The theorems of Maschke and Artin-Wedderburn

Let $\Bbbk$ be a field, and let G be a finite group. Suppose that the characteristic of $\Bbbk$ divides the order of G. Then $x := \sum_{g \in G} g \in \Bbbk G$ satisfies $gx = x$ for all $g \in G$ and $x^2 = |G|x = 0$. Thus $\Bbbk G x = \Bbbk x$ is a submodule of $\Bbbk G$ which contains no idempotent. In particular, $\Bbbk x$ is not projective, and hence $\Bbbk G$ is not semisimple.

Theorem 1 (Maschke, 1898)
If $\operatorname{char}(\Bbbk)$ *does not divide the order of* G*, then* $\Bbbk G$ *is semisimple.*

Proof: Let V be a finite dimensional $\Bbbk G$-module, and let W be submodule of V. Pick an idempotent $e \in \operatorname{End}_{\Bbbk}(V)$ with $eV = W$. Define $\overline{e} := \frac{1}{|G|} \sum_{g \in G} geg^{-1}$, where the elements of G are considered as endomorphisms of V. Then

$$h\overline{e} = \frac{1}{|G|} \sum_{g \in G} hgeg^{-1} = \frac{1}{|G|} \sum_{g \in G} (hg)e(hg)^{-1}h = \overline{e}h$$

for all $h \in G$ and thus $\overline{e} \in \operatorname{End}_{\Bbbk G}(V)$. Since W is a submodule of V, the endomorphism $\overline{e}$ still satisfies $\overline{e}V \leq W$ and $\overline{e}|_W = \mathrm{id}_W$. Hence $\overline{e}$ is an idempotent with $\overline{e}V = W$, and we have $V = W \oplus (1 - \overline{e})V$ as desired. □

Maschke's original proof is essentially the following: take $\Bbbk = \mathbb{C}$, and let $< \cdot, \cdot >$ be a G-invariant scalar product on V (which is known to exist by an avering process similar to the one above). Then $V = W \oplus W^{\perp}$.

Theorem 2 (Artin-Wedderburn, 1927-1907)
Let A be a (left) semisimple ring. Then $A \cong \bigoplus_{i=1}^{r} D_i^{n_i \times n_i}$ for some division rings D_i. Here r is the number of simple A-modules, and the (n_i, D_i) are determined by A up to isomorphism.

Proof: Write ${}_AA = \bigoplus_{i=1}^{r} n_i V_i$, where $\{V_1, \ldots, V_r\}$ is a set of representatives of the isomorphism classes of simple A-modules. Then

$$A \cong \operatorname{End}_A({}_AA)^{op} \cong \bigoplus_{i=1}^{r} \operatorname{End}_A(n_i V_i)^{op} \cong \bigoplus_{i=1}^{r} (\operatorname{End}_A(V_i)^{op})^{n_i \times n_i}.$$

The first isomorphism is given by the map $a \mapsto (\varrho_a : x \mapsto xa)$. Since the $\operatorname{End}_A(V_i)$ are division rings by Schur's lemma, existence is proved.

It remains to show that whenever $A \cong \bigoplus_{i=1}^{r'} (D_i')^{n_i' \times n_i'}$, we have $r = r'$, and, after renumbering, $n_i = n_i'$ and $D_i \cong D_i'$. To do this it suffices to show that for any division ring D, the natural module D^n is the unique simple $D^{n \times n}$-module, and that D isomorphic to $\operatorname{End}_{D^{n \times n}}(D^n)^{op}$. But $D^{n \times n} \cong \bigoplus_{j=1}^{n} D^{n \times n} e_{jj}$, where e_{jj} is the diagonal matrix with 1 in position (j, j) and zeros everywhere else. Clearly D^n is simple and all $D^{n \times n}$ are isomorphic to D^n. The theorem of Jordan-Hölder implies that D^n is indeed the unique simple D^n-module. The map

$$f : D \to \operatorname{End}_{D^{n \times n}}(D^n)^{op}, d \mapsto (\lambda_d : v \mapsto vd)$$

is a ring monomorphism. Pick $\lambda \in \operatorname{End}_{D^{n \times n}}(D^n)$ and write $\lambda(e_1) = de_1 + \sum_{j=2}^{n} a_j e_j$. Then $\lambda(v) = \lambda((v, 0, \ldots, 0)e_1) = (v, 0, \ldots, 0)\lambda(e_1) = vd$ for all $v \in D^n$. Thus f is onto. □

The theorem of Artin-Wedderburn implies in particular that a left semisimple ring is also right semisimple. Since the same proof – with right instead of left modules – works for a right semisimple ring, left semisimplicity is the same thing as right semisimplicity. Therefore we can simply speak of semisimple rings.

Let $A \cong \bigoplus_{i=1}^r D_i^{n_i \times n_i}$ be a semisimple ring. Recall that a central idempotent $0 \neq e \in Z(A)$ is called primitive if for any decomposition $e = e_1 + e_2$ with orthogonal central idempotents e_i either $e = e_1$ or $e = e_2$.

Corollary 1
Let $1 = e_1 + \cdots e_{r'}$ be a decomposition of 1 in central primitive idempotents. Then $r = r'$ and, after renumbering, $e_i A e_i = A e_i \cong D_i^{n_i \times n_i}$. □

Corollary 2
Let $\Bbbk$ be an algebraically closed field, A a semisimple $\Bbbk$-algebra, and $\{V_1, \ldots, V_r\}$ be a set of representatives of the isomorphism classes of simple A-modules. Then $r = \dim_{\Bbbk} Z(A)$, the multiplicity n_i of V_i in ${}_A A$ is $\dim_{\Bbbk} V_i$, and $A \cong \bigoplus_{i=1}^r \Bbbk^{n_i \times n_i}$. □

If $A = \Bbbk G$ is a group algebra, an easy computation shows that

$$Z(\Bbbk G) = \langle \sum_{c \in C} c \mid C \subseteq G \text{ conjugacy class } \rangle_{\Bbbk}.$$

Thus we have

Corollary 3
Let $\Bbbk$ be an algebraically closed field an G a finite group such that $\mathrm{char}(\Bbbk) \nmid |G|$. Then the number of simple $\Bbbk G$-modules is equal to the number of conjugacy classes of G. □

Let $\Bbbk$ be field of characteristic zero and let V be a $\Bbbk G$-module. Then the map

$$\chi_V : G \to \Bbbk, g \mapsto Tr_V(g)$$

which associates to each element of G its trace on V is called the character of G afforded by V. Assume that $\Bbbk$ is algebraically closed, and let $V_1, \ldots, V_r$ be the simple $\Bbbk G$-modules. Then the $\chi_i := \chi_{V_i}$ are called the irreducible characters of G. Corollary 2 implies

$$|G| = \dim_{\Bbbk}(\Bbbk G) = \sum_{i=1}^r (\dim_{\Bbbk}(V_i))^2 = \sum_{i=1}^r \chi_i(1)^2.$$

This is a special case of the so-called orthogonality relations.