NOTES FOR LECTURE 5

A recorded lecture covering the contents of this note up to Example 9 is available here.

Throughout we work over a field k which we assume to be algebraically closed unless otherwise s, that is, any polynomial $f(t) \in \mathsf{k}[t]$ has a root in k. The goal of this lecture will be to show that if A is a finite-dimensional semisimple k-algebra, then the number of irreducible A-modules up to isomorphism is equal to the dimension of the centre of A.

1. Schur's Lemma

We begin by recalling two simple results from earlier in the course. For the first of these, at least, we slightly rephrased the statement of Schur's Lemma slightly from that given in the online lecture notes.

Lemma 1 (Schur's Lemma). *Let A be a finite dimensional algebra over an algebraically closed field k and suppose that U and V are simple A-modules. Then $Hom_A(U, V)$ is a k-vector space of dimension 0 or 1, in the former case U and V are not isomorphic while in the latter, if $\phi: U \to V$ is an isomorphism between U and V then $Hom_A(U, V) = \mathsf{k}.\phi$.*

Proof. Suppose that $\theta \in \text{Hom}_A(U, V)$. Then $\ker(\theta) \leq U$ is an A-submodule of U and hence as U is irreducible we must have $\ker(\theta) = \{0\}$ or U, and so θ is either the zero map or it is injective. Similarly since $\theta(U) \leq V$ and V is irreducible, we must have $\theta(U) = \{0\}$ or V, that is, either θ is the zero map or θ is surjective. It follows that if both U and V are irreducible then θ is either the zero map or it is an isomorphism.

Now if $\phi: U \to V$ is an isomorphism, then $\theta \mapsto \theta \circ \phi^{-1}$ gives a linear map from $\text{Hom}(U, V)$ to $\text{Hom}(V, V)$ which has inverse $\psi \mapsto \psi \circ \phi$, hence $\text{Hom}(U, V) \cong \text{Hom}(V, V)$ as k-vector spaces. But if $\varphi: V \to V$ is an A-module map then because it is k-llnear, and V is finite-dimensional, it has an eigenvalue, λ say. But then $\varphi - \lambda.1_V \in \text{End}_A(V)$ and $\ker(\varphi - \lambda.1_V) \neq \{0\}$. Since V is irreducible it follows that $V = \ker(\varphi - \lambda.1_V)$, and hence $\varphi = \lambda.\mathbb{1}_V$. It follows that $\text{Hom}_A(U, V) = \mathsf{k}.\phi$ as required. ☐

Lemma 2. *Let A be a finite-dimensional semisimple algebra and suppose that $A = \bigoplus_{j=1}^m S_j$ where each S_j is a simple A-module, then if M is an arbitrary irreducible A-module, there is some $j \in \{1, \dots, m\}$ with the property that $S_j \cong M$. In particular, there are only finitely many A-modules up to isomorphism.*

Proof. Indeed if we fix $m \in M\backslash\{0\}$ then $e: A \to M$ given by $e(a) = a.m$ defines an A-module homomorphism from $e: A \to M$ which contains m in its image and hence is not the zero map. Now if $e_j: S_j \to M$ denotes the restriction of e to S_j, then since S_j and M are irreducible, e_j is either an isomorphism or it is the zero map. But if e_j is zero for all j then $e: \bigoplus S_j \to M$ vanishes, contradicting the fact that $m \in \text{im}(e)$. Thus it follows that there is at least one $j \in \{1, 2, \dots, r\}$ such that $e_j: S_j \to M$ is an isomorphism. ☐

Remark 3. The previous Lemma shows that if A is a finite-dimensional semisimple k-algebra then the number of isomorphism classes of simple A-modules is equal to the number of isomorphism classes of simple A-modules in $\{S_j : 1 \leq j \leq m\}$ where $A = \bigoplus_{j=1}^m S_j$ is a direct sum decomposition of A into simple submodules.

2. The number of simple A-modules up to isomorphism

Definition 4. Let A be a finite-dimensional k-algebra and suppose that (V, ρ) is an irreducible A-module. Then if $z \in Z(A)$, then $\rho(z) \in \text{End}_A(V)$ and hence by Schur's Lemma, z acts by a scalar on V, which we will denote by z_V. The map $z \mapsto z_V$ defines a ring homomorphism from $Z(A)$ to k which is caled a *central character*. It is easy to check that the homomorphism $z \mapsto z_V$ depends only on the isomorphism class of V, and not on V itself.

Definition 5. Let A be a finite-dimensional k-algebra and suppose that V is an irreducible A-module. Then if $z \in Z(A)$ is a central element, its action on V gives an element of $\text{End}_A(V)$. which by Schur's Lemma must be a scalar. It follows that follows z acts on V via a scalar which we denote by z_V. The map $z \mapsto z_V$ is then in fact a ring homomorphism from $Z(A)$ to k and we refer to it as a *central character*.

If $A = \bigoplus_{j=1}^m S_j$ is a direct sum decomposition of A into irreducible submodules S_j, then the relation on $\{1, \dots, m\}$ given by $i \sim j$ if $S_i \cong S_j$ is clearly an equivalence relation. Let $P_1, \dots, P_r$ denote the equivalence classes of $\sim$. Then r is the number of isomorphism classes of simple A-modules and if we set $B_i = \bigoplus_{j\in P_i} S_j$, we see that $A = \bigoplus_{i=1}^r B_i$, and by Schur's Lemma if $S_{j_1} \leq B_{i_1}, S_{j_2} \leq B_{i_2}$ where $i_1 \neq i_2$ then $\mathrm{Hom}(S_{j_1}, S_{j_2}) = \{0\}$ while if $S_{j_1}, S_{j_2} \leq B_i$ then $S_{j_1} \cong S_{j_2}$. Note that since, for each $i \in \{1, \dots r\}$, the direct summands of B_i are all isomorphic, they have the same associated central character, and hence we will denote this central character by $z \mapsto z_i$.

Proposition 6. *Let $A = \bigoplus_{i=1}^r B_i$ as above. Then*

i) Each B_i is a two-sided ideal of A.

ii) $Z(A) = \bigoplus_{i=1}^r Z(B_i)$ and $\dim_{\mathsf{k}}(Z(B_i)) = 1$ so that in particular the number of irreducible A-modules up to isomorphism is $\dim(Z(A))$.

Proof. For i) first note that by definition, the B_i are submodules of A and hence are automatically *left* ideals of A. To see that they are in fact two-sided ideals we must show that, for any $a \in A$, we have $B_i.a \subseteq B_i$, and to show this we define $\rho(a)\colon A \to A$ to be the map given by right-multiplication by a, that is $\rho(a)(x) = xa$. Now if we view A as a left A-module in the obvious way then $\rho(a) \in \mathrm{End}_A(A)$– indeed for any $r, x \in A$ we have

$$\rho(a)(r.x) = (r.x).a = r.(x.a) = r\rho(a)(x).$$

Now if $\pi_k\colon A \to S_k$ denotes the projection from A to S_k, then for each $k \in \{1, \dots, m\}$ the restriction of $\pi_k \circ \rho(a)$ to S_j gives an A-module map from S_j to S_k. But by Schur's Lemma, such a map must be zero unless $S_k \equiv S_j$, and hence we see that the restriction of $\rho(a)$ to S_j has image contained in B_i where $j \in P_i$, and since $B_i = \bigoplus_{j\in P_i} S_j$ it follows that $\rho(a)(B_i) \subseteq B_i$. Since $a \in A$ was arbitrary it follows that B_i is a two-sided ideal of A, establishing i).

For ii) note that since $B_i.B_j \subseteq B_i \cap B_j$, if $i \neq j$ then $B_i.B_j = \{0\}$. Now let $q_i : A \to B_i$ denote the projection from A to B_i (with kernel $\bigoplus_{j\neq i} B_j$) and let $e_i = q_i(1)$. Then $1 = \sum_{i=1}^r e_i$ and since for any $a \in A$ we have $a = a.1 = 1.a$, it follows that $a = \sum_{i=1}^r ae_i = \sum_{i=1}^r e_i a$. But since $e_i \in B_i$ we have $a.e_i, e_i.a \in B_i$ and hence we must have $q_i(a) = e_i.a = a.e_i$. In particular $e_i \in Z(A)$ and $e_i^2 = e_i$ while $e_ie_j = 0$ if $i \neq j$.

Now suppose that $z \in Z(A)$. Then $z = \sum_{i=1}^r ze_i$ and since $e_i, z \in Z(A)$ it follows that $ze_i \in B_i \cap Z(A) \subseteq Z(B_i)$ and hence $Z(A) = \bigoplus_{i=1}^r Z(A) \cap B_i$. Next recall that we write $z \mapsto z_i$ for the central characters associated to the simple summands of B_i so that $z \in Z(A) \cap B_i$ and $b \in B_i$ then writing $b = \sum_{j\in P_i} b_j$ it follows that

$$z.b = \sum_{j\in P_i} zb_j = \sum_{j\in P_i} z_ib_j = z_i \sum_{j\in P_i} b_j = z_ib$$

In particular, taking $b = e_i$ we see that $z = z_i.e_i \in \mathsf{k}.e_i$ and hence $Z(A)\cap B_i = \mathsf{k}.e_i$. Since $\mathsf{k}.e_i$ is clearly contained in $Z(B_i)$ it follows that $Z(A) \cap B_i = Z(B_i)$ and $\dim(Z(b_i)) = 1$ as required. □

Now suppose that G is a finite group. Then G has finitely many conjugacy classes which we will denote by $\mathscr{C}_1, \dots, \mathscr{C}_r$. For each conjugacy class $\mathscr{C}_i$ we set

$$\hat{\mathscr{C}_i} := \sum_{g\in\mathscr{C}_i} g \in \mathsf{k}G.$$

The set $\{\hat{\mathscr{C}_i} : 1 \leq i \leq r\}$ is clearly linearly independent because the conjugacy classes of G form a partition of G.

Lemma 7. *The set $\{\hat{\mathscr{C}_i} : 1 \leq i \leq r\}$ is a k-basis of $Z(\mathsf{k}G)$, the centre of the group algebra $\mathsf{k}G$.*

Proof. Let $z = \sum_{g\in G} c_g g$. Then since G is a basis of $\mathsf{k}G$ it follows that $z \in Z(\mathsf{k}G)$ if and only if $hz = zh$ for all $h \in G$. But

$$hz = zh \iff z = h^{-1}zh \iff \sum_{g\in G} c_g g = \sum_{g\in G} c_g hgh^{-1} = \sum_{k\in G} c_{h^{-1}kh} k,$$

where in the final equality we have changed variable to $k = hgh^{-}1$. Thus we see that $hz = zh$ for all $h \in H$ if and only if $c_g = c_{h^{-1}gh}$ for all $g, h \in G$. But this is clearly just the condition that the coefficients c_g are constant on the conjugacy classes of G which in turn is clearly equivalent to the condition that z lies in the span of the elements $\{\hat{\mathscr{C}_i} : 1 \leq i \leq r\}$. □

Remark 8. Note that the number of irreducible G-representations (when $\mathsf{k}G$ is semisimple) is $\dim(Z(\mathsf{k}G))$ is the dimension of the *centre of* $\mathsf{k}G$, the *group algebra* of G and *not* the cardinality $|Z(G)|$ of the centre $Z(G)$ of G.

In fact the group algebra $\mathsf{k}Z(G)$ of the centre $Z(G)$ of G is naturally a subalgebra of $Z(\mathsf{k}G)$ because the elements of $Z(G)$ correspond precisely to the conjugacy classes of G which have size 1 and hence the map $\zeta \mapsto \widehat{\{\zeta\}}$ from $Z(G)$ to $\{\hat{\mathscr{C}}_i : 1 \leq i \leq r\}$ induces an embedding of $\mathsf{k}Z(G)$ into $Z(\mathsf{k}G)$. This map is an isomorphism, however, if and only if G is abelian: G is non-abelian precisely when there exists conjugacy classes of cardinality greater than 1.

Example 9. Let $G = C_n$ be the cyclic group of order n and let $g \in C_n$ be a generator, so that $g^n = e_G$. Consider $\mathbb{Q}G$ the group algebra of G over the rational numbers. How many simple $\mathbb{Q}G$-modules are there up to isomorphism?

Since $\mathbb{Q}G$ is generated as a $\mathbb{Q}$-algebra by g the $\mathbb{Q}$-linear map $\alpha\colon \mathbb{Q}[t] \to \mathbb{Q}G$ given by $t \mapsto g$ is surjective and it is easy to see that its kernel is given by $\langle t^n - 1\rangle$, the ideal in $\mathbb{Q}[t]$ generated by the polynomial $t^n - 1$. Now $t^n - 1 \in \mathbb{C}[t]$ has n distinct roots and this implies that if we factorise $t^n - 1$ into a product of irreducibles $t^n - 1 = f_1 . \dots . f_r$ then the irreducibles $f_1, \dots, f_r$ must be pairwise distinct (since otherwise they have a common root which would then have multiplicity greater than 1 in $t^n - 1$). But then the Chinese Remainder Theorem shows that

$$\mathbb{Q}G \cong \bigoplus_{i=1}^{r} \mathbb{Q}[t]/\langle f_i \rangle,$$

where if $E_i := \mathbb{Q}[t]/\langle f_i\rangle$ then because f_i is irreducible, E_i is a field of degree $\deg(f_i)$ over $\mathbb{Q}$. Now if 1_i is the image of $1 \in \mathbb{Q}[t]$ in E_i and e_i the corresponding element of $\mathbb{Q}G$ we have $1 = \sum_{i=1}^{r} e_i$ in $\mathbb{Q}G$ where $e_i^2 = e_i$ and $e_ie_j = 0$ if $i \neq j$. It follows that if V is an irreducible $\mathbb{Q}G$-module then $V = e_iV$ for some $i \in \{1, \dots, r\}$, and if $v \in V\backslash\{0\}$ then the map $e_v\colon \mathbb{Q}G \to V$ given by $e_v(a) = a.v$ restricts to a nonzero map $e_v\colon E_i \to V$ which is a surjective map of E_i-modules, that is, of vector spaces over E_i. It follows that V must be 1-dimensional over E_i and e_v an isomorphism from E_i to V. It follows that $\mathbb{Q}G$ has r irreducible representations indexed by the irreducible factors of $t^n - 1$ over $\mathbb{Q}$.

In fact if $\mu_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\}$ denotes the mulitplicative group of the n-th roots of unity in $\mathbb{C}$ then we have

$$t^n - 1 = \prod_{d|n} \Phi_d(t), \quad \Phi_d(t) = \prod_{\substack{\zeta\in\mu_n \\ o(\zeta)=d}} (t - \zeta)$$

where $o(\zeta)$ denotes the order of ζ in $\mathbb{C}^{\times}$. It is known that $\Phi_d(t) \in \mathbb{Q}[t]$ is irreducible, hence $r = r(n) = |\{d \in \{1, \dots, n\} : d \mid n\}$ is just the number of divisors of n.

Example 10. For any $z, w \in \mathbb{C}$ let

$$h(z, w) := \begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{C}),$$

and let $\mathbb{H} = \{h(z, w) : z, w \in \mathbb{C}\} \subseteq \mathrm{Mat}_2(\mathbb{C})$. Then $\mathbb{H}$ is a *real* 4-dimensional subspace of $\mathrm{Mat}_2(\mathbb{C})$ but not a complex-linear subspace.

Now it is easy to see that $\det(h(z, w)) = |z|^2+|w|^2$ so that if $r = \det(h(z, w))^{1/2}$ and we set $u(z, w) := h(z/r, w/r)$, the columns of $u(z, w)$ form an orthonormal basis of $\mathbb{C}^2$ and $\det(u(z, w)) = 1$, that is, $u(z, w) \in \mathrm{SU}_2(\mathbb{C})$. Thus

$$\mathbb{H} = \mathbb{R}.\mathrm{SU}_2(\mathbb{C}) = \{r.g : r \in \mathbb{R}, g \in \mathrm{SU}_2(\mathbb{C})\},$$

and hence it follows that $\mathbb{H}$ is closed under matrix multiplication, and is thus a 4-dimensional $\mathbb{R}$-algebra. Note that the involution $A \mapsto A^* := \bar{A}^{\top}$ of $\mathrm{Mat}_2(\mathbb{C})$ satisfies $h(z, w)^* = h(\bar{z}, -\bar{w})$ and therefore it restricts to give an involution on $\mathbb{H}$ which satisfies $(h_1h_2)^* = h_2^*h_1^*$.

It is easy to write down an explicit $\mathbb{R}$-basis of $\mathbb{H}$. For example we may take $\{h(z, w) : z, w \in \{1, i\}\}$ gives a basis $\{\mathbb{1}, I, J, K\}$ of $\mathbb{H}$ where $h(1, 0) = I_2 = \mathbb{1}$ and

$$I := h(i, 0) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = h(0,1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \quad K = h(0, i) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

An easy calculation shows that $I^2 = J^2 = K^2 = IJK = -\mathbb{1}$, and from this it is easy to see that $\{\mathbb{1}, I, J, K\} \subseteq \mathrm{SU}_2(\mathbb{C})$ generate a subgroup $Q_8 = \{\pm\mathbb{1}, \pm I, \pm J, \pm K\}$ of order 8. Now the action of $\sigma\colon Q_8 \to \mathrm{GL}(\mathbb{H})$ given by $\sigma(g)(h) = g.h$ defines a real 4-dimensional representation $(\mathbb{H}, \sigma)$ of Q_8. Since $\sigma(Q_8) \supseteq \{\mathbb{1}, I, J, K\}$, it is clear that $\sigma(\mathbb{R}Q_8) = \mathbb{H}$ and hence Q_8-submodule of $\mathbb{H}$ would have to be a left ideal of $\mathbb{H}$. Since $\mathbb{H} = \mathbb{R}.\mathrm{SU}_2(\mathbb{C})$, any nonzero element of $\mathbb{H}$ is a unit, and hence clearly $\mathbb{H}$ has no nontrivial proper left ideals and thus $(\mathbb{H}, \sigma)$ is an irreducible 4-dimensional real representation of Q_8.

Similarly $\sigma(\mathbb{R}Q_8) = \mathbb{H}$ implies $E := \text{End}_{\mathbb{R}Q_8}(\mathbb{H}) = \text{End}_{\mathbb{H}}(\mathbb{H})$, so that the following Lemma implies that $E \cong \mathbb{H}^{\text{op}}$, which is a division algebra that is not a field. Indeed the conjugate-transpose map $h \mapsto h^*$ gives an isomorphism of $\mathbb{H}$ with $\mathbb{H}^{\text{op}}$ so that $\text{End}_{\mathbb{R}Q_8}(\mathbb{H}) \cong \mathbb{H}$.

Lemma 11. *Let B be a finite-dimensional algebra over a field* k*. Then if $L(B)$ denotes the B viewed as a left-module over itself we have $\text{End}_B(L(B)) \cong B^{op}$.*

Proof. We claim the map $\eta\colon \text{End}_B(L(B) \to B$ given by $\eta(\theta) = \theta(1)$ gives the required isomorphism. Indeed since θ is compatible with the left action of B on itself we have, for any $b \in B$,

$$\theta(b) = \theta(b.1) = b.\theta(1).$$

Thus θ is given by right-multiplication by $\theta(1) = \eta(\theta)$. It follows that the map η gives a bijection between $\text{End}_B(L(B))$ and B. To see that it is an isomorphism onto B^{op} note that

$$\eta(\theta_1 \circ \theta_2) = (\theta_1 \circ \theta_2)(1) = \theta_1(\theta_2(1)) = \theta_1(\theta_2(1).1) = \theta_2(1).\theta_1(1) = \eta(\theta_2)\eta(\theta_1)$$

□