Lecture 14
Representation Fields: A counterexample (proof of Theorem 1)

Patricio Quiroz

Wesleyan University 07.17.2014

We are using the following notation:

- A is a K-CSA, where K is a number field.
- $G = A^*/K^* = Aut(A)$.
- $\mathfrak{H} \subset A$ is an order contained in a maximal order $\mathfrak{D} \subset A$.
- $X = \{u \in G_{\mathbb{A}} |\ \mathfrak{H} \subset u\mathfrak{D}u^{-1}\}$ is the set of local generators for $\mathfrak{H}$ over $\mathfrak{D}$.
- $\Sigma = \Sigma_A$ is the spinor class field for maximal orders of A.

We will prove today:

Theorem 1. *Let A be a CSA of dimension at least 3^2 over a number field K. The representation field exists for every order $\mathfrak{H}$ in A if and only if the extension Σ/K has exponent 2.*

Before starting the proof let's remember what we have done so far. We established that Σ classifies maximal orders in the sense that, if $\mathbb{O}$ is the set of maximal orders of A, we have a map $\rho : \mathbb{O} \times \mathbb{O} \to Gal(\Sigma/K)$ given by $\rho(\mathfrak{D}, \mathfrak{D}') = [N_{\mathbb{A}}(\sigma), \Sigma/K]$ for $\sigma \in A^*_{\mathbb{A}}$ such that $\mathfrak{D}' = \sigma\mathfrak{D}\sigma^{-1}$, which satisfies the following properties:

1. $\rho(\mathfrak{D}, \mathfrak{D}') = id_\Sigma \Leftrightarrow \mathfrak{D}$ and $\mathfrak{D}'$ are in the same spinor genus (in the same conjugacy class under Eichler's condition).
2. $\rho(\mathfrak{D}, \mathfrak{D}') = \rho(\mathfrak{D}, \mathfrak{D}'')\rho(\mathfrak{D}'', \mathfrak{D}')$ for all $\mathfrak{D}, \mathfrak{D}'\mathfrak{D}'' \in \mathbb{O}$.

   Moreover, for an order $\mathfrak{H} \subset \mathfrak{D}$, we know that if the set

   $$\{\rho(\mathfrak{D}, \mathfrak{D}')|\ \mathfrak{H} \text{ is contained in a conjugate of } \mathfrak{D}'\} \subset Gal(\Sigma/K)$$

   is a subgroup, then it corresponds (via CFT) with a field $F = F(\mathfrak{H}) \subset \Sigma$ (the representation field) such that

3. $\mathfrak{H} \subset \mathfrak{D} \cap \mathfrak{D}' \Rightarrow \rho(\mathfrak{D}, \mathfrak{D}')|_F = id_F$ and

4. $\rho(\mathfrak{D}, \mathfrak{D}') = id_F \Rightarrow \mathfrak{H}$ is contained in a conjugate of $\mathfrak{D}'$.

Remember also that an Eichler order is the intersection of two maximal orders and that a local Eichler order of type $(t_1, ..., t_f)$ is any conjugate to

$$\mathfrak{D}_\mathfrak{p} \cap d\mathfrak{D}_\mathfrak{p} d^{-1} = \begin{pmatrix} \mathcal{O}_D & \mathcal{O}_D & \cdots & \mathcal{O}_D \\ u^{t_2-t_1}\mathcal{O}_D & \mathcal{O}_D & \cdots & \mathcal{O}_D \\ \vdots & \vdots & \ddots & \vdots \\ u^{t_f-t_1}\mathcal{O}_D & u^{t_f-t_2}\mathcal{O}_D & \cdots & \mathcal{O}_D \end{pmatrix},$$

with $d = diag(u^{t_1}, ..., u^{t_f}), t_1 \leq \cdots \leq t_f$, for a uniformazing parameter u of the local division CSA D, where $A_\mathfrak{p} = \mathbb{M}_f(D)$ and $\mathfrak{D}_\mathfrak{p} = \mathbb{M}_f(\mathcal{O}_D)$ ($\mathcal{O}_D$ the unique maximal order of D). We denote by $[t_1, ..., t_f]_\mathfrak{p}$ the set of local Eichler orders of type $(t_1, ..., t_f)$.

We proved that $[t_1, ..., t_f]_\mathfrak{p} = [t_1 + t, ..., t_f + t]_\mathfrak{p}$ for any integer t. We also proved the following result.

Lemma. If a local Eichler order of type $(t_1, ..., t_f)$ embeds into a local Eichler order of type $(s_1, ..., s_f)$, then

$$\sum_{i<j}(s_j - s_i) \leq \sum_{i<j}(t_j - t_i),$$

with equality if and only if both orders coincide.

Now we are ready to prove the theorem...

Proof. *(necessity)* Assume that the extension Σ/K is not of exponent 2. In other words, there exists an element $\sigma \in Gal(\Sigma/K)$ of order $q > 2$. We will construct an Eichler order for which the representation field does not exist. Let $\mathfrak{p}$ be a finite place of K such that the Frobenius automorphism at $\mathfrak{p}$ is σ (the Artin map is surjective). Now let $\mathfrak{H} = \mathfrak{D} \cap \mathfrak{D}'$, where $\mathfrak{D} = \mathfrak{D}'$ except at $\mathfrak{p}$. We identify $\mathfrak{D}_\mathfrak{p} = \mathbb{M}_f(\mathcal{O}_D)$ as before and set $\mathfrak{D}'_\mathfrak{p} = d\mathfrak{D}_\mathfrak{p} d^{-1}$, where $d = diag(1, ..., 1, u)$ for a uniformizing parameter u of D, so that $\mathfrak{H}_\mathfrak{p}$ is of type $(0, ..., 0, 1)$. Recall $\sigma^f = id$ by definition of Σ. By definition, $\mathfrak{H} \subset \mathfrak{D}$, $\mathfrak{H} \subset \mathfrak{D}'$ and $\rho(\mathfrak{D}, \mathfrak{D}') = \sigma$. It suffices to see that $\mathfrak{H}$ cannot be contained in an order $\mathfrak{D}''$ such that $\rho(\mathfrak{D}, \mathfrak{D}'') = \sigma^{-1}$. Suppose this is the case. Certainly $\mathfrak{D}''$ coincides with $\mathfrak{D}$ outside $\mathfrak{p}$, since $\mathfrak{H}$ is maximal there. Set $\mathfrak{D}''_\mathfrak{p} = g\mathfrak{D}_\mathfrak{p} g^{-1}$, where $g = p \cdot \mathrm{diag}(u^{s_1}, ..., u^{s_f}) \cdot q$, for some $p, q \in \mathfrak{D}^*_\mathfrak{p}$ and $s_1 \leq \cdots \leq s_f$. The order $\mathfrak{H}$ is contained in $\mathfrak{H}'' = \mathfrak{D} \cap \mathfrak{D}''$. Note that $\mathfrak{H}_\mathfrak{p}$ is of type

$(0,...,0,1)$ and $\mathfrak{H}''_{\mathfrak{p}}$ is of type $(s_1,...,s_f)$, where[1]

$$\sum_{i<j}(s_j-s_i)=\sum_{i=1}^{f-1}i(f-i)(s_{i+1}-s_i)\geq f-1.$$

It follows from the lemma above that equality must hold, whence $\mathfrak{H}=\mathfrak{H}''$ and we have either $(s_1,...,s_f)=(0,...,0,1)$ or $(s_1,...,s_f)=(0,1,...,1)$. Since

$$\sigma\neq\sigma^{-1}=\rho(\mathfrak{D},\mathfrak{D}'')=[\mathfrak{p},\Sigma/K]^{\sum_{i=1}^{f}s_i},$$

it follows that $(s_1,...,s_f)=(0,1,...,1)$.

Next consider the image $\mathbb{K}$ of $\mathfrak{H}$ in $\mathfrak{D}_{\mathfrak{p}}/u\mathfrak{D}_{\mathfrak{p}}$. By definition of $\mathfrak{D}_{\mathfrak{p}}$ and $\mathfrak{D}'_{\mathfrak{p}}$ we have that $\mathbb{K}$ is the algebra of matrices in $\mathbb{M}_f(\mathcal{O}_D/u\mathcal{O}_D)$ of the form[2]

$$\begin{pmatrix} B & w \\ 0 & a \end{pmatrix},$$

where B is a block of $f-1$ rows and $f-1$ columns. On the other hand, since $\mathfrak{H}=\mathfrak{H}''=\mathfrak{D}\cap\mathfrak{D}''$, the algebra $\mathbb{K}$ is conjugate to the algebra of matrices of the form[3]

$$\begin{pmatrix} a & v \\ 0 & B \end{pmatrix},$$

where B is a block of $(f-1)\times(f-1)$. When $f\geq ord(\sigma)>2$, these two algebras are not isomorphic, since only the first one has an element P that satisfies the following conditions:

---

[1]
$$\sum_{i<j}(s_j-s_i)=\sum_{j=1}^{f-1}\sum_{i=1}^{j-1}(s_j-s_i)=\sum_{j=1}^{f-1}\sum_{i=1}^{j-1}\sum_{l=i}^{j-1}(s_{l+1}-s_l)=\sum_{i\leq l<j}(s_{l+1}-s_l)=\sum_{l=1}^{j-1}l(f-l)(s_{l+1}-s_l).$$

[2]Since
$$\mathfrak{H}_{\mathfrak{p}}=\mathfrak{D}_{\mathfrak{p}}\cap d\mathfrak{D}_{\mathfrak{p}}d^{-1}=\begin{pmatrix} \mathcal{O}_D & \cdots & \mathcal{O}_D & \mathcal{O}_D \\ \vdots & \ddots & \vdots & \vdots \\ \mathcal{O}_D & \cdots & \mathcal{O}_D & \mathcal{O}_D \\ u\mathcal{O}_D & \cdots & u\mathcal{O}_D & \mathcal{O}_D \end{pmatrix}.$$

[3]Since
$$p\mathfrak{H}''_{\mathfrak{p}}p^{-1}=\mathfrak{D}_{\mathfrak{p}}\cap d_0\mathfrak{D}_{\mathfrak{p}}d_0^{-1}=\begin{pmatrix} \mathcal{O}_D & \mathcal{O}_D & \cdots & \mathcal{O}_D \\ u\mathcal{O}_D & \mathcal{O}_D & \cdots & \mathcal{O}_D \\ \vdots & \vdots & \ddots & \vdots \\ u\mathcal{O}_D & \mathcal{O}_D & \cdots & \mathcal{O}_D \end{pmatrix},$$
where $d_0=diag(u^{s_1},...,u^{s_f})$.

1. $P^2 = P$.
2. $\mathbb{K}P$ is an ideal of dimension 1 over the residue field.

In fact, any P with the prescribed conditions must satisfy[4] $P = E_{ii}$ (where E_{ij} are the elements of the canonical basis of a matrix algebra). It is easy to check that the element $P = diag(1, 0, ..., 0)$ in the second algebra satisfies the conditions above, but there are no elements in the first algebra satisfying them.

Remark. If the order of σ is bigger than 3, the equality $\rho(\mathfrak{D}, \mathfrak{D}'') = [\mathfrak{p}, \Sigma/K]^{\sum_{i=1}^{f} s_i}$ together with the condition $(s_1, ..., s_f) = (0, ..., 0, 1)$ or $(s_1, ..., s_f) = (0, 1, ..., 1)$ tell us that $\rho(\mathfrak{D}, \mathfrak{D}'') \in \{id, \sigma, \sigma^{-1}\}$ and then σ^2 cannot be reached.

Now we prove the sufficiency. We will prove that if the exponent of Σ/K is 2, then the image $[N(X), \Sigma/K]$ of the set X of local generators is a subgroup of $Gal(\Sigma/K)$.

Let $\sigma, \tau \in X$. We define $\lambda \in A_{\mathbb{A}}$ as follows:

- if the valuations $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\sigma_{\mathfrak{p}})]$ and $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\tau_{\mathfrak{p}})]$ have the same parity, we define $\lambda_{\mathfrak{p}} = 1$.
- if $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\sigma_{\mathfrak{p}})]$ is odd and $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\tau_{\mathfrak{p}})]$ is even, we define $\lambda_{\mathfrak{p}} = \sigma_{\mathfrak{p}}$.
- if $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\sigma_{\mathfrak{p}})]$ is even and $v_{\mathfrak{p}}[N_{\mathfrak{p}}(\tau_{\mathfrak{p}})]$ is odd, we define $\lambda_{\mathfrak{p}} = \tau_{\mathfrak{p}}$.
- if $\mathfrak{p}$ is archimedean, we define $\lambda_{\mathfrak{p}} = \sigma_{\mathfrak{p}}\tau_{\mathfrak{p}}$.

Since the property defining a local generator is local, the element λ is a generator. On the other hand

$$N(\lambda) = N(\sigma)N(\tau)cr^2,$$

for some ideles $r \in J_K$ and $c \in J_{K,\infty}^+$, where $J_{K,\infty}^+$ is the subgroup of ideles that are positive at real places and units at the finite places (see lecture 6). Since the extension Σ/K is unramified, the subgroup $J_{K,\infty}^+$ has trivial image under the Artin map. By the hypothesis on $Gal(\Sigma/K)$, also r^2 has trivial image.

[4] If P satisfies the second condition, then P has to have only one coefficient different from zero. If P has only one non-zero entry, then $P^2 = P$ implies $P = E_{ii}$.