Remark: In C6.14, also $Z_R(S)$ has center K

[Inspect proof of T6.13:

$$Z_R(S) \cong M_t(E^{op}), \quad S \otimes_K D^{op} \cong M_m(E), \quad R \cong M_n(D)$$

$$Z(R) = K \Rightarrow Z(D) = Z(S) = K \overset{T6.3}{\Longrightarrow} Z(S \otimes_K D^{op}) = K \Rightarrow Z(E) = K$$

$$\Rightarrow Z(Z_R(S)) = Z(E^{op}) = K. \quad]$$

6.6 Splitting Fields

Throughout: K field, R fin.-dim. central simple K-algebra

Then: $R \otimes_K \bar{K}$ is a f.d. central simple $\bar{K}$-algebra $\Rightarrow R \otimes_K \bar{K} \cong M_n(\bar{K})$,

because $\bar{K}$ is the only f.d. central $\bar{K}$-div. algebra

Def: A field $L \supseteq K$ is a **splitting field** for R if $R \otimes_K L \cong M_n(L)$

for some n. (in fact $n = \deg_K R$)

Observe: if L splits R, and $L' \supseteq L$ is a field ext, then

$$L' \otimes_K R \cong L' \otimes_L L \otimes_K R \cong L' \otimes_L M_n(L) \cong M_n(L'),$$

so also L' splits R.

Def: A **subfield** of R is a subring L that is a field,

it is a **maximal subfield** if $L' \supseteq L \Rightarrow L' = L$ for all subfields L'.

Note: $[R:K] < \infty \Rightarrow$ maximal subfields exist

(Take an element of max. K-dimension in $\{K \subseteq L \subseteq R : L \text{ subfield of } R\}$)

Lemma 6.15 If D is a division ring, a subfield L is maximal

$\Leftrightarrow L = Z_D(L)$

Proof: L commutative $\Rightarrow L \subseteq Z_D(L)$

„$\Rightarrow$": If $x \in Z_D(L)$, then $L[x] \subseteq Z_D(L)$, and further $L(x) \subseteq Z_D(L)$

So $L(x) \supseteq L$ is a field ext., so $L(x) = L$, i.e., $x \in L$.

„$\Leftarrow$": Suppose $L' \supseteq L$ is a field ext. in $D \Rightarrow L' \subseteq Z_D(L) = L$. □

Exm: „$\Leftarrow$" also holds for R a K-c.s.a. But not conversely, and R may not contain a subfield L w. $Z_R(L) = L$:

$R = M_n(\mathbb{H})$ has dim. $4n^2$. If $L \subseteq M_n(\mathbb{H})$ is a subfield w. $Z_R(L) = L$, then $[L:\mathbb{R}]^2 = 4n^2$ [T6.13], so $[L:\mathbb{R}] = 2n$.

Not possible for $n > 1$!

Thm 6.16 Let R be a K-c.s.a., $n^2 = [R:K] < \infty$

If $L \subseteq R$ is a subfield with $Z_R(L) = L$, then

(1) $[L:K] = n = \deg_K R$

(2) L is a splitting field for R

Def: If $L \subseteq R$ subfield w. $Z_R(L) = L$, then L strict maximal subfield of R

In particular: If R is a div. algebra, every max. subfield is a splitting field.

Proof: (1) [T6.13] $\Rightarrow n^2 = [L:K][Z_R(L):K] = [L:K]^2 \Rightarrow n = [L:K]$

(2) R is a (R,R)-bimodule, hence left $R \otimes_K R^{op}$-module.

This restricts to a $R \otimes_K L$-module structure on R

$\Rightarrow \exists K$-algebra hom $\varphi: R \otimes_K L \longrightarrow End(R_K)$

Since $\varphi(r \overset{R}{\otimes} \lambda \overset{L}{)}(x \overset{R}{,} \mu \overset{L}{)} = r x \mu \lambda = r x \lambda \mu = \varphi(r \otimes \lambda)(x)\,\mu$,

actually φ maps into $End(R_L) \underset{(1)}{\cong} M_n(L)$

$R \otimes_K L$ is simple [T6.4] $\Rightarrow \varphi$ injective

$\dim_K (R \otimes_K L) = n^3 = \dim_K M_n(L)$, so φ is surjective.

Cor 6.17 If R is a f.d. c.s.a / K, then exists a splitting field $L \supseteq K$ with $[L:K] = \mathrm{ind}_K(R)$.

Proof: $R = M_n(D)$ for some $n \geq 1$, D f.d. central division K-algebra,

[T6.16] $\Rightarrow \exists$ subfield $L \subseteq D$ with $[L:K] = \sqrt{[D:K]} = \mathrm{ind}_K R =: m$

s.t. $D \otimes_K L \cong M_m(L)$

$\Rightarrow R \otimes_K L \cong M_n(K) \otimes_K D \otimes_K L \cong M_n(K) \otimes M_m(L) \cong M_{nm}(L)$. $\square$

6.7 Seperable Splitting Fields

Lemma 6.18: Let $L \supseteq K$ be an algebraic field extension. If $a \in L$ is an inseperable element (i.e., the min. poly $m_a \in K[x]$ has repeated roots), then $\exists e \geq 1$: a^{p^e} is seperable over K $(p = \mathrm{char} K > 0)$

Proof: Since a is inseperable $(m_a' = 0)$, $m_a = f(x^p)$ for some $f \in K[x]$

Since m_a is irreducible, so is f. We iterate to find

$m_a = g(x^{p^e})$ with $e \geq 1$, $g \in K[x]$ irreducible and separable.

$\Rightarrow$ g is the min. poly of a^{p^e}, so a^{p^e} is separable. $\square$

Thm 6.19 (Jacobson–Noether) If D is a noncommutative division ring that is algebraic over its center K, then there exists a separable $a \in D \setminus K$.

Proof: If $\operatorname{char} K = 0$, then any $a \in D \setminus K$ works, because every field ext. is separable. Let $\operatorname{char} K = p > 0$. Suppose all $a \in D \setminus K$ are inseparable.

Then $\forall a \in D \setminus K \; \exists e \geq 1 : a^{p^e} \in K$ [L6.18]

$\Rightarrow \exists a \in D \setminus K : a^p \in K$.

Consider $\sigma \in \operatorname{Aut}_K(D)$, $\sigma(x) = axa^{-1}$.

Since $a \notin Z(D)$, $\sigma \neq id$. But $(\sigma - id)^p = \sigma^p - id = 0$ in $\operatorname{End}_K(D)$

Let $b \in D$, $t \geq 1$ s.t. $(\sigma - id)^t(b) \neq 0$, $(\sigma - id)^{t+1}(b) = 0$

$z := (\sigma - id)^{t-1}(b) \neq 0$, $w := (\sigma - id)^t(b) \neq 0$

$\Rightarrow (\sigma - id)(w) = 0$, $(\sigma - id)(z) = w$

$\Rightarrow \sigma(w) = w$, $\sigma(z) = z + w$

$\Rightarrow \sigma(\underbrace{w^{-1}z}_{\text{!! } x}) = \sigma(w)^{-1}\sigma(z) = \underbrace{w^{-1}z}_{\text{!! } x} + 1$, so $\sigma(x) = x + 1$.

Let $e \geq 1$ s.t. $x^{p^e} \in K$ [L6.18]

$\Rightarrow x^{p^e} = \sigma(x^{p^e}) = \sigma(x)^{p^e} = (x+1)^{p^e} = x^{p^e} + 1$ $\lightning$. $\square$

Thm 6.20 (Koethe) If D is a f.d. central div. K-algebra and $K \subseteq L \subseteq D$ is a subfield w. L/K separable, then there exists a max. subfield

$L' \supseteq L$ with L'/K separable.

In particular: L' is a separable splitting field for D.

Proof: Choose $L' \supseteq L$ a subfield of D maximal with L'/L separable. Then L'/L separable, L/K separable $\Rightarrow L'/K$ separable.

We show: $L' = Z_D(L')$, then L' is a max. subfield [L6.15], hence a splitting field [L6.16].

$L' \subseteq Z_D(L')$ ✓. $D' := Z_D(L')$. Then $L' = Z_D(D')$ [T6.13]

$\Rightarrow Z(D') = L'$ [since $Z(D') = D' \cap Z_D(D') = D' \cap L' = L'$]

Suppose $D' \supsetneq L' \overset{T6.19}{\Rightarrow} \exists a \in D' \setminus L'$ separable over $L' \Rightarrow L'(a)/L'$ separable $\Rightarrow L'(a)/L$ separable $\Rightarrow a \in L'$ by maximality of L' ↯. □

Cor 6.21 If R is a f.d. K-c.s.a, then R has a Galois splitting field

[Recall: a finite ext. L/K is Galois if it is separable & normal]

Proof: Using T6.20 (w. $L = K$), we get that R has a splitting field L_0 with L_0/K separable and $[L_0 : K] = \text{ind}_K(R)$ (like [C6.11])

Take L/L_0 a normal closure. Then L/K is Galois,

And L is a splitting field for R. □

6.8 Frobenius Theorem

Thm 6.22 (Frobenius) Every f.-d. division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$

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

Lemma 6.23 Let Q be an $\mathbb{R}$-algebra generated by some i', j' s.t. $(i')^2 = -1$, $(j')^2 = -1$, $i'j' = -j'i' =: k'$. Then $1, i', j', k'$ is an $\mathbb{R}$-basis of Q and $Q \cong \mathbb{H}$.

Proof: One checks $(k')^2 = -1$, $j'k' = -k'j' = i'$, $k'i' = j' = -i'k'$.

In particular $Q = {}_{\mathbb{R}}\langle 1, i', j', k' \rangle$. Still need to check that this is a basis. Suppose $0 = \alpha + \beta i' + \gamma j' + \delta k'$

$\overset{\text{computation}}{\Longrightarrow} (\alpha + \beta i' + \gamma j' + \delta k')(\alpha - \beta i' - \gamma j' - \delta k') = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$

$\Longrightarrow \alpha = \beta = \gamma = \delta = 0$. □

Proof of T6.22: Let D be a f.d. div. algebra $/\mathbb{R}$.

Let K be a max. subfield of D.

$\Rightarrow K \cong \mathbb{R}$ or $K \cong \mathbb{C}$ (the only f.d. field ext. of $\mathbb{R}$)

$\Rightarrow [K:\mathbb{R}] = 1$ or $[K:\mathbb{R}] = 2$

Case $[K:\mathbb{R}] = 1$: $\overset{T6.16}{\Longrightarrow} D = \mathbb{R}$.

Case $[K:\mathbb{R}] = 2$: $\overset{T6.16}{\Longrightarrow} [D:K] \in \{1, 2\}$

If $[D:K] = 1 \Rightarrow D = K \cong \mathbb{C}$.

Suppose $[D:K] = 2$. $K \cong \mathbb{C}$, and wlog $K = \mathbb{C}$.

$K \to K$, $a + bi \overset{z}{\mapsto} a - bi \overset{\bar{z}}{}$ is an $\mathbb{R}$-automorphism of the simple algebra $\mathbb{C} \Rightarrow \exists x \in D^\times \forall z \in K: \; xzx^{-1} = \bar{z}$

$\Rightarrow x^2 z x^{-2} = z \overset{[T6.10]}{\Longrightarrow} x^2 \in Z_D(K) \overset{L6.15}{=} K$.

Since $\overline{x^2} = x(x^2)x^{-1} = x^2$, even $x^2 \in R$.

Exc: Think about why this is true, but $w^2 = -1 \not\Rightarrow w \in \{\pm i\}$

If $x^2 > 0$, then $x^2 = r^2$, $r \in \mathbb{R} \Rightarrow x \in \{\pm r\}$ $\not\Rightarrow x \in D \setminus K$.

So $x^2 < 0 \Rightarrow \exists y \in \mathbb{R}^\times : x^2 = -y^2$

Define $j := xy^{-1} \Rightarrow j^2 = -1$ (note x, y commute)

$ij = ixy^{-1} = xiy^{-1} = -xiy^{-1} = -xy^{-1}i = -ji$ $\overset{L6.23}{\Rightarrow} D \cong \mathbb{H}$. $\square$

7. The Brauer Group

Now: K field, CSA always means f.d. central simple algebra over K (more explicit: K-CSA)

If R is a CSA, then $R \cong M_n(D)$ for D a division ring, with D, n unique up to isomorphism of D. (Wedderburn-Artin).

Also $D \cong \mathrm{End}(V_R)$, V_R unique simple right R-module.

Note $Z(R) = Z(D) = K$, so D is a K-CSA

Def: CSA R, S are similar, $R \sim S$, if when $R \cong M_m(D)$, $S \cong M_n(E)$, D, E div. rings, then $D \cong E$.

Note: Similarity is an equivalence relation on K-CSAs.

Lemma 7.1 For CSA R, S TFAE:

(a) $R \sim S$

(b) $\exists m, n \geq 1$: $R \otimes_K M_m(K) \cong S \otimes_K M_n(K)$

(c) $\exists m, n \geq 1$: $M_m(R) \cong M_n(S)$

(d) For the unique simple modules U_R, V_S: $End(U_R) \cong End(V_R)$

Proof: (a)⇒(b): Wlog $R \cong M_r(D)$, $S \cong M_s(D)$

Take $m=s$, $n=r$ ⇒ $R \otimes_K M_m(K) \cong M_{mr}(D) \cong M_{ns}(K) \cong S$.

(b)⇒(c) since $R \otimes_K M_m(K) \cong M_m(R)$, $S \otimes_K M_n(K) \cong M_n(S)$

(c)⇒(d) $R \cong M_r(D)$, $S \cong M_s(E)$ with $D = End(U_R)$, $E = End(V_R)$

Uniqueness of Wedderburn-Artin ⇒ $D \cong E$.

(d)⇒(a) R, S are matrix rings over $D = End(U_R) \cong End(V_S)$. □

$[R]$:= similarity class of R

Thm & Def 7.2 The Brauer group of K is the abelian group

$Br(K) := \{[R] : R \text{ } K\text{-CSA}\}$ with operation

$[R] + [S] := [R \otimes_K S]$.

Proof: $Br(K)$ is a set.

To check (1) Operation is a well-defined map $Br(K) \times Br(K) \to Br(K)$

(2) $Br(K)$ is an abelian group

(1) $R \otimes_K S$ is a K-CSA by C6.6.

Suppose $R' \sim R$, $S' \sim S$. Then $R \cong M_r(D)$, $R' \cong M_{r'}(D)$,

$S \cong M_s(E)$, $S' \cong M_{s'}(E)$ for $r, r', s, s' \geq 1$, div. alg. D, E.

$R \otimes_K S \cong (D \otimes_K M_r(K)) \otimes_K (E \otimes M_s(K))$

$\cong (D \otimes E) \otimes M_r(K) \otimes M_s(K) \cong D \otimes E \otimes M_{rs}(K) \sim D \otimes E$

and similarly $R' \otimes_k S' \sim D \otimes E$.

(2) $[K] \in Br(K)$, so $Br(K) \neq \emptyset$.

Note: $[R] = [M_n(R)]$ $\forall n \geq 1$, in particular: $[K] = [M_n(K)]$ $\forall n \geq 1$!

Commutativity: $[R] + [S] = [R \otimes S] = [S \otimes R] = [S] + [R]$,
$R \otimes S \cong S \otimes R$

Neutral element: $[R] + [K] = [R \otimes K] = [R]$
$R \otimes K \cong R$

Associativity: Since $(R \otimes S) \otimes T \cong R \otimes (S \otimes T)$

Inverses: $R \otimes R^{op} \cong M_n(K)$ with $n = [R:K]$ by (6.7),
so $[R] + [R^{op}] = [M_n(K)] = K$.

□

Exm 7.3: (1) $Br(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ by [T6.22]

$(\mathbb{H} \cong \mathbb{H}^{op}, \ \mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})) \Rightarrow Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

(2) If K is alg. closed, then K is the unique f.d. K-div. algebra [L2.3].

$\Rightarrow Br(K)$ is trivial

(3) If K is finite, then $Br(K)$ is trivial by „Little Wedderburn" [T4.13].