Chapter 2

RINGS

We intend to classify simple rings R using their (left) modules. For irreducible (left) R-modules M, $J = \operatorname{ann}_R M$ is an ideal in R hence $J = 0$. Moreover, Schur's Lemma implies that $\Delta = R' := \operatorname{End}_R M$ is a division ring and M can be regarded as a left vector space over Δ. The embedding $\rho : R \hookrightarrow \operatorname{End} M$ then factors as

$$\rho : R \hookrightarrow R'' := \operatorname{End}_\Delta M \hookrightarrow \operatorname{End} M,$$

with the left one being an embedding $\iota : R \hookrightarrow R''$ into Δ-linear maps.

To further investigate ι, the major tools we will develop is a kind of "density theorems" or "approximation theorems" for ring homomorphisms into certain endomorphism rings. For this purpose we first study some related and more flexible notions called (semi-)primitivity so that results on (completely reducible) modules in the previous chapter can be applied.

The major result is the classification theorem of (semi-)simple rings due to Wedderburn and Artin, under suitable finiteness assumption. More precisely, simple artinian rings are nothing but the matrix rings $M_n(\Delta)$ and semi-simple artinian rings are simply finite product of them.

Instead of giving the original proof, the proof via (semi-)primitivity and density presented here was due to Jacobson. The proof on Jacobson's density theorem was later simplified by Bourbaki via a version on density theorem on completely reducible modules. This later density theorem turns out to be powerful in other applications.

1. Semi-primitivity and the radical

Definition 2.1. Let R be a ring and by R-modules we mean left R-modules.

(1) R is (left) primitive if it admits a faithful irreducible module M.

(2) R is (left) semi-primitive (s.p.) if every $a \in R \setminus \{0\}$ acts non-trivially on some R-modules, i.e. $\rho(a) \neq 0$ for some ρ.

Clearly simple rings R are primitive: take $M = R/I$ for a maximal left ideal I and notice that $\operatorname{ann}_R M = 0$. Also primitive implies semi-primitive. Semi-primitivity is more flexible to work with due to the following fact:

Proposition 2.2. *The following are equivalent:*

(1) *R is semi-primitive.*
(2) *R has a faithful completely reducible module $M = \bigoplus M_i$.*
(3) *R is sub-direct product of primitive rings R_i's, namely*

$$\begin{tikzcd} R \arrow[r, hook, "\iota"] \arrow[dr] & \prod R_i \arrow[d, "\pi_i"] \\ & R_i \end{tikzcd}$$

Proof. (1) $\Rightarrow$ (2): Take $M = \bigoplus_{a \neq 0} M_a$ where $\rho_a(a) \neq 0$ on M_a.

(2) $\Rightarrow$ (3): M is faithful means $0 = \operatorname{ann}_R M = \bigcap \operatorname{ann}_R M_i$, hence

$$R \hookrightarrow \prod R/\operatorname{ann}_R M_i =: \prod R_i.$$

R_i is primitive since it is faithful on M_i. Also $R \twoheadrightarrow R_i$ clearly.

(3) $\Rightarrow$ (1): Denote $\rho_i : R_i \hookrightarrow \operatorname{End} M_i$. Let $a \in R$. If $\rho_i \pi_i \iota(a) = 0$ for all i then $a \in \bigcap \ker \rho_i \pi_i \iota = \bigcap \ker \pi_i \iota = \bigcap \ker \pi_i = \{0\}$. □

Recall that for any left ideal $I \subset R$,

$$\operatorname{ann}_R R/I = (I : R) := \{\, a \in R \mid aR \subset I \,\} \subset I,$$

which is the largest ideal contained in I. Also any irreducible R-module M is isomorphic to R/I for a maximal left ideal I. Hence

Corollary 2.3. (1) *R is primitive $\Longleftrightarrow$ $(I : R) = 0$ for some maximal left ideal I.* (2) *R is s.p. $\Longleftrightarrow$ $\bigcap_I (I : R) = 0$ among all maximal left ideals.*

Corollary 2.4. *Let R be commutative. Then* (1) *R is primitive if and only it is a field,* (2) *R is s.p. if and inly if it is a sub-direct product of fields.*

Example 2.5. (1) For a division ring Δ, the matrix ring $M_n(\Delta)$ is simple.

(2) Primitive rings might not be simple. Let V be an infinite dimensional vector space over Δ, $L = \operatorname{End}_\Delta V$ and $F \subset L$ be those linear maps $f \in L$ with $\dim_\Delta f(V) < \infty$. Then F is a non-trivial proper ideal and hence L is not simple. But V is clearly irreducible as L-modules, hence L is primitive.

(3) $\mathbb{Z}$ is s.p. by $\mathbb{Z} \hookrightarrow \prod_p \mathbb{Z}/(p)$ (since $\bigcap_p (p) = 0$ over all primes).

Definition 2.6. The Jacobson radical is the ideal

$$J(R) \equiv \operatorname{rad} R := \bigcap\nolimits_{I:\text{max left}} (I : R).$$

Proposition 2.7. *For any maximal left ideal I, the ideal $(I : R)$ is the intersection of all maximal left ideals I' with $R/I' \cong R/I$. In particular,*

$$J(R) = \bigcap\nolimits_{I:\text{max left}} I.$$

Proof. By definition, for any R-module M,

$$\operatorname{ann}_R M = \bigcap\nolimits_{x \in M} \operatorname{ann}_R x.$$

Moreover, M is irreducible ($M \cong R/I$ for a maximal left I) implies that

$$M = Rx \cong R/I_x$$

for any $0 \neq x \in M$ and $I_x := \operatorname{ann}_R x$ is a maximal left ideal. Clearly $(I_x : R) = \operatorname{ann}_R M = (I : R)$. This implies that $\bigcap (I : R) \supset \bigcap I$. Notice also that any $f : R/I' \cong R/I$ leads to $I' = I_x$ with $x = f(\bar{1})$.

The reverse direction $\bigcap (I : R) \subset \bigcap I$ follows by definition. □

Definition 2.8. An ideal $P \subset R$ is primitive if $\bar{R} := R/P$ is a primitive ring.

Corollary 2.9. *$P \subset R$ is a primitive ideal if and only if $P = (I : R)$ for some maximal left ideal I. In particular $J(R) = \bigcap P$ among primitive ideals.*

Proof. If $P = (I : R) = \operatorname{ann}_R M$ with $M = R/I$, then M is also a $\bar{R} := R/P$-module with $\operatorname{ann}_{\bar{R}} M = P/P = 0$. Conversely, let M be a faithful irreducible $\bar{R}$-module. By viewing M as a R-module via $R \twoheadrightarrow \bar{R}$, M is also irreducible with $\operatorname{ann}_R M = P$. But then $M \cong R/I$ for some maximal left ideal I and hence $P = (I : R)$. The last statement on $J(R)$ follows from Proposition 2.7. □

Remark 2.10. In Proposition 2.7, one might wonder if $(I : R)$ is indeed the intersection of all I' with $(I' : R) = (I : R)$. This is equivalent to ask if the primitive ring $\bar{R} := R/(I : R)$ has a unique faithful irreducible module M up to isomorphisms. This fails already for simple rings "without any finiteness assumptions". Classification of all irreducible modules of a simple ring is one the fundamental problems in ring theory. We will see shortly that the uniqueness does hold for simple (left) artinian rings.

Exercise 2.1. Following Example 2.5 (2), show that the ring L/F is simple which admits more than one irreducible modules.

Notice that the notion of primitivity of a ring depends on the left/right choices while the simplicity of a ring does not. The first example of a left primitive ring which is not right primitive was constructed by Bergman when he was an undergraduate (published in Proceedings AMS 1964).

On the contrary, we will now show that semi-primitivity on one side implies semi-simplicity on the other side. In fact we have

Theorem 2.11. *The left and right Jacobson radicals coincide:*

$$J_{\text{left}}(R) = \bigcap_{\text{max left}} I = \bigcap_{\text{max right}} I = J_{\text{right}}(R).$$

The proof is based on the notion of quasi-regularity:

Definition 2.12. Let R be a ring. An element $a \in R$ is called (left, right) quasi-regular if $1 - a$ has a (left, right) inverse.

Nilpotent elements are clearly quasi-regular: if $a^n = 0$ then $w(1-a) = (1-a)w = 1$ for $w := 1 + a + \ldots + a^{n-1}$.

Lemma 2.13. *Let I be a left/right ideal such that every $a \in I$ is left/right quasi-regular. Then all elements in I are quasi-regular.*

PROOF. We prove the left case. The right case is similar. If $w(1-a) = 1$, write $w = 1 - a'$ then $1 - a - a' + a'a = 1$, hence

$$a' = a - a'a \in I.$$

By assumption we have $(1 - a'')(1 - a') = 1$ for some $a'' \in R$. This implies that $1 - a'' = 1 - a$ and $a'' = a \in I$. In particular $1 - a$ is invertible. □

Definition 2.14. By Lemma 2.13, a left/right ideal consisting of (left/right) quasi-regular elements are referred as a quasi-regular left/right ideal.

Proposition 2.15. *$J(R)$ is the largest quasi-regular left ideal. In particular,*

$$J(R) = \{\, a \in R \mid 1 - ba \text{ has a left inverse for all } b \in R \,\}.$$

PROOF. We first prove that $J(R)$ is a quasi-regular left ideal. If $a \in J(R)$ is not left quasi-regular, then the left ideal $R(1-a) \neq R$ and hence $R(1-a) \subset I$ for some maximal left I. But $a \in J(R) \subset I$ and $1 - a \in I$ then leads to the contradiction $1 \in I$.

Next we prove that any quasi-regular left ideal Q is contained in $J(R)$. If not, then $Q \not\subset I$ for some maximal left I. Then $I + Q = R$ and we have $1 = a + q$ for some $a \in I$ and $q \in Q$. But then $a = 1 - q$ is invertible which leads to the contradiction $I = R$.

Fro the last statement, $a \in J(R) \Rightarrow ba \in Ra \subset J(R)$ which implies that a lies in the RHS. Conversely a lies in the RHS implies that Ra is a quasi-regular left ideal. Hence $a \in Ra \subset J(R)$. □

PROOF OF THEOREM 2.11. $J_{\text{left}}(R)$ is the largest quasi-regular left ideal. However from its original definition we know that $J_{\text{left}}(R)$ is an ideal. Thus $J_{\text{left}}(R)$ is also a quasi-regular right ideal. Proposition 2.15 then implies that $J_{\text{left}}(R) \subset J_{\text{right}}(R)$. Similarly we have $J_{\text{right}}(R) \subset J_{\text{left}}(R)$. □

From now on, there is no need to distinguish left/right quasi-regular ideals as well as left/right $J(R)$.

Corollary 2.16. *A ring R is left semi-primitive $\Longleftrightarrow J(R) = 0 \Longleftrightarrow R$ is right semi-primitive.*

2. Density theorems

Let R be s ring and $M = {}_RM$ be a R-module with $ax = \rho(a)(x)$ under $\rho : R \to \operatorname{End} M$. By definition $R' := \operatorname{End}_R M \subset \operatorname{End} M$ consists of group endomorphisms f commuting with the R-action

$$f(ax) = af(x), \qquad a \in R,\ x \in M.$$

Then M is naturally a R'-module ${}_{R'}M$.

Again let $R'' := \operatorname{End}_{R'} M \subset \operatorname{End} M$ be those group endomorphisms commuting with the R'-action. Then it is clear that

$$\rho(R) \subset R''$$

and it is an immediate question to ask if they are equal. If we keep on defining $R''' := \operatorname{End}_{R''} M \subset \operatorname{End} M$, then we have the trivial identity

$$R''' = R'.$$

Indeed $R' \subset (R')'' = R'''$. Also $a \in R'''$ means a commutes with the $R'' \supset R$ action. Thus $a \in R''$.

Example 2.17. (1) For $M = {}_RM = \bigoplus^n R$ a free module of finite rank. By presenting M as row vectors we had seen in last chapter that $R' \cong M_n(R)^{\text{op}}$ (right multiplication by matrices) and $R'' \cong R$ as scalar multiplications on the left. Thus $\rho(R) = R''$. The essential formula used is

$$f(v_j) = f(v_i e_{ij}) = f(v_i)e_{ij} \in Rv_j.$$

(2) The procedure also shows that (1) holds if the rank is infinite. Let $M = \bigoplus^{\mathbb{N}} R$. Then R' consists of row-finite infinite matrices.

Now let $S \subset R' \subset M_\infty(R)^{\text{op}}$ be the subring consisting of

$$aI_\infty + A_f, \qquad a \in R,$$

where A_f is a "finite $n \times n$ matrix" in $M_\infty(R)$ for some $n \in \mathbb{N}$. (If we put $a = 0$ then we get an ideal as in Example 2.5-(2).)

By viewing $M = {}_SM$ (matrix multiplication on right), the same procedure shows that $S' \cong R$ as left scalar multiplications. Hence $S'' \cong R'$ which is strictly larger than S.

Nevertheless, we do have the "finite approximation property" for the imbedding $S \hookrightarrow S''$: for any $x_1, \ldots, x_n \in M$ and $s'' \in S''$, there exists $s \in S$ such that

$$sx_i = s''x_i \qquad 1 \le i \le n.$$

(3) For $R = \mathbb{Z}$, $M := \bigoplus_{p:\text{prime}} \mathbb{Z}/(p)$, we have

$$R' = \hom_{\mathbb{Z}}(\bigoplus\nolimits_p \mathbb{Z}/(p), \bigoplus\nolimits_q \mathbb{Z}/(q)) \cong \prod \mathbb{Z}/(p)$$

since all cross terms vanish. Then $R'' = \text{End}_{R'} M \cong \prod \mathbb{Z}/(p)$ since the action on M by R' is component-wise. The embedding $R \hookrightarrow R''$:

$$\mathbb{Z} \hookrightarrow \prod \mathbb{Z}/(p)$$

is not surjective. But the "finite approximation" as in (2) holds by the Chinese Remainder Theorem: for any $x_1, \ldots, x_n \in M$ and $a'' \in R''$, there are only a finite number of primes T such that $a''x_i \neq 0$ for all $i \in [1, n]$. Over T we may solve $a \in \mathbb{Z}$ with $a \equiv a''_p \pmod{p}$ for $p \in T$. Then clearly

$$ax_i = a''x_i, \qquad 1 \le i \le n.$$

For a full endomorphism ring $S = R' = \text{End}_R M$, we have seen that $S = S''$. This, together with Example 2.17, suggests the following notion:

Definition 2.18. A subring $S \subset \text{End}_R M$ is dense if for every $f \in \text{End}_R M$ and $x_1, \ldots, x_n \in M$ there is a $s \in S$ such that $s(x_i) = f(x_i)$ for all i.

Remark 2.19. If $R = \Delta$ is a division ring, M is then a vector space over Δ and the condition is equivalent to: for every linearly independent $v_1, \ldots, v_n \in M$ and any $y_1, \ldots, y_n \in M$, there is a $s \in S$ such that $s(v_i) = y_i$ for all i.

Also if $n = \dim_\Delta M < \infty$, then it is clear that the only dense subring $S \subset \text{End}_\Delta M \cong M_n(\Delta)^{\text{op}}$ is the full matrix ring.

Here is a useful density theorem in the spirit of Example 2.17-(3):

Theorem 2.20 (Bourbaki)**.** *Let $M = {}_RM$ be completely reducible, $R' := \text{End}_R M$, $R'' := \text{End}_{R'} M$. Then $R \hookrightarrow R''$ is dense.*

PROOF. Step 1. Any submodule $N \subset {}_R M$ is a R''-submodule:

Indeed, the complete reducibility of M implies that $M = N \oplus P$ for some $P \subset {}_R M$. Let $e \in R'$ be the corresponding projection onto N. Then for $a'' \in R''$,

$$a''N = a''e(N) = e(a''M) \subset e(M) = N.$$

Step 2. Denote ${}_R M^{\oplus n} = \bigoplus_{i=1}^n {}_R M\, e_i$ and let $R'_n := \mathrm{End}({}_R M^{\oplus n})$. Then $a'' \in R''$ determines a map $a''_{(n)} \in \mathrm{End}({}_{R'_n} M^{\oplus n})$:

Indeed any $\ell \in R'_n$ is determined by $\ell(u) = \sum_{i=1}^n \ell(u_i e_i)$ where

$$\ell(u_i e_i) = \sum_{j=1}^n a'_{ij}(u_i)\, e_j, \qquad a'_{ij} \in R'.$$

Now $a'' \in R''$ gives a map on ${}_R M^{\oplus n}$ by $a''_{(n)} u := \sum_{i=1}^n a'' u_i\, e_i$. Then

$$\ell(a''_{(n)} u) = \sum_{i,j=1}^n a'_{ij}(a'' u_i)\, e_j = \sum_{i,j=1}^n a'' a'_{ij}(u_i)\, e_j = a''_{(n)}\, \ell(u)$$

for all $\ell \in R'_n$. This proves the claim.

Step 3. Proof of the theorem:

For $n = 1$, let $N := Rx_1 \subset {}_R M$, then Step 1 implies that $N \subset {}_{R''} M$. Hence $a'' \in R'' \Rightarrow a'' x_1 \in N = Rx_1$. That is, $a'' x_1 = a x_1$ for some $a \in R$.

For general $n \in \mathbb{N}$, $M^{\oplus n}$ is also completely reducible. By Step 2, we may apply the result for $n = 1$ to $a''_{(n)}$ and $M^{\oplus n}$ with $x = \sum_{i=1}^n x_i\, e_i \in M^{\oplus n}$. Namely there exists $a \in R$ such that $ax = a''_{(n)} x$. This means $a x_i = a'' x_i$ for $1 \le i \le n$ as expected. □

As the first application, we derive "Jacobson's density theorem":

Theorem 2.21 (Jacobson). *A ring R is primitive $\iff$ R is isomorphic to a dense subring of $\mathrm{End}_\Delta M$ where M is a vector space over a division ring Δ.*

PROOF. Given a faithful irreducible R-module $\rho : R \hookrightarrow \mathrm{End}_R M$, Schur's Lemma implies that $\Delta := R' = \mathrm{End}_R M$ is a division ring and M is a Δ vector space. Theorem 2.20 then implies that $R \subset R'' = \mathrm{End}_{\,\Delta} M$ is dense.

Conversely, if $R \subset \mathrm{End}_{\,\Delta} M$ is dense then for any $x \neq 0$ and y in M there exists $a \in R$ such that $ax = y$. This implies that $M = {}_R M$ is irreducible and thus R is primitive. □

If it happens that $\dim_\Delta M < \infty$ then in fact $R \cong \mathrm{End}_\Delta M$. This is the starting point of the Wedderburn–Artin theorem on (semi-)simple (left) artinian rings discussed in the next section.

Exercise 2.2. Investigate how Bourbaki's formal proof of the density theorem recovers the Chinese Remainder Theorem as in Example 2.17-(3).

It is clear that Theorem 2.20 does not take care of the phenomenon explained in Example 2.17 (1) and (2) if R is not a division ring. This suggests the existence of a more general density theorem beyond the completely reducible case. A hint towards this generalization is to investigate the case for finitely generated modules over a p.i.d..

Now we impose the artinian property as our "finiteness condition".

Theorem 2.22 (Wedderburn–Artin). *The following are equivalent:*

1. *R is simple and left artinian.*
2. *R is (left) primitive and left artinian.*
3. *$R \cong \mathrm{End}_\Delta M$ where Δ is a division ring and $\dim_\Delta M < \infty$.*

Proof. (1) $\Longrightarrow$ (2) since simple implies primitive.

(2) $\Longrightarrow$ (3): let $\rho : R \hookrightarrow \mathrm{End}\, M$ be faithful irreducible, then $\Delta := R' = \mathrm{End}_R M$ is a division ring and $\rho(R) \subset R'' = \mathrm{End}_\Delta M$ is dense by Theorem 2.20. (So far this is exactly the content of Jacobson's density theorem.) It remain to prove $\dim_\Delta M < \infty$ to conclude the equality.

Suppose the contrary and let $x_i \in M$, $i \in \mathbb{N}$ be linearly independent over Δ. Then $I_j := \mathrm{ann}_R x_j$ is a left ideal of R and $I_{(n)} := \bigcap_{j=1}^n I_j$ is the left ideal annihilating all x_j, $1 \le j \le n$ for every $n \in \mathbb{N}$. Now $\rho(R) \subset \mathrm{End}_\Delta M$ is dense implies that for $0 \ne y \in M$ there exists $a \in R$ with

$$ax_1 = 0, \ldots, ax_n = 0, \quad ax_{n+1} = y \ne 0.$$

Hence $I_{(1)} \supset I_{(2)} \supset \ldots$ is an infinite strictly decreasing chain which violates the left artinian assumption.

(3) $\Longrightarrow$ (1): $\mathrm{End}_\Delta M$ is anti-isomorphic to a full matrix ring $M_n(\Delta)$ which is simple—since its ideals are of the form $M_n(I)$ where I is an ideal of Δ which must be 0. Also $\dim_\Delta M_n(\Delta) = n^2$, which shows that any left ideal chain has length at most n^2. In particular R is left artinian (and also left noetherian). □

3. Semi-simple artinian rings and their modules

To extend the classification to the (not yet defined) "semi-simple" case, the principal goal is to find the exact conditions on a ring to characterize it as a finite direct sum of matrix rings.

Definition 2.23. A left ideal I is nilpotent if $I^k = 0$ for some $k \in \mathbb{N}$. I is nil if every element $a \in I$ is nilpotent: $a^k = 0$ for some $k = k_a \in \mathbb{N}$.

It is clear that I is nilpotent $\Rightarrow$ I is nil $\Rightarrow$ I is quasi-regular. In general the reverse direction fails. However we have

Proposition 2.24. *Let R be a left artinian ring. Then $J(R)$ is nilpotent.*

In particular $J(R) =$ the largest nilpotent ideal $=$ the largest nil ideal $=$ the largest quasi-regular ideal.

PROOF. Let $J(R) =: J \supset J^2 \supset \ldots \supset J^k = J^{k+1} = \ldots =: P$. Then J is nilpotent if and only if $P = 0$. If $P \neq 0$ then we consider the set

$$S := \{\, I : \text{ a left ideal in } P \mid PI \neq 0 \,\}.$$

Then $P \in S$ since $PP = P^2 = J^{2k} = P \neq 0$. Let I be a minimal element in S. Then $PI \neq 0$ implies that there is a $b \in I$ with the left ideal $Pb \neq 0$. Since $Pb \subset I$ and $P(Pb) = P^2 b = Pb \neq 0$, we must have $I = Pb$. Then

$$b = zb$$

for some $z \in P$ and hence $(1 - z)b = 0$. But $z \in P \subset J$ implies that $1 - z$ is invertible. Hence we get $b = 0$ which is a contradiction.

The second statement follows from Proposition 2.15 that $J(R)$ is the largest quasi-regular ideal. □

Inspired by Proposition 2.2 on semi-primitivity, we introduce

Definition 2.25. A ring is semi-simple if it is a subdirect product of simple rings.

Lemma 2.26. *Let M be a left artinian module which is a subdirect product of irreducible modules M_i. Then M is a finite direct sum of some M_j's.*

PROOF. Let $f : M \hookrightarrow \prod M_i$ be a subdirect product. For each component we have $f_i : M \twoheadrightarrow M_i$. Let $N_i := \ker f_i$. Then $\bigcap N_i = \ker f = 0$. The artinian property implies that there is a minimal element among all finite intersections of N_i's. Denote this element by $N = N_1 \cap \ldots \cap N_m$. Then $N \subset N_i$ for all i for otherwise $N \cap N_i \subset N$ will be smaller. This then implies that $N \subset \bigcap N_i = 0$ and we get an embeeding

$$M \hookrightarrow \bigoplus_{i=1}^m M_i.$$

Since $\bigoplus_{i=1}^m M_i$ is completely reducible, we conclude that M is also completely reducible and equal to a sum $\bigoplus_{j \in J} M_j$ for some $J \subset \{\, 1, \ldots, m \,\}$. □

Proposition 2.27. *Let R be a semi-simple ring whose ideals satisfy the DCC condition (i.e. artinian for two-sided ideals), then $R = \bigoplus_{i=1}^n R_i$ where the ideals $R_i \subset R$ are themselves simple rings.*

Proof. In order to apply the above lemma, we need to introduce a mechanism to transform ideals into left modules.

Consider the ring $M(R) = R \times R^{\mathrm{op}} \hookrightarrow \operatorname{End} R_{\mathbb{Z}}$ which acts on R by

$$(a, b)r := arb.$$

Then submodules of ${}_{M(R)}R$ corresponds to ideals of R.

Now R is a semi-simple ring means that $R \subset \prod_i R_i$ as a subdirect product of simple rings R_i. The surjective map $R \twoheadrightarrow R_i$ gives R_i a left $M(R)$-module structure which is irreducible since $N \subset {}_{M(R)}R_i$ corresponds to an ideal of R_i which must then be trivial. Lemma 2.26 then implies that $R = \bigoplus_{i=1}^n R_i$. Notice that $R_i \subset R$ is an ideal (instead of a subring). □

Remark 2.28. Later (in next section) we will define the enveloping algebra $R^e = R \otimes_F R^{\mathrm{op}}$ for an F-algebra R to replace $M(R)$.

Now we are ready to prove the fundamental structure theorem for semi-simple left artinian rings:

Theorem 2.29 (Wedderburn–Artin, Jacobson)**.** *The following are equivalent:*

(1) *R is left artinian without non-trivial nilpotent ideals.*
(2) *R is left artinian and left semi-primitive.*
(3) *R is left artinian and semi-simple.*
(4) *${}_R R$ is completely reducible (necessarily a finite direct sum).*
(5) *$R \cong \bigoplus_{i=1}^n R_i$ with R_i simple left artinian, i.e. $R_i \cong \operatorname{End}_{\Delta_i} M_i$.*

Proof. (1) ⇔ (2): since they are both equivalent to left artinian and $J(R) = 0$ by Proposition 2.24.

(2) ⇔ (3): since the primitive/simple factors R_i appeared in the subdirect product are also left artinian (as indued from the surjective map $R \twoheadrightarrow R_i$), and then primitivity is equivalent to simplicity by Theorem 2.22.

(2) ⇔ (4): for ⇒, $0 = J(R) = \bigcap_{\text{max left}} I$ implies $R \hookrightarrow \prod_{\text{max left}} R/I$. Since R is left artinian, Lemma 2.26 then gives $R = \bigoplus_{i=1}^n R/I_i$.

For ⇐, let ${}_R R = \bigoplus M_i$ with $M_i \subset R$ being irreducible R-modules. This means that $M_i = I_i$ is a minimal left ideal of R. Then

$$1_R = e_1 + \ldots + e_k, \qquad e_i \in I_i.$$

In particular $a = ae_1 + \ldots + ae_k$ and $a \neq 0$ implies $ae_j \neq 0$ for some j. So R is semi-primitive.

Moreover, $R = I_1 + \ldots + I_k$ and then $R = \bigoplus I_j$ over a subset of $\{1, \ldots, k\}$. By reordering let this subset be $\{1, \ldots, m\}$. Then

$$_RR = \bigoplus\nolimits_{j=1}^{m} I_j \supset \bigoplus\nolimits_{j=1}^{m-1} I_j \supset \ldots \supset I_1 \supset 0$$

is a composition series for $_RR$. Hence R is left artinian (and noetherian).

Since (1)–(4) are all equivalent, it suffices to show (3) ⇒ (5) ⇒ (2).

(3) ⇒ (5): left artinian implies artinian (DCC on ideals), Proposition 2.27 then gives $R = \bigoplus_{i=1}^{s} R_i$ with the simple ring $R_i \subset R$ being an ideal. Now $R_iR_j \subset R_i \cap R_j = 0$ for $i \neq j$, hence any left ideal of R_i is also a left ideal of R and this shows that R_i is left artinian. The statement $R_i \cong \operatorname{End}_\delta M_i$ follows from the case for simple artinian rings in Theorem 2.22.

(5) ⇒ (2): simple implies primitive so $R = \bigoplus_{i=1}^{n} R_i$ is semi-primitive. Also R_i is left artinian for $1 \leq i \leq n$ implies R is left artinian. □

Remark 2.30. The above decomposition $R = \bigoplus_{i=1}^{n} R_i$ into simple components (ideals) is unique. In fact we only need to require that R_i are indecomposable ideals to get the uniqueness.

Next we study the structure of modules over semi-simple artinian rings.

Lemma 2.31. *Let R be simple (left) artinian, then R has a unique irreducible module up to isomorphism. A representative is given by a minimal left ideal. In particular all minimal left ideals are isomorphic.*

PROOF. Minimal left ideals $0 \neq I \subset R$ exist by the artinian property. By definition I is also an irreducible R-module. For any other irreducible R-module M, R is simple implies that $\operatorname{ann}_R M = 0$. In particular $Ix \neq 0$ for some $x \in M$. Schur's Lemma then implies $I \xrightarrow{\bullet x} M$ is an isomorphism. The argument holds for all choices of M, hence the uniqueness. □

Example 2.32. We recall that a maximal left ideal is a maximal element among all proper left ideals $I \subsetneq R$ while a minimal left ideal, which is the dual notion, is a minimal element among all non-zero left ideals $0 \subsetneq I$.

(1) For a division ring Δ, the maximal left is 0, the minimal left is Δ.

(2) One may see Lemma 2.31 directly by noticing that for $R = M_n(\Delta)$, Δ a division ring, $1 = \sum_{i=1}^{n} e_{ii}$ with e_{ii} being orthogonal idempotents. Hence $_RR = \bigoplus_{i=1}^{n} Re_{ii}$ and left ideals $I \subset R$ (submodule of $_RR$) are precisely partial sums: $J \subset \{1, \ldots, n\}$,

$$I_J = \bigoplus\nolimits_{j \in J} M_n(\Delta) e_{jj}$$

as a column spaces over Δ with indices from J.

Thus I_J is left maximal $\iff |J| = n-1$ and I is left minimal $\iff |J| = 1$. Notice that $R = I_J \oplus I_{J^c}$ and $R/I_J \cong I_{J^c}$. It is unusual that a quotient module can also be understood as a submodule. Nevertheless this does happen for simple (left) artinian rings.

We will see below that this holds for all semi-simple artinian rings by showing that all their modules are completely reducible.

(3) Consider the group algebra $R = F[G]$ for a finite group G over a field F such that $p = \operatorname{char} F$ divides $|G|$. R is artinian. Let $z = \sum_{g\in G} g$ then $hz = z = zh$ for all $h \in G$, hence $Fz \subset R$ is an ideal. Also $z^2 = z\sum g = |G|z = 0$ in R, hence Fz is a nilpotent ideal and R is not semi-simple. We will see later that $F[G]$ is indeed semi-simple if $p \not| \, |G|$.

Exercise 2.3. Show that the Weyl algebra $W = \mathbb{C}[x, \partial]$ of polynomial differential operators is simple but not left artinian. Show that there are more than one, in fact infinitely many, irreducible left W-modules.

Theorem 2.33. *If $g : R_1 \overset{\sim}{\to} R_2$ is a ring isomorphism between simple left artinian rings $R_i = \operatorname{End}_{\Delta_i} M_i$, then there is an isomorphism $s : M_1 \to M_2$ such that*

$$g(A) = sAs^{-1}. \qquad \textit{for } A \in R_1.$$

Moreover s is semi-linear in the sense that there is an isomorphism on the coefficients $\sigma : \Delta_1 \cong \Delta_2$ such that $s(ax) = \sigma(a)s(x)$ for $a \in \Delta_1$, $x \in M_1$.

Proof. M_1 is an irreducible left R_1-module. M_2 can also be viewed as an irreducible left R_1-module via the map $g : R_1 \to R_2$. That is, for $A \in R_1$, $y \in M_2$, $Ay := g(A)y$. Lemma 2.31 then implies that there is an R_1-module isomorphism $s : M_1 \to M_2$. This means

$$s(Ax) = g(A)s(x), \qquad \forall x \in M_1,$$

hence $g(A) = sAs^{-1}$. Now s induces a group isomorphism $\tilde{g} : \operatorname{End} M_1 \to \operatorname{End} M_2$ via $B \mapsto \tilde{g}(B) := sBs^{-1}$ which restricts to g on R_1. Also Δ_i can be identified as $C_{\operatorname{End} M_i}(R_i)$ with left scalar multiplications, hence $\tilde{g}$ restricts to $\sigma : \Delta_1 \cong \Delta_2$. The above formula for $A = a \in \Delta_1$ gives the result. □

Corollary 2.34. *Denote by G the group of semi-linear transformations on a finite dimensional vector space M over Δ, then there is a short exact sequence*

$$1 \to \Delta^\times \to G \xrightarrow{I} \operatorname{Aut}(\operatorname{End}_\Delta M) \to 1,$$

where $I(s)(A) := sAs^{-1}$.

PROOF. If $s \in \ker I$ then $sA = As$ for all $A \in \mathrm{End}_{\Delta} M$. But then s is an invertible scalar multiplication as expected. □

Theorem 2.35. *Let R be a left artinian ring.*

(1) *If R is semi-simple then any left/right R-module is completely reducible.*
(2) *There is an one to one correspondence between the isomorphism classes of irreducible left/right R-modules and the simple components of $R/J(R)$*

PROOF. First we assume that R is semi-simple. By Theorem 2.29 R is a finite direct sum of matrix rings over division rings. Hence the left case implies the right case by taking R^{op}.

For (1), Theorem 2.29 implies that $R = \sum_{i\in\Lambda} I_i$ where each I_i is a minimal left ideal (contained in some simple component of R). Let M be a R-module and $0 \neq x \in M$. Then $x \in \sum I_i x$ with $I_i x = 0$ or $I_i x \cong I_i$ by Schur's Lemma. Hence $M = \sum_{x\in M} Rx = \sum_{i\in\Lambda, x\in M} I_i x$ as a sum of irreducible modules. Hence M is completely reducible.

(2) follows from Lemma 2.31 since I_i is a minimal left ideal in a simple component R_i of R.

If R is only left artinian, then $\bar{R} := R/J(R)$ is left semi-primitive and left artinian since $J(\bar{R}) = \bigcap_{\text{max left}} \bar{I} = \overline{J(R)} = 0$. Then Theorem 2.29 shows that $\bar{R}$ is also semi-simple. Now (2) follows from the semi-simple case since any irreducible R-module M satisfies $J(R)M = 0$ and hence M is also an irreducible $\bar{R}$-module. □

Of course (1) fails if R is not semi-simple by Theorem 2.29. Hence in general there are interesting non-completely reducible modules for left artinian rings which is not semi-simple.

4. Finite dimensional central simple algebras

In order to classify simple artinian rings $R = M_n(\Delta)$, it is equivalent to classify division rings Δ. Notice that the center $F = C(R)$ of a simple ring is necessarily a field: for $c \in F \setminus \{0\}$, $Rc = cR \subset R$ is an ideal hence $Rc = R$ and $bc = cb = 1$ for some $b \in R$. Thus R and Δ are vector spaces over F.

In general a ring R is called an algebra over a commutative ring S (an S-algebra) if $S \subset C(A)$. R is central over S if $S = C(A)$. Thus every simple ring R is a central simple algebra (CSA) over its center field F.

Definition 2.36. Let R be a CSA$/F$. R is centrally finite if $\dim_F R < \infty$. In this case R is called a finite dimensional CSA. Otherwise it is centrally infinite.

Centrally finite implies artinian trivially, but not the converse: if R is artinian, $R \cong M_n(\Delta)$ for a division F-algebra Δ. Hence R is centrally finite $\iff \dim_F \Delta < \infty$.

Thus it is a good idea to start with some classical results on division F-algebras A with $n = \dim_F A < \infty$. For $a \in A$, $1, a, a^2, \ldots, a^n$ are linearly dependent over F, hence there is a polynomial relation $f(a) = 0$ for some $f(x) \in F[x]$. The monic minimal polynomial $f_a(x) \in F[x]$ exists since $F[x]$ is a p.i.d., also $f_a(x)$ is irreducible over F since A is a division ring.

Example 2.37. (1) If $F = \bar{F}$ (algebraically closed, e.g. $\bar{\mathbb{Q}}$, $\mathbb{C}$), then $f_a(x)$ is linear which implies $a \in F$. Hence $A = F$.

(2) Next we consider the case $F = \mathbb{R}$:

Theorem 2.38 (Frobenius)**.** *A finite dimensional division $\mathbb{R}$-algebra A is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.*

PROOF. If $F = \mathbb{R}$, then $\mathbb{R}[\sqrt{-1}]$ is algebraically closed implies $f_a(x) = x - a$ ($a \in \mathbb{R}$) or $f_a(x) = x^2 + px + q \in \mathbb{R}[x]$ with $p^2 - 4q < 0$ ($a \notin \mathbb{R}$).

In the second case we set $b = a + p/2 \notin \mathbb{R}$ and get

$$b^2 = r \in \mathbb{R}_{<0}, \qquad \text{where } r = p^2/4 - q.$$

Inspired by Hamilton's quaternion $\mathbb{H} = \mathbb{R} \oplus (\mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k)$, we define

$$A' := \{\, b \in A \mid b^2 \in \mathbb{R}_{\le 0} \,\}.$$

Claim 2.39. $A' \subset A$ is vector subspace over $\mathbb{R}$. Hence $A = \mathbb{R} \oplus A'$.

It is equivalent to showing that if $a, b \in A'$ are linearly independent then $a + b \in A'$. Let $a^2 = u \in \mathbb{R}$, $b^2 = v \in \mathbb{R}$, then $\exists p, q, r, s \in \mathbb{R}$ such that

$$(a+b)^2 = u + (ab + ba) + v = p(a+b) + q,$$
$$(a-b)^2 = u - (ab + ba) + v = r(a-b) + s,$$

which leads to $2(u+v) = (p+r)a + (p-r)b + (q+s)$.

But any $\mathbb{R}$-relation $a = tb + t'$ gives $a^2 = t^2b^2 + 2tt'b + t'^2$. $b \notin \mathbb{R}$ implies $t = 0$ ($a = t'$) or $t' = 0$ ($a = tb$). In both cases we get contradictions. Hence we must have $p = r = 0$ and then $(a+b)^2 = q \in \mathbb{R}$. Again $a + b \notin \mathbb{R}$ implies $q < 0$. Hence $a + b \in A'$ as claimed.

Now $A = \mathbb{R} \oplus A'$ and we have a positive definite quadratic form on A' defined by $Q(a) = -a^2$ for $a \in A'$. The associated symmetric bilinear form

$$B(a, b) := Q(a, b) - Q(a) - Q(b) = -(ab + ba)$$

is then an inner product on A'.

If $A \supsetneq \mathbb{R}$, pick $i \in A'$ with $i^2 = -1$. Then $A \supset \mathbb{R} \oplus \mathbb{R}i = \mathbb{C}$.

If $A \supsetneq \mathbb{C}$, pick $j \in (\mathbb{R}i)^{\perp}$ in A' with $j^2 = -1$. Then

$$0 = B(j,i) = -(ji + ij), \qquad \text{i.e. } ij = -ji.$$

Let $k := ij$, then $k^2 = ijij = -i^2j^2 = -1 \Rightarrow k \in A'$. Also $k \perp i, j$ since $B(k,i) = -(iji + iij) = 0$ and $(B,j) = 0$. So $A \supset \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k = \mathbb{H}$.

If $A \supsetneq \mathbb{H}$, then there exists $\ell \in A'$, $\ell^2 = -1$ and $\ell \perp i, j, k$. However, $\ell ij = -i\ell j = ij\ell \Rightarrow \ell k = k\ell$, which contradicts to $\ell k = -k\ell$, so $A = \mathbb{H}$. □

(3) For finite division rings the situation is even simpler:

Theorem 2.40 (Wedderburn)**.** *Any finite division ring A is a finite field.*

Proof. Let $F = C(A)$ be a finite field with $|F| = q$ and let $n = \dim_F A$. If $n = 1$ we are done. If $n > 1$ we will derive a contradiction.

Consider the conjugation group action of $G := A^{\times}$ on $A^{\times}$. The class equation reads as $q^n - 1 = q - 1 + \sum_i [A^{\times} : C(x_i)]$ where x_i are representatives of the conjugacy classes not from F.

Notice that $A_i := \{g \in A \mid gx_i = x_i g\}$ is a division subring $\subsetneq A$ with $A_i^{\times} = C(x_i)$. Let $n_i := \dim_F A_i < n$. Since A is also a vector space over A_i, $n = [A : A_i][A_i : F]$ implies $n_i \mid n$. Hence we have

$$q^n - 1 = q - 1 + \textstyle\sum_i (q^n - 1)/(q^{n_i} - 1)$$

with each summand being in $\mathbb{Z}[q]$. Moreover, $x^m - 1 = \prod_{d|m} \ell_d(x)$ where $\ell_d(x) \in \mathbb{Z}[x]$ is the irreducible cyclotomic polynomial for $x^d = 1$. Hence $\ell_n(q)$ divides the sum as well as $q^n - 1$, and then $\ell_n(q) \mid (q-1)$.

However, since $\ell_n(q) = \prod_w (q - w)$ where w's are primitive n-th roots of 1, we have $|q - w| > |q - 1|$ for all w. This leads to a contradiction. □

Historically the first centrally infinite division ring was discovered by Hilbert it in his study of independence of geometry axioms!

Exercise 2.4. Let F be a field and $\sigma \in \operatorname{Aut} F$, and $\Delta = F((x,\sigma))$ be the ring of σ-twisted formal Laurent series $\sum_{i=n}^{\infty} a_i x^i$ with $n \in \mathbb{Z}$ and $a_i \in F$, with the non-commutative product being defined by $xa = \sigma(a)x$.

(1) Show that Δ is a division ring. (2) Moreover, let $k = F^{\sigma}$ be the fixed field of σ. Then $C(\Delta) = k$ if σ has infinite order. In this case Δ is centrally infinite. Give an explicit example of such a (F,σ). (3) Show that $C(\Delta) = k((x^r))$ when σ has order $r < \infty$ and in this case Δ is centrally finite.

From now on we focus on the basic structural theorems on finite dimensional CSA$/F$. It is based on tensor product of F-algebras.

Let A, B be F-algebras with vector space base x_i and y_j respectively. Then the tensor product over F is simply

$$D := A \otimes_F B = (\bigoplus F x_i) \otimes_F (\bigoplus F y_j) \cong \bigoplus F\, x_i \otimes y_j,$$

with the product structure between $A \subset D$ and $B \subset D$, under the standard embedding $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$, defined by

$$ab = (a \otimes 1) \cdot (1 \otimes b) = a \otimes b = (1 \otimes b) \cdot (a \otimes 1) = ba.$$

So $D = AB = BA$. The following simple characterization is useful:

Proposition 2.41. *Let $A, B \subset D$ be sub F-algebras. Then $D \cong A \otimes_F B$ if*

1. *$ab = ba$ for all $a \in A$, $b \in B$.*
2. *There is a F-base x_i of A such that any $z \in D$ can be written uniquely as $z = \sum b_i x_i$ with $b_i \in B$.*

If $\dim_F D < \infty$, then (2) is satisfied by $D = AB$ and $[D : F] = [A : F][B : F]$.

PROOF. Define the F-bilinear map $A \times B \to D$ by $(a, b) \mapsto ab$. This then induces $A \otimes_F B \to D$, which is a ring homomorphism by (1). The map is indeed a bijection by (2). □

Corollary 2.42. (1) *For any F-algebra B, $M_n(F) \otimes_F B \cong M_n(B)$.*
(2) *$M_m(F) \otimes_F M_n(F) \cong M_{mn}(F)$.*

PROOF. For (1), take $D = M_n(B)$ with $A = M_n(F) \subset D$ and $B \hookrightarrow D$ under the embedding $b \mapsto \operatorname{diag}(b, \ldots, b) \in D$. Then both conditions in Proposition 2.41 are satisfied. Hence $A \otimes_F B = D$.

For (2), simply apply (1) to $B = M_n(F)$ and then use the isomorphism of block decompositions of matrices $M_m(M_n(F)) \cong M_{mn}(F)$. □

Definition 2.43. The algebra $A^e := A \otimes_F A^{\mathrm{op}}$ is called the enveloping algebra of A. If $A \hookrightarrow B$, then $B = {}_{A^e}B$ via $(\sum a_i \otimes b_i)y = \sum a_i y b_i$.

For $B = A$, this shows that submodules of ${}_{A^e}A$ are precisely ideals of A. Hence A is simple $\Longleftrightarrow$ ${}_{A^e}A$ is irreducible. Also $\operatorname{End}_{A^e} A = C(A)$.

For the last statement, let $f \in \operatorname{End}_{A^e} A$, then

$$f(acb) = f((a \otimes b)c) = (a \otimes b) f(c) = a f(c) b.$$

Hence $f(a) = a f(1) = f(1) a$ and we may identify f with $f(1) \in C(A)$.

The following two theorems are fundamental:

Theorem 2.44. *Let A be a finite dimensional CSA/F with $n = \dim_F A$. Then $A^e := A \otimes_F A^{\mathrm{op}} \cong M_n(F)$.*

Proof. Let $R = A^e$, then ${}_R A$ is irreducible and $R' := \operatorname{End}{}_R A = C(A) = F$. Since $n = \dim_F A < \infty$, the density theorem (Theorem 2.20) for F-algebras implies that for all $a'' \in R'' := \operatorname{End}{}_{R'} A = \operatorname{End}_F A$, there exists $a \in R = A^e$ with $a \mapsto a''$. That is, $A^e \twoheadrightarrow \operatorname{End}_F A \cong M_n(F)$. Since both A^e and $M_n(F)$ have the same dimension n^2, the map is an isomorphism. □

Theorem 2.45. *Let A be a f.d. CSA/F, $A \subset B$ as a F-subalgebra. Then*

(1) *$B \cong A \otimes_F C$ with $C = C_B(A)$.*
(2) *There is a bijection between ideals of C and ideals of B via*

$$I \subset C \mapsto AI \subset B.$$

(3) *$C(C) = C(B)$.*

Proof. (1): Theorem 2.44 $\Rightarrow$ A^e is simple $\Rightarrow$ ${}_{A^e}A$ is irreducible $\Rightarrow$

$$B = \bigoplus Ac_i$$

as A^e-modules (by Theorem 2.35). Since $(a \otimes 1)1_A = a = (1 \otimes a)1_A$ and $Ac_i \cong A$ as A^e-modules, by choosing c_i such that $c_i \mapsto 1_A$ we then have $ac_i = (a \otimes 1)c_i = (1 \otimes a)c_i = c_i a$. Moreover $ac_i = 0 \Rightarrow a = 0$.

If $c \in C := C_B(A)$, by writing $c = \sum a_i c_i$ with $a_i \in A$, the condition $ca = ac$ for all $a \in A$ is equivalent to $aa_i = a_i a$ for all i, that is $a_i \in C(A) = F$. This shows that $C = \bigoplus Fc_i$. Proposition 2.41 $\Rightarrow$ $B \cong A \otimes_F C = AC$.

(2) $I \subset C \Rightarrow AI \subset AC = B$. We claim that $AI \cap C = I$: if A has a F-base $1 = x_i, \ldots, x_n$, then $B = \bigoplus x_i C$ as a vector space over F. If $d = \sum x_i d_i \in AI \cap C$, $d_i \in I$, then by (1) the expression is unique even allowing $d_i \in C$. Since $d = x_1 d$ is such an expression, we thus have $d = d_1 \in I$.

To show that every I' ideal in B is of the form AI, we simple take $I := I' \cap C$. Since $I' = \sum Ad_i$ with $d_i \in C \cap I' = I$, we get $I' = AI$.

(3) $C(B) \subset C_B(A) = C \Rightarrow C(B) \subset C(C)$. Also $c \in C(C)$ commutes with all elements in $B = AC$. Hence $C(C) \subset C(B)$ as well. □

The condition on A is necessary: for $B = A \otimes_F C$, $C_B(A)$ contains C and $C(A)$. Hence $C(A)$ must be the ground field to conclude $C_B(A) = C$.

Corollary 2.46. *Let A be a f.d. CSA/F and C be an arbitrary F-algebra. Then $B = A \otimes_F C$ is central/simple if C is central/simple.*

Hence if $A_1, \ldots, A_r$ are f.d. CSA/F then $A_1 \otimes_F \ldots \otimes_F A_r$ is also a f.d. CSA/F.

The second statement in Corollary 2.46 allows us to introduce

Definition 2.47 (Brauer group $\mathrm{Br}(F)$). Let A, B be f.d. CSA$/F$. We say that $A \sim B$ if there are $m, n \in \mathbb{N}$ such that $M_m(A) \cong M_n(B)$. Since $A \cong M_p(\Delta)$, $B \cong M_q(\Delta')$, this is equivalent to $M_{mp}(\Delta) \cong M_{nq}(\Delta')$, hence equivalent to $\Delta \cong \Delta'$ since divisions are local rings (as shown in last chapter).

It is clear that $\sim$ is an equivalence relation, namely $A \sim B \Rightarrow B \sim A$ and $A \sim B \sim C \Rightarrow A \sim C$. Hence we may define the abelian group

$$\mathrm{Br}(F) := (\{\text{ isomorphism classes of f.d. CSF}/F\}, \otimes_F)/\sim,$$

with $1 = [F] = [M_n(F)]$ for all $n \in \mathbb{N}$ and $[A]^{-1} = [A^{\mathrm{op}}]$ (by Theorem 2.44).

Hence Example 2.37 implies $\mathrm{Br}(\bar{F}) = \{1\} = \mathrm{Br}(\mathbb{F}_q)$ and $\mathrm{Br}(\mathbb{R}) = \langle [\mathbb{H}] \rangle \cong \{\pm 1\}$. Notice that $\mathbb{C}$ is not $\mathbb{R}$-central simple since $C(\mathbb{C}) = \mathbb{C}$.

Remark 2.48. Later we will show that for any p-adic number field $F = \mathbb{Q}_p$, $\mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z}, +)$. This is part of the "local class field theory".

For "global class field theory", there is a Hasse exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where v runs through all finite places $v = p$ (primes) as well as the infinite place $v = \infty$ ($\mathbb{Q}_\infty := \mathbb{R}$). Here $[A] \mapsto [A_v] := [A \otimes_{\mathbb{Q}} \mathbb{Q}_v]$ is non-trivial only for a finite set of places. Also $\mathrm{Br}(\mathbb{R})$ is identified as $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

Similar statements hold for a finite extension field $K/\mathbb{Q}$. After we defined the Galois cohomology, we will interprete Hilbert's theorem 90 in terms of H^1 and show that the Brauer group is exactly H^2.

The first statement in Corollary 2.46 leads to

Definition 2.49. Let A be a f.d. CSA$/F$ and E/F an extension field. Then $A_E := A \otimes_F E$ is f.d. CSA$/E$. E is called a splitting field of A If $A_E \cong M_n(E)$.

Example 2.50. Consider the standard embedding $\mathbb{H} \hookrightarrow M_2(\mathbb{C})$ of rings

$$a + bi + cj + dk = z + wj \mapsto \begin{pmatrix} a+bi & c+di \\ -c+d_i & a-bi \end{pmatrix} = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}.$$

It follows that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$.Notice that $\mathbb{C}$ is a maximal subfield of $\mathbb{H}$.

Proposition 2.51. *Let A, B be CSA/F and E an extension field of F. Then*

(1) *If E splits A and B then it splits A^{op} and $A \otimes_F B$.*
(2) *If $A = M_n(B)$ then E splits A if and only if E splits B.*

PROOF. (1) follows from the definitions easily. For (2) we only need to prove the direction ⇒: we have

$$A_E \cong M_n(B_E) \cong M_n(M_s(\Delta)) \cong M_{ns}(\Delta)$$

where Δ is a central division algebra over E.

If E splits A then $A_E \cong M_m(E)$. Hence $M_{ns}(\Delta) \cong M_m(E)$ which implies that $m = ns$ and $\Delta = E$ since Δ and E are local rings. □

In particular, E splits $A = M_n(\Delta)$ if and only if E splits the division F-algebra Δ. From this we see that splitting fields always exist. Indeed $E = \bar{F}$ is a splitting field since the only division algebra over $\bar{F}$ is $\bar{F}$ itself. Hence

$$A_{\bar{F}} = M_n(\Delta_{\bar{F}}) \cong M_n(M_s(\bar{F})) \cong M_{ns}(\bar{F}).$$

However $\bar{F}$ is generally an infinite extension. Much better results hold:

Theorem 2.52. *Let Δ be a finite dimensional division F-algebra. A finite dimensional extension field E of F splits Δ if and only if E is a subfield of $A := M_r(\Delta)$ for some r such that $C_A(E) = E$.*

In particular, taking $r = 1$ shows that any maximal subfield E of Δ is a splitting field for Δ. (There could be infinitely many of them, e.g. $\mathbb{C} \hookrightarrow \mathbb{H}$.)

We only give the proof that a maximal subfield E of Δ splits Δ. The general case is similar and is left to the readers.

First we noticed that $\Delta = \operatorname{End}_{\Delta^{\mathrm{op}}}\Delta$ consists of F-linear maps commute with Δ^{op}. Consider $R := \Delta_E^{\mathrm{op}} = \Delta^{\mathrm{op}} \otimes_F E$ which acts on Δ as a faithful irreducible R-module. $R' := \operatorname{End}_R\Delta \subset \operatorname{End}_F \Delta$ consists of F-linear maps which commute with R. Thus $R' = C_\Delta(E) = E$ since E is a maximal subfield. This implies $R'' := \operatorname{End}_{R'}\Delta = \operatorname{End}_E \Delta \cong M_n(E)$ where $n = \dim_E \Delta$. The density theorem for F-algebras then implies that

$$\Delta^{\mathrm{op}} \otimes_F E = R \cong R'' = M_n(E).$$

Remark 2.53. In particular, $[\Delta : F][E : F] = n^2[E : F] \Rightarrow [\Delta : F] = n^2$. Since $n = [\Delta : E]$, then $[E : F] = [\Delta : F]/[\Delta : E] = n^2/n = n$ as well. Thus the phenomenon occurs in the special case $\Delta = \mathbb{H}$ is really a general one.

There are other interesting basic results on CSA. All of them are derived from consideration of A^e-modules and the density theorems as above. We mention only two of them and leave the proofs as exercises:

Exercise 2.5. (1) (Skolem–Noether Theorem) show that any automorphism of a f.d. CSA is inner. (2) Let $A \subset B$ be a semi-simple sub-algebra of a f.d. CSA B, then $C_B(C_B(A)) = A$.