(*February 19, 2005*)

Algebras and Involutions

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

- Vectorspaces over division rings
- Matrices, opposite rings
- Semi-simple modules and rings
- Semi-simple algebras
- Reduced trace and norm
- Other criteria for simplicity
- Involutions
- Brauer group of a field
- Tensor products of fields
- Crossed product construction of simple algebras
- Cyclic algebra construction of simple algebras
- Quaternion algebras
- Examples
- Unramified extensions of local fields
- Division algebras over local fields, Brauer groups
- Local splitting almost everywhere
- Involutions on division algebras over local fields

---

1. Vectorspaces over division rings

In this section we quickly sketch a recapitulation of finite-dimensional linear algebra over division rings. That is, we give the usual proofs of the usual basic results on dimension without using commutativity of the division ring over which the 'vectorspaces' are modules. The point is that many basic parts of finite dimensional linear algebra over division rings works just as well as over fields.

Let D be a division ring. (All D-modules will be 'left' D-modules, which is mostly a notational issue.) An expression $\sum_i \alpha_i v_i = 0$ with $\alpha_i \in D$ and $v_i \in V$ is a **linear combination** of the elements v_i. A set $\{v_i\}$ of distinct elements of a D-module V is **linearly independent** if $\sum_i \alpha_i v_i = 0$ with $\alpha_i \in D$ implies that $\alpha_i = 0$ for all i. A set $\{v_i\}$ of generators for V is said to **span** V. A set which is both linearly independent and spans V is a **basis** for V.

Proposition: Let V be a finitely generated D-module.
- There is a unique integer n, the D-dimension of V, so that $V \approx D^n$ as a D-module. That is, the D-module isomorphism class of V is determined by the dimension of V.
- Any linearly independent set of elements of V is a subset of a basis.
- Let W be a submodule of V. Then W is finitely-generated, and there is a *complementary submodule* W' to W in V, that is, so that $V = W \oplus W'$. And $\dim_D V = \dim_D W + \dim_D W'$.
- Let $\varphi : V \to W$ be a D-homomorphism. Then

$$\dim_D V = \dim_D(\ker \varphi) + \dim_D(\mathrm{Im}\, \varphi)$$

Proof: Let $\{v_i\}$ be a set of generators for V of minimal (finite) cardinality. We claim that these generators are necessarily linearly independent. If there were a non-trivial relation $\sum_i \alpha_i v_i = 0$, we may suppose without loss of generality (by relabeling) that $\alpha_1 \neq 0$, and rearrange to

$$v_1 = \sum_{i>1} (-\alpha_1^{-1}\alpha_i)\, v_i$$

which contradicts the assumed minimality. Thus,

$$(\alpha_1, \ldots, \alpha_n) \to \sum_i \alpha_i v_i = 0$$

has trivial kernel. As it is surjective, is is an isomorphism.

Let $\{v_1, \ldots, v_n\}$ be a set of generators with minimal cardinality, and $\{w_1, \ldots, w_t\}$ a linearly independent set of elements in V. (The following argument is the *replacement principle*.) Express $w_1 = \sum_i \alpha_i v_i = 0$. Without loss of generality (by relabeling) $\alpha_1 \neq 0$, from which follows (by rearranging) that v_1 is a linear combination of $w_1, v_2, \ldots, v_n$. This also implies that $w_1, v_2, \ldots, v_n$ generate V. Suppose inductively that $w_1, \ldots, w_s, v_{s+1}, \ldots, v_n$ generate V. Then the same argument shows that w_{s+1} is a linear combination

$$w_{s+1} = \sum_{i \leq s} \alpha_i w_i + \sum_{i > s} \beta_i v_i$$

Some β_i must be non-zero, or else w_{s+1} would have been a linear combination of $w_1, \ldots, w_s$, contradicting the hypothesis. By renumbering, without loss of generality $\beta_{s+1} \neq 0$. Then v_{s+1} is a linear combination of $w_1, \ldots, w_{s+1}, v_{s+2}, \ldots, v_n$. Again, this implies that $w_1, \ldots, w_{s+1}, v_{s+2}, \ldots, v_n$ generate V. By induction, $w_1, \ldots, w_m$ generate V, where $m = \min(n, t)$. Thus, by the minimality hypothesis on n, $t \geq n$.

When the v_i's and w_i's both generate V, we can symmetrically argue that $t \leq n$, and, thus, that $t = n$. This proves that 'dimension' is well-defined, as the minimal number of generators of V.

With a basis $\{v_1, \ldots, v_n\}$, and given a linearly independent set $\{w_1, \ldots, w_t\}$, by now we know that $t \leq n$, and we can use the same argument (renumbering the v_i's if necessary) to show that $w_1, \ldots, w_t, v_{t+1}, \ldots, v_n$ is a basis. This shows that every linearly independent set can be extended to a basis.

Given a submodule W, from the previous any linearly independent subset has cardinality less than or equal n, the dimension of V. Thus, W is finitely-generated. Let $w_1, \ldots, w_m$ be a basis for W. As just above, for a basis $v_1, \ldots, v_n$ of V, extend the collection of w_j's to a basis $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$ (renumbering the v_i's if necessary). Then the subspace W' spanned by $v_{m+1}, \ldots, v_n$ is a complementary subspace to W in V.

The image of a D-module homomorphism φ is certainly finitely generated, and the submodule $\ker \varphi$ of V is finitely generated, from above. Let W' be a complementary subspace to $\ker \varphi$. Then $\varphi(V) = \varphi(W') \approx W'$ since φ is an isomorphism when restricted to W'. Then

$$\dim V = \dim \ker \varphi + \dim W' = \dim \ker \varphi + \dim \mathrm{Im}\, \varphi$$

as desired, from the dimension properties of complementary subspaces just proven. ///

---

2. Matrices, opposite rings

Let R be a (not necessarily commutative) ring with 1.

For a ring B, let $M_n(B)$ denote the ring of n-by-n matrices with entries in B.

Proposition: Let E be a not-necessarily-simple R-module, and E^n the direct sum of n copies of E. Then $\mathrm{End}_R(E^n) \approx M_n(\mathrm{End}_R E)$.

Proof: Let $p_i : E^n \to E$ be the 'projection' which takes the i^{th} component of an element of E^n, and let $s_i : E \to E^n$ be the inclusion which sends E to the i^{th} copy inside E^n. For an R-endomorphism φ of E^n, Let

$$\varphi_{ij} = p_i \circ \varphi \circ s_j$$

We will take φ_{ij} as the $(i,j)^{\text{th}}$ matrix entry (i^{th} row and j^{th} column entry) of a matrix attached to φ. We must show that $\varphi \to \{\varphi_{ij}\}$ is an isomorphism. Note that obviously

$$\sum_i s_i \circ p_i = 1_{E^n}$$

Then for two endomorphisms φ, ψ,

$$p_i \circ \varphi\psi \circ s_j = p_i \circ \varphi \circ 1_{E^n} \circ \psi \circ s_j = p_i \circ \varphi \circ (\sum_\ell s_\ell \circ p_\ell) \circ \psi \circ s_j = \sum_\ell (p_i \circ \varphi \circ s_\ell)(p_\ell \circ \psi \circ s_j) = \sum_\ell \varphi_{i\ell} \circ \psi_{\ell j}$$

as desired. Thus, the map is a homomorphism. It is injective, since any φ can be recovered from its φ_{ij}'s. It is surjective, since any collection of φ_{ij}'s gives an R-endormorphism. ///

Let B be a ring, and let $B^{\rm opp}$ denote the **opposite ring**, which by definition has the same underlying set, but whose multiplication $*$ is the reverse of that of B itself. That is, letting $\psi : B \to B^{\rm opp}$ be the set bijection of B to its opposite,

$$\psi(\alpha) \cdot \psi(\beta) = \psi(\beta\alpha)$$

(Associativity does hold.)

Proposition: For any ring R with unit 1, $\mathrm{End}_R R \approx R^{\rm opp}$, and the associated endomorphisms are simply right multiplications. Equivalently, $\mathrm{End}_{R^{\rm opp}} R \approx R$.

Proof: Certainly right multiplications $r \to rs$ by elements $s \in R$ are (left) R-module endomorphisms of R. Note that multiplying on the right requires reversal of multiplication in R for associativity, so that the ring that acts on the right is indeed $R^{\rm opp}$. On the other hand, let $T \in \mathrm{End}_R R$. Then for $r \in R$

$$T(r) = r \cdot T(1)$$

Thus, taking $s = T(1)$ shows that $T(r) = r \cdot s$. The proof of the second assertion is nearly identical. ///

Proposition: Let R be an arbitrary ring, with $\psi_R : R \to R^{\rm opp}$ the bijection to its opposite ring. (The map ψ is the identity on the underlying set.) The opposite ring of the n-by-n matrix ring $M_n(R)$ with entries in R is

$$T : M_n(R)^{\rm opp} \approx M_n(R^{\rm opp})$$

and the isomorphism is essentially given by transpose: in terms of entries,

$$(T\,\psi(\alpha))_{ij} = \psi_R(\alpha_{ji})$$

where ψ is the natural bijection of $M_n(R)$ to its opposite ring.

Proof: Let α, β be two matrices with $(i,j)^{\rm th}$ entries α_{ij}, β_{ij} in R. Compute directly

$$T(\psi(\alpha)\,\psi(\beta))_{ij} = T(\psi(\beta\alpha))_{ij} = \psi_R((\beta\alpha)_{ji})$$

$$= \psi_R(\sum_t \beta_{jt}\alpha_{ti})\} = \sum_t \psi_R(\alpha_{ti})\,\psi_R(\beta_{jt}) = \sum_t (T\psi\alpha)_{it}\,(T\psi\beta)_{tj} = ((T\psi\alpha)\,(T\psi\beta))_{ij}$$

This verifies the homomorphism propery. Bijectivity is obvious. ///

---

3. Semi-simple modules and rings, density theorem

Let R be a (not-necessarily commutative) ring with identity 1. A module M over R is **simple** if it has no proper submodule, that is, has no submodule other than $\{0\}$ and M itself.

Proposition: If M and N are simple R-modules, then every R-homomorphism $f : M \to N$ is either the zero map or is an isomorphism.

Proof: The kernel is a submodule of M, and the image is a submodule of N. ///

Corollary: *(Schur's Lemma)* If M is a simple R-module, then the ring $\mathrm{End}_R M$ of R-homomorphisms of M to itself is a division ring. ///

An R-module M is **semi-simple** if it satisfies the equivalent conditions of the following proposition.

Proposition: The following three conditions on a module M over R are equivalent:
• M is a direct sum of simple submodules E_α.
• M is a (not-necessarily direct) sum of simple submodules E_α.
• Every submodule N of M is a direct summand of M, that is, there is another submodule N' so that $M = N \oplus N'$.

Proof: Certainly the first assertion implies the weaker second assertion. Suppose, for the converse, that $M = \sum_\alpha E_\alpha$ with each E_α simple. Let J be a maximal set of indices so that the sum over J is a direct sum:

$$\sum_{\alpha\in J} E_\alpha = \bigoplus_{\alpha\in J} E_\alpha$$

For any simple $E_\beta \subset M$, the intersection of E_β with the sum $\sum_{\alpha\in J} E_\alpha$ is either $\{0\}$ or E_β, by simplicity. The intersection cannot be $\{0\}$, or maximality of J would be contradicted. Thus, the sum over J contains every E_β, so must be all of M.

To see that every submodule N of a direct sum expression $\bigoplus_{\alpha\in J} E_\alpha$ of simple modules is a direct summand, let J be a maximal set of indices so that

$$N + \sum_{\alpha\in J} E_\alpha$$

is a direct sum. The same argument as in the previous paragraph shows that every simple submodule E_β must be contained in such a sum, so the sum is all of M.

Now suppose that every submodule is a direct summand, and prove that M is a sum of simple modules. It suffices to show that every non-zero submodule N of M contains a simple module, since then the sum of all simple submodules must be the whole M, by the same argument used twice already above. To show that a submodule N of M contains a (non-zero) simple submodule, pick non-zero $n \in N$, and consider the submodule $R \cdot n$. The kernel of the R-homomorphism $r \to rn$ is a proper left ideal K in R, necessarily contained in a *maximal* proper left ideal L of R (since R has a unit 1). Then $L \cdot n \approx L/K$ is a maximal submodule of Rn not equal to Rn, but possibly $\{0\}$. Using the fact that every submodule of M is a direct summand, there is a submodule P of M so that $M = P \oplus Ln$. For $r \cdot n \in Rn$, write $rx = \ell n + p$ with $\ell \in L$ and $p \in P$. Then $p = (r - \ell)n \in Rn$. Thus,

$$Rn = Ln \oplus (P \cap Rn)$$

Since L is maximal proper in R, certainly Ln is maximal proper in Rn, so $P \cap Rn$ can have no proper submodules. Since $Ln \neq Rn$, $P \cap Rn$ is not $\{0\}$, so is simple. ///

Corollary: Submodules, quotient modules, and sums of semi-simple R-modules are semi-simple. ///

Theorem: *(Density Theorem)* Let M be a semi-simple R-module. Let $R' = \mathrm{End}_R M$, and $R'' = \mathrm{End}_{R'} M$. For every finite subset X of M, for every $r'' \in R''$ there is $r \in R$ so that $r''x = rx$ for every $x \in X$.

Proof: Certainly R naturally sits inside R''. First, show that R-submodules of M are actually R''-submodules. Given an R-submodule N, let N' be its complementary submodule, so $M = N \oplus N'$. Let π be the R-homomorphism projecting M to N with kernel N'. So $\pi \in R'$. Thus, for $r'' \in R''$,

$$r''N = r''(\pi M) = \pi(r''M) \subset \pi M = N$$

Thus, N is an R''-submodule. If X had only a single element x, then Rx is an R''-submodule of M, and the theorem follows. For arbitrary X with n elements, replace M by M^n, which is still semi-simple over R. The map $M^n \to M^n$ given by

$$\tilde{r}'' : (m_1, \ldots, m_n) \to (r''m_1, \ldots, r''m_n)$$

is in $\mathrm{End}_{\mathrm{End}_R M^n}(M^n)$, since $\mathrm{End}_R(M^n) \approx M_n(R')$. This reduces to the case that X has a single element. ///

Corollary: *(Burnside's theorem)* Let V be a finite-dimensional vector space over an algebraically closed field k, and R a k-subalgebra of $\mathrm{End}_k(V)$. If V is a simple R-algebra, then R is the full endomorphism algebra $\mathrm{End}_k(V)$.

Remark: This is irretrievably false without the assumption that k is algebraically closed.

Proof: By the simplicity of V as an R-module, $D = \mathrm{End}_R V$ is a division ring. It contains k in its center. By the finite-dimensionality of V over k, D is finite-dimensional over k. For $\alpha \in D$ but $\alpha \notin k$, $k(\alpha)$ would be a proper algebraic field extension of k, which is impossible, by the algebraic closedness of k, so $D = k$. Let $\{e_i\}$ be a (finite) basis for V. Using the Density Theorem, using $\mathrm{End}_R V = k$, for any $r'' \in \mathrm{End}_k V$ there is $r \in R$ so that $re_i = r''e_i$ for all i, which yields $r'' = r$. ///

Recall that an R-module M is *faithful* if for every $0 \neq r \in R$ there is $m \in M$ so that $r \cdot m \neq 0$.

Corollary: *(Wedderburn's theorem)* Let R be a ring with 1, and M a simple *faithful* R-module. Let $D = \mathrm{End}_R M$, and suppose that M is finite-dimensional over the division ring D. Then $R = \mathrm{End}_D M$.

Proof: Let $\{e_i\}$ be a D-basis for M. Given $r'' \in \mathrm{End}_D M$, by the Density Theorem there is $r \in R$ so that $re_i = r''e_i$ for all i. Thus, the natural map $R \to \mathrm{End}_D M$ is surjective. The faithfulness of M over R implies that the map is also injective. ///

A ring R is **semi-simple** if it is semi-simple as a left module over itself, and if it is not $\{0\}$. A ring R is **simple** if it is semi-simple and has a unique isomorphism class of simple left ideals.

Proposition: If R is a semi-simple ring then every R-module is semi-simple.

Proof: Let M be an R-module, and show that M is a sum of simple submodules. Let $m \in M$, and look at the submodule $R \cdot m \subset M$. Let I be the left ideal in R which is the kernel of the map $r \to rm$. Express R as a sum of simple left ideals $R = \sum_i L_i$. Then

$$R \cdot m = \sum_i L_i \cdot m$$

Since L_i is simple, $L_i m$ is either an isomorphic copy of L_i, or is $\{0\}$. Thus, $R \cdot m$ is a sum of simple modules. Thus, every element in M is contained in a sum of simple modules, so M itself is a sum of simple submodules. ///

A module M over a ring R is **Artinian** if any descending chain of submodules

$$M_1 \supset M_2 \supset M_3 \supset \dots$$

eventually stabilizes, that is, there exists an index i_o so that for $i \geq i_o$ we have $M_i = M_{i_o}$.

Remark: Finite-dimensional vectorspaces over fields are Artinian modules over the field. By contrast, many common rings such as the integers $\mathbf{Z}$ are *not* Artinian as modules over themselves. Our immediate use of the Artinian condition on modules is as an abstracted form of requiring modules to be finite-dimensional vectorspaces over a field.

Proposition: Let D be a division ring, and $A = M_n(D)$ the ring of n-by-n matrices with entries in D. Then A is a simple Artinian ring. The whole ring A is the direct sum of the (mutually isomorphic) simple left ideals consisting of matrices with non-zero entries only in a single column.

Proof: We must prove that A is a sum of simple left ideals, and that all these left ideals are isomorphic. Let L_j be the collection of n-by-n matrices with non-zero entries only in the j^{th} column. To see that L_j is simple, let e_{ij} denote a matrix with zeros everywhere except for a 1 in the $(i,j)^{\text{th}}$ entry. Suppose that some non-zero element

$$\ell = \sum_i d_i \, e_{ij}$$

lies in a left ideal I inside L_j, with $d_i \in D$. Let i_o be an index so that $d_{i_o} \neq 0$. Then

$$L_j \ni d_{i_o}^{-1} e_{i_o i_o} \cdot x = e_{i_o j}$$

And then for any index k

$$L_j \ni e_{k i_o} \cdot e_{i_o j} = e_{kj}$$

so L_j contains the D-basis $e_{1j}, e_{2j}, \ldots, e_{nj}$ for L_j. Thus, L_j is simple.

The $M_n(D)$-isomorphism from L_j to L_k is the obvious

$$\varphi : \sum_i d_i \, e_{ij} \to \sum_i d_i \, e_{ik}$$

We can check that φ respects left multiplication by matrices non-computationally by observing that the map φ can be realized by a *right* matrix multiplication by $e_{jk} + e_{kj}$. Thus, not surprisingly, all these column-ideals are isomorphic as left ideals over the matrix ring.

To prove that A is (left) Artinian, note that any chain of left modules certainly is a chain of (left) D-modules (with D imbedded in A as 'scalar' matrices). Since $A = M_n(D)$ is a finite-dimensional D-space, any descending chain of D subspaces is finite. ///

Theorem: Let R be a semi-simple ring. Then there is only a *finite* number of isomorphism classes of simple left ideals. Let $\{L_i\}$ be representatives for these. If R_i is the sum of all left ideals isomorphic to L_i, then R_i is a simple ring with a unit e_i, and $1_R = \sum_i e_i$. Further, $R = \bigoplus_i R_i$, and $e_i e_j = \delta_{ij}$ (Kronecker delta). And

$$R_i = e_i R = R e_i = e_i R e_i$$

Proof: Claim that if L is a simple left ideal of R and M is a simple R-module not isomorphic to L then $L \cdot M = 0$. Indeed, LM is an R-submodule of M, so is either $\{0\}$ or M. If it were M, then, for some non-zero $m \in M$, $L \cdot m = M$. Then the map $\ell \to \ell m$ is a surjective R-module map $L \to M$. Since L is simple, this map is an isomorphism. Thus, either $L \cdot M = 0$ or $L \approx M$.

Thus, $R_i R_j = 0$ unless $i = j$. Since by semisimplicity R is the sum of its simple left ideals, $R = \sum_i R_i$. Thus,

$$R_j \subset R_j \cdot R = R_j \cdot R_j \subset R_j$$

which shows that R_j is also a *right* ideal. Write $1_R = \sum_i e_i$ with $e_i \in R_i$. Since the $R = \sum_i R_i$ is algebraic, the expression $1_R = \sum_i e_i$ has only finitely-many non-zero summands. Since R_i is a two-sided ideal, it follows that there are only finitely-many R_i's. From the fact that $R_i \cdot R_j = 0$ unless $i = j$, we have

$$e_i = e_i \cdot 1 = e_i \cdot \sum_j e_j = \sum_j e_i \cdot e_j = e_i \cdot e_i$$

and $e_i e_j = 0$ unless $i = j$. That is, the e_i's are an orthogonal system of idempotents in R, and e_i is the unit in R_i. For $x \in R$

$$x = x \cdot 1 = x \cdot \sum_i e_i = \sum_i x \cdot e_i$$

$$x = 1 \cdot x = *\sum_i e_i) \cdot x = \sum_i e_i \cdot x$$

so $e_i x = x e_i \in R_i$ is the 'projection' of x to R_i. In particular, R_i is a ring itself, with unit e_i, and with a unique isomorphism class of left ideal, so by definition simple. ///

Theorem: A simple ring R is a finite direct sum of simple left ideals. There are no proper two-sided ideals.

Proof: Using semisimplicity, write R as a direct sum $\bigoplus_i L_i$ of simple left ideals L_i. Let $1 = \sum_i \ell_i$ with $\ell_i \in L_i$. Necessarily this sum has only finitely-many non-zero summands. Let J be the set of indices so that $\ell_i \neq 0$ for $i \in J$. Then

$$\bigoplus_i L_i = R = R \cdot 1 = \sum_{i \in J} R \cdot \ell_i = \sum_{i \in J} L_i$$

Thus, J is the whole index set, which is finite. For any simple left ideal, $L \cdot R$ is a left ideal, so is necessarily a direct sum $LR = \bigoplus_j L_j$ for some simple left ideals L_j. Using the direct summand property, $R = L \oplus N$ for some left ideal N in R. Let π be the projection of R to L with kernel N. Every simple left ideal I is isomorphic to L by the hypothesis of simplicity, so let $f : L \to I$ be an isomorphism. Then $f \circ \pi$ is a R-endomorphism of R. By the lemma, $(f \circ \pi)(r) = rs$ for some $s \in R^{\text{opp}}$. Thus, for $\ell \in L$,

$$f(\ell) = (f \circ \pi)(\ell) = \ell \cdot s$$

That is, every simple left ideal I is contained in $L \cdot R$, so $LR = R$. That is, R has no proper two-sided ideals. ///

Proposition: Let V be a vectorspace over a division ring D. Then $\text{End}_D V$ is simple if and only if V is finite-dimensional over D.

Proof: If V is finite-dimensional over D, then $V \approx (D^{\text{opp}})^n$ for some finite integer n, and $\text{End}_D V$ is isomorphic to a matrix ring

$$M_n(\text{End}_D D^{\text{opp}}) \approx M_n(D^{\text{opp}})$$

over D^{opp}. Let L_i be the left ideal of matrices with non-zero entires only in the i^{th} column. Clearly the L_i's are mutually isomorphic simple left ideals in the matrix algebra, and $M_n(D^{\text{opp}})$ is their direct sum. Thus, $M_n(D^{\text{opp}})$ is simple.

On the other hand, for V infinite-dimensional over D, let B_o be the subset of $\text{End}_D V$ consisting of endomorphisms with D-finite-dimensional images. It is clear that B_o is closed under left and right multiplication by D-endomorphisms. Since V is infinite-dimensional, the identity map is not in B_o, so B_o is not all of $\text{End}_D V$. The subset B_o is closed under addition, because

$$\text{Im}\,(T_1 + T_2) \subset \text{Im}\,T_1 + \text{Im}\,T_2$$

for any two endomorphisms. To see that B_o is not $\{0\}$, choose a basis $\{e_\alpha : \alpha \in A\}$, pick $\beta \in A$, and define

$$T(\sum_\alpha c_\alpha\, e_\alpha = c_\beta\, e_\beta$$

This T lies in B_o and is not the zero map. ///

Corollary: *(of Density Theorem)* Let M be a semi-simple Artinian module over a ring R with unit 1. Let $R' = \text{End}_R M$, and $R'' = \text{End}_{R'} M$. Then the natural map $R \to R'$ is a *surjection*. In particular, if M is a *faithful* R-module, then $R \approx R''$.

Proof: Writing M as a direct sum of simple submodules, the Artinian condition implies that the sum must be finite. Thus, M is finitely-generated as an R-module. Then the Density Theorem implies that for every $r'' \in R''$ there is $r \in R$ which has the same effect on M. This gives the surjectivity. The remark about faithfulness is then clear. ///

Theorem: Let B be a simple ring which is Artinian as a left module over itself. Then there is a division ring D (unique up to isomorphism) and a unique integer n so that B is isomorphic (as a ring) to the ring $M_n(D)$ of n-by-n matrices with entries in D. In particular, let L be a simple left ideal of B. Then $\text{End}_B L$ is a division ring, and $D \approx (\text{End}_B L)^{\text{opp}}$. Further, the integer n is the number of simple direct summands of B as left module over itself.

Proof: Write B as a direct sum $\bigoplus_\alpha L_\alpha$ of simple left ideals, mutually isomorphic as B-modules (by the definition of simplicity). The left Artinian property implies that this is a finite direct sum, of cardinality n, a finite integer. Let L be a simple left ideal, simple up to isomorphism. Then

$$\mathrm{End}_B B \approx \mathrm{End}_B(L^n) \approx M_n(\mathrm{End}_B L)$$

and the simplicity of the ideal L implies that $C = \mathrm{End}_B L$ is a division ring. By counting C-dimension we see that n is uniquely determined. The left ideal L must be faithful as a B-module, since if $bL = \{0\}$ for $b \in B$ then

$$b = b \cdot 1_B \in b \cdot B = b \cdot \sum_\alpha L_\alpha = \sum b \cdot L_\alpha = \sum \{0\}$$

Therefore, the corollary above yields

$$B = \mathrm{End}_C L$$

By the proposition above, L is finite-dimensional over C. Let m be the C-dimension of L. Then

$$B = \mathrm{End}_C L \approx \mathrm{End}_C(C^m) = M_m(\mathrm{End}_C C) \approx M_m(C^{\mathrm{opp}})$$

Let L_i be the left ideal of $M_m(C^{\mathrm{opp}})$ of matrices whose non-zero entires occur only in the i^{th} column. These are simple ideals. Then B is a direct sum of these m simple ideals, and clearly $m = n$. ///

Corollary: The center of an Artinian simple ring is a field.

Proof: Using the theorem just above, we equivalently can ask about the center of a matrix algebra $M_n(D)$ over a division ring D. It is elementary that the center consists of scalar (diagonal) matrices with entries in the center of D. Since D is a division ring, its center is a field. ///

---

4. Semi-simple algebras

The theorem just above asserting that Artinian simple rings are isomorphic to matrix algebras $M_n(D)$ over division rings D still has too weak a conclusion for further developments, since in general the division ring D may be of *infinite dimension* over its center. This precludes constructions such as taking tensor products of two such algebras over a common center k, since the resulting object may lose its Artinian property.

A ring A is a **central** over a field k if k is exactly its center. We will be mostly interested in the situation that A is *finite-dimensional* and central over a field k. More generally a k-algebra is a ring with a copy of k in its center.

A *k-algebra homomorphism* $T : A \to B$ of rings with units is a ring homomorphism T so that

$$T(\alpha \cdot 1_A) = \alpha \cdot 1_B$$

for all $\alpha \in k$. Note that this ensures not only the k-linearity of T, but also that the identity of A is mapped to that of B. In particular, this avoids irrelevant complications about the center.

Corollary: Let B be a semi-simple ring which is a k-algebra, and is finite-dimensional over k. Then B is isomorphic (as k-algebra) to a finite product of matrix rings $M_n(D)$ over division rings D whose center contains a copy of a finite algebraic field extension of k. The integers n and division rings D so occurring are unique up to permutations (and k-isomorphism).

Proof: Because B is a semi-simple ring, it is a finite product of simple rings, unique (up to isomorphism) up to permutations, so it suffices to treat the case of simple rings B. The finite-dimensionality over k implies that B is Artinian, so from just above is of the form $M_n(D)$ for a division ring D containing k in its center. The finite-dimensionality of B over k implies the finite-dimensionality of D over k, and also k is necessarily contained in the center K of D. Thus, also, K is finite-dimensional over k. As in the earlier argument, for

a simple finite-dimensional k-algebra S with (up to isomorphism unique) simple left ideal L, the division algebra D is determined as

$$D = (\mathrm{End}_S L)^{\mathrm{opp}}$$

which specifies D uniquely up to k-algebra isomorphism. ///

Let B^{opp} denote the **opposite ring** to a ring B, which has the same underlying set, but whose multiplication $*$ is the reverse of that of B itself:

$$\alpha * \beta = \beta\,\alpha$$

(Associativity does hold.)

Proposition: For a finite-dimensional central simple k-algebra A,

$$A \otimes_k A^{\mathrm{opp}} \approx \mathrm{End}_k A$$

and the latter is isomorphic to a matrix algebra over k.

Proof: Let $S = A \otimes_k A^{\mathrm{opp}}$. We give A a natural S-module structure by

$$(\alpha \otimes \beta)x = \alpha \cdot x \cdot \beta$$

This gives a k-algebra homomorphism $T : S \to \mathrm{End}_k A$. Since A has no proper two-sided ideals, A has no proper S-submodules, so is a simple S-module. By the Density Theorem, using the finite-dimensionality of A over k, T is surjective. By comparing k-dimensions, it also follows that T is injective, so is an isomorphism. ///

Theorem: For simple k-algebras A and B, if A is finite-dimensional and central over k, then $A \otimes_k B$ is a simple k-algebra. If also B is central over k, then so is $A \otimes_k B$. If K is a field extension of k and A is a central simple k-algebra, then $A \otimes_k K$ is a central simple K-algebra. In the latter situation, the K-dimension of $A \otimes_k K$ is equal to the k-dimension of A.

Proof: First, always

$$M_n(k) \otimes_k B \approx M_n(B)$$

If B is simple, then this matrix algebra is simple, since it is the sum of left ideals isomorphic to B^n, each of which is easily verified to be simple. Whatever the center Z of B is, the center of $M_n(B)$ consists of 'scalar' matrices with (equal) diagonal entries in Z. If $A \otimes_k B$ had a proper two-sided ideal then so would

$$A^{\mathrm{opp}} \otimes_k A \otimes_k B \approx (\text{matrix algebra with entries in } k) \otimes_k B \approx \text{matrix algebra with entries in } B$$

(using the previous theorem to identify $A^{\mathrm{opp}} \otimes A$). But we just noted that this algebra is simple, contradiction. Likewise, if both A and B are central over k, and if the center of $A \otimes_k B$ were larger than k, then the center of $A^{\mathrm{opp}} \otimes_k A \otimes_k B$ would also be larger than k, contradiction.

Certainly a field K is simple as a ring. Thus, for a field K containing k, $A \otimes_k K$ is simple, and it is clear that K is contained in its center. On the other hand, if the center were strictly larger than K, then so would be the center of

$$A^{\mathrm{opp}} \otimes_k A \otimes_k K \approx \mathrm{End}_k A \otimes_k K \approx (\text{matrix algebra over } k) \otimes_k K$$

which is false. ///

Corollary: Every finite-dimensional central division algebra D over a field k has dimension of the form n^2 for an integer n. There are no proper finite-dimensional division algebras over an algebraically closed field.

Proof: For the latter assertion, if $\alpha \in D$ by $\alpha \notin k$, then $k(\alpha)$ would be a proper finite-dimensional (therefore algebraic) field extension of k, which is impossible. Now let $\bar{k}$ be an algebraic closure of k, and consider the simple central $\bar{k}$-algebra $D \otimes_k \bar{k}$. From the classification of simple central algebras as matrix algebras over

central division algebras (above), and from the fact just noted that there are no proper finite-dimensional central division algebras over $\bar{k}$, this must be a matrix algebra over $\bar{k}$, so has $\bar{k}$-dimension a square n^2. Since dimension does not change when tensoring with a field extension, the k-dimension of D is also n^2. ///

Theorem: *(Skolem-Noether)* Let A be a simple k-subalgebra of a finite-dimensional central simple k-algebra B. Then every k-algebra isomorphism $\varphi : A \to A$ extends to an **inner automorphism** of B, that is, to an automorphism of the form $\alpha \to \beta\alpha\beta^{-1}$ for some $\beta \in B^\times$.

Proof: Give B two $R = A \otimes_k B^{\text{opp}}$-algebra structures E_1 and E_2, by

$$\begin{aligned} (\alpha \otimes \beta)x &= \alpha x \beta \quad (\text{for } E_1) \\ (\alpha \otimes \beta)x &= \varphi(\alpha) x \beta \quad (\text{for } E_2) \end{aligned}$$

By the previous theorem, R is a simple k-algebra, so there is a single isomorphism class of simple left ideals in it. Further, the k-dimension of an R-module determines its isomorphism class. Since E_1 and E_2 have the same k-dimension, they are isomorphic R-modules. Let $i : E_1 \to E_2$ be an R-isomorphism. Then the R-isomorphism property

$$i(\alpha b \beta) = i((\alpha \otimes \beta)b) = (\alpha \otimes \beta)\, i(b) = \varphi(\alpha)\, i(b)\, \beta$$

with $\alpha = 1$ gives

$$i(b\beta) = i(b)\, \beta$$

Since B is simple as a right B^{opp}-module, and since i is a B^{opp}-isomorphism, (from above) there is $b_o \in B^\times$ so that $i(b) = b_o b$. Taking $b = \beta = 1$ gives

$$b_o \alpha = i(\alpha) = i((\alpha \otimes 1)\, 1) = (\alpha \otimes 1)\, i(1) = (\alpha \otimes 1)\, b_o = \varphi(\alpha)\, b_o$$

Therefore,

$$\varphi(\alpha) = b_o \alpha b_o^{-1}$$

This certainly extends to an inner automorphism of B. ///

Corollary: Every k-algebra automorphism of a finite-dimensional simple central k-algebra is inner. ///

---

5. Reduced trace and norm

We will need the notion of *reduced trace* and *reduced norm* later, for elements of finite-dimensional simple central k-algebras. To this end we introduce the *reduced characteristic polynomial*.

Let B be a finite-dimensional central simple algebra over a field k. Let E be a finitely-generated B-module. Let x be an indeterminate. Then $k[x]$ is a principal ideal domain, and the $k[x]$ module

$$E' = E \otimes_k k[x]$$

is a free $k[x]$-module of finite rank (equal to the k-dimension of E). The highest non-vanishing exterior power of E' over $k[x]$ is a free $k[x]$-module of rank 1, so for $\beta \in B$ left multiplication on E' by

$$1 \otimes X - \beta \otimes 1 \in B \otimes_k k[x]$$

induces multiplication by a polynomial $\chi_{\beta,E}(x)$ on that exterior power of E'. This $\chi_{\alpha,E}(x)$ is the **characteristic polynomial** of β on E.

Proposition: For two finitely-generated B-modules M and N over the finite-dimensional simple central k-algebra B, for $\beta \in B$,

$$\chi_{\beta,M\oplus N}(x) = \chi_{\beta,M}(x) \cdot \chi_{\beta,N}(x)$$

And

$$\chi_{\beta,M\otimes_k K}(x) = \chi_{\beta,M}(x)$$

for a field extension K of k. ///

From the previous section, an algebraic closure K of k splits any finite-dimensional simple central k-algebra B. Let L be a simple left module in

$$M_n(K) \approx B \otimes_k K$$

Since K splits B the ideal L is an n-dimensional K-vectorspace, and as left $B \otimes_k K$ module

$$B \otimes_k K \approx \underbrace{L \oplus \ldots \oplus L}_{n}$$

Therefore, from the proposition, for $\beta \in B \subset B \otimes_k K$,

$$\chi_{\beta,B} = \chi_{\beta,B\otimes_k K} = \chi_{\beta,L^n} = \chi^n_{\beta,L} \in k[x]$$

Proposition: Let K be a separable field extension of k. If the n^{th} power $P(x)^n$ of a polynomial $P(x) \in K[x]$ is actually in $k[x]$, then the polynomial $P(x)$ itself is in $k[x]$.

Proof: If k is of characteristic 0, or if the characteristic p is positive but does not divide the exponent n, then a simple induction on coefficients proves the proposition. Thus, we reduce to the case of positive characteristic p and exponent $n = p$. In that case,

$$(a_o + a_1 x + \ldots + a_m x^m)^p = a_o^p + a_1^p x^p + \ldots + a_m^p x^{mp}$$

Thus, since K is separable over k, for $a_i \in K$, $a_i^p \in k$ implies $a_i \in k$ for every index i. ///

Then define the **reduced characteristic polynomial** of $\beta \in B$, with $\dim_k B = n^2$, to be the polynomial $\chi_\beta \in k[x]$ so that

$$\chi^n_\beta = \chi_{\beta,B}$$

The previous proposition assures that χ_β really does have coefficients in k, not merely in a splitting field of B. The **reduced trace** of β is -1 times the coefficient of $X^n - 1$ in $\chi_{\beta,B}$, where $\dim_k B = n^2$. The **reduced norm** of β is $(-1)^n$ times the constant coefficient of $\chi_{\beta,B}$. Note that both lie in k.

---

6. Other criteria for simplicity

Theorem: Let B be a finite-dimensional central k-algebra without any proper two sided ideal. Then B is a simple central k-algebra.

Proof: The finite-dimensionality over k certainly implies that B is left Artinian over itself, so it has a minimal left ideal L. We claim that L is a faithful simple B module. The simplicity is immediate from the minimality. The lack of proper two-sided ideals implies $L \cdot B = B$, since $L \cdot B \ni L \cdot 1$. Thus, if $\beta \cdot L = \{0\}$ for some $\beta \in B$, we would have

$$\beta = \beta \cdot 1 \in \beta \cdot B \subset \beta \cdot L \cdot B = 0 \cdot B = 0$$

so $\beta = 0$, proving faithfulness. Therefore, from above, $C = \text{End}_B L$ is a division algebra, and L is finite-dimensional over C because everything in sight is finite-dimensional over k. By Wedderburn's theorem, $B = \text{End}_C L$, and the latter is isomorphic to a matrix algebra over $C^{\text{opp}} = \text{End}_C C$, and (from above) is therefore simple. ///

Corollary: Let B be a finite-dimensional central k-algebra and suppose that K is a field extension of k so that $B \otimes_k K$ is simple. Then B is simple.

Proof: By the previous theorem, we need only show that B does not have any proper two-sided ideals. If J were a proper two-sided ideal of B, then $J \otimes_k K$ would be a two sided ideal of $B \otimes_k K$. By counting dimensions, noting that k-dimensions before tensoring are equal to K-dimensions after tensoring, $J \otimes_k K$ would necessarily be a *proper* two-sided ideal. This would contradict the simplicity of $B \otimes_k K$.
///

Next, we have the **trace-pairing** criterion for simplicity. Let V be a finite-dimensional vectorspace over a field k, with k-linear dual V^*. We can define the trace

$$\mathrm{tr} : \mathrm{End}_k(V) \to k$$

intrinsically, as follows. First, we have a natural isomorphism

$$t : V \otimes_k V^* \approx \mathrm{End}_k(V)$$

by taking

$$(v \otimes \mu)(x) = \mu(x) \cdot v$$

for $v, x \in V$ and $\mu \in V^*$ and then extending k-linearly. Then define the trace by

$$\mathrm{tr}\, v \otimes \mu = \mu(v)$$

and extending k-linearly. For a central k-algebra A, and for $x \in A$, let $\ell_x \in \mathrm{End}_k V$ be left multiplication by x. Then define the **trace pairing**

$$\langle , \rangle : A \times A \to k$$

by

$$\langle x, y \rangle = \mathrm{tr}\,(\ell_x \circ \ell_y)$$

This is symmetric and k-bilinear. As usual, a k-bilinear pairing $\langle , \rangle$ is said to be *non-degenerate* if $\langle x, y \rangle = 0$ for all y implies $x = 0$. Note that for $T, x, y \in A$

$$\langle Tx, y \rangle = \mathrm{tr}\,(\mu_{Tx} \circ \mu_y) = \mathrm{tr}\,(\mu_T \circ \mu_x \circ \mu_y) = \mathrm{tr}\,(\mu_x \circ \mu_y \circ \mu_T) = \mathrm{tr}\,(\mu_x \circ \mu_{yT}) = \langle x, yT \rangle$$

Even more simply,

$$\langle xT, y \rangle = \mathrm{tr}\,(\mu_{xT} \circ \mu_y) = \mathrm{tr}\,(\mu_x \circ \mu_T \circ \mu_y) = \mathrm{tr}\,(\mu_x \circ \mu_{Ty}) = \langle x, Ty \rangle$$

Theorem: The trace pairing on a finite-dimensional central k-algebra A is non-degenerate if and only if A is semi-simple.

Proof: First, suppose that the trace pairing is non-degenerate, and do induction on the k-dimension of A. Let I be a minimal non-zero two-sided ideal in A, which must exist by the finite-dimensionality. If $I = A$, then A is simple, from above. So suppose I is proper. Let $I^\perp$ be the orthogonal complement

$$I^\perp = \{b \in A : \langle b, i \rangle = 0 \text{ for all } i \in I\}$$

From the property that for $S, T, x, y \in A$

$$\langle SxT, y \rangle = \langle x, TyS \rangle$$

it follows that $I^\top$ is also a two-sided ideal. It is not A itself, by the non-degeneracy assumption. And $I \cap I^\perp$ is another two-sided ideal. If the intersection is non-zero, then by the minimality hypothesis on I it must be that $I \cap I^\perp = I$. That is, the trace pairing restricted to $I \times I$ is identically zero. The ideal $I \cdot I$ is another two-sided ideal, and is contained in I, so is either I or is $\{0\}$, by the minimality of I. If $I \cdot I = I$, then (still assuming $I \subset I^\perp = I$)

$$\langle I, A \rangle = \langle I \cdot I, A \rangle = \langle I, A \cdot I \rangle \subset \langle I, I \rangle = 0$$

contradicting the non-degeneracy of the pairing. Thus, $I \cdot I = \{0\}$. Then, for any $a \in A$ and $i \in I$, $(ai)^2 = 0$, so $\mu_{ai}^2 = 0$. In particular, μ_{ai} is *nilpotent*. Quite generally, nilpotent endomorphisms of finite-dimensional vectorspaces have trace 0. Thus,

$$0 = \operatorname{tr} \mu_{ai} = \operatorname{tr} (\mu_a \circ \mu_i) = \langle a, i \rangle$$

for every $a \in A$ and for every $i \in I$. But, again, this contradicts the non-degeneracy of the pairing. Therefore, it must have been that $I \cap I^\perp = \{0\}$, so $I^\perp$ and I are both algebras with a non-degenerate trace pairing, and we can invoke the induction hypothesis. This proves that non-degeneracy implies semi-simplicity.

Now suppose that A is semi-simple. It suffices to consider that case that A is simple and central over a separable extension E of k. Let L be a maximal separable subfield of A. Then by general structure results the reduced trace on A, when restricted to L, is the Galois trace from L to E. Thus, to prove non-degeneracy of the trace pairing it suffices to prove that the field-theoretic trace $\operatorname{tr} : L \to k$ is not identically zero for separable field extensions L of k. This is an immediate corollary of Artin's theorem on linear independence of distinct characters $L^\times \to \bar{k}^\times$, where $\bar{k}$ is an algebraic closure of k. ///

---

7. Involutions

Here we begin to classify involutions on semi-simple central k-algebras in terms of involutions on division algebras.

An **involution** on a ring R is a multiplication-*reversing* addition-preserving map $i : R \to R$ whose square is the identity map on R. That is, for all $r, s \in R$,

$$i(r + s) = i(r) + i(s)$$

$$i(r \cdot s) = i(s) \cdot i(r)$$

$$i(i(r)) = r$$

Proposition: Let R be a ring, and $\psi : R \to R^{\text{opp}}$ the (multiplication-reversing) bijection of R to its opposite ring R^{opp} which is the identity on the underlying set. Then the collection of involutions i on R is in bijection with the collection of ring isomorphisms $R \to R^{\text{opp}}$ by

$$i \to \psi \circ i$$

Proof: Given an involution i, $\psi \circ i$ is a ring isomorphism $R \to R^{\text{opp}}$. Conversely, an isomorphism $\varphi : R \to R^{\text{opp}}$ gives an involution $\psi^{-1} \circ \varphi$. ///

Theorem: Let Every involution σ on an Artinian simple ring B gives rise to an involution θ on the underlying division ring $D = \operatorname{End}_{B^{\text{opp}}} R$ for a simple right ideal R.

Proof: From above, an Artinian simple ring B is a finite direct sum of mutually isomorphic simple right ideals R, each $D = \operatorname{End}_{B^{\text{opp}}} R$ is a division ring, and

$$B = \operatorname{End}_{B^{\text{opp}}} B \approx M_n(\operatorname{End}_{B^{\text{opp}}} R)$$

where n is determined by

$$B \approx \underbrace{R \oplus \ldots \oplus R}_{n}$$

As noted earlier, an involution σ on B can be viewed as an isomorphism of B to its opposite ring. Thus,

$$M_n(D) \approx B \approx B^{\text{opp}} \approx M_n(D)^{\text{opp}} \approx M_n(D^{\text{opp}})$$

where (as above) the last isomorphism is transpose (and entrywise mapping D to $D^{\rm opp}$). Earlier we uniquely characterized (up to isomorphism) the division ring D so that a simple Artinian ring is isomorphic to $M_n(D)$, so we have an isomorphism $D \approx D^{\rm opp}$, which yields an involution on D. ///

Now let A be a central semi-simple algebra over a field k, and let σ be an involution on A. Say that σ is **of first kind** if it is the identity map on k, otherwise that σ is **of second kind**.

Proposition: Involutions of first kind on a central k-algebra A are in bijection with k-linear isomorphisms of A with its opposite ring. ///

Proposition: Any two involutions σ, τ of first kind on a finite-dimensional central simple algebra B over a field k differ by an inner automorphism of B, that is, there is $\gamma \in B^\times$ so that for $\beta \in B$

$$\beta^\tau = \gamma \beta^\sigma \gamma^{-1}$$

Proof: It is immediate that $\sigma \circ \tau$ is an isomorphism of B with itself, whose square is the identity map on B. Thus, by the Skolem-Noether theorem there is $\alpha \in B^\times$ so that for any $\beta \in B$

$$(\beta^\tau)\sigma = \alpha \beta \alpha^{-1}$$

Apply σ to both sides to obtain

$$\beta^\tau = (\alpha^{-1})^\sigma \beta^\sigma \alpha^\sigma$$

Letting $\gamma = (\alpha^{-1})^\gamma$ gives the result. ///

Corollary: A simple central algebra $A \approx M_n(D)$ over a field k has an involution σ of first kind if and only if D has an involution θ of first kind, and in that case there is $\gamma \mathbf{n} B^\times$ so that for all $\beta \in A$

$$\beta^\sigma = (\beta^\theta)^\top$$

where the notation means that θ is applied entrywise to a matrix β, and then the transpose is taken.

Proof: The proof is a variation of the proof above of the analogue for Artinian simple rings. That is, A is a direct sum of mutually isomorphic simple right ideals R, each $D = {\rm End}_{B^{\rm opp}} R$ is a division ring containing k in its center, and

$$B = {\rm End}_{B^{\rm opp}} B \approx M_n({\rm End}_{B^{\rm opp}} R)$$

where n is determined by

$$B \approx \underbrace{R \oplus \ldots \oplus R}_{n}$$

An involution σ of first kind on B can be viewed as a k-algebra isomorphism of B to its opposite ring. Thus,

$$M_n(D) \approx B \approx B^{\rm opp} \approx M_n(D)^{\rm opp} \approx M_n(D^{\rm opp})$$

where (as above) the last isomorphism is transpose (and entrywise mapping D to $D^{\rm opp}$). The division ring D so that $A \approx M_n(D)$ is unique up to k-algebra isomorphism, so we have a k-algebra isomorphism $D \approx D^{\rm opp}$, which yields an involution of first kind on D. ///

Remark: Not surprisingly, involutions of second kind are somewhat less tractable, in part because there may be many possibilities for the quadratic subfield of the center fixed by the involution.

---

8. Splitting by field extensions, Brauer groups

For a fixed field k, the collection of all finite-dimensional simple central algebras over k, or, equivalently, the collection of all finite-dimensional central simple division algebras over k, naturally forms a group, the

Brauer group of k, described below. Finite field extensions K of k give refinements of the structure of the Brauer group of k, from the fact that the map

$$B \to B \otimes_k K$$

(for finite-dimensional simple central algebras B over k) gives a group homomorphism from the Brauer group of k to the Brauer group of K. Further properties are catalogued below.

Two finite-dimensional central simple k-algebras A, B are **equivalent**, denoted $A \sim B$, if $A \approx M_m(D)$ and $B \approx M_n(D)$ for the same (isomorphic) underlying (finite-dimensional central simple) division algebra D over k (with possibly different matrix sizes m, n).

Proposition: The collection of equivalence classes of finite-dimensional central simple k-algebras, with 'multiplication' given by tensor product over k, forms an *abelian group*, the **Brauer group** $Br(k)$ of k. The identity element has representative k itself, and the inverse of (the class of) a finite-dimensional central simple k-algebra B is (the class of) its opposite algebra $B^{\rm opp}$.

Proof: First, the well-definedness of the equivalence follows from the well-definedness of the isomorphism class of the division algebra D so that a finite-dimensional central simple k-algebra A is isomorphic to $M_n(D)$. That is, for a simple left ideal L in A (whose isomorphism class is unique, by the definition of 'simple' ring),

$$D \approx (\mathrm{End}_B L)^{\rm opp}$$

The associativity follows from the associativity of the tensor product. The inverse property follows from the fact that

$$A \otimes_k A^{\rm opp} \approx \mathrm{End}_k A \sim k$$

which itself is a consequence of the Density Theorem. The abelian-ness of the group follows from the natural isomorphism

$$A \otimes_k B \approx B \otimes A$$

which follows from the fact that k is central in both A and B. Certainly

$$A \otimes_k k \approx A$$

which proves that (the class of) k is the identity. ///

The equivalence class of the identity is the collection of **split algebras** over k, and consists of all finite-dimensional central simple algebras isomorphic to some matrix algebra $M_n(k)$ over k.

Proposition: For a field extension K of k the map

$$A \to A \otimes_k K$$

(for finite-dimensional central simple k-algebra A) is a group homomorphism $Br(k) \to Br(K)$.

Proof: The well-definedness comes from the natural isomorphism

$$M_n(D) \otimes_k K \approx M_n(D \otimes_k K)$$

The homomorphism property is just the basic property

$$(A \otimes_k K) \otimes_K (B \otimes_k K) \approx (A \otimes_k B) \otimes_k K$$

of the tensor product. ///

For fixed k and K, and for a finite-dimensional central simple k-algebra A, if $A \otimes_k K \sim K$, that is, if $A \otimes_k K$ is a *split algebra*, then say that K **splits** A.

Corollary: For a field extension K of k, the set $Br(k, K)$ of $Br(k)$ consisting of algebras split by K is the kernel of $Br(k) \to Br(K)$, so is a subgroup of $Br(k)$. ///

Recall that an algebraic closure $\bar{k}$ of k splits *every* finite-dimensional central simple k-algebra, and that (above) this showed that the k-dimension of a finite-dimensional central (necessarily simple) division algebra over k is necessarily a *square*.

Theorem: Let D be a finite-dimensional central simple division algebra over a field k of dimension n^2.
• Every subfield K of D containing k is contained in a maximal subfield of D separable over K.
• Every maximal subfield of D has dimension n over k.
• The maximal subfields of D are those k-subalgebras which are their own centralizers in D.
• Any maximal subfield of D splits D.
• If a field K of degree n over k splits D, then there is a subfield of D isomorphic to K (and the isomorphism is the identity map on k).
• If an extension K of degree N over k splits D, then there is an imbedding $K \to M_{N/n}$ so that the image of K is its own centralizer (and the imbedding is the identity map on k).

Remark: In the course of the proof some further worthwhile information is noted.

Proof: Let K be a subfield of D containing k, and let $[K : k] < n$, and show that the centralizer Z of K in D is properly larger than K. Let D have the $= D \otimes_k K$-module structure given by

$$(\delta \otimes \alpha)x = \delta\, x\, \alpha$$

Then $Z^{\rm opp} \approx \mathrm{End}_R D$. Let

$$m = \dim_k D \,/\, \dim_k Z = n^2 \,/\, \dim_k Z$$

By Wedderburn's theorem,

$$R \approx \mathrm{End}_{Z^{\rm opp}} D \approx M_m(Z)$$

Thus, counting k-dimensions, noting that Z contains K,

$$n^2 \dim_k K = \dim_k R = \dim_k M_m(Z) = (\dim_k D / \dim_k Z)^2 \cdot \dim_k Z = n^4 / \dim_k Z = n^4/(\dim_K Z \dim_k K)$$

Therefore,

$$\dim_K Z = (n/\dim_k K)^2$$

Thus, if $[K : k] < n$ we may adjoin an element of Z to K to create a larger field. Also, maximal subfields are of degree n over k, and are their own centralizers. And every subfield is contained in a subfield of degree n over k.

Next we show that for $n > 1$ the central division algebra D contains a proper separable extension of k. If not, then there is a prime power q so that $\alpha^q \in k$ for every $\alpha \in D$. The map $\alpha \to \alpha^q$ is a polynomial map on the k-vectorspace D, and thus this property is preserved under tensoring with $\bar{k}$ over k. That is, the $q^{\rm th}$ power of every element of

$$D \otimes_k \bar{k} \approx M_n(\bar{k})$$

lies in its center. This obviously requires that $n = 1$.

Further, the arguments of the previous two paragraphs together show that every subfield K of D containing k is either of degree n over k or has a proper *separable* field extension inside D. In particular, there exists at least one separable extension of degree n over k inside D.

Let K be a maximal (degree n) subfield of D containing k. From above,

$$D \otimes_k K \approx End_{Z^{\rm opp}} D = \mathrm{End}_K D \approx M_n(K)$$

That is, K splits D.

Now suppose that K splits D, and let N be the dimension of K over k. Then

$$D^{\rm opp} \otimes_k K \approx (D \otimes_k K)^{\rm opp} \approx M_n(K)^{\rm opp} \approx M_n(K)$$

where the latter map is essentially by transpose. This simple ring has a simple module V which is an n-dimensional K-vectorspace, and by counting k-dimensions is of dimension

$$\frac{n \cdot \dim_k K}{\dim_k D^{\rm opp}} = \frac{n \cdot N}{n^2} = N/n$$

over $D^{\rm opp}$. Thus, certainly n divides N, and we have a natural imbedding

$$K \to {\rm End}_{D^{\rm opp}} V \approx M_{N/n}(D)$$

since the $D^{\rm opp}$-endomorphism ring of an ℓ-dimensional $D^{\rm opp}$ vectorspace is the matrix algebra of size ℓ over D. Let Z be the centralizer of K in $A = M_{N/n}(D)$. Let $A \otimes_k K$ act on A by

$$(\alpha \otimes \beta)x = \alpha x \beta$$

Then by definition $Z = {\rm End}_R A$, and by Wedderburn's theorem $R \approx {\rm End}_Z A$. Since $R \approx M_N(K)$ is simple, R has a unique simple module which is of K-dimension N. As A is of k-dimension N^2, A is of K-dimension N. Therefore, as the dimension of a module over a simple algebra determines its isomorphism class, it must be that A is that simple R-module. Then Z is a division algebra, and contains K. By counting k-dimensions,

$$N^3 = \dim_k A \cdot \dim_k K = \dim_k R = \dim_k({\rm End}_Z A) = \dim_k Z^{\rm opp} \cdot (\dim_Z A)^2$$

$$= \dim_k Z^{\rm opp} \cdot (\dim_k A / \dim_k Z^{\rm opp})^2 = N^4 / \dim_k Z^{\rm opp}$$

Therefore, Z can be no larger than K. ///

---

9. Tensor products of fields

In the study below of tensor products of crossed product algebras, and also in the examination below of splitting of crossed products and cyclic algebras by field extensions, a simpler yet essential sub-issue is understanding the structure of tensor products of fields.

Let K be a finite separable field extension of k, and let L be an arbitrary field extension of k. The theorem of the primitive element assures that there is $\alpha \in K$ so that $K = k(\alpha)$. Let $P(x)$ be the irreducible monic polynomial of α over k, so

$$K \approx k[x]/P$$

where $k[x]/P$ denotes the quotient of the ring $k[x]$ by the ideal generated by $P(x)$. Then

$$K \otimes_k L \approx k[x]/P \otimes_k L \approx L[x]/P$$

via the map

$$x^i \otimes c \to c\, x^i$$

Note that for a polynomial f with coefficients in k (rather than in a larger overfield), computing inside $k[x] \otimes L$,

$$f(x \otimes 1) = f(x) \otimes 1$$

Let $P = \prod_i P_i$ be the factorization of P into irreducible monics in $E[x]$. By the separability, pairwise these irreducibles have no common factors, so Sun Ze's theorem applies and

$$K \otimes_k L \approx L[x]/P \approx \bigoplus_i L[x]/P_i$$

and each $L[x]/P_i$ is a field. We can be more explicit about the last isomorphism. Let

$$\hat{P}_i(x) = \prod_{j \neq i} P_j(x)$$

and let $R_i(x) \in L[x]$ so that

$$\sum_i R_i(x)\, \hat{P}_i(x) = 1$$

Put

$$E_i = R_i(x)\, \hat{P}_i(x) \bmod P(x)$$

It is easily checked that $\{E_i\}$ is an orthogonal collection of idempotents in the commutative semi-simple L-algebra $K \otimes_k L$. The number of these idempotents matches the number of simple factors in the tensor product, so we are assured that it is a *maximal* collection. Indeed,

$$E_i \cdot (K \otimes_k L) \approx L[x]/P_i$$

and

$$K \otimes_k L = \bigoplus_i E_i \cdot (K \otimes_k L) \approx \bigoplus_i L[x]/P_i$$

As a very special case of the situation just considered, take $L = K$ and add the hypothesis that K is Galois over k, with Galois group G. Since K is Galois over k, the polynomial P factors into distinct linear factors $x - \sigma\alpha$ over K, where $\sigma \in G$. Thus, by Sun Ze's theorem,

$$K \otimes_k K \approx K \otimes_k k[x]/P \approx K[x]/P \approx \bigoplus_\sigma K[x]/(x - \sigma\alpha) \approx \underbrace{K \oplus \ldots \oplus K}_{n}$$

Note that in this case our index runs through the Galois group G. For $\sigma \in G$ the polynomials

$$Q_\sigma(x) = \prod_{\tau \neq \sigma} \frac{x - \tau\alpha}{\sigma\alpha - \tau\alpha}$$

have the property that $Q_\sigma(\tau\alpha) = 0$ for $\tau \neq \sigma$, while $Q_\sigma(\sigma\alpha) = 1$. Thus,

$$\sum_\sigma Q_\sigma(x) = 1 \bmod P(x)$$

$$Q_\sigma(x)\, Q_\tau(x) = 0 \bmod P(x) \quad \text{for } \tau \neq \sigma$$

Going back via the isomorphism $k[x] \otimes K \approx K[x]$ to $k[x] \otimes K$, the image of $Q_\sigma(x)$ is

$$\prod_{\tau \neq \sigma} \frac{x \otimes 1 - 1 \otimes \tau\alpha}{1 \otimes \sigma\alpha - 1 \otimes \tau\alpha} \in K \otimes_k K$$

Then, mapping $k[x] \to k[x]/P$ by sending x to α, thereby mapping $k[x] \otimes_k K \to k[x]/P(x) \otimes_k K$, we obtain idempotents

$$E_\sigma = \prod_{\tau \neq \sigma} \frac{\alpha \otimes 1 - 1 \otimes \tau\alpha}{1 \otimes \sigma\alpha - 1 \otimes \tau\alpha} \in K \otimes_k K$$

Note that the denominator is $1 \otimes P'(\sigma\alpha)$, and $P'(\alpha) \neq 0$ by separability. Thus, by construction, $\{E_\sigma : \sigma \in G\}$ is a maximal orthogonal set of idempotents in $K \otimes_k K$.

Next, compute

$$(\alpha \otimes 1 - 1 \otimes \sigma\alpha)\, E_\sigma = (1 \otimes P'(\sigma\alpha)^{-1}) \cdot \prod_\tau (\alpha \otimes 1 - 1 \otimes \tau\alpha)$$

and because

$$P(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_o$$

has coefficients c_i in k

$$\prod_\mu (\alpha \otimes 1 - 1 \otimes \mu\alpha) = \alpha^n \otimes 1 + \alpha^{n-1} \otimes c_{n-1} + \alpha^{n-2} \otimes c_{n-2} + \ldots + \alpha \otimes c_1 + 1 \otimes c_o$$

$$= \alpha^n \otimes 1 + c_{n-1}\alpha^{n-1} \otimes 1 + c_{n-2}\alpha^{n-2} \otimes 1 + \ldots + c_1\alpha \otimes 1 + c_o \otimes 1 = P(\alpha) \otimes 1 = 0 \otimes 1 = 0$$

Thus,

$$(\alpha \otimes 1 - 1 \otimes \sigma\alpha)\, E_\sigma = 0$$

which is the same as

$$(\alpha \otimes 1) \cdot E_\sigma = (1 \otimes \sigma\alpha) \cdot E_\sigma$$

We may take powers of both sides to see that the analogous identity holds for powers of α, as well. Further, since E_σ is an idempotent, we may *add* such identities, and thus find such an identity for all $\beta \in K$

$$(\beta \otimes 1) \cdot E_\sigma = (1 \otimes \sigma\beta) \cdot E_\sigma$$

The action of $1 \times \tau$ for $\tau \in G$ on E_σ is easy to understand. Since

$$(1 \times \tau)(\beta \otimes \gamma) = \beta \otimes \tau\gamma$$

for $\beta, \gamma \in K$, from the definition we find

$$(1 \times \tau)\, E_\sigma = E_{\tau\sigma}$$

The action of $\tau \times 1$ in $G \times \{1\}$ on E_σ is a little subtler. First, note that there are $[K : k]$ different homomorphisms $k[x] \to K$, namely by sending x to the $[K : k]$ different roots $\mu\alpha$ in K of $P(x) = 0$. Thus, for any $\mu \in G$ define

$$E_\sigma^{(\mu)} = \prod_{\tau \neq \sigma} \frac{\mu\alpha \otimes 1 - 1 \otimes \tau\alpha}{1 \otimes \sigma\alpha - 1 \otimes \tau\alpha}$$

Then

$$\{E_\sigma^{(\mu)} : \sigma \in G\}$$

is a maximal orthogonal collection of idempotents in $K \otimes_k K$. Therefore, the set of such must be the same regardless of μ, but the bijections between such sets for differing μ are not immediately clear. Partly to determine the bijection, but also to understand the action of $\tau \times 1$, we apply $\mu \times 1$ to the expression defining E_σ

$$(\mu \times 1)E_\sigma = \prod_{\tau \neq \sigma} \frac{\mu\alpha \otimes 1 - 1 \otimes \tau\alpha}{1 \otimes \sigma\alpha - 1 \otimes \tau\alpha} = E_\sigma^{(\mu)}$$

On the other hand, applying $\mu \times 1$ to both sides of the identity

$$(\beta \otimes 1) \cdot E_\sigma = (1 \otimes \sigma\beta) \cdot E_\sigma$$

gives

$$(\mu\beta \otimes 1) \cdot (\mu \times 1)E_\sigma = (1 \otimes \sigma\beta) \cdot (\mu \times 1)E_\sigma$$

Replace β by $\mu^{-1}\beta$ and use $(\mu \times 1)E_\sigma = E_\sigma^{(\mu)}$ to obtain

$$(\beta \otimes 1) \cdot E_\sigma^{(\mu)} = (\beta \otimes 1) \cdot (\mu \times 1)E_\sigma = (\beta \otimes 1) \cdot E_\sigma^{(\mu)} = (1 \otimes \sigma\mu^{-1}\beta) \cdot (\mu \times 1)E_\sigma = (1 \otimes \sigma\mu^{-1}\beta) \cdot E_\sigma^{(\mu)}$$

This property uniquely characterizes $E_{\sigma\mu^{-1}}$, so we conclude that

$$(\mu \times 1)E_\sigma = E_{\sigma\mu^{-1}}$$

For applications we need a slightly more general version of the last computation, namely $K \otimes_k L$ with K Galois over K and $k \subset L \subset K$. Let K have Galois group G over k, and let H be the subgroup of G fixing L. Keeping the notation from just above, let

$$E_{H\sigma} = \sum_{\mu \in H\sigma} E_\mu = \sum_{\eta \in H} (1 \times \eta)\, E_\sigma$$

(The second equality follows from properties noted just above.) The second equality shows that $E_{H\sigma}$ lies in the fixed subring in $K \otimes_k K$ of the Galois group $\{1\} \times H$. To be able to invoke ordinary Galois theory to conclude that therefore $E_{H\sigma}$ lies in $K \otimes_k L \subset K \otimes_k K$, look at the preimage in $k[x] \otimes_k K$, namely

$$\sum_{\mu \in H} \prod_{\tau \neq \sigma} \frac{x \otimes 1 - 1 \otimes \mu\tau\alpha}{1 \otimes \mu\sigma\alpha - 1 \otimes \mu\tau\alpha}$$

Under the natural isomorphism $k[x] \otimes_k K \to K[x]$ this yields a polynomial with coefficients in the fixed field L of H inside K. Thus, this entity is in $L[x]$, which is in bijection with $k[x] \otimes_k L$, which maps to $K \otimes_k L$ as desired. From the idempotent properties of the E_σ's, it follows immediately that

$$\{E_{H\sigma} : H\sigma \in H\backslash G\}$$

is a set of orthogonal idempotents. Their number, namely $|G|/|H|$, is equal to the known number of simple factors in $K \otimes_k L$, namely $[L : k]$, by Galois theory. Thus, this set is maximal. The action of $G \times \{1\}$ on these idempotents follows from the previous determination of the action on the underlying idempotents. That is,

$$(\tau \times 1)\, E_{H\sigma} = E_{H\sigma\tau^{-1}}$$

Other salient properties follow similarly from the computations above for the underlying idempotents E_σ.

---

10. Crossed product construction of simple algebras

The *crossed product* construction given below yields all finite-dimensional central algebras over a field k, up to isomorphism. Various aspects and refinements of this construction are used in the sequel.

Let k be a field, K a finite Galois extension of k with Galois group G. Let A be a (left) K-vectorspace with (left) K-basis $\{e_\sigma : \sigma \in G\}$, so

$$A = \bigoplus_{\sigma \in G} K \cdot e_\sigma$$

We wish to construct a central k-algebra structure on A related to the natural action of G on the indices for the K-basis and the action of G on K. For $\beta \in K$ and $\sigma, \tau \in G$, define

$$e_\sigma\, \beta = \beta^\sigma\, e_\sigma$$

and

$$e_\sigma\, e_\tau = f(\sigma, \tau)\, e_{\sigma\tau}$$

for a K-valued function f on $G \times G$ with additional properties to be specified shortly. These operations give a k-bilinear map $A \times A \to A$ which is left K-linear in the first argument, although the requirement of *associativity* surely puts a non-trivial condition on what f may be. It is clear that distributivity with respect to addition is no problem, so we only need consider associativity of monomials βe_σ with $\beta \in K$. In fact, it is not hard to see that it suffices to consider associativity of monomials e_σ, since the coefficients in K are not an obstacle to associativity.

To lighten notation, we may write

$$f_{\sigma,\tau} = f(\sigma, \tau)$$

Computing, on one hand

$$(e_\sigma e_\tau)e_\mu = f_{\sigma,\tau}\, e_{\sigma\tau} e_\mu = f_{\sigma,\tau} f_{\sigma\tau,\mu}\, e_{\sigma\tau\mu}$$

On the other hand,

$$e_\sigma(e_\tau e_\mu) = e_{\sigma\tau} f_{\tau,\mu} e_{tau\mu} = f^\sigma_{\tau,\mu} e_\sigma e_{\tau\mu} = f^\sigma_{\tau,\mu} f_{\sigma,\tau\mu} e_{\sigma\tau\mu}$$

Thus, the associativity condition is equivalent to the so-called **cocycle condition**

$$f_{\sigma,\tau}\, f_{\sigma\tau,\mu} = f^\sigma_{\tau,\mu}\, f_{\sigma,\tau\mu}$$

(and such f is a **cocycle**). Since the fixed field of G in K is exactly k, it is easy to see that the center of this algebra is exactly k. Write

$$A(k, K, f)$$

for the associative k-algebra defined as just above, assuming of course that f satisfies the cocycle condition. Such $A(k, K, f)$ is called a **crossed product** algebra.

The issue remains of testing for k-algebra isomorphism among these algebras constructed as crossed products. First, we consider special sorts of (left) K-linear maps

$$\Phi : A(k, K, f) \to A(k, K, g)$$

of the form

$$\Phi(\sum_\sigma \beta_\sigma e_\sigma) = \sum_\sigma \beta_\sigma\, \varphi(\sigma)\, e_\sigma$$

for $\sigma \in G$, $\beta_\sigma \in K$, where φ is a $K^\times$-valued function on the Galois group G. For such a map to be a ring homomorphism, it evidently is necessary and sufficient that

$$\Phi(e_\sigma\, e_\tau) = \Phi(e_\sigma)\, \Phi(e_\tau)$$

That condition is

$$f_{\sigma,\tau}\, \varphi(\sigma\tau)\, e_{\sigma\tau} = \Phi(f_{\sigma,\tau}\, e_{\sigma\tau}) = \Phi(e_\sigma\, e_\tau) = \Phi(e_\sigma)\, \Phi(e_\tau) = \varphi(\sigma) e_\sigma\, \varphi(\tau) e_\tau = \varphi(\sigma)\varphi(\tau)^\sigma\, g(\sigma,\tau)\, e_\sigma\, e_\tau$$

Thus, the condition for this special sort of map to be a k-algebra isomorphism is

$$f_{\sigma,\tau} = \varphi(\sigma)\varphi(\tau)^\sigma \varphi(\sigma\tau)^{-1}\, g(\sigma,\tau)$$

Thus, the latter condition is *sufficient* for isomorphism $A(k, K, f) \to A(k, K, g)$, and is *necessary* for the isomorphism to be of the special form indicated.

With this construction as motivation, define **two-cochains**

$$C^2(G, K^\times) = \{\ K^\times\text{-valued functions on } G \times G\ \}$$

which is an abelian group under pointwise multiplication. An element σ in the Galois group G acts on two-cocycles f pointwise, namely, by

$$(\sigma f)(\mu, \nu) = f(\mu, \nu)^\sigma$$

The define the **two-cocycles**

$$Z^2(G, K^\times) = \{f \in C^2(G, K^\times) : f_{\sigma,\tau}\, f_{\sigma\tau,\mu} = f^\sigma_{\tau,\mu}\, f_{\sigma,\tau\mu}\}$$

(using lighter notation as above). Define the **two-coboundaries**

$$B^2(G, \mathbf{K}^\times) = \{f \in C^2(G, K^\times) :\ \text{for some } \varphi : G \to K^\times\ f(\sigma,\tau) = \varphi(\sigma)\, \varphi(\tau)^\sigma\, \varphi(\sigma\tau^{-1})\}$$

One may verify that $B^2(G, K^\times) \subset Z^2(G, K^\times)$. The **second cohomology** group of G with coefficients in $K^\times$ is defined to be

$$H^2(G, K^\times) = Z^2(G, K^\times)/B^2(G, K^\times)$$

We have just shown that the collection of associative k-algebra structures on A, modulo the *special* isomorphisms above, is isomorphic to $H^2(G, K^\times)$. The next theorem in part shows that existence of an arbitrary isomorphism implies the existence of an isomorphism of this special form.

Theorem:
• The centralizer of K in $A(k, K, f)$ is K itself.
• Crossed products $A(k, K, f)$ over k are central simple k-algebras.
• Two crossed product algebras $A(k, K, f)$ and $A(k, K, g)$ are isomorphic as central k-algebras if and only if there is a central k-algebra isomorphism Φ of the form

$$\Phi(e_\sigma) = \varphi(\sigma)\, e_\sigma$$

for $\sigma \in G$, where φ is a K-valued function on the Galois group G.

Proof: The multiplicative identity in $A = A(k, K, f)$ is readily seen to be $f_{1,1}^{-1} e_1$, where 1 is the identity in G. The copy $K \cdot e_1$ of K in A is readily verified to be its own centralizer in A. To see that A is simple, suppose $J \neq A$ were a two-sided ideal, and let $q : A \to A/J$ be the quotient map. We claim that q is an injection on the image $K \cdot e_1$ of K in A. If not, then (since K is a field) $q(K \cdot e_1) = \{0\}$, and therefore

$$q(A) = q(K \cdot A) = q(K \cdot e_1 \cdot A) = q(K \cdot e_1) \cdot q(A) = 0 \cdot q(A) = 0$$

Thus, indeed, q is an injection on K. Next, we claim that the elements $q(e_\sigma)$ are a K-basis for $q(A)$ (which would prove the injectivity of q, whence that $J = \{0\}$). Let

$$\sum_\sigma \beta_\sigma\, q(e_\sigma) = 0$$

be a shortest non-trivial relation. Then

$$\sum_\sigma \beta_\sigma\, e_\sigma \in J$$

By right multiplication by some e_τ we may suppose that $\beta_1 \neq 0$, and then that $\beta_1 = 1$ by suitable left multiplication by $K^\times$. Then right multiplication by $\alpha \in K^\times$ and left multiplication by α^{-1} gives

$$\alpha^{-1}(e_1 + \sum_{\sigma \neq 1} \beta_\sigma\, e_\sigma)\alpha = e_1 + \sum_{\sigma \neq 1} \alpha^{-1}\beta^\sigma\, \alpha_\sigma\, e_\sigma \in J$$

Now note every $\alpha^{-1}\alpha^\sigma$ can be 1 for α taken not in k, so we can subtract

$$e_1 + \sum_{\sigma \neq 1} \alpha^{-1}\alpha^\sigma\, \beta_\sigma\, e_\sigma$$

from

$$e_1 + \sum_{\sigma \neq 1} \beta_\sigma\, e_\sigma$$

to get a shorter non-trivial linear combination in J, contradiction. Thus, $J = \{0\}$, and A is simple.

Now we show that existence of a k-algebra isomorphism $\Psi : A(k, K, f) \to A(k, K, g)$ implies the existence of an isomorphism of the special form above. By the Skolem-Noether theorem, there is $\gamma \in B^\times$ so that

$$\gamma\Psi(K \cdot e_1)\gamma^{-1} = K \cdot e_1$$

Thus, adjusting Ψ by this conjugation, we may assume without loss of generality that

$$\Psi(K \cdot e_1) = K \cdot e_1$$

Thus,

$$\Psi(\beta \cdot e_1) = \beta^\tau \cdot e_1$$

for some $\tau \in G$. Invoking Skolem-Noether again, further adjusting Ψ so as to undue this Galois conjugation, we may assume without loss of generality that Ψ is the identity on the imbedded copy of K in the two algebras, namely

$$\Psi(\beta \cdot e_1) = \beta \cdot e_1$$

for $\beta \in K$. Then for $\beta \in K$, in $A(k, K, g)$

$$e_\sigma \Psi(e_\sigma)^{-1}\, \Psi(\beta \cdot e_1)\Psi(e_\sigma)e_\sigma^{-1} = e_\sigma \Psi(e_\sigma^{-1}\beta \cdot e_1 e_\sigma)e_\sigma^{-1} = e_\sigma \Psi(\beta^{\sigma^{-1}} \cdot e_1)e_\sigma^{-1}$$

$$= e_\sigma \beta^{\sigma^{-1}} \cdot e_1 e_\sigma^{-1} = (\beta^{\sigma^{-1}})^\sigma \cdot e_1 = \beta \cdot e_1$$

Since $K \cdot e_1$ is its own centralizer in $A(k, K, g)$, it must be that $e_\sigma \Psi(e_\sigma)^{-1} \in K \cdot e_1$ for all $\sigma \in G$. That is, Ψ is of the special form given above. ///

The previous theorem determines the isomorphism classes of crossed-product algebras constructed via a Galois extension K of the central field k. The following shows that *every* finite-dimensional central simple k-algebra occurs in such a construction, at least up to equivalence in the Brauer group.

Theorem: Let A be a finite-dimensional central simple k-algebra, and let K be a finite Galois extension of k splitting A. Then there is a cocycle f so that

$$A(k, K, f) \sim A$$

Proof: From above, $A \approx M_n(D)$ for some central division algebra D over k, and it must be that K splits D. Therefore, from above, there is a matrix algebra $A' = M_m(D)$ into which K imbeds so as to be its own centralizer, and then necessarily the k-dimension of A' is $[K : k]^2$. By Skolem-Noether, any automorphism of K can be extended to an inner automorphism of A'. In particular, for all $\sigma \in G$ there is $e_\sigma \in A'$ so that for all $\beta \in K$

$$\beta^\sigma = e_\sigma\, \beta\, e_\sigma^{-1}$$

For $\sigma, \tau \in G$, define

$$f(\sigma, \tau) = e_\sigma\, e_\tau\, e_{\sigma\tau} \in A'$$

It is easy to check that this element $f(\sigma, \tau)$ of A' commutes with every element of K, so lies in K. Since multiplication in A' is associative, this f satisfies the cocycle condition. We have the obvious non-zero surjection of $A(k, K, f)$ to the subalgebra

$$A'' = \{\sum_{\sigma \in G} \beta_\sigma e_\sigma\}$$

which is an injection since $A(k, K, f)$ is simple. By counting k-dimensions, $A'' = A'$. Thus, we have constructed a crossed product in the same Brauer group class as the given algebra A. ///

To complete the basic description of (equivalence classes of) finite-dimensional central simple k-algebras as crossed products, we must examine the behavior of crossed products under tensor products over k.

Theorem:

$$A(k, K, f) \otimes_k A(k, K, g) \sim A(k, K, fg)$$

That is, the tensor product of two crossed products is equivalent to the crossed product obtained by pointwise multiplication of the cocycles.

Proof: Let G be the Galois group of K over k, with $[K:k] = n$. Let $\alpha \in K$ be such that $K = k(\alpha)$, and as earlier define a maximal orthogonal collection of idempotents in $K \otimes_k K$, indexed by $\sigma \in G$, by

$$E_\sigma = \prod_{\tau \neq \sigma} \frac{\alpha \otimes 1 - 1 \otimes \tau\alpha}{1 \otimes \sigma\alpha - 1 \otimes \tau\alpha}$$

In the tensor product $B = A(k, K, f) \otimes_k A(k, K, g)$, conjugation by any element $e_\sigma \otimes \tau$ stabilizes the subalgebra $K \otimes_k K$, so must permute the simple factors $K \cdot E_\sigma$, and therefore must permute the idempotents E_σ. Specifically, from the relation

$$(\alpha \otimes \beta)\, E_\sigma = (\alpha\beta^\sigma \otimes 1)\, E_\sigma$$

we have

$$(e_\sigma \otimes e_1) E_\tau (e_\sigma \otimes e_1)^{-1} = E_{\sigma\tau}$$

$$(e_1 \otimes e_\sigma) E_\tau (e_1 \otimes e_\sigma)^{-1} = E_{\tau\sigma^{-1}}$$

Now claim that

$$E_1 \left(A(k, K, f) \otimes_k A(k, K, g)\right) E_1 \approx A(k, K, fg)$$

To this end, we need a K-basis $\{v_\sigma\}$ so that the multiplication in those coordinates is obviously the same as that in $A(k, K, fg)$. Take $v_\sigma = E_1(e_\sigma \otimes e_\sigma)E_1$. The conjugation formula yields

$$v_\sigma\, v_\tau = E_1(e_\sigma \otimes e_\sigma)E_1 E_1(e_\tau \otimes e_\tau)E_1 = E_1 E_{\sigma 1 \sigma^{-1}}(e_\sigma \otimes e_\sigma)(e_\tau \otimes e_\tau)E_1$$

$$= E_1 E_1 (e_\sigma \otimes e_\sigma)(e_\tau \otimes e_\tau)E_1 = E_1(f_{\sigma,\tau} e_{\sigma\tau} \otimes g_{\sigma,\tau} e_{\sigma\tau})E_1$$

Using the case $\sigma = 1$ of

$$(1 \otimes \alpha)E_\sigma = (\alpha^\sigma \otimes 1)E_\sigma$$

the product becomes

$$E_1 f_{\sigma,\tau} g_{\sigma,\tau} (e_{\sigma\tau} \otimes e_{\sigma\tau}) E_1$$

Giving $E_1 B E_1$ the K-vectorspace structure arising from $\beta \to \beta \otimes 1$, this shows that

$$E_1 B E_1 \approx A(k, K, fg)$$

as desired. In fact, a similar computation shows that for *any* index σ we have $E_\sigma B E_\sigma \approx A(k, K, fg)$.

To finish the proof, we must show that for a simple algebra B if there is a simple algebra C and a set of orthogonal idempotents E_σ with $E_\sigma B E_\sigma \approx C$ for all indices σ, then B is isomorphic to a matrix algebra with entries in C. To prove this, let $C = E_1 B E_1$. For any index σ, by Skolem-Noether there is $z \in B^\times$ so that $E_\sigma B E_\sigma = z C z^{-1}$. In particular, $E_\sigma = z E_1 z$. Thus,

$$E_\sigma B E_1 = z E_1 z^{-1} B E_1 = z E_1 B E_1$$

Thus, the $E_\sigma B E_1$'s are all isomorphic as right C^{opp}-modules. now

$$\text{End}_{C^{\text{opp}}}(E_1 B E_1) = \text{End}_{C^{\text{opp}}} C = C$$

so for every index σ

$$\text{End}_{C^{\text{opp}}} E_\sigma B E_1) \approx C$$

Let $R = B \otimes_k C^{\text{opp}}$ act on

$$V = BE_1 = \bigoplus_\sigma E_\sigma B E_1 \subset B$$

in the natural manner by

$$(\alpha \otimes \gamma)(\sum_\sigma E_\sigma \beta_\sigma E_1) = \alpha \sum_\sigma E_\sigma \beta_\sigma E_1\, \gamma$$

This yields a k-algebra homomorphism

$$\varphi : B \to \mathrm{End}_{C^{\mathrm{opp}}} V$$

Since $1_V \in A$, $\varphi(A)$ is not 0. Since A is simple, A has no proper two-sided ideals, so φ is injective. As a C^{opp}-module, we saw that V is isomorphic to C^n, so $\mathrm{End}_{C^{\mathrm{opp}}} V \approx M_n(C)$. Since $B = \bigoplus_{\sigma,\tau} E_\sigma B E_\tau$, and since $E_\sigma B E_\tau \approx C$ as C^{opp}-modules, by counting k-dimensions we at last find that φ is an isomorphism of B to the indicated matrix algebra over C. ///

Corollary: For a fixed finite Galois extension K of k, the map from $H^2(G, K^\times)$ to the Brauer group of k given by $f \to A(k, K, f)$ is a bijective group homomorphism to the subgroup $Br(k, K)$ of $Br(k)$ consisting of (equivalence classes of) finite-dimensional central simple k-algebras split by K. ///

A similar argument proves that extension of scalars behaves in a reasonable manner on crossed product algebras.

Theorem: Let K be a finite Galois extension of the field k, with intermediate field E, and let H be the subgroup of G so that E is the fixed field of H. Then, for any cocycle f, in the Brauer group of E we have an equivalence of crossed product algebras

$$A(k, K, f) \otimes kE \sim A(E, K, f|_{H\times H})$$

where, as earlier, $A(k, K, f)$ is the crossed product algebra constructed via the extension K of k and $K^\times$-valued cocycle f on $G \times G$, and $f|_{H\times H}$ is the restriction of f to $H \times H \subset G \times G$.

Proof: The technical aspects of the proof are very similar in nature to those in the determination of the equivalence class of the tensor product of two crossed products over k. And, similarly, we need a preliminary computation of tensor products of fields. Let $A = A(k, K, f)$. As earlier, for $\sigma \in G$ let

$$E_{H\sigma} = \sum_{\mu\in H\sigma} \prod_{\tau\neq\sigma} \frac{\alpha \otimes 1 - 1 \otimes \mu\tau\alpha}{1 \otimes \mu\sigma\alpha - 1 \otimes \mu\tau\alpha}$$

be a maximal orthogonal collection of idempotents in $K \otimes_k L \subset A \otimes_k L$. Let $\{e_\sigma : \sigma \in G\}$ be the usual K-basis in the construction of A. Conjugation in $A \otimes_k L$ by e_σ stabilizes $K \otimes_k L$, so must permute the idempotents $E_{H\tau}$ (by the structure theorem applied to the commutative semi-simple L-algebra $K \otimes_k L$). Let

$$(e_\sigma \otimes 1)\, E_{H\tau}\, (e_\sigma \otimes 1)^{-1} = E_{H\mu}$$

for some $H\mu \in H\backslash G$. We will determine $H\mu$ via the characterization

$$(1 \otimes \nu\beta)E_{H\nu} = (\beta \otimes 1)E_{H\mu}$$

of $E_{\mathbf{H}\nu}$, for $\beta \in L$. On one hand,

$$(e_\sigma \otimes 1)\, (1 \otimes \tau\beta)E_{H\tau}\, (e_\sigma \otimes 1)^{-1} = (1 \otimes \tau\beta)E_{H\mu}$$

and on the other hand

$$(e_\sigma \otimes 1)\, (\beta \otimes 1)E_{H\tau}\, (e_\sigma \otimes 1)^{-1} = (\sigma\beta \otimes 1)E_{H\mu}$$

As $(1 \otimes \tau\beta)E_{H\tau} = (\beta \otimes 1)E_{H\tau}$, upon replacing β by $\sigma^{-1}\beta$ we have

$$(1 \otimes \tau\sigma^{-1}\beta)E_{H\mu} = (\beta \otimes 1)E_{H\mu}$$

From the characterization

$$(1 \otimes \nu\beta)E_{H\nu} = (\beta \otimes 1)E_{H\nu}$$

we conclude that

$$(e_\sigma \otimes 1)\, E_{H\tau}\, (e_\sigma \otimes 1)^{-1} = E_{H\tau\sigma^{-1}}$$

As this conjugation action is visibly transitive on the idempotents $E_{H\sigma}$, all the subalgebras $E_{H\sigma}(A\otimes_k L)E_{H\sigma}$ are isomorphic as central L-algebras. As we saw in our earlier discussion of tensor products of crossed product algebras, $A\otimes_k L$ is isomorphic to a matrix algebra over $E_H(A\otimes_k L)E_H$. From the conjugation properties just above, and from the orthogonality of the idempotents, we find that unless $H\tau = H\mu\sigma^{-1}$

$$E_{H\tau}(e_\sigma\otimes 1)E_{H\mu} = E_{H\tau}\,E_{H\mu\sigma^{-1}}\,(e_\sigma\otimes 1) = 0$$

In particular, by counting dimensions, it must be that

$$\bigoplus_{\sigma\in H} Ke_\sigma\otimes L \to E_H\,(\bigoplus_{\sigma\in G} Ke_\sigma\otimes L)\,E_H$$

is an injection. Since K and L commute with E_H, for $\sigma\tau\in H$ we have

$$E_H(e_\sigma\otimes 1)E_H\cdot E_H(e_\tau\otimes 1)E_H = E_H(e_\sigma\otimes 1)(e_\tau\otimes 1)E_H$$

from which the theorem follows easily. ///

---

11. Cyclic algebra construction of simple algebras

Cyclic algebras are the special case of the crossed product construction in which the Galois extension K of the base field k is *cyclic* (has cyclic Galois group). This special case is sufficiently general to treat the case of p-adic fields, as we will see later. (The latter fact is certainly good news, since then the structure of finite-dimensional central simple algebras over p-adic fields is more transparent than we might have expected.) In this context we give a slightly frivolous proof of Wedderburn's theorem that finite division rings are fields. The element of frivolity resides in the fact that, while the result comes out very simply from discussion of cyclic algebras, the result has a more elementary proof that is usually given. For finite-dimensional central simple algebras constructed as cyclic algebras we can often understand completely the structure of the algebra as a matrix algebra $M_n(D)$ over a division algebra D. In particular, we can often give clear necessary and conditions for cyclic algebras to be division algebras.

Let K be a *cyclic* finite Galois extension of the field k with Galois group generated by σ, with $[K;k] = n$. Consider cocycles of the special form

$$f(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{for } i+j<n \\ \gamma & \text{for } i+j\geq n \end{cases}$$

for some $\gamma\in k^\times$. Then the crossed product algebra $A(k,K,f)$ is called a **cyclic algebra**. We write $C(k,K,\gamma)$ for this cyclic algebra.

Theorem: For cyclic Galois extensions K of k, all isomorphism classes of crossed product algebras $A(k,K,f)$ have representatives which are cyclic algebras. Further, the cyclic algebras $C(k,K,\gamma)$ and $C(k,K,\gamma')$ are isomorphic as k-algebras if and only if

$$\gamma/\gamma'\in \mathrm{Norm}_{K/k}(K^\times)$$

Indeed, depending upon the choice of generator of the Galois group, we have a group isomorphism

$$\varphi_K : H^2(G,K^\times)\approx Gr(k,K)\approx k^\times/\mathrm{Norm}_{K/k}(K^\times)$$

Proof: We keep the notation of the previous section on crossed products. Recall that, given a cocycle f, $f(1,1)^{-1}e_1$ is the identity in the crossed product algebra $A(k,K,f)$. Let

$$\mu_i = (e_\sigma)^i\,(e_{\sigma^i})^{-1}$$

It is easy to check that μ_i centralizes (the image of) K, so lies in (the image of) K since we know that maximal subfields are their own centralizers. Thus,

$$(e_\sigma)^i = \mu_i \, e_{\sigma^i}$$

expresses $(e_\sigma)^i$ in terms of the basis e_{σ^j}'s. Thus, the elements

$$E_i = (e_\sigma)^i$$

are a K-basis for the algebra. Replacing e_{σ^i} by E_i visibly transforms f into another cocycle of the form asserted. The cocycle condition further shows that γ lies not merely in $K^\times$, but in $k^\times$.

As shown in the last section, two elements γ, γ' give isomorphic algebras if and only if the corresponding cocycles f and f' satisfy $f/f' \in B^2(G, K^\times)$. That is, there should be $\varphi : G \to K^\times$ so that

$$(f/f')(\sigma^i, \sigma^j) = \varphi(\sigma^i)\, \varphi(\sigma^j)^{\sigma^i}\, \varphi(\sigma^{i+j})^{-1}$$

When f and f' are of the special form as above, this condition is

$$\varphi(\sigma^i)\, \varphi(\sigma^j)^{\sigma^i}\, \varphi(\sigma^{i+j})^{-1} = \begin{cases} 1 & \text{for } i+j < n \\ \gamma/\gamma' & hbox for i+j < n \end{cases}$$

The first of these conditions is equivalent to the condition that $\varphi(\sigma^0) = 1$, and for $i < n-1$

$$\varphi(\sigma^{i+1}) = \varphi(\sigma)\, \varphi(\sigma^i)^\sigma$$

That is, $\varphi(\sigma)$ determines all the other values of φ. Inductively,

$$\varphi(\sigma^i) = \varphi(\sigma)\, \varphi(\sigma)^\sigma\, \varphi(\sigma)^{\sigma^2}\, \varphi(\sigma)^{\sigma^3}\, \dots \varphi(\sigma)^{\sigma^{i-1}}$$

Then the second condition becomes

$$1 = \varphi(\sigma^0) = \varphi(\sigma^n) = (\gamma'/\gamma)\, \varphi(\sigma)\, \varphi(\sigma^{n-1})^\sigma = (\gamma'/\gamma)\, \mathrm{Norm}_{K/k}(\varphi(\sigma))$$

This gives the indicated result.

That the obvious map of $Br(k, K)$ to $k^\times/\mathrm{Norm}_{K/k}(K^\times)$ is a group homomorphism follows from the general fact for arbitrary crossed products (above) that

$$A(k, K, f) \otimes_k A(k, K, g) \sim A(k, K, fg)$$

This finishes the theorem. ///

Corollary: Every finite division ring is commutative, hence, is a field.

Proof: Let D be a finite division ring. Then D is finite-dimensional over its center k, which is a finite field. Let K be a maximal subfield of D. From the theory of finite fields, the Galois group of K over k is cyclic. From above, D is equivalent to a cyclic algebra constructed via K. But norms on finite fields are surjective, so $Br(k, K) \approx \{1\}$. That is, $D = k$. ///

Corollary: Suppose that K is cyclic Galois over k with Galois group G of order N generated by σ, and $A = A(k, K, f)$ the simple algebra with cocycle f defined (for fixed $\gamma \in k^\times$) by

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < N \\ \gamma & \text{for } i+j \geq N \end{cases}$$

Let d be the smallest positive integer so that

$$\gamma^d \in \mathrm{Norm}_{K/k} K^\times$$

Then in the Brauer group of k we have $A \sim D$ for a central division algebra D over k of dimension d^2. In particular, A itself is a division algebra if and only if N is the least positive integer so that γ^N is a norm from K.

Proof: Let L be an intermediate field between k and K, so that K has Galois group H over L. Let $B = A(L, K, f)$ be the central simple algebra over L defined via the restriction of the cocycle f to $H \times H$. We have seen that B is split if and only if $\gamma \in \mathrm{Norm}_{K/L} K^\times$, and also $A \otimes_k L \sim B$. Thus, A splits over L if and only if γ lies in $\mathrm{Norm}_{K/L} K^\times$.

We claim that if $\gamma^d = \mathrm{Norm}_{K/k}\varepsilon$ with $\varepsilon \in K^\times$, then d divides $[K : k] = N$. Indeed, write the greatest common divisor δ of d and N as $\delta = rd + sN$ with integers r, s, and then

$$\mathrm{Norm}_{K/k}(\varepsilon^r \gamma^s) = \gamma^{dr} \gamma^{Ns} = \gamma^\delta$$

Thus, as K is cyclic over k, there is an intermediate field L with $[L : k] = d$, and $\gamma = \mathrm{Norm}_{K/L}\varepsilon$. That is, L splits A. Therefore, A is isomorphic to a matrix algebra over a central division algebra D over k with the k-dimension of D at most d^2. On the other hand, if D were of dimension n^2 with $n < d$, then D would be split by an intermediate field L of degree n over k. Then $\mathrm{Norm}_{K/L}\eta = \gamma$ for some $\eta \in K^\times$.

$$\mathrm{Norm}_{K/k}\eta = \mathrm{Norm}_{L/k}\,\mathrm{Norm}K/L\eta = \gamma^n$$

Therefore, in fact d divides $[L : k]$, and D is of dimension exactly d^2 over k. ///

Proposition: Let K be a Galois extension of k with Galois group G, and let L be a field extension of k linearly disjoint from K over k. Identify $K \otimes_k L$ with a compositum KL of K and L in some field containing k. Identify G with the Galois group of KL over L, by

$$\sigma(x \otimes y) = \sigma x \otimes y$$

Then, for any $K^\times$-valued cocycle f on $G \times G$,

$$A(k, K, f) \otimes_k L \approx A(L, KL, f)$$

Proof: The linear disjointness assures that any compositum of K and L is indeed isomorphic to $K \otimes_k L$. Consider the left K-linear map

$$\varphi : A(k, K, f) \otimes_k L \to A(L, KL, f)$$

given by

$$\varphi(e_\sigma \otimes x) = x\tilde{e}_\sigma$$

where $x \in L$, $\{e_\sigma\}$ is the K-basis used to construct $A(k, K, f)$, and $\{\tilde{e}_\sigma\}$ is the KL-basis used to construct $A(L, KL, f)$. Since $x \in L$ commutes with the $\tilde{e}_\sigma$'s, this map is also L-linear. All that remains to check is that

$$\varphi((e_\sigma \otimes 1)(e_\tau \otimes 1)) = \tilde{e}_\sigma \tilde{e}_\tau$$

Indeed,

$$\varphi((e_\sigma \otimes 1)(e_\tau \otimes 1)) = \varphi(f(\sigma, \tau)\,(e_{\sigma\tau} \otimes 1)) = f(\sigma, \tau)\, ph(e_{\sigma\tau} \otimes 1)) = f(\sigma, \tau)\,\tilde{e}_{\sigma\tau} = \tilde{e}_\sigma \tilde{e}_\tau$$

as desired. ///

---

12. Quaternion algebras

Four-dimensional central simple algebras play a special role, in part because they have a canonical involution of first kind. This construction is purely algebraic and is therefore completely general. Recall that it followed from the Skolem-Noether theorem every other involution of first kind differs from a given one by conjugation.

For us, a **quaternion algebra** over a field k is a central simple algebra of dimension 4 over k. We showed via the crossed product construction that every n^2-dimensional central simple algebra over a field is split by a separable extension of degree n over the center. Thus, quaternion algebras are split by separable quadratic extensions, which are necessarily *cyclic*. Thus, quaternion algebras are always cyclic algebras.

Proposition: Let B be a quaternion algebra over a field k. There is an involution of first kind, the **main involution** $\natural$, given by

$$\beta^\natural = \text{reduced trace}\beta - \beta$$

We have

$$\text{reduced trace}\beta = \beta + \beta^\natural$$

$$\text{reduced norm}\beta = \beta \cdot \beta^\natural$$

Proof: We must show that the map $\beta \to \beta^\natural$ is an involution and is trivial on the center k. If would suffice to prove these assertions for $B \otimes_k K$ where K is a field extension of k splitting B. We know that $B \otimes_k K$ is a two-by-two matrix algebra over K. Reduced trace respects tensor products, so the K-linear extension of $\natural$ is still given by the same expression, with reduced trace being the reduced trace in the matrix algebra. Then we observe that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\natural = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^\top \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}$$

Since transpose is an involution, this proves that $\natural$ is an involution. Triviality on the center is clear. (The fact that reduced norm is given by the indicated formula is also easy.) ///

---

13. Examples

The cyclic algebra construction makes possible some relatively straightforward construction of division algebras of dimension N^2 over $\mathbf{Q}$ for arbitrary integers N. And, using Galois extensions with dihedral Galois groups, the crossed product construction yields examples of algebras with involutions of second kind.

Fix a positive integer N, and let q be a prime congruent to 1 modulo n. (By Dirichlet's theorem on primes in arithmetic progressions there are infinitely many such q.) Let E be the field generated over $\mathbf{Q}$ by a primitive q^{th} root of unity, and let K be the subfield of E which is cyclic over $\mathbf{Q}$ of degree n, with Galois group generated by σ. For $\gamma \in \mathbf{Q}^\times$, we have the cyclic algebra

$$A(\gamma) = A(\mathbf{Q}, K, f)$$

given by

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < n \\ \gamma & \text{for } i+j \geq n \end{cases}$$

We saw above that $A(\gamma)$ is a division algebra if and only if $\ell = n$ is the smallest positive integer so that γ^ℓ is a norm from K.

Proposition: Let p be a prime number so that p generates the cyclic group $(\mathbf{Z}/q)^\times$. (By Dirichlet's theorem, there are infinitely many such primes congruent to a given primitive root modulo q.) Then the cyclic algebra $A(p)$ described just above is a central division algebra over $\mathbf{Q}$ of dimension n^2.

Proof: The condition on p is that $\ell = q-1$ is the smallest positive integer so that $p^\ell = 1 \bmod q$. That is, $\ell = q-1$ is the smallest integer so that q divides $p^\ell - 1$, which is to say that $\ell = q-1$ is the smallest integers so that a finite field with p^ℓ elements contains a primitive q^{th} root of unity. Thus, by elementary

algebraic number theory, p remains prime in the ring of integers of E, hence in the ring of integers of the sub-extension K. Thus, by unique factorization of ideals in the ring of integers of K, n is the smallest so that p^n is a norm from K. ///

Corollary: There are infinitely-many non-isomorphic central division algebras of dimension n^2 over $\mathbf{Q}$. In particular, the cyclic algebras $A(p)$ of the previous proposition are mutually non-isomorphic.

Proof: By Dirichlet's theorem, there are infinitely many primes p as in the statement of the previous proposition. We have seen that the cyclic algebras $A(p)$ and $A(p')$ are equivalent in the Brauer group of $\mathbf{Q}$ if and only if p/p' is a norm from the field K above. If there were a fractional ideal $\mathbf{a}$ of the integers $\mathbf{o}$ of K so that

$$\mathrm{Norm}_{K/\mathbf{Q}}\mathbf{a} = \frac{p}{p'} \cdot \mathbf{Z}$$

then

$$(p'\mathbf{o}) \prod_\sigma \sigma\mathbf{a} = p\mathbf{o}$$

where σ runs over the Galois group of K over $\mathbf{Q}$. By hypothesis, $p\mathbf{o}$ and $p\mathbf{o}$ are distinct prime ideals in $\mathbf{o}$, and are stable under the Galois action. By unique factorization of ideals in the Dedekind domain $\mathbf{o}$ it must be that $p\mathbf{o}$ divides some $\sigma\mathbf{a}$, hence (by Galois stability) divides *every* $\sigma\mathbf{a}$. But then p^N divides Norm$\mathbf{a}$, contradiction. ///

Previous discussions have reduced questions about involutions on simple algebras to corresponding questions about involutions on division algebras, without explicitly demonstrating any involutions on division algebras. Above we saw that 4-dimensional simple algebras (quaternion algebras) always have an involution of first kind, the *main involution*. This is a general and purely algebraic construct. On the other hand, we will also see later that over local fields there are no non-commutative central division algebras with involutions of *second* kind. Anticipating this, we might imagine that involutions of second kind are harder to come by than those of first kind, and that we cannot manufacture involutions of second kind in a purely algebraic fashion (that is, over an arbitrary field).

Nevertheless, again using some number theory, we can exhibit a family of examples of algebras with involution of second kind, depending upon construction of Galois extension with *dihedral* Galois group, that is, with Galois group having presentation

$$\sigma^n = 1 \quad \tau^2 = 1 \quad \tau\sigma\tau = \sigma^{-1}$$

Proposition: Let K be a Galois extension of a field k_o with dihedral Galois group with generators σ, τ with $\sigma^n = 1$ as just above. Let k be the subfield of K fixed by σ. Suppose that there is an element γ of $k_o^\times$ so that the smallest positive ℓ so that γ^ℓ is a norm from K is $\ell = n$. Then the cyclic algebra $B = A(k, K, f)$ over k defined via

$$\begin{array}{c} B = \bigoplus_{0\le i<n} K \cdot \pi^i \\ \pi\beta\pi^{-1} = \beta^\sigma \qquad \text{for } \beta \in K \\ \pi^n = \gamma \end{array}$$

is a division algebra. The map $x \to x^\natural$ on B defined for $\beta \in K$ and $0 \le i < n$ by

$$(\beta\pi^i)^\natural = \pi^i\beta^\tau$$

is an involution of second kind on B, whose fixed field in the center k of B is k_o.

Proof: The hypotheses are designed to assure that B is a division algebra. We must verify that $x \to x^\natural$ is an involution, that is, that

$$((\alpha\pi^i)\,(\beta\pi^j))^\natural = (\beta\pi^j)^\natural\,(\alpha\pi^i)^\natural$$

Since a factor of $\alpha^\natural$ comes out on the right, and a factor of π^j comes out on the left, it suffices to check the somewhat simpler version

$$(\pi^i\beta)^\natural = \beta^\natural\,(\pi^i)^\natural$$

First, with $\beta = 1$ and $i = n$ (so that $\pi^i = \gamma$) we find the condition $\gamma^\tau = \gamma$, that is, that $\gamma \in k_o$, which we have also taken as a hypothesis. For $0 \leq i < n$, the right hand side of the desired quality is

$$(\pi^i \beta)^\natural = (\beta^{\sigma^i} \pi^i)^\natural = \pi^i \, \beta^{\sigma^i \tau} = \beta^{\sigma^i \tau \sigma^i} \, \pi^i$$

On the other hand, by the definition of $\natural$ applied to the left-hand side of the desired equality, we obtain $\beta^\tau \pi^i$. Thus, we want

$$\tau = \sigma^i \, \tau \, \sigma^i$$

which indeed follows immediately from $\tau\sigma\tau = \sigma^{-1}$. ///

We can find a situation meeting the hypotheses of the proposition as follows. Fix an integer n, let ζ_n be a primitive n^{th} root of unity, and let $\xi_n = \zeta_n + \zeta_n^{-1}$, $k = \mathbf{Q}(\zeta_n)$, $k_o = \mathbf{Q}(\xi_n)$. Let p be a rational prime which splits completely in k, that is, $p = 1 \bmod n$. (By Dirichlet's theorem on primes in arithmetic progressions there are infinitely-many such.) Let D be a squarefree rational integer which is a primitive root modulo p, and which is relatively prime to n. Let

$$K = k(D^{1/n})$$

We claim that K is a dihedral extension of k_o, and that the cyclic algebra $A(p) = A(k, K, f)$ given by cocycle

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i + j < \\ p & \text{for } i + j \geq n \end{cases}$$

as above is a division algebra.

To see that K is a dihedral extension of k_o, first not that p splits completely in the extension k of $\mathbf{Q}$. Then the hypothesis that D is a primitive root modulo p guarantees that $D^{\mathbf{1n}}$ generates a residue class field extension of degree n over any prime $\mathbf{p}_i$ lying over p in k. Thus, the field extension K/k is of degree at least n, hence of degree n. Then the Galois action over k multiplies $D^{1/n}$ by powers of ζ_n. The Galois action over k_o sends $\zeta_n \to \zeta_n^{-1}$, so the Galois group of K/k_o is dihedral as desired.

To see that $A(p)$ is a division algebra, as above we must verify that p^i is not a norm from K to k for $1 \leq i < n$. Recall that we chose p depending on n so that p splits completely into prime ideals $\mathbf{p}_i$ in $k/\mathbf{Q}$ each of which has residue class field $\mathbf{Z}/p$. And the choice of D is designed to assure that $D^{1/n}$ generates a residue class field extension of $\mathbf{Z}/p$ of degree n. Thus, the primes $\mathbf{p}$ lying over p in k remain prime in K. For there to exist $\beta \in K$ so that $p^i = \text{Norm}_{K/k}\beta$ it is necessary (though not sufficient) that there be a prime ideal in K lying over p with residue class field extension of degree i over $\mathbf{Z}/p$, but we have arranged that the residue class field extension degree is n. Thus, p^i is not a norm for $1 \leq i < n$, and $A(p)$ is a division algebra.

Thus, by the proposition, $A(p)$ has involution of second kind with central fixed field k_o.

Remark: The above construction of non-trivial division algebras with involutions of second kind fails over local fields such as $\mathbf{Q}_p$, since for $p = 1 \bmod n$ the n^{th} roots of unity already lie inside $\mathbf{Q}_p$, so we do not obtain a dihedral Galois extension in the first place.

---

14. Unramified extensions of local fields

Here and in the sequel by 'local field' we mean a local field in the usual number-theoretic sense, namely a *locally compact* (but not discrete) field. It is a standard result that the class of such things consists exactly of finite algebraic extensions of a completion of $\mathbf{Q}$ and finite algebraic extensions of function fields $\mathbf{F}_p(x)$ in one variable x over finite fields $\mathbf{F}_p$. In particular, we include $\mathbf{R}$ and $\mathbf{C}$ as 'archimedean' local fields, although these sometimes require separate treatment. When necessary, 'non-archimedean local field' or 'ultrametric local field' will refer to all local fields other than $\mathbf{R}$ and $\mathbf{C}$. Note that this usage excludes more general fraction fields of complete discrete valuation rings. For ultrametric local fields, local compactness is equivalent to finiteness of residue class fields. The local compactness (or finiteness of residue class fields) is essential for many topological arguments, and for use of Haar measure, which we will need in the sequel.

The following well-known result is sufficiently important that we include it.

Theorem: Let k be an ultrametric local field, and fix a positive integer n. Then there is a unique *unramified* (separable) extension K of k of degree n, which is cyclic Galois and generated by suitable roots of unity. Further, the norm from K to k is a *surjection* on the local units.

Proof: For existence, let ζ be a p^{th} root of unity with p a rational prime not the characteristic of k, and $p = 1 \bmod n$ (invoking Dirichlet's theorem). Elementary algebraic number theory shows that $k(\zeta)$ is unramified (separable) over k, is cyclic Galois, and thus has a subfield of degree n over k.

For uniqueness, let K be an unramified (separable) extension of k. Then, by algebraic number theory, the Galois closure of K over K is also unramified over k, so without loss of generality we may consider the case that K is unramified and Galois over k. Then by algebraic number theory, using the unramified-ness, the Galois group of K over k is the decomposition group of $\mathbf{P}$ over $\mathbf{p}$, where $\mathbf{p}$ is the prime in k and $\mathbf{P}$ is the prime lying over it in K. The finiteness of the residue class fields assures that this Galois group is *cyclic*, so the Galois group of K over k is cyclic. Let m be the cardinality of the finite group $(\mathcal{O}/P)^\times$, where $\mathcal{O}$ is the ring of integers in K. Let φ be the m^{th} cyclotomic polynomial. Necessarily m is prime to the residue characteristic of k, so φ factors modulo $\mathbf{p}$ as $\prod_i \varphi_i$ where each φ_i is of degree n. By Hensel's lemma, φ factors in such manner over k. That is, a Galois unramified extension of k is cyclic and is generated over k by a root of unity. Thus, every unramified extension of k is in fact cyclic. And then recapitulation of this argument shows that K is generated by a root of unity.

To show that the norm from K to k is surjective when restricted to a map $\mathcal{O}^\times \to \mathbf{o}^\times$ on the local units, where $\mathcal{O}$ and $\mathbf{o}$ are the local rings of integers, We first reprove the even more elementary fact that norms $\mathcal{O}/\mathbf{P} \to \mathbf{o}/\mathbf{p}$ are surjective on finite fields. Let q be the cardinality of $\mathbf{o}/\mathbf{p}$, and n the degree of the field extension. Then the finite-field norm has an explicit expression in terms of powers of the Frobenius $\beta \to \beta^q$, given by

$$\begin{aligned}\text{Norm}(\beta) &= \beta \cdot \beta^q \cdot \beta^{q^2} \cdot \ldots \cdot \beta^{q^{n-2}} \cdot \beta^{q^{n-1}} \\ &= \beta^{1+q+q^2+\ldots+q^{n-1}} = \beta^{\frac{q^n-1}{q-1}}\end{aligned}$$

The whole group $(\mathcal{O}/\mathbf{P})^\times$ is cyclic of order $q^n - 1$, so the image has order $q - 1$. The image also is inside $(\mathbf{o}/\mathbf{p})^\times$, so must be the whole thing. This proves surjectivity of norms on finite fields. Similarly, *trace* on finite fields is surjective.

Given the latter result, to prove surjectivity of the norm $\mathcal{O}^\times \to \mathbf{o}^\times$ it would suffice to prove surjectivity to the subgroup

$$\{\alpha \in \mathbf{o} : \alpha = 1 \bmod \mathbf{p}\}$$

To this end, let ϖ be a local parameter in $\mathbf{o}$, and observe that for $x \in \mathcal{O}$ we have

$$\text{Norm}(1 + x\varpi^i) = 1 + \text{tr}\,(x) \cdot \varpi^i \bmod \varpi^{i+1}$$

for $i > 0$, where tr is trace. Since trace is surjective on finite fields, this shows the surjectivity modulo $\mathbf{p}^i$ for every i, and, by taking limits, proves the surjectivity. ///

---

15. Division algebras over local fields, Brauer groups

The previous discussion of simple algebras was entirely algebraic, not relying upon any special properties of the central field k. By contrast, now we will make use of topological aspects of the central field. First we dispatch the archimedean cases, $\mathbf{R}$, $\mathbf{C}$, and the Hamiltonian quaternions $\mathbf{H}$, and then treat the more interesting non-archimedean case.

Since $\mathbf{C}$ is algebraically closed, the only finite-dimensional central division algebra over $\mathbf{C}$ is just $\mathbf{C}$ itself.

The only proper algebraic extension of $\mathbf{R}$ is $\mathbf{C}$. Since every n^2-dimensional central division algebra over $\mathbf{R}$ is split by a finite field extension of $\mathbf{R}$ of degree n, the only candidate for n (other than 1) is 2. The latter

is a necessarily a cyclic algebra, constructed via the quadratic extension $\mathbf{C}$ of $\mathbf{R}$. Since the norms from $\mathbf{C}$ to $\mathbf{R}$ are of index 2, there is a unique isomorphism class of quaternion division algebras with center $\mathbf{R}$. The cyclic algebra description is

$$A = \mathbf{C} \cdot 1 \oplus \mathbf{C} \cdot \pi$$

where for $\beta \in \mathbf{C}$

$$\pi \cdot \beta = \bar{\beta}\pi$$

where the overbar is complex conjugation. This construction yields the usual Hamiltonian quaternions $\mathbf{H}$.

Now consider an ultrametric (locally compact, not discrete) field k, with ring of integers $\mathbf{o}$ and maximal ideal $\mathbf{p}$. Let p be the characteristic of $\mathbf{o}/\mathbf{p}$, and let q be the cardinality of $\mathbf{o}/\mathbf{p}$. Let A be a finite-dimensional central simple algebra over k, of dimension d^2. Let μ be a fixed additive Haar measure on A, and define the *modular function* Δ on $\alpha \in A$ by

$$\mu(\alpha E) = \Delta(\alpha) \cdot \mu(E)$$

for every measurable set E in A. From the definition, for any $x, y \in A$

$$\Delta(xy) = \Delta(x) \cdot \Delta(y)$$

Define

$$\mathcal{O} = \{\beta \in A : \Delta(\beta) \leq 1\}$$

$$\mathbf{P} = \{\beta \in A : \Delta(\beta) < 1\}$$

$$U = \{\beta \in A : \Delta(\beta) = 1\}$$

For any subfield K of A (containing k), the algebra A is a finite-dimensional K-vectorspace, so is isomorphic as topological vectorspace to a cartesian product of some number m of copies of K. Thus, the Haar measure on A is (the completion of) the product measure on these copies of K. Thus, for $\beta \in K$,

$$\Delta(\beta) = \Delta_K(\beta)^m$$

where $\Delta_K(\beta)$ is the modular function on K. From elementary algebraic number theory the latter is an ultrametric metric on K.

The following result uses Δ to distinguish division algebras from general simple algebras.

Proposition: The ultrametric property

$$\Delta(x + y) \leq \max(\Delta(x), \Delta(y))$$

holds if and only if A is a division algebra. In that case, $\mathcal{O}$ is the unique maximal compact subring of A, $U = \mathbf{Q}^\times$, and $\mathbf{P}$ is the unique maximal left ideal in $\mathcal{O}$. Also, $\mathbf{P}$ is the unique maximal two-sided (and right) ideal in $\mathcal{O}$. The quotient $\mathcal{O}/\mathbf{P}$ is a finite field extension of $\mathbf{o}/\mathbf{p}$. There is a *local parameter* $\varpi \in \mathcal{O}$ so that $\mathbf{P} = \varpi\mathcal{O} = \mathcal{O}\varpi$.

Proof: The local compactness of k and the finite-dimensionality of A assures that A is locally compact. The algebra A is a division algebra if and only if for every $\alpha \in A$ the ring $k(\alpha)$ is a field. In that case, as observed above, Δ restricted to $k(\alpha)$ is necessarily an ultrametric absolute value, so for all $x, y \in A^\times$

$$\Delta(x + y) = \Delta(x(1 + x^{-1}y)) = \Delta(x)\,\Delta(1 + x^{-1}y) \leq \Delta(x)\,\max(\Delta(1), \Delta(x^{-1}y))$$

$$= \max(\Delta(x), \Delta(x)\Delta(x^{-1}y)) = \max(\Delta(x), \Delta(y))$$

using the ultrametric property in $k(x^{-1}y)$. (If A is not a division algebra, it is easy to give counterexamples to the ultrametric property for Δ.)

The ultrametric inquality (together with multiplicativity) assures that $\mathcal{O}$ is a ring. It is easy to verify that the function Δ is continuous on A, so is bounded on any compact subring R of A. Since Δ is also multiplicative,

any compact subring must be contained in $\mathcal{O}$. To see that $\mathcal{O}$ is compact, note that for $\alpha \in \mathcal{O}$ the restriction of Δ to $k(\alpha)$ shows that α lies in the integers of $k(\alpha)$, which is a compact subring of A.

If $\Delta(\alpha) = 1$, then $\alpha \neq 0$, so α is invertible in A, and $\Delta(\alpha^{-1}) = 1$ by multiplicativity. Thus, $\alpha \in \mathcal{O}^\times$.

Thus, any proper left (or right, or two-sided) ideal J in $\mathcal{O}$ cannot contain any element α with $\Delta(\alpha) = 1$. The ultrametric property shows that $\mathbf{P}$ is an additive subgroup of $\mathcal{O}$, and then the multiplicative property shows that it is an ideal in $\mathcal{O}$. Thus, $\mathbf{P}$ is the unique maximal left, right, or two-sided ideal.

Then $\mathcal{O}/\mathbf{P}$ is a division ring. The open-ness of $\mathbf{P}$ implies that $\mathcal{O}/\mathbf{P}$ is discrete. The compactness of $\mathcal{O}$ implies that $\mathcal{O}/\mathbf{P}$ is compact. Together, we find that $\mathcal{O}/\mathbf{P}$ is finite. Since finite division rings are fields, $\mathcal{O}/\mathbf{P}$ is a field.

Since k is ultrametric and locally compact, for every $\alpha \in A$ Δ restricted to $k(\alpha)$ is discretely valued, and the set of values on $k(\alpha)$ is contained in the e^{th} roots of the values of Δ on k for some divisor e of $[k(\alpha) : k]$, by basic number theory. If $\dim_k A = n^2$, then all these field extension degrees $[k(\alpha) : k]$ are divisors of n, so the set of non-zero values of Δ is a discrete (closed) subset of $(0, \infty)$. We note that any (non-trivial) such group is a free group on one generator.

Let ϖ be in $\mathcal{O}$ with maximal value $\Delta(\varpi)$ less than 1. Given $x \neq 0$ in A there is a unique integer ℓ so that

$$\Delta(x) = \Delta(\varpi)^\ell$$

Then $\varpi^{-\ell} x \in \mathcal{O}^\times$. In particular, $\mathbf{P} = \varpi\mathcal{O} = \mathcal{O}\varpi$. ///

Theorem: Let D be a finite-dimensional central *division* algebras over an ultrametric field k. The limit

$$\omega(x) = \lim_{n\to\infty} x^{q^n}$$

exists for $x \in \mathcal{O}$. The set $M = \omega(\mathcal{O}^t o, es)$ is a cyclic subgroup of $D^\times$ order $q - 1$ where $q = \operatorname{card} \mathcal{O}/\mathbf{P}$. The group M is a maximal finite abelian subgroup of $D^\times$. The set $M \cup \{0\}$ is a set of representatives for $\mathcal{O}/\mathbf{P}$. There is a generator ϖ for $\mathbf{P}$ so that $\varpi M \varpi^{-1} = M$.

Proof: First, for $x \in \mathcal{O}^\times$, we claim that the limit

$$\omega(x) = \lim_{n\to\infty} x^{q^n}$$

exists. Write

$$\omega(x) = x + (x^q - x) + (x^{q^2} - x^q) + (x^{q^3} - x^{q^2}) + \dots$$

Since the absolute value is ultrametic, the series on the right-hand side converges if the terms go to 0. And

$$x^{q^{n+1}} - x^{q^n} = x^{q^n} \cdot (x^{q^{n+1} - q^n} - 1) = x^{q^n} \cdot \left((x^{q-1})^{q^n} - 1 \right)$$

Since $\mathcal{O}/\mathbf{P}$ is a finite field with q elements

$$x^{q-1} = 1 \bmod \mathbf{P}$$

Let $x^{q-1} = 1 + y\varpi^i$ with $y \in \mathcal{O}$ and $i \geq 1$. By the binomial theorem

$$(x^{q-1})^q - 1 = qy\varpi^i \bmod \varpi^{2i}$$

Whether the base field k is of characteristic 0 or is of characteristic p dividing q, ϖ divides q, and we have

$$(x^{q-1})^q = 1 \bmod \varpi^{i+1}$$

Thus, as $n \to \infty$,

$$(x^{q-1})^{q^n} \to 1$$

Thus, the limit $\omega(x)$ exists for $x \in \mathcal{O}$, and the expression above also shows that $\omega(x) = x \bmod \mathbf{P}$.

For $x \in \mathbf{P}$ the limit is obviously 0, and for $x \in 1 + \mathbf{P}$ it is obviously 1. If $x, y \in \mathcal{O}$ commute, then also

$$\omega(xy) = \omega(x)\,\omega(y)$$

In particular, for $x \in \mathcal{O}^\times$

$$\omega(x)^{q-1} = \omega(x^{q-1}) = 1$$

From these facts, the collection $\{\omega(x) : x \in \mathcal{O}^\times\}$ of images by ω is a cyclic group M of order $q-1$ inside $\mathcal{O}^\times$.

On the other hand, if G were any finite subgroup of $D^\times$, then $G \subset \mathcal{O}^\times$, since Δ is multiplicative. For G of order m prime to p, let q be of order N in $(\mathbf{Z}/m)^\times$. Then $g^m = 1$ for $g \in G$ (by Lagrange's theorem) implies that for every $k \in \mathbf{Z}$ we have $q^{kN} = 1 \bmod m$, so

$$g^{q^{kN}} = g$$

Thus, by the series expression for it, $\omega(g) = g$. In particular, $g = 1 \bmod \mathbf{P}$ implies $g = 1$, and thus the quotient map from G to $(\mathcal{O}/\mathbf{P})^\times$ is injective. This proves the indicated maximality of M.

Last, we must find a local parameter normalizing M. For any $\alpha \in D^\times$ the map $x \to \alpha x \alpha^{-1}$ stabilizes $\mathcal{O}$ and $\mathbf{P}$, so gives an automorphism $\lambda(\alpha)$ of the finite field $\mathcal{O}/\mathbf{P}$. If $\alpha \in \mathcal{O}^\times$, then for $x \in \mathcal{O}$

$$\lambda(\alpha)(x + \mathbf{P}) = \alpha x \alpha^{-1} + \mathbf{P} = (\alpha + \mathbf{P})(x + \mathbf{P})(\alpha + \mathbf{P})^{-1} = x + \mathbf{P}$$

since $\mathcal{O}/\mathbf{P}$ is commutative. From this,

$$\lambda(\alpha) = \lambda(\varpi^{\mathrm{ord}\alpha})$$

where $\mathrm{ord}\alpha$ is the integer so that $\alpha \in \varpi^\ell \mathbf{P}$. Since the field $\mathbf{P}/\mathbf{P}$ is finite, there is an integer m such that for all $x \in \mathcal{O}$

$$\lambda(\varpi)\, x = \varpi x \varpi^{-1} = x^{p^m} \bmod \mathbf{P}$$

That is,

$$\varpi x = x^{p^m}\, \varpi \bmod \mathbf{P}^2$$

Then define

$$\pi = \sum_{\mu \in M} \alpha^{p^m}\, \varpi \alpha^{-1} = \sum_{\mu \in M} \varpi \alpha \alpha^{-1} = (q-1)\varpi = -\varpi \bmod \mathbf{P}^2$$

So π is also a local parameter, $\lambda(\pi) = \lambda(\varpi)$, and π normalizes M. ///

Corollary: With M and π as in the theorem, every $x \in D^\times$ has a unique expression of the form

$$x = \sum_{i \geq m} \alpha_i\, \pi^i$$

with $\alpha_i \in M$, and where m is the uniquely determined integer so that

$$x \in \pi^m \cdot \mathcal{O}^\times$$

Proof: If $x \in \mathcal{O}^\times$, then $\alpha_o = \omega(x) \in M$ satisfies $\alpha = x \bmod \mathbf{P}$, and by the theorem is uniquely determined in M by this property. Thus, generally, if $x \in \pi^m \mathcal{O}^\times$ then $\pi^{-m} x \in \mathcal{O}^t imes$ has α_m uniquely determined. Induction gives the result. ///

Theorem: Let D be a finite-dimensional central division algebra over k for an ultrametric local field k. Let D be of dimension d^2 over k. Let $\mathbf{o}$ be the local integers in k, and $\mathcal{O}$ the maximal compact subring in D. There is a subfield K of D of degree d and *unramified* over k. Let $\tilde{\mathbf{o}}$ be the local integers in K. There

is a local parameter π in $\mathcal{O}$ so that π^d is a local parameter in k, so that $\{1, \pi, \ldots, \pi^{d-1}\}$ generates $\mathcal{O}$ as an $\tilde{\mathbf{o}}$-module, and so that the map $\alpha \to \pi\alpha\pi^{-1}$ stabilizes K and generates the Galois group action on K over k.

Remark: Thus, D is a cyclic algebra $A(k, K, f)$ over k, since the unique unramified extension of k of degree d is cyclic over k. And the theorem says that the cocycle is

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < d \\ \pi^d & \text{for } i+j \geq d \end{cases}$$

for suitable generator σ of the Galois group of K over k. Note that π^d is *some* prime element in k. Also note that implicit in this is a specification of generator σ for the Galois group. Finally, a converse to this theorem is clear, namely that every such cocycle yields a division algebra.

Proof: Let M be the finite cyclic group inside $\mathcal{O}^\times$ as in the theorem above. Let $K = k(M)$, and let $n = [K : k]$. Since this field extension is generated by roots of unity of order prime to the residue field characteristic, by elementary algebraic number theory it is unramified, and the ring of integers in K is $\tilde{\mathbf{o}} = \mathbf{o}[M]$. (We will prove that K is a maximal subfield of D.)

From the previous corollary expressing elements of D as infinite sums $\sum_i \alpha_i \pi^i$ with $\alpha_i \in M$, an element $y \in D$ is in the center k of D if and only if it commutes with every element of M, and with π. Because M is finite, conjugation with some positive power π^ν is the trivial automorphism on M. Let ν be the least such positive integer. Then π^ν commutes with π and with every element of M, so lies in $\mathbf{k}$. For any smaller power π^ℓ of π to lie in k would entail that π^ℓ commute with all elements of M, but ν was taken to be the smallest. Thus, ν is also definable as being the smallest positive integer so that π^ν lies in k.

Then any expression $\sum_i \alpha_i (\pi^\nu)^i$ with $\alpha_i \in M \cup \{0\}$ is in K, since the powers $(\pi^\nu)^i$ of π^ν are in k, and $K = k(M)$. Then

$$\sum_i \alpha_i \pi^i = \sum_{0 \leq j < \nu} \left(\sum_i \alpha_{j+i\nu} \, (\pi^\nu)^i \right) \pi^j$$

expresses any element of D as a linear combination over $K = k(M)$ of the elements $1, \pi, \pi^2, \ldots, \pi^{\nu-1}$.

By the uniqueness of the expansions $\beta = \sum_i \alpha_i \pi^i$ for $\beta \in D$, conjugation by π shows that β is in k if and only if the expansion is actually of the form

$$\beta = \sum_i \alpha_i (\pi^\nu)^i$$

and with all $\alpha_i \in (M \cup \{0\}) \cap k$. In particular, this shows that $\Delta(\pi^\nu) = \Delta(\pi)^\nu$ is largest value of Δ on k less than 1, so π^ν is a local parameter in k. From this (and from the ultrametric property) it follows that $1, \pi, \pi^2, \ldots, \pi^{\nu-1}$ are linearly independent over k. Thus, $k(\pi)$ is a subfield of D, with $[k(\pi) : k] = \nu$. Since any subfield of D has degree over k less than or equal d, we find $\nu \leq d$. For the same reason, $[K : k] \leq d$. At the same time, the existence of expressions $\sum_i \alpha_i \pi^i$ for elements of D shows that $n\nu \geq d^2$. Thus,

$$n = \nu = d$$

That is, K is indeed a maximal subfield of D. ///

Corollary: Over a non-archimedean local field k there is a unique quaternion division algebra up to isomorphism.

Proof: We know that any quaternion division algebra is obtained as a cyclic algebra over the unique unramified quadratic extension K of k, with cocycle

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < 2 \\ \varpi & \text{for } i+j \geq 2 \end{cases}$$

where ϖ is a local parameter in k. The parameter γ must not be a norm from K, and it is only the equivalence class of ϖ modulo norms from K that determines the isomorphism class of the division algebra. Since the extension is unramified, the norm is onto the local units (as recalled earlier), and, further, since the extension is quadratic the index $k^\times/\mathrm{Norm}_{K/k}(K^\times)$ is exactly 2. Thus, up to norms, there is a unique non-norm. ///

Corollary: A quaternion division algebra D over a non-archimedean local field k is split by every (separable) quadratic extension E of k.

Proof: We use the fact proven earlier that a field extension of degree n splits a division algebra of dimension n^2 if and only if the field imbeds as a (maximal) subfield of the division algebra. Thus, E splits D if and only if it imbeds in D. If E is the unramified quadratic extension, then we have already constructed D as a cyclic algebra over E, so E imbeds into D. If, on the other hand, E is ramified over k, then E is linearly disjoint from the unramified quadratic extension K. Thus, $E \otimes_k K$ is a field isomorphic to a compositum KE of E and K, and $D \otimes_k E$ is a cyclic algebra defined via the unramified quadratic extension KE of E. But now the parameter γ occurring in the cocycle

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < 2 \\ \varpi & \text{for } i+j \geq 2 \end{cases}$$

has order 2 in E, due to the ramification of E over K. Thus, by the surjectivity of norms on local units, γ is a norm from KE to E, and the algebra is split by E. ///

Corollary: In the situation of the theorem, let $\mathbf{o}$ be the integers of k. Define the dual module $\mathcal{O}^*$ to $\mathcal{O}$ with respect to reduced trace tr by

$$\mathcal{O}^* = \{x \in D : \mathrm{tr}\,(x\mathcal{O}) \subset \mathbf{o}\}$$

Then

$$\mathcal{O}^* = \pi^{1-d} \cdot \mathcal{O} = \cdot\mathcal{O}\pi^{1-d}$$

Proof: Since $\{1\,pi, \pi^2, \ldots, \pi^{d-1}\}$ is a K-basis for D, and since $\pi^i \in k$ if and only if $i = 0 \bmod d$, for $1 \leq i < d$ we have

$$(\text{full trace of left multiplication by } \alpha\pi^i \text{ on } D \ = 0$$

Thus, the reduced trace is also 0 on such elements. On the other hand, the restriction of the reduced trace on D to K is equal to the Galois trace from K to k. For $x \in D$, we may write

$$x = \sum_{0 \leq i < d} \alpha_i\, \pi^{-i}$$

with $\alpha_i \in K$. Then for β in the ring of integers $\tilde{\mathbf{o}}$ of K, and with $0 \leq j < d$,

$$\mathrm{tr}\,(x \cdot \beta\pi^j) = \mathrm{tr}\,(\sum_i \alpha_i \pi^{-i} \beta\pi^j) = \mathrm{tr}\,(\sum_i \alpha_i \pi^{-i} \beta\pi^i \pi^{j-i}) = \mathrm{tr}\,(\alpha_j \pi^{-j} \beta\pi^j)$$

The latter is a Galois trace, and K is unramified over k, so the trace is in the integers of k if and only if $\alpha_j \in \tilde{\mathbf{o}}$. Thus,

$$\mathcal{O}^* = \{ \sum_{0 \leq i < d} \alpha_i\, \pi^{-i} : \alpha_j \in \tilde{\mathbf{o}}\}$$

which is what the corollary asserts. ///

Corollary: Let A be a finite-dimensional central simple algebra over k, isomorphic to a matrix algebra over a central division algebra D over k of dimension d^2. Let π be a prime element of the maximal compact

subring $\mathcal{O}$ of D, and let R be the subring of A consisting of matrices with entries in $\mathcal{O}$. Let tr be reduced trace. Let $\mathbf{o}$ be the integers in k. Then

$$\{x \in A : \mathrm{tr}\,(x\mathcal{O}) \subset \mathbf{o}\} = \pi^{1-d}\,R = \pi^{1-d}\,R$$

Proof: This follows from the previous corollary by simple matrix computations. ///

Now we can use the general algebraic results on cyclic algebras to give a complete description of the Brauer group of a non-archimedean local field. We recall that the cyclic Galois group of an unramified extension K of a non-archimedean local field k, where the latter's residue class field has q elements, is generated by the **Frobenius** automorphism σ defined by

$$\alpha^\sigma = \alpha^q \bmod \mathbf{m}$$

where $\mathbf{m}$ is the maximal ideal in the integers $\mathbf{o}$ of k.

Theorem: The Brauer group $Br(k)$ of a non-archimedean local field k is canonically isomorphic to $\mathbf{Q}/\mathbf{Z}$. Elements of $Br(k)$ of order n are represented by division algebras of dimension n^2 over k.

Proof: We have already seen that every division algebra is split by an unramified extension, and that the subgroup $Br(k, K_n)$ of $Br(k)$ consisting of algebras split by the unique unramified extension K_n of degree n over k is isomorphic to $k^\times/\mathrm{Norm}_{K_n/k}K_n^\times$ as follows. Let σ be the Frobenius automorphism of K_n over k. (As n varies, all these are compatible!) We use cocycle $f = f_\gamma$ on the Galois group of K_n over k given (as above) by

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{for } i+j < n \\ \varpi & \text{for } i+j \geq n \end{cases}$$

Let $A(\gamma)$ be the cyclic algebra so specified. Then the map

$$A(\gamma) \to \gamma \cdot (\mathrm{Norm}_{K_n/k}K_n^\times)$$

is an isomorphism of the group $Br(k, K_n)$ to $k^\times/\mathrm{Norm}_{K_n/k}K_n^\times$.

Recall also that such a norm map is a surjection to local units $\mathbf{o}^\times$ in k, for any finite unramified extension. Thus, any one of these quotients $k^\times/\mathrm{Norm}_{K_n/k}K_n^\times$ is a quotient of $k^\times/\mathbf{o}^\times \approx \mathbf{Z}$. Choose a local parameter ϖ in k (This choice is not canonical, but the image in $k^\times/\mathbf{o}^\times \approx \mathbf{Z}$ is canonical.) Then

$$Br(k, K_n) \approx k^\times/\mathrm{Norm}_{K_n/k}K_n^\times \approx \varpi^{\mathbf{Z}}/\varpi^{n\mathbf{Z}} \approx \mathbf{Z}/nZ \approx n^{-1}\mathbf{Z}\,/\,\mathbf{Z} \subset \mathbf{Z}/\mathbf{Z}$$

The injections $Br(k, K_n) \to Br(k, K_N)$ for $n|N$ all fit together to give

$$Br(k) \approx \bigcup_n n^{-1}\mathbf{Z}\,/\,\mathbf{Z} = \mathbf{Q}/\mathbf{Z}$$

as claimed. ///

---

16. Local splitting almost everywhere

The important result here is easy in the context of facts developed above. The converse, while true, is significantly deeper and difficult to prove.

Recall that a **number field** is a finite field extension of the rationals $\mathbf{Q}$, while a **function field** (in this context) is a finite field extension of a function field in one variable $\mathbf{F}_p(T)$ over a finite field $\mathbf{F}_p$. A **global field** is either a number field or a function field.

Theorem: Let A be a finite-dimensional central simple algebra over a global field k. For all but finitely many places v of k, the completion k_v splits A. That is, for almost all places v,

$$A \otimes_k k_v \approx \text{ a matrix algebra over } k_v$$

Further, let e_i be a k-basis for A. Then, for almost all (non-archimedean) places v of k, the set $\mathcal{O}_v = \sum_i \mathbf{o}_v \cdot e_i$ is a maximal compact subring of $A \otimes_k k_v$, where $\mathbf{o}_v$ is the ring of local integers in the completion k_v.

Proof: Let $\mathcal{O} = \sum_i \mathbf{o} \cdot e_i$. This set will not necessarily be a subring of the algebra A, but that is irrelevant. Let tr be reduced trace, and define a dual module

$$\mathcal{O}' = \{x \in A : \mathrm{tr}\,(xy) \in \mathbf{o} \text{ for all } y \in \mathcal{O}\}$$

This dual module is certainly a finitely-generated $\mathbf{o}$ module inside A (although it need not be a *free* $\mathbf{o}$-module).

For almost all (finite) places v, the finitely many structure constants $c_{ij\mu}$ describing the multiplication in A in the coordinates e_i, given by

$$e_i \cdot e_j = \sum_\mu c_{ij\mu}\, e_\mu$$

are locally integral at v. Thus, at such v, $\mathcal{O} \otimes_{\mathbf{o}} \mathbf{o}_v$ is contained in a compact subring R_v of $A \otimes_k k_v$. Further, for almost all finite places v we have the self-duality

$$\mathcal{O}' \otimes_{\mathbf{o}} \mathbf{o}_v = \mathcal{O} \otimes_{\mathbf{o}} \mathbf{o}_v$$

because the $\mathbf{o}$ generators for $\mathcal{O}'$ are expressed in terms of the e_i with a finite set of coefficients all integral at v.

Since always

$$\mathcal{O} \otimes_{\mathbf{o}} \mathbf{o}_v \subset R_v \subset \mathcal{O}' \otimes_{\mathbf{o}} \mathbf{o}_v$$

we conclude that at almost all v we have equality

$$\mathcal{O} \otimes_{\mathbf{o}} \mathbf{o}_v = R_v = \mathcal{O}' \otimes_{\mathbf{o}} \mathbf{o}_v$$

That is, $\mathcal{O} \otimes_{\mathbf{o}} \mathbf{o}_v$ is a maximal compact subring *and* is self-dual with respect to trace. From the last corollary in the previous section, this is impossible unless the algebra $A \otimes_k k_v$ is split. That is, almost everywhere locally A is split. ///

---

17. Involutions on division algebras over local fields

Now we classify involutions on finite-dimensional central division algebras over local fields of characteristic not 2.

As usual, the case of an archimedean local field k is very easy. If $k = \mathbf{C}$, then there are no proper finite-dimensional division algebras anyway. If $k = \mathbf{R}$, then there is a unique proper finite-dimensional central division algebra, the ring of Hamiltonian quaternions, which has its main involution (which is of first kind).

Theorem: Let D be a finite-dimensional central division algebra over a non-archimedean local field k. Suppose that D has an involution θ. Then one of the following cases occurs:
• $D = k$ and θ is trivial.
• $D = k$ and θ is a field automorphism of order 2.
• D is the unique quaternion algebra over k, and θ is of first kind (so from the main involution by a conjugation) That is, a *non-commutative* division algebra with involution over a local field must be four-dimensional, and the involution is of first kind. There are no non-commutative division algebras with involutions of second kind in this context.

Proof: We use the earlier discussion of division rings over local fields. We must recall some of the details of the situation. Let D be an n^2-dimensional central division algebra over k, with matximal compact subring $\mathcal{O}$ and maximal (left, right, and two-sided) ideal $\mathbf{P}$. Let K be the unique unramified field extension of k of degree n. The quotient $\mathcal{O}/\mathbf{P}$ is a (commutative) field extension of degree n of the finite field $\mathbf{o}/\mathbf{p}$, where $\mathbf{o}$ is the local ring of integers in k and $\mathbf{p}$ is the maximal ideal in $\mathbf{o}$. For any generator π for $\mathbf{P}$, the automorphism

$\alpha \to \pi\alpha\pi^{-1}$ stabilizes both $\mathcal{O}$ and $\mathbf{P}$, so gives an automorphism λ of $\mathcal{O}/\mathbf{P}$ over $\mathbf{o}/\mathbf{p}$ independent of the choices of π. For q being the cardinality of $\mathbf{o}/\mathbf{p}$, λ is of the form $x \to x^{q^m}$ for some m relatively prime to n. That is, $\alpha \to \pi\alpha\pi^{-1}$ is a power σ^m of the Frobenius σ of K over k. This integer m uniquely determines the structure of D, and does not depend upon the k-algebra structure. This is exploited in the following proposition which is of some interest in its own right.

Proposition: Let τ be an automorphism of the non-archimedean local field k, and define a second k-vectorspace structure D^τ on a finite-dimensional central division algebra D over k by

$$\alpha(x) = \alpha^\tau \cdot x$$

where $\alpha \cdot x$ is the original k-vectorspace structure, with $\alpha \in k$ and $x \in D$. Then $D^\tau \approx D$ as central k-algebras.

Proof: (of proposition) Certainly $D \approx D^\tau$ as rings, and this is a topological isomorphism as well. Let $\dim_k D = n^2$. The (unique) unramified extension K of k of degree n splits both D and D^τ, and the (unique) maximal compact subring $\mathcal{O}$ of D is a maximal compact subring of D^τ as well. The unique maximal ideal in $\mathcal{O}$ is still maximal in $\mathcal{O}$ in D^τ. (Indeed, all these things depend only upon the topological algebra structure of D, not upon the k-vectorspace structure.) Certainly $\alpha \to \pi\alpha\pi^{-1}$ is the same map in either D or D^τ, so modulo $\mathbf{P}$ gives the same map on the quotient $\mathcal{O}/\mathbf{P}$. For some integer m the latter map is $x\tau^{q^m}$, where q is the cardinality of $\mathcal{O}/\mathbf{P}$. Thus, the invariant m is the same in both cases, so (from the earlier discussion of structure) $D \approx D^\tau$ as central k-algebra. ///

Now we return to the proof of the theorem. Let τ be the restriction to k of the involution θ. As usual, the existence of the involution gives an isomorphism $D^{\text{opp}} \approx D^\tau$ of k-algebras, where now (unlike an earlier discussion) we allow for the possibility that θ is not trivial on the center k. By the proposition, $D \approx D^\tau$ as k-algebras, so we conclude that $D \approx D^{\text{opp}}$ as k-algebras. By the structure of the Brauer group, this implies that the similariy class of D in the Brauer group $Br(k)$ is of order a divisor of 2. That is, from the structure theory of division algebras over local fields, D is of dimension $1 = 1^2$ or $4 = 2^2$. If $D = k$ we are done. This leaves the unique quaternion division algebra D to be considered.

The case that the involution θ on the quaternion division algebra D is of first kind is easy, since we already know that D has a main involution, so by Skolem-Noether any other involution of first kind differs by a conjugation.

Now suppose that θ is of second kind. Let $\backslash alf \to \alpha^\sharp$ be the main involution. Then $\alpha \to (\alpha^\theta)^\sharp$ is an automorphism of order 2 of D and gives a non-trivial automorphism τ on k. The set

$$D_o = \{x \in D : x^{\theta\sharp}\}$$

is a subring of D containing the subfield k_o of k fixed by τ. Because the characteristic is not 2, there is an element ω in k so that $\omega^\tau = -\omega \neq \omega$ and which generates k over k_o. Thus, we find that D_o is central simple over k_o, and

$$D = D_o \otimes_{k_o} k$$

But we saw that every (separable) quadratic extension of a local field k_o splits every quaternion algebra over k_o, so D cannot be a division ring, contradiction. Thus, in the case of an involution of second kind, the division ring must be a field. ///
