§2.1 Wedderburn's Thm

Setup : k : field

When we say "k-algebra", we mean it is finite dim $/k$.

Def: A k-algebra is called simple if does no (two-sided) ideal other than 0 and A.

A is central if its center equals to k.

Ex1: Any division algebra D $/k$ is simple:

$0 \neq I$: ideal of D. $aI = I$, $\forall a \in D$. $\Rightarrow 1 \in I \Rightarrow I = D$.

$Z(D) = \{a \in D \mid ab = ba, \forall b \in D\}$ is a field.

D is a central simple algebra over $Z(D)$.

(Prop 1.1.7)
Ex2: A non-splitting quaternion algebra is a division algebra, and central over k.

Ex3: Split ($\cong M_2(k)$) quaternion algebras are also simple.

D: division algebra $/k$.

$\Rightarrow M_n(D)$ of $n \times n$ matrices over D is simple for all $n \geq 1$.

WTS: two sided ideal $\langle M \rangle$ in $M_n(D)$ is $M_n(D)$ itself.

E_{ij} : $n \times n$ matrix w/ $m_{ij} = 1$, and other entries 0.

$\forall M \in M_n(D)$ is a linear combination of E_{ij}'s.

Then it suffices to show $E_{ij} \in \langle M \rangle$, $\forall i, j$.

Moreover, matrix multiplication shows $E_{ki} E_{ij} E_{jl} = E_{kl}$.

Then it suffices to show $E_{ij} \in \langle M \rangle$ for some i, j.

Construction : Pick i, j. s.t. $M = [m_{ij}]$, $m_{ij} = m \neq 0$.

then $E_{ij} = E_{ii} M E_{jj} \cdot m^{-1}$.

Moreover, $Z(M_n(D))$ contains only scalar multiplications of Id.

$\Rightarrow M_n(D)$ is a central simple algebra $/Z(D)$.

The Wedderburn theorem gives a converse to this example:

Thm (Wedderburn): A: finite dim simple algebra / a field k. Then $\exists\ n \geq 1$, $n \in \mathbb{Z}$, and a division algebra $D \supset k$, s.t. $A \cong M_n(D)$. And D is determined up to isomorphism.

Before we prove this thm, we need two lemmas, and several notions from module theory.

Def: A nonzero A-module M is simple if it has no A-submodules other than 0 and M.

Ex. (We will also need this example to prove the uniqueness of D in Thm of Wedderburn).

Q: What are the simple left modules over $M_n(D)$?

For all $1 \leq r \leq n$, consider $I_r = \{ M = [m_{ij}] \mid m_{ij} = 0 \text{ for } j \neq r \} \subseteq M$.

Can check that I_r is a left ideal of M.

I_r is also minimal wrt inclusion. ($E_{ki} \cdot E_{ir} = E_{ir}$. $m_{ir} \neq 0$).

Then I_r's are simple $M_n(D)$-modules.

Also, $M_n(D) \cong \bigoplus_{r=1}^{n} I_r$. And all I_r's are isomorphic.

$\Rightarrow$ A simple $M_n(D)$-module M is a quotient of $M_n(D) \cong \bigoplus_{r=1}^{n} I_r$.

Then $M \cong I_k$, for some k. but all I_k's are isomorphic. so wlog, $M \cong I_1$.

$\forall I_k$, $I_k \cong D^n$. by the construction.

Def: An endomorphism of a left A-module M over a ring A is an A-homomorphism $M \longrightarrow M$.

i.e. $\mathrm{End}_A(M) = \{ f: M \longrightarrow M \text{ is a } A\text{-homomorphism} \}$.

$\mathrm{End}_A(M)$ forms a ring: $\{ (\phi + \psi)(x) = \phi(x) + \psi(x)$.

$\lfloor\ \phi \cdot \psi = \phi \circ \psi.$

$x \in M,\ \phi \in \mathrm{End}_A(M)$

If A is a k-algebra, so is $\mathrm{End}_A(M)$. M is a left module / $\mathrm{End}_A(M)$: $\phi \cdot x := \phi(x)$.

If $\phi \in \mathrm{End}_A(M) : x \longmapsto kx$, $k \in k$, then $\phi \in Z(\mathrm{End}_A(M))$.

If A is a division algebra, M can be viewed as a left vector space / A.

then arguing similarly as in linearly algebra, can choose a basis of M / A,

then $\mathrm{End}_A(M)$ is isomorphic to a matrix algebra.

Let A^{opp} := opposite algebra of A, where A^{opp} & A have the same underlying v. sp / k,

but $\forall x, y \in A^{opp}$, $x \cdot y := yx$.

WHY? Take a simple case, M viewed a 1-dim vector space / A. w/ basis $\{x\}$.

then elements in $\mathrm{End}_A(M)$ are just scalar multiplications of A.

$$\phi : M \longrightarrow M, \qquad \psi : M \longrightarrow M$$
$$x \longmapsto ax \qquad\qquad x \longmapsto bx.$$

then $(\phi \cdot \psi)(x) = \phi(\psi(x)) = \phi(bx) = b\,\phi(x) = ba\,x$. This is when we swap order of mult.

<u>Lemma (Schur)</u> : Let M be a simple module over a k-algebra A. Then $\mathrm{End}_A(M)$ is a division algebra.

pf : $\phi : M \longrightarrow M$. A-module homomorphism. not trivial.

What is $\ker(\phi)$?

Since M is simple, $\ker(\phi) = 0$. then $\mathrm{im}(M) = M$. so $\phi : M \xrightarrow{\sim} M$.

$\Rightarrow \phi$ has an inverse in $\mathrm{End}_A(M)$. so $\mathrm{End}_A(M)$ is a division algebra. ▨

M: left A-module. $E := \mathrm{End}_A(M)$. $\Rightarrow$ M is a left E-module.

Consider $\mathrm{End}_E(M)$. Define $\lambda_M : A \longrightarrow \mathrm{End}_E(M)$

$$a \longmapsto (x \overset{\phi}{\longmapsto} ax).$$

Can check : λ_M is an E-endomorphism .

Lemma (Rieffel): L : non-zero left ideal in a simple k-algebra A. Let $E := \mathrm{End}_A(L)$.

Then $\lambda_L : A \longrightarrow \mathrm{End}_E(L)$ is an isomorphism.

Pf: Injectivity: b/c A is simple, $\lambda_L \neq 0$, $\ker(\lambda_L)$ is trivial.

Surjectivity: Can check that $\lambda_L(L)$ is a left ideal in $\mathrm{End}_E(L)$:

i.e. $\phi \in \mathrm{End}_E(L)$, $l \in L$. $\phi \cdot \lambda_L(l) = \lambda_L(\phi(l))$.

Now, LA, right ideal generated by L, is actually a two-sided ideal: $A(LA) = (AL)A = LA$.

Then as A is simple, $LA = A$.

then $1 = \sum l_i a_i$, $l_i \in L$, $a_i \in A$.

Take $\phi \in \mathrm{End}_E(L)$, $\phi \cdot 1 = \phi(\lambda_L(1)) = \phi(\lambda_L(\sum l_i a_i))$

$= \sum \phi(\lambda_L(l_i))\lambda_L(a_i))$

As $\lambda_L(L)$ is a left ideal, $\phi(\lambda_L(l_i)) \in \lambda_L(L)$, $\forall i$. $\Rightarrow \phi \in \lambda_L(A)$. ☒

Pf of Wedderburn:

As A is finite dim, a descending chain of left ideals must stabilize.

Let L be a minimal left ideal. then it is a simple A-module.

By Schur's lemma, $E := \mathrm{End}_A(L)$ is a division algebra.

By Rieffel's lemma, $A \cong \mathrm{End}_E(L) \cong M_n(E^{opp})$. where $n = \dim_E L$.

Let $D := E^{opp}$ then $A \cong M_n(D)$.

$\boxed{\text{Uniqueness:}}$ Sps D, D' division algebras, s.t. $A \cong M_n(D) \cong M_m(D')$.

Let L be a minimal ideal of $M_n(D) \cong M_m(D')$, then $L \cong D^n \cong (D')^m$.

Then $\mathrm{End}_A(L) \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(D'^m)$

Moreover, $\mathrm{End}_A(D^n) \cong D$ b/c $A \cong M_n(D) \cong M_m(D')$ and elements in

$\mathrm{End}_A(D'^m) \cong D'$ $\mathrm{End}_A(D^n)$ is scalar $\cdot I_n$.

So $D \cong D'$.

☒

<u>Cor.</u> k: field & $k=\bar{k}$. Then every central simple algebra is isomorphic to $M_n(k)$, for some $n \geq 1$.

Pf: By Wedderburn, it suffices to show that there does NOT exist finite dim division algebra $D \supsetneq k$.

If such a D exists, let $d \in D \setminus k$,

by a similar proof as in Cor 1.2.1, $\exists$ irreducible polynomial $f \in k[x]$, and a k-algebra homomorphism $k[x]/(f) \longrightarrow D$. the image contains d.

But k alg. closed. So $k[x]/(f) \cong k$. so $[k(d):k]=1$. $d \in k$. contradiction. $\boxtimes$

<u>§ 2.2. Splitting field</u>

<u>Thm</u>: k: field. A: finite dim. k-algebra. A is a central simple algebra $\Leftrightarrow$ $\exists n \in \mathbb{Z}, n>0$, and $K|k$, a finite field extension, s.t. $A \otimes_k K \cong M_n(K)$.

<u>Lemma</u>: A: finite dim k-algebra, $K|k$ an algebraic field extension.

A is central simple over k $\Longleftrightarrow$ $A \otimes_k K$ is central simple $/K$.

Pf: ($\Leftarrow$). If I is a non-trivial ideal of A, then $I \otimes_k K$ is also non-trivial of $A \otimes_k K$.

If A is not central, neither is $A \otimes_k K$.

Then if $A \otimes_k K$ is central simple, then so is A.

($\Rightarrow$). First reduce to the case that $K|k$ is finite. typo in the book

Can write $K|k$ as a union of its finite subextensions $K'|k$.

Then every ideal $I \subset A \otimes_k K$ is a union of ideals $I \cap K' \subset A \otimes_k K'$.

Also, $Z(A \otimes_k K) \subset Z(A \otimes_k K')$.

So it suffices to prove the case $K|k$ is finite.

WLG Wedderburn, may assume $A = D$ is a division algebra.

($A \cong M_m(D)$ is central. so only $D \cdot \mathrm{Id}_n$).

If $w_1, \dots, w_n$ is a k-basis of K, then $1 \otimes w_1, \dots, 1 \otimes w_n$: D-basis of $D \otimes_k K$.

$x \in Z(D \otimes_k K)$, $x = \sum \alpha_i (1 \otimes w_i)$.

then $\forall\, d \in D$, $x = (d^{-1} \otimes 1)\, x\, (d \otimes 1) = \sum (d^{-1} \alpha_i d)(1 \otimes w_i)$

$= \sum \alpha_i (1 \otimes w_i)$. $\Rightarrow$ $\alpha_i = d^{-1} \alpha_i d$.

As D is central $/k$, $\alpha_i \in k$. so $D \otimes_k K$ is central over K.

Let J be a non-zero ideal in $D \otimes_k K$. generated by $z_1, \dots, z_r$.

may consider J as a D-vector space, and $\{z_1, \dots, z_r\}$ be basis.

Extend them to a D-basis of $D \otimes_k K$ by adjoining some of the $1 \otimes w_i$'s.

New basis $\{z_1, \dots, z_r, 1 \otimes w_{r+1}, \dots, 1 \otimes w_n\}$

Say $1 \otimes w_{r+1}, \dots, 1 \otimes w_n$. Then for $1 \le i \le r$,

$$1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij} (1 \otimes w_j) + \underbrace{(d_{i1} z_1 + \dots + d_{ir} z_r)}_{y_i}$$

Apply $d^{-1}(\ )d$

$\Rightarrow$ $y_1, \dots, y_r$'s are linearly independent $/D$.

i.e. they form a basis for J.

As J is a two-sided ideal, for all $d \in D$, $d^{-1} y_i d \in J$.

i.e. $\exists\, \beta_{i\ell} \in D$, s.t. $d^{-1} y_i d = \sum \beta_{i\ell}\, y_\ell$.

Rewrite as

$$(1 \otimes w_i) - \sum_{j=r+1}^{n} (d^{-1} \alpha_{ij} d)(1 \otimes w_j) = \sum_{l=1}^{r} \beta_{i\ell} (1 \otimes w_\ell) - \sum_{\ell=1}^{r} \beta_{i\ell} \sum_{j=r+1}^{n} \alpha_{\ell j} (1 \otimes w_j).$$

$\Rightarrow$ $\beta_{ii} = 1$, $\beta_{i\ell} = 0$, $\ell \ne i$, and $d^{-1} \alpha_{ij} d = \alpha_{ij}$. $\Rightarrow$ $\alpha_{ij} \in k$, as D is central.

$\Rightarrow$ J can be generated by elements of K. (as k-subalgebra of $D \otimes_k K$).

$\Rightarrow$ $J \cap K = K$

$\Rightarrow$ $J = D \otimes_k K$. $\Rightarrow$ $D \otimes_k K$ is simple.

$\square$

Pf of thm:

($\Leftarrow$) follows from Lemma. & EX2, s.t. $M_n(D)$ is central / $Z(D)$.

($\Rightarrow$). Let $\bar{k}$ denote the algebraic closure of k.

$\Rightarrow$ $A \otimes_k \bar{k}$ is central simple, so $\cong M_n(\bar{k})$ for some n, by Cor to Wedderburn.

Let $K|k$, be a finite field extension, contained in $\bar{k}$.

$\Rightarrow$ $A \otimes_k K \hookrightarrow A \otimes_k \bar{k}$.

$\Rightarrow$ $A \otimes_k \bar{k} = \bigcup A \otimes_k K$.

Then for a sufficiently large finite extension $A \otimes_k K$,

it contains basis elements $e_1, \cdots, e_{n^2} \in M_n(\bar{k}) \cong A \otimes_k \bar{k}$.

and also a_{ij}, s.t. $e_i e_j = \sum_l a_{ijl} e_l$

Then map e_i to standard basis element of $M_n(K)$,

$\Rightarrow A \otimes_k K \cong M_n(K)$. ▨

Cor: A is a CSA $/k$, then $\dim_k A$ is a square.

Def: A field extension K/k over which $A \otimes_k K \cong M_n(K)$ for some n is called a **splitting field** for A. "A splits over K", "K splits A".

$\sqrt{\dim_k A}$ is called the **degree** of A.

Lemma: If A, B CSAs that split $/K$, then so is $A \otimes_k B$

Pf: $(A \otimes_k K) \otimes_K (B \otimes_k K) \cong (A \otimes_k B) \otimes_k K$

LHS $\cong M_n(K) \otimes_K M_m(K) \cong M_{nm}(K) \cong$ RHS. ▨

If A is a CSA, then so is A^{opp} so $A \otimes_k A^{opp}$ is also a CSA.

Prop: $A \otimes_k A^{opp} \xrightarrow{\sim} \mathrm{End}_k(A)$.

$\Rightarrow A \otimes_k A^{opp} \cong M_{n^2}(k)$. where $n = \deg A$.

Pf: $A \otimes_k A^{opp} \longrightarrow \mathrm{End}_k(A)$

$\sum a_i \otimes b_i \longmapsto (x \longmapsto \sum a_i x b_i)$. is not a zero map.

So must be injective b/c $A \otimes_k A^{opp}$ is simple.

Also surjective if we compute the dim. ▨

Thm: Every central division algebra D of degree n over an infinite field k is split by a separable extension K/k of degree n. Moreover, such a K may be found among the k-subalgebras of D.

Pf: By the following two props.

Prop: If a central simple algebra A/k of deg n contains a k-subalgebra K, which is a degree n field extension of k, then A splits over K.

Pf: By the above Prop, $A \otimes_k A^{opp} \cong \mathrm{End}_k(A)$.

$K \subset A \Rightarrow K \subset A^{opp}$ b/c K is a commutative.

$\Rightarrow i: A \otimes_k K \hookrightarrow \mathrm{End}_k(A)$.

Notice that the construction here shows that $i(A \otimes_k K) \subseteq \mathrm{End}_K(A) \cong M_n(K)$.

$\dim_K(M_n(K)) = n^2 = \dim_k(A) = \dim_K(A \otimes_k K)$.

So i is an isomorphism. ▨

Prop: If D is as in the thm, the $\exists\, a \in D$, s.t. $k(a)/k$ is separable of deg n.

<u>Cor</u>: A central simple algebra $/k$ has a splitting field that is finite and separable over k.

<u>Cor</u>: A finite-dim k-algebra A is a central simple algebra $\Leftrightarrow$ $\exists$ $n>0$, and a finite Galois field extension K/k, s.t. $A \otimes_k K \cong M_n(K)$.

<u>Pf</u>: ($\Leftarrow$) Already in thm.

($\Rightarrow$). Every finite separable field extension embeds in a finite Galois extension.