theorem 2.4.17 that $d(\varphi)$ is a sum of two squares if and only if $-d(\varphi)$ is a sum of two squares. We were not able to make a similar statement for the case $s(K) = 4$. However if K is local, than we can make use of the fact that there exists up to isometry only one anisotropic, 4-dimensional quadratic form over K.

Suppose that $s(K) = 4$. Let $a \in K^*$. Assume that $\langle\langle 1, a\rangle\rangle$ and $\langle\langle 1, -a\rangle\rangle$ are both anisotropic. Since up to isometry there exists only one anisotropic quadratic form of dimension 4 over K, this implies $\langle\langle 1, a\rangle\rangle \sim \langle\langle 1, -a\rangle\rangle$. It follows that $4 \times \langle a\rangle \sim 0$, which is impossible since $s(K) = 4$. Analogously it can be shown that not both $\langle\langle 1, a\rangle\rangle$ and $\langle\langle 1, -a\rangle\rangle$ can be hyperbolic. Hence either a is a sum of two squares in K or $-a$ is a sum of two squares in K. In particular exactly one of the elements $d(\varphi)$ and $-d(\varphi)$ is a sum of two squares. Thus we can state the following special case of Theorem 2.4.17.

2.5.1 Corollary. *Let K be a local field with finite residue field, and let φ be a quadratic form over K with $\dim(\varphi) = n \in \mathbb{N}_0$.*

(1) If $\varphi \sim r$ with $r \in \mathbb{Z}$, then $\mathrm{Ann}_{\{\varphi\}} = (2s(K), X - r) \subset \mathbb{Z}[X]$.

(2) If $\varphi \not\sim r$ for all $r \in \mathbb{Z}$, and

(a) if $s(K) = 1$, then see Theorem 2.4.17.

(b) if $s(K) = 2$, then see Theorem 2.4.17.

(c) if $s(K) = 4$, and

(i) if n is even, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (8, 2X, X^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+2), (X+2)^2) & \textit{otherwise.} \end{cases}$$

(ii) if n is odd, then

$$\mathrm{Ann}_{\{\varphi\}} \;=\; \begin{cases} (8, 2(X-1), (X-1)^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+1), (X+1)^2) & \textit{otherwise.} \end{cases}$$

We can now make use of the above results to determine the annihilating ideal of a quadratic form φ over a global field K with the help of the Hasse-Minkowski Theorem ([Lam05, Hasse-Minkowski-Principle 3.1, Chapter VI]). For an introduction to quadratic forms over global fields see [Lam05, Chapter VI].

Let K be a global field, and let V be the set of equivalence classes of absolute values of K. For every $\nu \in V$ choose a fixed representative $|\cdot|_\nu : K \to \mathbb{R}$ of the class ν. Denote by K_ν the completion of K with respect to $|\cdot|_\nu$. We can write V as the disjoint union $V = V_\mathbb{R} \cup V_\mathbb{C} \cup V_{\mathrm{fin}}$, where $K_\nu = \mathbb{R}$ for all $\nu \in V_\mathbb{R}$, $K_\nu = \mathbb{C}$ for all $\nu \in V_\mathbb{C}$, and K_ν is local with finite residue field for all $\nu \in V_{\mathrm{fin}}$.

If φ is a quadratic form over K and $P \in \mathbb{Z}[X]$, then it follows from the Hasse-Minkowski Theorem that P is an annihilating polynomial of $[\varphi]$, respectively $\{\varphi\}$, if and only if P is an annihilating polynomial of $[\varphi_{K_\nu}]$, respectively $\{\varphi_{K_\nu}\}$, for all $\nu \in V$. This implies

$$\mathrm{Ann}_{[\varphi]} \;=\; \bigcap_{\nu\in V} \mathrm{Ann}_{[\varphi_{K_\nu}]} \qquad \text{and} \qquad \mathrm{Ann}_{\{\varphi\}} \;=\; \bigcap_{\nu\in V} \mathrm{Ann}_{\{\varphi_{K_\nu}\}}\,.$$

Now the signature homomorphisms $W(K) \to \mathbb{Z}$ are in one-to-one correspondence with the absolute values $\nu \in V_\mathbb{R}$. More specifically, for every ring homomorphism $\chi : W(K) \to \mathbb{Z}$ there exists a unique $\nu \in V_\mathbb{R}$ such that χ equals the concatenation $W(K) \to W(K_\nu) \to \mathbb{Z}$, where the first map is induced by the completion $K \hookrightarrow K_\nu$ and the second map is the unique signature homomorphism $W(K_\nu) \to \mathbb{Z}$. We denote the signature homomorphism corresponding to a $\nu \in V_\mathbb{R}$ by sign_ν. From Example 2.4.8.(1) it follows that for a quadratic form φ over K a polynomial $P \in \mathbb{Z}[X]$ is an annihilating polynomial of $[\varphi_{K_\nu}]$, respectively $\{\varphi_{K_\nu}\}$, for all $\nu \in V_\mathbb{R}$ if and only if $P \in (Q_{[\varphi]})$, respectively $P \in (Q_{\{\varphi\}})$. Hence, once we have calculated the embracing polynomial, we can neglect the real completions of K.

Example 2.4.8.(2) shows that $Q_{[\varphi]}$ annihilates $[\varphi_{K_\nu}]$ for all $\nu \in V_\mathbb{C}$. Furthermore it becomes clear by considering Corollary 2.5.1 that $\mathrm{Ann}_{\{\varphi_{K_\mu}\}} \subset \mathrm{Ann}_{\{\varphi_{K_\nu}\}}$ for all $\mu \in V_{\mathrm{fin}}$ and $\nu \in V_\mathbb{C}$, i.e. every polynomial in $\mathbb{Z}[X]$ that annihilates $\{\varphi_{K_\mu}\}$ also annihilates $\{\varphi_{K_\nu}\}$. This observation shows that we do not need to consider the complex completions of K.

2.5.2 Proposition. *Let K be a global field, and let φ be a quadratic form over K. We have*

$$\mathrm{Ann}_{[\varphi]} \;=\; \bigl(Q_{[\varphi]}\bigr) \cap \bigcap_{\nu\in V_{\mathrm{fin}}} \mathrm{Ann}_{[\varphi_{K_\nu}]}$$

and

$$\mathrm{Ann}_{\{\varphi\}} \;=\; \bigl(Q_{\{\varphi\}}\bigr) \cap \bigcap_{\nu\in V_{\mathrm{fin}}} \mathrm{Ann}_{\{\varphi_{K_\nu}\}}\,.$$

By combining the previous proposition and Theorem 2.4.16 we obtain:

2.5.3 Theorem. *Let K be a global field, and let φ be an n-dimensional quadratic form over K.*

(1) If $\varphi \cong n$, then $\mathrm{Ann}_{[\varphi]} = (X-n) \subset \mathbb{Z}[X]$.

(2) If $\varphi \ncong n$, and

(a) if $|S_{[\varphi]}| = 1$, then

$$\mathrm{Ann}_{[\varphi]} = \begin{cases} (2(X-n), (X-n)^2) & \textit{if } \det(\varphi) \textit{ is a sum of two squares in } K, \\ (4(X-n), (X-n)(X-n+2)) & \textit{otherwise.} \end{cases}$$

(b) if $|S_{[\varphi]}| = 2$, then

$$\mathrm{Ann}_{\varphi} = \begin{cases} \big(2(X-s)(X-n), (X-s)(X-n)^2\big) & \textit{if } s \equiv n \ (\textit{mod}\ 4) \textit{ and } \det(\varphi) \textit{ is not a sum of two squares in } K, \\ \big((X-s)(X-n)\big) & \textit{otherwise,} \end{cases}$$

where $S_{\varphi} = \{s, n\}$.

(c) if $|S_{[\varphi]}| \geq 3$, then $\mathrm{Ann}_{[\varphi]} = (Q_{[\varphi]})$.

Proof. The points (1) and (2).(c) are clear.

Let $a \in K^*$. The Hasse-Minkowski Theorem states that $\langle 1, 1, -a\rangle$ is isotropic if and only if $\langle 1, 1, -a\rangle_{K_\nu}$ is isotropic for all $\nu \in V$. In other words a is a sum of two squares in K if and only if a is a sum of two squares in K_ν for all $\nu \in V$. Obviously we do not have to consider any complex closures of K, and for the real closures we know that a is a sum of two squares in K_ν for $\nu \in V_{\mathbb{R}}$ if and only if a is positive with respect to ν. Altogether this means that a is a sum of two squares in K if and only if a is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$ and a is positive with respect to all $\nu \in V_{\mathbb{R}}$.

Let $|S_{[\varphi]}| = 1$. This implies that $\mathrm{sign}_\nu(\varphi) = n$ for all $\nu \in V_{\mathbb{R}}$. In other words the entries of any diagonal representation of φ are all positive with respect to all $\nu \in V_{\mathbb{R}}$. Hence $\det(\varphi)$ is positive with respect to all $\nu \in V_{\mathbb{R}}$, and $\det(\varphi)$ is a sum of two squares in K if and only if $\det(\varphi_\mu)$ is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$. Point (2).(a) now follows directly from Theorem 2.4.16 and the Hasse-Minkowski Theorem.

Now consider the case $|S_{[\varphi]}| = 2$. If either $s \equiv n+2 \pmod 4$ or $s \equiv n \pmod 4$ and $\det(\varphi)$ is a sum of two squares in K then our calculations concerning the Clifford invariant in Example 2.4.15.(2) imply that $Q_{[\varphi]} = (X-s)(X-n)$ annihilates $\left[\varphi_{K_\mu}\right]$ for all $\mu \in V_{\text{fin}}$. Hence it follows from our previous observations that $\mathrm{Ann}_{[\varphi]} = ((X-s)(X-n))$.

Finally we consider the case where $n \equiv s \pmod 4$ and $\det(\varphi)$ is not a sum of two squares in K. The fact that $n \equiv s \pmod 4$ implies that for all $\nu \in V_{\mathbb{R}}$ any diagonal representation of φ has an even number of entries that are negative with respect to ν. Therefore $\det(\varphi)$ is positive with respect to all $\nu \in V_{\mathbb{R}}$, and $\det(\varphi)$ is a sum of two squares in K if and only if $\det(\varphi_{K_\mu})$ is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$. Since $\det(\varphi)$ is not a sum of two squares in K, there exists a $\mu_0 \in V_{\text{fin}}$ such that $\det(\varphi_{K_{\mu_0}})$ is not a sum of two squares in K_{μ_0}. Our calculations concerning the Clifford invariant imply that $Q_{[\varphi]} = (X-s)(X-n)$ does not annihilate $\left[\varphi_{K_{\mu_0}}\right]$. Hence $Q_{[\varphi]}$ does not annihilate $[\varphi]$. Since $2Q_{[\varphi]}$ and $(X-n)Q_{[\varphi]}$

do annihilate $\left[\varphi_{K_\mu}\right]$ for all $\mu \in V_{\text{fin}}$, it is now clear that those two polynomials generate $\mathrm{Ann}_{[\varphi]}$. □

Again an analogous theorem for $\mathrm{Ann}_{\{\varphi\}}$ demands the distinction of even more cases.

2.5.4 Theorem. *Let K be a global field, and let φ be an n-dimensional quadratic form over K.*

(1) If $\varphi \sim r$ for some $r \in \mathbb{Z}$, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (X-r) & \textit{if } s(K)=\infty, \\ (2s(K), X-r) & \textit{otherwise.} \end{cases}$$

(2) If $\varphi \not\sim r$ for all $r \in \mathbb{Z}$,

(a) if $|S_{\{\varphi\}}| = 0$, and

(i) if $s(K)=1$, then

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2, X^2) & \textit{if } n \textit{ is even,} \\ (2, (X+1)^2) & \textit{if } n \textit{ is odd.} \end{cases}$$

(ii) if $s(K)=2$, then for n even

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (4, 2X, X^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (4, X(X+2)) & \textit{otherwise,} \end{cases}$$

and for n odd

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (4, 2(X+1), (X+1)^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (4, (X-1)(X+1)) & \textit{otherwise.} \end{cases}$$

(iii) if $s(K)=4$, then for n even

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (8, 2X, X^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+2), (X+2)^2) & \textit{if } -d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 4X, X(X+2)) & \textit{otherwise,} \end{cases}$$

and for n odd

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (8, 2(X-1), (X-1)^2) & \textit{if } d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 2(X+1), (X+1)^2) & \textit{if } -d(\varphi) \textit{ is a sum of two squares in } K, \\ (8, 4(X+1), (X-1)(X+1)) & \textit{otherwise.} \end{cases}$$

(b) if $|S_{\{\varphi\}}| = 1$, *then*

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2(X-r),(X-r)^2) & \textit{if } (-1)^{\frac{r(r-1)}{2}} d(\varphi) \textit{ is a sum of two squares in } K, \\ (4(X-r),(X-r)(X-r+2)) & \textit{otherwise,} \end{cases}$$

where $S_{\{\varphi\}} = \{r\}$.

(c) if $|S_{\{\varphi\}}| = 2$, *then*

$$\mathrm{Ann}_{\{\varphi\}} = \begin{cases} (2(X-s)(X-r), (X-s)(X-r)^2) & \textit{if } r \equiv s \ (\textit{mod}\ 4) \textit{ and } (-1)^{\frac{r(r-1)}{2}} d(\varphi) \textit{ is not a sum of two squares in } K, \\ ((X-s)(X-r)) & \textit{otherwise,} \end{cases}$$

where $S_{\{\varphi\}} = \{r, s\}$.

(d) if $|S_{\{\varphi\}}| \geq 3$, *then* $\mathrm{Ann}_{\{\varphi\}} = (Q_{\{\varphi\}})$.

Proof. The points (1) and (2).(d) are clear. Point (2).(a) follows from Proposition 2.5.2, Corollary 2.5.1, and the Hasse-Minkowski Theorem since in this case $V_{\mathbb{R}} = \varnothing$. For point (2).(a).(iii) we have to take into account the possibility that neither $d(\varphi)$ nor $-d(\varphi)$ is a sum of 2 squares in K. So consider the case where $s(K) = 4$. First assume that $\dim(\varphi)$ is even. If $d(\varphi)$ is a sum of two squares in K, then $d(\varphi_{K_\mu})$ is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$. By Corollary 2.5.1 the polynomials $2X$ and X^2 annihilate $\{\varphi_{K_\mu}\}$ for all $\mu \in V_{\text{fin}}$. Hence by our observations $2X$ and X^2 annihilate $\{\varphi\}$.

If $-d(\varphi)$ is a sum of two squares, then $-d(\varphi_{K_\mu})$ is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$. Assume there exists a $\mu_0 \in V_{\text{fin}}$ such that $s(K_{\mu_0}) < 4$. Then we have seen that $d(\varphi)$ is also a sum of two squares over K_{μ_0}. Since $2(X+2) = 2X+4$ and $(X+2)^2 = X^2+4X+4$, and since $4 = 0$ in $W(K_{\mu_0})$, it follows that $2(X+2)$ and $(X+2)^2$ annihilate $\{\varphi_{K_{\mu_0}}\}$. Therefore by Corollary 2.5.1 the polynomials $2(X+2)$ and $(X+2)^2$ annihilate $\{\varphi_{K_\mu}\}$ for all $\mu \in V_{\text{fin}}$. Thus by Proposition 2.5.2 they also annihilate $\{\varphi\}$.

Suppose that neither $d(\varphi)$ nor $-d(\varphi)$ is a sum of two squares in K. Then there exists some $\mu_0 \in V_{\text{fin}}$ such that $d(\varphi_{K_{\mu_0}})$ is not a sum of two squares in K_{μ_0}. If $s(K_{\mu_0}) < 4$, then the polynomials $2X, 2(X+2), X^2, (X+2)^2$ do not annihilate $\{\varphi_{K_{\mu_0}}\}$. Hence they do not annihilate $\{\varphi\}$, neither. Assume that $s(K_{\mu_0}) = 4$, then by our observations $-d(\varphi_{K_{\mu_0}})$ is a sum of two squares in K_{μ_0}. But $-d(\varphi)$ is not a sum of two squares in K, hence there exists a $\mu_1 \in V_{\text{fin}}$ such that $-d(\varphi_{K_{\mu_1}})$ is not a sum of two squares in K_{μ_1}. If $s(K_{\mu_1}) < 4$, then none of the polynomials $2X, 2(X+2), X^2, (X+2)^2$ annihilate $\{\varphi_{K_{\mu_1}}\}$. Accordingly they do not annihilate $\{\varphi\}$, neither. If $s(K_{\mu_1}) = 4$, then $d(\varphi_{K_{\mu_1}})$ is a sum of two squares in K_{μ_1}, and by Corollary 2.5.1 the polynomials $2X$ and X^2 annihilate $\{\varphi_{K_{\mu_1}}\}$, but they do not annihilate $\{\varphi_{K_{\mu_0}}\}$ by Example 2.4.15.(2). Similarly $2(X+2)$ and $(X+2)^2$ annihilate $\{\varphi_{K_{\mu_0}}\}$, but they do not annihilate $\{\varphi_{K_{\mu_1}}\}$. Therefore none of the polynomials $2X, 2(X+2), X^2, (X+2)^2$ annihilate $\{\varphi\}$. The claim now follows, since $4X$ and $X(X+2)$ annihilate $\{\varphi_{K_\mu}\}$ for all $\mu \in V_{\text{fin}}$. In the case where n is odd we apply an analogous reasoning.

Now assume that $S_{\{\varphi\}} = \{r\}$. There exist $a, b \in \mathbb{N}_0$ such that $n = a + b$ and $r = a - b$. The determinant $\det(\varphi)$ is negative with respect to all $\nu \in V_\mathbb{R}$ if and only if b is odd. If b is even, then $\det(\varphi)$ is positive with respect to all $\nu \in V_\mathbb{R}$. Simple calculations show that

$$(-1)^{\frac{r(r-1)}{2}} d(\varphi) \; = \; (-1)^{a^2-a+b^2} \det(\varphi) \; = \; (-1)^b \det(\varphi).$$

This implies that $(-1)^{\frac{r(r-1)}{2}} d(\varphi)$ is positive with respect to all $\nu \in V_\mathbb{R}$. Hence $(-1)^{\frac{r(r-1)}{2}} d(\varphi)$ is a sum of two squares in K if and only if it is a sum of two squares in K_μ for all $\mu \in V_{\text{fin}}$. Point (2).(b) now follows from Example 2.4.15.(2) and the Hasse-Minkowski Theorem.

Next consider the case $S_{\{\varphi\}} = \{s, r\}$ with $s \neq r$. If $s \equiv r + 2 \pmod 4$, then it follows from our calculations that $(X - s)(X - r)$ annihilates $\left\{\varphi_{K_\mu}\right\}$ for all $\mu \in V_{\text{fin}}$. Since $(X - s)(X - r) = Q_{\{\varphi\}}$ we have $\operatorname{Ann}_{\{\varphi\}} = ((X - s)(X - r))$. If $r \equiv s \pmod 4$ and $(-1)^{\frac{r(r-1)}{2}} d(\varphi)$ is a sum of two squares in K then the same holds over K_μ for all $\mu \in V_{\text{fin}}$. Thus it follows from Example 2.4.15.(2) that $(X - s)(X - r)$ annihilates $\{\varphi\}$. Hence we have again $\operatorname{Ann}_{\{\varphi\}} = ((X - s)(X - r))$.

Finally consider the case where $s \equiv r \pmod 4$ and $(-1)^{\frac{r(r-1)}{2}} d(\varphi)$ is not a sum of two squares in K. By our observations earlier in this proof we know that $(-1)^{\frac{r(r-1)}{2}} d(\varphi)$ is positive for all $\nu \in V_\mathbb{R}$ with $\operatorname{sign}_\nu(\{\varphi\}) = r$. Since $s \equiv r \pmod 4$ the same holds for all $\nu \in V_\mathbb{R}$ with $\operatorname{sign}_\nu(\{\varphi\}) = s$. Thus there must exist a $\mu_0 \in V_{\text{fin}}$ such that $(-1)^{\frac{r(r-1)}{2}} d(\varphi_{K_{\mu_0}})$ is not a sum of two squares in K_{μ_0}. By our calculations and the Hasse-Minkowski Theorem $Q_{\{\varphi\}} = (X - s)(X - r)$ does not annihilate $\left\{\varphi_{K_{\mu_0}}\right\}$. This implies that we must have $\operatorname{Ann}_{\{\varphi\}} = (2Q_{\{\varphi\}}, (X - r)Q_{\{\varphi\}})$, which completes the proof of point (2).(c). □

2.5.5 Remark. Let K be a global field, and let V be the set of equivalence classes of absolute values of K. Consider a quadratic form φ over K. Assume that $e_0(\{\varphi\}) = 0$, $e_1(\{\varphi\}) = 1$, $e_2(\{\varphi\}) = 1$, and $\operatorname{sign}_\nu(\{\varphi\}) = 0$ for all $\nu \in V_\mathbb{R}$. For $\nu \in V_\mathbb{C}$ we have $\varphi_{K_\nu} \sim 0$ since $\dim(\varphi)$ is even. If $\nu \in V_\mathbb{R}$, then $\operatorname{sign}_\nu(\{\varphi\}) = 0$ implies that $\varphi_{K_\nu} \sim 0$. Finally, since $\dim(\varphi_{K_\nu})$ is even, $d(\varphi_{K_\nu}) = 1$, and $c(\varphi_{K_\nu}) = 1$ for $\nu \in V_{\text{fin}}$, it follows that also $\varphi_{K_\nu} \sim 0$. By the Hasse-Minkowski Theorem $\varphi \sim 0$. It follows that $\varphi \sim 0$ if and only if the first three cohomological invariants and all the signatures of $\{\varphi\}$ are trivial. We conclude that over K quadratic forms can be classified with the help of the dimension, the discriminant, the Clifford invariant, and the signatures. This observation constitutes another means to prove Theorems 2.5.3 and 2.5.4. △

2.5.6 Remark. Let K be a formally real global field. Then $8 \neq 0$ in $W(K)$ and hence $I^3(K) \neq \{0\}$. Consider a quadratic form φ with $\varphi \not\sim 0$ and $\{\varphi\} \in I^3(K)$. Then $\varphi_{K_\nu} \sim 0$ for all $\nu \in V_\mathbb{C} \cup V_{\text{fin}}$. Hence by the Hasse-Minkowski Theorem there exists a $\mu \in V_\mathbb{R}$ such that $\varphi_{K_\mu} \not\sim 0$. Since $W(\mathbb{R})$ is torsion free it follows that $m\left\{\varphi_{K_\mu}\right\} \neq 0$ for all $m \in \mathbb{Z} \setminus \{0\}$. This implies that $\{\varphi\}$ is not torsion. Hence we see that $I^3(K)$ is torsion free. In this setting we can use our observations about annihilating polynomials and our calculations concerning the Clifford invariant to prove a result by D. Lewis from his article [Lew92].

For $n \in \mathbb{N}_0$ consider the polynomial $Q_n \in \mathbb{Z}[X]$ with

$$Q_n \; = \; \begin{cases} X(X-2)\cdots(X-n) & \text{for } n \text{ even,} \\ (X-1)(X-3)\cdots(X-n) & \text{for } n \text{ odd.} \end{cases}$$

Since Q_n is the product of all those factors of $P_n = (X-n)(X-n+2)\cdots(X+n) \in \mathbb{Z}[X]$ that have a non-negative root, we call Q_n the *positive part* of the Lewis polynomial P_n. A quadratic form φ over an arbitrary formally real field K is called *positive*, if $\chi(\{\varphi\}) \geq 0$ for all signature homomorphisms $\chi \in \mathrm{Hom}(W(K), \mathbb{Z})$. In this case the signature polynomial $P_{[\varphi]}$ divides Q_n with $n = \dim(\varphi)$. If K is formally real and Pythagorean, then it follows from Corollary 2.4.5 that Q_n annihilates $[\varphi]$.

Now let K be an arbitrary formally real field such that $I^3(K)$ is torsion free, and let φ be a positive quadratic form over K with $n = \dim(\varphi) > 1$. Since $P_{[\varphi]}$ divides Q_n, it follows that $Q_n([\varphi])$ is torsion. If $n = 2$, then $Q_n = X(X-2)$, and if $n = 3$, then $Q_n = (X-1)(X-3)$. In both cases Example 2.4.15.(2) implies that the image of $Q_n([\varphi])$ via the canonical projection $\pi : \widehat{W}(K) \to W(K)$ lies in $I^3(K)$. Since $I^3(K)$ is torsion free, we must have $Q_n([\varphi]) = 0$. If $n > 3$, then $\pi(Q_n([\varphi]))$ clearly lies in $I^3(K)$, and Q_n must be an annihilating polynomial for $[\varphi]$. Thus we have shown that for $n > 1$ the polynomial Q_n annihilates the isometry and equivalence classes of all n-dimensional positive quadratic forms over K. Lewis proved this result with the help of direct calculations concerning certain factors of the polynomial Q_n (see [Lew92, Theorem 1]). △

2.6 Generic splitting

In this section we give a short introduction to the theory of generic splitting of quadratic forms. This theory was developed by M. Knebusch in his three articles [Kne73], [Kne76], and [Kne77], and it has since proven to be an exceedingly useful tool for the study of quadratic forms. The aim of this section is to give a short introduction to the elementary theory of generic splitting, and to quote some of the more important results. Most of the proofs will be left out.

2.6.1 Definition. *A quadratic form φ over K* splits *if* $\dim(\varphi_{\mathrm{an}}) \leq 1$.

Consider a field K, and a quadratic form (V, φ) over K. Let L be a field extension of K. In Section 2.1 we have already defined the quadratic form $\varphi_L : V \otimes_K L \to L$, $v \otimes \lambda \mapsto \varphi(v)\lambda^2$. If $\varphi \cong \psi \perp \chi$, then we clearly have $\varphi_L \cong \psi_L \perp \chi_L$. Since furthermore $\mathbb{H}_L$ is hyperbolic, the inclusion $\lambda : K \hookrightarrow L$ induces a ring homomorphism

$$\lambda_* : \quad W(K) \longrightarrow W(L), \quad \{\varphi\} \longmapsto \{\varphi_L\}.$$

In particular we see that $i(\varphi_L) \geq i(\varphi)$.

In general the homomorphism $\lambda_* : W(K) \to W(L)$ is neither injective nor surjective. For example, if L is an algebraic closure of K, then we have seen that φ_L splits. Hence if $W(K) \ncong \mathbb{Z}/2\mathbb{Z}$, then λ_* is surjective but not injective. If on the other hand L is a purely transcendental extension of K, then we can apply the following result.

2.6.2 Proposition. *Let φ be a quadratic form over K, and let $L = K(X)$ be the function field in one variable X over K. If φ_L is isotropic, then φ is isotropic.*

[Pfi95, Lemma 2.1, Chapter 1]

Let L be a purely transcendental extension of K, and let φ be an anisotropic quadratic form over K. Then it follows from the previous proposition that φ_L is anisotropic as well. We deduce that $\lambda_* : W(K) \to W(L)$ is injective. If $X \in L$ is transcendental over K with $X \notin (L^*)^2$, then $\{\langle X \rangle\} \notin \operatorname{im}(\lambda_*)$, which shows that λ_* is not surjective.

Consider an arbitrary field extension L of K and a quadratic form φ over K. We have seen that $i(\varphi_L) \geq i(\varphi)$, and in general it is not possible to strengthen this statement. Therefore it is necessary to study the behaviour of φ_L as a function of φ and L.

Assume that φ is an anisotropic quadratic form over K of dimension $n \in \mathbb{N}_0$. The following questions naturally arise:

(1) For which field extensions L of K is φ_L isotropic?

(2) For which field extensions L of K does φ_L split?

(3) For which $k \in \mathbb{N}_0$ with $k \leq \frac{n}{2}$ does there exist a field extension L of K such that $i(\varphi_L) = k$?

The theory of generic splitting does, at least to some extent, provide answers to all of these three questions.

Consider a field K. We form a new set by adding the formal symbol ∞ to the elements of K, and we write $K^\infty := K \cup \{\infty\}$. Now we can extend the addition and the multiplication in K to K^∞ by setting

$$\begin{aligned} \infty + x \;:=\; x + \infty \;:=\; \infty \qquad & \forall\, x \in K, \\ \infty \cdot x \;:=\; x \cdot \infty \;:=\; \infty \qquad & \forall\, x \in K^\infty \setminus \{0\}. \end{aligned}$$

We note that the addition and multiplication are not defined on arbitrary pairs of elements of K^∞. More specifically, the following operations are not defined $\infty + \infty$ and $\infty \cdot 0$, respectively $0 \cdot \infty$. But it is possible to define the following "inverses"

$$-\infty \;:=\; \infty, \qquad 0^{-1} \;:=\; \infty, \qquad \infty^{-1} \;:=\; 0.$$

Note that $-\infty$ is not in fact an actual additive inverse of ∞, since the operation $\infty + (-\infty) = \infty + \infty$ is not permitted. Analogously ∞ is not an actual multiplicative inverse of 0, and 0 is not an actual multiplicative inverse of ∞.

2.6.3 Definition. *Let M and N be two sets, and let M, respectively N, be equipped with a composition $\circ_M$, respectively $\circ_N$, which does not have to be defined on arbitrary pairs of elements of M, respectively N. A map $\lambda : M \to N$ is called a* morphism, *if for all $x, y \in M$ such that $\lambda(x) \circ_N \lambda(y)$ is defined, also $x \circ_M y$ is defined and $\lambda(x \circ_M y) = \lambda(x) \circ_N \lambda(y)$.*

2.6.4 Definition. *Let L and M be two fields.*

(1) A map $\lambda : L^\infty \to M^\infty$ with $\lambda(1) = 1$ is a place, *if λ is a morphism with respect to addition and multiplication.*

(2) If L and M are field extensions of a field K, then a place $\lambda : L^\infty \to M^\infty$ is called a K-place, *if $\lambda|_K = \mathrm{id}_K$.*

Consider a place $\lambda : L^\infty \to M^\infty$. Since $\infty + \infty$ is not defined, the same must hold for $\lambda(\infty) + \lambda(\infty)$. It follows that $\lambda(\infty) = \infty$. Analogously, since $0 \cdot \infty$ is not defined, $\lambda(0) \cdot \lambda(\infty)$ is not defined as well, whence we deduce that $\lambda(0) = 0$.

2.6.5 Examples.

(1) Every field homomorphism $\lambda : L \to M$ can be extended to a place $\lambda : L^\infty \to M^\infty$ by setting $\lambda(\infty) := \infty$.

(2) Let L be a purely transcendental extension of K with finite transcendence degree $n \in \mathbb{N}$, and let $\{X_1, \ldots, X_n\}$ be a transcendence basis of L over K. For any choice of elements $y_1, \ldots, y_n \in K$ there exists a place $\lambda : L^\infty \to K^\infty$ such that $\lambda(X_i) = y_i$ for $i = 1, \ldots, n$ (see [Bou89b, Examples of places (3), Chapter VI, §2]). △

If $\lambda : L^\infty \to M^\infty$ is a place, then it would be convenient if λ would induce a ring homomorphism $\lambda_* : W(L) \to W(M)$, as in the case where M is a field extension of L and $\lambda : L \hookrightarrow M$ is the inclusion. But in general this is not possible. However it is possible to develop a for our needs sufficient replacement.

2.6.6 Definition. *Let $\lambda : L^\infty \to M^\infty$ be a place, and let (V, φ) be a quadratic form over L. We say that φ has* good reduction *with respect to λ, if there exists a basis $\mathcal{B}$ of V such that for the matrix $A_{\varphi,\mathcal{B}} = (a_{ij})_{i,j=1,\ldots,n}$ associated to φ with respect to $\mathcal{B}$ the following conditions are satisfied:*

(i) $\lambda(a_{ij}) \neq \infty$ *for all* $i, j = 1, \ldots, n$,

(ii) $\det\big((\lambda(a_{ij}))_{i,j=1,\ldots,n}\big) \neq 0$.

In this case we denote the quadratic form associated to $\big((\lambda(a_{ij}))_{i,j=1,\ldots,n}\big)$ by $\lambda_*(\varphi)$ and call it the specialisation *of φ with respect to λ.*

If φ has good reduction with respect to λ, then it follows from [Kne73, Lemma 2.1] that $\lambda_*(\varphi)$ is independent from the choice of the basis $\mathcal{B}$. In particular, if $\psi \cong \varphi$, then ψ has good reduction as well and $\lambda_*(\varphi) \cong \lambda_*(\psi)$.

2.6.7 Example. We see immediately that the hyperbolic form $\mathbb{H}$ over a field L has good reduction with respect to any place $\lambda : L^\infty \to M^\infty$. △

Specialisation also respects orthogonal sums. More specifically, if φ has good reduction with respect to a place $\lambda : L^\infty \to M^\infty$, and if $\varphi \cong \psi \perp \chi$ such that ψ has good reduction with respect to λ, then by [Kne76, Theorem 2.1] the form χ has good reduction with respect to λ as well, and

$$\lambda_*(\varphi) \;\cong\; \lambda_*(\psi) \perp \lambda_*(\chi). \tag{2.9}$$

Together with the previous example this implies that, if φ and ψ are equivalent forms over L such that φ has good reduction with respect to λ, then ψ has good reduction with respect to λ and $\lambda_*(\varphi) \sim \lambda_*(\psi)$. In other words specialisation is invariant under equivalence of quadratic forms.

Now let L and M be field extensions of K, and let $\lambda : L^\infty \to M^\infty$ be a K-place. Consider a quadratic form φ over K. Then clearly φ_L has good reduction with respect to λ. By Example 2.6.7 and our previous observations it follows that also $(\varphi_L)_{\text{an}}$ has good reduction with respect to λ. Since $\lambda_*(\varphi_L) \cong \varphi_M$ and $\lambda_*(\mathbb{H}_L) \cong \lambda_*(\mathbb{H}_M)$, it follows from the isometry (2.9) that

$$\lambda_*((\varphi_L)_{\text{an}}) \sim (\varphi_M)_{\text{an}} \qquad \text{and} \qquad i(\varphi_L) \leq i(\varphi_M).$$

In particular $\lambda_*((\varphi_L)_{\text{an}})$ is independent from the choice of λ.

2.6.8 Definition. *Let φ be a quadratic form over K. A field extension L of K is called a* generic zero field *of φ if φ_L is isotropic, and if for every field extension M of K such that φ_M is isotropic there exists a place $L^\infty \to M^\infty$.*

We now study an especially important class of generic zero fields. Let (K^n, φ) be an n-dimensional quadratic form over K with $n \geq 1$. Consider the polynomial $\varphi((X_1, \ldots, X_n)^t)$ in the polynomial ring $K[X_1, \ldots, X_n]$ in n variables. Suppose that $n \geq 2$ and $\varphi \ncong \mathbb{H}$. Then $\varphi((X_1, \ldots, X_n)^t)$ is irreducible (see [Lam05, Lemma 3.1, Chapter X]). Hence we can define the quotient field

$$K(\varphi) := \operatorname{Quot}\Big(K[X_1, \ldots, X_n]/\varphi\big((X_1, \ldots, X_n)^t\big)\Big).$$

If $\dim(\varphi) \leq 1$ or if $\varphi \cong \mathbb{H}$, then we set $K(\varphi) := K$. Let (K^n, ψ) be another n-dimensional quadratic form over K. We see immediately that $\varphi \cong \psi$ implies the existence of a K-isomorphism of fields $K(\varphi) \cong K(\psi)$. Hence we can define $K(\chi)$ for an arbitrary quadratic form (V, χ) over K.

2.6.9 Definition. *Let φ be a quadratic form over K. The field extension $K(\varphi)$ of K is called the* function field *of φ.*

2.6.10 Proposition. *For a quadratic form φ over K, the function field $K(\varphi)$ is a generic zero field of φ.*
[Kne76, Theorem 3.3]

Let φ an n-dimensional quadratic form over K with $n \geq 2$ and $\varphi \ncong \mathbb{H}$. Without loss of generality we can assume that $\varphi = \langle a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in K^*$. Then $a_1 X_1^2 + \cdots + a_n X_n^2 = 0$ in $K(\varphi)$. We obtain

$$X_1 = \sqrt{-\frac{1}{a_1}\left(a_2 X_2^2 + \cdots + a_n X_n^2\right)} \in K(\varphi),$$

which shows that $X_1, \ldots, X_n$ are algebraically dependent over K. More specifically we can formulate the following proposition.

2.6.11 Proposition. *Let φ be an n-dimensional quadratic form over K with $n \geq 2$ and $\varphi \ncong \mathbb{H}$. Then the function field $K(\varphi)$ is a quadratic extension of a purely transcendental extension of degree $n-1$ over K.*

If φ is isotropic, then by the Propositions 2.1.16 and 2.1.18 we can assume that

$$\varphi\big((X_1,\dots,X_n)^t\big) \;=\; X_1X_2 + a_3X_3^2 + \cdots + a_nX_n^2.$$

Hence

$$X_1 \;=\; -\frac{1}{X_2}\left(a_3X_3^2 + \cdots + a_nX_n^2\right),$$

which shows that $K(\varphi)$ is purely transcendental over K.

2.6.12 Proposition. *For an n-dimensional quadratic form φ over K, $n \geq 2$ and $\varphi \ncong \mathbb{H}$, the function field $K(\varphi)$ is a purely transcendental extensions of K if and only if φ is isotropic.*

Proof. We have already seen that $K(\varphi)$ is purely transcendental over K if φ is isotropic. Now assume that $K(\varphi)$ is a purely transcendental extensions of K. Since $\varphi_{K(\varphi)}$ is isotropic it follows from Proposition 2.6.2 that φ is isotropic. □

2.6.13 Definition. *Let L and M be two field extensions of K. We say that L and M are* K-equivalent*, if there exist K-places $L^\infty \to M^\infty$ and $M^\infty \to L^\infty$.*

Let φ be a quadratic form over K. By definition of a generic zero field all generic zero fields of φ are K-equivalent. Hence, by our observations about good reduction, we can from now on restrict ourselves to considering function fields of quadratic forms.

Assume that φ and ψ are anisotropic quadratic form over K. Again a number of questions naturally arise, such as

(4) For which φ does $\varphi_{K(\varphi)}$ split?

(5) For which ψ does $\varphi_{K(\psi)}$ become isotropic or even split?

The following two important propositions give partial answers to question (5).

2.6.14 Definition. *Let φ be a quadratic form over K. A quadratic form ψ over K is called a* subform *of φ, if there exists some quadratic form χ over K such that $\varphi \cong \psi \perp \chi$.*

2.6.15 Proposition. *Let ψ be an n-dimensional quadratic form over K with $n \geq 2$ and $\psi \ncong \mathbb{H}$. If φ is a quadratic form over K such that $\varphi \not\sim 0$ and $\varphi_{K(\psi)} \sim 0$, then ψ is similar to a subform of φ. More specifically we have that $ab\psi$ is a subform of φ for all $a \in D_K^*(\varphi)$ and $b \in D_K^*(\psi)$.*
[Kne76, Lemma 4.5]

2.6.16 Proposition. *Let τ be a k-fold Pfister form over K with $k \geq 1$, and let φ be an anisotropic quadratic form over K. Then $\varphi_{K(\tau)} \sim 0$ if and only if there exists a quadratic form ψ over K such that $\varphi \cong \tau \otimes \psi$.*
[Kne76, Lemma 4.4]

Let τ be a k-fold Pfister form over K with $k \geq 1$. If τ is isotropic then τ is hyperbolic by Proposition 2.1.33. Hence $\tau_{K(\tau)}$ is hyperbolic.

2.6.17 Definition. *Let τ be a Pfister form over K. Then $\tau \cong \langle 1\rangle \perp \tau'$ with some subform τ' of τ. We call τ' the* pure part *of τ.*

Let τ' be the pure part of a Pfister form τ over K, then $\tau_{K(\tau')} \sim 0$ since τ' is a subform of τ. Hence $\tau'_{K(\tau')} \sim \langle -1 \rangle$, which means that τ' splits over $K(\tau')$. In fact quadratic forms that are similar to a Pfister form or the pure part of a Pfister form are the only quadratic forms that split over their own function field, which completely answers question (4).

2.6.18 Theorem. *Let φ be an anisotropic quadratic form over K with $\dim(\varphi) > 0$. Then $\varphi_{K(\varphi)}$ splits if and only if φ is similar to a k-fold Pfister form or the pure part of a k-fold Pfister form over K for some $k \geq 1$.*
[Kne76, Theorem 5.8]

We now introduce another exceedingly useful class of quadratic forms by generalising the definition of the pure part of a Pfister form.

2.6.19 Definition. *Let τ be a k-fold Pfister form over K, $k \in \mathbb{N}_0$. A quadratic form φ over K is called a* Pfister neighbour *of τ if φ is similar to a subform of τ with $\dim(\varphi) > \frac{1}{2}\dim(\tau)$. In this case there exists an $a \in K^*$ and a quadratic form ψ over K such that $a\tau \cong \varphi \perp \psi$. The form ψ is called the* complement *of φ.*

Let τ be a k-fold Pfister form over K, $k \in \mathbb{N}$, and let φ be a Pfister neighbour of τ. Then there exists an $a \in K^*$ and a quadratic form ψ over K such that $a\tau \cong \varphi \perp \psi$. Hence $\varphi_{K(\tau)} \sim -\psi_{K(\tau)}$. Since $\dim(\psi) < 2^{k-1} < \dim(\varphi)$, it follows that $\varphi_{K(\tau)}$ is isotropic. Furthermore, since φ is similar to a subform of τ, we obtain $\tau_{K(\varphi)} \sim 0$. Therefore $K(\varphi)$ and $K(\tau)$ are K-equivalent, which provides us with another partial answer to question (5).

2.6.20 Proposition. *If φ is a Pfister neighbour of a Pfister form τ over K, then $K(\varphi)$ and $K(\tau)$ are K-equivalent.*

We continue by again considering an arbitrary quadratic form φ over K. Set

$$K_0 := K \qquad \text{and} \qquad \varphi_0 := \varphi_{\mathrm{an}}. \tag{2.10}$$

If φ_0 splits, we set $h = 0$ and stop here. Otherwise we construct a tower of fields $K_0 \subset K_1 \subset \cdots \subset K_h$ and anisotropic quadratic forms φ_k over K_k, such that $\dim(\varphi_k) < \dim(\varphi_{k-1})$ for $k = 1, \ldots, h$, and such that φ_h splits. Assume that for $k \in \mathbb{N}$ the field K_{k-1} and the form φ_{k-1} have already been determined, and that φ_{k-1} is not split. Then let K_k be any generic zero field of φ_{k-1} over K_{k-1} In particular we could choose $K_k = K_{k-1}(\varphi_{k-1})$. Set

$$\varphi_k := \left((\varphi_{k-1})_{K_k}\right)_{\mathrm{an}}. \tag{2.11}$$

If φ_k splits we set $h = k$ and the construction is complete. Otherwise we proceed by defining K_{k+1} and φ_{k+1}. This process must stop after a finite number of steps since $\dim(\varphi_k) < \dim(\varphi_{k-1})$.

2.6.21 Definition. *Let φ be a quadratic form over K.*

(1) A tower of fields $K = K_0 \subset K_1 \subset \cdots \subset K_h$ as constructed above is called a generic splitting tower *of φ.*

(2) For $k = 0, \dots, h$, the quadratic form φ_k over K_k as defined in (2.10) *and* (2.11) *is the* k-th anisotropic kernel *of φ.*

(3) The natural number $i_k(\varphi) := i((\varphi_{k-1})_{K_k})$, $k = 1, \dots, h$, is the k-th Witt index *of φ. The 0-th Witt index $i_0(\varphi)$ is just $i(\varphi)$.*

(4) We call h the height *of φ, and we write $h(\varphi) := h$.*

Theorem 2.6.18 allows us to classify those anisotropic quadratic forms with height 1.

2.6.22 Corollary. *A quadratic form φ over K has height 1 if and only if φ is similar to a k-fold Pfister form with $k \geq 1$ or the pure part of a k-fold Pfister form with $k \geq 2$.*

The following theorem will justify the above definition. More specifically we will see, that the definition of the higher anisotropic kernels does not depend on the choice of the generic splitting tower. In addition the theorem will provide us with a complete answer to question (3).

2.6.23 Theorem. *Let φ be a quadratic form over K, let $K = K_0 \subset \cdots \subset K_{h(\varphi)}$ be a generic splitting tower of φ, and let L be an arbitrary field extension of K. Then there exists a $k \in \{0, \dots, h(\varphi)\}$ and a K-place $\lambda : K_k^\infty \to L^\infty$ such that φ_k has good reduction with respect to λ and $(\varphi_L)_{\mathrm{an}} \cong \lambda_*(\varphi_k)$. In particular $i(\varphi_L) = i_0(\varphi) + \cdots + i_k(\varphi)$.*

[Kne76, Theorem 5.1]

2.6.24 Definition. *Let L be a field extension of K, and let ψ be a quadratic form over L. We say that ψ is* defined over *K if there exists a quadratic form φ over K such that $\psi \cong \varphi_L$.*

We note that, for an anisotropic Pfister neighbour φ with complement ψ over K, the first anisotropic kernel of φ is defined over the ground field K. More specifically, if K_1 is a generic zero field of φ, and if the form φ_1 over K_1 is the first anisotropic kernel of φ, then $\varphi_1 \cong -\psi_{K_1}$. For an arbitrary quadratic form φ this statement does not hold. In fact this property can be used to characterise anisotropic Pfister neighbours.

2.6.25 Proposition. *Let φ be an anisotropic quadratic form over K with $\dim(\varphi) > 1$, let K_1 be a generic zero field of K, and let φ_1 be the first anisotropic kernel of φ over K_1. Then φ_1 is defined over K if and only if φ is a Pfister neighbour. In particular if φ is a Pfister neighbour with complement ψ, then $\varphi_1 \cong -\psi_{K_1}$.*

[Kne77, Theorem 7.13]

Next we define excellent quadratic forms, which are a special class of Pfister neighbours. For an excellent form φ over K the previous proposition can be strengthened to include all higher anisotropic kernels of φ.

2.6.26 Definition. *Let φ be a quadratic form over K. If $\dim(\varphi) = 0, 1$, then φ is* excellent. *If $\dim(\varphi) \geq 2$, then φ is* excellent *if φ is a Pfister neighbour such that the complement ψ of φ is excellent.*

If φ is an excellent quadratic form over K, then there exists a sequence of quadratic forms

$$\psi_0 = \varphi,\ \psi_1,\ \dots,\ \psi_r \tag{2.12}$$

over K such that ψ_{i-1} is a Pfister neighbour with complement ψ_i for $i = 1, \dots, r$, and such that ψ_r splits.

2.6.27 Definition. *If φ is an excellent form over K, then the quadratic form ψ_k over K as defined in* (2.12) *is called the k-*th complement *of φ.*

The following theorem can be deduced by induction from Proposition 2.6.25.

2.6.28 Theorem. *Let φ be an anisotropic quadratic form over K, let $K_0 = K \subset K_1 \subset \cdots \subset K_{h(\varphi)}$ be a generic splitting tower of φ, and for $k = 0, \dots, h(\varphi)$ let φ_k be the k-th anisotropic kernel of φ over K_k. The form φ is excellent if and only if φ_k is defined over K for all $k \in \{0, \dots, h(\varphi)\}$. In particular, if φ is excellent with higher complements $\psi_0 = \varphi, \psi_1, \dots, \psi_r$ as in* (2.12)*, then $r = h(\varphi)$ and $\varphi_k \cong (-1)^k (\psi_k)_{K_k}$.*
[Kne77, Theorem 7.14 & Remark 7.15]

Since the dimension of the complement of an anisotropic Pfister neighbour φ over K is uniquely determined by the dimension of φ, it follows that, if φ is excellent, the dimensions of the higher complements of φ and thus the dimensions of the higher anisotropic kernels of φ are uniquely determined by $\dim(\varphi)$. More specifically, the height, the dimensions of the higher anisotropic kernels, and the higher Witt indices of φ can be directly calculated from $\dim(\varphi)$ with the help of recursive functions (see [Kne77, Corollary 7.11]).

2.7 Annihilating polynomials for excellent forms

In the previous section we have defined excellent forms recursively with the help of Pfister neighbours. We can now make use of this recursive definition to construct annihilating polynomials for excellent forms. More specifically, in Proposition 2.7.1 we study annihilating polynomials of Pfister neighbours. Then we apply this proposition inductively to obtain, for $n \in \mathbb{N}_0$, a polynomial E_n which annihilates the isometry and equivalence classes of any n-dimensional excellent form φ over an arbitrary field K. The characterisations of Pfister neighbours and excellent forms with the help of the theory of generic splitting, makes it possible to use methods from that theory to study annihilating polynomials. In the general setting, when the higher anisotropic kernels are not defined over the ground field, this becomes substantially more difficult.

First we choose an approach which makes use of the results presented in the previous section. It is however also possible to employ a more elementary approach. To be more precise, it is possible to characterise excellent forms over K with the help of certain preimages in the group ring $Z[\mathcal{G}(K)]$. If $x \in \mathbb{Z}[\mathcal{G}(K)]$ is such a preimage, and if φ is its excellent image with $n = \dim(\varphi)$, then P_x divides E_n. In particular E_n is an annihilating polynomial for x.

Let K be a field. Consider the canonical projection $\pi : \widehat{W}(K) \to W(K)$. Let $x, y \in \widehat{W}(K)$. In what follows we allow the notation

$$x \sim y \quad :\Longleftrightarrow \quad \pi(x) = \pi(y).$$

Assume that $P \in \mathbb{Z}[X]$ is an annihilating polynomial for x and that $y \sim x$. Since π is a ring homomorphism it follows that $P(y) \sim 0$.

2.7.1 Proposition. *Let φ be a Pfister neighbour of dimension $n > 1$ with complement $-\psi$ over K, and let $a \in K^*$ and τ be a Pfister form such that $\varphi \perp -\psi \cong a\tau$. If $Q \in \mathbb{Z}[X]$ is an annihilating polynomial for $[\psi]$, then $P := Q \cdot (X^2 - n^2)$ is an annihilating polynomial for $[\varphi]$. In the case where $a \in (K^*)^2$ (in particular if φ is isotropic) the polynomial $\widetilde{P} := Q \cdot (X - n)$ suffices.*

Proof. If φ is isotropic, then τ is isotropic as well and therefore hyperbolic. Hence $\varphi \sim \psi$. By our observation above $Q([\varphi]) \sim 0$, and therefore

$$Q([\varphi]) \cdot [\varphi] \;\sim\; 0 \;\sim\; Q([\varphi]) \cdot n.$$

The claim follows since $\dim(Q([\varphi]) \cdot [\varphi]) = \dim(Q([\varphi]) \cdot n)$.

Now let φ be anisotropic. Since $\varphi_{K(\varphi)} \sim \psi_{K(\varphi)}$, we obtain $Q([\varphi_{K(\varphi)}]) \sim 0$. Proposition 2.6.20 states that $Q([\varphi_{K(\tau)}]) \sim 0$. Hence by Proposition 2.6.16 there exists an element $x \in \widehat{W}(K)$ such that $Q([\varphi]) \sim x \cdot [\tau]$. Now $a\varphi \subset \tau$. Since $b\tau \cong \tau$ for all $b \in K^*$ represented by τ, it follows that $a\varphi \otimes \tau \cong n \times \tau$. If $a \in (K^*)^2$, then

$$Q([\varphi]) \cdot ([\varphi] - n) \;\sim\; x \cdot [\tau] \cdot ([\varphi] - n) \;=\; x \cdot ([\varphi \otimes \tau] - [n \times \tau]) \;=\; x \cdot 0 \;=\; 0,$$

and the claim follows since

$$\dim\big(Q([\varphi]) \cdot ([\varphi] - n)\big) \;=\; 0 \;=\; \dim\big(x \cdot [\tau] \cdot ([\varphi] - n)\big).$$

Otherwise, if a is not a square, we still obtain

$$\begin{aligned} Q([\varphi]) \cdot \Big([\varphi]^2 - n^2\Big) \;&=\; x \cdot [\tau] \cdot \Big([\varphi]^2 - n^2\Big) \;=\; x \cdot \Big([\tau] \cdot [a\varphi]^2 - [\tau] \cdot n^2\Big) \\ &=\; x \cdot \big([a\varphi \otimes a\varphi \otimes \tau] - \big[n^2 \times \tau\big]\big) \;=\; x \cdot 0 \;=\; 0, \end{aligned}$$

which completes the proof. □

2.7.2 Theorem. *Let φ be an n-dimensional excellent quadratic form of height $h \in \mathbb{N}_0$ over K, let $\varphi = \psi_0, \psi_1, \ldots, \psi_h$ be the sequence of its higher complements, and for $j = 0, \ldots, h$ set $n_j := \dim(\psi_j)$. Then*

$$\mathbb{Z}[X] \;\ni\; E_n \;:=\; \begin{cases} X(X^2 - n_{h-1}^2) \cdots (X^2 - n_1^2)(X^2 - n^2) & \textit{for } n \textit{ even} \\ (X^2 - 1)(X^2 - n_{h-1}^2) \cdots (X^2 - n_1^2)(X^2 - n^2) & \textit{for } n \textit{ odd} \end{cases}$$

is an annihilating polynomial for $[\varphi]$. In particular E_n also annihilates $\{\varphi\}$.

Proof. We proceed by induction on h. If $h = 0$ and $\dim(\varphi) = 0$, then indeed $E_0 = X$ annihilates $\varphi = 0$. In the case $\dim(\varphi) = 1$ we have $\varphi = \langle a \rangle$ for some $a \in K^*$, and $[a]^2 = 1$. This shows, that $E_1 = X^2 - 1$ annihilates $[\varphi]$.

Now let $h > 0$. By induction E_{n_1} annihilates the isometry class of the excellent form ψ_1. Clearly $-\psi_1$ is an excellent form of dimension n_1 as well. This implies that E_{n_1} also annihilates $[-\psi_1]$. Since ψ_1 is the complement of φ, it follows from the previous proposition that $E_{n_1} \cdot (X^2 - n^2) = E_n$ annihilates $[\varphi]$. □

Let $n \in \mathbb{N}_0$. In Section 2.4 we have shown that the Lewis polynomial P_n (see (2.4)) is an optimal annihilating polynomial for the isometry and equivalence classes of n-dimensional quadratic forms in the sense that there exists a field K and an n-dimensional quadratic form φ over K such that $\mathrm{Ann}_{[\varphi]} = \mathrm{Ann}_{\{\varphi\}} = (P_n)$. We can now show an analogous statement for the polynomial E_n as defined in Theorem 2.7.2.

2.7.3 Proposition. *For $n \in \mathbb{N}_0$ there exists a field K and an n-dimensional excellent form φ over K such that* $\mathrm{Ann}_{[\varphi]} = \mathrm{Ann}_{\{\varphi\}} = (E_n)$.

Proof. The case $n = 0$ is trivial, since $E_0 = X \in \mathbb{Z}[X]$, and the annihilating ideal of the 0 element in the Witt-Grothendieck ring of any field is equal to the principal ideal (X). If K is formally real, then also the annihilating ideal of $0 \in W(K)$ is equal to (X). So we assume that $n > 0$.

Let F be an Euclidean field, and let $k \in \mathbb{N}_0$. Then by Example 2.4.6.(2) we know that $K := F((t_0))((t_1))\ldots((t_k))$, where t_i is transcendental over $F((t_0))\ldots((t_{i-1}))$ for $i = 0, \ldots, k$, is Pythagorean, $W(K)$ is torsion free, and there exist 2^{k+1} signature homomorphisms $W(K) \to \mathbb{Z}$. More precisely, if $U \subset \{0, \ldots, k\}$ is any subset, then there exists a unique signature homomorphism χ such that $\chi(\{\langle t_i\rangle\}) = 1$ if $i \in U$ and $\chi(\{\langle t_i\rangle\}) = -1$ otherwise. Consider the form $\tau := \langle\langle t_1, \ldots, t_k\rangle\rangle$ over K. Then

$$S_{[t_0\tau]} \;=\; S_{\{t_0\tau\}} \;=\; \begin{cases} \{-1, 1\} & \text{for } k = 0,\\ \{-2^k, 0, 2^k\} & \text{for } k > 0. \end{cases}$$

We proceed by induction on k to show that for all $n \in \mathbb{N}$ with $2^{k-1} < n \leq 2^k$ there exists an excellent n-dimensional subform φ of $t_0\tau$ that has $\mathrm{Ann}_{[\varphi]} = \mathrm{Ann}_{\{\varphi\}} = (E_n)$. If $k = 0$, then $\tau = \langle 1\rangle$ and $\varphi := \langle t_0\rangle$, and the claim follows immediately.

We continue with the case $k > 0$. Then $n_1 = 2^k - n < 2^{k-1}$. If $n_1 = 0$, then $\varphi := t_0\tau$, $h = 1$, and $\mathrm{Ann}_{[\varphi]} = \mathrm{Ann}_{\{\varphi\}} = (E_n) = (X(X^2 - n^2))$. Otherwise let $l \in \mathbb{N}_0$ be minimal such that $n_1 \leq 2^l$. By the induction hypothesis there exists an n_1-dimensional excellent subform ψ of $t_0\langle\langle t_1, \ldots, t_l\rangle\rangle$ over $F((t_0))((t_1))\ldots((t_l)) \subset K$ with $S_{[\psi]} = S_{\{\psi\}} = \{n_1, -n_1, n_2, -n_2, \ldots, n_h, -n_h\}$. If φ is a form over K such that $\varphi \perp \psi_K \cong t_0\tau$, then φ is excellent and

$$\chi(\{\varphi\}) + \chi(\{\psi_K\}) \;=\; \begin{cases} 2^k & \text{if } \chi(\{\langle t_i\rangle\}) = 1 \text{ for } i = 0, \ldots, k,\\ -2^k & \begin{array}{l}\text{if } \chi(\{\langle t_0\rangle\}) = -1 \text{ and}\\ \mathrm{sign}(\{\langle t_i\rangle\}) = 1 \text{ for } i = 1, \ldots, k,\end{array}\\ 0 & \text{otherwise,} \end{cases}$$

for $\chi \in \mathrm{Hom}(W(K), \mathbb{Z})$. Hence it follows easily that $S_{[\varphi]} = S_{\{\varphi\}} = \{n, -n\} \cup S_{\{\psi_K\}}$, which concludes the induction. □

The previous proof contains the key to a more elementary proof of Theorem 2.7.2. More specifically we will show: If φ is an n-dimensional, excellent form over K, then there exists a preimage $x \in \mathbb{Z}[\mathcal{G}(K)]$ of $[\varphi]$ such that P_x divides E_n.

Consider a group G of exponent 2. For a while we revert to considering the more general setting of group rings.

2.7.4 Definition. *Let G be a group of exponent* 2*, and let $z \in \mathbb{Z}[G]$ be k-fold Pfister preform with $k \in \mathbb{N}_0$. A preform $x \in \mathbb{Z}[G]$ is called a* Pfister neighbour *of z, if there exists a preform $y \in \mathbb{Z}[G]$ and an element $g \in G$ such that $gz = x + y$, and if $\frac{1}{2}\dim(z) < \dim(x) \leq \dim(z)$. The preform y is then called the* complement *of x.*

Consider a Pfister neighbour $x \in \mathbb{Z}[G]$ of a Pfister preform $z \in \mathbb{Z}[G]$ with complement $y \in \mathbb{Z}[G]$. Note that we have

$$|z| \;=\; \dim(z) \;=\; \dim(x) + \dim(y) \;=\; |x| + |y|.$$

2.7.5 Lemma. *Let G be a group of exponent* 2*, and let $x \in \mathbb{Z}[G]$ be an n-dimensional Pfister neighbour of a Pfister preform $z \in \mathbb{Z}[G]$. If $y \in \mathbb{Z}[G]$ such that $-y$ is the complement of x, and if $g \in G$ with $gz = x - y$, then $S_x \subset S_y \cup \{-n, n\}$. In particular $(X^2 - n^2)P_y \in \mathbb{Z}[X]$ is an annihilating polynomial for x.*

Proof. For all $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ we have $\chi(gz) = \chi(x) - \chi(y)$. Let $\dim(z) = 2^k$ with $k \in \mathbb{N}_0$. Then $\chi(x) - \chi(y) \in \{-2^k, 0, 2^k\}$. Recall that we always have $|\chi(x)| \leq \dim(x) = |x|$, and since $-y$ is a preform we also have $|\chi(y)| \leq -\dim(y) = |y|$. If $\chi(gz) = -2^k = -\dim(z)$, then it follows that we must have $\chi(x) = -\dim(x) = -n$. Similarly if $\chi(gz) = 2^k = \dim(z)$, then $\chi(x) = \dim(x) = n$. Finally, if $\chi(gz) = 0$, then we obtain $\chi(x) = \chi(y)$. □

2.7.6 Definition. *Let G be a group of exponent* 2*. Every preform $x \in \mathbb{Z}[G]$ with* $\dim(x) = 0, 1$ *is* excellent*. If $x \in \mathbb{Z}[G]$ with* $\dim(x) > 1$*, then x is* excellent *if x is a Pfister neighbour with complement $y \in \mathbb{Z}[G]$ such that y is excellent.*

Let $x \in \mathbb{Z}[G]$ be excellent. Exactly as for excellent quadratic forms there exists a sequence of preforms

$$y_0 = x,\; y_1,\; \ldots,\; y_h \;\in\; \mathbb{Z}[G]$$

with $h \in \mathbb{N}_0$ and $\dim(y_h) \in \{0, 1\}$ such that y_{i-1} is a Pfister neighbour with complement y_i for $i = 1, \ldots, h$. In particular we have $\dim(y_h) = 0$ if and only if $\dim(x)$ is even. As for quadratic forms we call $h(x) := h$ the *height* of x, and the y_i are the *higher complements* of x.

By applying Lemma 2.7.5 inductively we obtain the following proposition.

2.7.7 Proposition. *Let G be a group of exponent* 2*, let $x \in \mathbb{Z}[G]$ be excellent of dimension n and height h with $n, h \in \mathbb{N}_0$. If $y_0, y_1, \ldots, y_h$ is the sequence of higher complements of x, and if we set $n_j :=$* $\dim(y_j)$ *for $j = 0, \ldots, h$, then*

$$\mathbb{Z}[X] \;\ni\; E_n \;=\; \begin{cases} X(X^2 - n_{h-1}^2)\cdots(X^2 - n_1^2)(X^2 - n^2) & \textit{for } n \textit{ even} \\ (X^2 - 1)(X^2 - n_{h-1}^2)\cdots(X^2 - n_1^2)(X^2 - n^2) & \textit{for } n \textit{ odd} \end{cases}$$

is an annihilating polynomial for x.

We can now characterise excellent quadratic forms over a field K with the help of excellent group ring elements in $\mathbb{Z}[\mathcal{G}(K)]$. To prove this we need the following property of excellent quadratic forms: Let φ be an excellent quadratic form over K with higher complements

$\psi_0 = \varphi, \psi_1, \ldots, \psi_h$, where h is the height of φ. Now for $i = 0, \ldots, h-1$ the form ψ_i is a Pfister neighbour of a Pfister form τ_i over K. In [KN82, Theorems 2.1 & 2.4] D. Kijima and M. Nishi show that for any $a \in D_K^*(\varphi)$ we have

$$[a\varphi] \sim \begin{cases} [\tau_0] - [\tau_1] + [\tau_2] - \cdots + [\tau_{h-1}] - [\langle 1\rangle] & \text{for } n \text{ and } h \text{ odd,} \\ [\tau_0] - [\tau_1] + [\tau_2] - \cdots + [\tau_{h-2}] - [\tau_{h-1}] + [\langle 1\rangle] & \text{for } n \text{ odd and } h \text{ even,} \\ [\tau_0] - [\tau_1] + [\tau_2] - \cdots + [\tau_{h-3}] - [\tau_{h-2}] + [\tau_{h-1}] & \text{for } n \text{ even and } h \text{ odd,} \\ [\tau_0] - [\tau_1] + [\tau_2] - \cdots + [\tau_{h-2}] - [\tau_{h-1}] & \text{for } n \text{ and } h \text{ even.} \end{cases} \tag{2.13}$$

Under certain assumptions on the sequence of Pfister forms $\tau_0, \ldots, \tau_h$ excellent quadratic forms can be characterised by this property. In our situation we only need to know that, in the case where φ is excellent, the Pfister form τ_i is a subform of τ_{i-1} with $\dim(\tau_i) < \dim(\tau_{i-1})$ for $i = 1, \ldots, h-1$. This can be shown quite easily. Since $\psi_{i-1} \perp \psi_i \cong b\tau_{i-1}$ for some $b \in K^*$, it follows that $(\tau_{i-1})_{K(\psi_i)} \sim 0$. As $K(\psi_i)$ and $K(\tau_i)$ are K-equivalent, we obtain $(\tau_{i-1})_{K(\tau_i)} \sim 0$. By Proposition 2.6.15 we know that τ_i is a subform of τ_{i-1}. In particular this implies that the equivalence in (2.13) is actually an equality. During the proof of the following proposition we will need the stronger statement that τ_i divides τ_{i-1}, which follows from Proposition 2.6.16. By [EL72a, Theorem 2.7] this implies that there exists a Pfister form ρ_i over K such that $\tau_{i-1} \cong \tau_i \otimes \rho_i$.

2.7.8 Proposition. *An n-dimensional quadratic form φ over K is excellent if and only if there exists an excellent preimage $x \in \mathbb{Z}[\mathcal{G}(K)]$ of $[\varphi]$.*

Proof. Let $x \in \mathbb{Z}[\mathcal{G}(K)]$ be excellent with sequence of higher complements $y_0 = x, y_1, \ldots, y_h$. If φ is a quadratic form over K such that $[\varphi]$ is the image of x, and if ψ_j is a quadratic form over K such that $[\psi_j]$ is the image of y_j for $j = 1, \ldots, h$, then clearly φ is excellent and $\psi_0 := \varphi, \psi_1, \ldots, \psi_h$ is the sequence of higher complements of φ.

Now assume that φ is an excellent quadratic form over K with $n := \dim(\varphi)$ and $h := h(\varphi)$. For $i = 0, \ldots, h$ let ψ_i be the i-th complement of φ, and for $0 \le i < h$ let τ_i be the Pfister form over K such that ψ_i is a Pfister neighbour of τ_i. We have seen that for $i = 1, \ldots, h-1$ there exists a Pfister form ρ_i over K such that $\tau_{i-1} \cong \tau_i \otimes \rho_i$. In particular there exist $r_0, \ldots, r_{h-1} \in \mathbb{N}$ and $a_1, \ldots, a_{r_0} \in K^*$ such that $r_{h-1} < \cdots < r_0$ and $\tau_i \cong \langle\langle a_1, \ldots, a_{r_i}\rangle\rangle$ for $i = 0, \ldots, h-1$. For $i = 0, \ldots, h-1$ set

$$t_i \ := \ (1 + \overline{a_1}) \cdots (1 + \overline{a_{r_i}}) \ \in \ \mathbb{Z}[\mathcal{G}(K)],$$

and for $i = 1, \ldots, h-1$ set

$$d_i \ := \ t_{i-1} - t_i \ = \ t_i \cdot \big((1 + \overline{a_{r_i+1}}) \cdots (1 + \overline{a_{r_{i-1}}}) - 1\big) \ \in \ \mathbb{Z}[\mathcal{G}(K)].$$

We see immediately that d_i is a preform for $i = 1, \ldots, h-1$. Define

$$\mathbb{Z}[\mathcal{G}(K)] \ni x := \begin{cases} d_1 + d_3 + \cdots + d_{h-2} + t_{h-1} - 1 & \text{for } n \text{ and } h \text{ odd,} \\ d_1 + d_3 + \cdots + d_{h-1} + 1 & \text{for } n \text{ odd and } h \text{ even,} \\ d_1 + d_3 + \cdots + d_{h-2} + t_{h-1} & \text{for } n \text{ even and } h \text{ odd,} \\ d_1 + d_3 + \cdots + d_{h-1} & \text{for } n \text{ and } h \text{ even.} \end{cases}$$

Note that, if $h = 0$ then we obtain $x = 0$ for n even and $x = 1$ for n odd. Furthermore, if $h = 1$ then $x = t_0$ for n even and $x = t_0 - 1$ for n odd. Thus we see that in all cases x is a preform. In particular, if $a \in K^*$ with $a(\varphi \perp \psi_1) \cong \tau_0$ then $\overline{a} \cdot x$ is a preimage of $[\varphi]$.

We proceed by induction on $h \geq 0$ to show that x is excellent. If $h = 0$, then this is trivial. So assume that $h > 0$. Set

$$\mathbb{Z}[\mathcal{G}(K)] \ \ni \ y \ := \ \begin{cases} d_2 + d_4 + \cdots + d_{h-1} + 1 & \text{for } n \text{ and } h \text{ odd,} \\ d_2 + d_4 + \cdots + d_{h-2} + t_{h-1} - 1 & \text{for } n \text{ odd and } h \text{ even,} \\ d_2 + d_4 + \cdots + d_{h-1} & \text{for } n \text{ even and } h \text{ odd,} \\ d_2 + d_4 + \cdots + d_{h-2} + t_{h-1} & \text{for } n \text{ and } h \text{ even.} \end{cases}$$

It follows that

$$x + y \ = \ d_1 + d_2 + \cdots + d_{h-1} + t_{h-1} \ = \ t_0.$$

Thus x is a Pfister neighbour of t_0 with complement y. By induction y is excellent, which implies that x is excellent as well. Now $\overline{a} \cdot x$ is excellent if and only if x is excellent. Therefore $\overline{a} \cdot x$ is an excellent preimage of $[\varphi]$. □

Theorem 2.7.2 is now a consequence of the previous proposition and Proposition 2.7.7.

Appendix A

Appendix

A.1 Calculations concerning the Clifford invariant

In this section we cover in full detail the calculations needed to establish the formulas used in Section 2.4.

Throughout this section, let K be a field with $\mathrm{char}(K) \neq 2$. We will make use of the notation defined in 2.4.1 and 2.4.13.

A.1.1 Calculation. *Let $\varphi_1, \ldots, \varphi_m$ be even-dimensional quadratic forms over K, $m \in \mathbb{N}_0$. Then*

$$c(\varphi_1 \perp \ldots \perp \varphi_m) \;=\; c(\varphi_1) \cdots c(\varphi_m) \cdot \left(\prod_{1 \le i < j \le m} (d(\varphi_i), d(\varphi_j))_K \right).$$

Proof. We proceed by induction on m. For $m = 0$ the equality holds trivially. So assume that $m > 0$. Now

$$\begin{aligned} & c(\varphi_1 \perp \ldots \perp \varphi_m) \\ = \;& c(\varphi_1) c(\varphi_2 \perp \ldots \perp \varphi_m)\,(d(\varphi_1), d(\varphi_2) \cdots d(\varphi_m))_K \\ = \;& c(\varphi_1) c(\varphi_2) \cdots c(\varphi_m) \cdot \left(\prod_{2 \le i < j \le m} (d(\varphi_i), d(\varphi_j))_K \right) \cdot \left(\prod_{j=2}^{m} (d(\varphi_1), d(\varphi_j))_K \right) \\ = \;& c(\varphi_1) \cdots c(\varphi_m) \cdot \left(\prod_{1 \le i < j \le m} (d(\varphi_i), d(\varphi_j))_K \right) \end{aligned}$$

by the Lemmas 2.3.7 and 2.2.30, and by induction. □

A.1.2 Calculation. *Let φ and ψ be quadratic forms over K. Set $m = \dim(\psi)$. If $\dim(\varphi)$ is even, then*

$$c(\varphi \otimes \psi) \;=\; c(\varphi)^m \,(d(\varphi), d(\psi))_K\,.$$

Proof. Assume that $\psi = \langle b_1, \ldots, b_m \rangle$ with $m \in \mathbb{N}_0$ and $b_1, \ldots, b_m \in K^*$. Then

$$\begin{aligned} c(\varphi \otimes \psi) &= c(b_1\varphi \perp \ldots \perp b_m\varphi) \\ &= c(b_1\varphi) \cdots c(b_m\varphi) \cdot \left(\prod_{1 \leq i,j \leq m} (d(b_i\varphi), d(b_j\varphi))_K \right) \\ &= c(\varphi)^m \cdot \left(\prod_{i=1}^{m} (b_i, d(\varphi))_K \right) \cdot \left((-1)^{\frac{m(m-1)}{2}}, d(\varphi) \right)_K \\ &= c(\varphi)^m \, (d(\psi), d(\varphi))_K \end{aligned}$$

by Lemma 2.3.8 and Calculation A.1.1. □

A.1.3 Corollary. *If φ and ψ are even-dimensional quadratic forms over K, then*

$$c(\varphi \otimes \psi) \;=\; (d(\varphi), d(\psi))_K \,.$$

A.1.4 Calculation. *For $r \in \mathbb{Z}$ we have*

$$d(r) \;=\; (-1)^{\frac{r(r-1)}{2}}.$$

Proof. If $r \geq 0$, then the equality follows directly from the definition of the discriminant. So assume that $r < 0$. Then

$$d(r) \;=\; d((-r) \times \langle -1 \rangle) \;=\; (-1)^{\frac{-r(-r-1)}{2}} (-1)^{-r} \;=\; (-1)^{\frac{r(r-1)}{2}}.$$ □

A.1.5 Calculation. *Let φ be a quadratic form over K with $n = \dim(\varphi)$, and let $a, b \in \mathbb{Z}$ with $a \equiv b \equiv n \pmod 2$. We have*

$$c((\varphi \perp a) \otimes (\varphi \perp b)) \;=\; ((-1)^n d(\varphi), -1)_K^{1 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{\frac{a(a-1)}{2} \cdot \frac{b(b-1)}{2}} \,.$$

Proof. We use Lemma 2.3.7 and Calculations A.1.2 and A.1.4. If n is even, then

$$\begin{aligned} c((\varphi \perp a) \otimes (\varphi \perp b)) &= (d(\varphi \perp a), d(\varphi \perp b))_K \\ &= \left((-1)^{\frac{a(a-1)}{2}} d(\varphi), (-1)^{\frac{b(b-1)}{2}} d(\varphi) \right)_K \\ &= (d(\varphi), -1)_K^{1 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{\frac{a(a-1)}{2} \cdot \frac{b(b-1)}{2}} \,. \end{aligned}$$

If n is odd, then

$$\begin{aligned} & c((\varphi \perp a) \otimes (\varphi \perp b)) \\ =\; & (d(\varphi \perp a), d(\varphi \perp b))_K \\ =\; & \left((-1)^{1 + \frac{a(a-1)}{2}} d(\varphi), (-1)^{1 + \frac{b(b-1)}{2}} d(\varphi) \right)_K \\ =\; & (d(\varphi), -1)_K^{3 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{(1 + \frac{a(a-1)}{2})(1 + \frac{b(b-1)}{2})} \\ =\; & (d(\varphi), -1)_K^{1 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{1 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{\frac{a(a-1)}{2} \cdot \frac{b(b-1)}{2}} \\ =\; & (-d(\varphi), -1)_K^{1 + \frac{a(a-1)}{2} + \frac{b(b-1)}{2}} \, (-1,-1)_K^{\frac{a(a-1)}{2} \cdot \frac{b(b-1)}{2}} \,. \end{aligned}$$

By summarising these two cases we obtain the claimed equality. □

A.1.6 Corollary. *Let φ be an n-dimensional quadratic form over K, and let $a, b \in \mathbb{Z}$ with $a \equiv b \equiv n \pmod 2$. The following tables display the values of $c((\varphi \perp a) \otimes (\varphi \perp b))$. For n even we have*

b a	$\equiv 0 \pmod 4$	$\equiv 2 \pmod 4$
$\equiv 0 \pmod 4$	$(d(\varphi), -1)_K$	1
$\equiv 2 \pmod 4$	1	$(-d(\varphi), -1)_K$

,

and for n odd we have

b a	$\equiv 1 \pmod 4$	$\equiv 3 \pmod 4$
$\equiv 1 \pmod 4$	$(-d(\varphi), -1)_K$	1
$\equiv 3 \pmod 4$	1	$(d(\varphi), -1)_K$

.

A.1.7 Corollary. *If φ is an n-dimensional quadratic form over K, and if $a, b \in \mathbb{Z}$ with $a \equiv n \pmod 2$ and $b \equiv a \pmod 4$, then the following table displays the values of $c((\varphi \perp a) \otimes (\varphi \perp b))$:*

n a	*even*	*odd*
$\equiv 0, 1 \pmod 4$	$(d(\varphi), -1)_K$	$(-d(\varphi), -1)_K$
$\equiv 2, 3 \pmod 4$	$(-d(\varphi), -1)_K$	$(d(\varphi), -1)_K$

.

A.1.8 Corollary. *Let φ be a quadratic form of dimension n over K. Consider $r, s \in \mathbb{Z}$ with $r \equiv s \equiv n \pmod 2$. The following table displays the values of $c((\varphi \perp -r) \otimes (\varphi \perp -s))$:*

s r	$\equiv 0, 1 \pmod 4$	$\equiv 2, 3 \pmod 4$
$\equiv 0, 1 \pmod 4$	$(d(\varphi), -1)_K$	1
$\equiv 2, 3 \pmod 4$	1	$(-d(\varphi), -1)_K$

.

A.1.9 Corollary. *Let φ be an n-dimensional quadratic form over K, and let $r \in \mathbb{Z}$ with $r \equiv n \pmod 2$. Then the following table displays the possible values of $c((\varphi \perp -n) \otimes (\varphi \perp -r))$:*

n r	$\equiv 0, 1 \pmod 4$	$\equiv 2, 3 \pmod 4$
$\equiv 0, 1 \pmod 4$	$(\det(\varphi), -1)_K$	1
$\equiv 2, 3 \pmod 4$	1	$(\det(\varphi), -1)_K$

Proof. In the case that $r \equiv s \pmod 4$ we can summarise the table from Corollary A.1.8 as follows:

$$c((\varphi \perp -r) \otimes (\varphi \perp -s)) \;=\; \Big((-1)^{\frac{s(s-1)}{2}} d(\varphi), -1\Big)_K .$$

In our case $s = n$. So if $r \equiv n \pmod 4$, then we obtain

$$c((\varphi\perp - n) \otimes (\varphi\perp - r)) \;=\; \Big((-1)^{\frac{n(n-1)}{2}} d(\varphi), -1\Big)_K \;=\; (\det(\varphi), -1)_K \,,$$

which proves the claim in this case. The case $r \equiv n + 2 \pmod 4$ follows directly from Corollary A.1.8. □

A.1.10 Calculation. *Let φ be a quadratic form over K, $n = \dim(\varphi)$, and let $a \in \mathbb{Z}$ with $a \equiv n \pmod 2$. Then*

$$c(2 \times (\varphi\perp a)) \;=\; ((-1)^n d(\varphi), -1)_K \, (-1, -1)_K^{\frac{a(a-1)}{2}} \,.$$

Proof. We use Calculation A.1.2. If n is even, then

$$\begin{aligned} c(2 \times (\varphi\perp a)) &= (d(2), d(\varphi\perp a))_K \\ &= \Big(-1, (-1)^{\frac{a(a-1)}{2}} d(\varphi)\Big)_K \\ &= (d(\varphi), -1)_K \, (-1, -1)_K^{\frac{a(a-1)}{2}} \,. \end{aligned}$$

If n is odd, then

$$\begin{aligned} c(2 \times (\varphi\perp a)) &= \Big(-1, (-1)^{1+\frac{a(a-1)}{2}} d(\varphi)\Big)_K \\ &= (-d(\varphi), -1)_K \, (-1, -1)_K^{\frac{a(a-1)}{2}} \,. \end{aligned}$$

The claimed equality is the summary of these two cases. □

A.1.11 Corollary. *If φ is an n-dimensional quadratic form over K, and if $a \in \mathbb{Z}$ with $a \equiv n \pmod 2$, then the following table displays the values of $c(2 \times (\varphi\perp a))$:*

n a	*even*	*odd*
$\equiv 0, 1 \pmod 4$	$(d(\varphi), -1)_K$	$(-d(\varphi), -1)_K$
$\equiv 2, 3 \pmod 4$	$(-d(\varphi), -1)_K$	$(d(\varphi), -1)_K$

.

A.1.12 Corollary. *Let φ be a quadratic form over K, and let $r \in \mathbb{Z}$ with $r \equiv n \pmod 2$. Then*

$$c(2 \times (\varphi\perp - r)) \;=\; (d(\varphi), -1)_K \, (-1, -1)_K^{\frac{r(r-1)}{2}} \,.$$

Proof. By Calculation A.1.10

$$\begin{aligned} c(2 \times (\varphi\perp - r)) &= ((-1)^n d(\varphi), -1)_K \, (-1, -1)_K^{\frac{r(r+1)}{2}} \\ &= \begin{cases} (d(\varphi), -1)_K \, (-1, -1)_K^{\frac{r(r+1)}{2}} & \text{if } n \text{ is even,} \\ (d(\varphi), -1)_K \, (-1, -1)_K^{1+\frac{r(r+1)}{2}} & \text{if } n \text{ is odd.} \end{cases} \end{aligned}$$

Now the claim follows, since for r even we have $r(r + 1) \equiv r(r - 1) \pmod 4$, and for r odd $2 + r(r + 1) \equiv r(r - 1) \pmod 4$. □

A.1.13 Corollary. *For an n-dimensional quadratic form φ over K the following equality holds:*

$$c(2 \times (\varphi\perp -n)) \;=\; (\det(\varphi), -1)_K\,.$$

Proof. From Corollary A.1.12 it follows that

$$c(2 \times (\varphi\perp -n)) \;=\; \left((-1)^{\frac{n(n-1)}{2}} d(\varphi), -1\right)_K \;=\; (\det(\varphi), -1)_K\,. \qquad \square$$

Bibliography

[Ara75a] Arason, Jón K.: Cohomologische Invarianten quadratischer Formen. In: *J. Algebra* 36 (1975), no. 2, pp. 448–491

[Ara75b] Arason, Jón K.: Primideale im graduierten Witt ring und im mod 2 Cohomologiering. In: *Math. Z.* 145 (1975), no. 2, pp. 139–143

[Ayo83] Ayoub, Christine W.: On constructing bases for ideals in polynomial rings over the integers. In: *J. Number Theory* 17 (1983), no. 2, pp. 204–225

[BF07] Bayer-Fluckiger, Eva: Multiples of trace forms and algebras with involution. In: *Int. Math. Res. Not. IMRN* (2007), no. 23, pp. Art. ID rnm112, 15

[Bou89a] Bourbaki, Nicolas: *Algebra I, Chapter 1-3*. Springer, 1989 (Elements of Mathematics)

[Bou89b] Bourbaki, Nicolas: *Commutative algebra, Chapters 1-7*. Springer, 1989 (Elements of Mathematics)

[Bou90] Bourbaki, Nicolas: *Algebra II, Chapters 4-7*. Springer, 1990 (Elements of Mathematics)

[DW07] De Wannemacker, Stefan: Annihilating polynomials for quadratic forms and Stirling numbers of the second kind. In: *Math. Nachr.* 280 (2007), no. 11, pp. 1257–1267

[Eis95] Eisenbud, David: *Graduate Texts in Mathematics*. Vol. 150: *Commutative algebra with a view towards algebraic geometry*. Springer, 1995

[EKM08] Elman, Richard ; Karpenko, Nikita ; Merkurjev, Alexander S.: *American Mathematical Society Colloquium Publications*. Vol. 56: *The algebraic and geometric theory of quadratic forms*. American Mathematical Society, 2008

[EL72a] Elman, Richard ; Lam, Tsit-Yuen: Pfister forms and K-theory of fields. In: *J. Algebra* 23 (1972), pp. 181–213

[EL72b] Elman, Richard ; Lam, Tsit-Yuen: Quadratic forms over formally real fields and pythagorean fields. In: *Amer. J. Math.* 94 (1972), pp. 1155–1194

[GS06] Gille, Philippe ; Szamuely, Tamás: *Cambridge Studies in Advanced Mathematics.* Vol. 101: *Central simple algebras and Galois cohomology*. Cambridge University Press, 2006

[Hof95] Hoffmann, Detlev W.: Isotropy of quadratic forms over the function field of a quadric. In: *Math. Zeitschrift* 220 (1995), pp. 461–476

[HR93] Hurrelbrink, Jürgen ; Rehmann, Ulf: Splitting patterns of excellent quadratic forms. In: *J. Reine Angew. Math.* 444 (1993), pp. 183–192

[HR95] Hurrelbrink, Jürgen ; Rehmann, Ulf: Splitting patterns of quadratic forms. In: *Math. Nachr.* 176 (1995), pp. 111–127

[HR98] Hurrelbrink, Jürgen ; Rehmann, Ulf: Splitting patterns and trace forms. In: *Canad. Math. Bull.* 41 (1998), no. 1, pp. 71–78

[Hur89] Hurrelbrink, Jürgen: Annihilating polynomials for group rings and Witt rings. In: *Canad. Math. Bull.* 32 (1989), no. 4, pp. 412–416

[Kap94] Kaplansky, Irving: *Commutative rings.* Polygonal Publishing House, 1994

[Ker90] Kersten, Ina: *Aspects of mathematics.* Vol. D6: *Brauergruppen über Körpern*. Vieweg, 1990

[KM03] Karpenko, Nikita A. ; Merkurjev, Alexander S.: Essential dimension of quadrics. In: *Invent. Math.* 153 (2003), pp. 361–372

[KN82] Kijima, Daiji ; Nishi, Mieo: A note on exzellent forms. In: *Hiroshima Math. J.* 12 (1982), pp. 249–258

[Kne73] Knebusch, Manfred: Specialization of quadratic and symmetric bilinear forms, and a norm theorem. In: *Acta Arith.* 24 (1973), pp. 279–299

[Kne76] Knebusch, Manfred: Generic splitting of quadratic forms I. In: *Proc. London Math. Soc.* 33 (1976), pp. 65–93

[Kne77] Knebusch, Manfred: Generic splitting of quadratic forms II. In: *Proc. London Math. Soc.* 34 (1977), pp. 1–31

[KRW72] Knebusch, Manfred ; Rosenberg, Alex ; Ware, Roger: Structure of Witt rings and quotients of Abelian group rings. In: *Amer. J. Math.* 94 (1972), no. 1, pp. 119–155

[Lam05] Lam, Tsit-Yuen: *Graduate Studies in Mathematics.* Vol. 67: *Introduction to quadratic forms over fields*. American Mathematical Society, 2005

[Lan02] Lang, Serge: *Graduate Texts in Mathematics.* Vol. 211: *Algebra*. Revised third edition. Springer, 2002

[Lew87] LEWIS, David W.: Witt rings as integral rings. In: *Invent. Math.* 90 (1987), pp. 631–633

[Lew89] LEWIS, David W.: New proofs of the structure theorems for Witt rings. In: *Expo. Math.* 7 (1989), pp. 83–88

[Lew92] LEWIS, David W.: Annihilating polynomials and positive forms. In: *Canad. Math. Bull.* 35 (1992), no. 1, pp. 103–107

[Lew01] LEWIS, David W.: Annihilating polynomials for quadratic forms. In: *Int. J. Math. Math. Sci.* 27 (2001), no. 7, pp. 449–455

[LM00] LEWIS, David W. ; MCGARRAGHY, Seán: Annihilating polynomials, étale algebras, trace forms and the Galois number. In: *Arch. Math.* 75 (2000), no. 2, pp. 116–120

[Mat86] MATSUMURA, Hideyuki: *Cambridge Studies in Advanced Mathematics.* Vol. 8: *Commutative ring theory*. Cambridge University Press, 1986

[McG02] MCGARRAGHY, Séan: Exterior powers of symmetric bilinear forms. In: *Algebra Colloq.* 9 (2002), no. 2, pp. 197–218

[Mer81a] MERKURJEV, Alexander S.: On the norm residue symbol of degree 2. In: *Dokladi Akad. Nauk. SSSR* 261 (1981), pp. 542–547. – English translation: [Mer81b]

[Mer81b] MERKURJEV, Alexander S.: On the norm residue symbol of degree 2. In: *Soviet Math. Doklady* 24 (1981), pp. 546–551

[Mil70] MILNOR, John: Algebraic K-theory and quadratic forms. In: *Invent. Math.* 9 (1970), pp. 318–344

[OG97] ONGENAE, Veerle ; VAN GEEL, Jan: Polynomials annihilating the Witt ring. In: *Math. Nachr.* 185 (1997), pp. 213–226

[OVV07] ORLOV, Dmitry ; VISHIK, Alexander ; VOEVODSKY, Vladimir: An exact sequence for $K_*^M/2$ with applications to quadratic forms. In: *Ann. of Math. (2)* 165 (2007), no. 1, pp. 1–13

[Pfi65] PFISTER, Albrecht: Multiplikative quadratische Formen. In: *Arch. Math.* 16 (1965), pp. 363–370

[Pfi95] PFISTER, Albrecht: *London Mathematical Society Lecture Note Series.* Vol. 217: *Quadratic forms with applications to algebraic geometry and topology*. Cambridge University Press, 1995

[Réd67] RÉDEI, László: *Algebra, Volume 1.* Pergamon Press, 1967

[Rüh08] RÜHL, Klaas-Tido: *Annihilating ideals of quadratic forms over local and global fields.* Aug. 2008. – 22 pages, to appear in *Int. J. Number Theory*

[Rüh08] Rühl, Klaas-Tido: Annihilating polynomials of excellent quadratic forms. In: *Arch. Math.* 90 (2008), no. 3, pp. 217–222

[Sch85] Scharlau, Winfried: *Grundlehren der Mathematischen Wissenschaften.* Vol. 270: *Quadratic and Hermitian forms*. Springer, 1985

[Ser95] Serre, Jean-Pierre: *Graduate Texts in Mathematics.* Vol. 67: *Local fields*. Second corrected printing. Springer, 1995

[Ser02] Serre, Jean-Pierre: *Galois cohomology.* Corrected second printing. Springer, 2002

[Sol80] Solow, Anita E.: The square class invariant for quadratic forms and the classification problem. In: *Linear Multilinear Algebra* 9 (1980), no. 1, pp. 39–50

[Sze52] Szekeres, George: A canonical basis for the ideals of a polynomial domain. In: *Amer. Math. Monthly* 6 (1952), pp. 379–386

[Tro78] Trotter, Peter G.: Ideals in $\mathbb{Z}[x, y]$. In: *Acta Math. Acad. Sci. Hungar.* 32 (1978), no. 1-2

[Voe03] Voevodsky, Vladimir: Motivic cohomology with $\mathbb{Z}/2$-coefficients. In: *Publ. Math. Inst. Hautes Études Sci.* 98 (2003), pp. 59–104

[War73] Ware, Roger: When are Witt rings group rings? In: *Pacific J. Math.* 49 (1973), pp. 279–284

[War78] Ware, Roger: When are Witt rings group rings? II. In: *Pacific J. Math.* 76 (1978), no. 2, pp. 541–564

[Wit37] Witt, Ernst: Theorie der quadratischen Formen in beliebigen Körpern. In: *J. Reine Angew. Math.* 176 (1937), pp. 31–44

Nomenclature

$\varphi \perp \psi$ the orthogonal sum of the quadratic forms φ and ψ, page 44

$U \perp W$ the orthogonal sum of the subvector spaces U and W, page 42

$(V, \varphi) \perp (W, \psi)$ the orthogonal sum of the quadratic spaces (V, φ) and (W, ψ), page 44

$v \perp w$ the vectors v and w are orthogonal, page 42

$a \cdot_{\mathrm{op}} b$ the product of a and b in the opposite algebra, page 55

$\varphi \cong \psi$ isometry of the quadratic maps φ and ψ, page 41

$(V, \varphi) \cong (W, \psi)$ isometry of the quadratic spaces (V, φ) and (W, ψ), page 41

$\langle a_1, \ldots, a_n \rangle$ the quadratic form associated to the diagonal matrix $\operatorname{diag}(a_1, \ldots, a_n)$, page 43

$\langle\langle b_1, \ldots, b_k \rangle\rangle$ the k-fold Pfister form $\langle 1, b_1 \rangle \otimes \cdots \otimes \langle 1, b_k \rangle$, page 50

$\varphi \otimes \psi$ the tensor product of the quadratic forms φ and ψ, page 46

$A \sim B$ equivalence of the central simple algebras A and B, page 54

$\varphi \sim \psi$ equivalence of the quadratic forms φ and ψ, page 46

$n \times \varphi$ the n-fold sum of the quadratic form φ, page 45

$(a, b)_K$ the quaternion algebra over K with standard basis $\{1, u, v, uv\}$ such that $u^2 = a$ and $v^2 = b$, page 57

$< m_\nu \mid \nu \in N >_R$ the R-submodule of an S-module M generated by $\{m_\nu\}_{\nu \in N} \subset M$, where S is an R-algebra, page 28

χ_H the ring homomorphism $\mathbb{Z}[G] \to \mathbb{Z}$ associated to a subgroup $H \subset G$, where G is a group of exponent 2, page 27

$\lambda_*(\varphi)$ the specialisation of the quadratic form φ with respect to the place λ, page 84

$[\varphi]$ the isometry class of the quadratic form φ, page 45

$\{\varphi\}$ the equivalence class of the quadratic form φ, page 46

φ_A the quadratic form associated to a symmetric matrix A, page 41

φ_L the quadratic form φ considered over the field extension L, page 50

φ_P the quadratic map associated to the homogeneous polynomial P of degree 2, page 41

φ_{an} the anisotropic kernel of the quadratic form φ, page 45

φ_b the quadratic map associated to the symmetric bilinear form b, page 40

φ_k the k-th anisotropic kernel of the quadratic form φ, page 88

τ' the pure part of the Pfister form τ, page 86

$[A]$ the equivalence class of the central simple algebra A, page 54

A_φ the symmetric matrix associated to the quadratic map φ with respect to a certain basis, page 41

$A_{\varphi,\mathcal{B}}$ the symmetric matrix associated to the quadratic map φ with respect to the basis $\mathcal{B}$, page 41

A_L the L-algebra $A \otimes_K L$, where K is a field and A is a K-algebra, page 55

$\mathrm{Ann}_{W(K)}$ the ideal in $\mathbb{Z}[X]$ consisting of the polynomials, which annihilate all $x \in W(K)$, page 74

$\mathrm{Ann}^{(e)}_{W(K)}$ the ideal in $\mathbb{Z}[X]$ consisting of the polynomials, which annihilate all $x \in I(K)$, page 74

$\mathrm{Ann}^{(o)}_{W(K)}$ the ideal in $\mathbb{Z}[X]$ consisting of the polynomials, which annihilate all $x \in W(K) \setminus I(K)$, page 74

Ann_x the annihilating ideal of an element $x \in R$, where R is a commutative ring, page 23

A^{op} the opposite algebra of an algebra A, page 55

A_P the symmetric matrix associated to the homogeneous polynomial P of degree 2, page 41

b_φ the symmetric bilinear form associated to the quadratic form φ, page 40

$\mathrm{Br}(K)$ the Brauer group of a field K, page 54

$c(\varphi)$ the Clifford invariant of the quadratic form φ, page 62

$C_d^{(I)}$ the ideal of leading coefficients of all degree d polynomials in $(I : (Q_I))$, where I is an ideal, page 13

$d(\varphi)$	the discriminant of the quadratic form φ, page 60
$\det(\varphi)$	the determinant of the quadratic form φ, page 47
$\operatorname{diag}(a_1, \ldots, a_n)$	the diagonal matrix with entries $a_1, \ldots, a_n$, page 43
$\dim(\varphi)$	the dimension of the quadratic map φ, page 40
$\dim(V, \varphi)$	the dimension of the quadratic space (V, φ), page 40
$\dim(x)$	the dimension of an element $x \in \mathbb{Z}[G]$, where G is a group of exponent 2, page 21
$D_K^*(\varphi)$	the set $D_K(\varphi) \setminus \{0\}$, page 42
$D_K(\varphi)$	the set of all elements represented by the quadratic form φ over the field K, page 42
e_0	the dimension index, page 30
e_1	the first cohomological invariant, page 60
e_2	the second cohomological invariant, page 63
$\overline{g}$	the element $gN \in {}^{G}\!/_{N}$, where G is a group and $N \subset G$ is a normal subgroup, page 19
gcd	the greatest common divisor of a set of elements in a unique factorisation domain, page 12
$\mathcal{G}(K)$	the square class group of the field K, page 47
$G_K(\varphi)$	the set of similarity factors of the quadratic form φ over the field K, page 49
$\mathbb{H}$	the hyperbolic plane $\langle 1, -1 \rangle$, page 44
H_χ	the subgroup of G associated to a ring homomorphism $\chi : \mathbb{Z}[G] \to \mathbb{Z}$, where G is a group of exponent 2, page 27
$h(\varphi)$	the height of the quadratic form φ, page 88
$i(\varphi)$	the Witt index of the quadratic form φ, page 45
$I(G)$	the fundamental ideal of the group ring $\mathbb{Z}[G]$, where G is a group of exponent 2, page 30
$I(K)$	the fundamental ideal of the Witt ring $W(K)$, where K is a field, page 51
$i_k(\varphi)$	the k-th Witt index of the quadratic form φ, page 88
$I^k(K)$	the k-th power of the fundamental ideal $I(K)$, where K is a field, page 60

$I(R)$	the fundamental ideal of a Witt ring R for a group of exponent 2, page 30
K^∞	the set consisting of the elements of the field K and the symbol ∞, page 83
$K(\varphi)$	the function field of the quadratic form φ over the field K, page 85
lc	the leading coefficient of a polynomial, page 13
M_{tor}	the torsion submodule of the module M, page 19
$\mathbb{N}$	the natural numbers (excluding 0), page 12
$\mathbb{N}_0$	the set $\mathbb{N} \cup \{0\}$, page 12
$\mathrm{Nil}(R)$	the nilradical of a ring R, page 33
P_φ	the quadratic form associated to the quadratic map φ with respect to a certain basis, page 42
$P_{\varphi,\mathcal{B}}$	the quadratic form associated to the quadratic map φ with respect to the basis $\mathcal{B}$, page 42
$\mathfrak{p}_H$	the prime ideal in $\mathbb{Z}[G]$ associated to a subgroup $H \subset G$, where G is a group of exponent 2, page 28
P_n	the Lewis polynomial of degree $n+1$, $n \in \mathbb{N}_0$, page 24
P_x	the signature polynomial of the element x, page 23
Q_0	the subvector space of pure quaternions of the quaternion algebra Q, page 57
Q_I	the embracing polynomial of the ideal I, page 12
$\mathrm{Quot}(R)$	the quotient field of the integral domain R, page 85
$\mathrm{Rad}(\varphi)$	the radical of the quadratic form φ, page 43
$r(I)$	$r(I)+1$ is the number of elements of a modest set of generators for the ideal $I \subset R[X]$, page 15
$r_{L/K}$	the restriction map $\mathrm{Br}(K) \to \mathrm{Br}(L)$, where L is a field extension of the field K, page 56
R_{tor}	the torsion subgroup of a Witt ring R for a group of exponent 2, page 33
$s(\varphi)$	the Hasse invariant of the quadratic form φ, page 61
$s(I)$	$s(I)+1$ is the number of elements of a convenient set of generators for the ideal $I \subset R[X]$, page 13
$s(K)$	the level of the field K, page 50

S_x	the signature set of the element x, page 23
$U^\perp$	the orthogonal complement of a subvector space U, page 42
$\widehat{W}(K)$	the Witt-Grothendieck ring of the field K, page 46
$W(K)$	the Witt ring of the field K, page 46
$\|x\|$	the norm of the group ring element x, page 23
$\mathcal{Z}(A)$	the center of the algebra A, page 53
$\mathrm{zd}(R)$	the set of zero-divisors of a ring R, page 33

Index

Curriculum Vitae

Personal Data

name	Klaas-Tido Rühl
mother	Jovanka Rühl, born Milosavljevic
father	Hans-Georg Rühl
date of birth	May 2, 1979
place of birth	Essen, Germany
citizenship	German

School Education

08/1985 - 07/1989	elementary school: St. Michael Grundschule, Wachtendonk, Germany
08/1989 - 05/1998	high school: Liebfrauenschule Mülhausen, Grefrath, Germany
05/1998	Reifeprüfung (”Abitur”)

Civilian Service

07/1998 - 10/1998	training as a state-licensed paramedic
10/1998 - 07/1999	ambulance driver for the Malteser Hilfsdienst, Kempen, Germany

University Education

10/1999 - 03/2005	**Georg-August-Universität Göttingen**, Germany studies in mathematics (minor: computer studies), **degree received: Diplom-Mathematiker**, title of diploma thesis: “Generic Splitting of Quadratic Forms”, grade point average: 1.1 (scaled between 1.0 best and 6.0 worst)
08/2005 - 05/2006	**University of California Berkeley**, USA graduate studies in mathematics, through the Education Abroad Program (see below), grade point average: 4.0

03/2008 - 06/2008 **Universiteit Leiden**, Netherlands
3 months research stay (in the context of the GTEM network)

09/2008 - 10/2008 **Université Bordeaux 1**, France
5 weeks research stay (in the context of the GTEM network)

12/2008 **Université Pierre et Marie Curie (Paris 6)**, France
2 weeks research stay (in the context of the GTEM network)

08/2009 **Université Pierre et Marie Curie (Paris 6)**, France
2 weeks research stay (in the context of the GTEM network)

09/2006 - 07/2010 **École Polytechnique Fédérale de Lausanne**, Switzerland
Ph.D. studies in mathematics,
thesis title: "Annihilating Polynomials for Quadratic Forms",
date of the Ph.D. oral exam: March 26, 2010,
date of the public defence: April 30, 2010

Scholarships

08/2005 - 05/2006 **Education Abroad Program** of the University of California:
full scholarship for the purpose of spending an academic year at UC Berkeley

08/2007 - 07/2010 **Marie Curie Fellow** of the European Union:
Early Stage Researcher for the Lausanne node of the GTEM (Galois Theory and Explicit Methods) Research and Training Network, financed by the Marie Curie Actions program

Publications

2008 **Annihilating polynomials of excellent quadratic forms**,
Archiv der Mathematik, Vol. 9, No. 3, 2008

08/2008 **Annihilating ideals of quadratic forms over local and global fields**,
to appear in *International Journal of Number Theory*

Professional Experience

10/2000 - 03/2002 **Prof. Schumann GmbH**, Göttingen, Germany
programmer in Java, developing and maintaining a credit risk management software

04/2002 - 09/2002 **Georg-August Universität Göttingen**, Germany
teaching assistant for the course "Discrete mathematics" held by Prof. Ina Kersten

10/2002 - 03/2003	**Georg-August Universität Göttingen**, Germany co-authoring and typing the script for the course “Functional analysis” held by Adj. Prof. Margit Rösler in the winter semester 01/02
04/2003 - 09/2003	**Georg-August Universität Göttingen**, Germany teaching assistant for the course “Cryptography” held by Prof. Ina Kersten
10/2003 - 03/2004	**Georg-August Universität Göttingen**, Germany teaching assistant for the course “Mathematics for biologists and geologists” held by Prof. Ina Kersten
04/2005 - 07/2005	**Georg-August Universität Göttingen**, Germany teaching assistant for the course “Number theory” held by Prof. Samuel J. Patterson
09/2006 - 07/2010	**École Polytechnique Fédérale de Lausanne**, Switzerland assistant to Prof. Eva Bayer-Fluckiger, Chaire de structures algébriques et géométriques, Institut de Mathématiques B

Languages

German	mother tongue
English	fluent speaking and writing skills
French	proficient speaking and writing skills
Spanish	basic speaking and reading skills
Latin	basic reading skills