Semisimple algebras and Maschke's Theorem

~ I Definition

Def$^{\underline{n}}$: A ring A is called semisimple if every finitely generated A-module is semisimple.

Theorem 1: A is semisimple if and only if the regular module A is semisimple. Furthermore, in this case A is both Artinian and Noetherian.

Proof: If A is semisimple then the regular module is semisimple, by def$^{\underline{n}}$. Conversely, if the regular module is semisimple then any free module is semisimple. Hence any finitely gen^d module M is semisimple, as it is a quotient of a finite rank free module $\bigoplus_{i=1}^{r} A \to M$. [Prop 9, Simples].

In any case any finitely generated semisimple module is necessarily a finite sum of simples, and thus admits a composition series. In particular, A itself admits a composition series, and is therefore both Artinian and Noetherian [Thm 7 & Lemma 10, Fin dim]. ∎

— I.2 Semisimplicity via proj/inj

Def$^{\underline{n}}$: An A-module M is called projective (resp. injective) if the functor $\mathrm{Hom}_A(M,-)$ (resp. $\mathrm{Hom}_A(-,M)$) preserves exact sequences.

Proposition 3: For an Artinian + Noetherian ring A, TFAE:

a) A is semisimple,

b) All finitely generated A-modules are projective.

c) All finitely generated A-modules are injective.

Let's take a second to think about this. For any exact sequence $0 \to L' \xrightarrow{i} N \xrightarrow{\pi} L \to 0$ and A-mod M, we have the <u>inclusion</u> of $\mathbb{Z}$-mod

$$i_* : \mathrm{Hom}_A(M, L') \to \mathrm{Hom}_A(M, N)$$
$$f \longmapsto i \circ f$$

and the image of that inclusion is the kernel of the map $\pi_* : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,L)$.

This is to say, we obtain a left exact sequence

$$0 \to \mathrm{Hom}_A(M, L') \xrightarrow{i_*} \mathrm{Hom}_A(M, N) \xrightarrow{\pi_*} \mathrm{Hom}_A(M,L)$$

for free.

Similarly, the functor $\mathrm{Hom}_A(-,M)$ applied to such an exact sequence produces a left exact sequence

$$0 \to \mathrm{Hom}_A(L,M) \xrightarrow{\pi^*} \mathrm{Hom}_A(N,M) \to \mathrm{Hom}_A(L',M).$$

$$f \mapsto f\pi, \quad f' \mapsto f'\circ i = f'|_{L'}.$$

So to say M is <u>projective</u> is to say that any surjection $\pi : N \to L$ and arbitrary $f : M \to L$ admits some $\tilde{f} : M \to N$ which completes a diagram

$$\begin{tikzcd} & M \arrow[dl, dashed, "\tilde{f}"'] \arrow[d, "f"] \\ N \arrow[r] & L \end{tikzcd}.$$

To say M is <u>injective</u> says that every inclusion $i : L' \to N$ and map $g : L' \to M$ admits some $\tilde{g} : N \to M$ for which we have a diagram

$$\begin{tikzcd} L' \arrow[r] \arrow[d, "g"'] & N \arrow[dl, dashed, "\tilde{g}"] \\ M & \end{tikzcd}.$$

Example: The regular module A is projective over A.

Example: $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Example: The regular module $k[x]/(x^n)$ is injective over $k[x]/(x^n)$.

Proof of prop 3: (a) $\Rightarrow$ (b) and (c) If A is semisimple then any exact sequence

$$0 \to L' \to N \to L \to 0$$

splits. We can then use the implied splitting maps $s: L \to N$ and $t: N \to L'$ to lift any map $f: M \to L$ to a map $\tilde{f} = sf: M \to N$ and any map $g: L' \to M$ to $\tilde{g} = gt: N \to M$. So we see any A-module M is both projective and injective in this case.

(b) $\Rightarrow$ (a) If all modules are projective, take any module N and a surjection $\pi: N \to L$ onto simple L. Then we can lift the identity $id: L \to L$ along π to get a map $s: L \to N$ with $\pi s = id_L$, and hence split N as

$$N = L \oplus N' \text{ for } N' = \ker(\pi).$$

Noting that $\mathrm{length}(N') = \mathrm{length}(N) - 1$, we see by induction on the length that N is semisimple. Since N was chosen arbitrarily, we find that A is semisimple. $\blacksquare$

(c) $\Rightarrow$ (a) Similar.

~ II. Examples of semisimple algebras: Maschke's Thm

Take k a field.

Let G be a (finite) group, and consider the group alg. kG. For any G-rep M (over k) we define the invariants

$M^G = \{ m \in M : g \cdot m = m \text{ at all } g \in G \} \subseteq M.$

Obviously any map of G-reps preserves invariants, as

$g \cdot f(m) = f(g \cdot m) = f(m)$ whenever $m \in M^G$

and $f : M \to N$ is a map of G-reps. Hence we have the invariants functor

$-^G : kG\text{-mod} \to \mathrm{Vect}_k.$

For $k = k_{triv}$ the trivial rep, we have

$k = k^G$ so that any module map $k \to M$ has image in the G-invariants $M^G \subseteq M$.

Lemma 4: For any group G and field k, and kG-module M, there is a natural isomorphism

$ev_1 : \mathrm{Hom}_G(k, M) \xrightarrow{\sim} M^G, \quad f \mapsto f(1).$

Proof: Apparent. $\blacksquare$

~ II.½ A little aside

For any group G, and G-reps M and N, we have the G-action on $\mathrm{Hom}_k(M,N)$ given by

$$g\cdot f = \{ m \longmapsto g f(g^{-1}\cdot m) \}.$$

This gives the vector space $\mathrm{Hom}_k(M,N)$ the structure of a G-rep / kG-module.

Lemma 3: The invariant $\mathrm{Hom}_k(M,N)^G$ are precisely the kG module maps

$$\mathrm{Hom}_G(M,N) = \mathrm{Hom}_k(M,N)^G.$$

Proof: If $f: M \to N$ is a kG-module map then $gf(g^{-1}\cdot m) = gg^{-1}\cdot f(m) = f(m)$ at all m in M. Thus f is G-invariant in $\mathrm{Hom}_k(M,N)$. Conversely if $f: M \to N$ is G-invariant then at all m in M and g in G we have

$$f(g\cdot m) = g\, f(g^{-1}(g\cdot m)) = g f(m).$$

So f is a kG-module map. $\blacksquare$

Corollary 4: For any finite group G, and field

k, kG is a semisimple ring if and only if the trivial module $k = k_{triv}$ is projective.

Proof: If kG is semisimple then k is projective, by Proposition 3. Conversely, suppose k is projective. Then the invariants functor $Hom_G(k, -) \cong -^G$ preserves exact sequences. Hence for an arbitrary exact sequence

$$0 \to L' \to N \to L \to 0$$

and arbitrary M, we have the exact sequence

$$0 \to Hom_k(M, L') \to Hom_k(M, N) \to Hom_k(M, L) \to 0$$

(since all vector spaces are proj over k, or whatever) and applying invariants we see that the sequence

$$0 \to Hom_G(M, L') \to Hom_G(M, N) \to Hom_G(M, L) \to 0$$

is exact. Thus, M is projective. Since M was chosen arbitrarily we find that kG is semisimple, by Proposition 3. ∎

— II 2/3 Maschke's Theorem

Theorem (Maschke): Let G be a finite group and k be a field. If $char(k) \nmid |G|$, then

kG is a semisimple ring/algebra.

Proof: Since $|G|$ is a unit in k we have the element

$$e_{triv} = \frac{1}{|G|} \sum_{g \in G} g \quad \in kG.$$

Note that for any group element $h \in G$,

$$h \cdot e_{triv} = e_{triv} \qquad (*)$$

and for any invariant vector $v \in V^G$ in a G-rep V we have $e_{triv} \cdot v = \frac{1}{|G|} \sum_g v = v$.

Now, suppose we have a surjective kG-module map $\pi : N \to L$ and a map of kG-mods $f : k = ke_{triv} \to L$.

Take $n' \in N$ an arbitrary preimage of $f(1)$ along π, and let $n = e_{triv} \cdot n'$. Then by $(*)$ we have $g \cdot n = g \cdot e_{triv} n' = n$ at all g in G, giving $n \in N^G$, and also

$$\pi(n) = \pi(e_{triv} \cdot n') = e_{triv} \cdot \pi(n')$$
$$= e_{triv} f(1) = f(1).$$

So n is a G-invariant lift of $f(1)$, and the map of kG-modules

$$\tilde{f} : k \to N, \quad \tilde{f}(1) = n$$

completes a diagram

$$\begin{tikzcd} & k \arrow[dl, "\tilde{f}"'] \arrow[d, "f"] \\ V \arrow[r, "\pi"] & W \end{tikzcd}.$$

So we see that the trivial module rep k is projective over kG, and hence that kG is semisimple by Corollary 4. ∎

HW: The converse to Maschke is also true. If $\mathrm{char}(k) \mid |G|$ then kG is <u>not</u> semisimple.

Example: For any finite group G,

$\mathbb{Q}G$, $\mathbb{R}G$, $\mathbb{C}G$

are all semisimple algebras. So, like,

$\mathbb{Q}\,\mathbb{Z}/p\mathbb{Z}$ is semisimple

$\mathbb{Q}S_n$ is semisimple, $\mathbb{C}S_3$ is semisimple

etc.

Ex: $\mathbb{F}_p\,\mathbb{Z}/n\mathbb{Z}$ is nonsemisimple if and only if $p \mid n$.

$\overline{\mathbb{F}}_5 D_7$ is semisimple. $\overline{\mathbb{F}}_7 D_7$ is nonsemisimple.

<u>Question</u>: For S_n, for example, can we classify S_n-reps over $\mathbb{C}$ up to isomorphism?

Can we say how many of them there are?

Can we determine the dimensions that occur?

~ III Artin-Wedderburn

Lemma 5: For any division algebra D,

i) D^{op} is also a division algebra

ii) There is $Z(D)$-algebra isomorphism
$$M_n(D) \xrightarrow{\sim} M_n(D^{op})^{op}.$$

Proof: (i) Apparent. (ii) Take the transpose. ∎

Proposition 6: For any semisimple module
$M \cong \bigoplus_{i=1}^{r} n_i L_i$ over a k-alg A
with the L_i distinct, and $D_i = \mathrm{End}_A(L_i)$,
there is an isomorphism of k-algebras
$$\prod_{i=1}^{r} M_{n_i}(D_i) \xrightarrow{\sim} \mathrm{End}_A(M).$$

Proof: From any explicit choice of module $\cong$
$f: \bigoplus_i n_i \cdot L_i \xrightarrow{\sim} M$ we get an alg iso
$$\mathrm{Ad}_f : \mathrm{End}_A(M) \xrightarrow{\sim} \mathrm{End}_A(\textstyle\bigoplus_i n_i L_i)$$
$$\xi \longmapsto f \circ \xi \circ f^{-1}.$$
So we may assume $M = \bigoplus_{i=1}^{r} n_i \cdot L_i$. Now
for $M_i = n_i \cdot L_i \subseteq M$ any module map
$\xi : M \to M$ sends M_i into M_i,

by Schur's Lemma say, so that

$$\xi = \begin{bmatrix} \xi_1 & & 0 \\ & \ddots & \\ 0 & & \xi_r \end{bmatrix} : M = \bigoplus_{i=1}^r M_i \to M = \bigoplus_{i=1}^r M_i$$

for $\xi_i = \xi | M_i$. So we see

$$\mathrm{End}_A(M) = \prod_{i=1}^r \mathrm{End}_A(M_i). \quad (*)$$

At fixed M_i now take

$$i_t : L_i \to M_i \quad \text{and} \quad p_t : M_i \to L_i$$

the inclusion and projection onto the t-th copy of L_i in the given decomp $M_i = \bigoplus_{j=1}^{n_i} L_i$ we have

$$\xi = \sum_{s,t} \xi_{st}, \quad \xi_{st} = i_s p_s \xi i_t p_t$$

since

$$\mathrm{id}_{M_i} = \sum_t i_t p_t.$$

We note that composition satisfies

$$\xi' \circ \xi = \sum_{s,t,u} \xi'_{su} \circ \xi_{ut}.$$

Hence, for

$$\bar{\xi}_{st} = p_s \xi i_t \in \mathrm{End}_A(L_i) = D_i$$

we get an explicit algebra isomorphism

$$\mathrm{End}_A(M_i) \xrightarrow{\cong} M_{n_i}(D_i)$$
$$\xi \longmapsto [\bar{\xi}_{ij}].$$

Taking this onto (*) gives
$$\mathrm{End}_A(M) \cong \prod_{i=1}^{r} M_{n_i}(D_i). \blacksquare$$

Theorem (Artin-Wedderburn Thm): For any semisimple k-algebra A, there is an isom of k-algs
$$A \xrightarrow{\sim} \prod_{i=1}^{r} M_{n_i}(D_i)$$
for some division algebras D_i.

Proof: Write $D_i = \mathrm{End}_A(L_i)^{op}$ for a complete list of simple A-mods $L_1, \dots, L_r$, up to isomorphism, and $n_i = [L_i : A]$, to get
$$A \underset{HW}{\xrightarrow{\sim}} \mathrm{End}_A(A)^{op} \underset{\text{Prop } 6}{\xrightarrow{\sim}} \prod_{i=1}^{r} M_{n_i}(D_i^{op})^{op}$$
$$\underset{\text{Lem } 5}{\xrightarrow{\sim}} \prod_{i=1}^{r} M_{n_i}(D_i). \blacksquare$$

Remark: Recall that for any division ring D the corresponding matrix algebra $M_n(D)$ is semisimple, for any n. Hence so is a product $\prod_{i=1}^{n} M_n(D_i)$. So the Artin-Wedderburn classifies semisimple algs completely, up to a classification of div. algs.

Classification of division algebras, in general, is an interesting problem, which is impossible to achieve in general. (E.g. Contains the classification of all fields.)

Corollary 7: Suppose $k = \bar{k}$ is alg closed field, and that A is a finite-dimensional, semisimple k-algebra. Then there is a k-algebra isomorphism

$$A \xrightarrow{\sim} \prod_{i=1}^{r} M_{n_i}(k). \quad (*)$$

Proof: Each division alg D_i appearing in the AW decomp

$$A \cong \prod_i M_{n_i}(D_i)$$

is a finite-dim div. alg over k. Since there are no such div algs besides k itself, by alg closure [Lemma 3, Simples], we conclude

$$A \cong \prod_i M_{n_i}(D_i).$$

∎

Note that, since we know the unique simple $M_n(k)$-module is of dim n, namely $\dim_k(k^n) = n$, we see that in (*)

$$\{n_1, \ldots, n_r\} = \{\dim_k(L_1), \ldots, \dim_k(L_r)\},$$

where we run across all distinct simples L_i for A.

Example: We saw in HW that S_3 has two 1-dim reps over $\mathbb{C}$, and one 2-dim simple rep. Since

$$\dim S_3 = 6 = 1 + 1 + 2^2$$

this gives the AW decomp

$$\mathbb{C}S_3 \cong \mathbb{C} \times M_2(\mathbb{C}) \times \mathbb{C}$$

You can deduce from AW that this isomorphism can be realized via the action maps

$$\mathbb{C}S_3 \xrightarrow{\text{action}} \begin{matrix} \mathrm{End}_{\mathbb{C}}(\mathbb{C}_{\mathrm{triv}}) \\ \mathrm{End}_{\mathbb{C}}(\mathcal{L}(2)) \\ \mathrm{End}_{\mathbb{C}}(\mathbb{C}_{\mathrm{sign}}) \end{matrix}.$$

§ IV Splitting division algebras

Let me record a fundamental Thm which we don't prove. Below we employ the following basic construction: Given a comm. ring map $k \to K$ and a k-alg A, $K \otimes_k A$ inherits a unique K-alg structure for which the inclusion $K \to K \otimes_k A$, $c \mapsto c \otimes 1$, is the unit map and $A \to K \otimes_k A$, $a \mapsto 1 \otimes a$, is a ring map. We have the expected multiplication on $K \otimes_k A$

$$\left(\sum_i c_i \otimes a_i\right) \cdot \left(\sum_j c_j' \otimes a_j'\right) = \sum_{ij} c_i c_j' \otimes a_i a_j'.$$

Theorem 8: Let D be a division algebra which is finite over its center $k = Z(D)$.

a) For any field extension $k \to K$ the base change $K \otimes_k D$ is a semisimple K-algebra.

b) $\bar{k} \otimes_k D \cong M_n(\bar{k})$, as a $\bar{k}$-alg. for some n.

c) There is a finite field extension $k \to K_0$ for which $K_0 \otimes_k D \cong M_n(K_0)$, as a K_0-alg.

Proof: (a) We take for granted. (b) Follows by (a) and Artin-Wedderburn for finite semisimple $\bar{k}$-alg. (c) We have for each matrix element

$$E_{ij} \in \bar{k} \otimes_k D \cong M_n(\bar{k})$$

$$E_{ij} = \sum_{t=1}^{m_{ij}} \alpha_t^{ij} \otimes d_t$$

for some $\alpha_t^{ij} \in \bar{k}$ and d_t in D. Take $K_0 = k(\alpha_t^{ij} : 1 \leq i, j \leq n, t \leq m_{ij})$ to get

$$K_0 \otimes_k D \cong M_n(K_0) \subseteq M_n(\bar{k}). \quad \blacksquare$$

Rem: We need the assumption $k = Z(D)$ for (a)–(c) to hold.

Any field extension $k \to K$ st $K \otimes_k D \cong M_n(K)$ is called a splitting field for D.

Corollary 9: If D is finite over its center $k = Z(D)$, then $\dim_k D = n^2$ for some $n \in \mathbb{Z}_{>0}$.

H/W

1. Let P be projective, and suppose that P decomposes as $P \cong M \oplus M'$. Prove that M and M' are also projective.
(b) Prove that a module M is projective if and only if M appears as a summand of a free module $M \oplus M' \cong \bigoplus_{\lambda \in \Lambda} A$.

2. Let $H \to G$ be an inclusion of groups. Prove that, for k any field (or comm ring), kG is a projective module over kH. Specifically, kG is free over kH.

3. Let G be a group and $H \leq G$ be a subgroup. If kH is nonsemisimple, prove that kG is nonsemisimple as well.

4. Let k be a field of characteristic $p > 0$. Prove that $k\mathbb{Z}/p\mathbb{Z}$ is nonsemisimple. You can do this for example, by producing a non-split extension

$$0 \to k \to V \to k \to 0$$

of the trivial module $k = k_{triv}$.

5. Let G be a finite group, and suppose $\mathrm{char}(k) \mid |G|$. Prove that kG is nonsemisimple.

6. Provide an example of the following: D is a finite dimensional division algebra over a field k — so, possibly a finite field extension for example — for which the base change $\bar{k} \otimes_k D$ is nonsemisimple. [Hint: We say in this case that D is not separable over k.]

(