ACTA ARITHMETICA
125.4 (2006)

Steinitz classes of central simple algebras

by

ANTHONY C. KABLE (Stillwater, OK),
HEATHER RUSSELL (Bowling Green, KY) and
NILABH SANAT (Bowling Green, KY)

1. Introduction. The Steinitz class of an extension of number fields is a familiar object of study. Numerous algebraic results concerning it are known, and recently ([2], [4]) density and distribution results have been obtained for suitable families of extensions. Our purpose here is to present analogous results for the case where the extension field is replaced by a central simple algebra over the base field. Since central simple algebras generally have several conjugacy classes of maximal orders, it is not obvious at first that a Steinitz class can be defined in this setting. However, it emerges (see Corollary 3.2) that all maximal orders are isomorphic as modules over the integers of the base field, and so we may define the Steinitz class of a central simple algebra to be the common Steinitz invariant of these modules. Next we determine (see Proposition 3.5) precisely which classes may appear as Steinitz classes of central simple algebras. In Section 4, we find the asymptotic frequency with which each of these possible classes occurs as the algebra is varied in the family of central division algebras with fixed dimension and fixed splitting type at infinity, ordered by the norm of the discriminant. The distribution of Steinitz classes is not generally uniform, but is so in some cases, including that of algebras of prime degree. The possible non-uniformity is demonstrated in the last section by giving a specific example.

2. Notation. We begin by introducing our notation for arithmetical objects. Let k be a number field, $\mathcal{O}$ the ring of integers of k, and $\mathfrak{M}$, $\mathfrak{M}_{\mathrm{f}}$, $\mathfrak{M}_\infty$, $\mathfrak{M}_{\mathrm{r}}$, $\mathfrak{M}_{\mathrm{c}}$, the set of all places, finite places, infinite places, real places,

2000 *Mathematics Subject Classification*: Primary 16H05; Secondary 11R52, 16K20, 11R45.

Key words and phrases: Steinitz class, central simple algebra, asymptotic distribution.
The first-named author was partially supported by NSF grant DMS-0244741.

and complex places of k, respectively. Let k_v be the localization of k at v. If $v \in \mathfrak{M}_{\mathrm{f}}$ then let $\mathcal{O}_v$ be the ring of integers of k_v, $\mathcal{P}_v$ the maximal ideal of $\mathcal{O}_v$, $\varpi_v \in \mathcal{P}_v$ a generator, q_v the cardinality of $\mathcal{O}_v/\mathcal{P}_v$, and $\mathfrak{p}_v = \mathcal{P}_v \cap \mathcal{O}$. If $\mathfrak{a}$ is an ideal of $\mathcal{O}$ then we shall write $\mathcal{N}(\mathfrak{a}) \in \mathbb{N}$ for the absolute ideal norm of $\mathfrak{a}$, that is, the cardinality of the ring $\mathcal{O}/\mathfrak{a}$.

Let $\mathbb{A}^\times$ be the group of ideles of k and write

$$\mathbb{A}_0^\times = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \mathcal{O}_v^\times, \qquad \mathbb{A}_\infty^\times = \prod_{v\in\mathfrak{M}_\infty} k_v^\times .$$

It is well known that the ideal class group $\mathrm{Cl}(k)$ of k may be identified with the group

$$\mathbb{A}^\times/(k^\times \cdot \mathbb{A}_\infty^\times \cdot \mathbb{A}_0^\times)$$

and we shall make this identification here. The class group may equally be identified with the Picard group of $\mathcal{O}$, that is, the group of isomorphism classes of rank one projective $\mathcal{O}$-modules under the operation induced by the tensor product. If M is a finitely generated torsion-free $\mathcal{O}$-module of rank r then the class of the module $\bigwedge^r M$ in $\mathrm{Cl}(k)$ is called the *Steinitz invariant* of M and denoted by $S(M)$.

Next we introduce notation and terminology pertaining to central simple algebras. Let K be a field. Whenever we consider a K-algebra, it is assumed to be finite-dimensional over K. Let A be a central simple K-algebra. Then $\dim_K(A)$ is a square and we refer to $\deg(A) = \sqrt{\dim_K(A)}$ as the *degree* of A. There is a division algebra D over K and an integer κ such that $A \cong \mathrm{M}(\kappa, D)$. We call $\mathrm{ind}(A) = \sqrt{\dim_K(D)}$ the *index* of A, $\mathrm{con}(A) = \kappa$ the *content* of A, and D the *spine* of A.

Now suppose that A is a central simple algebra over a number field k of degree m and let $n = m^2$. By an *order* in A we shall always mean an $\mathcal{O}$-order, that is, a subring of A sharing the same unit element that is also an $\mathcal{O}$-lattice in A. We refer to [8] for the basic theory of such orders. If R is an order in A then we let $\mathrm{disc}(R)$ denote its discriminant [8, p. 126]. Given any set of elements $x_1, \dots, x_n$ we define

$$\mathrm{disc}(x_1, \dots, x_n) = \det[\mathrm{tr}(x_i x_j)],$$

where tr denotes the reduced trace in A [8, p. 116].

3. The Steinitz class of a central simple algebra. In order to define the Steinitz class of a central simple algebra, we first require the following analogue of the famous result of Emil Artin [1] that describes the Steinitz class of an extension of a number field.

PROPOSITION 3.1 (Artin's theorem). *Let $a_1, \dots, a_n$ be a k-basis for a central simple k-algebra A and R an order in A. Then there is a fractional* *ideal* $\mathfrak{a}$ *such that*

$$\operatorname{disc}(R) = (\operatorname{disc}(a_1, \ldots, a_n))\mathfrak{a}^2$$

and we have $S(R) = [\mathfrak{a}]$.

Proof. We first recall the correspondence of elements of the Picard group of $\mathcal{O}$ with classes in $\mathrm{Cl}(k)$. Let N be a rank one projective $\mathcal{O}$-module. Then $k \otimes_{\mathcal{O}} N$ is a one-dimensional k-vector space and we choose a basis a for it. For each $v \in \mathfrak{M}_{\mathrm{f}}$, $N_v = \mathcal{O}_v \otimes_{\mathcal{O}} N$ is a free $\mathcal{O}_v$-module of rank one and we choose a basis r_v for it. For each $v \in \mathfrak{M}_{\mathrm{f}}$, we may regard both a and r_v as elements of the one-dimensional k_v-vector space

$$k_v \otimes_k (k \otimes_{\mathcal{O}} N) \cong k_v \otimes_{\mathcal{O}_v} N_v$$

and then choose $x_v \in k_v^\times$ such that $r_v = x_v a$. The idele x with component x_v at $v \in \mathfrak{M}_{\mathrm{f}}$ and component 1 at $v \in \mathfrak{M}_\infty$ represents $S(N)$ in $\mathrm{Cl}(k)$.

We apply the preceding discussion to $N = \bigwedge^n R$. For each $v \in \mathfrak{M}_{\mathrm{f}}$, we may choose an $\mathcal{O}_v$-basis $r_{1,v}, \ldots, r_{n,v}$ for R_v. Let $g_v \in \mathrm{Aut}(k_v \otimes_k A)$ be the element that satisfies $g_v(a_i) = r_{i,v}$ for $1 \leq i \leq n$. Define $a = a_1 \wedge \cdots \wedge a_n$ and $r_v = r_{1,v} \wedge \cdots \wedge r_{n,v}$ and note that $(\bigwedge^n g_v)(a) = r_v$. This equation may be written as $\det(g_v)a = r_v$ and it follows that the idele with components $x_v = \det(g_v)$ for $v \in \mathfrak{M}_{\mathrm{f}}$ and $x_v = 1$ for $v \in \mathfrak{M}_\infty$ represents the class of $S(R)$. On the other hand, from the basic properties of the discriminant we get the equation

$$\operatorname{disc}(R)_v = (\operatorname{disc}(r_{1,v}, \ldots, r_{n,v})) = (\operatorname{disc}(a_1, \ldots, a_n))(x_v^2)$$

for all $v \in \mathfrak{M}_{\mathrm{f}}$. Thus we need only let $\mathfrak{a}$ be the fractional ideal corresponding to the idele x. ∎

In contradistinction to the number field case, there may be more than one conjugacy class of maximal orders in a given central simple k-algebra. However, we are now in a position to show that all these maximal orders are isomorphic to one another as $\mathcal{O}$-modules. This is the crucial fact that allows us to define the Steinitz class of a central simple k-algebra.

COROLLARY 3.2. *Let A be a central simple algebra over a number field k and R and R' maximal orders of A. Then $S(R) = S(R')$.*

Proof. It is known that $\operatorname{disc}(R) = \operatorname{disc}(R')$ [8, Theorem 25.3] and the claim follows at once from this and Proposition 3.1. ∎

DEFINITION 3.3. The *Steinitz class* $\mathrm{St}(A)$ of a central simple algebra A over a number field is the Steinitz invariant of any maximal order in A.

Let A be a central simple k-algebra of degree m. If $v \in \mathfrak{M}$ then $A_v = k_v \otimes_k A$ is a central simple k_v-algebra and we write κ_v for its capacity and l_v for its index. Note that $m = \kappa_v l_v$ for all v. We have in addition a Hasse invariant $\mathrm{inv}(A_v) \in \mathbb{Q}/\mathbb{Z}$ for each v (see [8, equation (31.7)]). We shall write

$\mathrm{inv}_v(A)$ rather than $\mathrm{inv}(A_v)$ for this invariant below. If D_v is the spine of A_v then $\mathrm{inv}_v(A) = \mathrm{inv}(D_v)$ and this invariant has the form $[s_v/l_v]$ with $\gcd(s_v, l_v) = 1$. The invariant may be rewritten as $\mathrm{inv}_v(A) = [t_v/m]$ if we define $t_v = s_v\kappa_v$. In terms of t_v, we have $\kappa_v = \gcd(t_v, m)$. It is known [8, Theorem 32.1] that the discriminant of any maximal order in A is given by the expression

$$D(A) = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \mathfrak{p}_v^{m(l_v-1)\kappa_v}.$$

In terms of the notation just introduced, this may also be written as

$$D(A) = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \mathfrak{p}_v^{m(m-\gcd(t_v,m))}. \tag{1}$$

PROPOSITION 3.4. *With notation and hypotheses as above, we have*

$$\mathrm{St}(A) = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} [\mathfrak{p}_v]^{m(m-\gcd(t_v,m))/2}.$$

Proof. Choose a basis $a_1, \ldots, a_n$ for the algebra A over k and write

$$\delta = \mathrm{disc}(a_1, \ldots, a_n).$$

By Theorem 1.3 of [5], we have $\delta = \pm c^2$ for some $c \in k^\times$ (the sign is made precise in Lewis' result, but we do not need it). Note that every exponent in (1) is even and hence we may define an ideal in $\mathcal{O}$ by

$$\mathfrak{b} = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \mathfrak{p}_v^{m(m-\gcd(t_v,m))/2},$$

so that $\mathfrak{b}^2 = D(A)$. By Proposition 3.1 there is a fractional ideal $\mathfrak{a}$ such that $D(A) = (\delta)\mathfrak{a}^2$ and $\mathrm{St}(A) = [\mathfrak{a}]$. The former equation is equivalent to $\mathfrak{b}^2 = (c)^2\mathfrak{a}^2$ and, by unique factorization, this implies that $\mathfrak{b} = (c)\mathfrak{a}$. Thus $\mathrm{St}(A) = [\mathfrak{a}] = [(c^{-1})\mathfrak{b}] = [\mathfrak{b}]$, as claimed. ∎

Our next task is to determine precisely which classes in $\mathrm{Cl}(k)$ can appear as the Steinitz class of a central simple algebra of degree m. Recall that, by Hasse's theorem [7, Propositions 18.7a and 18.7b], the isomorphism classes of central simple k-algebras of degree m are in one-to-one correspondence with sequences $\{i_v\}_{v\in\mathfrak{M}}$ in $\mathbb{Q}/\mathbb{Z}$ such that $i_v = 0$ for all but finitely many v, $i_v = 0$ for all $v \in \mathfrak{M}_{\mathrm{c}}$, $2i_v = 0$ for all $v \in \mathfrak{M}_{\mathrm{r}}$, $\sum_{v\in\mathfrak{M}} i_v = 0$, and $mi_v = 0$ for all v.

If m is a natural number then we define

$$\alpha(m) = \gcd_{0\le t\le m-1} (m - \gcd(t, m)).$$

We note that $\alpha(m) = 1$ if m is even and that $\alpha(m)$ is even if m is odd. If m is a power of the prime number p then $\alpha(m) = p - 1$. One may verify that

$$\alpha(m_1m_2) = \gcd(\alpha(m_1), \alpha(m_2))$$

for any natural numbers m_1 and m_2, from which it follows that

$$\alpha(m) = \gcd_{p|m}(p-1).$$

This formula and Dirichlet's theorem on primes in an arithmetic progression easily imply that every even natural number lies in the range of α.

It is convenient to be able to fix the splitting type of the central simple algebras under consideration at all infinite places and we now introduce terminology to do so. We define an *infinity type* to be a choice of $\tau_v \in \mathbb{Q}/\mathbb{Z}$ for each $v \in \mathfrak{M}_\infty$ in such a way that $\tau_v = 0$ for all $v \in \mathfrak{M}_\mathrm{c}$ and $2\tau_v = 0$ for all $v \in \mathfrak{M}_\mathrm{r}$. Any central simple k-algebra A gives rise to an infinity type $\tau(A)$ by setting $\tau(A)_v = \mathrm{inv}_v(A)$ for all $v \in \mathfrak{M}_\infty$. If τ is any infinity type then we define $\varepsilon(\tau) = \sum_{v\in\mathfrak{M}_\infty} \tau_v$. Given a positive natural number m, we say that an infinity type τ is *compatible with* m if m is even or if m is odd and $\tau_v = 0$ for all $v \in \mathfrak{M}_\infty$.

PROPOSITION 3.5. *Let m be a positive natural number and τ a compatible infinity type. Then we have*

$$\{\mathrm{St}(A) \mid \deg(A) = m,\, \tau(A) = \tau\} = \mathrm{Cl}(k)^{m\alpha(m)/2}.$$

The equality remains true if we also restrict A to be a division algebra.

Proof. In the exceptional case where $m = 1$, the claim is true by inspection. We now assume that $m \geq 2$. Since $\alpha(m) \mid (m - \gcd(t,m))$ for all natural numbers t, the expression for $\mathrm{St}(A)$ given in Proposition 3.4 makes it clear that $\mathrm{St}(A)$ always lies in $\mathrm{Cl}(k)^{m\alpha(m)/2}$.

To prove the reverse inclusion, let $C \in \mathrm{Cl}(k)$. By the definition of α, we may choose integers $b_1, \ldots, b_{m-1}$ such that

$$\sum_{t=1}^{m-1} b_t(m - \gcd(t,m)) = \alpha(m).$$

By the Prime Ideal Theorem for Classes [6, Corollary 4 to Proposition 7.17], we may choose distinct $v_1, \ldots, v_{m-1} \in \mathfrak{M}_\mathrm{f}$ such that $[\mathfrak{p}_{v_t}] = C^{b_t}$ for $1 \leq t \leq m-1$. We may also choose a place $w \in \mathfrak{M}_\mathrm{f}$ such that $w \notin \{v_1, \ldots, v_{m-1}\}$ and $[\mathfrak{p}_w]$ is trivial in $\mathrm{Cl}(k)$. Consider the sequence $\{i_v\}_{v\in\mathfrak{M}}$ in $\mathbb{Q}/\mathbb{Z}$ given by $i_v = 0$ if $v \notin \{v_1, \ldots, v_{m-1}, w\} \cup \mathfrak{M}_\infty$, $i_{v_t} = [t/m]$ for $1 \leq t \leq m-1$, $i_v = \tau_v$ for $v \in \mathfrak{M}_\infty$, and

$$i_w = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ [\varepsilon(\tau) + 1/2] & \text{if } m \text{ is even.} \end{cases}$$

This sequence satisfies the requirements of Hasse's theorem and hence there is a central simple k-algebra A of degree m such that $\mathrm{inv}_v(A) = i_v$ for all

$v \in \mathfrak{M}$. By Proposition 3.4, we have

$$\begin{aligned}\mathrm{St}(A) &= \prod_{v\in\mathfrak{M}_{\mathrm{f}}} [\mathfrak{p}_v]^{m(m-\gcd(t_v,m))/2} = \prod_{t=1}^{m-1} [\mathfrak{p}_{v_t}]^{m(m-\gcd(t,m))/2} \\ &= \prod_{t=1}^{m-1} C^{mb_t(m-\gcd(t,m))/2} = C^{m\alpha(m)/2}.\end{aligned}$$

This establishes the reverse inclusion. For the last claim, note that the A with $\mathrm{St}(A) = C^{m\alpha(m)/2}$ that was just constructed is a division algebra, since A_{v_1} has index m equal to its degree and is therefore a division algebra. ∎

Corollary 3.6. *Let k be a number field, e the exponent of* $\mathrm{Cl}(k)$, *and m a natural number. Then all maximal orders in central simple k-algebras of degree m are free $\mathcal{O}$-modules if and only if e divides $m\alpha(m)/2$.*

Proof. Indeed, the condition holds if and only if $\mathrm{St}(A)$ is the trivial class for all such k-algebras A. By Proposition 3.5, this happens if and only if $\mathrm{Cl}(k)^{m\alpha(m)/2}$ is trivial. ∎

Note that it also follows from Proposition 3.5 that every class in $\mathrm{Cl}(k)$ is representable as the Steinitz class of a quaternion algebra over k and that, among central simple algebras, quaternion algebras are the only ones that have this property in general.

4. Asymptotic distribution of Steinitz classes. We wish to refine Proposition 3.5 by considering how $\mathrm{St}(A)$ varies as A varies over algebras of a given degree $m \geq 2$ and compatible infinity type τ, fixed in the ensuing discussion. Because the most natural analogue of an extension field of k in this setting is a central division algebra over k, rather than a general central simple algebra over k, it is most interesting to study this distribution when A is additionally restricted to be a division algebra.

Let A be a central simple k-algebra of degree m and write the local invariant of A at a place v in the form $\mathrm{inv}_v(A) = [t_v/m]$ with $0 \leq t_v \leq m-1$. It follows from [8, Theorem 32.19] that the content of A is given by

$$\mathrm{con}(A) = \gcd_{v\in\mathfrak{M}}(t_v, m).$$

In particular, A is a division algebra if and only if $\gcd_{v\in\mathfrak{M}}(t_v)$ is relatively prime to m.

With $m \geq 2$ and a compatible infinity type τ fixed, we write $\varepsilon = \varepsilon(\tau)$, $\beta(m) = m\alpha(m)/2$, $\gamma(t) = m - \gcd(t, m)$, and $G_m = \mathrm{Cl}(k)^{\beta(m)}$. Let P be the set of primes that divide m. If $S \subset P$ and t is an integer then we shall write $S \mid t$ to mean that $p \mid t$ for all $p \in S$. For any $S \subset P$, let $\mathcal{A}[S]$ be the set of isomorphism classes of central simple k-algebras of degree m and infinity type τ such that $S \mid t_v$ for all $v \in \mathfrak{M}$. Note that $\mathcal{A}[\emptyset]$ is the set of all central simple k-algebras of degree m and infinity type τ and

$$\widehat{\mathcal{A}} = \mathcal{A}[\emptyset] - \bigcup_{p\in P} \mathcal{A}[\{p\}]$$

is the subset of $\mathcal{A}[\emptyset]$ consisting of the division algebras. It is possible that $\mathcal{A}[S] = \emptyset$. This occurs precisely when m is exactly divisible by 2, $2 \in S$, and $\tau_v \neq 0$ for some $v \in \mathfrak{M}_{\mathrm{r}}$. We shall say that S is *incompatible with* τ if these conditions hold, and that S is *compatible with* τ otherwise.

For χ a character of G_m and $S \subset P$ we consider the formal Dirichlet series

$$\Phi(s,\chi;S) = \sum_{A\in\mathcal{A}[S]} \frac{\chi(\mathrm{St}(A))}{\mathcal{N}(D(A))^s}.$$

Note that $\Phi(s,\chi;S) = 0$ if S is incompatible with τ. In order to reexpress $\Phi(s,\chi;S)$ when S is compatible with τ, we introduce the character ψ of $\mathbb{Z}/m\mathbb{Z}$ defined by $\psi(x) = \exp(2\pi i x/m)$. For each $v \in \mathfrak{M}_{\mathrm{f}}$ and $a \in \mathbb{Z}$ define

$$\begin{aligned} F_v(s,\chi,a;S) &= \sum_{0\le t\le m-1,\, S\mid t} \psi(at)\chi([\mathfrak{p}_v]^{m\gamma(t)/2})q_v^{-m\gamma(t)s}, \\ F(s,\chi,a;S) &= \prod_{v\in\mathfrak{M}_{\mathrm{f}}} F_v(s,\chi,a;S). \end{aligned}$$

LEMMA 4.1. *If S is compatible with τ then*

$$\Phi(s,\chi;S) = \frac{1}{m}\sum_{a=0}^{m-1} \psi(am\varepsilon)F(s,\chi,a;S).$$

Proof. Suppose that S is compatible with τ. By Hasse's theorem, (1), and Proposition 3.4, we may express $\Phi(s,\chi;S)$ in the form

$$\Phi(s,\chi;S) = \sum_{(t_v)} \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \chi([\mathfrak{p}_v]^{m\gamma(t_v)/2})q_v^{-m\gamma(t_v)s},$$

where the sum is over all sequences $(t_v)_{v\in\mathfrak{M}_{\mathrm{f}}}$ such that $t_v = 0$ for all but finitely many v, $0 \le t_v \le m-1$ for all v, $S \mid t_v$ for all v, and

$$\sum_{v\in\mathfrak{M}_{\mathrm{f}}} t_v + m\varepsilon \equiv 0 \pmod{m}.$$

This, in turn, may be expressed as

$$\Phi(s,\chi;S) = \frac{1}{m}\sum_{a=0}^{m-1} \psi(am\varepsilon) \sum_{(t_v)} \prod_{v\in\mathfrak{M}_{\mathrm{f}}} \psi(at_v)\chi([\mathfrak{p}_v]^{m\gamma(t_v)/2})q_v^{-m\gamma(t_v)s},$$

where the inner sum is over all sequences $(t_v)_{v\in\mathfrak{M}_{\mathrm{f}}}$ such that $t_v = 0$ for all but finitely many v, $0 \le t_v \le m-1$ for all v, and $S \mid t_v$ for all v. By the standard argument from unique factorization, the inner sum is precisely $F(s,\chi,a;S)$. ∎

The set of characters of the group G_m may be identified with the set of characters of $\mathrm{Cl}(k)$ that are trivial on $\mathrm{Cl}(k)[\beta(m)] = \{C \in \mathrm{Cl}(k) \mid C^{\beta(m)} = C_0\}$, where C_0 denotes the trivial class. This identification is made by associating a character χ' of $\mathrm{Cl}(k)$ that is trivial on $\mathrm{Cl}(k)[\beta(m)]$ with the character χ of G_m defined by $\chi(C) = \chi'(C')$, where $C' \in \mathrm{Cl}(k)$ is any element such that $(C')^{\beta(m)} = C$. If χ' is a character of $\mathrm{Cl}(k)$ then the identification of $\mathrm{Cl}(k)$ with $\mathbb{A}^\times/(k^\times \cdot \mathbb{A}_\infty^\times \cdot \mathbb{A}_0^\times)$ allows us to regard χ' as an unramified idele class character of k. For any such character we define

$$L(s,\chi') = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1-\chi'_v(\varpi_v)q_v^{-s})^{-1},$$

where χ'_v is the component of χ' at v. As is conventional, we write $\zeta_k(s)$ for $L(s,\chi')$ when χ' is the trivial character. Denote by ϱ_0 the residue of $\zeta_k(s)$ at $s=1$.

In the following, we assume that $0 \le t \le m-1$. Let $\gamma_0 < \gamma_1 < \cdots < \gamma_k$ be the distinct values of $\gamma(t)$. We have $\gamma_0 = \gamma(0) = 0$ and $\gamma_1 = \gamma(m/p_1) = m-(m/p_1)$, where p_1 is the least prime dividing m. Note that $\gamma(t) = \gamma_i$ if and only if $\gcd(t,m) = m-\gamma_i$, and that t has this property if and only if $t = (m-\gamma_i)r$ with $\gcd(r, m/(m-\gamma_i)) = 1$. If $S \subset P$ then define

$$I(S) = \{i \mid \gamma(t) = \gamma_i \text{ for some } t \text{ such that } S \,|\, t\} - \{0\}.$$

Note if $S\,|\,t$ and $\gamma(t) = \gamma(t')$ then $S\,|\,t'$. Thus if we define

$$c_i(a) = \sum_{\{t \,|\, \gamma(t)=\gamma_i\}} \psi(at)$$

then we may write

$$F_v(s,\chi,a;S) = 1 + \sum_{i\in I(S)} c_i(a)\chi([\mathfrak{p}_v]^{\beta(m)})^{\gamma_i/\alpha(m)} q_v^{-m\gamma_i s}. \tag{2}$$

In fact, the $c_i(a)$ are Ramanujan sums [3, Section 16.6] and it is known that if $N_i = m/\gcd(m, a(m-\gamma_i))$ then

$$c_i(a) = \frac{\mu(N_i)\phi(m/(m-\gamma_i))}{\phi(N_i)},$$

where μ and ϕ are, respectively, the Möbius function and the Euler function [3, Theorem 272].

Lemma 4.2. *Let $\sigma_1 = 1/(m\gamma_1)$ and $S \subset P$. The Dirichlet series $F(s,\chi,a;S)$ converges absolutely in the open half-plane* $\mathrm{Re}(s) > \sigma_1$ *and has a meromorphic continuation to an open set containing the closed half-plane* $\mathrm{Re}(s) \ge \sigma_1$. *Its only possible singularity in this closed half-plane is a pole of order at most*

$p_1 - 1$ at the point $s = \sigma_1$. If $s = \sigma_1$ is a singularity of $F(s,\chi,a;S)$ then $\chi^{\gamma_1/\alpha(m)} = 1$, $p_1 \mid a$, $1 \in I(S)$, and we have

$$\begin{aligned}\lim_{s\to\sigma_1^+} &(s-\sigma_1)^{p_1-1} F(s,\chi,a;S)\\ &= \left(\frac{\varrho_0\sigma_1}{\zeta_k(2)}\right)^{p_1-1} \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-1})^{-(p_1-1)}\Big(1+(p_1-1)q_v^{-1}\\ &\quad + \sum_{i\in I(S)-\{1\}} c_i(a)\chi([\mathfrak{p}_v]^{\beta(m)})^{\gamma_i/\alpha(m)} q_v^{-\gamma_i/\gamma_1}\Big).\end{aligned}$$

Proof. The coefficient of $q_v^{-m\gamma_i s}$ in (2) is uniformly bounded in terms of m. In light of this, comparison with a suitable power of the series

$$\frac{\zeta_k(m\gamma_1 s)}{\zeta_k(2m\gamma_1 s)} = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-m\gamma_1 s})$$

establishes that $F(s,\chi,a;S)$ converges absolutely for $\mathrm{Re}(s) > \sigma_1$. If $1 \notin I(S)$ then a similar argument shows that $F(s,\chi,a;S)$ in fact converges absolutely for $\mathrm{Re}(s) > 1/(m\gamma_2)$ and so all the other claims are immediate. We shall assume henceforth that $1 \in I(S)$.

Let χ' be the character of $\mathrm{Cl}(k)$ corresponding to the character χ of G_m as explained above, so that $\chi([\mathfrak{p}_v]^{\beta(m)}) = \chi'([\mathfrak{p}_v])$. Define the Dirichlet series $\Psi(s,\chi,a;S)$ by

$$\Psi(s,\chi,a;S) = \left(\frac{L(m\gamma_1 s,(\chi')^{\gamma_1/\alpha(m)})}{L(2m\gamma_1 s,(\chi')^{2\gamma_1/\alpha(m)})}\right)^{-c_1(a)} F(s,\chi,a;S).$$

This Dirichlet series may be analyzed for convergence by the method just used for $F(s,\chi,a;S)$ and the result is that there is some $\sigma_2 < \sigma_1$ such that $\Psi(s,\chi,a;S)$ is absolutely convergent in the half-plane $\mathrm{Re}(s) > \sigma_2$. We have

$$F(s,\chi,a;S) = \left(\frac{L(m\gamma_1 s,(\chi')^{\gamma_1/\alpha(m)})}{L(2m\gamma_1 s,(\chi')^{2\gamma_1/\alpha(m)})}\right)^{c_1(a)} \Psi(s,\chi,a;S)$$

and so the analytic behavior of $F(s,\chi,a;S)$ in $\mathrm{Re}(s) \ge \sigma_1$ is controlled by that of the first factor on the right-hand side.

If p_1 does not divide a then $c_1(a) = -1$. This, and the standard analytic properties of the L-functions (as described in [6, Section 7.1]), imply that the first factor is regular on an open set containing $\mathrm{Re}(s) \ge \sigma_1$. Now suppose that p_1 does divide a, so that $c_1(a) = p_1 - 1$. The function $L(2m\gamma_1 s,(\chi')^{2\gamma_1/\alpha(m)})^{-1}$ is regular in the half-plane $\mathrm{Re}(s) > \sigma_1/2$. The function $L(m\gamma_1 s,(\chi')^{\gamma_1/\alpha(m)})$ is regular in the half-plane $\mathrm{Re}(s) \ge \sigma_1$ unless $(\chi')^{\gamma_1/\alpha(m)}$ is the trivial character. In this latter case, $L(m\gamma_1 s,(\chi')^{\gamma_1/\alpha(m)}) = \zeta_k(m\gamma_1 s)$ has a simple pole at $s = \sigma_1$ with residue $\varrho_0\sigma_1$ and no other singularities in the half-plane $\mathrm{Re}(s) \ge \sigma_1$. Under the assumption that $\chi^{\gamma_1/\alpha(m)}$ is trivial and p_1 divides a, we obtain

$$\lim_{s\to\sigma_1^+}(s-\sigma_1)^{p_1-1}F(s,\chi,a;S)=\left(\frac{\varrho_0\sigma_1}{\zeta_k(2)}\right)^{p_1-1}\varPsi(\sigma_1,\chi,a;S).$$

The formula given in the statement follows on expressing $\varPsi(\sigma_1,\chi,a;S)$ as a convergent Euler product. ∎

When $\chi^{\gamma_1/\alpha(m)}$ is trivial and p_1 divides a, let us define

$$R(\chi,a;S)=\lim_{s\to\sigma_1^+}(s-\sigma_1)^{p_1-1}F(s,\chi,a;S).$$

The statement of Lemma 4.2 gives an explicit expression for $R(\chi,a;S)$. Note that $R(\chi,a;S)=0$ unless $1\in I(S)$.

LEMMA 4.3. *Let $\sigma_1=1/(m\gamma_1)$ and $S\subset P$ be compatible with τ. The Dirichlet series $\varPhi(s,\chi;S)$ converges absolutely in the open half-plane* $\mathrm{Re}(s)>\sigma_1$ *and has a meromorphic continuation to an open set containing the closed half-plane* $\mathrm{Re}(s)\ge\sigma_1$. *Its only possible singularity in this closed half-plane is a pole of order at most p_1-1 at the point $s=\sigma_1$. If $s=\sigma_1$ is a singularity of $\varPhi(s,\chi;S)$ then $\chi^{\gamma_1/\alpha(m)}=1$ and we have*

$$\lim_{s\to\sigma_1^+}(s-\sigma_1)^{p_1-1}\varPhi(s,\chi;S)=\frac{1}{m}\sum_{\substack{0\le a\le m-1\\ p_1\mid a}}R(\chi,a;S).$$

Proof. If m is odd then $\varepsilon=0$. If m is even then $p_1=2$ and ε is either an integer or a half-integer. In either case, $\psi(am\varepsilon)=1$ when $p_1\mid a$. All the claims follow from this observation and the expression for $\varPhi(s,\chi;S)$ given in Lemma 4.1. ∎

Now define

$$\widehat{\varPhi}(s,\chi)=\sum_{A\in\widehat{\mathcal{A}}}\frac{\chi(\mathrm{St}(A))}{\mathcal{N}(D(A))^s}.$$

Since the sum here is restricted to division algebras, the inclusion-exclusion principle implies that

$$\widehat{\varPhi}(s,\chi)=\sum_{S\subset P}(-1)^{|S|}\varPhi(s,\chi;S). \tag{3}$$

By Lemma 4.3, this series converges absolutely in the open half-plane $\mathrm{Re}(s)>\sigma_1$ and has a meromorphic continuation to an open set containing the closed half-plane $\mathrm{Re}(s)\ge\sigma_1$. The only possible singularity of $\widehat{\varPhi}(s,\chi)$ in this closed half-plane is a pole of order at most p_1-1 at $s=\sigma_1$. If $s=\sigma_1$ is a singularity of $\widehat{\varPhi}(s,\chi)$ then $\chi^{\gamma_1/\alpha(m)}$ is the trivial character and we have

$$\lim_{s\to\sigma_1^+}(s-\sigma_1)^{p_1-1}\widehat{\varPhi}(s,\chi)=R(\chi),$$

where

$$R(\chi) = \frac{1}{m} \sum_{S \subset P} \sum_{\substack{0 \le a \le m-1 \\ p_1 | a}} (-1)^{|S|} R(\chi, a; S). \tag{4}$$

In connection with this formula, it might be worth pointing out that if S is incompatible with τ then $1 \notin I(S)$ and so $R(\chi, a; S) = 0$. Thus the zero terms in (3) are matched by zero terms in (4).

LEMMA 4.4. *We have $R(1) \neq 0$.*

Proof. The claim is equivalent to the claim that $\widehat{\Phi}(s, 1)$ has a pole of order $p_1 - 1$ at $s = \sigma_1$. Choose distinct finite places v_1 and v_2 and consider the set $\mathcal{A}'$ consisting of isomorphism classes of central simple k-algebras A of degree m and infinity type τ such that $\mathrm{inv}_{v_1}(A) = [1/m]$, $\mathrm{inv}_{v_2}(A) = [(m-1)/m]$, and if $v \in \mathfrak{M}_{\mathrm{f}} - \{v_1, v_2\}$ then either $\mathrm{inv}_v(A) = 0$ or $\mathrm{inv}_v(A) = [t_v/m]$ with $\gamma(t_v) = \gamma_1$. Since A_{v_1} is a division algebra for any such A, we have $\mathcal{A}' \subset \widehat{\mathcal{A}}$ and so

$$\widetilde{\Phi}(s) = \sum_{A \in \mathcal{A}'} \mathcal{N}(D(A))^{-s}$$

is a subseries of $\widehat{\Phi}(s, 1)$. Since the coefficients in the Dirichlet series $\widehat{\Phi}(s, 1)$ are all positive and it is known that this series has a pole of order at most $p_1 - 1$ at $s = \sigma_1$, it suffices to show that $\widetilde{\Phi}(s)$ has a pole of order $p_1 - 1$ at $s = \sigma_1$.

To do this, we repeat the analysis that was applied to $\Phi(s, 1; S)$ above for $\widetilde{\Phi}(s)$. Note that because $\mathrm{inv}_{v_1}(A) + \mathrm{inv}_{v_2}(A) = 0$, the condition on the invariants in Hasse's theorem is

$$\sum_{v \in \mathfrak{M}_{\mathrm{f}} - \{v_1, v_2\}} t_v + m\varepsilon \equiv 0 \pmod{m}.$$

This observation is necessary to obtain the analogue of Lemma 4.1. Also, the Euler factors at v_1 and v_2 are fixed, and the Euler factors at the other finite places do not contain the terms coming from γ_i with $i \geq 2$. This makes the analysis somewhat simpler. The result is that

$$\begin{aligned} \lim_{s \to \sigma_1^+} (s - \sigma_1)^{p_1 - 1} \widetilde{\Phi}(s) = \frac{1}{p_1} \left(\frac{\varrho_0 \sigma_1}{\zeta_k(2)} \right)^{p_1 - 1} \prod_{j=1}^{2} (1 + q_{v_j}^{-(m-1)/\gamma_1}) \\ \times \prod_{v \in \mathfrak{M}_{\mathrm{f}} - \{v_1, v_2\}} (1 + q_v^{-1})^{-(p_1 - 1)} (1 + (p_1 - 1) q_v^{-1}) \end{aligned}$$

and this quantity is visibly positive. ∎

THEOREM 4.5. *Let $m \geq 2$ and τ be a compatible infinity type. If $C \in \mathrm{Cl}(k)^{\beta(m)}$ then*

$$\lim_{X\to\infty} \frac{|\{A \mid \tau(A)=\tau,\, \mathrm{St}(A)=C,\, \mathcal{N}(D(A))\leq X\}|}{|\{A \mid \tau(A)=\tau,\, \mathcal{N}(D(A))\leq X\}|} = \frac{1}{|\mathrm{Cl}(k)^{\beta(m)}|}\sum_{\chi^{\gamma_1/\alpha(m)}=1}\chi^{-1}(C)\,\frac{R(\chi)}{R(1)},$$

where A runs over isomorphism classes of central division algebras over k of degree m, and the sum on the right-hand side is over all characters of $\mathrm{Cl}(k)^{\beta(m)}$ that satisfy the indicated condition.

Proof. Throughout the proof, let A stand for a division algebra with the properties enunciated in the statement. We have described the analytic properties of the Dirichlet series $\widehat{\Phi}(s,1)$ above. Given these properties, Ikehara's Tauberian theorem implies that there is a non-zero constant κ depending only on k, m, σ_1 and p_1 such that

$$|\{A \mid \tau(A)=\tau,\, \mathcal{N}(D(A))\leq X\}| \sim \kappa R(1) X^{\sigma_1}(\log(X))^{p_1-2}$$

as $X\to\infty$. Let $C\in \mathrm{Cl}(k)^{\beta(m)}$. In the half-plane $\mathrm{Re}(s)>\sigma_1$ we have

$$\sum_{A,\,\mathrm{St}(A)=C}\frac{1}{\mathcal{N}(D(A))^s} = \frac{1}{|\mathrm{Cl}(k)^{\beta(m)}|}\sum_{\chi}\chi^{-1}(C)\widehat{\Phi}(s,\chi),$$

where the sum is over all characters of $\mathrm{Cl}(k)^{\beta(m)}$. The analytic properties of this function follow from those of $\widehat{\Phi}(s,\chi)$ described above, and another application of Ikehara's Tauberian theorem gives

$$|\{A \mid \tau(A)=\tau,\, \mathrm{St}(A)=C,\, \mathcal{N}(D(A))\leq X\}| \sim \frac{\kappa}{|\mathrm{Cl}(k)^{\beta(m)}|}\Big(\sum_{\chi^{\gamma_1/\alpha(m)}=1}\chi^{-1}(C)R(\chi)\Big)X^{\sigma_1}(\log(X))^{p_1-2} \quad \text{as } X\to\infty.$$

These two asymptotic evaluations combine to give the required limit. ∎

For a given choice of m, τ and k, we shall say that the Steinitz class is *asymptotically uniformly distributed* in $\mathrm{Cl}(k)^{\beta(m)}$ with respect to $\mathcal{N}(D(A))$ if the limit that is evaluated in Theorem 4.5 is independent of the class $C\in \mathrm{Cl}(k)^{\beta(m)}$.

COROLLARY 4.6. *Let $m\geq 2$ and τ be a compatible infinity type. Suppose that $|\mathrm{Cl}(k)^{\beta(m)}|$ and $\gamma_1/\alpha(m)$ are relatively prime. Then the Steinitz class of central division algebras over k of degree m with $\tau(A)=\tau$ is asymptotically uniformly distributed in $\mathrm{Cl}(k)^{\beta(m)}$ with respect to $\mathcal{N}(D(A))$.*

Proof. Under these assumptions, the only character of $\mathrm{Cl}(k)^{\beta(m)}$ whose $\gamma_1/\alpha(m)$ power is trivial is the trivial character. Thus the sum over χ in Theorem 4.5 has only one term and the limit is independent of C. ∎

COROLLARY 4.7. *Let $m \geq 2$ be a prime and τ be a compatible infinity type. Then the Steinitz class of central division algebras over k of degree m with $\tau(A) = \tau$ is asymptotically uniformly distributed in* $\mathrm{Cl}(k)^{\beta(m)}$ *with respect to* $\mathcal{N}(D(A))$.

Proof. Since m is prime, we have $\alpha(m) = m - 1$ and $\gamma_1 = m - 1$. Thus $\gamma_1/\alpha(m) = 1$ and so the statement follows from the previous corollary. ∎

5. An example of non-uniform distribution. The results described so far leave open the possibility that the Steinitz class is always asymptotically uniformly distributed, because the right-hand side of the formula in Theorem 4.5 is in fact always independent of C. We show that this is not the case by sketching an example.

Let $m = 4$ and take $k = \mathbb{Q}(\sqrt{-14})$. This number field has no real places, so only one infinity type is possible, and $\mathrm{Cl}(k)$ is cyclic of order 4. We write $\mathrm{Cl}(k) = \{C_0, C_1, C_2, C_3\}$ with $C_j = C_1^j$. For $m = 4$ we have $\alpha(4) = 1$, $\beta(4) = 2$, $p_1 = 2$, $\gamma_1 = 2$, $\gamma_2 = 3$, $\sigma_1 = 1/8$, $c_2(0) = 2$, $c_2(2) = -2$, $I(\emptyset) = \{1, 2\}$, and $I(\{2\}) = \{1\}$. Thus $G_4 = \mathrm{Cl}(k)^2 = \{C_0, C_2\}$. We let χ_1 denote the trivial character of G_4 and χ_2 the non-trivial character. Also, set $\varrho = \varrho_0/(8\zeta_k(2))$.

The Steinitz class of a central division algebra of degree 4 over k may be either C_0 or C_2, and these classes occur, respectively, with asymptotic frequencies

$$\phi_1 = \frac{R(\chi_1) + R(\chi_2)}{2R(\chi_1)}, \qquad \phi_2 = \frac{R(\chi_1) - R(\chi_2)}{2R(\chi_1)}.$$

By definition,

$$R(\chi) = \frac{1}{4}\left(R(\chi, 0; \emptyset) + R(\chi, 2; \emptyset) - R(\chi, 0; \{2\}) - R(\chi, 2; \{2\})\right)$$

with

$$R(\chi, 0; \emptyset) = \varrho \prod_{v \in \mathfrak{M}_{\mathrm{f}}} (1 + q_v^{-1})^{-1}(1 + q_v^{-1} + 2\chi([\mathfrak{p}_v]^2)^3 q_v^{-3/2}),$$

$$R(\chi, 2; \emptyset) = \varrho \prod_{v \in \mathfrak{M}_{\mathrm{f}}} (1 + q_v^{-1})^{-1}(1 + q_v^{-1} - 2\chi([\mathfrak{p}_v]^2)^3 q_v^{-3/2})$$

and

$$R(\chi, 0; \{2\}) = R(\chi, 2; \{2\}) = \varrho \prod_{v \in \mathfrak{M}_{\mathrm{f}}} (1 + q_v^{-1})^{-1}(1 + q_v^{-1}) = \varrho.$$

We define the numbers

$$\xi_1 = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-1})^{-1}(1+q_v^{-1}+2q_v^{-3/2}),$$

$$\xi_2 = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-1})^{-1}(1+q_v^{-1}-2q_v^{-3/2}),$$

$$\xi_3 = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-1})^{-1}(1+q_v^{-1}+2\chi_2([\mathfrak{p}_v]^2)q_v^{-3/2}),$$

$$\xi_4 = \prod_{v\in\mathfrak{M}_{\mathrm{f}}} (1+q_v^{-1})^{-1}(1+q_v^{-1}-2\chi_2([\mathfrak{p}_v]^2)q_v^{-3/2}).$$

In terms of these numbers, we have

$$\phi_1 = \frac{\xi_1+\xi_2+\xi_3+\xi_4-4}{2(\xi_1+\xi_2-2)}, \qquad \phi_2 = \frac{\xi_1+\xi_2-\xi_3-\xi_4}{2(\xi_1+\xi_2-2)}.$$

A numerical calculation making use of the PARI package shows that $\phi_1 \approx 0.4430$ and $\phi_2 \approx 0.5570$. Thus the Steinitz class of a central division algebra of degree 4 over $k = \mathbb{Q}(\sqrt{-14})$ is not uniformly distributed with respect to the norm of the discriminant. Loosely speaking, the probability that such an algebra chosen at random will have maximal orders that are free as modules over $\mathcal{O} = \mathbb{Z}[\sqrt{-14}]$ is about 44.3%. It is interesting to note that, in this example, non-free maximal orders predominate over free ones.

References

[1] E. Artin, *Questions de base minimale dans la théorie des nombers algébriques*, in: Collected Papers, S. Lang and J. Tate (eds.), Addison-Wesley, Reading, MA, 1965, 229–231.
[2] E. Bekyel, *Steinitz classes and discriminant counting*, Acta Arith. 118 (2005), 27–40.
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.
[4] A. C. Kable and D. J. Wright, *Uniform distribution of the Steinitz invariants of quadratic and cubic extensions*, Compos. Math. 142 (2006), 84–100.
[5] D. W. Lewis, *Trace forms of central simple algebras*, Math. Z. 215 (1994), 367–375.
[6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin, 2004.
[7] R. S. Pierce, *Associative Algebras*, Springer, New York, 1982.
[8] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

Department of Mathematics
Oklahoma State University
Stillwater, OK 74078, U.S.A.
E-mail: akable@math.okstate.edu

Department of Mathematics
Western Kentucky University
Bowling Green, KY 42101, U.S.A.
E-mail: heather.russell@wku.edu
nilabh.sanat@wku.edu

Received on 20.6.2006
and in revised form on 24.8.2006 (5224)