Lecture 25: Skew-fields, II.

1) Structure of skew-fields.

2) Finite skew-fields.

3) Bonus: Brauer group

Ref: [V], Sec 11.6.

1.0) Recap

Suppose $\mathbb{F}$ is a field and S is a finite dimensional central $\mathbb{F}$-algebra that is a skew-field. Our goal is to prove:

Theorem: Suppose $\operatorname{char} \mathbb{F}=0$. Then the following claims hold:

1) $\forall$ maximal subfields $K^1, K^2 \subset S$, have $\dim_{\mathbb{F}} K^1 = \dim_{\mathbb{F}} K^2$.

2) if the dimension in 1) is n, then $\dim_{\mathbb{F}} S = n^2$.

3) Let K^1, K^2 be maximal subfields and $\tau: K^1 \xrightarrow{\sim} K^2$ be an $\mathbb{F}$-linear isomorphism. Then $\exists\, s \in S \setminus \{0\} \mid \tau(x) = sxs^{-1}\ \forall x \in K^1$.

1.1) Approach to proof.

To prove the theorem we'll use the base change to the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ (meaning that $\mathbb{F} \subset \overline{\mathbb{F}}$, $\overline{\mathbb{F}}$ is algebraically closed, and any element $x \in \overline{\mathbb{F}}$ is algebraic over $\mathbb{F}$).

The proof is in two big steps. Recall that for an $\mathbb{F}$-algebra A, we write $A_{\tilde{\mathbb{F}}} := A \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ for its base change.

The following proposition shows that base change preserves certain properties.

Proposition: Suppose $\operatorname{char} \mathbb{F} = 0$, and $\tilde{\mathbb{F}}$ is a field extension of $\mathbb{F}$.

1) If A is semisimple, then so is $A_{\tilde{\mathbb{F}}}$.
2) If A is central simple, then so is $A_{\tilde{\mathbb{F}}}$.
3) If $B \subset A$ is a maximal commutative subalgebra, then so is $B_{\tilde{\mathbb{F}}} \subset A_{\tilde{\mathbb{F}}}$.

Using this we will show that $S_{\overline{\mathbb{F}}} \simeq \operatorname{Mat}_n(\overline{\mathbb{F}})$, while $K^i_{\overline{\mathbb{F}}} \subset \operatorname{Mat}_n(\overline{\mathbb{F}})$ are subalgebras conjugate to the subalgebra of diagonal matrices. This will establish 1) & 2) of Theorem, while 3) will require a bit more work.

1.2) Proof of 1) of Proposition

We use Theorem from Sec 1.2 of Lec 23: over a field of char 0, an algebra is semisimple iff the trace form is nondegenerate. Recall that, for $a,b\in A$, we have $(a,b)_A = tr((ab)_A)$. Next, $A\subset A_{\overline{\mathbb{F}}}$ & any $\mathbb{F}$-basis of A is an $\overline{\mathbb{F}}$-basis of $A_{\overline{\mathbb{F}}}$. So, for all $x\in A$, the matrices of operators x_A & $x_{A_{\overline{\mathbb{F}}}}$ are the same (b/c $A\subset A_{\overline{\mathbb{F}}}$ is a subring). So $(a,b)_A = tr((ab)_A) = tr((ab)_{A_{\overline{\mathbb{F}}}}) = (a,b)_{A_{\overline{\mathbb{F}}}}$. In particular, in a basis of A, the matrices of the trace forms for $A, A_{\overline{\mathbb{F}}}$ are the same, therefore, one form is nondegenerate iff the other is. $\square$

Remarks: 1) Let $\mathbb{F}=\mathbb{F}_p(t^p)$, $\tilde{\mathbb{F}}=A=\mathbb{F}_p(t)$ (fields of rational functions). Then $A_{\tilde{\mathbb{F}}}$ is not semisimple (exercise*)

2) Suppose that $\tilde{\mathbb{F}}$ is an algebraic and <u>separable</u> extension of $\mathbb{F}$. Then $Rad(A_{\tilde{\mathbb{F}}}) = Rad(A)_{\tilde{\mathbb{F}}}$ (exercise*, hint: reduce to the case when $\tilde{\mathbb{F}}$ is a finite & normal extension and consider the natural action of $Gal(\tilde{\mathbb{F}}:\mathbb{F})$ on $A_{\tilde{\mathbb{F}}}$.

1.3) Proofs of 2) and 3) of Proposition

Lemma: Let $\mathbb{F} \subset \tilde{\mathbb{F}}$ be a field extension, A be a finite dimensional $\mathbb{F}$-algebra, $B \subset A$ a subspace. Set $Z_A(B) := \{a \in A \mid ab = ba\ \forall b \in B\}$. Then $Z_A(B)_{\tilde{\mathbb{F}}} = Z_{A_{\tilde{\mathbb{F}}}}(B_{\tilde{\mathbb{F}}})$

Proof:

Claim: Let U, V be fin. dim. $\mathbb{F}$-vector spaces & $\varphi: U \to V$ an $\mathbb{F}$-linear map. Consider $\tilde{\varphi}: U_{\tilde{\mathbb{F}}} = U \otimes_{\mathbb{F}} \tilde{\mathbb{F}} \longrightarrow V_{\tilde{\mathbb{F}}} = V \otimes_{\mathbb{F}} \tilde{\mathbb{F}}$, the unique $\tilde{\mathbb{F}}$-linear map w. $\tilde{\varphi}(u \otimes f) = \varphi(u) \otimes f$, $\forall u \in U, f \in \tilde{\mathbb{F}}$. Then $\ker \tilde{\varphi} = (\ker \varphi)_{\tilde{\mathbb{F}}}$.

Proof: exercise (hint: pick bases $u_1, \dots u_n \in U$, $v_1, \dots v_m \in V$ s.t. $u_{k+1}, \dots u_n$ is a basis in $\ker \varphi$, $v_i = \varphi(u_i)$, $i = 1, \dots k$).

We apply Claim as follows. Let $b_1, \dots b_k$ be a basis in B. Consider $U = A$, $V = A^{\oplus k}$, $\varphi(u) = (b_i u - u b_i)_{i=1}^{k}$. Then

$$\ker \varphi = [\{a \in A \mid a b_i = b_i a\ \forall i = 1, \dots k\}] = [b_1, \dots b_k \text{ is basis of } B] = Z_A(B).$$

Then $\ker \tilde{\varphi} = [b_1, \dots b_k \text{ form } \tilde{\mathbb{F}}\text{-basis in } B_{\tilde{\mathbb{F}}}] = Z_{A_{\tilde{\mathbb{F}}}}(B_{\tilde{\mathbb{F}}})$. $\square$

Proof of 2) of Proposition: By 1) of Proposition, $A_{\tilde{\mathbb{F}}}$ is semisimple. So $A_{\tilde{\mathbb{F}}} \simeq \bigoplus_{i=1}^{k} Mat_{n_i}(S_i)$, where S_i's are skew-fields. By Exercise in Sec 2 of Lec 23, $Z(A_{\tilde{\mathbb{F}}}) \simeq \bigoplus_{i=1}^{k} Z(Mat_{n_i}(S_i))$.

By Lemma applied to $B=A$, $Z(A_{\tilde{\mathbb{F}}}) = Z(A)_{\tilde{\mathbb{F}}} = [Z(A)=\mathbb{F}$ b/c A is central $] = \tilde{\mathbb{F}}$. It follows that $k=1$ & $Z(Mat_{n_1}(S_1)) = \tilde{\mathbb{F}}$, which gives the claim of 2). $\square$

Proof of 3) of Proposition: The claim that B is maximal commutative is equivalent to $Z_A(B)=B$ (and same for $B_{\tilde{\mathbb{F}}} \subset A_{\tilde{\mathbb{F}}}$). Indeed, if $x \notin Z_A(B) \setminus B$, then the subalgebra generated by B & x $(:= Span_{\mathbb{F}}(bx^i \mid b \in B, i \geq 0))$ is commutative and strictly contains B, contradicting the maximality of B.

Now apply Lemma to $B \subset A$: $Z_{A_{\tilde{\mathbb{F}}}}(B_{\tilde{\mathbb{F}}}) = Z_A(B)_{\tilde{\mathbb{F}}} = B_{\tilde{\mathbb{F}}}$. $\square$

1.4) Proofs of 1) & 2) of Theorem

Let $K \subset S$ be a maximal subfield (= commutative subalgebra). By 2) of Proposition, $S_{\overline{\mathbb{F}}}$ is simple, and so is $Mat_n(\overline{\mathbb{F}})$ b/c $\overline{\mathbb{F}}$ is algebraically closed. Let $D_n(\mathbb{F})$ denote the subalgebra of diagonal matrices. We claim that $K_{\bar{\mathbb{F}}}$ is conjugate to $\mathcal{D}_n(\bar{\mathbb{F}})$ (i.e. $\exists\, g \in GL_n(\bar{\mathbb{F}}) \mid K_{\bar{\mathbb{F}}} = g\mathcal{D}_n(\bar{\mathbb{F}})g^{-1}$). This will imply 1) & 2).

By 1) of Proposition, $K_{\bar{\mathbb{F}}}$ is semisimple & by 3), it's maximal commutative. Any semisimple algebra is of the form $\bigoplus_{i=1}^{k} \mathrm{Mat}_{n_i}(\bar{\mathbb{F}})$, it's commutative iff all $n_i = 1$. Consider the $\mathrm{Mat}_n(\bar{\mathbb{F}})$-module $\bar{\mathbb{F}}^n$ as a $K_{\bar{\mathbb{F}}}$-module. It's the direct sum of irreducible $K_{\bar{\mathbb{F}}}$-modules, all of which are 1-dimensional: $\bar{\mathbb{F}}^n = \bigoplus_{i=1}^{n} V_i$. Choose $g \in GL_n(\bar{\mathbb{F}})$ w. $ge_i \in V_i$ (where $e_1, \dots e_n$ are the tautological basis elements), then $K_{\bar{\mathbb{F}}} \subset g\mathcal{D}_n(\bar{\mathbb{F}})g^{-1}$. Since $\mathcal{D}_n(\bar{\mathbb{F}})$ (and hence $g\mathcal{D}_n(\bar{\mathbb{F}})g^{-1}$) is a commutative subalgebra & $K_{\bar{\mathbb{F}}}$ is maximal commutative, we have

$$K_{\bar{\mathbb{F}}} = g\mathcal{D}_n(\bar{\mathbb{F}})g^{-1}.$$

1.5) Proof of 3) of Theorem.

Let $K^1, K^2 \subset S$ be maximal subfields. Consider $\tilde{\tau}: K^1_{\bar{\mathbb{F}}} \xrightarrow{\sim} K^2_{\bar{\mathbb{F}}}$, $\tilde{\tau}(k \otimes f) = \tau(k) \otimes f$, this is an $\bar{\mathbb{F}}$-algebra isomorphism.

Step 1: we claim that $\exists\, g \in GL_n(\bar{\mathbb{F}})$ s.t $\tilde{\tau}(x) = gxg^{-1}$, $x \in K^1$. Note that $K^i_{\bar{\mathbb{F}}} \simeq \bigoplus_{i=1}^{n} \mathrm{Mat}_1(\bar{\mathbb{F}}) = \bar{\mathbb{F}}^{\oplus n}$ has exactly n pairwise non-isomorphic 1-dimensional irreducible representations, denote them by $V_1^i, \dots V_n^i$, $i=1,2$. We have the decompositions

$$\overline{\mathbb{F}}^n = \bigoplus_{j=1}^n V_j^1 = \bigoplus_{j=1}^n V_j^2:$$

if $K_{\overline{\mathbb{F}}}^i = g_i \mathcal{D}_n(\overline{\mathbb{F}}) g_i^{-1}$, $g \in GL_n(\overline{\mathbb{F}})$, then we can pick $V_j^i = \overline{\mathbb{F}}(g_i e_j)$.

Let $\varphi_j^i : K_{\overline{\mathbb{F}}}^i \to End(V_j^i) = \overline{\mathbb{F}}$ be the corresponding homomorphisms: $K_{\overline{\mathbb{F}}}^i \simeq \overline{\mathbb{F}}^{\oplus n}$ as an algebra and φ_j^i's are projections to the summands, $j=1, \dots n$. The homomorphisms $\varphi_j^2 \circ \tilde{\tau}$ correspond to n pairwise non-isomorphic 1-dimensional representations of $K_{\overline{\mathbb{F}}}^1$, and so, after renumbering φ_j^2's we can assume that

(1) $$\varphi_j^2 \circ \tilde{\tau} = \varphi_j^1 \quad \forall j = 1, \dots n.$$

Take $g = g_2 g_1^{-1} \Rightarrow g K_{\overline{\mathbb{F}}}^1 g^{-1} = g_2 \mathcal{D}_n(\overline{\mathbb{F}}) g_2^{-1} = K_{\overline{\mathbb{F}}}^2$. Moreover, for $x \in K_{\overline{\mathbb{F}}}^1$, x acts on $g_1 e_j$ by scalar $\varphi_j^1(x)$, so gxg^{-1} acts on $g_2 e_j = g g_1 e_j$ by $\varphi_j^1(x)$ and, on the side, $gxg^{-1} \in K_{\overline{\mathbb{F}}}^2$ acts on $g_2 e_j$ by $\varphi_j^2(gxg^{-1}) \Rightarrow \varphi_j^1(x) = \varphi_j^2(gxg^{-1})$. Combining this w. (1) we see that

(2) $$\varphi_j^2(\tilde{\tau}(x)) = \varphi_j^2(gxg^{-1}) \quad \forall x \in K_{\overline{\mathbb{F}}}^1.$$

But φ_j^2 is the projection $\overline{\mathbb{F}}^{\oplus n} \to \overline{\mathbb{F}}$ to the jth summand. So $\varphi_j^2(gxg^{-1}) = \varphi_j^2(\tilde{\tau}(x)) \ \forall j = 1, \dots, n \Rightarrow gxg^{-1} = \tilde{\tau}(x) \Rightarrow$

(3) $$gx = \tau(x) g \quad \forall x \in K^1$$

Step 2: Now we prove the original claim: $\exists\, s \in S \setminus \{0\}$ $\tau(x) = sxs^{-1}$ $\forall\, x \in K$. Pick a basis $x_1, \dots x_n \in K$ (over $\mathbb{F}$) and consider the $\mathbb{F}$-linear map $\varphi: S \longrightarrow S^n$, $y \mapsto (yx_i - \tau(x_i)y)$ and the induced linear map $\tilde{\varphi}: S_{\overline{\mathbb{F}}} \longrightarrow S^n_{\overline{\mathbb{F}}}$. Recall (Claim in Sec 1.3) that $\ker \tilde{\varphi} = (\ker \varphi)_{\overline{\mathbb{F}}}$. We know that g (viewed as a matrix, i.e. an element of $S_{\overline{\mathbb{F}}}$) is in $\ker \tilde{\varphi}$ by (3). So $\ker \varphi \neq \{0\}$. Take any $s \in \ker \varphi \setminus \{0\}$. It's invertible b/c S is a skew-field so $sx = \tau(x)s \Rightarrow sxs^{-1} = \tau(x)$. $\square$

2) Finite skew-fields

In general, it's hard to classify finite dimensional skew-fields S over $\mathbb{F}$, so $\mathbb{F} = \mathbb{R}$ is an exception. Another nice case is when $\mathbb{F}$ is finite. Here S is also finite.

Theorem (Wedderburn) Every finite skew-field S is commutative

Proof:

Can take $\mathbb{F} = Z(S)$, let $|\mathbb{F}| = q$. Let $n := \dim_{\mathbb{F}} S \Rightarrow |S| = q^n$. Assume $\mathbb{F} \neq S \Leftrightarrow n > 1$. Let $G = S \setminus \{0\}$ be the multiplicative group. Let $s_1, \dots s_k$ be representatives of the G-conjugacy classes in $G \setminus Z(G) = S \setminus \mathbb{F}$. Then

$$(4) \qquad |G| = |Z(G)| + \sum_{i=1}^{k} |G|/|Z_G(s_k)|.$$

Note that $Z_G(s_k) = Z_S(s_k) \setminus \{0\}$. Let $d_k := \dim_{\mathbb{F}} Z_S(s_k)$ $\Rightarrow |Z_G(s_k)| = q^{d_k} - 1$. Next, note that $Z_S(s_k)$ is a skew-field, and S is its finite dimensional module $\Rightarrow S \simeq Z_S(s_k)^{\oplus ?}$ $\Rightarrow |S| = |Z_S(s_k)|^{?} \Leftrightarrow d_i \mid n \ \forall i$. Since $s_k \notin Z(G) \Rightarrow d_k < n$.

(4) becomes:

$$(5) \quad q^n - 1 = q - 1 + \sum_{i=1}^{k} (q^n - 1)/(q^{d_i} - 1)$$

Let $\Phi_d(x) \in \mathbb{Z}[x]$ denote the dth cyclotomic polynomial, $\Phi_d(x) = \prod_{\varepsilon} (x - \varepsilon)$, where the product is taken over primitive dth roots of 1. In particular, $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$ & $\Phi_d, \Phi_{d'}$ are coprime for $d \neq d'$. In particular, $\exists\, h(x), h_i(x) \in \mathbb{Z}[x]$, $i = 1, \dots k$ s.t. $x^n - 1 = \Phi_n(x) h(x) = \Phi_n(x)(x^{d_i} - 1) h_i(x)$

Combining this with (5), we get

$$\Phi_n(q) h(q) = (q-1) + \sum_{i=1}^{k} \Phi_n(q) h_i(q) \Rightarrow \Phi_n(q) \mid (q-1)$$

Observing $|\Phi_n(q)| > |q-1|$ (exercise) we arrive at a contradiction w. $n > 1$ $\square$

3) Bonus: Brauer group.

It turns out that the set of isomorphism classes of finite dimensional skew-fields over $\mathbb{F}$ carries a group structure, the resulting group is called the Brauer group of $\mathbb{F}$ & is denoted by $Br(\mathbb{F})$.

The construction of the group structure is based on the following observation

Theorem: Let A, B be finite dimensional central simple $\mathbb{F}$-algebras. Then

1) $A\otimes B$ is a central simple algebra
2) $A\otimes A^{opp} \xrightarrow{\sim} End_{\mathbb{F}}(A)$

Sketch of proof:

Step 1: Note that A is an irreducible $A\otimes A^{opp}$-module via $a_1\otimes a_2 . a = a_1 a a_2$ $(a, a_1, a_2 \in A)$, which, in particular gives a homomorphism of algebras $A\otimes A^{opp} \longrightarrow End_{\mathbb{F}}(A)$. Note that $End_{A\otimes A^{opp}}(A) \xrightarrow{\sim} Z(A) = [A \text{ is central}] = \mathbb{F}$.

Step 2: We use Proposition in Sec 1 of Lec 22: every $A\otimes A^{opp}$-submodule in $A\otimes B$ is of the form $A\otimes B'$, where $B'\subset B$ is an $\mathbb{F}$-subspace. Similarly, every $B\otimes B^{opp}$-submodule is of the form $A'\otimes B$ for an $\mathbb{F}$-subspace $A'\subset A$. It follows that there are just two subspaces in $A\otimes B$ that are both $A\otimes A^{opp}$- & $B\otimes B^{opp}$-submodules: $\{0\}$ & $A\otimes B$. Such a subspace is exactly the same thing as a two-sided ideal (exercise). So $A\otimes B$ is simple. To show it's central is also an exercise.

3) Since $A\otimes A^{opp}$ is simple, the homomorphism

$$A\otimes A^{opp}\longrightarrow End_{\mathbb{F}}(A)$$

is injective. Both dimensions are $(\dim A)^2$, so the homomorphism is an isomorphism. $\square$

For a central skew-field S, let $[S]$ denote it's isomorphism class. Fix two such skew-fields S_1, S_2. By the previous theorem $S_1\otimes S_2$ is a central simple algebra, and by our classification of simple algebras, $S_1 \otimes S_2 \simeq \mathrm{Mat}_n(S_3)$ for a uniquely determined skew-field S_3 that must be central.

We define $[S_1][S_2] := [S_3]$. An easy check using the associativity of tensor products of algebras & Exercise in Sec 2.1 of Lec 24, shows that this product is associative. It's also commutative & $[\mathbb{F}]$ is the unit. By 2) of the previous theorem $[S^{opp}]$ is the inverse of $[S]$. So we indeed get an abelian group.

An important property of $Br(\mathbb{F})$ is that every element has finite order. More precisely, Thm in Sec 1.0 (and it's char p versions) imply that $\dim_{\mathbb{F}} S$ is a complete square. Define the index of S, $\mathrm{ind}(S)$, to be $(\dim_{\mathbb{F}} S)^{1/2}$. One can show that $[S]^{\mathrm{ind}(S)} = [\mathbb{F}]$.