Section 1.3, The Associated Conic

The associated conic of (a, b) is the curve in $\mathbf{P}^2$ defined by

$$ax^2 + by^2 = z^2$$

The circle $x^2 + y^2 = z^2$, for example, defines $(1, 1) \xrightarrow{\sim} M_2(k)$
This is an invariant of the quaternion algebra: if two quaternion algebras (a, b) and (c, d) are isomorphic as k-algebras then their associated conics are also isomorphic over k.

In algebraic geometry, one says the conic $C(a, b)$ has a $k-$rational point if we have $x_0, y_0, z_0 \in k$ not all zero that satisfy the equation $C(a, b) = ax^2 + by^2 = z^2$

[1]this has a characteristic 2 counterpart

In algebraic geometry, one says the conic $C(a, b)$ has a $k-$rational point if we have $x_0, y_0, z_0 \in k$ not all zero that satisfy the equation $C(a, b) = ax^2 + by^2 = z^2$

Proposition

The quaternion algebra (a, b) is split if and only if the conic $C(a, b)$ has a k-rational point [1]

[1] this has a characteristic 2 counterpart

Proof.

$\leftarrow$ If $(x_0, y_0, z_0$ has a k-rational point on $C(a, b)$ with $y_0 \neq 0$ then

$$b = \left(\frac{z_0}{y_0}\right)^2 - a\left(\frac{x_0}{y_0}\right)^2$$

and we see it's split by (4) of proposition 1.1.7.

Proof.

$\leftarrow$ If $(x_0, y_0, z_0$ has a k-rational point on $C(a, b)$ with $y_0 \neq 0$ then

$$b = \left(\frac{z_0}{y_0}\right)^2 - a\left(\frac{x_0}{y_0}\right)^2$$

and we see it's split by (4) of proposition 1.1.7. If instead $y_0 = 0$ then $x_0 \neq 0$ and we get a as a norm of $k(\sqrt{b})|k$ instead.

Proof.

$\leftarrow$ If $(x_0, y_0, z_0$ has a k-rational point on $C(a, b)$ with $y_0 \neq 0$ then

$$b = \left(\frac{z_0}{y_0}\right)^2 - a\left(\frac{x_0}{y_0}\right)^2$$

and we see it's split by (4) of proposition 1.1.7. If instead $y_0 = 0$ then $x_0 \neq 0$ and we get a as a norm of $k(\sqrt{b})|k$ instead.
$\rightarrow$ If $b = r^2 - as^2$ for some $r, s \in k$ then $(s, 1, r)$ is a k rational point on $C(a, b)$

$$as^2 + b = r^2$$

example 1.3.4

If $a \neq 1$ then $ax^2 + (1-a)y^2 = z^2$ has the k-rational point $(1,1,1)$, hence $(a, 1-a)$ splits.[2]

[2] special case of the steinberg relation

example 1.3.4

If $a \neq 1$ then $ax^2 + (1-a)y^2 = z^2$ has the k-rational point $(1,1,1)$, hence $(a, 1-a)$ splits.[2]

Remark

From algebraic geometry we get that a smooth projective conic defined over a field k is isomorphic to the projective line $\mathbf{P}^1$ if and only if it has a k rational point.
This gets us another equivalent condition for saying (a, b) is split.

[2] special case of the steinberg relation

Examples:

1.3.6

Let k be the finite field with q elements (q odd). Then any quaternion algebra over k is split.

[3] counting 0

Examples:

1.3.6

Let k be the finite field with q elements (q odd). Then any quaternion algebra over k is split.

k's multiplicative group is cyclic of order $q-1$ so there are $1+\frac{q-1}{2}$ squares[3] and thus $\{ax^2 : x \in k\}$ and $\{1-by^2 | y \in k\}$ both have cardinality of $1+(q-1)^2$ and their shared element s gives us a k rational point at $(s, s, 1)$.

[3] counting 0

1.3.7

Let (a, b) be a quaternion algebra over k. Then (a, b) is split over k if and only if $(a, b) \otimes_k k(t)$ is split over $k(t)$.

[4] the map $k(t) \to k$ we get by setting $t = 0$

1.3.7

Let (a, b) be a quaternion algebra over k. Then (a, b) is split over k if and only if $(a, b) \otimes_k k(t)$ is split over $k(t)$.

$\rightarrow$ is clear
$\leftarrow$ assume we have $(x_t, y_t, z_t) \in C(a, b)$ defined over $k(t)$. As $C(a, b) := ax^2 + by^2 = z^2$ is homogeneous, we may assume after multiplication of some element of $k(t)$ that x_t, y_t, z_t all lie in $k[t]$ and one of them has nonzero constant term. Then specialization[4] gives a k-point $(x_t(0), y_t(0), z_t(0))$ of $C(a, b)$.

[4] the map $k(t) \rightarrow k$ we get by setting $t = 0$

1.3.8

For $a \in k^\times$ the $k(t)$-algebra (a, t) is split if and only if a is a square in k.

1.3.8

For $a \in k^\times$ the $k(t)$-algebra (a, t) is split if and only if a is a square in k.

$\leftarrow$ scale and see it is isomorphic to $(1, t) \sim M_2(k)$.
$\rightarrow$ Assume we have some $k(t)$-point (x_t, y_t, z_t) of $C(a, b)$ as on the last slide. Again, we may assume x_t, y_t, z_t are all in $k[t]$. If x_t and z_t were both divisible by t then the equation

1.3.8

For $a \in k^\times$ the $k(t)$-algebra (a, t) is split if and only if a is a square in k.

$\leftarrow$ scale and see it is isomorphic to $(1, t) \sim M_2(k)$.
$\rightarrow$ Assume we have some $k(t)$-point (x_t, y_t, z_t) of $C(a, b)$ as on the last slide. Again, we may assume x_t, y_t, z_t are all in $k[t]$. If x_t and z_t were both divisible by t then the equation $C(a, b) := ax^2 + by^2 = z^2$ would imply the same for y_t, so after division, we can assume they are not. Then setting $t = 0$ and get $ax_t^2(0) = z_t(0)^2$ and thus $a = x_t^2(0)^{-1} z_t(0)^2$ is a square.

Section 1.4, A theorem of Witt

Recall that the function field of an algebraic curve C is the field $k(C)$ of the rational functions defined over some Zariski open subset of C. For our conics $C(a, b)$ we can define the function field as the fraction field of the integral domain

$$k[x, y]/(ax^2 + by^2 - 1)$$

Recall that the function field of an algebraic curve C is the field $k(C)$ of the rational functions defined over some Zariski open subset of C. For our conics $C(a, b)$ we can define the function field as the fraction field of the integral domain

$$k[x, y]/(ax^2 + by^2 - 1)$$

Remark

The quaternion algebra $(a, b) \otimes_k k(C(a, b))$ is always split over $k(C(a, b))$. The conic $C(a, b)$ always has the point $(x, y, 1)$ in $(a, b) \otimes_k k(C(a, b))$ over the field which is called the generic point of the conic.

Theorem

1.4.2 (Witt) *Let $Q_1 = (a_1, b_1)$, $Q_2 = (a_2, b_2)$ be quaternion algebras and let $C_i = C(a_i, b_i)$ be the associated conics. The algebras Q_1 and Q_2 are isomorphic over k if and only if the function fields $k(C_1)$ and $k(C_2)$ are isomorphic over k.*

Theorem

1.4.2 (Witt) *Let $Q_1 = (a_1, b_1)$, $Q_2 = (a_2, b_2)$ be quaternion algebras and let $C_i = C(a_i, b_i)$ be the associated conics. The algebras Q_1 and Q_2 are isomorphic over k if and only if the function fields $k(C_1)$ and $k(C_2)$ are isomorphic over k.*

Remark

It is known from algebraic geometry that two smooth projective curves are isomorphic if and only if their function fields are. With this theorem and what we had from section 1.3 we can therefore say two quaternion algebras are isomorphic if and only if their associated conics are isomorphic as algebraic curves.

Lemma

If (a, b) is a quaternion algebra and $c \in k^\times$ is a norm from the field extension $k(\sqrt{a}|k)$, then $(a, b) \cong (a, bc)$.

Proof.

We can write $c = x^2 - ay^2$ with $x, y \in k$, making c the norm of $q = x + yi$. Set $\mathbf{J} = qj = xj + yij$. This is a pure quaternion with

$$i\mathbf{J} = -\mathbf{J}i, \quad \mathbf{J}^2 = -N(\mathbf{J}) = -N(q)N(j) = bc,$$

and evidently $1, i, \mathbf{J}, i\mathbf{J}$ is a basis of (a, b) over k and $(a, b) \cong (a, bc)$ □

sketch of 1.4.2's proof

$\leftarrow$ is clear since if they have the same function fields they have isomorphic conics and are isomorphic algebras

$\rightarrow$ if both are split, the thoerem is obvious, so assume Q_1 is nonsplit. We know $Q_1 \otimes_k k(C_1)$ is split, which means $Q_1 \otimes_k k(C_2)$ is too by our assumption. If Q_2 is split, then $k(C_2)$ is a rational function field, and therefore Q_1 is also split by example 1.3.7

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1
3. Likewise note $Q_2 \otimes_k L(C)$ is split over $L(C)$ and $Q_2 \otimes L$ is split over L

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1
3. Likewise note $Q_2 \otimes_k L(C)$ is split over $L(C)$ and $Q_2 \otimes L$ is split over L
4. Proposition 1.2.3 gives us $Q_2 \xrightarrow{\sim} (a_1, c)$ for some $c \in k^\times$

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1
3. Likewise note $Q_2 \otimes_k L(C)$ is split over $L(C)$ and $Q_2 \otimes L$ is split over L
4. Proposition 1.2.3 gives us $Q_2 \xrightarrow{\sim} (a_1, c)$ for some $c \in k^\times$
5. It follows from proposition 1.1.7 $c = N_{L(C)/k(C)}(f)$ for some $f \in L(C)^\times$.

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1
3. Likewise note $Q_2 \otimes_k L(C)$ is split over $L(C)$ and $Q_2 \otimes L$ is split over L
4. Proposition 1.2.3 gives us $Q_2 \xrightarrow{\sim} (a_1, c)$ for some $c \in k^\times$
5. It follows from proposition 1.1.7 $c = N_{L(C)/k(C)}(f)$ for some $f \in L(C)^\times$.
6. Identify f up to a constant: $f = c_0 h^d$, $h = b_1 y(z + \sqrt{a_1} z)^{-1}$. c_0 is a constant in $L^\times$ and d is the degree of a certain expression[5]

[5] this part takes over a page

Therefore we assume both are non-split. this remaining case is what takes up two pages in the book.
Essentially the steps are:

1. Note $Q_1 \otimes_k L$ is split over $L := k(\sqrt{a_1})$
2. Note $L(C_1) = L \otimes_k k(C_1)$ is the function field of the curve C_L obtained from the extension of C_1
3. Likewise note $Q_2 \otimes_k L(C)$ is split over $L(C)$ and $Q_2 \otimes L$ is split over L
4. Proposition 1.2.3 gives us $Q_2 \xrightarrow{\sim} (a_1, c)$ for some $c \in k^\times$
5. It follows from proposition 1.1.7 $c = N_{L(C)/k(C)}(f)$ for some $f \in L(C)^\times$.
6. Identify f up to a constant: $f = c_0 h^d$, $h = b_1 y(z + \sqrt{a_1} z)^{-1}$. c_0 is a constant in $L^\times$ and d is the degree of a certain expression[5]
7. Some computations show $c = N_{L|k}(c_0) b_1^d$ and thus $Q_2 \cong (a_1, c) \cong (a_1, b_1^d)$, since Q_2 is nonsplit d is odd and $Q_2 \cong (a_1, b_1)$ as desired

□

[5] this part takes over a page

Section 1.5, Tensor products of quaternion algebras

We move our consideration to higher dimensional k-algebras, where k is still assumed to be a field of characteristic $\neq 2$. The simplest are biquaternion algebras, k-algebras isomorphic to a tensor product of two quaternion algebras over k.

We move our consideration to higher dimensional k-algebras, where k is still assumed to be a field of characteristic $\neq 2$. The simplest are biquaternion algebras, k-algebras isomorphic to a tensor product of two quaternion algebras over k.

Lemma

The tensor product of two matrix algebras $M_n(k)$ and $M_m(k)$ over k is isomorphic to the matrix algebra $Mnm(k)$

Proof.

Note that given k-endomorphisms $\phi \in \mathrm{End}_k(k^n)$ and $\psi \in \mathrm{End}_k(k^m)$, the pair ϕ, ψ induces an element $\psi \otimes \psi$ of $\mathrm{End}_k(k^n \otimes_k k^m)$. The resulting map $\mathrm{End}_k(k^n) \otimes \mathrm{End}_k(k^m) \to \mathrm{End}_k(k^n \otimes_k k^m)$ is injective and surjective. □

Lemma

Given elements $a, b, b' \in k^\times$ we have an isomorphism $(a, b) \otimes_k (a, b') \xrightarrow{\sim} (a, bb') \otimes_k M_2(k)$.

Lemma

Given elements $a, b, b' \in k^\times$ we have an isomorphism $(a, b) \otimes_k (a, b') \xrightarrow{\sim} (a, bb') \otimes_k M_2(k)$.

Denote by $(1, i, j, ij)$ and $(1, i', j', i'j')$ the bases of (a, b) and (a, b') and consider the following k-subspaces of $(a, b) \otimes_k (a, b')$:

$$A_1 = k(1 \otimes 1) \oplus k(i \otimes 1) \oplus k(j \otimes j') \oplus k(ij \otimes j'),$$

$$A_2 = k(1 \otimes 1) \oplus k(1 \otimes j') \oplus k(i \otimes i'j') \oplus k((-b'i) \otimes i')$$

$A_1 = k(1\otimes 1)\oplus k(i\otimes 1)\oplus k(j\otimes j')\oplus k(ij\otimes j')$
$A_2 = k(1\otimes 1)\oplus k(1\otimes j')\oplus k(i\otimes i'j')\oplus k((-b'i)\otimes i')$

Proof.

A_1, A_2 are subalgebras if $(a,b)\otimes_k (a,b')$[6] and they are respectively isomorphic to (a, bb'), $(b', -a^2b')$. We see $A_2 \sim (b', -a^2b') \sim (b', -b')$ and A_2 is split since $C(b', -b')$ has the k-rational point $(1, 1, 0)$
Now if we consider the map $\rho : A_1 \otimes_k A_2 \to (a,b)\otimes_k (a,b')$ induced by the k-linear map $(x,y) \to xy$. We see all basis elements of $(a,b)\otimes_k (a,b')$ lie in ρ's image, so it's injective and gives the required isomorphism. □

[6] since they are closed

Corollary

For a quaternion algebra (a, b) the tensor product algebra $(a, b) \otimes_k (a, b)$ is isomorphic to the matrix algebra $M_4(k)$

Proof.

Set $b = b'$ in the previous lemma and see

$$(a, b) \otimes_k (a, b) \cong (a, b^2) \otimes_k M_2(k) \cong (a, 1) \otimes_k M_2(k) \cong M_2(k) \otimes_k M_2(k)$$

□

A biquaternion algebra $A = Q_1 \otimes_k Q_2$ is equipped with an involution σ defined as the product of the conjugation involutions on Q_1, Q_2

$$\sigma(q_1 \otimes q_2) = \overline{q_1} \otimes \overline{q_2}$$

This involution depends on our decomposition of $A \cong Q_1 \otimes_k Q_2$.

[7] Q_i^- denotes the pure quaternions in Q_i

A biquaternion algebra $A = Q_1 \otimes_k Q_2$ is equipped with an involution σ defined as the product of the conjugation involutions on Q_1, Q_2

$$\sigma(q_1 \otimes q_2) = \overline{q_1} \otimes \overline{q_2}$$

This involution depends on our decomposition of $A \cong Q_1 \otimes_k Q_2$.

Lemma

Let V be the k-subspace of A consisting of elements satisfying $\sigma(a) = -a$ and W the subspace of those with $\sigma(a) = a$. One has a direct sum decomposition $A = V \oplus W$, and moreover one may write.

$$V = (Q_1^- \otimes_k k) \oplus (k \otimes_k Q_2^-) \quad \textit{and} \quad W = k \oplus (Q_1^- \otimes_k Q_2^-).^7$$

[7] Q_i^- denotes the pure quaternions in Q_i

Proof.

$V \cap W = 0$ and clearly

$$(Q_1^- \otimes_k k) \oplus (k \otimes_k Q_2^-) \subset V \quad \text{and} \quad k \oplus (Q_1^- \otimes_k Q_2^-) \subset W.$$

For dimension reasons these must be isomorphisms and $V \oplus W$ must be all of A. □

Denote by N_1 and N_2 the quaternion norms on Q_1 and Q_2 and consider

$$\phi(x, y) = N_1(x) - N_2(y)$$

on V. this is the *Albert form* of A. It also depends on our decomposition.

Denote by N_1 and N_2 the quaternion norms on Q_1 and Q_2 and consider

$$\phi(x, y) = N_1(x) - N_2(y)$$

on V. this is the *Albert form* of A. It also depends on our decomposition.

Theorem

Theorem 1.5.5 (Albert) *For a biquaternion algebra $A \cong Q_1 \otimes_k Q_2$ over k, the are equivalent*

1. *The algebra A is not a division algebra.*
2. *There exist $a, b, b' \in k^\times$ such that $Q_1 \xrightarrow{\sim} (a, b)$ and $Q_2 \xrightarrow{\sim} (a, b')$.*
3. *The Albert form has a nontrivial zero on A*

(1)$\rightarrow$(2), we show that if (2) is false, so is (1). Both Q_1, Q_2 are division algebras and we can tensor them with quadratic extensions contained in the other to form new division algebras $Q_1 \otimes_k K_2$ and $Q_2 \otimes_k K_1$. We fix a quaternion basis for Q_2 such that $K_2 = k(j)$ and write

$$\alpha = (\beta_1 + \beta_2 j) + (\beta_3 + \beta_4 j)ij$$

with $\beta_i \in Q_1$. $\gamma := \beta_3 + \beta_4 j \neq 0$ so γ^{-1} exists in $Q_1 \otimes_k K_2$. After replacing α by $\gamma^{-1}\alpha$ we can reuce things to cases only with $\alpha = \beta_1 + \beta_2 j + ij$ If β_1 and β_2 commute then $k(\beta_1, \beta_2)$ is either K or a quadratic extension contained in Q_1 and it's inverse exists.

(1)$\rightarrow$(2) continued
If β_1 and β_2 do not commute then set $\alpha^* := \beta_1 - \beta_2 j - ij$ and see

$$\alpha^*\alpha = (\beta_1 - \beta_2 j - ij)(\beta_1 + \beta_2 j + ij) = (\beta_1 - \beta_2 j)(\beta_1 + \beta_2 j) - (ij)^2 =$$
$$= \beta_1^2 - \beta_2^2 j^2 - (ij)^2 + (\beta_1\beta_2 - \beta_2\beta_1)j,$$

Since j^2 and $(ij)^2$ lie in k and $\beta_1\beta_2 - \beta_2\beta_1 \neq 0$ $\alpha^*\alpha \in (Q_1 \otimes_k K_2)\ \{0\}$
so $\alpha, \alpha^* \in A$ have inverses and A is, in fact, a division algebra $\square$

For reference:

1. The algebra A is not a division algebra.
2. There exist $a, b, b' \in k^\times$ such that $Q_1 \xrightarrow{\sim} (a, b)$ and $Q_2 \xrightarrow{\sim} (a, b')$.
3. The Albert form has a nontrivial zero on A

Remaining implications

Proof.

(2)$\to$(3), $\exists q_i \in Q_i$ with $q_i^2 = -N_i(q_i) = a$ so $\phi(q_1, q_2) = a - a = 0$
(3)$\to$(1), See by $0 = \phi(q_1, q_2) = q_1^2 - q_2^2 = (q_1 + q_2)(q_1 - q_2)$[8] that we have zero-divisors. □

[8] $q_1 \in Q_1$, and $q_2 \in Q_2$ commute since Q_1 and Q_2 centralize one-another in the tensor product

example 1.5.7

Let k be a field of characteristic $\neq 2$ as usual. Let F be the purely transcendental extension $k(t_1, t_2, t_3, t_4)$. Then the biquaternion algebra

$$(t_1, t_2) \otimes_F (t_3, t_4)$$

is a division algebra over F.

This is shown in the book by an argument that shows it's Albert form has no nontrivial zero by assuming that it does and then forming a contradiciton.

In general, we say that a finite dimensional division algebra D over a field k has *period 2* if $D \otimes_k D$ is isomorphic to a matrix algebra over k. Our examples of this are quaternion algebras[9] and tensor products of division algebras that are themselves of period 2.[10]
By proposition 1.2.1 a 4-dimensional central division algebra over k is a quaternion algebra. Moreover a 16-dimensional central division algebra of period 2 is isomorphic to a biquaternion algebra.[11]

[9] by corollary 1.5.3
[10] by lemma 1.5.1
[11] proved in 1932 by Albert

A more general notion, that a central division algebra of period 2 and 4^m dimensions is always a tensor product of m quaternion algebras, is false, sadly.[12]
We do, however get the following

Theorem

1.5.8 (Merkurjev) *Let D be a central division algebra of period 2 over a field k. There exist positive integers m_1, m_2, n and quaternion algebras $Q_1, \ldots, Q_n$ over k such that there is an isomorphism*

$$D \otimes_k M_{m_1}(k) \cong Q_1 \otimes_k Q_2 \otimes_k \ldots \otimes_k Q_n \otimes M_{m_2}(k).$$

[12] Shown in 1979 by Amitsur, Rowen, and Tignol with a 64 dimensional counterexample