Idempotent 2-by-2 matrices

Holger P. Petersson
Fakultät für Mathematik und Informatik
FernUniversität in Hagen
D-58084 Hagen
Germany
Email: Holger.Petersson@FernUni-Hagen.de

Franz Locher aus Anlass seiner Emeritierung gewidmet

Abstract

(Idempotent) 2-by-2 matrices of determinant 0 and trace 1 over a commutative ring are related to line bundles on two generators. This is used to describe their orbits under inner (resp. arbitrary) automorphisms and to construct explicit examples of line bundles on two generators having infinite order in the Picard group of the base ring.

1. Introduction

This paper may be regarded as an exercise in maths education. Starting out from a topic in linear algebra that could hardly be more elementary, we proceed to explore its ramifications as the underlying base field is replaced by an arbitrary commutative associative ring of scalars. The results obtained along the way are neither deep nor original, but serve as an instructive illustration of what commutative algebra can do for us even when dealing with very simple-minded questions over arbitrary commutative rings.

The key notion of the paper is that of an elementary idempotent: an idempotent 2-by-2 matrix c with entries in a commutative ring k is said to be *elementary* if it is different from $0, 1$ not only over k itself but over all non-trivial scalar extensions as well; as it turns out, this is equivalent to c having determinant 0 and trace 1.

An important feature of elementary idempotents is that they survive in the more general set-up of conic algebras (Section 3) and are related to line bundles in a natural way (Section 5); more specifically, with very little effort we will be able to set up a bijective correspondence between isomorphism classes of line bundles on two generators over k and orbits of elementary idempotents under the action of the full linear group by inner automorphisms (Prop 5.7). As an amusing corollary we conclude that, over the ring of integers of a (finite) algebraic number field, the number of these orbits agrees with the class number of that field (Cor. 5.9). Returning to the setting of arbitrary base rings in Section 6, we find natural obstructions to the validity of the Skolem-Noether theorem for Azumaya algebras (Cor. 6.3) and obtain counter-examples to Witt cancellation for non-singular quadratic forms that have some bearing on the study of composition algebras (6.7). The paper concludes in Section 7 with a brief visit to the scheme of elementary idempotents that allows us to construct explicit "hands-on" examples of line bundles on two generators having infinite order in the Picard group of the base ring (Thms. 7.3, 7.4).

With the possible exception of these two theorems, whose proofs rely on some classical results from algebraic geometry, the level of the paper is completely elementary. In order to emphasize this aspect, and for the convenience of the reader, a few standard facts about line bundles over commutative rings that will be used frequently later on have been collected in Section 4.

Notations. Throughout we let k be an arbitrary commutative ring. Unadorned tensor products are always to be taken over k. We write $M_2(k)$ for the k-algebra of 2-by-2 matrices with entries in k and $\mathbf{1}_2 \in M_2(k)$ for the 2-by-2 unit matrix. The category of commutative associative k-algebras with 1 will be denoted by k-**alg**. We write $\mathrm{Spec}(k)$ for the prime spectrum of k, i.e., for the totality of prime ideals in k endowed with the Zariski topology. For a k-module M, $x \in M$, $R \in k$-**alg**, $\mathfrak{p} \in \mathrm{Spec}(k)$, we denote by $k_{\mathfrak{p}}$ the localization of k at $\mathfrak{p}$ and put

$$M_R := M \otimes R, \quad x_R := x \otimes 1_R \in M_R, \quad M_{\mathfrak{p}} := M_{k_{\mathfrak{p}}}, \quad x_{\mathfrak{p}} := x_{k_{\mathfrak{p}}} = x/1 \in M_{k_{\mathfrak{p}}}.$$

The bilinearization of a quadratic form $q : M \to k$ will always be denoted by the same letter, so

$$q(x,y) := q(x+y) - q(x) - q(y). \qquad (x, y \in M)$$

The canonical pairing between a k-module M and its dual $M^* := \mathrm{Hom}_k(M,k)$ will be indicated by

$$M \times M^* \longrightarrow k, \quad (x, x^*) \longmapsto \langle x, x^* \rangle := x^*(x).$$

We think of n-dimensional column space k^n over k as being equipped with the canonical scalar product $k^n \times k^n \to k$, $(x,y) \mapsto x^t y$.

Acknowledgement. The author is greatly indebted to O. Loos, who carefully read an earlier version of the paper and made several important suggestions for improvement. In particular, the short proof of Prop. 6.6 is basically due to him. He also clarified the picture around Thm. 7.3, giving rise to Thm. 7.4 as a separate result in the process. He also generalized both theorems considerably; the reader is referred to [6] for details.

2. Linear algebra.

For the time being, we assume that k is a field. An idempotent $c \in M_2(k)$ is said to be *non-trivial* if $c \neq 0, \mathbf{1}_2$. The following characterization of non-trivial idempotents is a standard fact from linear algebra.

2.1. Proposition. *Let k be a field and $c \in M_2(k)$. Then the following conditions are equivalent.*

(i) *c is a non-trivial idempotent.*

(ii) $\det c = 0, \quad \mathrm{tr}(c) = 1.$

(iii) *There exists $g \in \mathrm{GL}_2(k)$ satisfying $gcg^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.*

(iv) *There exists an automorphism φ of $M_2(k)$ satisfying $\varphi(c) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.*

(v) *There exist column vectors $x, y \in k^2$ satisfying $c = xy^t$ and $x^t y = 1$.*

If these conditions are fulfilled and $x, y \in k^2$ satisfy $c = xy^t$, then $x^t y = 1$ and

$$\operatorname{Im} c = kx, \quad \operatorname{Ker} c = (ky)^{\perp}.$$

In particular, the pair (x, y) is unique up to transformations of the form $(x, y) \mapsto (\alpha x, \alpha^{-1} y)$, $\alpha \in k^{\times}$. $\square$

The only thing worth mentioning here is that the equivalence of (iii) and (iv) derives from (a special case of) the classical Skolem-Noether theorem: every automorphism of a central simple associative algebra of finite dimension (e.g., a full matrix algebra) over a field is inner.

2.2. Key question. What happens to Prop. 2.1 if the field k is replaced by an arbitrary commutative associative ring of scalars? In this paper, we will try to answer this question as completely as possible. The following example shows that the answer cannot be entirely straightforward.

2.3. Example. Let k_0 be a field and $k = k_0^3$ with componentwise operations. Write ε_i $(1 \le i \le 3)$ for the unit vectors in k, so $\sum \varepsilon_i = 1_k$, $\varepsilon_i \varepsilon_j = \delta_{ij} \varepsilon_i$ $(1 \le i, j \le 3)$, and put

$$c := \begin{pmatrix} \varepsilon_1 + \varepsilon_3 & 0 \\ 0 & \varepsilon_2 + \varepsilon_3 \end{pmatrix} \in M_2(k).$$

Then c is an idempotent $\neq 0, \mathbf{1}_2$ but $\det c = \varepsilon_3 \neq 0, \operatorname{tr}(c) = 1_k + \varepsilon_3 \neq 1_k$. Hence the equivalence of (i), (ii) in Prop. 2.1 founders badly over rings. Notice also that the projection onto the third factor makes $R = k_0$ a k-algebra and $c_R = \mathbf{1}_2$ in $M_2(R)$.

3. Conic algebras and elementary idempotents.

Returning to our arbitrary base ring k, Example 2.3 tells us that the property of an idempotent in $M_2(k)$ to be different from $0, \mathbf{1}_2$ is not preserved under scalar extensions. This simple observation gives rise to the notion of an elementary idempotent. We prefer to phrase it in a considerably more general context.

3.1. The concept of a conic algebra. By a *conic algebra* over k we mean a pair (C, n) consisting of a unital (non-associative) k-algebra C over k and a quadratic form $n : C \to k$ (the *norm*) such that

$$n(1_C) = 1, \quad x^2 - t(x)x + n(x)1_C = 0, \qquad (x \in C) \tag{1}$$

where $t := n(1_C, -)$ is called the *trace* of (C, n). For a systematic treatment of conic algebras the reader may consult [8, 1.4].

3.2. Key facts about conic algebras. a) Conic algebras are invariant under base change.
b) If (C, n) is a conic algebra over k and $x \in C$, then $k[x] := k1_C + kx \subseteq C$ is a unital commutative associative subalgebra and n *permits local composition*, so

$$n(yz) = n(y)n(z). \qquad (y, z \in k[x])$$

Also, x is invertible in $k[x]$ if and only if $n(x) \in k^{\times}$.

3.3. Key example. For our purposes, the key example of a conic algebra is $(C, n) := (M_2(k), \det)$. Other examples arise naturally in the study of composition algebras over rings, cf. [8, 1.5,1.6].

3.4. Elementary idempotents in conic algebras. Let (C, n) be a conic algebra over k. An element $c \in C$ is called an *elementary idempotent* if it is an idempotent and $c_R \neq 0, 1$ for all $R \in k$-**alg**, $R \neq \{0\}$. We wish to understand conditions (i)-(v) of Prop. 2.1 for elementary (rather than non-trivial) idempotents over rings and begin with the following simple observation. Recall that k is connected if it contains no idempotents other than 0 and 1.

3.5. Proposition. *Assume $k \neq \{0\}$ is connected and let (C, n) be a conic algebra with trace t over k. For $c \in C$ to be an idempotent $\neq 0, 1_C$ it is necessary and sufficient that $n(c) = 0, t(c) = 1$.*

Proof. If $n(c) = 0, t(c) = 1$, then c is an idempotent by (1), which cannot be zero since $t(c) = 1$ and cannot be 1_C since $n(c) = 0$. Conversely, suppose c is an idempotent $\neq 0, 1_C$. By 3.2 b), $n(c)$ is an idempotent in k, forcing $n(c) = 1$ or $n(c) = 0$ by connectedness. Assuming $n(c) = 1$, c would be invertible in $k[c]$ (3.2 b)), and $c(1_C - c) = 0$ would imply $c = 1_C$. This contradiction shows $n(c) = 0$. But then (1) reduces to $c = c^2 = t(c)c$ and applying the trace shows that $t(c)$ is an idempotent in k. Thus $t(c) = 0$ or $t(c) = 1$, and since $t(c) = 0$ implies $c = 0$, we end up with $t(c) = 1$. □

Remark. Prop. 3.5 explains why the use of idempotents in the base ring is unavoidable in Example 2.3. It also shows, in conjunction with Key Example 3.3, that for elementary rather than non-trivial idempotents, conditions (i), (ii) of Prop. 2.1 are equivalent over arbitrary commutative rings:

3.6. Corollary. *For a conic algebra (C, n) with trace t over k and $c \in C$, the following conditions are equivalent.*

(i) *c is an elementary idempotent.*

(ii) *$c_{\mathfrak{p}}$ is an idempotent $\neq 0, 1_{C_{\mathfrak{p}}}$ in $C_{\mathfrak{p}}$, for all prime ideals $\mathfrak{p} \subseteq k$.*

(iii) *$n(c) = 0$, $t(c) = 1$.*

Proof. While (iii) $\Rightarrow$ (i) follows from (1), the implication (i) $\Rightarrow$ (ii) is obvious. Finally, to prove (ii) $\Rightarrow$ (iii), Prop. 3.5 implies $n(c)_{\mathfrak{p}} = 0$, $t(c)_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in \mathrm{Spec}(k)$ since $k_{\mathfrak{p}} \neq \{0\}$ is connected, and (iii) follows. □

4. Line bundles.

Here we collect what little is needed about line bundles (= finitely generated projective modules of rank 1, also called invertible modules) over arbitrary commutative rings. We refer to Bourbaki [1, II §5] for details. Given $f \in k$, a k-module M and $x \in M$, we put

$$S := \{1, f, f^2, \dots\} \subseteq k, \quad k[f^{-1}] := S^{-1}k,$$
$$M[f^{-1}] := M_{k[f^{-1}]}, \quad x[f^{-1}] : = x_{k[f^{-1}]} = x/1 \in M[f^{-1}].$$

Our notation will not always distinguish carefully between elements $x \in M$ and their images $x/1 \in M[f^{-1}]$.

4.1. The concept of a line bundle. By a *line bundle* over k we mean k-module L such that the following equivalent conditions hold.

(i) L is finitely generated and, for all $\mathfrak{p} \in \mathrm{Spec}(k)$, the $k_{\mathfrak{p}}$-module $L_{\mathfrak{p}}$ is free of rank 1.

(ii) There are elements $f_1, \ldots, f_m \in k$ such that $\sum kf_i = k$ and, for each $i = 1, \ldots, m$, the $k[f_i^{-1}]$-module $L[f_i^{-1}]$ is free of rank 1.

4.2. Key facts. Let L, L' be line bundles over k.
a) Line bundles are finitely generated projective k-modules, so L is a direct summand of k^n, for some $n \in \mathbb{N}$.
b) $L \otimes L'$ and $L^* = \mathrm{Hom}_k(L, k)$ are line bundles over k.
c) $\mathrm{Pic}(k) := \{[L] | L \text{ is a line bundle over } k\}$, where $[L]$ stands for the isomorphism class of L, is an abelian group under the operation $[L][L'] := [L \otimes L']$, with unit element and inverse of $[L]$ given by $[k]$ and$[L^*]$, respectively. $\mathrm{Pic}(k)$ is called the *Picard group* of k. Setting $L^{\otimes n} := L \otimes \cdots \otimes L$ (n-times) and $L^{\otimes -n} := L^{*\otimes n}$ for $n \in \mathbb{N}_0$, we obtain $[L^{\otimes n}] = [L]^n$ for all $n \in \mathbb{Z}$.
d) For $R \in k$-**alg**, $L_R = L \otimes R$ is a line bundle over R and $L \mapsto L_R$ gives a group homomorphism $\mathrm{Pic}(k) \to \mathrm{Pic}(R)$. Thus we obtain a (covariant) functor Pic from k-algebras to abelian groups.
e) There is a natural isomorphism $L^* \otimes L' \xrightarrow{\sim} \mathrm{Hom}_k(L, L')$ sending $x^* \otimes x'$, for $x^* \in L^*$, $x' \in L'$, to the linear map $L \to L'$, $x \mapsto \langle x, x^* \rangle x'$.
f) If $\varphi : L \to L'$ is an epimorphisms, it is, in fact, an isomorphism.

The proof of the following well known proposition will be included here for completeness.

4.3. Proposition. *Let L be a line bundle over k.*

a) *If L is generated by a single element, then $L \cong k$ is free of rank 1.*

b) *If $f_1, \ldots, f_m \in k$ satisfy $\sum kf_i = k$ and have L_{f_i} free over k_{f_i} for all $i = 1, \ldots, m$, then L is generated by m elements.*

Proof. a) Any generator of L gives an epimorphism $k \to L$, allowing us to apply 4.2 f).
b) Let $x_i/1$ be a basis of $L[f_i^{-1}]$ over $k[f_i^{-1}]$, for $i = 1, \ldots, m$. Given $x \in L$, there exist $n \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_m \in k$ such that $x/1 = (\alpha_i/f_i^n)(x_i/1) = (\alpha_i x_i)/f_i^n$ in $L[f_i^{-1}]$ for all $i = 1, \ldots, m$. Hence for some integer $p \geq n$ and all $i = 1, \ldots, m$, $f_i^p x = \beta_i x_i$, $\beta_i = f_i^{p-n}\alpha_i$. Since the $f_1^p, \ldots, f_m^p$ continue to generate k as an ideal, we find $g_1, \ldots, g_m \in k$ such that $\sum f_i^p g_i = 1$. But this implies $x = \sum \beta_i g_i x_i$, so $L = \sum kx_i$ is generated by $x_1, \ldots, x_m$. $\square$

5. Elementary idempotents in $M_2(k)$.

We are now ready to analyze elementary idempotents of the conic algebra $(M_2(k), \det)$.

5.1. The line bundle of an elementary idempotent. Let $c \in M_2(k)$ be an elementary idempotent. By Cor. 3.6, c has trace 1 and determinant 0, so

$$c = \begin{pmatrix} \alpha & \beta \\ \gamma & \overline{\alpha} \end{pmatrix}, \quad \alpha, \beta, \gamma \in k, \quad \overline{\alpha} = 1 - \alpha, \quad \alpha\overline{\alpha} = \beta\gamma. \tag{2}$$

The last condition means

$$\alpha^2 - \alpha + \beta\gamma = 0. \tag{3}$$

Viewing c as a linear map $k^2 \to k^2$, we consider its image

$$L_c := \operatorname{Im} c = k \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} + k \begin{pmatrix} \beta \\ \overline{\alpha} \end{pmatrix} \tag{4}$$

and, using (2), record the relations

$$\beta \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \alpha \begin{pmatrix} \beta \\ \overline{\alpha} \end{pmatrix}, \quad \overline{\alpha} \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \gamma \begin{pmatrix} \beta \\ \overline{\alpha} \end{pmatrix} \tag{5}$$

on the two generators of L_c. Now observe that

$$\overline{c} = \mathbf{1}_2 - c = \begin{pmatrix} \overline{\alpha} & -\beta \\ -\gamma & \alpha \end{pmatrix} \in M_2(k) \tag{6}$$

is an elementary idempotent as well and since $\operatorname{Ker} c = L_{\overline{c}}$, we have

$$k^2 = L_c \oplus L_{\overline{c}}, \tag{7}$$

so $L_c, L_{\overline{c}}$ are finitely generated projective k-modules such that, for each $\mathfrak{p} \in \operatorname{Spec}(k)$, $\operatorname{rk}_{\mathfrak{p}}(L_c) + \operatorname{rk}_{\mathfrak{p}}(L_{\overline{c}}) = 2$. Moreover, both summands on the left are different from 2 since $\det c = \det \overline{c} = 0$ and we conclude *that L_c, $L_{\overline{c}}$ are line bundles over k*. We call L_c the line bundle *of* (or *associated with*) c.

More detailed information will now be supplied by the following lemma.

5.2. Lemma. *Notations being as in 5.1, the following statements hold.*

a) $k\alpha + k\overline{\alpha} = k$.

b) $(L_c)[\alpha^{-1}]$ *is a free* $k[\alpha^{-1}]$*-module of rank* 1*, with basis* $\left(\begin{smallmatrix} \alpha \\ \gamma \end{smallmatrix}\right)$*, and* $(L_c)[\overline{\alpha}^{-1}]$ *is a free* $k[\overline{\alpha}^{-1}]$*-module of rank* 1*, with basis* $\left(\begin{smallmatrix} \beta \\ \overline{\alpha} \end{smallmatrix}\right)$*.*

c) *The map*

$$\det : L_c \otimes L_{\overline{c}} \xrightarrow{\sim} k, \quad x \otimes y \longmapsto \det(x, y),$$

is an isomorphism, forcing $L_{\overline{c}} \cong L_c^*$ to be the dual of L_c, hence its inverse in $\operatorname{Pic}(k)$*.*

Proof. While a) is obvious, b) follows immediately from (4), (5). In c) it suffices to show that det is an isomorphism over $k[\alpha^{-1}]$, $k[\overline{\alpha}^{-1}]$. By b) and (6), $(L_c)[\alpha^{-1}]$,

$(L_{\overline{c}})[\alpha^{-1}]$ are free of rank 1 over $k[\alpha^{-1}]$ with bases $\binom{\alpha}{\gamma}, \binom{-\beta}{\alpha}$, respectively. Hence (3) gives

$$\det \begin{pmatrix} \alpha & -\beta \\ \gamma & \alpha \end{pmatrix} = \alpha^2 + \beta\gamma = \alpha \in k[\alpha^{-1}]^\times.$$

Similarly, $(L_c)[\overline{\alpha}^{-1}], (L_{\overline{c}})[\overline{\alpha}^{-1}]$ are free of rank 1 over $k[\overline{\alpha}^{-1}]$ with bases $\binom{\beta}{\overline{\alpha}}, \binom{\overline{\alpha}}{-\gamma}$, respectively, and

$$-\det \begin{pmatrix} \beta & \overline{\alpha} \\ \overline{\alpha} & -\gamma \end{pmatrix} = \overline{\alpha}^2 + \beta\gamma = 1 - 2\alpha + \alpha^2 + \beta\gamma = 1 - \alpha = \overline{\alpha} \in k[\overline{\alpha}^{-1}]^\times.$$

The assertion follows. $\square$

Remark. Since we know from 5.1 that L_c is a line bundle over k, the isomorphism $L_{\overline{c}} \cong L_c^*$ also follows from (7) by taking determinants (i.e., second exterior powers) and invoking Bourbaki [1, III §7, Cor. of Prop. 10, p.517].

The interplay between elementary idempotents and line bundles set up by 5.1 and Lemma 5.2 will now be described more closely in a series of easy propositions and their corollaries.

5.3. Proposition. *Let $c \in M_2(k)$ be an elementary idempotent and $R \in k$-$\mathbf{alg}$. Then there is a canonical isomorphism $L_{c_R} \cong L_c \otimes R$.*

Proof. The property of the sequence

$$0 \longrightarrow L_{\overline{c}} \longrightarrow k^2 \xrightarrow{c} L_c \longrightarrow 0$$

to be split exact is preserved under scalar extensions, and the assertion follows.

$\square$

5.4. Proposition. *Let $c \in M_2(k)$ be an idempotent. Then c is elementary if and only if $L_c := \operatorname{Im} c$ is a line bundle over k.*

Proof. The condition on L_c is necessary for c to be elementary, by 5.1. Conversely, suppose L_c is a line bundle over k. For $\mathfrak{p} \in \operatorname{Spec}(k)$, $\operatorname{Im} c_{\mathfrak{p}} = (L_c)_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^2$ is a free submodule of rank 1, so $c_{\mathfrak{p}} \neq 0, \mathbf{1}_2$ in $M_2(k_{\mathfrak{p}})$ and Cor. 3.6 implies that c is elementary. $\square$

5.5. Proposition. *Let L be a line bundle over k. There exists an elementary idempotent $c \in M_2(k)$ satisfying $L_c \cong L$ if and only if L is generated by two elements.*

Proof. By (4), L_c is generated by two elements, for any elementary idempotent $c \in M_2(k)$. Conversely, suppose L is generated by two elements. Then we obtain a short exact sequence $0 \to L' \to k^2 \to L \to 0$ of k-modules, which splits since L is projective. Thus $k^2 \cong L \oplus L'$, and the projection onto the first summand gives an idempotent $c \in M_2(k)$ satisfying $\operatorname{Im} c \cong L$ and c is elementary by Prop. 5.4.

$\square$

5.6. Corollary. *If L is a line bundle on two generators over k, so is $L^{\otimes n}$ for all $n \in \mathbb{Z}$.*

Proof. By Prop. 5.5, there exists an elementary idempotent $c \in M_2(k)$ as in 5.1 such that $L \cong L_c$. Now Lemma 5.2 b) shows that $L[\alpha^{-1}]$, $L[\overline{\alpha}^{-1}]$ are free of rank 1 over $k[\alpha^{-1}]$, $k[\overline{\alpha}^{-1}]$, respectively. But then so are $(L^{\otimes n})[\alpha^{-1}] \cong (L[\alpha^{-1}])^{\otimes n}$, $(L^{\otimes n})[\overline{\alpha}^{-1}] \cong (L[\overline{\alpha}^{-1}])^{\otimes n}$. Hence $L^{\otimes n}$ is generated by two elements (Prop. 4.3 b)). $\square$

5.7. Proposition. *Elementary idempotents $c, d \in M_2(k)$ are conjugate under the inner automorphism group of $M_2(k)$ if and only if $L_c \cong L_d$.*

Proof. If $d = gcg^{-1}$ for some $g \in \mathrm{GL}_2(k)$, then g maps $L_c = \mathrm{Im}\, c$ isomorphically onto $\mathrm{Im}\, gc = \mathrm{Im}\, gcg^{-1} = \mathrm{Im}\, d = L_d$. Conversely, if L_c, L_d are isomorphic, so are $L_{\overline{c}}, L_{\overline{d}}$ by Lemma 5.2 c). Hence, given any isomorphisms $\rho : L_c \xrightarrow{\sim} L_d, \overline{\rho} : L_{\overline{c}} \xrightarrow{\sim} L_{\overline{d}}$,

$$g := \rho \oplus \overline{\rho} : k^2 = L_c \oplus L_{\overline{c}} \xrightarrow{\sim} L_d \oplus L_{\overline{d}} = k^2$$

belongs to $\mathrm{GL}_2(k)$, and for $x \in L_c$, $y \in L_{\overline{c}}$ we obtain

$$gc(x + y) = g(x) = \rho(x) = d\big(\rho(x) + \overline{\rho}(y)\big) = dg(x + y).$$

Hence $d = gcg^{-1}$, as claimed. $\square$

5.8. Example: Dedekind domains. Let k be a Dedekind domain. Then line bundles over k are basically the same as fractional ideals, and $\mathrm{Pic}(k)$ identifies canonically with the class group of k, so algebraic number theory provides us with lots of examples where this group (is finite but) has a rich and sufficiently complicated structure. Also, thanks to the strong approximation theorem, every fractional ideal of any Dedekind ring k is generated by two elements (O'Meara [7, 22:5a, p.48]), hence by Prop. 5.5 has the form L_c for some elementary idempotent $c \in M_2(k)$. Combining this with Prop. 5.7, we end up with the following amusing conclusion.

5.9. Corollary. *Let K be a (finite) algebraic number field and write $\mathfrak{o}_K$ for its ring of integers. Then the number of orbits of elementary idempotents in $M_2(\mathfrak{o}_K)$ under the action of $\mathrm{GL}_2(\mathfrak{o}_K)$ by conjugation is finite and, in fact, agrees with the class number of K.* $\square$

We are now in a position to analyze conditions (ii), (iii), (v) of Prop. 2.1 over arbitrary commutative rings.

5.10. Proposition. *For $c \in M_2(k)$, the following conditions are equivalent.*

(i) *c is an elementary idempotent and the k-module L_c is free of rank 1.*

(ii) *There exists $g \in \mathrm{GL}_2(k)$ satisfying $gcg^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.*

(iii) *There exist column vectors $x, y \in k^2$ satisfying $c = xy^t$ and $x^t y = 1$.*

If these conditions are fulfilled and $x, y \in k^2$ satisfy $c = xy^t$, then $x^t y = 1$ and

$$L_c = \operatorname{Im} c = kx, \quad L_{\overline{c}} = \operatorname{Ker} c = (ky)^{\perp}. \tag{8}$$

In particular, the pair (x, y) is unique up to transformations of the form $(x, y) \mapsto (\alpha x, \alpha^{-1} y)$, $\alpha \in k^{\times}$.

Proof. (i) $\Longleftrightarrow$ (ii). Since $d = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is an elementary idempotent having $L_d = k\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ free of rank 1, this follows from Prop. 5.7.
(iii) $\Longrightarrow$ (i). For any $x, y \in k^2$ satisfying $c = xy^t$, $x^t y = 1$ and for $z \in k^2$ we obtain $cz = (z^t y)x$, hence $cx = x$ and $c^2 z = cz$. Thus c is an idempotent such that $L_c := \operatorname{Im} c = kx$ is free of rank 1, forcing c to be elementary by Prop. 5.4, and (8) holds.
(i) $\Longrightarrow$ (iii). We require the relation

$$\det(x, y) = x^t J y \qquad \left(J := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right) \tag{9}$$

for all $x, y \in k^2$. By Lemma 5.2 c), since L_c is free of rank 1, so is $L_{\overline{c}}$, and we find basis vectors x of L_c, $\overline{x}$ of $L_{\overline{c}}$, respectively, such that $\det(x, \overline{x}) = 1$. Therefore $(x, \overline{x})$ is a basis of k^2 and setting $y = J\overline{x}$, (9) shows $x^t y = 1$, $(ky)^{\perp} = k\overline{x}$. But now, by the implication (iii) $\Rightarrow$ (i) and (8), $d := xy^t$ is an elementary idempotent satisfying $L_d = kx = L_c$, $\operatorname{Ker} d = (ky)^{\perp} = k\overline{x} = \operatorname{Ker} c$, hence $c = d$.
It remains to prove the final statement of the proposition, so suppose (i) $-$ (iii) hold and $x, y \in k^2$ satisfy $c = xy^t$. Then $c = c^2 = (x^t y)c$, and taking traces yields $x^t y = 1$. But then (8) has already been settled while establishing the implication (iii) $\Rightarrow$ (i). The remaining assertion is now obvious. $\square$

5.11. Twisted powers of elementary idempotents. Let $c \in M_2(k)$ be an elementary idempotent and $n \in \mathbb{Z}$. By Prop. 5.5 and Cor. 5.6, there exists an elementary idempotent $c^{\langle n \rangle} \in M_2(k)$ such that $L_{c^{\langle n \rangle}} \cong L_c^{\otimes n}$; moreover, by Prop. 5.7, $c^{\langle n \rangle}$ is unique up to conjugation by inner automorphisms. Skipping most of the details, a representative for the conjugacy class of $c^{\langle n \rangle}$ may be found as follows.

Applying 4.2 c) and Lemma 5.2 c), we obtain $L_c^{\otimes -1} \cong L_{\overline{c}}$, and since $c^{\langle 0 \rangle} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ up to conjugation (Prop. 5.10), we may assume $n \in \mathbb{N}$. Writing c as in (2), we conclude

$$\alpha^n \alpha_n + \overline{\alpha}^n \delta_n = 1,$$

where

$$\alpha_n := \sum_{i=0}^{n-1} \binom{2n-1}{i} \alpha^{n-1-i} \overline{\alpha}^i, \quad \delta_n := \sum_{i=0}^{n-1} \binom{2n-1}{n+i} \alpha^{n-1-i} \overline{\alpha}^i,$$

and

$$c^{\langle n \rangle} := \begin{pmatrix} \alpha^n \alpha_n & \beta^n \delta_n \\ \gamma^n \alpha_n & \overline{\alpha}^n \delta_n \end{pmatrix} \in M_2(k)$$

is an elementary idempotent satisfying $L_{c^{\langle n \rangle}} \cong L_c^{\otimes n}$.

6. Obstructions to the Skolem-Noether theorem and to Witt cancellation.

We wish to understand condition (iv) of Prop. 2.1 in a purely ring-theoretical setting. To this end, we require the Peirce decomposition of associative algebras: every idempotent c of an associative algebra A induces a direct sum decomposition $A = A_{11} \oplus A_{10} \oplus A_{01} \oplus A_{00}$ of k-modules $A_{ij} := A_{ij}(c) := \{x \in A \mid cx = ix, xc = jx\}$, $i, j = 0, 1$. We begin with a digression into twisted matrix algebras.

6.1. Twisted 2-by-2 matrices. Let L be a line bundle over k. Then

$$A := \mathrm{End}_k(L \oplus k) = \begin{pmatrix} k & L \\ L^* & k \end{pmatrix}$$

is a reduced quaternion algebra in the sense of [8, 1.9]. In the present context, it will be totally adequate to view A merely as a conic algebra, with norm and trace being given by the ordinary determinant and the ordinary trace of matrices:

$$\det x = \alpha\delta - \langle u, u^* \rangle, \quad \mathrm{tr}(x) = \alpha + \delta, \qquad (\text{for } x = \begin{pmatrix} \alpha & u \\ u^* & \delta \end{pmatrix} \in A)$$

and to observe with [8, Ex. 1.24] that isomorphisms between such algebras always preserve norms and traces. Finally,

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A$$

is an elementary idempotent (Cor. 3.6) and

$$A_{10}(e) = \begin{pmatrix} 0 & L \\ 0 & 0 \end{pmatrix} \cong L$$

as k-modules.

We will see in a moment that condition (iv) of Prop. 2.1 is *not* equivalent to c being an elementary idempotent. Instead, we obtain:

6.2. Proposition. *For $c \in A := M_2(k)$, the following conditions are equivalent.*

(i) *c is an elementary idempotent.*

(ii) *There exist a line bundle L over k and an isomorphism*

$$\Phi : M_2(k) \longrightarrow \mathrm{End}_k(L \oplus k) = \begin{pmatrix} k & L \\ L^* & k \end{pmatrix}$$

such that

$$\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

In this case, L as in (ii) *is unique up to isomorphism; more precisely, $L \cong L_c^{\otimes 2} \cong A_{10}(c)$.*

Proof. (ii) $\Longrightarrow$ (i). Since Φ preserves norms and traces by 6.1, c is an elementary idempotent.
(i) $\Longrightarrow$ (ii). Setting $L := L_c$, $\overline{L} := L_{\overline{c}}$, we obtain the decomposition $k^2 = L \oplus \overline{L} = \binom{L}{\overline{L}}$. Therefore 4.2 e) and Lemma 5.2 c) give rise to a chain of isomorphisms, all but the very first one being "slot preserving",

$$M_2(k) \cong \mathrm{End}_k(\begin{pmatrix} L \\ \overline{L} \end{pmatrix}) \cong \begin{pmatrix} \mathrm{Hom}_k(L,L) & \mathrm{Hom}_k(\overline{L},L) \\ \mathrm{Hom}_k(L,\overline{L}) & \mathrm{Hom}_k(\overline{L},\overline{L}) \end{pmatrix}$$
$$\cong \begin{pmatrix} L^* \otimes L & \overline{L}^* \otimes L \\ L^* \otimes \overline{L} & \overline{L}^* \otimes \overline{L} \end{pmatrix} \cong \begin{pmatrix} k & L^{\otimes 2} \\ L^{\otimes 2*} & k \end{pmatrix}$$

under which c is eventually transformed into $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. In particular, $A_{10}(c) \cong L_c^{\otimes 2}$. To establish the final statement of the proposition, let L, Φ be as in (ii). Then 6.1 and what has been proved in (i) $\Rightarrow$ (ii) imply $L \cong A_{10}(c) \cong L_c^{\otimes 2}$. $\square$

6.3. Corollary. *Two elementary idempotents $c, d \in M_2(k)$ are conjugate under the full automorphism group of $M_2(k)$ if and only if $L_c^{\otimes 2} \cong L_d^{\otimes 2}$.*

Proof. Suppose c, d are conjugate under the full automorphism group of $A = M_2(k)$, so $d = \varphi(c)$ for some $\varphi \in \mathrm{Aut}(A)$. Then $\varphi(A_{10}(c)) = A_{10}(d)$, and Prop. 6.2 implies $L_c^{\otimes 2} \cong L_d^{\otimes 2}$. Conversely, let this be so and put $L := L_c$. By Prop. 6.2, there are isomorphisms

$$\Phi, \Psi : M_2(k) \xrightarrow{\sim} \begin{pmatrix} k & L^{\otimes 2} \\ L^{\otimes 2*} & k \end{pmatrix}$$

satisfying

$$\Phi(c) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \Psi(d).$$

Setting $\varphi := \Psi^{-1} \circ \Phi \in \mathrm{Aut}(A)$, we obtain $\varphi(c) = d$, as desired. $\square$

Remark. Combining Prop. 5.7, Cor. 6.3 and 5.8, we obtain natural obstructions to the validity of the Skolem-Noether theorem for Azumaya algebras over commutative rings. More generally, given any Azumaya algebra A over k, we have the exact sequence of Rosenberg-Zelinsky:

$$0 \longrightarrow \mathrm{Int}(A) \longrightarrow \mathrm{Aut}(A) \longrightarrow \mathrm{Pic}(k).$$

For this and other details, some of them directly related to results obtained here, we refer to [5, IV, §1].

6.4. Corollary. *Let M be a line bundle over k. Then $\mathrm{End}_k(M \oplus k) \cong M_2(k)$ if and only if there exists a line bundle L over k that is generated by two elements and satisfies $M \cong L^{\otimes 2}$.*

Proof. If $M \cong L^{\otimes 2}$ for some line bundle L on two generators over k, then $\mathrm{End}_k(M \oplus k) \cong M_2(k)$ by Propositions 5.5, 6.2. Conversely, let

$$\Psi : \mathrm{End}_k(M \oplus k) \xrightarrow{\sim} M_2(k)$$

be an isomorphism and consider the elementary idempotent $c := \Psi((\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix})) \in M_2(k)$. Then M and $\Phi := \Psi^{-1}$ satisfy condition (ii) of Prop. 6.2. Hence $M \cong L_c^{\otimes 2}$. □

6.5. Hyperbolic planes. The preceding results combined with 5.8 or Thm. 7.3 below also yield easy counter-examples to Witt cancellation in the theory of quadratic forms. These counter-examples are based on the following construction. Let L be a line bundle over k. Then the map

$$\mathbf{h}_L : L \oplus L^* \longrightarrow k, \quad v \oplus v^* \longmapsto \mathbf{h}_L(v \oplus v^*) := \langle v, v^* \rangle$$

is a non-singular quadratic form satisfying $\mathbf{h}_L \cong \langle \alpha \rangle . \mathbf{h}_L$ for all $\alpha \in k^\times$. Following Knus [4, I (3.5)], we refer to $\mathbf{h}_L$ or $(L, \mathbf{h}_L)$ as a *hyperbolic plane*, while $\mathbf{h} := \mathbf{h}_k$ is called the *split* hyperbolic plane. Conditions that are necessary and sufficient for a hyperbolic plane to be split are presented in the following proposition.

6.6. Proposition. *Given a line bundle L over k, the following conditions are equivalent.*

(i) *The hyperbolic plane $\mathbf{h}_L$ is split, i.e., isometric to $\mathbf{h}$.*

(ii) *There are elements $e_\pm \in L \oplus L^*$ satisfying the relations*

$$\mathbf{h}_L(e_+) = \mathbf{h}_L(e_-) = 0, \quad \mathbf{h}_L(e_+, e_-) = 1. \tag{10}$$

(iii) *The line bundle L is trivial.*

Proof. The implications (iii) ⇒ (i) ⇒ (ii) being obvious, it suffices to prove (ii) ⇒ (iii), which we do by adopting a suggestion of O. Loos. Writing $e_\pm = v_\pm \oplus v_\pm^*, v_\pm \in L, v_\pm^* \in L^*$, relations (10) imply

$$\langle v_+ + v_-, v_+^* + v_-^* \rangle = \mathbf{h}_L(e_+ + e_-) = 1.$$

Therefore $v_+ + v_-$ is a unimodular vector and hence a basis of L over k. □

6.7. Counter-examples to Witt cancellation. Let L be a line bundle on two generators over k such that $M := L^{\otimes 2}$ is non-trivial. From Cor. 6.4 we conclude

$$M_2(k) \cong \mathrm{End}_k(M \oplus k) \cong \begin{pmatrix} k & M \\ M^* & k \end{pmatrix}$$

as isomorphisms of quaternion algebras, so both algebras have isometric norms. But the norm of $M_2(k)$ is $\mathbf{h} \perp \mathbf{h}$, while the norm of $\mathrm{End}_k(M \oplus k)$ is $\mathbf{h} \perp \mathbf{h}_M$. Hence $\mathbf{h} \perp \mathbf{h} \cong \mathbf{h} \perp \mathbf{h}_M$ even though $\mathbf{h}$ and $\mathbf{h}_M$ are not isometric by Prop. 6.6, and we have obtained a counter example to Witt cancellation of non-singular quadratic forms over rings.

6.8. Example. Let L be a line bundle on two generators over k that is not a square in $\mathrm{Pic}(k)$. Then

$$\mathrm{End}_k(L \oplus k) = \begin{pmatrix} k & L \\ L^* & k \end{pmatrix}$$

is a reduced quaternion algebra over k that is free as a k-module (since $L \oplus L^* \cong k^2$ by Lemma 5.2 c), (7) and Prop. 5.5) but is not isomorphic to $M_2(k)$ (Cor. 6.4).

7. Elementary idempotents and algebraic geometry.

We wish to construct examples of elementary idempotents $c \in M_2(k)$, for appropriate base rings k, such that the corresponding line bundle L_c is as complicated as one could possibly hope for. One way of achieving this consists in looking at Dedekind domains (5.8). But there are other, more direct, means of constructing elementary idempotents whose associated line bundles are sufficiently complicated. They derive from looking at the set of *all* elementary idempotents in *all* scalar extensions.

7.1. The scheme of elementary idempotents. Let $\mathbf{X}$ be the functor from k-algebras to sets defined by

$$\mathbf{X}(R) := \{c \in M_2(R) \mid c \text{ is an elementary idempotent}\} \quad \text{for } R \in k\text{-}\mathbf{alg}$$

and $\mathbf{X}(f) : \mathbf{X}(R) \to \mathbf{X}(S)$, for a k-algebra homomorphism $f : R \to S$, being the set map that sends an elementary idempotent of $M_2(R)$ to its componentwise image under f in $M_2(S)$. By (3), $\mathbf{X}$ is an affine scheme represented by the k-algebra

$$k[\mathbf{X}] = k[X, Y, Z]/(Z^2 - Z + XY), \tag{11}$$

so we have natural identifications

$$\mathrm{Hom}_{k\text{-}\mathbf{alg}}(k[\mathbf{X}], R) = \mathbf{X}(R) \quad \text{for all } R \in k\text{-}\mathbf{alg}. \tag{12}$$

Writing $\pi : k[X, Y, Z] \to k[\mathbf{X}]$ for the canonical projection and setting $u = \pi(X), v = \pi(Y), w = \pi(Z)$, a straightforward verification shows that u, v are algebraically independent over k (so no non-zero $f \in k[X, Y]$ kills (u, v)), allowing us to identify $u = X, v = Y$ via π. Then

$$k[\mathbf{X}] = k[X, Y][w],$$

where $w \in k[\mathbf{X}]$ satisfies the defining relation

$$w^2 - w + XY = 0.$$

Hence $k[\mathbf{X}]$ is a conic $k[X, Y]$-algebra that is a free $k[X, Y]$-module of rank 2, with basis $1, w$. Now

$$e := \begin{pmatrix} w & X \\ Y & \overline{w} \end{pmatrix} \in M_2(k[\mathbf{X}]), \quad \overline{w} := 1 - w, \tag{13}$$

is an elementary idempotent in $M_2(k[\mathbf{X}])$, corresponding to the identity transformation $k[\mathbf{X}] \to k[\mathbf{X}]$ via (12)and satisfying the following property.

7.2. Specialization property. Let $R \in k$-**alg**. By (12), giving an elementary idempotent $c \in M_2(R)$ amounts to making R a $k[\mathbf{X}]$-algebra, which we denote by $R^{\langle c\rangle}$. In this case, $c = e_{R^{\langle c\rangle}}$ and Prop. 5.3 implies

$$L_e \otimes_{k[\mathbf{X}]} R^{\langle c\rangle} \cong L_c. \tag{14}$$

7.3. Theorem. *Notations being as in 7.1 and assuming $k \neq \{0\}$, the line bundle L_e over $k[\mathbf{X}]$ has infinite order in* $\mathrm{Pic}(k[\mathbf{X}])$.

Proof. Replacing k by $\kappa(\mathfrak{p}), \mathfrak{p} \in \mathrm{Spec}(k)$, and invoking the specialization property 7.2, we reduce to the case that k is a field. Then we can actually prove a much stronger result.

7.4. Theorem. *Notations being as in 7.1 and assuming that k is a field,* $\mathrm{Pic}(k[\mathbf{X}]) \cong \mathbb{Z}$ *is generated by* $[L_e]$.

Proof. We will make free use of standard facts from classical algebraic geometry and refer to Hartshorne [3, II §6] for details. In order to keep formal prerequisites at a minimum, we also assume that k is algebraically closed; with the appropriate scheme-theoretic adjustments, our proof will go through in the general case virtually unchanged. We now regard $\mathbf{X}$ as a (possibly reducible) algebraic k-variety and perform the following steps.

1^0. Writing projective n-space $\mathbb{P}^n := \{[x] \mid x \in k^{n+1} - \{0\}\}$ in homogeneous co-ordinates, we recall that the Segre embedding (cf. Prop. 2.1 (v))

$$\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3 = \big\{[u] \mid u \in M_2(k) - \{0\}\big\}, \quad ([x],[y]) \longmapsto [xy^t],$$

identifies

$$\mathbb{P}^1 \times \mathbb{P}^1 = \{[u] \in \mathbb{P}^3 \mid \mathrm{rk}(u) = 1\} = \{[u] \in \mathbb{P}^3 \mid \det u = 0\}$$

as a (quadratic hyper) surface in $\mathbb{P}^3$, with the corresponding closed immersion

$$i : \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3.$$

Now consider the open affine

$$\begin{aligned} U : &= \{[u] \in \mathbb{P}^1 \times \mathbb{P}^1 \mid \mathrm{tr}(u) \neq 0\} = \{[u] \in \mathbb{P}^3 \mid \det u = 0 \neq \mathrm{tr}(u)\} \\ &= \{c \in M_2(k) \mid \det c = 0,\ \mathrm{tr}(c) = 1\} = \mathbf{X}, \end{aligned}$$

so

$$\mathbf{X} = (\mathbb{P}^1 \times \mathbb{P}^1) - \{[u] \in \mathbb{P}^1 \times \mathbb{P}^1 \mid \mathrm{tr}(u) = 0\}$$

identifies in $\mathbb{P}^1 \times \mathbb{P}^1$ as a dense open subvariety, with the corresponding open immersion

$$j : \mathbf{X} \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1.$$

2^0. Algebraic geometry provides us with a *contra*variant functor Pic from k-varieties to abelian groups having the following properties.

- On *affine* k-varieties, Pic is contra-equivalent to the covariant functor Pic from reduced k-algebras of finite type to abelian groups.

- There are canonical identifications

$$\mathrm{Pic}(\mathbb{P}^n) = \mathbb{Z}, \quad \mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{Z} \oplus \mathbb{Z}.$$

- $i^* := \mathrm{Pic}(i) : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ is the diagonal embedding.
- The ν-th projection $\pi_\nu : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ $(\nu = 1, 2)$ induces the ν-th coordinate embedding $\pi_\nu^* : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$.
- The top row of

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "i^*"'] & \mathbb{Z} \oplus \mathbb{Z} \arrow[r, "j^*"'] & \mathrm{Pic}(k[\mathbf{X}]) \arrow[r] & 0 \\ & & \mathbb{Z} \arrow[u, "\pi_\nu^*"] & & \end{tikzcd} \tag{15}$$

  is exact.

Hence $\mathrm{Pic}(k[\mathbf{X}]) \cong (\mathbb{Z} \oplus \mathbb{Z})/\mathrm{Diag}(\mathbb{Z} \oplus \mathbb{Z}) \cong \mathbb{Z}$ is a free abelian group of rank 1 generated by $j^*(1 \oplus 0)$.
3^0. Now consider the morphism $\varphi := \pi_1 \circ j : \mathbf{X} \to \mathbb{P}^1$. It follows from (15) and [3, II Thm. 7.1] that

$$L := \varphi^* \mathcal{O}_{\mathbb{P}^1}(1) = j^* \circ \pi_1^*(1) = j^*(1 \oplus 0)$$

is a line bundle on two generators over $k[\mathbf{X}]$, so Prop. 5.5 combines with (14) to yield an elementary idempotent $c \in M_2(k[\mathbf{X}])$ such that

$$L \cong L_c \cong L_e \otimes_{k[\mathbf{X}]} k[\mathbf{X}]^{\langle c \rangle}.$$

Since $[L]$ generates $\mathrm{Pic}(k[\mathbf{X}])$ by 2^0, the natural map (cf. 4.2 d))

$$\mathbb{Z} \cong \mathrm{Pic}(k[\mathbf{X}]) \longrightarrow \mathrm{Pic}(k[\mathbf{X}]^{\langle c \rangle}) = \mathrm{Pic}(k[\mathbf{X}]) \cong \mathbb{Z},$$

which sends $[L_e]$ to $[L]$, is surjective, hence an isomorphism, and the proof is complete. $\square$

7.5. Remark. a) A result considerably more general than Thms. 7.3, 7.4 above, dealing with flag schemes and $\mathbf{GL}_n$-torsors, may be found in Demazure-Gabriel [2, III §4 no. 7].
b) For a generalization of the aforementioned theorems in another direction, see Loos [6].

References

[1] N. Bourbaki, *Elements of mathematics. Commutative algebra*, Hermann, Paris, 1972. Translated from the French.

[2] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris, 1970. Avec un appendice *Corps de classes local* par Michiel Hazewinkel.

[3] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[4] M.-A. Knus, *Quadratic and Hermitian forms over rings*, vol. 294 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 1991. With a foreword by I. Bertuccioni.

[5] M.-A. Knus and M. Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. 389.

[6] O. Loos, *Remarks on "Idempotent* 2*-by-*2 *matrices" by Holger P. Petersson*, Preprint, (2007), pp. 1–9.

[7] O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, Bd. 117, Academic Press Inc., Publishers, New York, 1963.

[8] H. P. Petersson and M. L. Racine, *Albert algebras*, Springer-Verlag, In preparation.