J. Austral. Math. Soc. (*Series A*) **52** (1992), 154–174

CONJUGATE POLYNOMIALS OVER QUADRATIC ALGEBRAS

TIMOTHY STOKES

(Received 2 November 1989)

Communicated by T. E. Hall

Abstract

This paper gives variants of results from classical algebraic geometry and commutative algebra for quadratic algebras with conjugation. Quadratic algebras are essentially two-dimensional algebras with identity over commutative rings with identity, on which a natural operation of conjugation may be defined. We define the ring of conjugate polynomials over a quadratic algebra, and define c-varieties. In certain cases a close correspondence between standard varieties and c-varieties is demonstrated, and we establish a correspondence between conjugate and standard polynomials, which leads to variants of the Hilbert Nullstellensatz if the commutative ring is an algebraically closed field. These results may be applied to automated Euclidean geometry theorem proving.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*) primary 17 A 45; secondary 16 A 28, 13 F 20.

1. Introduction

The connection between the complex numbers $\mathbb{C}$ (with conjugation) and the orthogonal transformations of $\mathbb{R}^2$ is well known. Indeed, the product of two complex numbers has a geometrical interpretation in terms of the two Argand plane vectors in $\mathbb{R}^2$ corresponding to those two complex numbers.

This generalises to $\mathbb{F}^2$ where $\mathbb{F}$ is an arbitrary field. In particular, $\mathbb{F}(i) = \{a + bi | a, b \in \mathbb{F},\ i^2 = -1\}$ is a two-dimensional associative algebra over $\mathbb{F}$ (the "complexification" of $\mathbb{F}$). Choosing $\{1, i\}$ as an orthonormal basis of the $\mathbb{F}$-vector space $\mathbb{F}(i)$, we may define a symmetric bilinear product for

elements $\alpha = a+bi$, $\beta = c+di$ in $\mathbb{F}(i)$: $\alpha \cdot \beta = (a+bi)\cdot(c+di) = ac+bd$, which, when $\mathbb{F} = \mathbb{R}$, is the usual dot product of vectors in the Euclidean plane. Furthermore, $\alpha \times \beta = (a+bi)\times(c+di) = ad-bc$ is an antisymmetric product. However, defining conjugation on $\mathbb{F}(i)$ as for $\mathbb{C} = \mathbb{R}(i)$, we have, using the algebra product on $\mathbb{F}(i)$, $\overline{\alpha}\overline{\beta} = \overline{(a+bi)}(c+di) = (a-bi)(c+di) = ac+bd+i(ad-bc)$, so that $\alpha \cdot \beta = \frac{1}{2}(\overline{\alpha}\beta + \alpha\overline{\beta})$, $\alpha \times \beta = \frac{-1}{2}i(\overline{\alpha}\beta - \alpha\overline{\beta})$. Consequently, geometrical relations in the plane $\mathbb{F}^2$ may be represented using a formalism based on the ring with involution $\mathbb{F}(i)$.

We generalise further by considering quadratic algebras over commutative rings with identity, as defined in Bourbaki [1]. These are essentially two-dimensional associative algebras with identity over a commutative ring with identity. Again, a natural conjugation operation may be defined and viewed as an additional unary operation. If the commutative ring is an algebraically closed field, then there is only one quadratic algebra with conjugation up to isomorphism over that field.

We formally define the ring of "conjugate polynomials" associated with a fixed quadratic algebra R, and, in the case where R is a quadratic algebra over a field, define "c-varieties" and "c-ideals". Using the earlier results concerning quadratic algebras over commutative rings, we exhibit a close correspondence with standard elementary algebraic geometry as in Zariski and Samuel [4]. In particular, we prove variants of the Hilbert Nullstellensatz. These variants permit the development of techniques for the automation of plane metric geometry theorems in which the basic entities are plane vectors, analogous to methods which utilise coordinatizations of the plane in which the basic entities are the coordinates of points, such as those occurring in Chou and Schelter [3]. It follows from results in this paper that the scope of these two approaches is essentially the same.

Throughout what follows, all rings are commutative with identity and all fields are assumed to have characteristic other than 2.

2. Rings with involution and conjugate polynomials

DEFINITION 2.1. A *ring with involution*, R, is a commutative ring with identity 1 together with a unary operation of involution $\bar{}$ satisfying, for all $r, s \in R$, $\bar{\bar{r}} = r$, $\overline{r+s} = \bar{r}+\bar{s}$, $\overline{rs} = \overline{r}\,\overline{s}$ and $\bar{1} = 1$.

We note that this is narrower than the usual definition of a ring with involution. The class of rings with involution as defined above may be viewed as being a variety (in the sense of universal algebra) in which the algebras have two nullary operations (0 and 1), two unary operations ($-$ and $\bar{}$) and two binary operations ($+$ and $\cdot$). Every ring K may be considered a ring

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

with involution in which $\overline{a} = a$ for all $a \in K$.

DEFINITIONS 2.2, 2.3. Let R be a ring with involution. Then I is a *c-ideal* of R if I is an ideal of R for which $a \in I$ implies $\overline{a} \in I$. Let S be a subset of R. The *c-ideal generated by* S is the smallest c-ideal containing S, and is denoted by $\langle S \rangle$.

The ideal generated by S will be denoted by (S). (Clearly if $\overline{a} = a$ for all $a \in R$, then c-ideals and ideals of R coincide.) It is easy to see that if $S = \{s_1, s_2, \ldots, s_r\}$ is a finite subset of a ring with involution R, then

$$\left\{ \sum_{k=1}^{r} a_k s_k + \sum_{k=1}^{r} b_k \overline{s}_k | a_k, b_k \in R, s_k \in S, k = 1, 2, \ldots, r \right\} \subseteq \langle S \rangle .$$

Moreover, the set on the left is easily verified to be a c-ideal containing S (remembering that R has an identity), and is therefore equal to $\langle S \rangle$. For such finite S, we will often denote $\langle S \rangle$ by $\langle s_1, s_2, \ldots, s_r \rangle$.

For c-ideals I_1 and I_2 of R, the ideal-theoretic product $I_1 I_2$ and intersection $I_1 \cap I_2$ are in fact c-ideals, as is easily checked.

The following result links c-ideals with homomorphisms of rings with involution and is a special case of a more general result concerning rings with involution which are not necessarily commutative or possessing an identity.

THEOREM 2.4. *Let R be a ring with involution, I an ideal of R. Then I is a c-ideal if and only if R/I is a ring with involution, with involution defined by $\overline{a + I} = \overline{a} + I$ for all $a \in R$.*

PROOF. If I is a c-ideal of R, then for $a, b \in R$ such that $a \equiv b \pmod{I}$, we have $a - b \in I$, and so $\overline{a - b} \in I$. Thus $\overline{a} - \overline{b} \in I$ (as $\overline{-a} = -\overline{a}$) and so $\overline{a} \equiv \overline{b} \pmod{I}$. Of course, I is an ideal, so that I defines a ring congruence.

Conversely, suppose R/I is a ring with involution. Then $\overline{a + I} = \overline{a} + I$ is well defined. If $r \in I$, then $\overline{a} + I = \overline{a + I} = \overline{a + (r + I)} = \overline{(a + r)} + I$, so $\overline{a + r} - \overline{a} = (\overline{a} + \overline{r}) - \overline{a} = \overline{r} \in I$. Thus I is a c-ideal.

DEFINITIONS 2.5, 2.6, 2.7. Let R be a ring with involution. A *c-prime* c-ideal P of R is a c-ideal such that, for any $r_1, r_2 \in R$, if $r_1 r_2$ and $\overline{r}_1 r_2$ are in P then at least one of r_1 and r_2 is in P. An ideal I of R is said to be *radical* if, for all $r \in R$, $r \in I$ whenever there is a positive integer ρ such that $r^\rho \in I$. The *radical* of an ideal I of R is the smallest radical ideal containing I, and is equal to $\mathscr{R}(I) = \{a \in R | \exists \rho > 0, a^\rho \in I\}$.

If $\overline{a} = a$ for all $a \in R$, then the c-prime c-ideals of R are exactly its prime ideals (see Zariski and Samuel [4]). The definition of $\mathscr{R}(I)$ is the usual one for commutative rings (see [4] for example).

THEOREM 2.8. *Let R be a ring with involution, I a c-ideal of R. Then $\mathscr{R}(I)$ is a c-ideal of R. If I is c-prime, then $\mathscr{R}(I) = I$.*

PROOF. If I is a c-ideal of R with $a \in \mathscr{R}(I)$, then $a^\rho \in I$ for some $\rho > 0$. Hence $(\overline{a})^\rho = \overline{a^\rho} \in I$, so that $\overline{a} \in \mathscr{R}(I)$, and so $\mathscr{R}(I)$ is a c-ideal.

Let I be a c-prime c-ideal of R, $c \in R$. If $c^\rho \in I$ for some $\rho > 0$, then $c^\rho \cdot \overline{c}^\rho = (c\overline{c})^\rho \in I$. Hence $(c\overline{c})^{\rho-1}(c\overline{c})$ and $(c\overline{c})^{\rho-1}(\overline{c\overline{c}}) = (c\overline{c})^{\rho-1}(c\overline{c})$ are in I, so that either $(c\overline{c})^{\rho-1}$ or $c\overline{c}$ is in I. It follows by induction that $c\overline{c} \in I$, whence $c^{\rho-1} \cdot c \in I$ and $c^{\rho-1}\overline{c} = c^{\rho-2}(c\overline{c})$ are in I. Hence $c^{\rho-1}$ or c is in I. Again, induction yields $c \in I$, so I is radical.

DEFINITION 2.9. For a ring with involution R,

$$s(R) = \{r | \overline{r} = r, r \in R\}$$

is the set of *symmetric elements* of R.

It is easy to verify that the set of symmetric elements of a ring with involution R is always a subring of R.

DEFINITIONS 2.10, 2.11, 2.12, 2.13. We define the *conjugate polynomial ring of order* (n, m) over the ring with involution R,

$$R[x_1, x_2, \ldots, x_n; w_1, w_2, \ldots, w_m] = R[x^{(n)}; w^{(m)}],$$

to be the ring with involution generated by R together with the *vector variables* $\{x_1, x_2, \ldots, x_n\}$ and the *scalar variables* $\{w_1, w_2, \ldots, w_m\}$, subject to $\overline{w}_k = w_k$, $k = 1, 2, \ldots, m$, and otherwise free. The elements of $R[x^{(n)}; w^{(m)}]$ are *c-polynomials*. (If $m = 0$, then we abbreviate to $R[x^{(n)}]$, and if $n = 0$, to $R[w^{(m)}]$.)

That the conjugate polynomial ring exists uniquely and is a ring with involution, for any choice of n and m and for any ring with involution R, is easily seen; it may be constructed analogously to the way in which a multivariate polynomial ring over a ring is constructed. We note that R is embedded in $R[x^{(n)}; w^{(m)}]$. A typical element of $R[x^{(n)}; w^{(m)}]$ is denoted by

$$f(x_1, x_2, \ldots, x_n, w_1, w_2, \ldots, w_m)$$

or, more briefly, $f(x^{(n)}, w^{(m)})$.

The definition of the conjugate polynomial ring over a ring with involution in a sense generalises that of the polynomial ring over a ring: let $n = 0$ and let R be such that $s(R) = R$; then, as a ring, $R[w^{(m)}]$ is isomorphic to the polynomial ring in m indeterminates over R, and $s(R[w^{(m)}]) = R[w^{(m)}]$. However, if R is such that $s(R) \neq R$, then $R[w^{(m)}]$ is not to be confused with the polynomial ring in m indeterminates over the ring R, because the

conjugation operation can still act non-trivially on elements of R and hence on c-polynomials in $R[w^{(m)}]$.

Occasionally, characters other than x_j or w_j will be employed to denote variables, but it will always be the case that underlined variables denote vector variables and those not underlined denote vector variables.

For the remainder of this section, let L be a ring with involution such that R is a subring of L closed under involution. For every $f \in R[x^{(n)}; w^{(m)}]$ there is a natural action on elements of $L^n \times s(L)^m$: for

$$\underline{a} = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m)$$

in $L^n \times s(L)^m$, replace x_j by a_j $(j = 1, 2, \ldots, n)$ and w_j by b_j $(j = 1, 2, \ldots, m)$ in $f(x^{(n)}, w^{(m)})$, thereby yielding in the obvious way an element of L, denoted by $f(\underline{a})$. In this way, we associate with every $f \in R[x^{(n)}; w^{(m)}]$ a polynomial function $f: L^n \times s(L)^m \to L$.

For example, if $L = \mathbb{C}$ with the usual conjugation, then $s(L) = \mathbb{R}$; let $R = \mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$. We let $f(x_1, x_2, w_1) = \frac{1}{2}w_1x_1^2 - 3ix_1\overline{x_2} + 4\overline{x_2}^3$, an element of $R[x^{(2)}; w^{(1)}]$; then

$$f(1 + i, i, \tfrac{2}{3}) = \tfrac{1}{3}(1 + i)^2 - 3i(1 + i)(-i) + 4(-i)^3 = -3 + \tfrac{5}{3}i.$$

DEFINITION 2.14, 2.15. Given $F \subseteq R[x^{(n)}; w^{(m)}]$, we define

$$\mathscr{V}_{n,m}(F) = \{\underline{a} \in L^n \times s(L)^m | f(\underline{a}) = 0 \text{ for all } f \in F\},$$

the *c-variety corresponding to* F. Given $S \subseteq L^n \times s(L)^m$, we define

$$\mathscr{I}_{n,m}(S) = \{f \in R[x^{(n)}; w^{(m)}] | f(\underline{a}) = 0 \text{ for all } \underline{a} \in S\},$$

the *c-ideal corresponding to* S.

It is easy to verify that $\mathscr{I}_{n,m}(S)$ is in fact a c-ideal in $R[x^{(n)}; w^{(m)}]$, for each $S \subseteq L^n \times s(L)^m$.

3. Quadratic algebras and c-ideals

Throughout the remainder of the paper, K will be a fixed ring and $\mathbb{F}$ will be a fixed field.

The following family of rings with involution will feature in what follows. The definition is essentially that found in Bourbaki [1].

DEFINITION 3.1. Let $\alpha, \beta \in K$. The *quadratic algebra of type* (α, β) *over* K is the free module of dimension 2 over K, with distinguished basis $\{1, i\}$, on which is defined a distributive product $\cdot$ (sometimes denoted by

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

juxtaposition) for which $1 \cdot 1 = 1$, $1 \cdot i = i \cdot 1 = i$ and $i \cdot i = \alpha 1 + \beta i$; it is denoted by $Q_{(\alpha,\beta)}(K)$.

Clearly the basis element 1 is an identity for the algebra $Q_{(\alpha,\beta)}(K)$. For $a \in K$, we blur the distinction between a and $a1 \in Q_{(\alpha,\beta)}(K)$, thereby viewing K as being embedded in $Q_{(\alpha,\beta)}(K)$ in the obvious fashion.

The most familiar examples of quadratic algebras are those in which $\alpha = -1$ (the additive inverse of the identity in K) and $\beta = 0$, such as $Q_{(-1,0)}(\mathbb{Z}) \cong \mathbb{Z}(i)$, the Gaussian integers, and $Q_{(-1,0)}(\mathbb{R}) \cong \mathbb{C}$, the complex numbers. Another familiar example is

$$Q_{(n,0)}(\mathbb{Q}) \cong \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} | a, b \in \mathbb{Q}\},$$

where $\mathbb{Q}$ is the rational field and $n \in \mathbb{Z}$. Indeed any quadratic extension of $\mathbb{Q}$ may be viewed as a quadratic algebra over $\mathbb{Q}$ in like manner.

The following facts concerning $Q_{(\alpha,\beta)}(K)$ appear in Bourbaki [1].

PROPOSITION 3.2. (1) *Every K-algebra admitting a basis of two elements is isomorphic to $Q_{(\alpha,\beta)}(K)$ for some $\alpha, \beta \in K$.*

(2) *$Q_{(\alpha,\beta)}(K)$ is associative and commutative.*

(3) *The mapping $\bar{}: Q_{(\alpha,\beta)}(K) \to Q_{(\alpha,\beta)}(K)$ defined by*

$$\overline{a + bi} = (a + \beta b) - bi$$

for all $a, b \in K$, is an involution, and is uniquely determined by the structure of $Q_{(\alpha,\beta)}(K)$ as an algebra.

(4) *The mapping $N: Q_{(\alpha,\beta)}(K) \to K$ defined by*

$$N(a + bi) = (a + bi)\overline{(a + bi)} = a^2 + \beta ab - \alpha b^2$$

is a quadratic form, and $c \in Q_{(\alpha,\beta)}(K)$ is invertible in $Q_{(\alpha,\beta)}(K)$ if and only if $N(c)$ is invertible in K.

(5) *If $\mathbb{F}$ is a field containing no element γ such that $\gamma^2 = \alpha + \beta\gamma$, then $Q_{(\alpha,\beta)}(\mathbb{F})$ is a field.*

(6) *Suppose K contains an element γ such that $\gamma^2 = \alpha + \beta\gamma$. If $\beta - 2\gamma$ is zero, then $Q_{(\alpha,\beta)}(K) \cong Q_{(0,0)}(K)$. If $\beta - 2\gamma$ is invertible, then*

$$Q_{(\alpha,\beta)}(K) \cong Q_{(0,1)}(K) \cong K \times K,$$

with the associated involution on $K \times K$ given by $\overline{(a, b)} = (b, a)$ for all $a, b \in K$, and the second isomorphism defined by $a + bi \mapsto (a, a + b)$. In each case the isomorphism respects involution.

DEFINITIONS 3.3, 3.4, 3.5, 3.6. The involution of Proposition 3.2.3 above is called *conjugation*; $\bar{c}$ is the *conjugate of* c for any $c \in Q_{(\alpha,\beta)}(K)$. If

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

$\beta^2 + 4\alpha$ is invertible in K, then $Q_{(\alpha,\beta)}(K)$ is *non-singular*; otherwise it is *singular*.

From now on, $Q_{(\alpha,\beta)}(K)$ will refer to the ring with involution consisting of the quadratic algebra of type (α, β) together with involution given by conjugation as above. Clearly, $s(Q_{(\alpha,\beta)}(K)) = K$.

Returning to the examples after Definition 3.1, we see that the induced conjugations on $\mathbb{Z}(i) \cong Q_{(-1,0)}(\mathbb{Z})$ and $\mathbb{C} \cong Q_{(-1,0)}(\mathbb{R})$ are the usual ones. For $a + b\sqrt{n}$ in $\mathbb{Q}(\sqrt{n})$, $\overline{a + b\sqrt{n}} = a - b\sqrt{n}$.

Examples of non-singular quadratic algebras are easily obtained and include $\mathbb{Q}(\sqrt{n})$ where the positive integer n is not a perfect square. Each of these is a field by Proposition 3.2.5, as is $Q_{(-1,0)}(\mathbb{R})$. However, by Proposition 3.2.6, $Q_{(-1,0)}(\mathbb{C})$ is not a field. Indeed we may generalise this. Writing $\mathbb{F}(i) = Q_{(-1,0)}(\mathbb{F})$, it follows from Proposition 3.2.5 and 3.2.6 that $\mathbb{F}(i)$ is a field if and only if there is no $a \in \mathbb{F}$ such that $a^2 = -1$. Hence in particular we may employ the following result appearing in Burn [2]: if p is an odd prime, then p is congruent to 1 (modulo 4) if and only if there exists $a \in \mathbb{Z}$ such that p divides $a^2 + 1$. Thus for an odd prime p, $\mathbb{Z}_p(i)$ is a field if and only if p is not congruent to 1 (modulo 4). The singular algebra $Q_{(0,0)}(\mathbb{R})$ is, as an algebra, the exterior algebra of order 1 over $\mathbb{R}$.

LEMMA 3.7. *Let $Q_{(\alpha,\beta)}(K)$ be non-singular. If $c = a + bi \in Q_{(\alpha,\beta)}(K)$ with $a, b \in K$, then $2i - \beta$ is invertible, and*

$$a = (2i - \beta)^{-1}((i - \beta)c + i\bar{c}),\ b = (2i - \beta)^{-1}(c - \bar{c}).$$

PROOF. Now $2i - \beta$ is invertible if and only if $N(2i - \beta)$ is invertible, by Proposition 3.2.4; and $N(2i - \beta) = -(\beta^2 + 4\alpha)$ which is by assumption invertible in K.

If $c = a + bi$, then $\bar{c} = a + \beta b - bi$ by Proposition 3.2.3, so $c - \bar{c} = 2bi - \beta b = (2i - \beta)b$. Thus if $2i - \beta$ is invertible, $b = (2i - \beta)^{-1}(c - \bar{c})$. Similarly $c + \bar{c} = 2a + \beta b$, so $a = \frac{1}{2}[c + \bar{c} - \beta b]$, that is,

$$a = \tfrac{1}{2}(2i - \beta)^{-1}[(2i - \beta)(c + \bar{c}) - \beta(c - \bar{c})] = (2i - \beta)^{-1}[(i - \beta)c + i\bar{c}].$$

DEFINITIONS 3.8, 3.9. For a subset T of $Q_{(\alpha,\beta)}(K)$, $\mathrm{crd}(T)$, is the set

$$\{a \in K | \exists b \in K,\ a + bi \in T \text{ or } b + ai \in T\}.$$

For $S \subseteq K$, we define $S(i) = \{a + bi | a, b \in S\}$. We define $\mathrm{crd}_j(a_1 + a_2 \cdot i) = a_j$ for all $a_j \in K$, $j = 1, 2$.

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

Clearly, for $T \subseteq Q_{(\alpha,\beta)}(K)$, we have

$$\operatorname{crd}(T) = \bigcup_{a \in T} \{\operatorname{crd}_1(a), \operatorname{crd}_2(a)\}.$$

THEOREM 3.10. *Let $S \subseteq K$. Then, in $Q_{(\alpha,\beta)}(K)$, $\langle S\rangle = (S)(i)$. Conversely, suppose $Q_{(\alpha,\beta)}(K)$ is non-singular and $T \subseteq Q_{(\alpha,\beta)}(K)$. Then $\langle T\rangle = (\operatorname{crd}(T))(i) = \langle \operatorname{crd}(T)\rangle$.*

PROOF. If $S \subseteq K$, then $s \in \langle S\rangle$ in $Q_{(\alpha,\beta)}(K)$ if and only if there are $r_1, r_2, \ldots, r_k$ in $Q_{(\alpha,\beta)}(K)$ such that

$$s = \sum_{j=1}^{k} r_j s_j \text{ for } \{s_1, s_2, \ldots, s_k\} \subseteq S$$

since $\bar{s}_j = s_j$ for $j = 1, 2, \ldots, k$, which happens if and only if there are $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ in K such that $r_j = a_j + b_j i$ for $j = 1, 2, \ldots, k$, and such that we have

$$s = \sum_{j=1}^{k} (a_j + b_j i) s_j \sum_{j=1}^{k} a_j s_j + i \cdot \sum_{j=1}^{k} b_j s_j.$$

Hence $s \in \langle S\rangle$ if and only if $s \in (S)(i)$.

Now suppose $Q_{(\alpha,\beta)}(K)$ is non-singular and $T \subseteq Q_{(\alpha,\beta)}(K)$. Then by Lemma 3.7, if $a + bi \in T$, with $a, b \in K$, then $a, b \in \langle T\rangle$. Thus $\operatorname{crd}(T) \subseteq \langle T\rangle$ and so $\langle \operatorname{crd}(T)\rangle \subseteq \langle T\rangle$. Further, if $t = a + bi$ is in T with $a, b \in K$, then $a, b \in \operatorname{crd}(T)$, and so $t \in \langle \operatorname{crd}(T)\rangle$, so that $\langle T\rangle \subseteq \langle \operatorname{crd}(T)\rangle$. Hence $\langle T\rangle = \langle \operatorname{crd}(T)\rangle$, and $\langle T\rangle = (\operatorname{crd}(T))(i)$ by the first part of the proof.

We note that $Q_{(-1,0)}(\mathbb{Z}) \cong \mathbb{Z}(i)$, the Gaussian integers with conjugation, is an example of a quadratic algebra in which there are subsets T for which the c-ideal generated by T does not equal the c-ideal generated by $\operatorname{crd}(T)$. For instance, we have $\mathbb{Z}(i) = \langle 1\rangle \neq \langle 1 + i\rangle$. Now -4 has no inverse in $\mathbb{Z}$, so that $\mathbb{Z}(i)$ is singular. Hence the converse of the above theorem does not apply to singular $Q_{(\alpha,\beta)}(K)$.

COROLLARY 3.11. *Let $Q_{(\alpha,\beta)}(K)$ be non-singular. If J is a c-ideal of $Q_{(\alpha,\beta)}(K)$, then $\operatorname{crd}(J) = J \cap K$.*

PROOF. By Theorem 3.10, $\operatorname{crd}(J) \subseteq J \cap K$. Conversely, any $c \in J \cap K$ is by definition in $\operatorname{crd}(J)$.

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

THEOREM 3.12. *Let J_1 be the lattice of ideals of K and J_2 the lattice of c-ideals of $Q_{(\alpha,\beta)}(K)$ (both lattices ordered by inclusion). Then the map $\theta: J_1 \to J_2$, defined by $\theta(I) = I(i)$ for all $I \in J_1$, is an injective homomorphism. If $Q_{(\alpha,\beta)}(K)$ is non-singular, then θ is an isomorphism with inverse $\theta^{-1}: J_2 \to J_1$ defined by $\theta^{-1}(J) = \mathrm{crd}(J)$ for all $J \in J_2$.*

PROOF. Let I be an ideal of K. Then $\langle I\rangle = (I)(i) = I(i)$ by Theorem 3.10, so that we may define $\theta: J_1 \to J_2$ such that $\theta(I) = I(i)$ for all $I \in J_1$. Then θ is clearly order preserving, and so is a homomorphism of partially ordered sets. Indeed it is injective, since if I and J are non-equal ideals of K, then $I(i) \neq J(i)$.

Suppose now that $Q_{(\alpha,\beta)}(K)$ is non-singular. If J is a c-ideal of $K(i)$ then $J = \langle \mathrm{crd}(J)\rangle = (\mathrm{crd}(J))(i)$ by Theorem 3.10. We show $\mathrm{crd}(J)$ is an ideal of K. By Corollary 3.11, $\mathrm{crd}(J) = J \cap K$. Hence, if $a, b \in \mathrm{crd}(J) \subseteq J$, then $a - b \in J \cap K = \mathrm{crd}(J)$, and if $r \in K$, then $ra \in J \cap K$, so that $\mathrm{crd}(J)$ is indeed an ideal of K. Hence $J = \mathrm{crd}(J)(i) = \theta(\mathrm{crd}(J))$. Thus θ as above is surjective, and so is an isomorphism, with inverse $\theta^{-1}: J_2 \to J_1$ defined by $\theta(J) = \mathrm{crd}(J)$ for all $J \in J_2$.

If the c-ideal $\langle 1 + i\rangle$ of $\mathbb{Z}(i)$ were equal to $I(i)$ for any ideal I of K, then

$$1 \in \mathrm{crd}(\langle 1 + i\rangle) = \mathrm{crd}(I(i)) = I,$$

so that $\langle 1 + i\rangle = \langle 1\rangle = \mathbb{Z}(i)$, a contradiction.

THEOREM 3.13. *The ideal I of K is prime if $I(i)$ is a c-prime c-ideal of $Q_{(\alpha,\beta)}(K)$. If $Q_{(\alpha,\beta)}(K)$ is non-singular, then the converse holds, namely that J is a c-prime c-ideal of $Q_{(\alpha,\beta)}(K)$ if $\mathrm{crd}(J)$ is a prime ideal of K.*

PROOF. Suppose that I is an ideal of K and that $I(i)$ is c-prime. If $ab \in I$ for some $a, b \in K$ then $ab \in I(i)$ also, so ab and $\bar{a}b = ab$ are in $I(i)$. Thus a or b is in $I(i) \cap K = I$, so I is prime.

Conversely, suppose $Q_{(\alpha,\beta)}(K)$ is non-singular. If J is a c-ideal of $Q_{(\alpha,\beta)}(K)$, then $J = I(i)$ for some ideal $I = \mathrm{crd}(J)$ of K, by Theorem 3.12. Suppose I is a prime ideal of K, and that c_1c_2 and $c_1\bar{c}_2$ are in $I(i)$ for some $c_1, c_2 \in Q_{(\alpha,\beta)}(K)$, with $c_1 = a_1 + b_1 i$, $c_2 = a_2 + b_2 i$, for $a_1, b_1, a_2, b_2 \in K$. By Lemma 3.7, $2i - \beta$ is invertible. Hence

$$\begin{aligned} b_1b_2 &= (2i - \beta)^{-1}(c_1 - \bar{c}_1) \cdot (2i - \beta)^{-1}(c_2 - \bar{c}_2) \\ &= (2i - \beta)^{-2}(c_1c_2 - c_1\bar{c}_2 - \bar{c}_1c_2 + \overline{c_1c_2}) \in I(i) \cap K = I, \end{aligned}$$

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

so b_1 or b_2 is in I, by the primeness of I. But $c_1c_2 = (a_1 + b_1i)(a_2 + b_2i)$ is in $I(i)$, so

$$a_1a_2 + b_1b_2\alpha,\ a_1b_2 + b_1a_2 + b_1b_2\beta \in I.$$

Since $b_1b_2 \in I$, we have $a_1a_2,\ a_1b_2 + b_1a_2 \in I$. Hence a_1 or a_2 is in I. Suppose without loss of generality that $b_1 \in I$. Then $a_1b_2 \in I$ and if $b_2 \notin I$ then $a_1 \in I$ and so $c_1 = a_1 + b_1i \in I(i)$; if $b_1, b_2 \in I$ then, since a_1 or a_2 is in I, either $c_1 = a_1 + b_1i$ or $c_2 = a_2 + b_2i$ is in $I(i)$. Hence in all cases, either c_1 or c_2 is in $I(i)$, which is therefore c-prime.

Now (2) is a prime ideal of $\mathbb{Z}$ and yet $(2)(i)$ is not a c-prime c-ideal of $\mathbb{Z}(i)$: $(1 + i)^2 = 2i$ and $(1 + i)(\overline{1 + i}) = 2$ are both in $(2)(i)$, yet $1 + i$ is not. Hence if $Q_{(\alpha,\beta)}(K)$ is singular, it need not be the case that $I(i)$ is a c-prime c-ideal of $Q_{(\alpha,\beta)}(K)$ whenever I is a prime ideal of K.

THEOREM 3.14. *The ideal I of K is radical if $I(i)$ is a radical c-ideal of $Q_{(\alpha,\beta)}(K)$. If $Q_{(\alpha,\beta)}(K)$ is non-singular, then the converse holds, namely that J is a radical c-ideal of $Q_{(\alpha,\beta)}(K)$ if $\mathrm{crd}(J)$ is a radical ideal of K.*

PROOF. Let I be an ideal of K with $I(i)$ a radical c-ideal of K, $a \in K$. If $a^\rho \in I$ for some $\rho > 0$, then $a^\rho \in I(i)$. Thus $a \in I(i)$ and so $a \in I(i) \cap K = I$, whence I is radical.

Conversely, suppose $Q_{(\alpha,\beta)}(K)$ is non-singular. By Theorem 3.12, if J is a c-ideal of $Q_{(\alpha,\beta)}(K)$, then $J = I(i)$ for some ideal $I = \mathrm{crd}(J)$ of K. Suppose I is a radical ideal of K. If $c = a + bi \in Q_{(\alpha,\beta)}(K)$ where $a, b \in K$, then, by Lemma 3.7, $b = (2i - \beta)^{-1}(c - \bar{c})$. If $c^\rho = (a + bi)^\rho \in I(i)$, then $c^\rho\bar{c}^\rho = (c\bar{c})^\rho \in I(i)$. But $c\bar{c} = a^2 + \beta ab - \alpha b^2 \in K$, so $(c\bar{c})^\rho \in K \cap I(i) = I$. Thus $c\bar{c} \in I$, since I is radical. Further, $\bar{c}^\rho = \overline{c^\rho} \in I(i)$. Hence

$$b^\rho = ((2i - \beta)^{-1}(c - \bar{c}))^\rho \in I(i) \cap K = I,$$

so $b \in I$, since I is radical. But $a^2 + \beta ab - \alpha b^2 \in I$, so $a^2 \in I$ and hence $a \in I$, again since I is radical. Thus $c = a + bi \in I(i)$, so $I(i)$ is a radical c-ideal of $Q_{(\alpha,\beta)}(K)$.

The c-ideal $(2)(i)$ of $\mathbb{Z}(i)$ is not radical, since $(1 + i)^2 \in (2)(i)$, yet $1 + i \notin (2)(i)$. However, (2) is a prime ideal of K and hence radical, again showing that not even an appropriately weakened converse of Theorem 3.13 holds in case $Q_{(\alpha,\beta)}(K)$ is singular.

COROLLARY 3.15. *Every c-prime c-ideal of $Q_{(\alpha,\beta)}(K)$ is radical.*

This readily follows in the non-singular case as a consequence of Theorems 3.12, 3.13 and 3.14, and the fact that every prime ideal of K is radical (see

Zariski and Samuel [4]). We have already given a direct proof (Theorem 2.8) which holds for all rings with involution R and hence does not require $Q_{(\alpha,\beta)}(K)$ to be non-singular.

COROLLARY 3.16. *Let $Q_{(\alpha,\beta)}(K)$ be non-singular, I an ideal of K. Then $\mathscr{R}(I) = \operatorname{crd}(\mathscr{R}(I(i)))$.*

PROOF. Let $J = \operatorname{crd}(\mathscr{R}(I(i)))$. Then J is an ideal of K by Theorem 3.12 and is radical by Theorem 3.14. Then $I(i) \subseteq \mathscr{R}(I(i)) = J(i)$ by Theorem 3.12, so $I \subseteq J$ and hence $\mathscr{R}(I) \subseteq J$.

If $j \in J$, then $j \in J(i) = \mathscr{R}(I(i))$, so there is $\rho > 0$ such that $j^\rho \in I(i)$. But $j^\rho \in K$, so that $j^\rho \in I(i) \cap K = I$, and hence $j \in \mathscr{R}(I)$. Thus $J \subseteq \mathscr{R}(I)$, and so $J = \mathscr{R}(I)$.

LEMMA 3.17.

$$Q_{(\alpha,\beta)}(K)[w^{(m)}] \cong Q_{(\alpha,\beta)}(K[w^{(m)}]).$$

Moreover, $Q_{(\alpha,\beta)}(K[w^{(m)}])$ is non-singular if and only if $Q_{(\alpha,\beta)}(K)$ is non-singular.

PROOF. The isomorphism is clear. Now $Q_{(\alpha,\beta)}(K)$ is non-singular if and only if $\beta^2+4\alpha$ is invertible in K, which is if and only if $\beta^2+4\alpha$ is invertible in $K[w^{(m)}]$, and this holds if and only if $Q_{(\alpha,\beta)}(K[w^{(m)}])$ is non-singular.

4. C-polynomials and c-varieties for $Q_{(\alpha,\beta)}(\mathbb{F})$

Throughout the remainder of the article, k will be a subfield of $\mathbb{F}$ containing α and β, and $K = k(i) \cong Q_{(\alpha,\beta)}(k)$ will denote the corresponding sub-quadratic algebra of $Q_{(\alpha,\beta)}(\mathbb{F})$.

We employ some additional abbreviations: we let

$$f((y, z)^{(n)}, w^{(m)}) = f(y_1, z_1, y_2, z_2, \ldots, y_n, z_n, w_1, w_2, \ldots, w_m)$$

be a c-polynomial in

$$H[(y, z)^{(n)}, w^{(m)}] = H[y_1, z_1, y_2, z_2, \ldots, y_n, z_n, w_1, w_2, \ldots, w_m],$$

where $H = k$ or K. We view $k[(y, z)^{(n)}, w^{(m)}]$ as being embedded in $K[(y, z)^{(n)}, w^{(m)}]$ in the obvious way.

DEFINITIONS 4.1, 4.2, 4.3, 4.4. Define

$$\text{sca}: K[x^{(n)}; w^{(m)}] \to K[(y, z)^{(n)}, w^{(m)}]$$

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

by setting

$$\mathrm{sca}(f) = f(y_1 + iz_1, y_2 + iz_2, \ldots, y_n + iz_n, w_1, w_2, \ldots, w_m).$$

For $F \subseteq K[x^{(n)}; w^{(m)}]$, define $\mathrm{sca}(F) = \{\mathrm{sca}(f) | f \in F\}$. Lemma 3.17 permits us to define $\mathrm{crd}(F)$ in the obvious way for all $F \subseteq K[(y, z)^{(n)}, w^{(m)}]$; similarly we define $\mathrm{crd}_1(f)$ and $\mathrm{crd}_2(f)$ for all $f \in K[(y, z)^{(n)}, w^{(m)}]$.

DEFINITIONS 4.5, 4.6. Let $Q_{(\alpha,\beta)}(\mathbb{F})$ be non-singular. We define the map $\mathrm{vec}: K[(y, z)^{(n)}, w^{(m)}] \to K[x^{(n)}; w^{(m)}]$ by setting

$$\mathrm{vec}(g) = g[(2i - \beta)^{-1}[(x_1 + \overline{x}_1)i - \beta x_1], (2i - \beta)^{-1}(x_1 - \overline{x}_1), \ldots,$$
$$(2i - \beta)^{-1}[(x_n + \overline{x}_n)i - \beta x_n], (2i - \beta)^{-1}(x_n - \overline{x}_n), w_1, \ldots, w_m].$$

For $G \subseteq K[(y, z)^{(n)}, w^{(m)}]$, we define $\mathrm{vec}(G) = \{\mathrm{vec}(g) | g \in G\}$.

DEFINITIONS 4.7, 4.8. We define vec and crd to act on elements of $\mathbb{F}^{2n+m}$, $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$ respectively, as follows:

$$\mathrm{vec}(c_1, d_1, \ldots, c_n, d_n, b_1, \ldots, b_m)$$
$$= (c_1 + id_1, \ldots, c_n + id_n, b_1, \ldots, b_m),$$
$$\mathrm{crd}(a_1 + ib_1, \ldots, a_n + ib_n, c_1, \ldots, c_m)$$
$$= (a_1, b_1, \ldots, a_n, b_n, c_1, \ldots, c_m).$$

Clearly the meaning of vec in Definition 4.7 depends upon the choices of n and m (as well of course on the choice of basis element i of $Q_{(\alpha,\beta)}(\mathbb{F})$); knowledge of $2n + m$ alone is not sufficient. Thus we really have a different definition of vec and crd in Definitions 4.5 and 4.7 for each different pair of values for n and m.

The next two results follow immediately from Definitions 4.1 to 4.8 with the help of Lemma 3.7. The theorem that follows them spells out the correspondence between c-varieties and the varieties of standard elementary algebraic geometry.

LEMMA 4.9. *The mappings*

$$\mathrm{vec}: \mathbb{F}^{2n+m} \to [Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$$

and

$$\mathrm{crd}: [Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m \to \mathbb{F}^{2n+m}$$

are mutually inverse; in case $Q_{(\alpha,\beta)}(\mathbb{F})$ is non-singular, so are the isomorphisms

$$\mathrm{vec}: K[(y, z)^{(n)}, w^{(m)}] \to K[x^{(n)}; w^{(m)}]$$

and

$$\mathrm{sca}: K[x^{(n)}; w^{(m)}] \to K[(y, z)^{(n)}, w^{(m)}].$$

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

LEMMA 4.10. *Let* $f \in K[x^{(n)}; w^{(m)}]$, $a \in [Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$. *Then*

$$f(a) = \mathrm{crd}(f)(\mathrm{crd}(a)) = \mathrm{crd}_1(f)(\mathrm{crd}(a)) + i \cdot \mathrm{crd}_2(f)(\mathrm{crd}(a)).$$

Suppose $Q_{(\alpha,\beta)}(\mathbb{F})$ *is non-singular,*

$$g \in K[(y, z)^{(n)}, w^{(m)}], \mathscr{A} \in \mathbb{F}^{2n+m}.$$

Then $g(\mathscr{A}) = \mathrm{vec}(g)(\mathrm{vec}(\mathscr{A}))$.

THEOREM 4.11. *Let* $Q_{(\alpha,\beta)}(\mathbb{F})$ *be non-singular. The partially ordered set* L_1 *of c-varieties in* $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$ *associated with subsets of* $K[x^{(n)}; w^{(m)}]$, *ordered by inclusion, is naturally isomorphic to the partially ordered set* L_2 *of (c-)varieties in* $\mathbb{F}^{2n+m}$ *associated with subsets of* $k[(y, z)^{(n)}, w^{(m)}]$, *also ordered by inclusion. The map* $\Phi: L_1 \to L_2$ *defined by*

$$\Phi(\mathscr{V}_{n,m}(F)) = \mathrm{crd}(\mathscr{V}_{n,m}(F)) = \mathscr{V}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}F))),$$

for all $F \subseteq K[x^{(n)}; w^{(m)}]$, *is an isomorphism with inverse* $\Psi: L_2 \to L_1$ *defined by*

$$\Psi(\mathscr{V}_{0,2n+m}(G)) = \mathrm{vec}(\mathscr{V}_{0,2n+m}(G)) = \mathscr{V}_{n,m}(\mathrm{vec}(G)),$$

for all $G \subseteq k[(y, z)^{(n)}, w^{(m)}]$.

PROOF. Let $F \subseteq K[x^{(n)}; w^{(m)}]$. Now $b \in \mathrm{crd}(\mathscr{V}_{n,m}(F))$ if and only if $\mathrm{vec}(b) \in \mathscr{V}_{n,m}(F)$, which is if and only if $f(\mathrm{vec}(b)) = 0$ for all $f \in F$, which holds if and only if

$$\mathrm{crd}_1(f)(\mathrm{crd}(\mathrm{vec}(b))) = \mathrm{crd}_2(f)(\mathrm{crd}(\mathrm{vec}(b))) = 0$$

for all $f \in F$ by Lemma 4.10, and this holds if and only if $\mathrm{crd}_1(f)(\mathscr{A}) = \mathrm{crd}_2(f)(\mathscr{A}) = 0$ for all $\mathrm{crd}_1(f)$ and $\mathrm{crd}_2(f)$ in $\mathrm{crd}(F)$, which holds if and only if

$$\mathscr{A} \in \mathscr{V}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}(F))).$$

This establishes that

$$\mathscr{V}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}(F))) = \mathscr{V}_{0,2n+m}(\mathrm{sca}(F)) = \mathrm{crd}(\mathscr{V}_{n,m}(F)),$$

whence $\mathrm{crd}(\mathscr{V}_{n,m}(F))$ is a variety.

Similarly, let $G \subseteq k[(y, z)^{(n)}, w^{(m)}]$. Then

$$G = \mathrm{sca}(\mathrm{vec}(G)) = \mathrm{crd}(\mathrm{sca}(\mathrm{vec}(G))),$$

as each element of $\mathrm{vec}(G)$ is symmetric, so

$$\begin{aligned}\mathrm{vec}(\mathscr{V}_{0,2n+m}(G)) &= \mathrm{vec}(\mathscr{V}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}(\mathrm{vec}(G))))\\ &= \mathrm{vec}(\mathrm{crd}(\mathscr{V}_{n,m}(\mathrm{vec}(G))) = \mathscr{V}_{n,m}(\mathrm{vec}(G))\end{aligned}$$

by the first part.

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

Both Φ and Ψ are clearly order preserving and mutually inverse. Consequently each is an isomorphism.

Clearly, the same c-varieties are associated with both $K[(y, z)^{(n)}, w^{(m)}]$ and $k[(y, z)^{(n)}, w^{(m)}]$ – a c-polynomial f in $K[(y, z)^{(n)}, w^{(m)}]$ vanishes exactly when $\mathrm{crd}_1(f)$ and $\mathrm{crd}_2(f)$ in $k[(y, z)^{(n)}, w^{(m)}]$ vanish.

Much is known about L_2. We refer the reader to Zariski and Samuel [4]. Although the results there concerning algebraic varieties apply to cases where the "coordinate domain" is an algebraically closed field, it is easy to see that the assumption of algebraic closure is not required in the proof of many of the elementary results which will be employed in what follows. The lattice L_2 is a complete distributive lattice, in which meets and finite joins are set-theoretic intersections and unions respectively. Theorem 4.11 allows us to say exactly the same things about L_1. In fact, the isomorphism between the lattice of c-ideals of the form $\mathscr{I}_{n,m}(S)$ and the associated lattice of c-varieties, and between the lattice of (c-)ideals of the form $\mathscr{I}_{0,n}(S)$ and the associated lattice of varieties in standard algebraic geometry, yields the corollary that the two lattices of such c-ideals are isomorphic. We return to the details of this relationship shortly.

First we deal with the correspondence between polynomial ideals and c-polynomial c-ideals in general.

THEOREM 4.12. *Let $Q_{(\alpha,\beta)}(\mathbb{F})$ be non-singular. The lattice D_3 of c-ideals in $K[x^{(n)}; w^{(m)}]$ is naturally isomorphic to the lattice D_1 of (c-)ideals in $k[(y, z)^{(n)}, w^{(m)}]$, an isomorphism $\varphi: D_3 \to D_1$ defined by*

$$\varphi(\langle F\rangle) = \mathrm{crd}(\mathrm{sca}(\langle F\rangle)) = (\mathrm{crd}(\mathrm{sca}(F))) \text{ for all } F \in K[x^{(n)}; w^{(m)}].$$

PROOF. Suppose $Q_{(\alpha,\beta)}(\mathbb{F})$ is non-singular. Then so is $Q_{(\alpha,\beta)}(k)$. Also

$$K[x^{(n)}; w^{(m)}] \cong Q_{(\alpha,\beta)}(k)[(y, z)^{(n)}, w^{(m)}] \text{ (by Lemma 4.9)}$$
$$\cong Q_{(\alpha,\beta)}(k[y, z)^{(n)}, w^{(m)}]). \text{ (by Lemma 3.17).}$$

By Lemma 3.17, $Q_{(\alpha,\beta)}(k[y, z)^{(n)}, w^{(m)}])$ is non-singular. Let D_2 be the lattice of c-ideals of $K[(y, z)^{(n)}, w^{(m)}]$. Then by Theorem 3.12, the map $\psi: D_2 \to D_1$ taking $J \in D_2$ to $\mathrm{crd}(J) \in D_1$ is a lattice isomorphism, as is the map $\mathrm{sca}: D_3 \to D_2$, taking $I \in D_3$ to $\mathrm{sca}(I) \in D_2$, by Lemma 4.9. Then $\varphi = \psi \circ \mathrm{sca}: D_3 \to D_1$ is an isomorphism.

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

THEOREM 4.13. *Let* $Q_{(\alpha,\beta)}(\mathbb{F})$ *be non-singular. The lattice* I_1 *of radical c-ideals in* $K[x^{(n)}; w^{(m)}]$ *is isomorphic to the lattice* I_2 *of radical ideals in* $K[(y, z)^{(n)}, w^{(m)}]$, *an isomorphism given by* $\delta: I_1 \to I_2$ *defined by*

$$\delta(\mathscr{I}_{n,m}(S)) = \mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S))) = \mathscr{I}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}(S))),$$

for all $S \subseteq [Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$.

PROOF. That δ is an isomorphism of partially ordered sets follows from the fact that

$$\mathrm{sca}: K[x^{(n)}; w^{(m)}] \to K[(y, z)^{(n)}; w^{(m)}]$$

is an isomorphism by Lemma 4.9, and from Theorem 3.14: δ does indeed map all radical ideals to all radical c-ideals, and, since it is injective and order preserving, is an isomorphism. That each partially ordered set is in fact a lattice follows from the fact that I_2 is known to be one (see [4]). Finally, for $S \subseteq [Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$, we have

$$\begin{aligned}
&\mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S))) \\
&\quad = \mathrm{crd}(\mathrm{sca}(\{f \in K[x^{(n)}; w^{(m)}] \mid f(s) = 0 \text{ for all } s \in S\})) \\
&\quad = \{\mathrm{crd}_1(f), \mathrm{crd}_2(f) \in K[(y, z)^{(n)}, w^{(m)}] \mid f \in K[x^{(n)}; w^{(m)}] \\
&\qquad \text{satisfies } \mathrm{crd}_1(f(t)) = \mathrm{crd}_2(f(t)) = 0 \text{ for all } t \in \mathrm{crd}(S)\} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemma 4.10)} \\
&\quad \subseteq \{g \in K[(y, z)^{(n)}, w^{(m)}] \mid g(t) = 0 \text{ for all } t \in \mathrm{crd}(S)\} \\
&\quad = \mathscr{I}_{0,2n+m}(\mathrm{crd}(S)).
\end{aligned}$$

Hence $\mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S))) \subseteq \mathscr{I}_{0,2n+m}(\mathrm{crd}(S))$.

Conversely, if $g \in \mathscr{I}_{0,2n+m}(\mathrm{crd}(S))$, then $g(t) = 0$ for all $t \in \mathrm{crd}(S)$, so $\mathrm{vec}(g)(s) = 0$ for all $s \in S = \mathrm{vec}(\mathrm{crd}(S))$ by Lemma 4.10. Hence we have $\mathrm{vec}(g) \in \mathscr{I}_{n,m}(S)$, whence $g = \mathrm{sca}(\mathrm{vec}(g)) \in \mathrm{sca}(\mathscr{I}_{n,m}(S))$. Indeed, $g \in \mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S)))$, so

$$\mathscr{I}_{0,2n+m}(\mathrm{crd}(S)) \subseteq \mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S))).$$

Thus in fact

$$\mathrm{crd}(\mathrm{sca}(\mathscr{I}_{n,m}(S))) = \mathscr{I}_{0,2n+m}(\mathrm{crd}(S)).$$

We now examine the case where $\mathbb{F}$ is an algebraically closed field. We shall obtain variants of the Hilbert Nullstellensatz, together with some other results corresponding to basic results of classical algebraic geometry, as occur in Zariski and Samuel [4]. We begin by giving the structure of $Q_{(\alpha,\beta)}(\mathbb{F})$ in the case where $\mathbb{F}$ is algebraically closed.

THEOREM 4.14. *Let* $\mathbb{F}$ *be algebraically closed. If* $Q_{(\alpha,\beta)}(\mathbb{F})$ *is non-singular, then it is isomorphic to* $\mathbb{F}\times\mathbb{F}$, *with conjugation defined by* $\overline{(a,b)}=(b,a)$. *If* $Q_{(\alpha,\beta)}(\mathbb{F})$ *is singular, then it is isomorphic to* $Q_{(0,0)}(\mathbb{F})$.

PROOF. Since $\mathbb{F}$ is algebraically closed, it contains an element γ such that $\gamma^2=\alpha+\beta\gamma$. Then

$$(\beta-2\gamma)^2=\beta^2-4\beta\gamma+4\gamma^2=\beta^2-4(\gamma^2-\alpha)+4\gamma^2=\beta^2+4\alpha.$$

If $Q_{(\alpha,\beta)}(\mathbb{F})$ is non-singular, then $\beta^2+4\alpha\neq 0$, so that $\beta-2\gamma\neq 0$ and so by Proposition 3.2.6, $Q_{(\alpha,\beta)}(\mathbb{F})\cong\mathbb{F}\times\mathbb{F}$ as algebras. If $Q_{(\alpha,\beta)}(\mathbb{F})$ is singular, then $\beta^2+4\alpha=0$, and so $\beta-2\gamma=0$. Hence, by Proposition 3.2.6, $Q_{(\alpha,\beta)}(\mathbb{F})$ is isomorphic to $Q_{(0,0)}(\mathbb{F})$ as an algebra. That conjugation is preserved by each of these isomorphisms is a consequence of Proposition 3.2.3.

The above theorem shows that, for each algebraically closed field $\mathbb{F}$, there is up to isomorphism (of rings with involution) only one non-singular quadratic algebra $Q_{(\alpha,\beta)}(\mathbb{F})$.

We now give variants of the Hilbert Nullstellensatz.

THEOREM 4.15. *Let* $Q_{(\alpha,\beta)}(\mathbb{F})$ *be non-singular. Let* $\mathbb{F}$ *be algebraically closed. Let* F *be a finite subset of* $K[x^{(n)};w^{(m)}]$. *Then* $1\in\langle F\rangle$ *if and only if* $\mathscr{V}_{n,m}(F)=\varnothing$.

PROOF. If $\mathscr{V}_{n,m}(F)=\varnothing$, then

$$\mathscr{V}_{0,2n+m}(\mathrm{crd}(\mathrm{sca}(F)))=\mathrm{crd}(\mathscr{V}_{n,m}(F))=\varnothing$$

by Theorem 4.11, so $1\in(\mathrm{crd}(\mathrm{sca}(F)))$, by the Hilbert Nullstellensatz (see cite3). Therefore $1=\mathrm{vec}(1)\in\langle F\rangle$ by Theorem 4.12. The converse is clear.

Algebraic closure of $\mathbb{F}$ is necessary and sufficient for such a theorem to hold, just as it is in the standard case. If $\mathbb{F}$ is not algebraically closed, then there is a non-constant $g\in\mathbb{F}[y]\subseteq\mathbb{F}[y,z]$ without a root, and $1\notin(g)$ in $\mathbb{F}[y,z]$ (and hence also $1\notin(g)$ in $\mathbb{F}[y]$) as g is not invertible. Then $\mathrm{vec}(g)\in\mathbb{F}[\mathbf{x}]$, and, by Theorem 4.11, $\mathrm{vec}(g)$ has no zero in $Q_{(\alpha,\beta)}(\mathbb{F})$, so $\mathscr{V}_{1,0}(\{g\})=\varnothing$; however, by Theorem 4.12, $1\notin\langle\mathrm{vec}(g)\rangle$. Thus for no such non-algebraically closed $\mathbb{F}$ will Theorem 4.15 hold.

We next obtain a result analogous to the most familiar version of the Hilbert Nullstellensatz.

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

THEOREM 4.16. *Let* $Q_{(\alpha,\beta)}(\mathbb{F})$ *be non-singular. Let* $\mathbb{F}$ *be algebraically closed and let* $\{f\} \cup F$ *be a finite subset of* $K[x^{(n)}; w^{(m)}]$. *Then we have* $\mathscr{I}_{n,m}(\mathscr{V}_{n,m}(F)) = \mathscr{R}(\langle F\rangle)$.

PROOF. Now $f \in \mathscr{I}_{n,m}(\mathscr{V}_{n,m}(F))$ if and only if

$$\operatorname{sca}(f) \in \operatorname{sca}(\mathscr{I}_{n,m}(\mathscr{V}_{n,m}(F)));$$

if and only if

$$\begin{aligned}\operatorname{crd}_1(f), \operatorname{crd}_2(f) &\in \operatorname{crd}(\operatorname{sca}(\mathscr{I}_{n,m}(\mathscr{V}_{n,m}(F))))\\ &= \mathscr{I}_{0,2n+m}(\operatorname{crd}(\mathscr{V}_{n,m}(F))) \qquad \text{(by Theorem 4.13)}\\ &= \mathscr{I}_{0,2n+m}(\mathscr{V}_{0,2n+m}(\operatorname{crd}(\operatorname{sca}(F)))) \qquad \text{(by Theorem 4.11)};\end{aligned}$$

that is, if and only if

$$\operatorname{crd}_1, \operatorname{crd}_2(f) \in \mathscr{R}(\operatorname{crd}(\operatorname{sca}(F)))$$

by the Hilbert Nullstellensatz [4]; which is if and only if

$$\operatorname{crd}_1(f), \operatorname{crd}_2(f) \in \mathscr{R}(\operatorname{crd}(\langle \operatorname{sca}(F)\rangle))$$

since, by Theorem 3.10,

$$\operatorname{crd}(\langle \operatorname{sca}(F)\rangle) = \operatorname{crd}((\operatorname{crd}(\operatorname{sca}(F))(i)) = (\operatorname{crd}(\operatorname{sca}(F)));$$

this holds if and only if

$$\operatorname{crd}_1(f), \operatorname{crd}_2(f) \in \operatorname{crd}(\mathscr{R}(\langle \operatorname{sca}(F)\rangle))$$

by Corollary 3.16; this holds if and only if

$$\operatorname{sca}(f) = \operatorname{crd}_1(f) + i \cdot \operatorname{crd}_2(f) \in \operatorname{crd}(\mathscr{R}(\langle \operatorname{sca}(F)\rangle))(i) = \mathscr{R}(\langle \operatorname{sca}(F)\rangle)$$

by Theorem 3.10; and this holds if and only if $f \in \mathscr{R}(\langle F\rangle)$ by Lemma 4.9.

In fact Theorem 4.16 implies Theorem 4.15: if $\mathscr{V}_{n,m}(F) = \varnothing$, then $1 \in \mathscr{I}_{n,m}(\mathscr{V}_{n,m}(F))$, and so $1^\rho = 1 \in \langle F\rangle$ for some ρ, by Theorem 4.16. Consequently, the remarks following Theorem 4.15 apply equally to Theorem 4.16.

Corollary 3.15 shows that c-prime c-ideals are all of the form $\mathscr{I}_{n,m}(\mathscr{V}_0)$ where $\mathscr{V}_0$ is a c-variety; we later characterise those c-varieties $\mathscr{V}_0$ which arise in this way.

We note that we have not considered the property corresponding to algebraic closure for $Q_{(\alpha,\beta)}(\mathbb{F})$, that is, whether or not all non-constant c-polynomials in $Q_{(\alpha,\beta)}(\mathbb{F})[x]$ have at least one zero in $Q_{(\alpha,\beta)}(\mathbb{F})$. Now the non-constant c-polynomial in one vector variable $\mathbf{x}\cdot\bar{\mathbf{x}}+1 \in \mathbb{R}[x]$ has no root

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

in $Q_{(-1,0)}(\mathbb{R}) \cong \mathbb{C}$, but does have one in $Q_{(-1,0)}(\mathbb{C})$, which seems analogous to $x^2 + 1 \in \mathbb{R}[x]$ having no root in $\mathbb{R}$ but having one in $\mathbb{C}$. This seemingly simplest possible example encourages the hope that $Q_{(\alpha,\beta)}(\mathbb{F})$ will be "c-algebraically closed" if $\mathbb{F}$ is algebraically closed. In fact, if it is the case that $\mathscr{V}(f) = \varnothing$ if and only if $1 \in (f)$ for all $f \in \mathbb{F}[w]$, so that any f without a root is invertible and hence a constant other than zero, then $\mathbb{F}$ is algebraically closed. Thus if the Hilbert Nullstellensatz "holds" for an arbitrary field $\mathbb{F}$, then that field must be algebraically closed. Similarly we might hope that if $Q_{(\alpha,\beta)}(\mathbb{F})$ is non-singular and Theorem 4.15 "holds" (equivalently, if $\mathbb{F}$ is algebraically closed) then $Q_{(\alpha,\beta)}(\mathbb{F})$ is "c-algebraically closed".

Let $\mathbb{F}$ be algebraically closed and $Q_{(\alpha,\beta)}(\mathbb{F})$ non-singular. Then by Theorem 4.15, any $f \in Q_{(\alpha,\beta)}(\mathbb{F})[x]$ without a root generates the unit c-ideal. Thus, for such f, there are $p, q \in Q_{(\alpha,\beta)}(\mathbb{F})[x]$ for which $pf + q\overline{f} = 1$. However, in contrast to the standard case, this does not imply that f is a constant: let $f(x) = \frac{1}{2}(1 + x - \overline{x})$, and then $1 \cdot f + 1 \cdot \overline{f} = 1$. Hence f has no root in $Q_{(\alpha,\beta)}(\mathbb{F})$. Indeed this choice of f is non-constant and generates the unit ideal for any choice of $\mathbb{F}$, algebraically closed or not, and any choices of α and β in $\mathbb{F}$, so that quadratic algebras over fields are *never* "c-algebraically closed".

The following theorem provides a direct proof of the closure under unions of c-varieties in $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$, as well as providing a link between the lattices of c-varieties and c-ideals, and holds for all fields $\mathbb{F}$.

THEOREM 4.17. *Let $Q_{(\alpha,\beta)}(\mathbb{F})$ be non-singular. Let $H = k$ or K. Let I_1 and I_2 be c-ideals in $H[x^{(n)}; w^{(m)}]$ and let $\mathscr{V}_1$ and $\mathscr{V}_2$ be c-varieties in $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$. Then we have*

$$\mathscr{V}_{n,m}(I_1 I_2) = \mathscr{V}_{n,m}(I_1 \cap I_2) = \mathscr{V}_{n,m}(I_1) \cup \mathscr{V}_{n,m}(I_2),$$
$$\mathscr{I}_{n,m}(\mathscr{V}_1 \cup \mathscr{V}_2) = \mathscr{I}_{n,m}(\mathscr{V}_1) \cap \mathscr{I}_{n,m}(\mathscr{V}_2).$$

PROOF. For all $F \subseteq K[x^{(n)}; w^{(m)}]$,

$$\begin{aligned}\mathscr{V}_{n,m}(F) &= \mathrm{vec}(\mathrm{crd}(\mathscr{V}_{n,m}(F))) \text{ by Lemma 4.9}\\ &= \mathrm{vec}(\mathscr{V}_{0,2n+m}(\mathrm{crd}(F))) \text{ by Theorem 4.11}.\end{aligned}$$

Hence if I_1 and I_2 are c-ideals of $K[x^{(n)}; w^{(m)}]$, then we have

$$\begin{aligned}\mathscr{V}_{n,m}(I_1 I_2) &= \mathrm{vec}[\mathscr{V}_{0,2n+m}(\mathrm{crd}(I_1 I_2))] = \mathrm{vec}[\mathscr{V}_{0,2n+m}(\mathrm{crd}(I_1) \cdot \mathrm{crd}(I_2))]\\ &\qquad \text{(since crd is an isomorphism by Lemma 4.9)}\\ &= \mathrm{vec}[\mathscr{V}_{0,2n+m}(\mathrm{crd}(I_1) \cap \mathrm{crd}(I_2))] \qquad \text{(by a basic result in [4])}\\ &= \mathrm{vec}[\mathscr{V}_{0,2n+m}(\mathrm{crd}(I_1 \cap I_2))] = \mathscr{V}_{n,m}(I_1 \cap I_2)\\ &\qquad \text{(by Theorem 4.11)}.\end{aligned}$$

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

But also

$$\begin{aligned}\mathscr{V}_{n,m}(I_1 I_2) &= \operatorname{vec}[\mathscr{V}_{0,2n+m}(\operatorname{crd}(I_1)) \cup \mathscr{V}_{0,2n+m}(\operatorname{crd}(I_2))] \qquad \text{(again by [4])} \\ &= \operatorname{vec}[\mathscr{V}_{0,2n+m}(\operatorname{crd}(I_1))] \cup \operatorname{vec}[\mathscr{V}_{0,2n+m}(\operatorname{crd}(I_2))] \\ &= \mathscr{V}_{n,m}(I_1) \cup \mathscr{V}_{n,m}(I_2) \qquad \text{(by Theorem 4.11).}\end{aligned}$$

The second part is immediate.

DEFINITION 4.18, 4.19. An *irreducible* c-variety is one which cannot be expressed as the union of two proper sub-c-varieties (proper subsets which are c-varieties). An *irreducible representation* of a c-variety is a (finite) collection of proper sub-c-varieties whose union is equal to the given c-variety.

The isomorphism between L_1 and L_2, discussed in Section 3, enables us to state the following

THEOREM 4.20. *Let $Q_{(\alpha,\beta)}(\mathbb{F})$ be non-singular. For every c-variety $\mathscr{V}_0$, there is a unique irreducible representation $\mathscr{V}_0 = \mathscr{V}_1 \cup \mathscr{V}_2 \cup \cdots \cup \mathscr{V}_n$ of $\mathscr{V}_0$ as a union of irreducible c-varieties.*

The proof of the corresponding fact for L_2 may be found in Zariski and Samuel [4]. Both results are in any case corollaries of a more general result holding for all distributive lattices with descending chain condition.

We conclude with a characterisation of those c-ideals which correspond to irreducible c-varieties, a result readily seen to be a generalisation of the standard result in [4], for example.

THEOREM 4.21. *Let $Q_{(\alpha,\beta)}(\mathbb{F})$ be non-singular. A c-variety $\mathscr{V}_0$ is irreducible if and only if $\mathscr{I}_{n,m}(\mathscr{V}_0)$ is c-prime.*

Suppose $\mathbb{F}$ is algebraically closed. A c-ideal I of $K[x^{(n)}; w^{(m)}]$ is c-prime if and only if $I = \mathscr{I}_{n,m}(\mathscr{V}_0)$ for some irreducible c-variety $\mathscr{V}_0$ in $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^n$.

PROOF. Now $\mathscr{V}_0$ is irreducible in $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$ if and only if $\operatorname{crd}(\mathscr{V}_0)$ is irreducible in $\mathbb{F}^{2n+m}$ (by Theorem 4.11), which is if and only if $\mathscr{I}_{0,2n+m}(\operatorname{crd}(\mathscr{V}_0))$ is prime (by a basic result in [4]), which holds if and only if $\operatorname{crd}(\operatorname{sca}(\mathscr{I}_{n,m}(\mathscr{V}_0)))$ is prime (by Theorem 4.13), and this holds if and only if $\mathscr{I}_{n,m}(\mathscr{V}_0)$ is c-prime (by Theorem 3.13 and Lemma 4.9).

Also I is c-prime in $K[x^{(n)}; w^{(m)}]$ if and only if $\operatorname{crd}(\operatorname{sca}(I))$ is prime in $k[y, z)^{(n)}, w^{(m)}]$ (by Theorem 3.10), which is if and only if $\operatorname{crd}(\operatorname{csa}(I)) =$

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

$\mathscr{I}_{0,2n+m}(\mathscr{V}_1)$ for $\mathscr{V}_1$ an irreducible variety in $\mathbb{F}^{2n+m}$ (again by a result appearing in [4]), which holds if and only if

$$\operatorname{crd}(\operatorname{sca}(I)) = \operatorname{crd}(\operatorname{sca}(\mathscr{I}_{n,m}(\operatorname{vec}(\mathscr{V}_1)))) \quad \text{(by Theorem 4.13)},$$

and this holds if and only if $I = \mathscr{I}_{n,m}(\operatorname{vec}(\mathscr{V}_1))$ by Theorem 4.12, with $\operatorname{vec}(\mathscr{V}_1)$ an irreducible c-variety in $[Q_{(\alpha,\beta)}(\mathbb{F})]^n \times \mathbb{F}^m$ by Theorem 4.11. (Moreover, all irreducible c-varieties arise in this way by Theorem 4.11.)

The second part of Theorem 4.21 may be proved more simply by using Theorem 4.16, as is done for the corresponding result in Zariski and Samuel [4]. However, we wished to show how it could be proved from Theorems 4.11, 4.12 and 4.13. Indeed, other results concerning c-prime and radical c-ideals flow directly from the correspondence between polynomial ideals and c-polynomial c-ideals as given in Theorems 4.12 and 4.13. Essentially, any statement concerning set-theoretic properties of prime, radical or ordinary ideals in any polynomial ring over a field $\mathbb{F}$, such as those occurring in Zariski and Samuel [4], will be translatable into a result for the corresponding c-polynomial ring over the corresponding non-singular quadratic algebra over $\mathbb{F}$, which, if $\mathbb{F}$ is algebraically closed, is essentially unique by Theorem 4.14. Theorem 4.11 completes the picture and permits one to obtain results such as Theorem 4.17 and others concerning c-varieties.

5. Concluding remarks

Many of the results of this paper were obtained with applications in mind. The author is currently using them to develop methods for the automation of plane Euclidean geometry theorem proving. The bulk of standard methods for doing this rely for their theoretical basis on elementary algebraic geometry results concerning algebraically closed fields. In particular, such methods are based on the conversion of geometrical relations to algebraic equations in the coordinates of the points of the theorem relative to a pair of Cartesian axes, and, often, subsequent use of the Hilbert Nullstellensatz; for example see Chou and Schelter [3]. There are good grounds for believing that algorithms based on the formalism considered here, with $\alpha = -1$, $\beta = 0$, will, for a wide variety of theorems, be more efficient than the existing algorithms. This is largely a result of the greater simplicity and naturalness with which geometrical relations may be stated using the formalism discussed here in comparison to the usual one based on coordinatisation of the plane.

However, apart from the results after Theorem 4.13 which generalise the Hilbert Nullstellensatz, there is no requirement of algebraic closure on the

https://doi.org/10.1017/S1446788700034327 Published online by Cambridge University Press

field $\mathbb{F}$ in the results of Section 4. Furthermore, the results of Section 3 apply to all commutative rings with identity K, and so have wide applicability.

Acknowledgement

I would like to thank Desmond Fearnley-Sander for introducing me to the general concept of automated theorem proving in geometry using rewrite rules, without which the ideas behind this paper would not have occurred, for pointing out the possible relevance of quadratic algebras in Bourbaki [1] which led to the scope and generality of this paper being increased, and for assisting in the proof reading.

References

[1] N. Bourbaki, *Elements of Mathematics, Algebra I*, Addison-Wesley (1973).
[2] R. P. Burn, *A pathway into number theory*, Cambridge University Press (1982).
[3] S. Chou and W. F. Schelter, 'Proving Geometry Theorems with Rewrite Rules', *Automated Reasoning* **2** (1986), 253–273.
[4] O. Zariski and P. Samuel, *Commutative Algebra*, Van Nostrand (1958).

University of Tasmania
Box 252C Hobart
Tasmania 7001
Australia