III.C. Semisimple algebras

In this section we will discuss two principal examples of semisimple rings, which both come from the world of (associative, finite-dimensional) algebras over a field $\mathbb{F}$: group rings and central simple algebras. The main things to remember here from [**Algebra I**, §V.A] are that:

- an $\mathbb{F}$-algebra is a ring A together with an embedding of $\mathbb{F}$ in its center $C(A)$;
- this makes A into an $\mathbb{F}$-vector space, so we can speak of $\dim_{\mathbb{F}}(A)$;
- algebra ideals (left, right, or 2-sided) are the same as ring ideals since multiplication by $\mathbb{F}$ is already included in multiplication by A; and
- algebra homomorphisms are more specific than ring homomorphisms (unless $\mathbb{F}$ is just the prime field), since they intertwine the embedding of (equiv. scalar multiplication by) $\mathbb{F}$.

An algebra is **semisimple** if the underlying ring is.

III.C.1. DEFINITION. Let G be a finite group, and R a ring. The **group ring** of G over R is

$$R[G] := \{\textstyle\sum_{\text{finite}} r_i[g_i] \mid r_i \in R,\, g_i \in G\},$$

with products defined by $r[g] \cdot r'[g'] := rr'[gg']$. The **group algebra** of G over a field $\mathbb{F}$ is simply the special case where $R = \mathbb{F}$, regarded as an $\mathbb{F}$-algebra.

III.C.2. MASCHKE'S THEOREM. *Let R be a ring, and G a finite group. Then $R[G]$ is semisimple $\iff$ R is semisimple and $|G|$ is invertible in R.*

PROOF. ($\underline{\Longrightarrow}$): Given a ring homomorphism $\theta\colon \mathcal{S} \to \mathcal{R}$, if $\mathcal{S}$ is semisimple then so is $\theta(\mathcal{S})$. (Simply regard $\theta(\mathcal{S}) \cong \mathcal{S}/\ker(\theta)$ as a quotient module of ${}_{\mathcal{S}}\mathcal{S}$, and invoke III.A.3 and III.A.7.) Applying this to the *augmentation* homomorphism

$$\begin{aligned} \epsilon\colon R[G] &\twoheadrightarrow R \\ \textstyle\sum r_i[g_i] &\mapsto \textstyle\sum r_i, \end{aligned}$$

we get semisimplicity of R from that of $R[G]$.

Now suppose $p \big| |G|$, and write $S := R[G]$. I claim that $p \in R^*$ (which will finish this direction). By Cauchy's theorem, there exists $g \in G$ of order p; write $H := \langle g \rangle$ and $s := [1] - [g] \in S$.

Consider the principal left ideal $(s) := Ss$; by semisimplicity of ${}_SS$, there is another left ideal $I \subset S$ with ${}_SS = (s) \oplus I$. Hence we may write $1 = e + \imath$ with $e \in (s)$ and $\imath \in I$, so that for any $t \in (s)$ we have $t = te + t\imath \implies t\imath = t - te \in (s) \cap I = \{0\} \implies t = te$. Taking $t := e$, this gives $e = e^2$ (e is idempotent); taking $t := s$, we get $(s) = (se) \subset (e) \subset (s) \implies (s) = (e)$.

So we have $e = xs$ and $s = ye = ye^2 = ye \cdot e = s \cdot xs = sxs$ hence

$$(1 - sx)s = 0.$$

Writing $\sigma := 1 - sx = \sum r_\gamma [\gamma]$, this equation says $\sigma \cdot ([1] - [g]) = 0$, i.e. $\sigma \cdot [g] = \sigma$. So the coefficients r_γ are constant on left cosets of H, and $\sigma = \sum_{\gamma H \in G/H} r_\gamma [\gamma] \sum_{j=0}^{p-1} [g^j] =: \sigma_0 \sum_{j=0}^{p-1} [g^j]$. The augmentation gives

$$\epsilon(\sigma_0)p = \epsilon(\sigma) = \epsilon(1 - ([1] - [g])x) = 1 - 0\sigma(x) = 1$$

in R, which makes p a unit as claimed.

$\underline{(\impliedby)}$: Let V be an $S\,(:= R[G])$-module, with submodule W. This is trivially also an R-submodule since $R \subset S$ is a subring. Since R is semisimple, we have ${}_RV = W \oplus W'$ and a corresponding projection $f_W \in \mathrm{Hom}_R(V, W)$, with $f_W|_W = \mathrm{id}_W$. Namely, take f_W to send $v = w + w' \mapsto w$. But W' [resp. f_W] may not be an S-submodule [resp. S-module homomorphism]. How to fix this?

Well, we define a new map $\varphi_W \colon V \to W$ by "averaging" over G:

$$\varphi_W(v) := \frac{1}{|G|} \sum_{g \in G} [g^{-1}].f_W([g].v). \tag{III.C.3}$$

(This is of course where we use $|G| \in R^*$.) Clearly the RHS belongs to W, and

$$\varphi_W(w) = \tfrac{1}{|G|} \textstyle\sum_{g \in G} [g^{-1}].f_W([g].w) = \tfrac{1}{|G|} \sum_{g \in G} [g^{-1}].[g].w = w$$

shows that $\varphi_W|_W = \mathrm{id}_W$ and φ_W is surjective. Reindexing by $\eta = g\gamma$ ($g^{-1} = \gamma\eta^{-1}$) to write

$$\begin{aligned}\varphi_W([\gamma].v) &= \tfrac{1}{|G|}\textstyle\sum_{g\in G}[g^{-1}].f_W([g\gamma].v) = \tfrac{1}{|G|}\sum_{\eta\in G}[\gamma\eta^{-1}].f_W([\eta].v)\\ &= [\gamma].\varphi_W(v),\end{aligned}$$

we see that φ_W is also an S-module homomorphism.

So $\ker(\varphi_W)$ is a left S-submodule of V. If $v \in W \cap \ker(\varphi_W)$, then $v = \varphi_W(v) = 0$; so $W \cap \ker(\varphi_W) = \{0\}$. By writing $v = \varphi_W(v) + (v - \varphi_W(v))$, we see that $W + \ker(\varphi_W) = V$. Conclude that $V = W \oplus \ker(\varphi_W)$. Since $W \subset V$ was arbitrary, S is semisimple. □

So if R is semisimple and $|G| \in R^*$, Artin-Wedderburn (Theorem III.B.4) now produces a decomposition

$$_{R[G]}R[G] = \oplus_{i=1}^{r} V_i^{\oplus n_i} \tag{III.C.4}$$

in which the $\{V_i\}$ constitute all of the simple left $R[G]$-modules. Moreover, setting $D_i := \mathrm{End}_{R[G]}(V_i)^{\mathrm{op}}$, we have $V_i \cong D_i^{\oplus n_i}$ (as D_i-modules). Passing to the case where $R = \mathbb{F}$ is a field, (III.C.4) becomes the **regular representation** of G on the $|G|$-dimensional $\mathbb{F}$-vector space $\mathbb{F}[G]$ and we have the

III.C.5. COROLLARY. *For a finite group G and field $\mathbb{F}$ with* $\mathrm{char}(\mathbb{F}) \nmid |G|$, *the regular representation of G over $\mathbb{F}$ decomposes as in* (III.C.4), *where the $\{V_i\}$ are all of the irreducible representations of G over $\mathbb{F}$. Their multiplicities n_i match their ranks over the $\mathbb{F}$-division algebras D_i. In particular, if $\mathbb{F}$ is algebraically closed, then all $D_i = \mathbb{F}$ and $n_i = \dim_{\mathbb{F}} V_i$.*

PROOF. Everything follows from the discussion except the last statement, which holds because algebraically closed fields have no nontrivial finite-dimensional division algebras over them (which was proved in [**Algebra I**, V.B.5]). □

Central simple algebras.

Wedderburn's original proof of Theorem III.B.4 was for simple algebras. This case is still quite important and relevant, particularly the special case in the next

III.C.6. DEFINITION. A **central simple algebra (CSA)** over a field $\mathbb{F}$ is a simple $\mathbb{F}$-algebra, in the sense of having no nontrivial 2-sided proper ideals, with $\dim_{\mathbb{F}}(A) < \infty$ and center $C(A) = \mathbb{F}$.

Note that I have *not* included semisimplicity in the definition here, because we are going to *prove* it:

III.C.7. THEOREM. (i) *Let A be a simple algebra of finite dimension over $\mathbb{F}$; then A is semisimple, and $A \cong M_n(D)$ for a division algebra D over $\mathbb{F}$.*

(ii) *If A is a CSA/$\mathbb{F}$, then $A \cong M_n(D)$ with $C(D) = \mathbb{F}$. Conversely, any $M_n(D)$ of this form is a CSA.*

PROOF. (i) The strategy of proof is going to be to *directly* show $A \cong M_n(D)$, rather than using Artin-Wedderburn. By the finite-dimensionality, there exists a minimal left ideal $I \subset A$. This is simple as an A-module, and so $D^{\mathrm{op}} := \mathrm{End}_A({}_AI)$ must be a division ring by Schur. Since $\mathrm{End}_A({}_AI) \subset \mathrm{End}(I)\,(:= \mathrm{End}_{\mathbb{Z}}(I))$, the resulting ring homomorphism $D^{\mathrm{op}} \to \mathrm{End}(I)$ defines a right D-module structure on I, cf. [**Algebra I**, IV.A.11].

Now D is simple as a D-module, so by III.A.7 is semisimple as a ring. Moreover, the simple D-modules are just copies of D itself, by the usual argument with Jordan-Hölder. By semisimplicity of D, I_D is a semisimple (right) D-module, with $I_D = D^{\oplus n}$. I claim that $A \cong \mathrm{End}_D(I_D)$. By III.B.1, $\mathrm{End}_D(I_D) \cong M_n(D)$, and so this will finish the proof.

To prove the claim, consider the left-multiplication homomorphism $\ell\colon A \to \mathrm{End}_D(I_D) =: E$ sending $a \mapsto \ell_a$. (We also write ℓ_A, ℓ_I for images of A, I.) Since A is simple, and the kernel is a 2-sided ideal, ℓ must be injective. It remains to check surjectivity.

Let $\imath, \jmath \in I$ and $\varphi \in E$. First note that $\mathfrak{r}_\jmath$ (right mult. by $\jmath$) belongs to $\mathrm{End}_A({}_AI) = D^{\mathrm{op}}$. It follows that $\varphi(\ell_\imath(\jmath)) = \varphi(\imath\jmath) = \varphi(\imath)\jmath = \ell_{\varphi(\imath)}(\jmath) \implies \varphi \circ \ell_\imath = \ell_{\varphi(\imath)}$ in E, whence $E \circ \ell_I \subset \ell_I$. By simplicity of A, we must have $A = AIA = IA \implies \ell_A = \ell_I \circ \ell_A \implies E \circ \ell_A = E \circ \ell_I \circ \ell_A \subset \ell_I \circ \ell_A = \ell_A \implies \ell_A$ is a left ideal in E. But ℓ_A contains the identity. So $\ell_A = E$ and we are done.

(ii) Immediate from (i), III.B.7 and [**Algebra I**, III.A.11]. □

III.C.8. COROLLARY. *If $\mathbb{F}$ is algebraically closed or finite, then the only CSAs over $\mathbb{F}$ are the matrix algebras $M_n(\mathbb{F})$. If $\mathbb{F} = \mathbb{R}$, then we can have $M_n(\mathbb{R})$ or $M_n(\mathbb{H})$.*

PROOF. This follows at once from III.C.7 and the theorems of Frobenius and Wedderburn [**Algebra I**, V.B.5,8,11]. □

III.C.9. COROLLARY. *For A any CSA over $\mathbb{F}$, $\dim_{\mathbb{F}} A$ is a square.*

SKETCH. Consider the "extension of scalars" $\bar{A} := A \otimes_{\mathbb{F}} \bar{\mathbb{F}}$, where $\bar{\mathbb{F}}$ is an algebraic closure. One checks that $C(\bar{A}) = \bar{\mathbb{F}}$ and $\dim_{\bar{\mathbb{F}}} \bar{A} = \dim_{\mathbb{F}} A =: d$. But by III.C.8, $\bar{A} = M_n(\bar{\mathbb{F}})$ for some n, and so we have $d = n^2$. □

The obvious example here is $A = \mathbb{H}$ as a CSA/$\mathbb{R}$, whose complexification $\bar{A} := A \otimes_{\mathbb{R}} \mathbb{C}$ is $M_2(\mathbb{C})$, both of dimension 4.

III.C.10. EXAMPLE. We haven't said much about $\mathbb{F} = \mathbb{Q}$. A rich source of examples of simple and semisimple $\mathbb{Q}$-algebras, and even of division algebras, comes from bilinear forms. Suppose (W, B) is a symplectic or orthogonal space, and $G \leq \mathrm{Aut}(W, B)$ a subgroup which acts irreducibly on W. Put $D := \mathrm{End}_G(W) =$ endomorphisms commuting with G; by a version of Schur's lemma, this is a division algebra (over $\mathbb{Q}$). Its center $K := C(D)$ is clearly a number field of some sort.

But not any sort. There is a constraint: since B is nondegenerate, we can define adjoints of endomorphisms by

$$B(\xi^\dagger w_1, w_2) = B(w_1, \xi w_2) \quad (\forall w_1, w_2 \in W),$$

producing an involution $\dagger\colon D \to D^{\mathrm{op}}$. Its restriction to K defines an automorphism $\rho \in \mathrm{Aut}(K/\mathbb{Q})$ of order 1 or 2. Let K_0 denote the fixed field. If we assume furthermore that our involution is *positive*, which is to say that $\mathrm{Tr}_{K_0/\mathbb{Q}}(\rho(k)k) > 0$ for all $k \in K^*$, then you can show that:

(1) if $\rho = \mathrm{id}_K$, then $K = K_0$ is a totally real field; and

(2) if $\rho \neq \mathrm{id}_K$, then $[K{:}K_0] = 2$, K_0 is totally real, and K is totally imaginary. (In this case, K is called a CM field.)[1]

One then arrives at the following classification of the possible D's, due to Albert. In case (1), either D is the totally real field K or a quaternion algebra over it (which either splits or doesn't split under every real embedding). In case (2), all one can say is that $\dim_K(D)$ is a square (by III.C.9).

More generally, of course, we could choose G to be an arbitrary *reductive*[2] linear algebraic subgroup of $\mathrm{Aut}(W, B)$, in which case W breaks into irreducible representations of G, viz. $W \cong \oplus_j W_j^{\oplus n_j}$. Clearly then we will have $\mathrm{End}_G(W) \cong \times_j M_{n_j}(D_j)$, with the previous constraints on the division algebras D_j.

[1]The terminology "totally real" and "totally imaginary" refer to having only real embeddings resp. no real embeddings; "CM" stands for "complex multiplication", due to the role played by these fields in the study of abelian varieties. Deducing (1) and (2) is a nice exercise using the fact that the cartesian product of real embeddings and real and imaginary parts of the complex embeddings embed K as a dense subset of $\mathbb{R}^{[K:\mathbb{Q}]}$.

[2]These are precisely the linear algebraic groups whose representations decompose into direct sums of irreducibles. They include all the classical groups.