CENTRAL SIMPLE ALGEBRA SEMINAR

JACKSON S. MORROW

Contents

Date: March 2, 2015.

1. LECTURE (1/9): WEDDERBURN-ARTIN THEORY

Preliminaries. We will make a few conventions:

1. Ring will always be associative and unital, but not necessarily commutative;
2. Ring homomorphisms will be unital (i.e., $f(1) = 1$) and the zero ring is allowed;
3. Modules will be left or right and for notations sake we will denote a left R-module M as ${}_RM$ and a right S-module N as N_S.

Definition 1.1. Given rings R, S an $R - S$ bi-module M is an Ableian group both with left R-module and right S-module structure satisfying:

$$r(ms) = (rm)s \quad \forall\, r \in R, s \in S,\, m \in M.$$

Note that we will denote an $R - S$ bi-module P by ${}_RP_S$.

Structure Theory. Let R be a ring.

Definition 1.2. A left R-module P is **simple** if it has no proper non-zero sub-modules.

Definition 1.3. If P is a left R-module and $X \subset P$, then

$$\operatorname{ann}_R(x) = \{r \in R : rx = 0 \forall\, x \in X\}.$$

Remark 1.4. $\operatorname{ann}_R(x)$ is always a left ideal and is 2-sided if $X = P$.

Definition 1.5. We will denote an **ideal** I of R by $I \leqslant R$. A **left ideal** will be denoted by $I \leqslant_\ell R$ and similarly, $I \leqslant_r R$ for a **right ideal**. An ideal $I \leqslant R$ is said to be **left primitive** if it is of the form $I = \operatorname{ann}_R(P)$, where P is simple.

Proposition 1.6. *Suppose P is a non-zero right R-module, then the following are equivalent:*

(1) P is simple;
(2) $mR = P$ for all $m \in P \setminus \{0\}$;
(3) $P = R/I$ for some $I \leqslant_r R$ maximal.

Proof. (1) $\Rightarrow$ (2). Since mR is a non-zero ideal and P is simple, $mR = P$. (2) $\Rightarrow$ (3). Consider the map $R \twoheadrightarrow P$ defined by $r \mapsto mr$. By the first isomorphism theorem, we have that $R/\ker \cong P$. Furthermore, ker has to be maximal, else $R/\ker$ is not simple. (3) $\Rightarrow$ (1). This is a direct consequence of the Lattice Isomorphism theorem. $\square$

Definition 1.7. A left R-module P is **semi-simple** if

$$P \cong \bigoplus_{i=1}^{n} P_i \quad \text{where each } P_i \text{ is simple.}$$

Proposition 1.8. *Let A be an algebra over a field F and M a semi-simple left A-module which is finite dimensional as a F-vector space. If $P \subset M$ is a sub-module, then*

(1) P is semi-simple;
(2) M/P is semi-simple;
(3) there exists $P' \subset M$ such that $M \cong P \oplus P^\perp$.

Remark 1.9. If F is a field, then an F-algebra is a ring A together with a vector space structure such that for every $\lambda \in F, a, b \in A$, we have

$$(\lambda a)b = \lambda(ab) = a(\lambda b),$$

hence $F \hookrightarrow Z(A)$.

Proof. (1). Let $P \subset N \subset M$ be sub-modules and write $M = N \oplus N' = P \oplus P'$ for some N' and P'. We need to find Q such that $N = P \oplus Q$. Let $Q = P' \cap N$. This is a sub-module of N so we need to show that $N = P + Q$ and $P \cap Q = 0$. Let $n \in N$, then $n \in M$ so we can write $n = a + b$ for some uniquely determined $a \in P, b \in P'$. Since $P \subset N$, we have that $b = n - a \in N$, and hence $b \in Q$. Thus, we have $n \in P + Q$ and consequently, $N = P + Q$. To show that other claim, let $n \in P \cap Q$, then $n \in P'$ as well. By choice of P and P', if $n \in P$ and $n \in P'$, then $n = 0$, and hence $P \cap Q = 0$.

(2). To show that M/P is semi-simple, choose $Q \leqslant M/P$ that is that maximal semi-simple sub-module. Suppose that $Q \neq M/P$. ♠♠♠Jackson: Ask Bastian about proof. □

Definition 1.10. Let R be a ring. Define

$$\begin{aligned} J_r(R) &= \bigcap \text{all maximal right ideals} \\ J_\ell(R) &= \bigcap \text{all maximal left ideals .} \end{aligned}$$

Remark 1.11. Note that annihilators of elements in a simple R-module are the same as maximal right ideals in R. Hence we have that

$$\begin{aligned} J_r(R) &= \bigcap \text{all annihilators of simple } R\text{-modules} \\ &= \bigcap_{\substack{M \in \mathrm{Mod}_R \\ M \text{ simple}}} \mathrm{ann}_R(M) \end{aligned}$$

Thus, we have that $J_r(R) \leqslant R$.

Lemma 1.12. *Suppose that A is a finite dimensional F-algebra, then A_A is semi-simple if and only if $J_r(A) = 0$.*

Proof. ($\Rightarrow$). First, we write $A_A = \bigoplus_{j=1}^{n} P_i$ where P_i are simple. Let $\widehat{P}_j = \bigoplus_{j \neq i} P_j$. We can easily see that $\widehat{P}_j$ is a maximal right ideal. By Definition 1.10, we have that

$$J_r(A) \subset \bigcap_{j=1}^{n} \widehat{P}_j = 0.$$

($\Leftarrow$). Suppose that $J_r(A) = 0$. Since A is a finite dimensional vector space over F, there exists a finite collection of maximal ideals I_i such that $\bigcap I_i = 0$. By Proposition 1.6, we have that for each i, A/I_i is simple, hence $\bigoplus_i A/I_i$ is semi-simple by definition. Since $\bigcap I_i = 0$, we have that the map

$$A \longrightarrow \bigoplus_i A/I_i$$

is injective, hence we can consider A as a sub-module of a semi-simple module. We have our desired result by Proposition 1.8. □

Definition 1.13. An element $r \in R$ is **left-invertible** if there exists $s \in R$ such that $sr = 1$ and is **right-invertible** if $rs = 1$.

Lemma 1.14. *Let A be a finite dimensional algebra over F. An element $a \in A$ is right invertible if and only if a is left invertible.*

Proof. Pick $a \in A$. Consider the linear transformation of F-vector spaces

$$\begin{aligned} \phi : A &\longrightarrow A \\ b &\longmapsto ab \end{aligned}$$

If a is right invertible, then ϕ is surjective. Indeed, since if $ax = 1$, then for $y \in A$, $\phi(xy) = axy = y$. If ϕ is bijective, then $\det(T) \neq 0$, where T is the matrix associated to ϕ for some choice of basis. Let

$$\chi_T(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$$

be the characteristic polynomial of T, so $c_0 = \pm\det(T)$. By the Cayley-Hamilton theorem, we have that $\chi_T(T) = 0$, which implies that

$$\frac{(a^{n-1} + c_{n-1}a^{n-2} + \cdots + c_1)a}{-c_0} = 1.$$

So we have found a left inverse to a that is also a right inverse due to commutativity. $\square$

Lemma 1.15. *Let R be a ring and $r, s, t \in R$ such that $sr = 1 = rt$, then $s = t$.*

Definition 1.16. Let R be a ring and $r \in R$. We say that r is **left quasi-regular** if $1 - r$ is left invertible. We will say that r is **quasi-regular** if $1 - r$ is invertible.

Lemma 1.17. *Let $I \leqslant_r R$ such that all elements of I are right quasi-regular. Then all elements of I are quasi-regular.*

Proof. Let $x \in I$. We want to show that $1 - x$ has a left inverse. We know that there exists an element $s \in R$ such that $(1 - x)s = 1$. Let $y = 1 - s$ and $s = 1 - y$. Then $(1 - x)(1 - y) = 1 = 1 - x - y + xy$, which implies that $xy - x - y = 0$, so $y = xy - x$. Since $x \in I$, y must also be in I. By assumption, y is right quasi-regular ($1 - y$ is right invertible) but $1 - y$ is also left invertible with inverse $1 - x$. Then $(1 - y)(1 - x) = 1$, so $(1 - x)$ is left invertible, and thus x is quasi-regular. $\square$

Lemma 1.18. *Let $x \in J_r(R)$, then x is quasi-regular.*

Proof. By Lemma 1.17, it is enough to show that x is right quasi-regular for all $x \in J_r(R)$. If $x \in J_r(R)$, then x is an element of all maximal ideals of R. Hence $1 - x$ is not an element of any maximal ideal in R, so $(1 - x)R = R$. Thus there exists some $s \in R$ such that $(1 - x)s = 1$. $\square$

Lemma 1.19. *Suppose that $I \leqslant R$ such that all elements are quasi-regular. Then $I \subset J_r(R)$ and $I \subset J_\ell(R)$.*

Proof. Suppose that K is a maximal right ideal. To show that $K \supset I$, consider $K + I$. If $I \nsubseteq K$, then $K + I = R$, so $K + x = 1$ for $k \in K$ and $x \in I$. This tells us that $K = 1 - x$ and since $1 - x$ is invertible, we have that K is invertible, but this contradicts our assumption that K is a maximal right ideal; therefore, $I \subset K$. $\square$

Corollary 1.20. *$J_r(R)$ is equal to the unique maximal ideal with respect to the property that each of its elements is quasi-regular. Moreover, we have that $J_r(R) = J_\ell(R)$, so we will denote this ideal by $J(R)$.*

Definition 1.21. A ring R is called **semi-primitive** if $J(R) = 0$.

Theorem 1.22 (Schur's Lemma). *Let P be a simple right R-module and $D = \mathrm{End}_R(P_R)$, then D is a division ring.*

Remark 1.23. D acts on P on the left, and P has a natural $D - R$ bi-modules structure. Indeed, for $f \in \mathrm{End}_R(P_R)$, we have

$$f(pr) = f(p)r.$$

Proof. Suppose that $f \in D \backslash \{0\}$. We want to show that f is invertible. Consider $\ker(f)$ and $\mathrm{im}(f)$, which are sub-modules of P as right R-modules. Since $P \neq 0$, $\ker(f) \neq P$, which implies that $\ker(f) = 0$ since P is simple. Hence $\mathrm{im}(f) \neq 0$, so $\mathrm{im}(f) = P$ by the same logic. Thus f is a bijection. Let f^{-1} denote the inverse map of f. It is easily verified that f^{-1} is also R-linear, hence $f^{-1} \in D$. Moreover, D is a division ring. □

Endomorphisms of Semi-simple Modules. Let M, N be semi-simple R-modules, so we can represent them as a direct sum of simple R-modules M_i, resp. N_i. If $f : M \to N$ is a right R-modules homomorphism, then $f_j = f_{|M_j}$ can be represented as a tuple

$$(f_{1,j}, f_{2,j}, \ldots, fn, j)$$

where $f_{i,j} : M_j \longrightarrow N_i$. From this notation, it is clear that we can represent f as a $n \times m$ matrix

$$f = \begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \vdots & \vdots \\ f_{n,1} & \cdots & f_{n,m} \end{pmatrix}$$

i.e.,

$$\mathrm{Hom}_R(M_R, N_R) = \begin{pmatrix} \mathrm{Hom}_R(M_1, N_1) & \cdots & \mathrm{Hom}_R(M_1, N_m) \\ \vdots & \vdots & \vdots \\ \mathrm{Hom}_R(M_n, N_1) & \cdots & \mathrm{Hom}_R(M_n, N_m) \end{pmatrix}$$

with standard matrix multiplication by composition.

Theorem 1.24 (Artin- Wedderburn). *Let A be a finite dimensional algebra over a field and $J(A) = 0$. Then we may write $A = \bigoplus_{i=1}^n P_i^{d_i}$ with P_i mutually non-isomorphic and $A \cong (\mathrm{M}_{d_i}(D_i))^{\times n}$ where $D_i = \mathrm{End}(P_i)$ a division ring.*

Proof. Note that $A \cong \mathrm{End}_A(A_A)$ and $J(A) = 0$ implies that $A_A = P_i^{d_i}$ by Lemma 1.12. Schur's Lemma (Lemma 1.22) says that $D_i = \mathrm{End}_A((P_i)_A)$ is a division algebra. We can write

$$\mathrm{End}_A(A_A) = \begin{pmatrix} \mathrm{Hom}_R(P_1^{d_1}, P_1^{d_1}) & \cdots & \mathrm{Hom}_R(P_1^{d_1}, P_n^{d_n}) \\ \vdots & \vdots & \vdots \\ \mathrm{Hom}_R(P_n^{d_n}, P_1^{d_1}) & \cdots & \mathrm{Hom}_R(P_n^{d_n}, P_n^{d_n}) \end{pmatrix}$$

We can decompose this further by noting that

$$\mathrm{Hom}_R(P_i^{d_i}, P_j^{d_j}) = d_j \left\{ \underbrace{\begin{pmatrix} \mathrm{Hom}_R(P_i, P_j) & \cdots & \mathrm{Hom}_R(P_i, P_j) \\ \vdots & \vdots & \vdots \\ \mathrm{Hom}_R(P_i, P_j) & \cdots & \mathrm{Hom}_R(P_i, P_j) \end{pmatrix}}_{d_i} \right.$$

Since P_i is simple, $\mathrm{Hom}(P_i, P_j) = 0$ unless $i = j$. Note that in this case we have that $\mathrm{Hom}(P_i, P_i) = \mathrm{End}(P_i) = D_i$, so

$$\mathrm{End}_A(A_A) = \begin{pmatrix} M_{d_1}(D_1) & & & \\ & M_{d_2}(D_2) & & \\ & & \ddots & \\ & & & M_{d_n}(D_n) \end{pmatrix}$$

therefore, $\mathrm{End}_A(A_A) = M_{d_1}(D_1) \times \cdots \times M_{d_n}(D_n)$. □

Corollary 1.25. *If A is a finite dimensional, simple F algebra, then $A \cong M_n(D)$ where D is a division algebra over F and $Z(A) = Z(D)$.*

Proof. Since $J(A) \leqslant A$ and $1 \notin J(A)$, we have that $J(A) = 0$ since A simple. By Theorem **??**, we have that $A = (M_{d_i}(D_i))^{\times n}$. Since each factor $M_{d_i}(D_i)$ is an ideal and A is simple, we have that $n = 1$, and hence we have our desired decomposition.

For the second statement, using matrix representations for $Z(A)$ and $Z(D)$, we can construct an isomorphism $Z(D) \longrightarrow Z(A)$ sending $d \longmapsto d \cdot I_n$. □

Definition 1.26. An F-algebra A is called a **central simple algebra** over F (**CSA/F**) if A is simple and $Z(A) = F$.

2. Lecture (1/16): Tensors and Centralizers

Today we will discuss tensors and centralizers.

Tensor Products. Let R, S, T be rings. Let ${}_RM_S, {}_SN_T$ bi-module, and a map to ${}_RP_T$

$$\phi : M \times N \longrightarrow P$$

We say that ϕ is $R - S - T$ linear if

(1) for all $n \in N$, $m \mapsto \phi(m, n)$ is left R-module homomorphism;
(2) for all $m \in N$, $n \mapsto \phi(m, n)$ is right T-module homomorphism;
(3) $\phi(ns, m) = \phi(n, sm)$.

Definition 2.1. Given ${}_RM_S, {}_SN_T$, we say that a bi-module ${}_RP_T$ together with a $R - S - T$ linear map $M \times N \longrightarrow P$ is a **tensor product** of M and N over S is for all $M \times N \longrightarrow Q$

$R - S - T$ linear there exists a unique factorization:

$$\begin{tikzcd} M \times N \arrow[r] \arrow[d] & Q \\ P \arrow[ur, dashed, "\exists!"] & \end{tikzcd}$$

Definition 2.2. We define $M \otimes_S N$ to be the quotient of the free Abelian group generated by $M \times N$ by the subgroup generated by the relations

$$\begin{aligned} (m, n_1 + n_2) &= (m, n_1) + (m, n_2) \\ (m_1 + m_2, n) &= (m_1, n) + (m_2, n) \\ (ms, n) &= (n, sn) \end{aligned}$$

In the case where R commutative, left modules have right module structure and vice versa. In this way, $M_R \otimes_R {}_R N$ has an R-modules structure; so when R commutative, we will refer to a $R - R - R$ linear map as R bi-linear. We have the notation that the ordered pair (m, n) is the equivalence class $m \otimes n$, which are called **simple tensors**. We note that elements in $M \otimes_R N$ are linear combinations of simple tensors.

In the case of tensors over fields, a lot of the structure is much more transparent and simpler.

Proposition 2.3. *If V, W are vector space over a field F with bases $\{v_i\}, \{w_j\}$, then $V \otimes W$ is a vector space with basis given by $\{v_i \otimes w_j\}$.*

Proof. Clearly, this basis spans. To see independence, define a function $\phi_{k,l} : V \times W \longrightarrow F$ which maps $(\sum \alpha_i v_i, \sum \beta_j w_j) \longmapsto \alpha_k \beta_l$. This map is bi-linear, and the induced map on tensors is a group homomorphism. Hence we have linear independence. $\square$

If V/F is some vector space L/F field extension, then $L \otimes_F V$ is an L-vector space with basis $\{1 \otimes v_i\}$ where $\{v_i\}$ is a basis for V. Similarly, given a linear transformation $T : V \longrightarrow W$, then

$$L \otimes T : L \otimes V \longrightarrow L \otimes W$$

where $L \otimes T(x \otimes v) \mapsto x \otimes T(v)$. If we identify the bases of V and $L \otimes V$, we see that T and $L \otimes T$ have the "same" matrix. Thus

$$L \otimes (\ker T) = \ker(L \otimes T),$$

and similarly, for cokernel, image, etc.

Tensor Products of Algebras. If A, B are F-algebras, then $A \otimes B$ is naturally an F-algebra since

$$(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$$

Note that A, B are not necessarily commutative rings, so we are somewhat forcing this construction. In fact, something funny is actually happening. Inside $A \otimes B$, $A \otimes 1$ and $1 \otimes B$ are sub-algebras that are isomorphic to A and B, respectively. In particular, $A \otimes 1$ commutes with $1 \otimes B$.

Proposition 2.4. *Suppose A, B are F-algebras, then for any F-algebra C, there is a bijection between the following two sets:*

$$\{\mathrm{Hom}(A \otimes B, C)\} \leftrightarrow \{A \to C, B \to C \text{ such that images of } A \text{ and } B \text{ commute in } C\}$$

Proof. The inclusion $\subseteq$ is clear by our previous comment. For the reverse inclusion, $A \otimes B$ is generated as an algebra by $A \otimes 1$ and $1 \otimes B$. So given $\phi_1 : A \longrightarrow C, \phi_2 : B \longrightarrow C$, then $\rho : A \otimes B \longrightarrow C$ is defined by $a \otimes b \mapsto \phi_1(a) \cdot \phi_2(b)$. □

Given A, B F-algebras and ${}_AM_B$ we have homomorphisms $A \longrightarrow \mathrm{End}_F(M)$ and $B^{\mathrm{op}} \longrightarrow \mathrm{End}_F(M)$. Moreover, there images commute i.e., the images of A, B^{op} commute so $(am)b = a(mb)$. So we get a map

$$A \otimes B^{\mathrm{op}} \longrightarrow \mathrm{End}_F(M)$$

which defined a left $A \otimes B^{\mathrm{op}}$-modules structure on M. Thus, we have a natural equivalence of the categories $A - B$ bi-modules and left $A \otimes B^{\mathrm{op}}$-modules.

Commutators. Given A/F some algebra, and $\Lambda \subset A$, then

$$C_A(\Lambda) = \{a \in A : a\lambda = \lambda a \, \forall a \in A\},$$

and $C_A(A) = Z(A)$. Suppose that M is a right A-module, then we have a homomorphism $A^{\mathrm{op}} \longrightarrow \mathrm{End}_F(M)$. If we let $C = C_{\mathrm{End}_F(M)}(A^{\mathrm{op}}) = \mathrm{End}_A(M)$. To preserve our sanity, we will regard M as a left C-module. This gives M the structure of a $C - A$ bi-module.

Theorem 2.5 (Double Centralizer Theorem Warm-Up)**.** *Let B be an F-algebra, M a faithful, semi-simple right B-module, finitely dimensional over F. Let $E = \mathrm{End}_F(M)$, $C = C_E(B^{\mathrm{op}})$, then $B^{\mathrm{op}} = C_E(C) = C_E(C_E(B^{\mathrm{op}}))$.*

Proof. Let $\phi \in C_E(C)$. Choose $\{m_1, \ldots, m_n\}$ a basis for M/F. Write $N = \bigoplus^n M \ni w = (m_1, \ldots, m_n)$. Since M is semi-simple, so N is semi-simple. This allows us to write

$$N = wB \oplus N' \text{ for some } N'$$

Set $\pi : N \longrightarrow N'$ be a projection (right B-module map) that factors through wB. Since $\pi \in \mathrm{End}_B(N) = \mathrm{M}_n(\mathrm{End}_B(M)) = \mathrm{M}_n(C_{\mathrm{End}_F(M)}(B^{\mathrm{op}})) = \mathrm{M}_n(C)$.

Set $\phi^{\oplus n} : N \longrightarrow N$ doing ϕ on each entry. Then $w\phi^{\oplus n} = (\pi w)\phi^{\oplus n} = \pi(w\phi^{\oplus n}) = \pi(wb) \in wB$. The general principle is the following: $\mathrm{M}_N(\{\cdot\})$ commute with "scalar matrices" whose entries commute with $\{\cdot\}$, which is why we can move the w inside □

Our next goal is to prove that:

Theorem 2.6. *If A is a CSA/F, then $A \otimes_F A^{\mathrm{op}} \cong \mathrm{End}_F(A)$.*

Proof. Notice that A is an $A - A$ b-module, so it defines a map $A \otimes A^{\mathrm{op}} \longrightarrow \mathrm{End}_F(A)$. The question is why is this bijective. Suppose that $\{a_i\}$ is a baiss for A and (A^{op}). We wan to see when

$$\sum c_{i,j} a_i \otimes a_j \overset{?}{\longmapsto} 0 \in \mathrm{End}(A)$$

More abstractly, if we have A, B commuting sub-algebras of E. Let $a_i \in A$, $b_j \in B$ be linearly independent over F, then $a_i b_j$ is independent in E. Since E is an $A - A$ bi-module, so $A \otimes A^{\mathrm{op}}$ left module. E is also a right B-module, in particular $A \otimes A^{\mathrm{op}} - B$ bi-module. A is a CSA, so it is a simple $A \otimes A^{\mathrm{op}}$-module, and $\mathrm{End}_{A \otimes A^{\mathrm{op}}}(A) = F = Z(A)$. Thus

$$C_{\mathrm{End}_F(A)}(C_{\mathrm{End}_F(A)}(\mathrm{im}(A \otimes A^{\mathrm{op}}))) = C_{\mathrm{End}_F(A)}(F) = \mathrm{End}_F(A).$$

Then Theorem 2.5 tells us that $\mathrm{im}(A \otimes A^{\mathrm{op}}) = \mathrm{End}_F(A)$, which is what we desired.[1] $\square$

Thus, if A is a CSA, then $A \otimes A^{\mathrm{op}} \cong \mathrm{End}_F(A) = \mathrm{M}_n(F)$, where $n = \dim_F(A)$.

Proposition 2.7. *A is a CSA if and only if there exists B such that $A \otimes B \cong \mathrm{M}_n(F)$.*

Proof. $(\Rightarrow)$. This is clear. $(\Leftarrow)$. If $A \otimes B \cong M_n(F)$, note that $M_n(F)$ are central simple. If $I \leqslant A$, then $I \otimes B \leqslant \mathrm{M}_n(F)$ by dimension counting. If I is non-trivial, so is $I \otimes B$, hence A is simple. Thus, $Z(A) = C_{\mathrm{M}_n(F)}(A) \cap A$. We know that $B \subset C_{\mathrm{M}_n(F)(A)}$, which implies that $A \otimes C_{\mathrm{M}_n(F)}(A) \hookrightarrow \mathrm{M}_n(F)$. But we also know that $A \otimes B \cong \mathrm{M}_n(F)$ by assumption, hence we have $B = C_{\mathrm{M}_n(F)}(A)$. Thus $Z(A) = C_{\mathrm{M}_n(F)}(A) \cap A = B \cap A = F$. $\square$

Proposition 2.8. *A is a CSA/F if and only if for all field extensions L/F such that $L \otimes_F A$ CSA/L if and only if $\overline{F} \otimes_F A \cong \mathrm{M}_n(\overline{F})$.*

Proof. A is a CSA $\Rightarrow A \otimes A^{\mathrm{op}} \cong \mathrm{M}_n(F) \Rightarrow (A \otimes_F A^{\mathrm{op}}) \otimes_F L \cong \mathrm{M}_n(L)$. Notice that we can re-write $(A \otimes_F A^{\mathrm{op}}) \otimes_F L = (A \otimes L) \otimes_L (A^{\mathrm{op}} \otimes L)$, so by Proposition 2.7, we have that $A \otimes L$ is a CSA for all L. In particular, $A \otimes_F \overline{F}$ is a CSA. Thus by Theorem 1.24, $A \otimes_F \overline{F} \cong \mathrm{M}_n(D)$ for some finite dimensional division algebra $D/\overline{F}$. Hence for all $d \in D^\times$, $\overline{F}[d]/\overline{F}$ is a finite extension of $\overline{F}$. Since it is a finite extension, $d \in \overline{F}$, which implies that $D = \overline{F}$ i.e., $A \otimes_F \overline{F} \cong \mathrm{M}_n(\overline{F})$.

Now suppose that $A \otimes_F \overline{F} \cong \mathrm{M}_n(\overline{F})$. So A must be simple, otherwise, $I \otimes \overline{F} \leqslant A \otimes \overline{F} = \mathrm{M}_n(\overline{F})$. Now we want to show that $Z(A \otimes \overline{F}) = Z(A) \otimes \overline{F}$. This is true by considering the kernel of a linear map and just extending scalars. $\square$

Definition 2.9. If A is a CSA, then $\deg A = \sqrt{\dim_F(A)}$. This makes sense since $\overline{F} \otimes A \cong \mathrm{M}_n(\overline{F})$ has dimension n^2.

Definition 2.10. By Theorem 1.24, $A \cong \mathrm{M}_n(D)$, and we can check that $Z(D) = F$, hence D is a CSA, which we will call a **central division algebra (CDA)**. We define the **index of A** as $\mathrm{ind}(A) = \deg(D)$, where D is the underlying division algebra. We know that this is unique up to isomorphism, since $D = \mathrm{End}_A(P)$, where P is a simple right A-module.

Remark 2.11. Note that

$$\dim_F(A) = m^2 \dim_F(D)$$

so that $\deg A = m \deg D = m \,\mathrm{ind}\, A$, and in particular, $\mathrm{ind}\, A | \deg A$.

Brauer Equivalence.

Definition 2.12. CSA's A, B are **Brauer equivalent** $A \backsim B$ if and only if there exists r, s such that $\mathrm{M}_r(A) \cong \mathrm{M}_s(B)$. This essentially says that $\mathrm{M}_r(\mathrm{M}_n(D_A)) \cong \mathrm{M}_s(\mathrm{M}_m(D_B))$, which implies that $D_A \cong D_B$. Alternatively,

$$A \backsim B \iff \text{underlying divison algebras are isomorphic.}$$

N.B. If $A, B/F$ are CSA's, then $A \otimes_F B$ is also a CSA. The "cheap" way to prove this is to just tensor over $\overline{F}$ and see what happens.

[1] There was a lot of confusion on this proof. Review Danny's online notes for valid proof.

Definition 2.13. The **Brauer group** $\mathrm{Br}(F)$ is the group of Brauer equivalence classes of CSA's over F with operation $[A]+[B]=[A\otimes_F B]$. The identity element is $[F]$, and note that
$$[A]+[A^{\mathrm{op}}]=[A\otimes_F A^{\mathrm{op}}]=[\mathrm{M}_{\dim_F A}(F)]=[F].$$

Definition 2.14. The **exponent of A** (or **period of A**) is the order of $[A]$ in $\mathrm{Br}(F)$.

N.B. We will show that per $A|$ ind A.

3. Lecture (1/23): Noether-Skolem and Examples

Last time, we had a number of ways to characterize CSA's. A CSA if and only if there exists B such that $A\otimes B\in \mathrm{M}_n(F)$ if and only if $A\otimes A^{\mathrm{op}}\cong \mathrm{End}(A)$ if and only if $A\otimes_F L\cong \mathrm{M}_n(F)$ for some L/F if and only if $A\otimes_F \overline{F}\cong \mathrm{M}_n(\overline{F})$ if adn only if for every CSA B, $A\otimes B$ is a CSA (similarly for field extensions).

If A,B CSA, then $A\otimes B$ is a CSA. In Definition 2.12, we defined the relation that gave rise to the Brauer group. Moreover, in Definition 2.13, we gave the Brauer group a group structure.

Lemma 3.1. *A/F is a CSA and B/F simple, finite dimensional, then $A\otimes B$ is simple.*

Proof. If $L=Z(B)$, then B/L is a CSA. Hence $A\otimes_F B\cong A\otimes_F(L\otimes_L B)\cong(A\otimes_F L)\otimes_L B$ i.e., we are tensoring over two CSA's. Thus, we have a CSA$/L$, in particular, simple. □

Lemma 3.2. *Let $A=B\otimes C$ CSA's, then $C=C_A(B)$.*

Proof. By definition, everything in C centralizes A, so $C\subset C_A(B)$. But
$$\dim_F(C_A(B))=\dim_{\overline{F}}(C_A(B)\otimes\overline{F})=\dim_{\overline{F}}(C_{A\otimes\overline{F}}(B\otimes\overline{F}))$$
Without lose of generality, $B=\mathrm{M}_n(\overline{F}), C=\mathrm{M}_m(\overline{F})$. Hence
$$A=\mathrm{M}_n(\overline{F})\otimes\mathrm{M}_m(\overline{F})=\mathrm{M}_m(\mathrm{M}_n(\overline{F})).$$
So we want to look at
$$C_{\mathrm{M}_m(\mathrm{M}_n(\overline{F}))}(\mathrm{M}_n(\overline{F}))=\mathrm{M}_m(C_{\mathrm{M}_n(\overline{F})}\mathrm{M}_n(\overline{F}))=\mathrm{M}_m(Z(\mathrm{M}_n(\overline{F})))=\mathrm{M}_m(\overline{F})=C$$
by Lemma 3.4.1 of Danny's notes.

□

Theorem 3.3 (Noether-Skolem)**.** *Suppose that A/F is a CSA, $B,B'\subset A$ is a simple sub-algebra and $\psi: B\cong B'$. Then there exists $a\in A^\times$ such that $\psi(b)=aba^{-1}$.*

N.B. Think about inner automorphisms of matrices.

Proof. So $B\hookrightarrow A, B'\hookrightarrow A$ and $A\hookrightarrow A\otimes A^{\mathrm{op}}\cong\mathrm{End}_F(A)=\mathrm{End}_F(V)$ where $V=A$.[2] V is a $A-A$ bi-module, so it is a $B-A$ module or $B\otimes A^{\mathrm{op}}$ left module. Since B is simple

[2]We want to do this to remind ourselves that A is a vector space and also for notational reasons.

and A^{op} CSA, we have $B \otimes A^{\mathrm{op}}$ is simple, so it has a unique simple left module. V is determined by its dimension as a $B \otimes A^{\mathrm{op}}$ module since it can be regarded as a $B \otimes A^{\mathrm{op}}$ module in two different ways by two different actions, $(\psi(b) \otimes a)(v)$ and $(b \otimes a)(v)$. These two modules are isomorphic, that is to say that there exists $\phi : V \cong V$ such that $\phi((b \otimes a')(b)) = (\psi(b) \otimes a')(\phi(v))$.

Note that $\phi \in \mathrm{End}(V)^{\times} = \mathrm{End}(A)^{\times} = (A \otimes A^{\mathrm{op}})^{\times}$ by the sandwich map. Hence ϕ is a right A-module map i.e., $\phi \in C_{A \otimes A^{\mathrm{op}}}(A^{\mathrm{op}}) = A \otimes 1$. This means that ϕ is left-multiplication by $a \in A^{\times}$. Then for all $a \in A^{\times}$, let $a' = 1$, then

$$\begin{aligned} a \otimes 1(b \otimes 1(v)) &= \psi(b) \otimes 1(a \otimes 1(v)) \\ abv &= \psi(b)av \\ ab &= \psi(b)a \\ aba^{-1} &= \psi(b) \end{aligned}$$

□

Theorem 3.4 (Double Centralizer Theorem Step 3)**.** *Let A be a CSA, $B \subset A$ simple, then*

$$(\dim_F(C_A(B)))(\dim_F(B)) = \dim_F(A).$$

Proof. We want to look at $C_A(B)$. Since B is simple, B is a CSA$/L$ where $L = Z(B)$. Since $L \hookrightarrow B \hookrightarrow A \hookrightarrow A \otimes A^{\mathrm{op}} = \mathrm{End}_F(A)$. We remark that A is a left L-vector space, B acts on A as L-linear maps, so $B \subset \mathrm{End}_L(A) \subset \mathrm{End}_F(A)$. We now look at $C_{A \otimes A^{\mathrm{op}}}(B) = C_A(B) \otimes A^{\mathrm{op}}$. Since $L \subset B$, then $C_{A \otimes A^{\mathrm{op}}}(B)$ acts on A via L-linear maps. Hence

$$C_{A \otimes A^{\mathrm{op}}}(B) = C_{\mathrm{End}_F(A)}(B) = C_{\mathrm{End}_L(A)}(B).$$

So Theorem 4.1 tells us that

$$\mathrm{End}_L(A) = B \otimes_L C_{\mathrm{End}_L(B)} = B \otimes_L (B).$$

Now we want to compute the dimensions,

$$\begin{aligned} \dim_L(\mathrm{End}_L(A)) &= \dim_L(A)^2 = \left(\frac{\dim_F(A)}{[L:F]}\right)^2, \\ \dim_L(B) &= \frac{\dim_F(B)}{[L:F]} \\ \dim_L(C_{\mathrm{End}_L(A)}(B)) &= \frac{\dim_F C_{\mathrm{End}_L(B)}}{[L:F]} = \frac{\dim_F C_{\mathrm{End}_F(A)}(B)}{[L:F]} \\ &= \frac{\dim_F C_{A \otimes A^{\mathrm{op}}}(B)}{[L:F]} = \frac{(\dim_F C_A(B)) \dim_F A}{[L:F]} = \frac{\dim_F C_A(B) \otimes A^{\mathrm{op}}}{[L:F]} \end{aligned}$$

Thus

$$\left(\frac{\dim_F(A)}{[L:F]}\right)^2 = \frac{\dim_F B}{[L:F]} \left(\frac{\dim_F C_A(B) \dim_F(A)}{[L:F]}\right).$$

□

Existence of Maximal Subfields.

Definition 3.5. If A/F is a CSA, $F \subset E \subset A$ is a sub-field, we say that E is a **maximal sub-field** if $[E:F] = \deg A$.

Theorem 3.6. *If A is a division algebra, then there exists maximal and separable sub-fields.*

Proof. We will show in the case when F is infinite. Given some $a \in A$, look at $F(a)$. We know that $[F(a) : F] \leqslant n = \deg A$, so it is spanned by $\{1, a, a^2, \ldots, a^{n-1}\}$. We want these to be independent over F, so have an n dimension extension as well as the polynomial satisfied by a of $\deg n$ to be separable. This polynomial at $\overline{F}$ is χ_n, the characteristic polynomial. If χ_n has distinct roots, then it will be minimal, hence the unique polynomial of degree n satisfied by $a_{\overline{F}}$. The discriminant of the polynomial gives a polynomial in the coefficients which are polynomials in the coordinates of a and is non-vanishing if distinct eigenvalues.

Lemma 3.7. *Suppose V is a finite dimensional vector space over F, $F \subset L$, and F is infinite. If $f \in L[x_1, \ldots, x_n]$ non-constant, then there exists $a_1, \ldots, a_n \in F$, then $f(\vec{a}) \neq 0$*

Proof. For $n = 1$, any polynomial has only finitely many zeros if it is non-zero. Then we induct and just consider $k(x_1, \ldots, x_{n-1})[x_n]$. □

Hence by Lemma 3.7, we have our desired polynomial. □

Remark 3.8. From Theorem 3.4,

$$(\dim_F E)(\dim_F C_A(E)) = \dim_F A.$$

If $C_A(E) \supsetneq E$, then add another element to get a commutative sub-algebra. Indeed, if $\dim_F E \leqslant \sqrt{\dim_F(A)} = \deg A$ we can always get a bigger field. If F finite, then all extensions are separable, so we are done.

Structure and Examples.

Definition 3.9. A **quaternion algebra** is a degree 2 CSA. The structure is given by $\mathrm{M}_2(F)$ or D a division algebra.

There exists quadratic separable sub-fields if division algebra (and usually with matrices.) Let E/F be of degree 2, then E acts on itself by left multiplication, and $E \hookrightarrow \mathrm{End}_F(E) = \mathrm{M}_2(F)$. Suppose A is a quadratic extension, where $\operatorname{char} F \neq 2$, then $E = F(\sqrt{a})$, and let $i = \sqrt{a}$. Then we have an automorphism of E/F where $i \mapsto -i$. So Theorem 3.3, says that there exists $j \in A^\times$ such that $jij^{-1} = -i$, so $ij = -ji$. This says that j^2 commutes with i and j.

Lemma 3.10. *We have that $A = F \oplus Fi \oplus Fi \oplus Fij$.*

Proof. As a left $F(i)$ space, 1 does not generated and $\dim_{F(i)} A = 2$ and $j \notin F(i)$ for commutativity reasons. So this implies that $A = F(i) \oplus F(i)j$. Since j^2 commutes with ij, we have $j^2 \in Z(A) = F$, so $j^2 = b \in F$. Hence A is generated by i, j such that $i^2 = a \in F^\times, j^2 = b \in F^\times$ and $ij = -ji$. We can also deduce our usually anti-commutativity properties that we expect in a quaternion algebra.

Conversely, given any $a, b \in F^\times$, we can define $(a, b/F)$ to be the algebra above; this is a CSA since it is a quaternion algebra. It is enough to show that $(a, b/\overline{F})$ works. If we replace $i \mapsto i/\sqrt{a} = \tilde{i}$ and $j \mapsto j/\sqrt{b} = \tilde{j}$. Now we have $\tilde{i}^2 = 1 = \tilde{j}^2$, hence we want to show that $(1, 1/F)$ is a CSA. Note that $(1, 1/F) \cong \mathrm{End}_F(F[i])$ via $F[i] \mapsto$ left multiplication and $j \mapsto$ Galois action $i \mapsto -i$. It is an exercise to show that this map is an injection. □

Symbol Algebras. Given A/F a CSA of degree n. Suppose that there exists $E \subset A$ a maximal sub-field where $E = F(\sqrt[n]{a})$.[3] Let $\sigma \in \mathrm{Gal}(E/F)$ be a generator via $\sigma(\alpha) = \zeta\alpha$ where $\alpha = \sqrt[n]{a}$ and ζ is a primitive n^{th} root of unity. Theorem 3.3, there exists some $\beta \in A^\times$ such that $\beta\alpha\beta^{-1} = \omega\alpha$.

Lemma 3.11. *We can write*

$$A = E \oplus E\beta \oplus E\beta^2 \oplus \cdots \oplus E\beta^{n-1}.$$

Proof. This is true via the linear independence of characters. Consider the action of β on A via conjugation, then $E\beta^i = E$ as a vector space over E or over F. We have that $\alpha(x\beta^i)\alpha^{-1} = \zeta^{-i}x\beta^i$, so $E\beta^i$ consists of eigenvectors from conjugacy by α with value ζ^{-i}. This implies that β^n is central, hence $\beta^n = b \in F^\times$. So

$$A = \bigoplus_{i,j \in \{1,\ldots,n\}} F\alpha^i\beta^j$$

where $\beta\alpha = \zeta\alpha\beta$ and $\alpha^n = a$ and $\beta^n = b$. $\square$

Definition 3.12. If we define the **symbol algebra**, denoted by $(a,b)_\zeta$, to be

$$\bigoplus_{i,j \in \{1,\ldots,n\}} F\alpha^i\beta^j$$

where $\beta\alpha = \zeta\alpha\beta$ and $\alpha^n = a$ and $\beta^n = b$, then $(a,b)_\zeta$ is a CSA$/F$.

What if we don't assume Kummer extension? What about just a Galois extension?

Cyclic Algebras. Assume that E/F is cyclic with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ where $\sigma^n = \mathrm{Id}_E$. Suppose that $E \subset A$ is a maximal sub-field, we can choose $\mu \in A$ such that $\mu x = \sigma(x)\mu$ for all $x \in E$ via Theorem 3.3, then

$$A = E \oplus E\mu \oplus E\mu^2 \oplus \cdots \oplus E\mu^{n-1}.$$

Like before, it will follow that $\mu^n = b \in F = Z(A)$.

Definition 3.13. Then we say that $A = \Delta(E, \sigma, b)$ is a **cyclic algebra.**

It turns out that over a number field, all CSA's are of this form. There is a result due to Albert, that shows that these all CSA's are not cyclic. If E/F is an arbitrary Galois extension and $E \subset A$ is maximal. For every $g \in G$, there exists $u_g \in A$ such that $u_g x = g(x)u_g$ so that $A = \bigoplus_{g \in G} Eu_g$.

4. Lecture (1/30): Crossed Products

Last time, we did some warm-ups to the Double Centralizer Theorem (Theorem 2.5 and Theorem 3.4) i.e., if $B \subset \mathrm{End}_F(V)$ where B is simple, then $C_{\mathrm{End}_F(V)}(C_{\mathrm{End}_F(V)}B) = B$

[3]We call this a cyclic Kummer extension.

and if $A \cong B \otimes C$ all CSA$/F$, then $C = C_A(B)$. As well as the Noether-Skolem Theorem (Theorem 3.3).

Theorem 4.1 (Double Centralizer Theorem Warm-up 3). *If $B \subset A$ are CSA$/F$, then*

(1) $C_A(B)$ is a CSA$/F$,
(2) $A = BC_A(B) \cong B \otimes C_A(B)$.

Proof. If (2) holds, then A simple implies $C_A(B)$ is simple. If we look at $1 \otimes Z(C_A(B)) \hookrightarrow Z(A) = F$, hence $C_A(B)$ is central. To prove (2), we consider the map

$$B \otimes C_A(B) \longrightarrow A.$$

Without lose of generality, $F = \bar{F}$, in particular, $B = M_n(F)$ and $A = \mathrm{End}_F(V)$. Since B is simple, there exists a simple module, and since F^n is one such module, it is our unique one. If $B \subset A$, then V is a B-module, which implies that $V = (F^n)^m$. Hence $A = M_{nm}(F) = M_m(M_n(F))$.

Now we can compute $C_A(B) = C_{M_m(M_n(F))}(M_n(F))$, where $M_n(F)$ are block scalar matrices. Note that $C_{M_m(M_n(F))}(M_n(F)) = M_m(Z(M_n(F))) = M_m(F)$. Thus we have

$$M_n(F) \otimes M_m(F) \cong M_{mn}(F).$$

□

Theorem 4.2 (Full-on Double Centralizer Theorem). *Let $B \subset A$ where A is a CSA$/F$ and B is simple. We have the following:*

(1) $C_A(B)$ is simple;
(2) $(\dim_F B)(\dim_F(C_A(B))) = \dim_F(A)$ (Theorem 3.4);
(3) $C_A(C_A(B)) = B$;
(4) If B is a CSA$/F$, then $A \cong B \otimes C_A(B)$ (Theorem 4.1).

Proof. To prove (3), we can think of $B \hookrightarrow A \hookrightarrow A \otimes A^{\mathrm{op}} = \mathrm{End}_F(A)$. By Theorem 2.5, we know that $B = C_{\mathrm{End}_F(A)}(C_{\mathrm{End}_F(A)}(B))$. We note that

$$C_{\mathrm{End}_F(A)}(B) = C_{A \otimes A^{\mathrm{op}}}(B) = C_A(B) \otimes A^{\mathrm{op}},$$

and for the second centralizer

$$C_{A \otimes A^{\mathrm{op}}}(C_A(B) \otimes A^{\mathrm{op}}) = C_A(C_A(B)) \otimes 1 = B.$$

(1) follows from the fact that $C_{A \otimes A^{\mathrm{op}}}(B) = C_A(B) \otimes A^{\mathrm{op}}$ is simple. □

Suppose A is a CSA$/F$ and $E \subset A$ maximal sub-field i.e., $[E : F] = \deg A$ and E/F is Galois with Galois group G. In this case, if $\sigma \in G$, there exists $u_\sigma \in A^\times$ such that $u_\sigma \times u_\sigma^{-1} = \sigma(x)$ for $x \in E$[4]. We will show that

$$A = \bigoplus_{\sigma \in G} E u_\sigma.$$

Lemma 4.3. *These Noether-Skolem elements u_σ are independent of E.*

Proof. If not, then choose some minimal dependence relation

$$\begin{aligned} \sum x_\sigma u_\sigma &= 0 \\ \Rightarrow 0 &= \sum x_\sigma u_\sigma y = \sum x_\sigma \sigma(y) u_\sigma y. \end{aligned}$$

[4]We will call these elements u_σ Noether-Skolem elements.

This implies that $\lambda x_\sigma = x_\sigma \sigma(y)$ for all σ for some fixed λ i.e., $\sigma(y) = \lambda$ for all σ. Thus $y \in F$, so by dimension count $A = Eu_\sigma$. If u_σ and v_σ are both Noether-Skolem for $\sigma \in G$, then $u_\sigma v_\sigma^{-1} x = x u_\sigma v_\sigma^{-1}$ for $x \in E$. We note that $u_\sigma v_\sigma^{-1} \in C_A(E) = E$ by Double Centralizer Theorem, so $v_\sigma = \lambda_\sigma u_\sigma$ for some $\lambda_\sigma \in E^\times$. □

Conversely, such a v_σ is Noether-Skolem for σ. Notice that $u_\sigma u_\tau$ and $u_{\sigma\tau}$ are both Noether-Skolem for $\sigma\tau$, so $u_\sigma u_\tau = c(\sigma,\tau) u_{\sigma\tau}$ for some $c(\sigma,\tau) \in E^\times$. We can also check associativity meaning that $u_\sigma(u_\tau u\gamma) = (u_\sigma u_\tau)u\gamma$. We will find that

$$c(\sigma,\tau)c(\sigma\tau,\gamma) = c(\sigma,\tau\gamma)\sigma(c(\sigma,\gamma)). \tag{4.3.0.1}$$

Definition 4.4. We call this the **2-cocycle condition** for a function $c : G \times G \longrightarrow E^\times$ if

$$c(\sigma,\tau)c(\sigma\tau,\gamma) = c(\sigma,\tau\gamma)\sigma(c(\sigma,\gamma)).$$

Definition 4.5. If E/F is Galois, $c : G \times G \longrightarrow E^\times$ a 2-cocycle condition, then define (E,G,c) to be the **crossed product algebra**, which we denote by $\bigoplus Eu_\sigma$ with multiplication defined by

$$(xu_\sigma)(yu_\tau) = x\sigma(y)c(\sigma,\tau)u_{\sigma\tau}.$$

Proposition 4.6. *$A = (E,G,c)$ as above is a CSA$/F$.*

Proof. If $A \twoheadrightarrow B$, then $E \hookrightarrow B$ since E is simple and $u_\sigma \longrightarrow v_\sigma \in B$ are Noether-Skolem in B for E. Due to the independence of B, then we have injection. Note that $Z(A) \subset C_A(E) = E$ and note that $C_A(\{u_\sigma\}_{\sigma\in G}) \cap E = F$ due to the Galois action, so we have that A is central. □

Question 1. When is $(E,G,c) \cong (E,G,c')$?

By Noether-Skolem, the isomorphism must preserve E so $\varphi(E) = E$. Hence $\varphi(u_\sigma)$ is a Noether-Skolem in (E,G,c'). Since $(E,G,c) = \bigoplus Eu_\sigma$ and $(E,G,c') = \bigoplus Eu_{\sigma'}$, hence $\varphi(u_\sigma) = x_\sigma u_{\sigma'}$. The homorphism condition says that

$$\varphi(c(\sigma,\tau)u_{\sigma\tau}) = c(\sigma,\tau)x_{\sigma\tau}u'_{\sigma\tau} = \varphi(u_\sigma u_\tau) = \varphi(u_\sigma)\varphi(u_\tau) = (x_\sigma u'_\sigma)(x_\tau u'_\tau),$$

which implies that

$$c(\sigma,\tau)x_{\sigma\tau} = x_\sigma \sigma(x_\tau)c'(\sigma,\tau)$$

i.e., $c(\sigma,\tau) = x_\sigma\sigma(x_\tau)x_{\sigma\tau}^{-1}c'(\sigma,\tau)$ for some elements $\sigma \in E^\times$ for each $\sigma \in G$.

Definition 4.7. We say that c, c' are **cohomologous** if there exists $b : G \longrightarrow E^\times$ such that

$$c(\sigma,\tau) = b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1}c'(\sigma,\tau).$$

Definition 4.8. Set

$$B^2(G,E^\times) = \left\{ f : G \times G \longrightarrow E^\times | f = b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1} \text{ for some } b : G \longrightarrow E^\times \right\}$$

and

$$Z^2(G,E^\times) = \left\{ f : G \times G \longrightarrow E^\times | \text{2 cocyles} \right\}.$$

These are groups via point-wise multiplication. We define

$$H^2(G,E^\times) = \frac{Z^2(G,E^\times)}{B^2(G,E^\times)}.$$

Proposition 4.9. *$H^2(G, E^\times)$ is in bijection with isomorphism classes if CSA$/F$ such that $E \subset A$ is maximal.*

To approach the group structure, we need to learn about idempotents.

Idempotents.

Definition 4.10. We call an element $e \in A$ an **idempotent** if $e^2 = e$.

If e is central, then it is clear that $e(1-e) = 0$ and $(1-e)^2 = 1-e$. Now
$$A = A \cdot 1 = A(e + (1-e)) = Ae \times A(1-e).$$
The point is that $e \in eA$ and $(1-e) \in (1-e)A$ act as identities, hence $(ae)(b(1-e)) = abe(1-e) = 0$. Writing a ring $A = A_1 \times A_2$ is equivalent to finding idempotents i.e., identity elements in A_1 and A_2. If e is not central, $f = 1-e$ and $e + f = 1$. So we can write
$$1A1 = (e+f)A(e+f) = eAe + eAf + fAe + fAf$$
where eAe and fAf are rings with identities e and f.

If we think of
$$A = \mathrm{End}(A_A) = \mathrm{End}(eA \oplus fA) = \begin{pmatrix} \mathrm{End}(eA) & \mathrm{Hom}(fA, eA) \\ \mathrm{Hom}(eA, fA) & \mathrm{End}(fA) \end{pmatrix}$$
We claim that this decomposition falls in line with $A = eAe \oplus eAf \oplus fAe \oplus fAf$. Suppose we take $(eaf)(eb) = 0$ and $(eaf)(fb) \in eA$. We note that
$$eaf = \begin{pmatrix} 0 & \star \\ 0 & 0 \end{pmatrix}$$
so we have that
$$eAf = \begin{pmatrix} 0 & \mathrm{Hom}(fA, eA) \\ 0 & 0 \end{pmatrix}$$
So $eAe = \mathrm{End}_A(eA)$and $eAf = \mathrm{Hom}_A(fA, eA)$, and so on and so on. This is called **Pierce decomposition**. So as a matrix algebra we have
$$A = \begin{pmatrix} eAe & fAe \\ eAf & fAf \end{pmatrix}$$
Let's assume that A is a CSA$/F$ and let $e \in A$ be an idempotent. So we have $eAe = \mathrm{End}_A(eA) = \mathrm{End}_A(P^n) = M_n(D)$ and $A = \mathrm{End}_A(A_A) = \mathrm{End}_A(P^m) = M_m(D)$, where $D = \mathrm{End}_A(P_A)$, which implies that $eAe \backsim A$ under the Brauer equivalence. So idempotents give us a way to recognize Brauer equivalence.

If we take two cross product algebras, $(E, G, c) \otimes (E, G, c') \backsim (E, G, cc')$. We want an idempotent in the tensor product that will allow us to "chop" or deduce our equivalence. Note that
$$E \otimes E = E \otimes F[x]/f(x) = E[x]/f(x) = \prod E[x]/(x - \alpha_i) = \prod_{\sigma \in G} E[x]/(x - \sigma(\alpha)) = \prod_{\sigma \in G} E,$$
where α is just some root. This says that there are idempotents in the product, namely $e_\sigma \in E \otimes E$, where $\sigma \in G$. The punchline is that e_1 will work, but we will need to prove it.

Let's look at the map

$$\begin{array}{rcl} E\otimes E & \longrightarrow & \dfrac{E[x]}{x-\sigma(\alpha)} \cong E \\ a\otimes b & \longmapsto & a\sigma(b) \\ 1\otimes\alpha & \longmapsto & x \\ (1\otimes z)e_\sigma & \longmapsto & E\sigma(a) \\ (\sigma(a)\otimes 1)e_\sigma & \longmapsto & \sigma(a) \end{array}$$

Hence $(1\otimes a)E_\sigma = (\sigma(z)\otimes 1)e_\sigma$. Let $(E,G,c) = A \ni u_\sigma$ and $(E,G,c') = A' \ni u'_\sigma$. Let $e = e_1$ so $eAe \ni ew_\sigma$ where $w_\sigma = u_\sigma \otimes u'_\sigma$, which does exists. We note that $E\otimes E \subset A\otimes A'$. We want to see how the e and the Noether-Skolem elements interact,

$$\begin{array}{rcl} (1\otimes u'_\sigma)e(1\otimes u'^{-1}_\sigma)(1\otimes x) & = & (1\otimes u'^{-1}_\sigma)e(1\otimes\sigma(x))(1\otimes u'_\sigma) \\ & = & (1\otimes u'^{-1}_\sigma)e(\sigma(x)\otimes 1)(1\otimes u'_\sigma) \\ & = & (1\otimes u'^{-1}_\sigma)e(1\otimes u'_\sigma)(\sigma(x)\otimes 1). \end{array}$$

This did what e_σ should do. Note that conjugation takes idempotents to idempotents, so $(1\otimes u'^{-1}_\sigma)$ is in fact idempotent. We can note that $(u_\sigma\otimes u'_\sigma)e = e(u_\sigma\otimes u'_\sigma)$, so if we let $w_\sigma = (u_\sigma\otimes u'_\sigma)$. Then we have that $ew_\sigma = e^2 w_\sigma = ew_\sigma e \in eA\otimes A'e$. We want $eA\otimes A'e$ as (E,G,c). Since $eE\otimes E \cong E$ via the map $e(E\otimes 1)$.

We want to show that if we have

$$\begin{array}{rcl} ew_\sigma(x\otimes 1)e & = & e(u_\sigma\otimes u'_\sigma)(x\otimes 1)e \\ & = & e(\sigma(x)\otimes 1)(u_\sigma\otimes u'_\sigma)e \\ & = & e(\sigma(x)\otimes 1)w_\sigma e \end{array}$$

So ew'_σ's are Noether-Skolem elements, so

$$eA\oplus A'e \supseteq \bigoplus_{\sigma\in G} e(E\otimes 1)ew_\sigma.$$

For equality, let $e(xu_\sigma\otimes yu'_\tau)e \in eA\otimes A'e$. We can re-write this as so,

$$\begin{array}{rcl} e(xu_\sigma\otimes yu'_\tau)e & = & e(x\otimes y)(u_\sigma\otimes u'_\tau)e \\ & = & e(x\otimes y)(u_\sigma u'^{-1}_\tau\otimes 1)(u_\tau\otimes u'_\tau)e \\ & = & (xy\otimes 1)e(u_\sigma u_\tau^{-1}\otimes 1)ew_\tau e \\ & = & (xy\otimes 1)\lambda e(u_\sigma u_{\tau^{-1}}\otimes 1)e \\ & = & (xy\otimes 1)\lambda(u_\sigma u_{\tau^{-1}}\otimes 1)e_{\sigma\tau^{-1}}e \\ & = & \begin{cases} 0 & \text{if } \sigma\neq\tau \\ \lambda'' e & \text{otherwise.} \end{cases} \\ & = & \begin{cases} 0 & \text{if } \sigma\neq\tau \\ (xy\otimes 1)(\lambda\otimes 1)e\lambda'' ew_\sigma e \in \bigoplus_{\sigma\in G} e(E\otimes 1)ew_\sigma & \text{otherwise.} \end{cases} \end{array}$$

since $u_\tau^{-1} = \lambda u_{\tau^{-1}}$ for some $\lambda\in E^\times$. Hence $eA\otimes A'e \cong A\otimes A' \cong (E,G,cc')$. Danny checks the cocycle condition, however, I will not repeat this computation. Thus we have shown that the operation in $H^2 =$ Br group operation i.e.,

$$\mathrm{Br}(E/F) := \{[A] : A \;\; CSA/F \text{ with } E \subset A \text{ maximal}\}$$

is a subgroup of $\mathrm{Br}(F) \cong H^2(G, E^\times)$. We sometimes call this group $\mathrm{Br}(E/F)$ the **relative Brauer group of F.**

5. Lecture (2/6): First and Second Cohomology Groups

Last time we defined that $\mathrm{Br}(E/F)$ is the set of equivalence classes of CSA$/F$ with E maximal sub-field and E/F is Galois. We showed that his is actually a group, namely, $\mathrm{Br}(E/F) \cong \mathrm{H}^2(G, E^\times) = Z^2(G, E^\times)/B^2(G, E^\times)$. The mapping from $\mathrm{H}^2(G, E^\times)$ to $\mathrm{Br}(E/F)$ was defined by $c \mapsto (E, G, c)$, then crossed product algebra as defined in 4.5. We want to relate splitting fields to maximal subfields.

Definition 5.1. We say that E/F **splits** if $A \otimes_F E \cong M_n(E)$.

We always have splitting fields, namely the algebraic closure; moreover, there are splitting fields which are finite extensions.

Lemma 5.2. *If A CSA $/F$, $E \subset A$ subfield, then $C_A(E) \backsim A \otimes_F E$.*

Proof. Note that $\otimes E \hookrightarrow A \otimes A^{\mathrm{op}} = \mathrm{End}_F A$. We look at

$$\begin{aligned}\mathrm{End}_E(A) &= C_{\mathrm{End}_F(A)}(E) = A \otimes C_{A^{\mathrm{op}}}(E) = A \otimes_F E \otimes_E C_{A^{\mathrm{op}}}(E) \\ &= (A \otimes_F E) \otimes_E C_{A^{\mathrm{op}}}(E) = (A \otimes_F E) \otimes_E C_A(E)^{\mathrm{op}}.\end{aligned}$$

Since $\mathrm{End}_E(A)$ is a split E-algebra, thus

$$[A \otimes E] - [C_A(E)] = 0 \in \mathrm{Br}\, E.$$

□

Corollary 5.3. *If $E \subset D$ D CSA $/F$, then $(\mathrm{ind}\ D \otimes E)[E : F] = \mathrm{ind}\, D$.*

Proof. By Theorem 4.2, we have that $\dim_F C_D(E)[E : F] = \dim_F D$. By taking the dimension over E, we have

$$\begin{aligned}\deg C_D(E)^2[E : F]^2 &= (\deg D)^2 \\ \deg C_D(E)[E : F] &= (\deg D) = \mathrm{ind}\, D \\ \Rightarrow \mathrm{ind}\, C_D(E)[E : F] &= \mathrm{ind}\, D \\ (\mathrm{ind}\, D \otimes E)[E : f] &= \mathrm{ind}\, D.\end{aligned}$$

□

Remark 5.4. If $E \subset A$ is a maximal subfield, then $A \otimes E$ is split. Indeed, since $A \otimes E \backsim C_A(E) = E$ by Theorem 4.2.

Proposition 5.5. *If A CSA $/F$, $E \otimes A \cong M_n(F)$, and $[E : F] = \deg A = n$, then E is isomorphic to a maximal subfield of A.*

Proof. Note that $E \hookrightarrow \mathrm{End}_F(E) = M_n(F) \hookrightarrow A \otimes M_n(F)$. Now we compute

$$\begin{aligned} C_{A\otimes M_n(F)}(E) &\cong (A \otimes M_n(F)) \otimes_F E \\ &\cong M_n(F) = E \otimes M_n(F) \end{aligned}$$

We have the map

$$\begin{aligned} \varphi : E \otimes M_n(F) &\longrightarrow A \otimes M_n(F) \\ M_n(F) &\longmapsto B \end{aligned}$$

By Noether-Skolem, we acn replace φ by φ composed with an inner automorphism so that $B \cong 1 \otimes M_n(F)$. So now note that $C_{E\otimes M_n(F)}(M_n(F)) \subset E \subset E \otimes M_n(F)$, hence $\varphi(E) \subset C_{E\otimes M_n(F)}(M_n(F))E = A \otimes 1$. $\square$

If we have a splitting field for our algebra with appropriate dimension, then it must a maximal field.

Corollary 5.6. *Let A/F be a* CSA $/F$*, then $[A] \in$* Br(E/F) *for some E/F is Galois.*

Proof. Write $A = M_m(D)$, where $[A] = [D]$. WLOG A is a division algebra. We know that D has a maximal separable subfield $L \subset D$. Let E/F be the Galois closure of L/F. We claim that $E \hookrightarrow M_m(D)$. We have that $E \hookrightarrow \mathrm{End}_L(E) = M_{[E:L]}(L)$ via left-multiplication. If we look at $D \otimes_F M_{[E:L]}(F) \supset L \otimes M_{[E:L]}(F) = M_{[E:L]}(L) \supset E$. Note that the left hand side has degree equal to $[E : F]$ since $\deg D[E : L] = [L : F][E : L] = [E : F]$. By Lemma 5.5, we have that E is a maximal subfield of $D \otimes M_{[E:L]}(F)$. Therefore, $[A] = [D] \in \mathrm{Br}(E/F)$. $\square$

Galois Descent. We fix E/F a G-Galois extension. A is a CSA $/F$ if and only if $A \otimes E \cong M_n(E)$ for some E/F Galois. We can interpret this as saying that A is a "twiseted form" of a matrix algebra.

Definition 5.7. Given an algebra A/F, we say that B/F is a **twisted form of** A if $A \otimes_F E \cong B \otimes_F E$ for some E/F separable and Galois.[5]

Descent is the process of going from E to F i.e., descending back down. We use that fact that $E^G = F$ where G is the Galois group. The idea is as follows: given $A \otimes E$, G acts on the E-part and the invariatns give A. The issue here is that the isomorphism in Definition 5.7 does not respect the Galois action, meaning that different actions could produce different isomorphisms.

Definition 5.8. A **semi-linear action** of G on an E-vector space V is an action of G on V (as F-linear transformations) such that

$$\sigma(xv) = \sigma(x)\sigma(v) \quad \forall\, x \in E, v \in V. \tag{5.8.0.2}$$

Theorem 5.9. *There is an equivalence of categories*

$$\begin{aligned} \{F\text{-vector spaces}\} &\longleftrightarrow \{E\text{-vector spaces with semi-linear action}\} \\ V &\longmapsto V \otimes_F E \\ W^G &\longleftarrow W \end{aligned}$$

[5]We could make an equivalent definition for any *algebraic structure*. We leave this vague on purpose.

If V is an E-space with semi-linear action, we get an action of $(E, G, 1)$ on V where $E = \bigoplus Eu_\sigma$ and $u_\sigma u_\tau = u_{\sigma\tau}$ and $u_\sigma x = \sigma(x)u_\sigma$ via $(xu_\sigma)(v) = x\sigma(v)$. We can check well-definedness as so

$$\begin{aligned} (xu_\sigma)(yu_\tau)(v) &= xu_\sigma(y\tau(v)) = x\sigma(y)\sigma\tau(v) \\ \Rightarrow (x\sigma(y)u_\sigma u_\tau)(v) = x\sigma(y)u_{\sigma\tau}(v) = x\sigma(y)\sigma\tau(v) &= x\sigma(y)\sigma\tau(v) \end{aligned}$$

Actually, a semi-linear action on U is a $(E, G, 1)$ module structure $u_\sigma v$. Hence $(E, G, 1)$ has a unique simple module E. If V is semi-linear, then $V \cong E^n$ and vice versa. To see the equivalence of Theorem 5.9, we notice that the unique simple E goes to F and the F goes back to E, and these are unique.

If V is some semi-linear space, so a $(E, G, 1)$ module, then $V^G \cong E' \otimes_{(E,G,1)} V$, where E' is the unique simple $(E, G, 1)$ module. We hope to describe this later.

Definition 5.10. If V, W are semi-linear spaces, then a semi-linear morphism is $\varphi : V \to W$ is an F linear map such that $\varphi(\sigma(v)) = \sigma\varphi(v)$.

Under the equivalence of Theorem 5.9, we can see that

$$\bigoplus Fe_i \cong W \longrightarrow \bigoplus Ee_i \cong W \otimes E \longrightarrow (W \otimes E)^G = \bigoplus E^G e_i \cong \bigoplus Fe_i$$

In the reverse direction, we know that

$$V = \bigoplus Ee_i \longrightarrow \bigoplus E^G e_i = \bigoplus Fe_i \longrightarrow \bigoplus (F \otimes_F E)e_i = \bigoplus Ee_i.$$

We have shown that there is a *natural* isomorphism of objects, so now we must consider arrows. If $\varphi : W \longrightarrow W$ is an F- linear map, then $\varphi \otimes E : W \otimes E \longrightarrow W' \otimes E$. Then

$$\begin{tikzcd} a \otimes x \arrow[r] \arrow[d, "\sigma"] & \varphi(a) \otimes x \arrow[d, "\sigma"] \\ a \otimes \sigma(x) \arrow[r] & \varphi(a) \otimes \sigma(x) \end{tikzcd}$$

i.e., σ acts on the left component. If $\psi : V \longrightarrow V'$ is semi-linear, then ψ induces a map via restriction to $V^G \longrightarrow (V')^G$, so the arrows correspond as well.

If V, W are semi-linear spaces, how should we define the action on $V \otimes_E W$? It is sort of induced on us, meaning $V = \overline{V} \otimes E$ and $W = \overline{W} \otimes E$. Hence

$$V \otimes_E W = (\overline{V} \otimes E) \otimes_E (\overline{W} \otimes E) = (\overline{V} \otimes \overline{W}) \otimes E.$$

We can check the compatibility of the action by consider the diagram:

$$\begin{tikzcd} (\overline{V} \otimes E) \otimes_E (\overline{W} \otimes E) \arrow[r, leftrightarrow] & (\overline{V} \otimes \overline{W}) \otimes E \\ \overline{V} \otimes \overline{W} \arrow[u] \arrow[ur] & \end{tikzcd}$$

Hence the answer to our previous question is that σ must act on the right component. Thus we have an equivalence of categories with tensors.

Definition 5.11. A **semi-linear action** of G on an algebra A/E is a map from $G \longrightarrow \mathrm{Aut}(A/F)$ such that $\sigma(xa) = \sigma(x)\sigma(a)$ for all $x \in E, a \in A$. In particular, $\sigma(ab) = \sigma(a)\sigma(b)$ implies that $A \otimes A \longrightarrow A$ is semi-linear.

Theorem 5.9 says that semi-linear algebras over E correspond to F-algebras by taking invariants and tensoring up. We now want to classify these semi-linear mappings. If A is some interesting algebra, we want to find all twisted forms A. If B is a twisted form and we have an isomorphism $\phi : B \otimes E \longrightarrow A \otimes E$. We can define a new action where $\sigma_B(\alpha) = \phi(\sigma(\phi^{-1}(\alpha)))$ where $\alpha \in A \otimes E$. How do these actions compare?

We can compute $\sigma^{-1}(\sigma_B(\alpha)) \in \mathrm{Aut}_E(A \otimes E)$ and we can check that $\sigma^{-1}(\sigma_B(x\alpha)) = x\sigma^{-1}(\sigma_B(\alpha))$. For similar reasons, $\sigma_B \circ \sigma^{-1} \in \mathrm{Aut}_E(A \otimes E)$ so $\sigma_B = a_\sigma \circ \sigma$ for some $a_\sigma \in \mathrm{Aut}_E(A \otimes E)$. We can check that $\sigma_B \tau_B = (\sigma\tau)_B$; moreover that $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$, which is called the **1-cocycle** or equivalently $a(\sigma\tau) = a(\sigma)\sigma(a\tau)$ a **cross homomorphism**.

Theorem 5.12. *If B is a twisted form of A, there there exists a map G to $\mathrm{Aut}_E(A \otimes E)$ which is a 1-cocycle and such that $B = (A \otimes E)_a^G$ where the subscript means $A \otimes E$ with the new action $\sigma_a(\alpha) = a_\sigma \sigma(\alpha)$. Conversely, every such 1-cocycle gives a twisted form.*

Proof. Given a 1-cocycle $a : G \longrightarrow \mathrm{Aut}(A \otimes E)$, let's check that the action of $(A \otimes E)_a$ is semi-linear. We want to know that $\sigma_a \tau_a(\alpha) = (\sigma\tau)_a(\alpha)$ and $\sigma_a(x\alpha) = \sigma(x)\sigma_a(x)$. Using the assumption that a is a 1-cocycle and doing a cohomology calculation, we can verify these results. Once we picked an isomorphism $A \otimes E \longrightarrow B \otimes E$, then everything else was well-defined. If we pick different φ's then how is everything related. We can find that a_σ and a'_σ are cohomologous if $a'_\sigma = ba_\sigma(\sigma b^{-1}\sigma^{-1})$ for some $b \in \mathrm{Aut}(A \otimes E)$. The equivalence classes under cohomology are in bijective correspondence with isomorphism classes of semi-linear actions and therefore, in bijection with twisted forms of A.

□

Definition 5.13. We define $\mathrm{H}^1(G, \mathrm{Aut}(A \otimes E))$ is the *set* of these cohomology classes i.e., cocycles up to equivalence. The base point of this pointed set is $a_\sigma = 1$, which refers to A as a twisted algebra of itself A.

6. Lecture (2/13): Cohomology and the Connecting Map

Let E/F be G Galois and some vector space V/F. We can tensor up to $V \otimes E$ with a G action on the second component. We note that $V \cong (V \otimes E)^G$ by hitting the tensor with G and seeing what doesn't move. Recall Theorem 5.9. Suppose that $V = F^n$, then $V \otimes E = E^n$ and we can write $\mathrm{End}_E(V \otimes E) = E^{n^2}$. By thinking about the action of G coordinate wise on $\mathrm{End}_E(V \otimes E)$, we can deduce that some $\sigma \in G$ acts on $f \in \mathrm{End}_E(V \otimes E)$ by $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. For example, if $f = xe_{ij}$ such that

$$\sigma(f)(e_k) = \sigma(f(e_k)) = \sigma(xe_{ij}e_k) = \sigma(x\delta_{jk}e_i) = \sigma(x)\delta_{jk}e_i.$$

Give a "model" algebra A_0/F, we can ask to classify all of the A/F such that $A \otimes E \cong A_0 \otimes E$, in particular, we are looking for CSA $/F$ that split over E of degree n. If

$\phi : A \otimes E \longrightarrow A_0 \otimes E$, then we can transport the action of G on the left to the right i.e., we want to analyze the Galois action on E. Hence

$$\sigma \cdot x = \phi\sigma\phi^{-1}(x). \tag{6.0.0.3}$$

If we set $b(\sigma) = \phi\sigma\phi^{-1}\sigma^{-1} \in \mathrm{Aut}_E(A_0 \otimes E)$, then we can rewrite (6.0.0.3) as

$$\sigma \cdot x = b(\sigma) \circ \sigma(x). \tag{6.0.0.4}$$

If we set $b(\sigma\tau) = b(\sigma)\sigma(b(\tau))$, then we can say that $\sigma \circ (\tau \circ x) = \sigma\tau \circ x$. We can also modify ϕ by hitting $A_0 \times E$ by an automorphism a. Set $\phi' = a^{-1}\phi$. The new action will be

$$\begin{aligned}
\phi'\sigma\phi'^{-1}\sigma'^{-1} &= a^{-1}\phi\sigma(a^{-1}\phi)^{-1}\sigma^{-1} \\
&= a^{-1}\phi\sigma\phi^{-1}a\sigma^{-1} \\
&= a^{-1}\phi\sigma\phi^{-1}\sigma^{-1}\sigma a\sigma^{-1} \\
&= a^{-1}b(\sigma)\sigma(a),
\end{aligned}$$

hence we say that

$$b \backsim b' \iff b'(\sigma) = a^{-1}b(\sigma)\sigma(a) \text{ for some } a \in \mathrm{Aut}_E(A_0 \otimes E).$$

Definition 6.1. Suppose that X is a group with action of G.Then we define

$$Z^1(G, X) = \{b : G \longrightarrow X \mid b(\sigma\tau) = b(\sigma)\sigma(b(\tau))\}$$

and $b \backsim b'$ if there exist some $x \in X$ such that $b'(\sigma) = x^{-1}b(\sigma)\sigma(x)$ for all $\sigma \in G$. We define $\mathrm{H}^1(G, X)$ to be the set of equivalence classes of the above form.

In particular, we know that

$$\text{CSA } /F \text{ of degree } n \text{ with splitting field } E/F \quad \longleftrightarrow \quad \mathrm{H}^1(G, \mathrm{Aut}_E(M_n(E)))$$

Note that $\mathrm{GL}_n(E) \twoheadrightarrow \mathrm{Aut}_E(M_n(E))$ with conjugation by T and the kernel of this map are the central matrices which are the scalars i.e., $E^\times$.

Definition 6.2. We define $\mathrm{PGL}_n(E) = \mathrm{GL}_n(E)/E^\times$. From Definition 6.1, we have that

$$\mathrm{H}^1(G, \mathrm{Aut}_E(M_n(E))) \cong \mathrm{H}^1(G, \mathrm{PGL}_n(E)).$$

Recall that $(E, G, c) = \bigoplus_{\sigma \in G} Eu_\sigma$ where $u_\tau = c(\sigma, \tau)u_{\sigma\tau}$. For this course, we say that given $u_{\#1}, u_{\#1}, u_{\#1}$, we have that

$$c(\sigma, \tau)c(\sigma\tau, \gamma) = c(\sigma, \tau\gamma)\sigma(c(\tau, \gamma))$$

i.e., the two co-cycle condition. If we altered $u_{\#1}$ to $v_\sigma = b(\sigma)u_{\#1}$. This alteration does give an equivalence between the co-cycles by setting

$$c'(\sigma, \tau) = b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1}c(\sigma\tau), \tag{6.2.0.5}$$

which leads us to the notion of cohomologus. We say that $c \backsim c$ if and only if $\exists\, b$ that satisfies (6.2.0.5). The equivalence classes for a group $\mathrm{H}^2(G, E^\times) = \mathrm{Br}(E/F)$.

Thinking about H^2 Abstractly. Abstractly, we can think of H^2 by letting X be an Abelian group with G action. We set

$$Z^2(G, X) = \{c : G \times G \longrightarrow X \mid c(\sigma, \tau)c(\sigma\tau, \gamma) = c(\sigma, \tau\gamma)\sigma(c(\tau, \gamma))\}$$

We set $C^1(G,X)$ as the arrows from G to X. For a $b \in C^1(G,X)$, we say that the **boundary** is

$$\partial b(\sigma,\tau) = b(\sigma)\sigma(b(\tau))$$

Then we have

$$\mathrm{H}^2(G,X) = \frac{Z^2(G,X)}{B^2(G,X)}.$$

If X is a set with G action, then

$$\mathrm{H}^0(G,X) = Z^0(G,X) = \{x \in X : \sigma(x) = x\} = X^G.$$

The Long Exact Sequences.

Theorem 6.3. *Given a SES*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

of groups with G action. Taking cohomology gives a long exact sequence

$$\begin{tikzcd}
1 \arrow[r] & H^0(G,A) \arrow[r] & H^0(G,B) \arrow[r] & H^0(G,C) \arrow[dll, "\delta_0"] \\
 & H^1(G,A) \arrow[r] & H^1(G,B) \arrow[r] & H^1(G,C) \arrow[dll, "\delta_1"] \\
 & H^2(G,A) \arrow[r] & H^2(G,B) \arrow[r] & H^2(G,C)
\end{tikzcd}$$

and we stop at a certain point if $A \subset Z(B)$ or unless B is Abelian.

Remark 6.4. If X, Y, Z are pointed sets, we say that $X \xrightarrow{f} Y \xrightarrow{g} Z$ if and only if $\ker g = \operatorname{im} f$ as pointed sets.

What are the transgression maps when the groups are not Abelian? For δ_0, we can take this for granted. We want to look at δ_1. Assume that $A \subset Z(B)$ choose a $c \in Z^1(G,C)$. Pick some $b \in C^1(G,C)$, then $b(\sigma) \in B$ which happens to map to $c(\sigma) \in A$. We look that

$$\partial b(\sigma\tau) = b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1} \in C^2(G,B),$$

hence $\partial b(\sigma,\tau) = a(\sigma,\tau) \in C^2(G,A)$. We want to show that

$$a(\sigma,\tau)a(\sigma\tau,\gamma) = a(\sigma,\tau\gamma)\sigma(a(\tau,\gamma)).$$

Writing everything out with $a(\sigma,\tau) = b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1}$, we have prove this equality.

We want to specialize to the sequence

$$1 \longrightarrow E^\times \longrightarrow \mathrm{GL}(V \otimes E) \longrightarrow \mathrm{PGL}(V \otimes E) \longrightarrow 1.$$

Taking cohomology, we have

$$\mathrm{H}^1(G, \mathrm{PGL}(V \otimes E)) \longrightarrow \mathrm{H}^2(G, E^\times) = \mathrm{Br}(E/F).$$

Let's fix $n = [E : F] = \dim V$. We claim that under these assumptions, the above map is surjective. Pick $c \in Z^2(G, E^\times)$. Let e_σ be a basis for V induced by G. We define $b \in C^1(G, \mathrm{GL}(V \otimes E))$ via $b(\sigma)(e_\tau) = c(\sigma, \tau)e_{\sigma\tau}$. Note that

$$\begin{aligned}
b(\sigma)\sigma(b(\tau))(e_\gamma) &= b(\sigma)(\sigma b(\tau)\sigma^{-1}(e_\gamma) \\
&= b(\sigma)(\sigma(b(\tau)e_\gamma)) \\
&= b(\sigma)\sigma(c(\sigma,\gamma)e_\gamma) \\
&= b(\sigma)\sigma(c(\tau,\gamma))e_{\gamma\tau} \\
&= \sigma(c(\tau,\gamma))c(\sigma,\tau\gamma)e_{\sigma\tau\gamma} \\
&= c(\sigma,\tau)c(\sigma\tau,\gamma)e_{\sigma\tau\gamma} \\
&= c(\sigma,\tau)b(\sigma,\tau)e_\gamma \\
\Rightarrow b(\sigma)\sigma(b(\tau)) &= c(\sigma,\tau)b(\sigma,\tau) \\
\Rightarrow b(\sigma)\sigma(b(\tau))b(\sigma\tau)^{-1} &\backsim c(\sigma,\tau)
\end{aligned}$$

This implies that modulo $E^\times$, we have that

$$\overline{b(\sigma)}\,\overline{\sigma(b(\tau))} = \overline{b(\sigma\tau)},$$

hence $\partial b = c$ is a lift if $\bar{b} \in Z^1(G, \mathrm{PGL})$. What we have said is that if we tweak the standard Galois action on $\mathrm{End}_E(V \otimes E)$ by the $\bar{b} \in Z^1(G, \mathrm{PGL})$, then the image of $\bar{b}$ under δ_1 is$c$ from (E, G, c) via δ_1. We want to determine the algebra from $\bar{b}$. We want to take the invariants of the tweaked Galois action in order to recover this algebra, where we define the new action for $f \in \mathrm{End}_E(V \otimes E)$ as

$$\sigma(f) = \bar{b}(\sigma) \circ \sigma(f) = b(\sigma) \circ \sigma(f) \circ b(\sigma)^{-1}$$

where b is a representative of $\bar{b}$. We want to find elements f that are invariant under the tweaked action. Hence we can think of $f \mapsto \bar{b}\sigma(f) = b(\sigma) \circ \sigma(f) \circ b(\sigma)^{-1}$. The invariants are a CSA and we want to compare it with (E, G, c). We set

$$\mathrm{End}_E(V \otimes E)^{G,\bar{b}} = \{f : b(\sigma)\sigma(f) = fb(\sigma) \quad \forall \sigma \in G\}.$$

If $\sigma \in G$, define $y_\sigma \in \mathrm{End}_E(V \otimes E)$ via $y_\sigma(e_\tau) = c(\tau, \sigma)e_{\tau\sigma}$. If $x \in E$, we define $v_x \in \mathrm{End}_E(V \otimes E)$ via $v_x(e_\tau) = \tau(x)e_\tau$. We note that these are fixed. Indeed, let's look at $b(\sigma)\sigma(v_x) = v_x b(\sigma)$. Since we have defined these notions on a basis, it suffices to consider

$$\begin{aligned}
v_x b(\sigma)(e_\tau) &= v_x(c(\sigma,\tau)e_{\sigma\tau}) \\
&= c(\sigma,\tau)v_x(e_{\sigma\tau}) \\
&= c(\sigma,\tau)\sigma\tau(x)e_{\sigma\tau} \\
\Rightarrow b(\sigma)\sigma(v_x)(e_\tau) &= b(\sigma)(\sigma(v_x(\sigma^{-1}e_\tau))) \\
&= b(\sigma)(\sigma(v_x e_\tau)) \\
&= b(\sigma)(\sigma(\tau(x)e_\tau)) \\
&= b(\sigma)(\sigma\tau(x)e_\tau) \\
&= \sigma\tau(x)b(\sigma)e_\tau \\
&= \sigma\tau(x)c(\sigma,\tau)e_{\sigma\tau} \\
\therefore v_x b(\sigma)(e_\tau) &= b(\sigma)\sigma(v_x)(e_\tau).
\end{aligned}$$

Similary, we can show that y_σ, namely, $y_\tau b(\sigma) = b(\sigma)\sigma(y\tau)$. We can check this

$$\begin{aligned}
y_\tau b(\sigma)(e_\gamma) &= y_\tau(c(\sigma,\gamma)e_{\sigma\gamma}) \\
&= c(\sigma,\gamma)c(\sigma\gamma,\tau)e_{\sigma\gamma\tau} \\
\Rightarrow b(\sigma)\sigma(y_\tau)(e_\gamma) &= b(\sigma)(\sigma y_\tau \sigma^{-1}(e_\gamma)) \\
&= b(\sigma)(\sigma y_\tau(e_\gamma)) \\
&= b(\sigma)(\sigma(c(\gamma,\tau)e_{\gamma\tau})) \\
&= b(\sigma)(\sigma(c(\gamma,\tau))e_{\gamma\tau}) \\
&= \sigma(c(\gamma,\tau))b(\sigma)e_{\gamma\tau} \\
&= \sigma(c(\gamma,\tau))c(\sigma,\gamma\tau)e_{\sigma\gamma\tau} \\
\therefore y_\tau b(\sigma)(e_\gamma) &= b(\sigma)\sigma(y_\tau)(e_\gamma)
\end{aligned}$$

This allows us to define

$$\begin{aligned}
(E,G,c) &\longrightarrow (\mathrm{End}(V\otimes E))^{G,b} \\
xu_\sigma &\longmapsto v_x \circ y_\sigma
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathrm{H}^1(G,\mathrm{PGL}_n) &\longrightarrow \mathrm{H}^2(G,E^\times) \cong \mathrm{Br}(E/F) \\
A &\rightsquigarrow [A^{\mathrm{op}}]
\end{aligned}$$

Operations. What we want to do is: given two algebras given by a co-cycle of PGL, how do we add them? We will use that fact that

$$\mathrm{End}(V)\otimes \mathrm{End}(W) \cong \mathrm{End}(V\otimes W),$$

which makes more sense when we think about matrices. Given $a \in \mathrm{GL}(V)$ and $b \in \mathrm{GL}(V)$, then we define $a\otimes b \in \mathrm{GL}(V\otimes W)$ by $a\otimes b(v\otimes w) = a(v)\otimes b(w)$. This induces a homomorphism from $\mathrm{GL}(V)\times\mathrm{GL}(W) \longrightarrow \mathrm{GL}(V\otimes W)$ of groups. If $\bar{a}\in\mathrm{PGL}(V), \bar{b} \in \mathrm{PGL}(W)$, then we can similarly define $\bar{a}\otimes\bar{b} = \overline{a\otimes b} \in \mathrm{PGL}(V\otimes W)$, however, this is not a homomorphism since we are moding out by two different scalars so our map is not well-defined. If we think about

$$\mathrm{GL}(V) \xhookrightarrow{\Delta} \overbrace{\mathrm{GL}(V)\times\cdots\times\mathrm{GL}(V)}^{k \text{ times}} \longrightarrow \mathrm{GL}(V^{\otimes k})$$

then we do get an induced homomorphism, namely

$$\begin{aligned}
\mathrm{PGL}(V) &\longrightarrow \mathrm{PGL}(V^{\otimes k}) \\
\bar{a} &\longmapsto \overline{a\otimes a\otimes\cdots\otimes a} \\
[A] &\longmapsto k[A]
\end{aligned}$$

Given $\bar{a}\in Z^1(G,\mathrm{PGL}(V\otimes E)), \bar{b}\in Z^1(G,\mathrm{PGL}(W\otimes E))$, we can define $\bar{a}\otimes\bar{b}\in Z^1(G,\mathrm{PGL}(V\otimes W\otimes E))$ by $\bar{a}\otimes\bar{b}(\sigma) = \bar{a}(\sigma)\otimes\bar{b}(\sigma)$. We remark that $\bar{a}\otimes\bar{b}$ is a co-cycle and describes the action of the Galois group G on $A \otimes B$, where A corresponds to a and similarly for b. So

$$\begin{aligned} [A] &\leftrightarrow a \in \mathrm{H}^1(G, \mathrm{PGL}(V)) \\ [B] &\leftrightarrow b \in \mathrm{H}^1(G, \mathrm{PGL}(W)) \\ a \otimes b &\leftrightarrow [A \otimes B] \in \mathrm{H}^1(G, \mathrm{PGL}(V \otimes W)) \end{aligned}$$

Torsion in the Brauer Group. Suppose we have $b \in Z^1(G. \mathrm{PGL}(V \otimes E))$ and $V = W_1 \oplus W_2$ such that

$$b(\sigma) = \begin{pmatrix} b_1(\sigma) & 0 \\ 0 & b_2(\sigma) \end{pmatrix}$$

is given in some block form with $b_i(\sigma) \in \mathrm{GL}(W_i \otimes E)$. Then

$$\partial b(\sigma, \tau) = \begin{pmatrix} \partial b_1(\sigma, \tau) & 0 \\ 0 & \partial b_2(\sigma, \tau) \end{pmatrix}$$

in particular, since $\partial b(\sigma, \tau)$ is a scalar matrix, which means that for some $\lambda \in E^\times$, $\lambda = \partial b_i$ i.e., $\partial b_i = \partial b$. Then $\bar{b_i} \in \mathrm{H}^1(G, \mathrm{PGL}(W_i))$ represents something Brauer equivalent to b. Recall that the wedge power of the vector space V,

$$\bigwedge^k V \subset \bigotimes^k V \supset \text{ Rest }^k V.$$

Considering

$$\mathrm{PGL}(V) \longrightarrow \mathrm{PGL}\left(\bigotimes^k V\right) = \mathrm{PGL}\left(\bigwedge^k V \oplus \mathrm{Rest}^{\,k} V\right)$$

$$\begin{tikzcd} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \arrow[r, bend left, "\partial"] & \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \arrow[l, bend left, "\partial^{-1}"] \end{tikzcd}$$

i.e., the k^{th} power is replaced by something in $\mathrm{H}^1(G, \mathrm{PGL}(\bigwedge^k, V))$. If $n = \dim V$, then the n^{th} power represents $\mathrm{H}^1(G, \mathrm{PGL}(\bigwedge^n V)) = \mathrm{H}^1(G, \mathrm{PGL}(E)) = \{F\}$. We have torsion because $n\,[A] = 0$ implies that per $A|$ ind A.

7. Lecture (2/20): Primary Decomposition and some Involutions

Primary Decomposition. If M is some group, $m \in M$ and torsion, then

$$m = m_1 m_2 \dots m_r, \tag{7.0.0.6}$$

where m_i's commute with prime order and m_i has prime power order. This is equivalent to defining a homomorphism

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & M \\ 1 & \longmapsto & m \end{array}$$

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow M$$

where m is a n-torsion element where $n = \prod_{i=1}^s p_i^{r_i}$. The Chinese Remainder theorem says that the above map factors through $\mathbb{Z}/n\mathbb{Z} = \bigoplus_{i=1}^s \mathbb{Z}/p_i^{r_i}\mathbb{Z}$. If we consider a tuple $(a_1, \dots, a_s)$ in the direct sum and set b_i to be the tuple with 1 in the i^{th} component and 0 elsewhere, we can write $1 = \sum a_i b_i$. Hence

$$m = m^{\sum a_i b_i} = \prod_{i=1}^s m^{a_i b_i},$$

which implies that $|m^{a_i b_i}|$ divides $p_i^{r_i}$.

Proposition 7.1. *If D is a division algebra, then if we re-write $[D] = [D_1] + \cdots + [D_s]$ in terms of its primary components, then*

$$D = D_1 \otimes \cdots \otimes D_s.$$

Backtracking a Bit. If E/F is any field extension, then

$$\begin{array}{rcl} \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(E) \\ [A] & \longmapsto & [A \otimes E] \end{array}$$

is a group homomorphism since $(A \otimes B) \otimes E \cong (A \otimes E) \otimes_E (B \otimes E)$. Recall E splits A if and only if $[A] \in \ker(\mathrm{Br}(F) \to \mathrm{Br}(E)) = \mathrm{Br}(E/F)$.

Proposition 7.2. *If E/F is a splitting field for A, then there exists $B \backsim A$ such that E is a maximal sub-field of B.*[6]

Proof. We know that E acts on itself by left multiplication, so $E \hookrightarrow \mathrm{End}_F(F) = M_n(F)$. It is clear that $E \subset A \otimes M_n(F) \supset C_{A \otimes M_n(F)}(E)$. Then

$$C_{A \otimes M_n(F)}(E) \backsim A \otimes M_n(F) \otimes E \backsim A \otimes E,$$

[6] We simply want to prove the converse of Proposition 5.5.

and we note that $C_{A\otimes M_n(F)}(E) \cong M_{\deg A}(E) \supset M_{\deg A}(F)$. We want to compute

$$E \subset C_{A\otimes M_n(F)}(M_{\deg A}(F)).$$

We know that $C_{A\otimes M_n(F)}(M_{\deg A}(F))$ is a CSA equivalent to A and the degree is equal to n.

□

Corollary 7.3. *Every* CSA *is equivalent to a crossed product.*

Proof. Give D choose $L \subset D$ a maximal separable subfield. Let E/L be the Galois closure, then $E \otimes D = E \otimes_L (L \otimes_F D)$, so $D \backsim B$. Hence $E \subset B$ is a maximal sub-field, so $[D] \in \mathrm{Br}(E/F)$.

□

Alternate Characterization of Index.

Proposition 7.4. *Let A/F be a* CSA $/F$, *then*

$$\begin{aligned} \operatorname{ind} A &= \min\{[E:F] : E/F \text{ finite with } A \otimes E \text{ split}\} \\ &= \gcd\{[E:F] : E/F \text{ finite with } A \otimes E \text{ split}\} \\ &= \min\{[E:F] : E/F \text{ finite, separable with } A \otimes E \text{ split}\} \\ &= \gcd\{[E:F] : E/F \text{ finite, separable with } A \otimes E \text{ split}\} \end{aligned}$$

Proof. Suppose that E/F splits A. Without lose of generality, suppose that A is a division algebra. There must be some $B \backsim A$ with $E \subset B$ is a maximal sub-field by Proposition 7.2. We can conclude that $B \cong M_m(A)$, which implies that $[E:F] = m \cdot \deg A = m \operatorname{ind} A$. Therefore, $\operatorname{ind} A | [E:F]$ for every splitting field E/F. In other words, we cannot get any smaller, and the smallest size we can get is the size of the index. In particular, there exists maximal separable sub-field of any division algebra, so we have shown that above statements.

□

We want to relate the index and period a more precise manner. We note that if $[A] \in \mathrm{Br}(F)$ and E/F, then $\operatorname{per} A \otimes E | \operatorname{per} A$.

Lemma 7.5. *As with the period, we have that* $\operatorname{ind}(A \otimes E) | \operatorname{ind} A$.

Proof. Suppose that $K \subset A$ is a maximal separable sub-field and A a division algebra. Consider the diagram:

$$\begin{tikzcd} & KE \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash, "\operatorname{ind} A"'] & & E \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Now KE/E is a splitting field for A_E and the index $[KE : E]$ divides $\operatorname{ind} A$. Thus, we have that

$$\operatorname{ind}(A \otimes E) | [KE : E] | \operatorname{ind} A.$$

□

Therefore, the index and the period can drop when we tensor up, which can be further seen by Corollary 5.3.

Lemma 7.6. *If E/F is a finite field extension, then $\operatorname{ind} A | \operatorname{ind}(A \otimes E)[E : F]$.*

Proof. Let L/E split $A \otimes E$ with $[L : E] = \operatorname{ind}(A \otimes E)$, then L/F splits A. Hence $\operatorname{ind} A | [L : F] = [L : E][E : F] = \operatorname{ind}(A \otimes E)[E : F]$ by Proposition 7.4.

□

Corollary 7.7. *If E/F is relatively prime to $\operatorname{ind} A$, then $\operatorname{ind} A = \operatorname{ind}(A \otimes E)$.*

Lemma 7.8. *If E/F is separable and $[E : F]$ is relatively prime to $\deg A$, then $\operatorname{per}(A \otimes E) = \operatorname{per}(A)$.*

Proof. Omit for the time being.

□

Lemma 7.9. *Let A have period $n = p^k$, then as A has index a prime power.*

Proof. Let $F \hookrightarrow E \hookrightarrow L$ where L/F is a Galois closure and E/F a splitting field

$$\begin{tikzcd}
 & L & \\
 & E \arrow[u, dash] & K \arrow[ul, "p"'] \\
 & F \arrow[u, dash, "md"] \arrow[ur, dash, "\text{primes to } p"'] \arrow[uu, dash, bend left=60, "\text{Galois closure}"] &
\end{tikzcd}$$

Lemma 7.8 says that $\operatorname{ind}(A \otimes K) = \operatorname{ind} A$. Since L/K splits $A \otimes K$, we have that $\operatorname{ind}(A \otimes K)$ is a p -power.

□

From Proposition 7.1, the p_i-primary part D_i of D has index p_i-power. We know that if E/F is a maximal sub-field for D, then E/F splits D_i so $\operatorname{ind} D_i | [E : F]$ and it must be a p_i-power. Hence $\operatorname{ind} D = \prod_{i=1}^{s} p_i^{t_s}$ and $\operatorname{ind} D_i | p_i^{t_i}$.

If $\operatorname{ind} D_i < p_i^{t_i}$, then $\bigotimes D_i$ is smaller than the degree of D, which cannot happen since D has minimal degree in Brauer class. Thus, $\operatorname{ind} D_i = p_i^{t_i}$, which implies that D and the tensor product of the D_i's have the same degree; therefore,

$$D \cong \bigotimes_{i=1}^{s} D_i,$$

hence we have proved Proposition 7.1.

Given a vector space with a symmetric bi-linear form (V, b), so

$$b : V \otimes V \longrightarrow F,$$

where $b(v, w) = b(w, v)$. We want to say that this induces some structure on the matrix algebra. We will need the assumption that b is non-degenerate i.e., if

$$\begin{aligned} V &\longrightarrow V^\vee \\ v &\longmapsto b(v, \bullet) \end{aligned}$$

is an isomorphism. Recall that the standard inner product on F^n, then $b(v, w) = v^t w$, then if $b(Tv, w) = (Tv)^t w = v^t T^t w = b(v, T^t w)$, so the matrix moves through the form by the transpose operation. Similarly, given some general b on V/F and $T \in \mathrm{End}(V)$, then consider

$$w \longmapsto b(w, T(\bullet) \in V^\vee.$$

By non-degeneracy, $b(w, T(\bullet)) = b(v, \bullet)$ for some v.

Definition 7.10. An **involution** on a CSA A/F is a anti-homomorphism $\tau : A \cong A^{\mathrm{op}}$ with $\tau^2 = \mathrm{Id}_A$.

Definition 7.11. We define τ_b to be

$$\tau_b(T)(w) = v,$$

where v is as above. We have that $b(w, Tu) = b(\tau_b(T)w, u)$, so $\tau \in \mathrm{End}(V)$. We call τ_b the **adjoint involution of** b

Remark 7.12. One should check that τ_b is well-defined i.e., $\tau_b(T) \in \mathrm{End}(V)$, an anti-homomorphism, and has period 2.

Recall that given a bi-linear form, we can define an associated quadratic form by

$$q_b(x) = b(x, x) \tag{7.12.0.7}$$

Hence q_b is a degree 2 homogeneous polynomial. Given q a quadratic form, we can recover a symmetric bi-linear form

$$\tilde{b}_q(x, y) = q(x + y) - q(x) - q(y).$$

One can check that

$$\tilde{b}_{q_b} = 2b,$$

so in a field of characteristic not equal to 2, $b_q = \tilde{b}_q/2$. Thus we have a bijective correspondence between symmetric bi-linear forms and quadratic forms.

We want to answer the following questions in the upcoming lectures:

(1) To what extend is b (or q) determined by τ_b?

(2) Does every involution on $\mathrm{End}(V)$ come from bi-linear forms?[7]
(3) When do CSA's that are non-split have involutions?
(4) What structural properties of quadratic forms carry over to CSA's with involution?

The goal is to understand groups that are defined by algebraic equations. Suppose we have coordinates $x_1, \ldots, x_n$ on some vector space $V = F^n$. Let $G(f)$ be equal to the set of equations for some polynomial equations on V with the group law described by polynomial functions.

Example 7.12.1. Consider $\mathrm{GL}_n(F) = (\det \neq 0)$. Similarly, orthogonal matrices $\mathcal{O}_n(F) = \{TT^t = 1\}$.

We will look at connected groups with no subgroups that are normal, connected, and defined by equations $f_1, \ldots, f_n = 0$; we will refer to these are **simple** groups. Note that $\mathrm{GL}_n(F)$ is not simple since the scalar diagonal matrices are normal and connected, however, $\mathrm{SL}_n(F)$ is simple. The orthogonal group fails to be simple since it has two components, but the special orthogonal $\mathrm{SO}_n(F)$ is simple when characteristic is not 2.

$$\begin{tikzcd}
A_n & B_n & C_n & D_n & G_2 & F_4 & E_6 \\
\mathrm{SL}_{n+1}, \mathrm{SU} \arrow[u] & \mathrm{SO}_{n+1} \arrow[u] & \mathrm{Sp}_{2n} \arrow[u] & \mathrm{SO}_{2n} \arrow[u] & \bullet \arrow[u] & \bullet \arrow[u] & \bullet \arrow[u]
\end{tikzcd}$$

The punchline is that simple linear algebraic groups of types A, B, C, D except D_4 come from CSA's with involutions. In answering (1) above, we will see that $\tau_b = \tau_b' \iff b' = \lambda b$ for some $\lambda \in F$. Notice that (3) is trivial for split CSA's since we can just take the transpose. For the non-split case, if τ is an involution on A, then since it is an anti-automorphism, $\tau : A \cong A^{\mathrm{op}}$, hence $A \otimes A \cong A \otimes A^{\mathrm{op}} \cong 1$, which is split. Thus, $\mathrm{per}[A] = 2$ or 1. Conversely, if per $A|2$, then there exists involutions. We will prove this using Galois Descent (5).

8. Lecture (2/27): Involutions and other Anti-automorphisms

Bi-linear forms on a vector space. Let V be a finite dimensional vector space.

[7]We can show that this is not necessarily true since we will need skew-symmetric forms.

Definition 8.1. A **bi-linear form** b is a function $b : V \times V \to F$ that is linear in each variable i.e., b factors through

$$\begin{tikzcd} V \times V \arrow[rr] \arrow[dr] & & F \\ & V \otimes V \arrow[ur] & \end{tikzcd}$$

Definition 8.2. b is **symmetric** if $b(v, w) = b(w, v)$ i.e., b factors through

$$\begin{tikzcd} V \times V \arrow[rr] \arrow[dr] & & F \\ & V \otimes V / \langle v \otimes w - w \otimes w \rangle \arrow[ur] & \end{tikzcd}$$

Hence b is symmetric if and only if $b \in (\mathrm{Sym}^2 B)^\times$.

Definition 8.3. b is **left-nondegenerate** if

$$\begin{array}{rcl} V & \longrightarrow & V^\times \\ v & \longmapsto & b(v, \bullet) \end{array}$$

is injective, equivalently isomorphic. Similarly, for **right-nondegenerate**.

Definition 8.4. (V, b), (V', b') is **isometric** if there exists $\phi : V \cong V'$ such that $b(v, w) = b'(\phi(v), \phi(w))$.

Definition 8.5. b, b' are **right-isometric** if there exists $\phi : V \cong V$ such that $b(v, w) = b'(v, \phi(w))$. Similarly, for **left-isometric**.

Example 8.5.1. Consider the inner product, $\langle \bullet \rangle$ on F^n where $\langle x, y \rangle = x^t y$. This is both left and right non-degenerate.

Lemma 8.6. *If b,b' are both left non-degenerate, then they are left isometric.*

Proof. For all x, $b'(x, \bullet) \in V^\times$ and can be mapped to $b(\phi x, \bullet)$ for some ϕx. We can check that ϕ is a linear map. Hence $b'(x, y) = b(\phi x, y)$ and similarly, $b(x, y) = b'(\psi x, y)$. Thus,

$$\begin{array}{rcl} b(x, y) & = & b'(\psi x, y) \\ & = & b(\phi \psi x, y) \\ \Rightarrow x & = & \phi \psi x \end{array}$$

So, $\phi \psi = \mathrm{Id}$, so ϕ is an isomorphism.

□

In particular, any left non-degenerate b

$$b(x,y) = \langle \phi x, y \rangle = (M^t x)^t y = x^t M y \tag{8.6.0.1}$$

where $\phi = M^t$ for some matrix. We call this matrix M the **Gram matrix** for b. Therefore, b left non-degenerate implies that for all x, $x^t M \neq 0$ if and only if M non-singular if and only if b is right non-degenerate. Thus,

$$\boxed{\text{non-degenerate = right non-degenerate = left non-degenerate}}$$

Given b bi-linear on V, we can form σ_b^L, σ_b^R, the **left and right adjoint anti automorphisms**. Here's the idea, we want to define

$$b(x, Ty) = b(\sigma_b^L(T)x, y) \quad \text{and} \quad b(Tx, y) = b(x, \sigma_b^R(T)y).$$

To define this explicitly, we look at

$$b(x, T(\bullet)) = b(\sigma_b^L(T)x, \bullet)$$

It is easy to check that

$$\begin{aligned} \sigma_b^L(T_1 + T_2) &= \sigma_b^L(T_1) + \sigma_b^L(T_2) \\ \sigma_b^L(T_1 T_2) &= \sigma_b^L(T_2)\sigma_b^L(T_1) \\ \sigma_b^R \circ \sigma_b^L &= \sigma_b^R \circ \sigma_b^L = \mathrm{End}(V) \end{aligned}$$

Given b, b' both non-degenerate, we know that $b'(x,y) = b(x, uy)$. We want to relate the adjoint automorphisms:

$$\begin{aligned} b'(x, Ty) &= b'(\sigma_{b'}^L(T)x, y) \\ &= b(\sigma_{b'}^L(Tx), uy) \\ &= b(\sigma_b^L(u)\sigma_{b'}^L(T)x, y) \\ \Rightarrow b(x, uTy) &= b(\sigma_b^L(u)\sigma_{b'}^L(T)x, y) \\ b(\sigma_b^L(uT)x, y) &= b(\sigma_b^L(u)\sigma_{b'}^L(T)x, y) \\ \Rightarrow \sigma_b^L(uT) &= \sigma_b^L(u)\sigma_{b'}^L(T) \\ \Rightarrow uT &= \sigma_b^{L^{-1}}(\sigma_b^L(u)\sigma_{b'}^L(T)) \\ &= \sigma_b^{L^{-1}}(\sigma_{b'}^L(T))u \\ \mathrm{inn}_u(T) &= uTu^{-1} \\ \mathrm{inn}_u(T) &= \sigma_b^{L^{-1}}(\sigma_{b'}^L(T)) \end{aligned}$$

Hence we conclude by stating that

$$(\sigma_{b'}^L) = \sigma_b^L \circ \mathrm{inn}_u \quad \text{where}\, b'(x,y) = b(x, uy). \tag{8.6.0.2}$$

We have shown a map between

$$\begin{array}{rcl}\{\text{Non-degenerate bi-linear forms}\} & \longrightarrow & \{\text{Anti-automorphisms}\} \\ b(x,y) = x^t My & \longmapsto & b'(x,y) = b(x,uy) = x^t Muy\end{array}$$

If $\sigma_b = \sigma_{b'}$, then by the above we have that $\mathrm{inn}_M = \mathrm{inn}_{Mu}$ if and only if $\mathrm{inn}_u = \mathrm{Id}$ if and only if $u \in Z(\mathrm{End}(V)) = f$. Thus, $\sigma_b = \sigma_{b'}$ if and only if there exists some λ such that for every y $b'(x,y) = b(x,\lambda y) = \lambda b(x,y)$.

Definition 8.7. b, b' are **homethetic** if $b = \lambda b'$ for some $\lambda \in F^\times$. Hence

$$\{\text{Non-degenerate, homethetic class of bi-linear forms}\} \quad \leftrightarrow \quad \{\text{Anti-automorphims}\}$$

Given any σ in the latter group, then $t \circ \sigma \in \mathrm{Aut}(\mathrm{End}(V))$ there exists a M such that $t \circ \sigma = \mathrm{inn}_M$ so $\sigma = t \circ \mathrm{inn}_M$, thus σ is adjoint to b so $b(x,y) = x^t My$.

Involutions.

Definition 8.8. A bilinear form b is

(1) **symmetric** if $b(x,y) = b(y,x)$
(2) **skew** if $b(x,y) = -b(y,x)$
(3) **alternating** if $b(x,x) = 0$ for all x.

In each case, we have $b(x,y) = \varepsilon b(y,x)$ where $\varepsilon^2 = 1$; we will refer to this as ε **- symmetric**. If b satisfies one of the above conditions, σ its adjoint then

$$\begin{aligned} b(x,Ty) &= b(\sigma Tx, y) = \varepsilon b(y, \sigma Tx) \\ &= \varepsilon b(\sigma^2 tY, x) = \varepsilon^2 (b(x, \sigma^2 Ty)) \\ &= b(x, \sigma^2 Ty) \end{aligned}$$

Definition 8.9. A is a ring and $\sigma : A \to A$ an anti-autormorphism is an **involution** of A is $\sigma^2 = \mathrm{Id}$. If A is a CSA then we say that σ is of the **first kind** if $\sigma_{|Z(A)} = \mathrm{Id}$.

If not, then $\sigma(F) \subset F$, then $\sigma(\lambda)a = \sigma(\lambda)\sigma^2 a = \sigma(\sigma(a)\lambda)$. So $\sigma_{|F}$ is an order 2 non-trivial automorphim, then F/F^σ is a Galois group with group $C_2 = \langle \sigma_{|F} \rangle$. We will call this an involution of the **second kind**.

Definition 8.10. A matrix $T \in \mathrm{M}_n(F)$ is **symmetrized** if $T = S + S^T$ for some S and **skew-symmetrized** if $T = S - S^T$ for some S.

Example 8.10.1. A symmetric matrix is

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

A symmetrized matrix is

$$\begin{pmatrix} 2a & b \\ b & 2a \end{pmatrix}$$

A natural question is do all involutions come as adjoints to symmetric or skew symmetric bi-linear forms? The answer is yes and we will see why shortly. If $\sigma \in \mathrm{Inv}_f(\mathrm{End}(V))$ is of the first kind, then $\sigma = \sigma_b$ for some bi-linear b. By (8.6.0.2), $\sigma = \sigma_b = t \circ \mathrm{inn}_M$. Thus,

$$\begin{aligned} \mathrm{Id} &= \sigma^2 = t \circ \mathrm{inn}_M \circ t \circ \mathrm{inn}_M \\ \sigma^2(T) &= (M(MTM^{-1})^t M^{-1})^t \\ &= (M(M^{t^{-1}} T^t M^t) M^{-1})^t \\ &= (M^{t^{-1}}) MTM^{-1} M^t \\ &= \mathrm{inn}_{(M^{t^{-1}} M} T \end{aligned}$$

Then $M^{t^{-1}} M \in F^\times$, so $M^t = \varepsilon M$. Hence $M = M^{t^t} = (\varepsilon M)^t = \varepsilon^2 M = M$, so we have answered our above question.

Lemma 8.11. *Suppose M is the Gram matrix for some bi-linear form b, then*

(1) b is symmetric if and only if M is symmetric,
(2) b is skew if and only if M is skew,
(3) b is alternating if and only if M is skew-symmetrized.

We will need the following result:

Lemma 8.12. *M is skew'd if and only if M is skew and diagonal entries all 0.*

Proof. The only non-obvious part is (3). If M is skew'd, then b is alternating. Lemma 8.12 shows that it is clear that b is alternating.

□

Definition 8.13. If A is a CSA $/F$, σ an involution on A of the first kind, we say that σ is **orthogonal** if $\sigma_{\overline{F}}$ = adjoint for symmetric and **sympletic** if $\sigma_{\overline{F}}$ = adjoint for skew.

Gram/Schmitt and Darboux.

Lemma 8.14. *If ω is non-degenerate, alternating, then we can write*

$$V = \langle x_1, y_1 \rangle \perp \langle x_2, y_2 \rangle \perp \cdots \perp \langle x_n, y_n \rangle,$$

where $W_1 \perp W_2 = W_1 \otimes W_2$ and $\omega(w_1, w_2) = 0$ for all $w_i \in W_i$ and $\omega(x_i, y_i) = 1$.

Proof. Proceed by induction on $\dim V$. Choose $x_1 \in V \setminus \{0\}$ and non-degenerate y_1 such that $\omega(x_1, y_1) = 1 \neq 0$. Then $\langle x, y \rangle \cap \langle x, y \rangle^\perp = 0$. By induction hypothesis, we are done.

□

Proposition 8.15. *If b is ε-symmetric, then we can write*

$$V = W \perp V^{\text{alt}}$$

where V^{alt} is alternating and $W = \langle z_1 \rangle \perp \langle z_2 \rangle \perp \cdots \langle z_n \rangle$ and $b(z_i, z_i) = a_i \neq 0$.

Proof. It is standard to write $W = \langle a_1, \ldots, a_n \rangle$. We induce on the dimension of V. Either V is alternating or there exists z_1 such that $b(z_1, z_1) = a_1 \neq 0$, so $\langle z_1 \rangle \cap \langle z_1 \rangle^{\perp} = 0$, so $V = \langle z_1 \rangle \perp \langle z_1 \rangle^{\perp}$.

$\square$

If ω is alternating, then after a change of basis it looks like the above perp decomposition. Moreover, the Gram matrix is of the form

$$\Omega = \begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & 1 & & & \\ & -1 & 0 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & 0 & 1 \\ & & & & -1 & 0 \end{pmatrix}$$

We remark that $\det M = 1$.

The Pfaffian. Classically, the Pfaffian is the square root of the determinant. Let M be a skew symmetrized invertible matrix which corresponds to an alternating form ω and $M = \Omega$ after a change of basis i.e.,

$$\omega(xm, y) = (\phi x)^t \Omega \phi y.$$

For notation's sake, let A^t be the matrix for ϕ, then we can write the above as follows:

$$w(x, y) = x^t A^t \Omega A x$$

so $M = A^t \Omega A$. Moreover, $\det(M) = \det(A)^2$.

Definition 8.16. We define the **Pfaffian** of M as $\mathrm{Pf}(M) = \det(A)$ i.e., $\mathrm{Pf}(M)^2 = \det M$. General non-sense implies that $\mathrm{Pf}(M)$ is a rational function in the entries of M. Moreover, if $\mathrm{Pf}(M)^2$ is a polynomial function, then $\mathrm{Pf}(M)$ is a polynomial.

If (V, ω) is a space with an alternating form, we want to define something symmetrized for (End, ω) i.e., a $T = S + \sigma_\omega(S)$. Write $\omega(x, y) = x^t v y$ then $v^t = -v$ and $\sigma_\omega = \mathrm{inn}_v \circ t$. Then

$$\begin{aligned} T &= S + \sigma_\omega(S) = S + \mathrm{inn}_V(S^t) \\ &= S + VS^tV^{-1} = (SV + VS^t)V^{-1} \\ &= (SV - (SV)^t)V^{-1} \end{aligned}$$

The characteristic polynomial of T,

$$\begin{aligned}\chi_T(x) &= \det(x - T) = \det(x - (SV - (SV)^t)V^{-1}) \\ &= \det(XV - (SV - (SV)^t))(\det V)^{-1} \\ &= \mathrm{Pf}(XV - (SV - (SV)^t))^2(\mathrm{Pf}(V)^2)^{-1}\end{aligned}$$

Since $\chi_T(x)$ is a square of a polynomial, we can take a square root.

Definition 8.17. The **Pfaffian characteristic polynomial** is define by the monic square root above. The **Pfaffian norm** is the last coefficient and the **Pfaffian trace** is the second coefficient.

Theorem 8.18 (Pfaffian-Cayley-Hamilton). *If T is symmetrized for ω an alternating form, then* $\mathrm{Pf}\,\chi_T(x) = 0$*.*

Given a degree five algebra A over F. Given $E \subset A$ maximal, how Galois is it? More precisely, consider the Galois closure, the Galois group must be a transitive subgroup of S_5. If A is of degree 5, does there exists $E \subset A$ maximal such that the Galois closure does not satisfy $G \cong S_5$.

Theorem 8.19 (Rowen). *If* $\deg A = 8$ *and* $\mathrm{per}\,A|2$*, then there exists a $C_2 \times C_2 \times C_2$ Galois maximal subgroup.*

If $\mathrm{per}\,A = 2$ and $\mathrm{ind} = 2^n$, then there exists a half maximal sub-field where $F \hookrightarrow L \hookrightarrow E$ and $[E : L] = 2$. Characteristics of the algebras in terms of index, period, and degrees can provide interesting results involving the arithmetic of fields.

Transitioning to Algebras.

Lemma 8.20. *Let (V, b) is a space with bi-linear form and* $\dim V = n$*. Then b is symmetric if and only if* $\mathrm{Sym}(\mathrm{End}(V), \sigma_b)$ *has dimension $n(n+1)/2$. b is skew if and only if* $\mathrm{Skw}(\mathrm{End}(V), \sigma_b)$ *has dimension $n(n+1)/2$.*

Proof. Consider the isomorphism

$$\begin{array}{ccc}\mathrm{Sym}(\mathrm{M}_n(F), t) & \simeq & \mathrm{Sym}^{\varepsilon}(A, \sigma) \\ TM^{-1} & \longleftarrow & T,\end{array}$$

where M is the Gram matrix for b. ∎

Theorem 8.21 (Existence of Involutions). *Given a* CSA $/F$ *A with period 2, there exists $\sigma \in$* $\mathrm{Inv}_f(A)$ *that is orthogonal.*

Proof. Since $A \cong \mathrm{H}^1(F, \mathrm{PGL}(V))$. The action of $\mathrm{GL}(V)$ on $(\mathrm{Sym}^2 V)^\times$ gives rise to a map $\mathrm{GL} \to \mathrm{GL}(\mathrm{Sym}^2 V)^\times$. Moreover,

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
F^\times \arrow[r, "x \longmapsto x^{-2}"] \arrow[d] & F^\times \arrow[d] \\
\mathrm{GL}(V) \arrow[r] \arrow[d] & \mathrm{GL}((\mathrm{Sym}^2(V))^\times) \arrow[d] \\
\mathrm{PGL}(V) \arrow[r] \arrow[d] & \mathrm{PGL}((\mathrm{Sym}^2(V))^\times) \arrow[d] \\
0 & 0
\end{tikzcd}$$

Taking cohomology of the columns gives the diagram

$$\begin{tikzcd}
\mathrm{H}^1(G, \mathrm{GL}(V \otimes E)) \arrow[r] \arrow[d] & \mathrm{H}^1(G, \mathrm{PGL}(V \otimes)) = [A] \arrow[r] \arrow[d] & \mathrm{H}^2(G, F^\times) \arrow[d, "\cdot(-2)"] \\
\mathrm{H}^1(\mathrm{GL}(\mathrm{Sym}^2(V \otimes E)^\times)) \arrow[r] & \mathrm{H}^1(\mathrm{PGL}(\mathrm{Sym}^2(V \otimes E)^\times)) \arrow[r] & \mathrm{H}^2(G, F^\times)
\end{tikzcd}$$

$\square$