1. Division Algebras

A **division ring** is a ring with 1 in which every nonzero element is invertible. Equivalently, the only one-sided ideals are the zero ideal and the whole ring. A **division algebra** over a field $K$ is just a division ring that is also a $K$-algebra. Every division ring is a division algebra over its center.

You may think of a division ring as a field with the axiom of commutativity removed; indeed, they are sometimes called “skew fields.” This line of thinking may lead you to hypothesize that division rings are more common—and harder to classify—than fields. On the other hand, you may only know one non-field division ring, the quaternions:

$$\mathbb{H} := \mathbb{R}(i, j : i^2 = j^2 = -1, ij = -ji).$$

(1)

Here, the angle brackets mean that $i$ and $j$ don’t necessarily commute with each other, but do commute with elements of $\mathbb{R}$. As it turns out, finite-dimensional division algebras can get a good deal more complicated than the quaternions. However, that complexity has a hard limit. For all of your favorite fields $K$, like number fields and function fields, finite-dimensional division algebras with center $K$ have been classified and described explicitly. That classification is the subject of these notes.

In Monday’s notes, we’ll first review some basic theorems about finite-dimensional simple algebras over a field. Then, we’ll give examples of division algebras, and give a construction that we’ll later show to give all finite-dimensional division algebras.

2. Notation

If $K$ is a field, then a **matrix algebra over** $K$ means $M_n(K)$ for some $n \geq 1$.

If $K$ is a field, then $K^{\text{alg}}$ denotes a fixed algebraic closure of $K$. $K^{\text{sep}}$ denotes the separable closure, the maximal separable extension of $K$ within $K^{\text{alg}}$.

If $K$ is a non-archimedian local field, then $K^{\text{nr}}$ denotes the maximal unramified extension within $K^{\text{alg}}$. These terms will be defined in detail later.

3. Central Simple Algebras

A **simple algebra** is a generalization of a division algebra. A division $K$-algebra may be characterized as a $K$-algebra with no one-sided ideals except for the zero ideal and the whole algebra. A simple $K$-algebra is a $K$-algebra with no two-sided ideals except for the zero ideal and the whole algebra.

A **central simple $K$-algebra** is a $K$-algebra with center $K$; a finite-dimensional central simple $K$-algebra will be called a **CSA** over $K$. The following theorem classifies CSAs and is proved in the appendix.

**Theorem 1.** [Wedderburn-Artin-Noether] Let $A$ be a finite-dimensional $K$-algebra. Then, the following are equivalent:

(a) $A$ is central simple.
(b) $A \otimes_K K_{\text{alg}}$ is isomorphic to a matrix algebra over $K_{\text{alg}}$.
(c) $A \otimes_K K_{\text{sep}}$ is isomorphic to a matrix algebra over $K_{\text{sep}}$.
(d) There is some finite extension $L/K$ such that $A \otimes_K L$ is isomorphic to a matrix algebra over $L$.
(e) There is some finite separable extension $L/K$ such that $A \otimes_K L$ is isomorphic to a matrix algebra over $L$.
(f) There is some finite Galois extension $L/K$ such that $A \otimes_K L$ is isomorphic to a matrix algebra over $L$.
(g) $A$ is isomorphic to a matrix algebra over a division algebra with center $K$.

**Corollary 2.** The dimension of a finitely-generated central simple $K$-algebra is a perfect square.

**Proof.** Let $A$ be a finitely-generated central simple $K$-algebra, and choose $L/K$ as in c. Then we have $A \otimes_K L \cong M_n(L)$. Taking the dimension of both sides over $K$, we get the formula $\dim_K(A) \dim_K(L) = n^2 \dim_K(L)$. In other words, $\dim_K(A) = n^2$. □

By criterion (g) of Theorem 1, a CSA is described by a division algebra $D$ and positive integer $n$. We may declare that we don’t care about $n$, and say that $M_n(D)$ and $M_m(D)$ are **Brauer equivalent**. A partial justification, and an observation that will be important later, is that tensor product preserves Brauer equivalence. This follows immediately from the fact that $M_{n_1}(D_1) \otimes M_{n_2}(D_2) \cong M_{n_1n_2}(D_1 \otimes D_2)$.

A better justification comes from **Morita equivalence**. Two rings $R$ and $S$ are Morita equivalent iff the categories mod-$R$ (right $R$-modules) and mod-$S$ (right $S$-modules) are equivalent (in the sense that there is an equivalence of categories between them). Morita equivalence of CSAs is the same as Brauer equivalence: A division algebra is Morita equivalent to matrix algebras over itself, and to nothing else.

4. **Generalized Quaternions**

We’ll give a few examples of division algebras. Let $K$ be a field with $\text{char} K \neq 2$, and $a, b \in K^\times$. Consider the following modest generalization of the quaternions:

$$D(a, b) := k\langle i, j : i^2 = a, j^2 = b, ij = -ji \rangle$$

**Proposition 3.** $D(a, b)$ is a simple algebra with center $K$.

**Proof.** Let $I$ be a nonzero two-sided ideal of $D(a, b)$, and choose some nonzero $x \in I$. Write $x = x_1 + x_2i + x_3j + x_4ij$ for $x_k \in K$. WLOG $x_1 \neq 0$; otherwise we can multiply $x$ by $i$, $j$, or $ij$ on the left so that this term is nonzero. It’s easy to check that

$$x = x_1 + x_2i + x_3j + x_4ij,$n_i^{-1} = x_1 + x_2i - x_3j - x_4ij,$

$$jxj^{-1} = x_1 - x_2i + x_3j - x_4ij,$

$$ijx(ij)^{-1} = x_1 - x_2i - x_3j + x_4ij.$$ 

Thus,

$$\frac{1}{4x_1}(x + ix_i^{-1} + jxj^{-1} + ijx(ij)^{-1}) = 1,$$

and therefore $1 \in I$ and $I = D$. So $D(a, b)$ is simple.

To find the center of $D(a, b)$, consider any $y = y_1 + y_2i + y_3j + y_4ij \in Z(D(a, b))$. The formula given above for conjugation by $i$ shows that $y_3 = 0$ and $y_4 = 0$. Conjugation by $j$ shows that $y_2 = 0$. Therefore, $Z(D(a, b)) = K$. □

**Proposition 4.** If $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0$ has a nonzero solution in $K$, then $D(a, b) \cong M_2(K)$. Otherwise, $D(a, b)$ is a division algebra over $K$. 
Proposition 5. Consider $x \in D(a, b)$, and write $x = x_1 + x_2i + x_3j + x_4k$ for $x_k \in K$. Define $\bar{x} = x_1 - x_2i - x_3j - x_4k$. Then,

\[ x\bar{x} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2. \]  

(5)

If $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0$ has a nonzero solution in $K$, then $D(a, b)$ has zero divisors and cannot be a division algebra, so $D(a, b) \cong M_2(K)$. If $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0$ does not have a nonzero solution in $K$, then every nonzero element of $D(a, b)$ is invertible, so $D(a, b)$ is a division algebra.

5. Crossed Products

Suppose $\sqrt{a} \notin K$. The construction of the generalized quaternions $D(a, b)$ from $K$ may be done in two stages. First, consider the field extension $L = K(i)$, where $i^2 = a$. Then, introduce a new variable $j$ that acts by Galois conjugation $(x + iy)j = j(x - iy)$, and so that $j^2 = b$.

This construction may be generalized to arbitrary Galois extensions. Before giving the general construction, we’ll do one more specific example, our first 9-dimensional division algebra. Consider the field $L = \mathbb{Q}(\alpha)$, where $\alpha = 2 \cos \left(\frac{2\pi}{7}\right)$. The Galois group $\text{Gal}(L/\mathbb{Q})$ is cyclic of order 3; write $\text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$ such that $\alpha^\sigma = 2 \cos \left(\frac{4\pi}{7}\right) = \alpha^2 - 2$. Set $D = L \oplus uL \oplus u^2L$, and define a multiplication of $D$ by $\ell u = u\ell^\sigma$ for $\ell \in L$, and $u^3 = 5$.

Exercise 1. $D$ is a division algebra over $\mathbb{Q}$. Moreover, $D \otimes \mathbb{R} \cong M_3(\mathbb{R})$; $D \otimes \mathbb{Q}_5$ and $D \otimes \mathbb{Q}_7$ are division algebras over $\mathbb{Q}_5$ and $\mathbb{Q}_7$, respectively; and $D \otimes \mathbb{Q}_p \cong M_3(\mathbb{Q}_p)$ for other primes $p$. (These claims will be easier to prove later, but thinking about them now may be beneficial.)

Okay, now for the general construction of a crossed product. The input to the construction will be a Galois extension $L/K$ with Galois group $G = \text{Gal}(L/K)$ and a 2-cocycle $t$ in Galois cohomology $H^2(G, L^\times)$, that is, a function $t : G^2 \to L^\times$ obeying the relation

\[ t(gh, k)t(g, h)^k = t(g, hk)t(h, k). \]

(6)

(The Galois cohomology groups will be defined in full generality and their importance justified in Tuesday’s notes.) As a right $L$-vector space, we’ll have $A = L^{[L:K]}$, but we write

\[ A = \bigoplus_{g \in G} u_g L. \]

(7)

The multiplication on $A = A(L/K, t)$ is then defined as

\[ (u_g \ell)(u_h m) = u_{gh} t(g, h) \ell^h m \]

(8)

Exercise 2. Show that the 2-cocycle condition of $t$ is equivalent to the associativity of multiplication in $A$.

Exercise 3. Show that $u_1 t(1, 1)^{-1}$ is the (unique, two-sided) identity for $A$. Also compute the two-sided inverse $(u_g \ell)^{-1}$.

By applying a “diagonal” change of basis to our algebra,

\[ u'_g = u_g t(1, 1)^{-1}, \]

\[ t'(g, h) = t(g, h) t(1, 1)^{-h-1}, \]

(9)

we have $u'_1 = 1$ and $A(L/K, t) \cong A(L/G, t')$. In other words, we may assume WLOG that $u_1 = 1$, and we’ll do so from now on.

Proposition 5. The crossed product $A = A(L/K, t)$ is simple, and $Z(A) = K$. 

Moreover, Exercise 4.

So, for all \( x \in L \),

\[
  z = \sum_{g \in G} u_g z_g.
\]

Proof. Suppose \( z \in Z(A) \). For some \( z_g \in L \),

\[
  z = \sum_{g \in G} u_g z_g.
\]

Thus, the coefficients \( x^g z_g = x z_g \) for all \( x \in L \), and thus \( z_g = 0 \) for all \( g \neq 1 \). That is, \( z \in L \). Moreover, for all \( g \in G \), \( u_g z = z u_g = u_g z^g \), and since the \( u_g \) are invertible, \( z = z^g \).

That is, \( z \in K \). On the other hand, any element of \( K \) is obviously central, so \( Z(A) = K \).

To prove \( A \) is simple, consider a nonzero two-sided ideal \( I \) of \( A \). Choose an element \( 0 \neq a \in A \) whose expression

\[
  a = \sum_g u_g \ell_g
\]

has the minimum possible number of nonzero coefficients \( \ell_g \). WLOG we may assume \( \ell_1 \neq 0 \), because otherwise we can multiply on the left by some \( u_g^{-1} \) to make it so. For any \( \ell \in L \),

\[
  a \ell - \ell a = \sum_g u_g \ell_g (\ell - \ell^g),
\]

and of course \( a \ell - \ell a \in I \). This element has fewer nonzero coefficients than \( a \) because the \( u_1 \) coefficient vanishes, and so \( a \ell - \ell a = 0 \). Thus, each \( \ell_g (\ell - \ell^g) = 0 \). For \( g \neq 1 \), there is some \( \ell \in L \) so that \( \ell - \ell^g \neq 0 \), so \( \ell_g = 0 \). Hence, \( a = u_1 \ell_1 = \ell_1 \) is in \( L \) and, in particular, invertible. So \( I = A \). Therefore, \( A \) is simple.

Amazingly, this construction builds all CSAs over \( K \) up to Brauer equivalence; we’ll prove this tomorrow. We’ll also show that 2-coboundaries in Galois cohomology define isomorphisms of central simple algebras. Therefore, central simple algebras over \( K \) containing \( L \) as a maximal subfield are in bijection with the elements of the abelian group \( H^2(G, L^\times) \). The group operation on this set of algebras will be described in a much more direct manner in the next section of these notes.

We’ll do one more example to show how a crossed product may arise in nature. If \( \Gamma \) is a finite group and \( K \) is a field of characteristic zero, then \( K\Gamma \) is semisimple, and so its direct summands (the finite dimensional irreducible representation of \( \Gamma \)) are matrix algebras over division rings. Consider the 63-element group \( \Gamma = C_9 \times C_7 \), where \( C_9 \) acts by an automorphism or order 3. For concreteness, a presentation of \( \Gamma \) is given by

\[
  \Gamma = \langle a, b : a^7 = b^9 = 1, ab = ba^2 \rangle.
\]

We’ll work over the field \( K = \mathbb{Q}(\omega, \sqrt{-7}) \subset \mathbb{C} \), where \( \omega = e^{2\pi i/3} \) and \( \sqrt{-7} = i\sqrt{7} \). Let \( L = K(\zeta) \), where \( \zeta = e^{2\pi i/7} \). Check that \( L/K \) is a degree three Galois extension; specifically, the minimal polynomial of \( \zeta \) over \( K \) is \( x^3 + \frac{1 - \sqrt{-7}}{2}x^2 - \frac{1 + \sqrt{-7}}{2}x - 1 \), and \( \text{Gal}(L/K) = \langle \sigma \rangle \) where \( \zeta^3 = \zeta^2 \).

Consider the crossed product \( D = A(L/K, t) \), where

\[
  t(\sigma^a, \sigma^b) := \begin{cases} 1, & \text{if } a + b < 3 \\ \omega, & \text{if } a + b \geq 3 \end{cases}
\]

for \( 0 \leq a, b < 3 \). Setting \( \mu = u_\sigma \), we may alternatively write

\[
  D = K\langle \zeta, \mu : \zeta \mu = \mu \zeta^2, \mu^3 = \omega \rangle.
\]

Exercise 4. Check that setting \( \rho(a) = \zeta \) and \( \rho(b) = \mu \) defines a \( K \)-representation \( \rho \) of \( \Gamma \). Moreover, \( \rho \) is irreducible over \( K \) and remains irreducible over \( \mathbb{C} \).
Exercise 5. Show that $D$ is a central division $K$-algebra.

Exercise 6. Write $D$ as a crossed product over $M/K$, where $M = K(\mu)$. Hint: You can do this very nicely by using the Gauss sum $\gamma = \zeta + \omega^2 \zeta^2 + \omega \zeta^3 + \omega^2 \zeta^4 + \omega^2 \zeta^5 + \zeta^6$, which satisfies $\gamma^3 = -7(1 + 3\omega)$.

The algebra $D$ (as we originally constructed it) is an example of a cyclotomic crossed product, with the values of $t$ lying in the group of roots of unity. The Brauer-Witt Theorem in representation theory says that, for an irreducible $\mathbb{C}$-representation $\rho$ of a finite group $\Gamma$, and a subfield $K \subset \mathbb{Q}$ containing all the character values $\text{Tr}(\rho(g))$, the corresponding simple algebra $K\langle \rho(\Gamma) \rangle$ is Brauer equivalent to a cyclotomic crossed product over $K$.

6. The Brauer Group of a Field

The set of central simple algebras over a field $K$ become an abelian monoid under the operation $\otimes_K$. The fact that the tensor product of two central simple algebras is central simple is a consequence of Theorem 1. Specifically, $A_1$ and $A_2$ are central simple $\iff A_1 \otimes_K K_{\text{alg}} \cong M_{n_1}(K_{\text{alg}})$ for some $n_i$, $\implies (A_1 \otimes_K A_2) \otimes_K K_{\text{alg}} \cong M_{n_1 n_2}(K_{\text{alg}}) \iff A_1 \otimes_K A_2$ is central simple.

To get a group, we'll mod out by Brauer equivalence. We've already noted that tensor products preserve Brauer equivalence, so it remains only to construct inverses. The Brauer inverse of the CSA $A$ is the opposite algebra $A^{\text{op}}$, which has the same underlying $K$-vector space structure as $A$ but multiplication defined by $a \cdot b := ba$ (concatenation denoting multiplication in $A$).

Proposition 6. If $A$ is $K$-central simple, then $A \otimes_K A^{\text{op}} \cong \text{End}_K(A) \cong M_n(K)$, where $n = \dim_K(A)$.

Proof. Consider the $K$-bilinear map from $A \times A^{\text{op}}$ to $\text{End}_K(A)$ defined by $(a, b) \mapsto (x \mapsto axb)$. The universal property of tensor products gives a corresponding $K$-linear map $\phi$ from $A \otimes_K A^{\text{op}}$ to $\text{End}_K(A)$, with $\phi(a \otimes b)(x) = axb$. In fact, $\phi$ is an (identity-preserving) morphism of $K$-algebras: $\phi(1 \otimes 1)(x) = x$, and $\phi((a_1 \otimes b_1)(a_2 \otimes b_2))(x) = \phi(a_1 a_2 \otimes b_2 b_1)(x) = a_1 a_2 x b_2 b_1 = (\phi(a_1 \otimes b_1) \circ \phi(a_2 \otimes b_2))(x)$. The kernel of $\phi$ is a two-sided ideal but not the full domain, so, by the simplicity of $A \otimes_K A^{\text{op}}$, the map is injective. But any injective map between vector spaces of the same dimension (in this case, $n^2$) is automatically bijective. Hence, $\phi$ is an isomorphism.

The second isomorphism is just the standard description of the endomorphisms of a vector space obtained by choosing a basis. □

We define several objects. The Brauer class $[A]$ of a CSA $A$ is simply its Brauer equivalence class:

$$[A] = \{B \text{ CSA over } K : M_n(A) \cong M_{n'}(B) \text{ for some positive integers } n, n'\}. \ (17)$$

The Brauer group is

$$\text{Br}(K) = \{[A] : A \text{ CSA over } K\}. \ (18)$$

By the arguments at the beginning of this section, we've shown that $\text{Br}(K)$ is an abelian group with multiplication $[A][B] = [A \otimes_K B]$, identity $[M_n(K)]$, and inverse $[A]^{-1} = [A^{\text{op}}]$.

The relative Brauer group is a subgroup

$$\text{Br}(L/K) = \{[A] \in \text{Br}(K) : A \otimes_K L \text{ is a matrix algebra over } L\}. \ (19)$$

We also give a notation to the pointed set

$$\text{Br}_n(L/K) = \{A \text{ CSA over } K : A \otimes_K LM_n(L)\}, \ (20)$$

which contain the distinguished element $M_n(K)$. 
Exercise 7. The Brauer class of the quaternions \([\mathbb{H}]\) has order two in \(\text{Br}(\mathbb{R})\). Indeed, the same is true for quaternion algebra in general: \([D(a, b)]^2 = 1\).

Exercise 8. For any field \(K\), \(\text{Br}(K)\) is torsion.

In the sequel, we will prove that, for \(L/K\) Galois, \(\text{Br}(L/K) \cong H^2(\text{Gal}(L/K), L^\times)\), via the map \(H^2(\text{Gal}(L/K), L^\times) \to \text{Br}(L/K)\) defined by crossed products.

Appendix A. Theorems about CSAs

Proposition 7. Let \(A\) be a ring containing an idempotent \(e\) with \(AeA = A\). Then, \(A \cong \text{Hom}_{eAe}(Ae, Ae)\), the algebra of right \(eAe\)-module endomorphisms of \(Ae\) (\(eAe\) is a ring with identity \(e\)).

Proof. Define \(\phi : A \cong \text{Hom}_{eAe}(Ae, Ae)\) by \(\phi(a)(x) := ax\). This will be the isomorphism we seek. Because \(AeA = A\), there are \(a_i, b_i \in A\) such that \(1 = \sum_i a_i e b_i\). To see that \(\phi\) is injective, examine its kernel. Suppose \(\phi(a) = 0\), that is, \(ax = 0\) for all \(x \in Ae\). Then, \(aa_i e = 0\) for all \(i\), so \(a = a \cdot 1 = \sum_i a_i e b_i = \sum_i 0 \cdot b_i = 0\). For surjectivity, take \(f \in \text{Hom}_{eAe}(Ae, Ae)\). Then, for \(x \in Ae\), \(f(x) = f(1 \cdot x) = f(\sum_i a_i e b_i x) = \sum_i f(a_i e b_i x) = \sum_i (f(a_i) e b_i x) = (f(a_i) e b_i) x\), so \(f = \phi(\sum_i f(a_i) e b_i)\).

Proposition 8. Let \(A\) be a simple ring containing a minimal ideal. Then, \(A\) is isomorphic to a matrix algebra over a division ring.

Proof. Let \(I\) be a minimal (nonzero) left ideal in \(A\). Because \(A\) is simple, the two-sided ideal \(AIA = A\). Clearly \(I\) is principle; indeed, \(I = Ab\) for every non-zero \(b \in I\). Choose some such \(b\). Because \(AbA = AIA = A\), \(I^2 = AbAb = Ab = I\), so there are \(c, d \in A\) such that \(cbdb \neq 0\). Thus, \(db \neq 0\), so \(0 \subseteq Adb \subseteq Ab\), and by minimality \(Adb = Ab\). Thus, \(cb = d'db\) for some \(d' \in A\), so \((d')(db)^2 = cbdb \neq 0\) and thus \((db)^2 \neq 0\). By minimality, \(A(db)^2 = I = Adb\), so \(db = p(db)^2\) for some \(p \in A\). Setting \(e := pdb\), it is now immediate that \(e^2 = e, I = Ae\), and \(AeA = A\). That is, \(e\) satisfies the hypotheses of Proposition 7. Thus, \(A \cong \text{Hom}_{eI}(I, I) \cong M_n(eI)\), where \(n\) is the rank of \(I\) over \(eI\) as an \(eI\)-module. To see that \(eI = eAe\) is a division ring, notice that, for all \(eae \in eAe \setminus \{0\}\), \(eAeae = eAeae = eAe\) because \(eAeae = Ae\) by minimality. Thus, every nonzero element of \(eI\) has a left inverse. It follows that the nonzero elements of \(eI\) form a group, and, therefore, \(eI\) is a division ring.

Proposition 9. Let \(D\) be a finite-dimensional division \(K\)-algebra, and let \(L\) be any maximal subfield of \(D\) containing \(K\). Then, \(D \otimes_K L \cong M_n(L)\), where \(n = [D : L] = [L : K]\), and \([D : K] = n^2\).

Proof. Notice that \(C_D(L)\) is a field containing \(L\); thus, \(L = C_D(L)\). Similarly, \(L = C_{D^{op}}(L)\). Consider \(D\) as a right \(L\)-module, and let \(E = \text{End}_L(D)\). Restrict the map \(\phi\) from \(D \otimes_K D^{op}\) to \(\text{End}_K(D)\) given in Proposition 6 to \(D \otimes_K L^{op} = D \otimes_K L\). The restriction is injective because the original map is. Say \(\alpha \in D \otimes D^{op}\), and express \(\alpha = \sum_i a_i \otimes b_i\) with the \(a_i\) independent. Then,

\[
\phi(\alpha) \in E \iff \sum_i a_i x b_i = \sum_i a_i x b_i l \text{ for all } x \in D, l \in L
\]

\[
\iff \sum_i a_i x (lb_i - b_i l) \text{ for all } x \in D \text{ (in particular, } x = 1\), \(l \in L
\]

\[
\iff b_i l = lb_i \text{ for all } l \in L
\]

\[
\iff \alpha \in D \otimes_K C_{D^{op}}(L) = D \otimes_K L.
\]
That is, the image of $\phi|_{D \otimes_K L}$ is precisely $E$; we have $D \otimes_K L \cong \text{End}_L(D)$.

If $n := [D : L]$, then $D \otimes_K L \cong \text{End}_L(D) \cong M_n(L)$. Taking the vector space dimension of both sides over $K$ gives $[D : K][L : K] = n^2[L : K]$, so $[D : K] = n^2$. The fact that $[L : K] = n$ now follows. □

**Lemma 10.** Let $K$ be an infinite field, and let $f \in K[x_1, \ldots, x_n]$. If $f$ vanishes at every point of $K^n$, then $f \equiv 0$. (Consequently, $K^n$ is Zariski dense in $K^n_{\text{alg}}$.)

**Proof.** Write $f(x_1, \ldots, x_n) = \sum_{0 \leq k_i \leq d_i} a_{k_1\cdots k_n} x_1^{k_1} \cdots x_n^{k_n}$. For $1 \leq i \leq n$, choose $d_i + 1$ distinct elements $c_i(0), \ldots, c_i(d_i) \in K$. The fact that $f(c_1(j_1), \ldots, c_n(j_n)) = 0$ gives us $\prod_i (d_i + 1)$ linear equations in the $a_{k_1\cdots k_n}$; specifically, $V \cdot (a_{k_1\cdots k_n}) = 0$, where $V$ is the $(\prod_i (d_i + 1)) \times (\prod_i (d_i + 1))$ matrix

$$V := (c_1(j_1)^{k_1}, \ldots, c_n(j_n)^{k_n})_{j,k}$$

whose rows are indexed by tuples $j = (j_1, \ldots, j_n)$ and whose columns are indexed by tuples $k = (k_1 \ldots k_n)$. But this $V$ is a Kronecker product of Vandermonde matrices, and it has determinant

$$\det V = \prod_{i=1}^n \prod_{j > j'} (c_i(j') - c_i(j)) \neq 0. \tag{23}$$

Thus, the vector $(a_{k_1\cdots k_n}) = 0$, so $f \equiv 0$. □

**Proposition 11.** If $D$ is a finite-dimensional division algebra over $K$, then $A$ contains a maximal subfield $L$ which is separable over $K$.

**Proof.** If $D = K$, the claim is trivial, so assume $[D : K] = n^2 > 1$. If $K$ is finite or of infinite characteristic (or more generally, perfect), any maximal subfield will do, so assume $K$ is infinite and char $K = p$. If we can show that $D$ contains some $\alpha \notin K$ that is a root of a separable polynomial over $K$, then we have reduced to the lower-dimensional problem of showing that the centralizer $C_K(\alpha)(D)$ contains a maximal subfield over $K(\alpha)$, and we may proceed by induction. Assume for the purpose of contradiction that every $\alpha \in D \setminus K$ is inseparable over $K$. That implies that $\alpha^{p^k} \in K$ for some positive integer $k(\alpha)$, but $p^{k(\alpha)} = [K(\alpha) : K] \leq n$, so there is some $k$ so that $\alpha^{p^k} \in K$ for all $\alpha \in D$.

Choose a basis $\alpha_1, \ldots, \alpha_n$ for $D$ over $K$, with $\alpha_1 = 1$. For $x_i \in K$, write

$$\left( \sum_i x_i \alpha_i \right)^{p^k} = \sum_i f_i(x_1, \ldots, x_n) \alpha_i \tag{24}$$

for polynomials $f_i \in K[x_1, \ldots, x_n]$. For $2 \leq i \leq n^2$, $f_i$ vanishes everywhere on $K^n_{\text{alg}}$. By Lemma 10, $f_i$ is identically zero. After base change to $K_{\text{alg}}$, we have that $\alpha^{p^k} \in K_{\text{alg}}$ for all $\alpha \in M_n(K_{\text{alg}})$. But this is not true (consider any idempotent $e \neq 0, 1$), and we have a contradiction. □

We are now in a position to classify CSAs over $K$.

**Exercise 9.** Prove Theorem 1 using the results of this appendix. There is nothing difficult to show; we are essentially just gathering several theorems into one.