GRADUATE ALGEBRA II. NOTES

MANOJ KUMMINI

OUTLINE

(1) Basic ring theory: examples, ideals and modules; centre, algebras; radical; artinian and noetherian rings; review of tensor products.
(2) Semisimplicity: Artin-Wedderburn theorem; Jacobson density theorem;
(3) Group rings: Schur's lemma.
(4) Introduction to representation theory: chiefly finite groups; somethings about reductive groups.

References.

(1) N. Bourbaki, Algebra, Ch. I.
(2) N. Bourbaki, Algebre, Ch. VIII, Springer, 2012 (the revised edition; in French.) This is our primary reference for semi-simplicity.
(3) N. Jacobson, Basic Algebra I and II.
(4) S. Lang, Algebra.
(5) Appendix "A short digest of non-commutative algebra" in J. A. Dieudonné and J. B. Carrell, *Invariant theory, old and new* Adv. in Math. 1970.

1. BASIC RING THEORY

For the most part, we will follow Bourbaki, *Algebra*, Ch. I, using Jacobson and Lang for supporting material and exercises.

1.1. **Definition.** A *ring* is a set R with two operations $+$ (*addition*) and $\cdot$ (*multiplication*) such that

(1) $(R, +)$ is an abelian group;
(2) multiplication is associative and has an identity;
(3) multiplication is distributive over addition, i.e., for all $a, b, c \in R$, $a(b+c) = ab + ac$ and $(a+b)c = ab + bc$.

If the multiplication is commutative, then we say that R is a *commutative ring*.

1.2. **Remark.** We denote the additive identity by 0 and the multiplicative identity by 1. We will refer to $(R, +)$ as the *additive group* of R.

1.3. **Example.** (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are commutative rings, with the usual addition and multiplication.

(2) Rings of functions: Let R be a ring and X a set. The set of functions from X to R form a ring as follows. For functions $f, g : X \longrightarrow R$, set $(f+g)$ to be the function $x \mapsto f(x) + g(x)$, $x \in X$ and fg be the function $x \mapsto f(x)g(x)$, $x \in X$. The additive identity is the constant function $x \mapsto 0$ and the multiplicative identity is the constant function $x \mapsto 1$. If R is commutative, then this ring is commutative. By imposing conditions on X, on R and on the functions that we are interested in, we get many variants of this construction: For example, if X is a topological space, we can consider the ring of continuous $\mathbb{R}$-valued functions, the ring of continuous $\mathbb{C}$-valued functions etc.

(3) Endomorphism rings: Let G be an abelian group, written additively. Let R be the set of group endomorphisms of G, made into a ring as follows: for endomorphisms α, β of G, set $\alpha + \beta$ to be the function $g \mapsto \alpha(g) + \beta(g)$ and $\alpha\beta$ to be function $g \mapsto \alpha(\beta(g))$. These are endomorphisms of G. The additive identity is the zero endomorphism $g \mapsto 0$, $g \in G$ and the multiplicative identity is is the identity map $g \mapsto g$, $g \in G$. Endomorphism rings are not commutative, in general.

(4) A variant of the previous construction: Let $\Bbbk$ be a field and V a $\Bbbk$-vector-space. On the set of all $\Bbbk$-linear endomorphisms of V, define addition and multiplication as earlier, to get a ring. This is usually denoted as $\operatorname{End}_{\Bbbk}(V)$. If $V = \Bbbk^n$, then this ring can be thought of as the set $M_n(\Bbbk)$ of $n \times n$ matrices over $\Bbbk$, with usual matrix addition and usual matrix multiplication.

(5) In general, if R is a ring then the set $M_n(R)$ of $n \times n$ matrices with entries in R can be made into a ring with usual matrix addition and usual matrix multiplication.

1.4. **Definition.** Let R and S be rings. A *ring homomorphism* $f : R \longrightarrow S$ is a function f such that $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ and $f(1) = 1$, for all $x, y \in R$. A ring homomorphism $f : R \longrightarrow S$ is an *isomorphism* if there exists a ring homomorphism $g : S \longrightarrow R$ such that $gf = \mathrm{id}_R$ and $fg = \mathrm{id}_S$. An *endomorphism* of R is a homomorphism $R \longrightarrow R$; an endomorphism is an *automorphism* if it is additionally an isomorphism.

1.5. **Remark.** (1) Since R and S are abelian groups, the requirement $f(x+y) = f(x) + f(y)$ for all $x, y \in R$ forces f to be a map of abelian groups (Exercise 1.18). Hence we may think of a ring homomorphism as a homomorphism of abelian groups f satisfying $f(xy) = f(x)f(y)$ and $f(1) = 1$, for all $x, y \in R$

(2) Most rings that we look at a natural multiplicative identity, and the most natural functions between these rings take the multiplicative identity of one ring to that of another ring; see the examples above. Therefore we require that $f(1) = 1$ in the definition of ring homomorphisms.

(3) Ring isomorphisms are exactly the bijective ring homomorphisms (Exercise 1.19).

(4) Let $f : R \longrightarrow S$ and $g : S \longrightarrow T$ be ring homomorphisms. Then the composite $gf : R \longrightarrow T$ is a ring homomorphism (Exercise 1.20).

1.6. **Definition.** A *invertible* element of R is an element r such that there exists s such that $rs = sr = 1$. A *nilpotent* element of R is an element r such that there exists $n \geq 1$ such that $r^n = 0$. An *idempotent* element of R is an element r such that $r^2 = r$.

1.7. **Definition.** Let R be a ring, and X a subset of R. The *centralizer* of X is $\{r \in R : rx = xr \text{ for every } x \in X\}$. The *centre* of R is the centralizer of R.

1.8. **Definition.** Let R be a ring. A *subring* of R is a subset S that is an abelian subgroup of R, is closed under multiplication and contains the multiplicative identity.

In other words, the subset S is a ring (on its own) and the inclusion map $S \subseteq R$ is a ring morphism. Examples of subrings are:

(1) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$;

(2) the natural inclusion (as the constant polynomials) of R inside $R[X]$.

(3) For every subset X, its centralizer is a subring of R. In particular, the centre of R is a commutative subring of R. (Exercise 1.24)

1.9. **Definition.** A *left ideal* (respectively, *right ideal*) of R is an abelian subgroup I such that for every $r \in R$ and $a \in I$, $ra \in I$ (respectively, $ar \in I$. A *two-sided ideal* is an abelian subgroup that is both a left-ideal and a right-ideal. A *maximal left ideal* (respectively, *maximal right ideal*) is a left ideal that is distinct from R and is maximal (by inclusion) among left ideals (respectively, right ideals).

In the following, most of the statements we make about left ideals will hold, *mutatis mutandis*, for right ideals and two-sided ideals also.

1.10. **Theorem.** *Let R be a ring and $I \subsetneq R$ a left ideal. Then there exists a maximal left ideal containing I.*

Proof. Let $\mathcal{P}$ be the collection of all the left ideals distinct from R containing I. It is non-empty since $I \in \mathcal{P}$. If $I_\lambda, \lambda \in \Lambda$ is a chain in $\mathcal{P}$, then $\cup_{\lambda\in\Lambda} I_\lambda$ is a left ideal and hence an upper bound for the chain. By Zorn's lemma, $\mathcal{P}$ has a maximal element. $\square$

1.11. **Discussion.** Let $X \subseteq R$ be a subset. Then the collection of finite sums $\sum r_\lambda x_\lambda$ where $r_\lambda \in R$ and $x_\lambda \in X$ is a left ideal. Let $I_\lambda, \lambda \in \Lambda$ be a family of left ideals. Then the collect of finite sums $\sum_{r_\lambda a_\lambda}$ where $r_\lambda \in R$ and $a_\lambda \in I_\lambda$ form a left ideal, called the *sum* of $I_\lambda, \lambda \in \Lambda$ and denoted $\sum_{\lambda\in\Lambda} I_\lambda$.

1.12. **Definition.** Let R be a ring and I a two-sided R-ideal. The *quotient* ring R/I is the abelian group R/I with multiplication defined by $\bar{r}\bar{s} = \overline{rs}$, where $\bar{(.)}$ denote the coset modulo I.

This definition forces the multiplicative identity of R/I to be $\bar{1}$, and the natural map $R \longrightarrow R/I$ to be a ring homomorphism.

TBD: discussion about universal property to be added

Products.

1.13. **Discussion.** Let $A_\lambda, \lambda \in \Lambda$ be sets. The *(cartesian) product set* $\prod_{\lambda\in\Lambda} A_\lambda$ is the set $\{(a_\lambda)_{\lambda\in\Lambda} \mid a_\lambda \in A_\lambda \text{ for every } \lambda \in \Lambda\}$. Let us denote it by A. There is a family of functions (called *projection maps*) $\mathrm{pr}_\lambda : A \longrightarrow A_\lambda, \lambda \in \Lambda$ satisfying $\mathrm{pr}_\mu((a_\lambda)_{\lambda\in\Lambda}) = a_\mu$ for every $\mu \in \Lambda$. This family satisfies the following *universal property*: Given any family $f_\lambda : B \longrightarrow A_\lambda$, $\lambda \in \Lambda$ of functions, there is a unique function $f : B \longrightarrow A$ such that $f_\lambda = \mathrm{pr}_\lambda f$ for every $\lambda \in \Lambda$. (If such a function existed, then $f_\lambda(b) = \mathrm{pr}_\lambda f(b)$ for every $b \in B$ and every $\lambda \in \Lambda$; now check that $b \mapsto (f_\lambda(b))_{\lambda\in\Lambda}$ indeed satisfies this.) $\square$

1.14. **Discussion.** Let $R_\lambda, \lambda \in \Lambda$ be rings. The product set $\prod_{\lambda\in\Lambda} R_\lambda$ can be made into a ring with $(r_\lambda)_{\lambda\in\Lambda} + (s_\lambda)_{\lambda\in\Lambda} = (r_\lambda + s_\lambda)_{\lambda\in\Lambda}$ and $(r_\lambda)_{\lambda\in\Lambda}(s_\lambda)_{\lambda\in\Lambda} = (r_\lambda s_\lambda)_{\lambda\in\Lambda}$. With these definitions, $(0_{R_\lambda})_{\lambda\in R_\lambda}$ and $(1_{R_\lambda})_{\lambda\in R_\lambda}$ are, respectively, the additive and multiplicative identities. Moreover the projection maps pr_λ are ring homomorphisms. In fact, this is the unique ring structure on $\prod_{\lambda\in\Lambda} R_\lambda$ that ensures that pr_λ is a ring homomorphism for every $\lambda \in \Lambda$. Further, let $f_\lambda S \longrightarrow R_\lambda$ be ring homomorphisms. Then the unique function $f : S \longrightarrow \prod_{\lambda\in\Lambda} R_\lambda$ obtained in Discussion 1.13 is a ring homomorphism. $\square$

1.15. **Proposition.** *Let $R, R_1, \ldots, R_n$ be rings. Then R is isomorphic to $\prod_{i=1}^n R_i$ if and only if there exist two-sided R-ideals $I_1, \ldots, I_n$ such that R_i is isomorphic to R/I_i for every i and such that the natural map $R \longrightarrow \prod_{i=1}^n R/I_i$ is an isomorphism.*

Proof. 'If' is immediate. 'Only if': Let $\phi : R \longrightarrow \prod_{i=1}^n R_i$. Write pr_i for the projection $\prod_{i=1}^n R_i \longrightarrow R_i$. Define $I_i := \ker(\mathrm{pr}_i \cdot \phi)$. Since $\mathrm{pr}_i \cdot \phi$ is surjective, we get an isomorphism $f_i : R/I_i \longrightarrow R_i$. Write $g_i = f_i^{-1}$ and $g = \prod_{i=1}^n g_i$. Note that g is an isomorphism. The composite

$$R \xrightarrow{\phi} \prod_{i=1}^n R_i \xrightarrow{\mathrm{pr}_i} R_i \xrightarrow{g_i} R/I_i$$

is a ring homomorphism, so it is the natural map $R \longrightarrow R/I_i$. Hence $g \circ \phi : R \longrightarrow \prod_{i=1}^n R/I_i$ is the natural map, and is an isomorphism. $\square$

1.16. **Theorem.** *Let R be a ring, S its centre and $I_1, \ldots, I_n$ two-sided R-ideals. Then the following are equivalent:*

(1) The natural map $R \longrightarrow \prod_{i=1}^n R/I_i$ is an isomorphism.

(2) There exist idempotents $e_1, \ldots, e_n \in S$ such that $e_i e_j = 0$ for all $i \neq j$, $\sum_{i=1}^n e_i = 1$ and $I_i = R(1 - e_i)$

(3) For all $i \neq j$, $I_i + I_j = R$ and $\bigcap_{i=1}^n I_i = 0$

(4) There exist ideals $J_1, \ldots, J_n$ of S such that the map $S \longrightarrow \prod_{i=1}^{n} S/J_i$ is an isomorphism and $I_i = RJ_i$ for every i.

Proof. TBD. $\square$

Exercises

1.17. Using the distributive property, show the following, for every $x, y \in R$: $0x = x0 = 0$; $x(-y) = (-y)x = -(xy)$; $(-x)(-y) = xy$.

1.18. Let G and H be groups and $f : G \longrightarrow H$ a function such that $f(gg') = f(g)f(g')$. Show that $f(g^{-1}) = (f(g))^{-1}$ for every $g \in G$ and that $f(e_G) = e_H$. (Hint: apply with $g' = e_G$ and $g' = g^{-1}$.)

1.19. Let $f : R \longrightarrow S$ be a ring homomorphism. Show that f is a ring isomorphism if and only it is bijective. (Hint: Show that if f is bijective, then the inverse *function* $f^{-1} : S \longrightarrow R$ is a ring homomorphism.)

1.20. Show that the composite of two ring homomorphisms is a ring homomorphism.

1.21. If r is nilpotent, then $1 - r$ is invertible.

1.22. For $x \in R$, the *left homothety* λ_x (respectively, *right homothety* ρ_x) is the map $R \longrightarrow R$, $y \mapsto xy$ (respectively, $y \mapsto yx$). Show that these are endomorphisms of the additive group of R.

1.23. Show that $|R| = 1$ if and only if $0 = 1$, in which case $R = \{0\}$. This is the *zero ring*.

1.24. Let X be a subset of R. Show that the centralizer of X in R is a subring of R. The centre of R is a commutative subring.

1.25. Show that the endomorphism ring of the additive group $\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}$.

1.26. Let X be a subset of R. The *left annihilator* of X in R is the set $\{y \in R \mid yx = 0 \text{ for every } x \in X\}$. Show that it is a left ideal.

1.27. Let $f : R \longrightarrow S$ be a ring homomorphism. Write $\pi : R \longrightarrow R/\ker(f)$ and $\iota : \operatorname{Im}(f) \longrightarrow S$. Show that there is a ring homomorphism $\overline{f}$ such that $f = \iota \overline{f} \pi$. Show that it is an isomorphism.

1.28. Say that $x \in R$ is *left-invertible* (respectively, *right-invertible*) if there exists $y \in R$ such that $yx = 1$ (respectively, $xy = 1$). Show that x is left-invertible (respectively, right-invertible) if and only if the right homothety (respectively, left homothety)is surjective. Show that x is invertible if and only if it is left- and right-invertible. Show that in this case, the inverse of x is unique, and that this element is also the unique left- and right-inverses.

1.29. An *integral domain* is a commutative ring that is non-zero and that does not have any zero-divisors. Let R be a commutative ring and I an R-ideal. Show that the following are equivalent: (1) R/I is an integral domain; (2) For every $x, y \in R$, if $xy \in I$ and $x \notin I$, then $y \in I$; (3) I is the kernel of a ring homomorphism from R to an integral domain. A proper ideal satisfying these conditions is called a *prime ideal*. Show that maximal ideals are prime.

1.30. An *idempotent* element in R is an element e such that $e^2 = e$; an idempotent element is *central* if it belongs to the centre of R. Show that if R is a commutative ring and e an idempotent element, then for every prime ideal I of R, $e \in I$ or $1 - e \in I$, and that these conditions are mutually exclusive.

1.31. Show that the set of 2×2 complex matrices of the form

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

(where $\bar{(\cdot)})$ denotes complex conjugation) forms a subring of $M_2(\mathbb{C})$. This is called the *quaternion ring*. Show that it can also be described as the ring of all $\mathbb{R}$-linear combinations of the following four matrices:

$$I_2, \begin{bmatrix} \imath & 0 \\ 0 & -\imath \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & \imath \\ \imath & 0 \end{bmatrix}.$$

Determine its dimension as a $\mathbb{R}$-vector space.

1.32. Let $q_1, \ldots, q_r$ be pairwise relatively prime integers. Show that the natural map $\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/q_i\mathbb{Z}$ is surjective and that it induces an isomorphism $\mathbb{Z}/(q_1 \cdots q_r)\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/q_i\mathbb{Z}$.

1.33. Let $R_i, 1 \leq i \leq n$ be rings and $R = R_1 \times \cdots \times R_n$. Show that R_i is a quotient ring of R, for each i.

1.34. Let R be a ring and S the ring of 2×2 matrices over R. Relate the centres of R and of S.

1.35. Give an example of ideals $I, J, K \subseteq \mathbb{Z}$ such that $IJ \neq I \cap J$ and $(I + J)(I + K) \neq (I + JK)$.

1.36. Let R be a ring and I the two-sided ideal generated by $\{xy - yx \mid x, y \in I\}$. Show that every ring map $R \longrightarrow S$ with S commutative has I in its kernel. Hence we can think of I as the smallest two-sided ideal such that R/I is commutative.

2. Modules

2.1. **Definition.** A *left R-module* M is an abelian group M with an R-action $R \times M \longrightarrow M$ satisfying $(r + s)m = rm + sm$, $(sr)m = s(rm)$ and $1m = m$ for all $r, s \in R$ and $m \in M$. A *right R-module* M is an abelian group M with an R-action $M \times R \longrightarrow M$ satisfying $m(r + s) = mr + ms$, $m(rs) = (mr)s$ and $m1 = m$. A *homomorphism of R-modules* is a map $f : M \longrightarrow N$ that is a morphism of abelian groups and satisfies *R-linearity*: $f(rx) = r(f(x))$ for every $r \in R$ and $x \in M$. The set of R-homomorphisms from M to N is denoted $\mathrm{Hom}_R(M, N)$.

If M is a left (respectively, right) R-module, then, for every $r \in R$, the map $h_r : M \longrightarrow M$, $x \mapsto rx$ (respectively, $x \mapsto xr$) is a morphism of abelian groups called the *left homothety* (respectively, *right homothety*) defined by r. Homotheties are not R-homomorphisms in general (since $h_r(sx)$ need not equal $s(h_r(x))$ unless $rs = sr$); if r is central, then h_r is a R-homomorphism. The map $R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ $r \mapsto h_r$ is a ring homomorphism. Its image in $\mathrm{End}_{\mathbb{Z}}(M)$ is called the *ring of homotheties* (more precisely the *ring of R-homotheties*)of M and is denoted R_M. Conversely, if M is an abelian group, then every ring homomorphism $R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ defines an R-module structure on M.

The set $\mathrm{Hom}_R(M, N)$ does not have any 'natural' R-module structure, even with $N = M$, for more-or-less the same reason why homotheties are not R-homomorphisms. Similarly, there is no 'natural' ring map from $R \longrightarrow \mathrm{End}_R(M)$. The map $r \mapsto h_r$ from the centre of R of $\mathrm{End}_R(M)$ is a ring map, since central homotheties are R-homomorphisms.

Hereafter, unless otherwise mentioned, by a *module*, we mean a left module.

If $M_\lambda, \lambda \in \Lambda$ is a family of R-modules, then the cartesian product $\prod_{\lambda \in \Lambda} M_\lambda$ has a natural R-module structure $r(x_\lambda)_{\lambda \in \Lambda} = (rx_\lambda)_{\lambda \in \Lambda}$. It is also a product in the category of R-modules, i.e., if $f_\lambda : N \longrightarrow M_\lambda$ are R-homomorphisms, then there is a unique R-homomorphism $f : N \longrightarrow \prod_{\lambda \in \Lambda} M_\lambda$ such that $f_\lambda = \mathrm{pr}_\lambda \cdot f$ where the pr_λ are the projection maps. Therefore $\prod_{\lambda \in \Lambda} M_\lambda$ is called *the product module* of the family $M_\lambda, \lambda \in \Lambda$. The *(external) direct sum* of the family $M_\lambda, \lambda \in \Lambda$ is the submodule $\{y \in \prod_{\lambda \in \Lambda} M_\lambda \mid \mathrm{pr}_\lambda(y) = 0 \text{ except for finitely many } \lambda\}$ and is denoted $\bigoplus_{\lambda \in \Lambda} M_\lambda$. Fix $\lambda \in \Lambda$, and consider the family of R-homomorphisms $f_\mu : M_\lambda \longrightarrow M_\mu$, $\mu \in \Lambda$, defined by

$$f_\mu = \begin{cases} \mathrm{id}_{M_\lambda}, & \text{if } \mu = \lambda; \\ 0, & \text{otherwise.} \end{cases}$$

Therefore there is a map $\iota_\lambda : M_\lambda \longrightarrow \prod_{\mu\in\Lambda} M_\mu$ such that $\mathrm{pr}_\lambda \circ \iota_\lambda = \mathrm{id}_{M_\lambda}$ and $\mathrm{pr}_\mu \circ \iota_\lambda = 0$ for every $\mu \neq \lambda$. Since ι_λ is injective, it identifies M_λ with the submodule $\{(x_\mu)_{\mu\in\Lambda} \in \prod_{\mu\in\Lambda} M_\mu \mid x_\mu = 0 \text{ for every } \mu \neq \lambda\}$. Moreover $\mathrm{Im}(\iota_\lambda) \subseteq \bigoplus_{\mu\in\Lambda} M_\mu$ so ι_λ (by abuse of notation) will be thought of as an R-homomorphism $M_\lambda \longrightarrow \bigoplus_{\mu\in\Lambda} M_\mu$. Direct sum is a co-product in the category of R-modules: if $f_\lambda : M_\lambda \longrightarrow N$ are R-homomorphisms, then there is a unique R-homomorphism $f : \bigoplus_{\lambda\in\Lambda} M_\lambda \longrightarrow N$ such that $f_\lambda = f \cdot \iota_\lambda$.

2.2. **Proposition.** *Let M be an R-module, and $N_\lambda, \lambda \in \Lambda$ a family of submodules of M. Then the following are equivalent:*
(1) $\sum_{\lambda\in\Lambda} N_\lambda = \bigoplus_{\lambda\in\Lambda} N_\lambda$;
(2) If $\sum_{\lambda\in\Lambda} x_\lambda = 0$, with $x_\lambda \in N_\lambda$ for every $\lambda \in \Lambda$, then $x_\lambda = 0$ for every $\lambda \in \Lambda$.
(3) for every $\lambda \in \Lambda$, $N_\lambda \cap \sum_{\mu\in\Lambda} N_\lambda = 0$.

Proof. TBD □

If X is a set and R a ring, R^X (the cartesian product of a family indexed by X, with each member being R) is both the product ring (when this family is thought of as a family of rings) and the product R-module (when this family is thought of as a family of R-modules). By $R^{(X)}$, we mean the direct sum of this family of R-modules. For $x \in X$, the image of 1 under $\iota_x : R \longrightarrow R^{(X)}$ is denoted by e_x. Then every element of $R^{(X)}$ can be uniquely expressed a finite sum $\sum_{x\in X} r_x e_x$. This construction has the following property: if M is an R-module and $X \subseteq M$, then there exists a unique R-homomorphism $R^{(X)} \longrightarrow M$ with $e_x \mapsto x$. An R-module M is said to be *free* if there exists a subset $X \subseteq M$ such that the R-homomorphism $R^{(X)} \longrightarrow M$, $e_x \longrightarrow x$ is an isomorphism.

2.3. **Remark.** Let M be an R-module. Then $\mathrm{Hom}_R(M, -)$ (*respectively*, $\mathrm{Hom}_R(-, M)$) is a covariant (*respectively*, contravariant) left-exact functor from the category of R-modules to the category of abelian groups.

2.4. **Definition.** Let M be a right R-module and N a left R-module. The *tensor product* of M and N, denoted $M \otimes_R N$, is the abelian group $\mathbb{Z}^{(M\times N)}/B$, where B is the subgroup generated by the elements $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$ and $(xr, y) - (x, ry)$ for all $x, x' \in M$, $y, y' \in N$ and $r \in R$. The image of $(x, y) \in \mathbb{Z}^{(M\times N)}$ under the canonical surjective map $\mathbb{Z}^{(M\times N)} \longrightarrow M \otimes_R N$ is denoted by $x \otimes_R y$.

The set $\{x \otimes_R y \mid x \in M, y \in N\}$ generate $M \otimes_R N$ as an abelian group. There is no natural R-module structure on $M \otimes_R N$: if we try to define $r(x \otimes_R y) := (xr \otimes_R y) = (x \otimes_R ry)$, then $r(xr' \otimes_R y) = r(x \otimes_R r'y) = (x \otimes_R rr'y)$ one way and $r(xr' \otimes_R y) = (xr' \otimes_R ry) = (x \otimes_R r'ry)$ another way. However, the above calculation implies that if R is commutative, then there is a natural R-module structure on $M \otimes_R N$.

2.5. **Remark** (Universal property of tensor products)**.** See Bourbaki, Chapter II, Section 3.1, Proposition 1. See Proposition 3.1 for a restatement.

2.6. **Remark.** Let M be a right R-module and N a left R-module. Then $- \otimes_R N$ (*respectively*, $M \otimes_R -$) is a right-exact covariant functor from the category of right R-modules (*respectively*, left) to the category of abelian groups.

Exercises

(1) Let $\Bbbk$ be an algebraically closed field and R a finite-dimensional $\Bbbk$-algebra that has no zero-divisors. Show that $\Bbbk = R$. (Hint: Let $0 \neq r \in R$. Show that there is a map of $\Bbbk$-algebras $\Bbbk[X] \longrightarrow R$, $X \mapsto r$. What about the kernel of this map?)

(2) An R-module M is *faithful* if its annihilator is 0. Show that M is faithful if and only if the map $R \longrightarrow R_M$ (the ring of homotheties) is injective.

3. CHANGE OF RINGS

Let R and S be rings. An (S, R)-*bimodule* is an abelian group M that is a left S-module and a right R-module, such that the two structures are compatible with each other: $(sx)r = s(xr)$ for every $r \in R$, $s \in S$ and $x \in M$.

Let M be an (S, R)-bimodule, N a left R-module and P a left S-module. The abelian group $M \otimes_R N$ has a natural left S-module structure: $s(x \otimes_R y) = sx \otimes_R y$. This is well-defined since $s(x \otimes_R ry) = s(xr \otimes_R y) = (sxr) \otimes_R y$ and the element sxr is well-defined. The module $\operatorname{Hom}_S(M, P)$ has a natural left R-module structure: $r\phi := [x \mapsto \phi(xr)]$. (Check: $((r'r)\phi)(x) = \phi(x(r'r)) = \phi((xr')r) = (r\phi)(xr') = (r'(r\phi))(x)$; S-linearity: $(r\phi)(sx) = \phi(sxr) = s((r\phi)(x))$.)

The following is a restatement of the universal property of tensor products (Remark 2.5).

3.1. **Proposition.** *Let M (respectively, N) be a right (respectively, left) R-module and P an abelian group. Then the function*

$$\begin{array}{rcl} \operatorname{Hom}_{\mathbb{Z}}(M \otimes_R N, P) & \xrightarrow{\Phi} & \operatorname{Hom}_{\mathbb{Z}}(N, \operatorname{Hom}_{\mathbb{Z}}(M, P)) \\ g & \mapsto & [y \mapsto [x \mapsto g(x \otimes_R y)]] \end{array}$$

is an injective map of abelian groups, with $\operatorname{Im}\Phi = \operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(M, P))$. In particular the above map gives an isomorphism between $\operatorname{Hom}_{\mathbb{Z}}(M \otimes_R N, P)$ and $\operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(M, P))$.

Proof. It is easy to check that Φ is a map of abelian groups. Suppose that g is in the kernel. Then $g(x \otimes_R y) = 0$ for all $x \in M$ and $y \in N$, so $g = 0$. To prove the assertion about the image, note, first, that $\operatorname{Hom}_{\mathbb{Z}}(M, P)$ is indeed a left R-module. Let $g \in \operatorname{Hom}_{\mathbb{Z}}(M \otimes_R N, P)$, $y \in N$ and $r \in R$. We want to show that $\Phi(g)(ry) = r(\Phi(g)(y))$. Let $x \in M$; then $\Phi(g)(ry)(x) = g(x \otimes ry) = g(xr \otimes y) = \Phi(g)(y)(xr) = (r(\Phi(g)(y)))(x)$. Hence $\Phi(g)(ry) = r(\Phi(g)(y))$, proving that $\operatorname{Im}\Phi \subseteq \operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(M, P))$. Conversely let $\phi : N \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(M, P)$ be R-linear. Let $x \in M$ and $y \in N$. Then $\Phi : M \times N \longrightarrow P$, $(x, y) \mapsto \phi(y)(x)$ is $\mathbb{Z}$-bilinear, and satisfies $\Phi(xr, y) = \phi(y)(xr) = \phi(ry)(x) = \Phi(x, ry)$ for every $r \in R$. By the universal property of tensor products (Remark 2.5), there exists $g : M \otimes_R N \longrightarrow P$ such that $\phi(y)(x) = g(x \otimes y)$, i.e., $\phi = \Phi(g)$. Hence $\operatorname{Im}\Phi \supseteq \operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(M, P))$. □

3.2. **Proposition.** *Let M be an (S, R)-bimodule, N a left R-module and P a left S-module. The isomorphism of Proposition 3.1 restricts to an isomorphism*

$$\begin{array}{rcl} \operatorname{Hom}_S(M \otimes_R N, P) & \longrightarrow & \operatorname{Hom}_R(N, \operatorname{Hom}_S(M, P)) \\ g & \mapsto & [y \mapsto [x \mapsto g(x \otimes_R y)]] \end{array}$$

of abelian groups.

Proof. Consider the isomorphism

$$\begin{array}{rcl} \operatorname{Hom}_{\mathbb{Z}}(M \otimes_R N, P) & \xrightarrow{\Phi} & \operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(M, P)) \\ g & \mapsto & [y \mapsto [x \mapsto g(x \otimes_R y)]] \end{array}$$

from Proposition 3.1. It suffices to show that

$$\operatorname{Im}\Phi|_{\operatorname{Hom}_S(M \otimes_R N, P)} = \operatorname{Hom}_R(N, \operatorname{Hom}_S(M, P)).$$

Let $g \in \operatorname{Hom}_S(M \otimes_R N, P)$ and $y \in N$. Then, for every $x \in M$ and $s \in S$,

$$\Phi(g)(y)(sx) = g(sx \otimes y) = g(s(x \otimes y)) = s(g(x \otimes y)) = s((\Phi(g)(y))(x));$$

hence $\Phi(g)(y)$ is S-linear. Conversely, let $\phi : N \longrightarrow \operatorname{Hom}_S(M, P)$ be an R-linear map. We want to show that $g := \Phi^{-1}(\phi)$ is S-linear. Let $s \in S$, $x \in M$ and $y \in N$. Then

$$g(s(x \otimes y)) = g(sx \otimes y) = \phi(y)(sx) = s(\phi(y)(x)) = s(g(x \otimes y)),$$

so, indeed, g is S-linear. □

Now suppose, additionally, that R is commutative and that S is an R-algebra with the image of R in S lying inside the centre of S. Then $\mathrm{Hom}_S(M \otimes_R N, P)$ has a natural R-module structure: define rg to be the S-linear map $t \mapsto g(rt)$ for $t \in M \otimes_R N$. Hence the map in Proposition 3.2 is a R-homomorphism: $\Phi(rg)(y)(x) = (rg)(x \otimes_R y) = r(g(x \otimes_R y)) = r\Phi(g)(y)(x)$, and hence an R-isomorphism.

3.3. **Definition.** Let $\rho : R \longrightarrow S$ be a ring morphism, M a left R-module and N a left S-module. The left S-module $S \otimes_R M$ (treating S as a right R-module through $s \cdot r = s\rho(r)$) is denoted $\rho^* M$. The composite $R \xrightarrow{\rho} S \longrightarrow \mathrm{End}_{\mathbb{Z}}(N)$ makes N into a left R-module (i.e., $r \cdot y = \rho(r)y$); this R-module is denoted as $\rho_* N$.

3.4. **Proposition.** *Let $\rho : R \longrightarrow S$ be a ring morphism, M a left R-module and N a left S-module. Then there is an isomorphism*

$$\mathrm{Hom}_S(\rho^* M, N) \longrightarrow \mathrm{Hom}_R(M, \rho_* N)$$

Proof. This follows from Proposition 3.2, after observing that $\mathrm{Hom}_S(S, N) = N$ as S-modules and that $\mathrm{Hom}_R(M, N)$ is really $\mathrm{Hom}_R(M, \rho_* N)$. □

4. Semisimplicity

In this section, modules are left modules, unless specified otherwise.

4.1. **Definition.** An R-module M is said to be *simple* if it has no submodules different from M and 0.

4.2. **Example.** We give some examples of simple modules.

(1) ${}_R R$ simple if and only if 0 is a maximal left ideal, which holds if and only if R is a division ring. Indeed, if R is a division ring, then every non-zero element generates the unit ideal, so 0 is a maximal left ideal. Conversely, suppose that 0 is a maximal left ideal (which implies that $1 \neq 0$) and let $0 \neq r \in R$. Then $Rr = R$, so there exists $0 \neq r' \in R$ such that $r'r = 1$, and, furthermore, $0 \neq r'' \in R$ such that $r''r' = 1$. Hence r' is left-invertible and right-invertible, so it is invertible and its inverse is $r = r''$. Hence r is invertible.

(2) Let D be a division ring and M a finitely generated D-module. Then M is free. Write $R = \mathrm{End}_D(M)$. We now argue that M is a simple R-module. More precisely, we show the following: let $0 \neq x \in M$ and $y \in M$; then there exists $\phi \in R$ such that $\phi(x) = y$. To this end, let $f \in M^*$ be such that $f(x) = 1$ and define $\phi \in R$ as the map $v \mapsto f(v)y$.

(3) More examples to come.

4.3. **Proposition.** *Let M be an R-module. An R-submodule $N \subsetneq M$ is maximal among the proper R-submodules of M if and only if the quotient M/N is simple. If $M_1 \subsetneq M$ is an R-submodule, then there exists An R-submodule $N \subsetneq M$ that is maximal among the proper R-submodules of M containing M_1.*

Proof. TBD. □

4.4. **Definition.** A *Jordan-Hölder series* of M is a decreasing filtration $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = 0$ of submodules such that for every $1 \leq i \leq s$, M_{i-1}/M_i is a simple R-module; the integer s above is the *length* of the above Jordan-Hölder series. Say that an R-module N is *of finite length* (or is a *finite length* module) if N has a Jordan-Hölder series.

4.5. **Remark.** Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = 0$ be a Jordan-Hölder series of M and N a submodule of M. Then $(N \cap M_{i-1})/(N \cap M_i)$ is a submodule of M_{i-1}/M_i, so it is either 0 or simple. Hence by deleting repetitions from among the modules $N \cap M_i$, we obtain a Jordan-Hölder series of N. Similarly $(N + M_{i-1})/(N + M_i)$ is a quotient of M_{i-1}/M_i, so by deleting repetitions from among the modules $(N + M_i)/N$, we obtain a Jordan-Hölder series of M/N.

4.6. **Proposition.** *Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = 0$ and $M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_t = 0$ be two Jordan-Hölder series of M. Then $s = t$ and there exists a permutation σ of $\{1, \dots, s\}$ such that for every $1 \leq i \leq s$, $N_{i-1}/N_i = M_{\sigma(i-1)}/M_{\sigma(i)}$.*

Proof. Without loss of generality, $1 \leq s \leq t$. If $s = 1$, then M is simple, so the assertions are true. We proceed by induction. Assume that the assertions are true for all R-modules that have a Jordan-Hölder series of length at most $s - 1$. If $M_1 = N_1$, then by induction, the assertions hold for $M_1 = N_1$, so they hold for M. Therefore we may assume that $M_1 \neq N_1$.

Note that $N_1 \not\subset M_1$; for, otherwise, we have $N_1 \subsetneq M_1 \subsetneq M$, violating the simplicity of M/N_1. Similarly $M_1 \not\subset N_1$. Write $K = M_1 \cap N_1$. Then $M_1 \subsetneq M_1 + N_1$, so the simplicity of M/M_1 implies that $M_1 + N_1$; hence, $M_1/K \simeq M/N_1$ is simple. Similarly $N_1/K \simeq M/M_1$ is simple.

The assertions of the proposition hold for M_1, by induction. Let $K = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_r = 0$ be a Jordan-Hölder series of K. Then $M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r = 0$ is a Jordan-Hölder series of M_1. Hence $s - 1 = r + 1$, and the quotients in this Jordan-Hölder series are the same as the quotients in the series $M_1 \supsetneq \cdots \supsetneq M_s = 0$ after a suitable permutation.

Now, $N_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r = 0$ is a Jordan-Hölder series of N_1 of length $r + 1 = s - 1$, so, by induction, the assertions hold for N_1. Therefore $t - 1 = s - 1$ and the the quotients in this Jordan-Hölder series are the same as the quotients in the series $N_1 \supsetneq \cdots \supsetneq N_t = 0$ after a suitable permutation. Hence the assertions hold for the two given Jordan-Hölder series of M. ☐

4.7. **Remark.** Let R be a ring and M an R-module. Then M is simple as an R-module if and only if it is simple as a module over its ring of homotheties. This follows from noting that the structure of M as an R-module is defined through the ring map $R \longrightarrow \operatorname{End}_{\mathbb{Z}}(M)$, so it is the same as the structure of M as a module over the image of the above ring map.

4.8. **Proposition** (Schur lemma, version 1)**.** *Let R be a ring and M and N R-modules. Let $f : M \longrightarrow N$ be a non-zero R-morphism. Then:*

(1) If M is simple, f is injective.
(2) If N is simple, f is surjective.
(3) If M and N are simple, f is an isomorphism.

Proof. Since $f \neq 0$, $\ker f \subsetneq M$ and $0 \neq \operatorname{Im} f \subseteq N$. if M is simple, then $\ker f = 0$; if N is simple, then $\operatorname{Im} f = N$. ☐

4.9. **Corollary** (Schur lemma, version 2)**.** *If M is a simple R-module, then $\operatorname{End}_R(M)$ is a division ring.*

Proof. Every non-zero endomorphism of M is an isomorphism, i.e., an invertible element of $\operatorname{End}_R(M)$. ☐

4.10. **Corollary.** *Let $\Bbbk$ be an algebraically closed field, R a $\Bbbk$-algebra, M a simple R-module which is finite-dimensional as a $\Bbbk$-vector space. Then for every $\phi \in \operatorname{End}_R(M)$, there exists $\lambda \in \Bbbk$ such that $\phi(x) = \lambda x$ for every $x \in M$.*

Proof. Since $\operatorname{End}_R(M) \subseteq \operatorname{End}_{\Bbbk}(M)$ it is a finite-dimensional division ring over $\Bbbk$. Now use Section 1, Exercise 1.

Here is another proof. Let λ be an eigen-value of ϕ considered as a $\Bbbk$-endomorphism of M. The maps $\lambda \mathrm{id}_M$ and $\phi - \lambda \mathrm{id}_M$ are R-morphisms. Since λ is an eigen-value, $\ker(\phi - \lambda \mathrm{id}_M) \neq 0$, so, since M is a simple R-module, $\phi = \lambda \mathrm{id}_M$. ☐

4.11. **Corollary.** *With notation as in Corollary 4.10, if additionally R is commutative, then $\dim_{\Bbbk} M = 1$.*

Proof. Let $r \in R$. Then the homothety $x \mapsto rx$ is a R-morphism. Hence there exists $\lambda \in \Bbbk$ such that $rx = \lambda x$ for every $x \in M$. Therefore the ring R_M of homotheties coincides with the image of $\Bbbk$ in $\operatorname{End}_{\mathbb{Z}}(M)$. Hence M is simple over $\Bbbk$. ☐

4.12. **Proposition.** *Let M be an R-module that is the sum of a family $S_\lambda, \lambda \in \Lambda$ of simple submodules, and N a submodule of M. Then there exists $\Lambda_1 \subseteq \Lambda$ such that $M = N \oplus \bigoplus_{\lambda \in \Lambda_1} S_\lambda$.*

Proof. Without loss of generality $N \neq M$. Let $\mathcal{P}$ be the set of subsets $\Lambda' \subseteq \Lambda$ such that the sum $N + \sum_{\lambda \in \Lambda'} S_\lambda$ is a direct sum. It is non-empty, there exists $\lambda \in \Lambda$ such that $S_\lambda \not\subseteq N$, and, for such λ, $S_\lambda \cap N = 0$, so $S_\lambda + N = S_\lambda \oplus N$. Order $\mathcal{P}$ by inclusion. Let $\Lambda_i, i \in \mathcal{I}$ be a chain in $\mathcal{P}$. Then by Proposition 2.2 $\cup_{i \in \mathcal{I}} \Lambda_i \in \mathcal{P}$, so by Zorn's lemma, $\mathcal{P}$ has a maximal element Λ_1. Set $N' = N + \sum_{\lambda \in \Lambda_1} S_\lambda$. Now for every $\lambda \in \Lambda \smallsetminus \Lambda_1$, $\Lambda_1 \cup \{\lambda\} \notin \mathcal{P}$, so $S_\lambda \cap N' \neq 0$ (again by Proposition 2.2) which implies that $S_\lambda \subseteq N'$. Hence $M = N'$. $\square$

4.13. **Corollary.** *Let M be an R-module. Then the following are equivalent:*

(1) M is a sum of a family of simple submodules.
(2) M is the direct sum of a family of simple submodules.
(3) Every submodule of M is a direct summand of M.

We first need a lemma:

4.14. **Lemma.** *If every submodule of M is a direct summand of M then every non-zero submodule of M has a simple submodule.*

Proof. Let N be a non-zero submodule of M and $0 \neq x \in N$. Write $Rx \simeq R/I$ for some left R-ideal $I \neq R$. Let $\mathfrak{m}$ be a maximal left R-ideal containing I. We claim that $\mathfrak{m}x \subsetneq Rx$. Assume that claim: Then we have $\mathfrak{m}x \subsetneq Rx \subseteq M$. Since $\mathfrak{m}x$ is a direct summand of M, it is a direct summand of Rx. Hence Rx contains a submodule isomorphic to the simple module $R/\mathfrak{m}$. Now to prove the claim, assume, by way of contraction, that $\mathfrak{m}x = Rx$. Then there exist $a_1, \ldots, a_t \in \mathfrak{m}$ and $r_1, \ldots, r_t \in R$ such that $\sum_{i=1}^t r_i a_i x = x$. Hence $1 - \sum_{i=1}^t r_i a_i \in I \subseteq \mathfrak{m}$, so $1 \in \mathfrak{m}$, a contraction. $\square$

Proof of Corollary 4.13. (1) $\implies$ (2): Apply Proposition 4.12 with $N = 0$. (2) $\implies$ (1): Immediate. (1) $\implies$ (3): Apply Proposition 4.12. (3) $\implies$ (1): Let M' be the sum of simple submodules of M. Write $M = M' \oplus M''$. If M'' is non-zero, then it has a simple submodule by Lemma 4.14, which contradicts the fact that $M' \cap M'' = 0$. Hence $M = M'$. $\square$

4.15. **Definition.** An R-module M is said to be *semisimple* of it satisfies the (equivalent) conditions of Corollary 4.13.

4.16. **Remark.** Let M be a semisimple R-module.

(1) Let $S_\lambda, \lambda \in \Lambda$ be a family of simple submodules of M such that $M = \sum_{\lambda \in \Lambda} S_\lambda$. Let N be a submodule of M. Then there exists $\Lambda_1 \subseteq \Lambda$ such that $M = N \oplus \bigoplus_{\lambda \in \Lambda_1} S_\lambda$. (Proposition 4.12.) Write $N' = \bigoplus_{\lambda \in \Lambda_1} S_\lambda$. The composite map $N' \hookrightarrow M \twoheadrightarrow M/N$ is an isomorphism, and the images of $S_\lambda, \lambda \in \Lambda_1$ in M/N are simple submodules of M/N; hence M/N is semisimple. Applying the above argument to N', we see that $N \simeq M/N'$ is semisimple.

(2) M is simple if and only if $\operatorname{End}_R(M)$ is a division ring. 'Only if' follows from the Schur lemma (Corollary 4.9). Conversely, if M is not simple, then it has a simple direct summand N; the projection to N followed by the inclusion $N \longrightarrow M$ gives a non-invertible endomorphism of M.

4.17. **Definition.** Let E be a ring and B a subset of E. The *commutant* of B (in E) is the subring $\{e \in E \mid eb = be \text{ for every } b \in B\}$ of E. The *bicommutant* of B is the commutant of the commutant of B.

4.18. **Remark.** Let E and B be as in the definition above. Write B' and B'' for the commutant and the bicommutant, respectively, of B in E.

(1) $B \subseteq B''$ and B' equals its bicommutant. Proof: TBD.

(2) If B is a subring of E, then $B' \cap B = \{e \in B \mid eb = be \text{ for every } b \in B\}$ is the centre of B. Therefore $B'' \cap B$ is the centre of B'. Additionally, if $b \in B'' \cap B$, then for every $c \in B''$, $cb = bc$, so $B'' \cap B$ is the centre of B'' also. In particular, B' and B'' have the same centre.

(3) If B is a commutative subring of E (not necessarily central in E) then $B \subseteq B'$. Hence $B'' \subseteq B'$, and, therefore, B'' is the centre of B'.

4.19. **Definition.** Let M be an R-module. The *commutant* and the *bicommutant* of M are the commutant and the bicommutant of the ring R_M of homotheties in $\mathrm{End}_{\mathbb{Z}}(M)$, respectively.

4.20. **Remark.** The commutant of M is $\mathrm{End}_R(M)$. To see this, note that if $h_r \in R_M$ is the homothety $x \mapsto rx$ and $f \in \mathrm{End}_{\mathbb{Z}}(M)$, then the condition $h_r f = f h_r$ is another way of stating that for every $x \in M$, $rf(x) = (h_r f)(x) = (f h_r)(x) = f(rx)$. Hence the bicommutant of M is $\mathrm{End}_{\mathrm{End}_R(M)}(M)$.

4.21. **Proposition.** *Let R be a ring and M an R-module. Write R'' for the bicommutant of M.*

(1) Let I be a set. The bicommutant of the R-module $M^{(I)}$ is the ring of homotheties of the R''-module $M^{(I)}$.

(2) Suppose that M is semisimple. Then for every $x \in M$ and every $s \in R''$, there exists $r \in R$ such that $sx = rx$. In particular, every R-submodule of M is also an R''-submodule.

Proof. (1): TBD

(2): Let $x \in M$. Then Rx is an R-direct summand of M. Let $\phi \in \mathrm{End}_R(M)$ be the projection endomorphism with image Rx. Let $s \in R''$. Then $s\phi = \phi s$ (as elements of $\mathrm{End}_{\mathbb{Z}}(M)$). Hence for every $y \in Rx$, $sy = s\phi(y) = \phi(sy)$, so $sy \in Rx$. □

4.22. **Theorem** (Jacobson density theorem)**.** *Let R be a ring and M a semisimple R-module. Write R'' for the bicommutant of M. Let $s \in \mathrm{End}_{\mathbb{Z}}(M)$. Then $s \in R''$ if and only if for every finite subset $X \subseteq M$, there exists $r \in R$ such that $sx = rx$ for every $x \in X$.*

Proof. 'If': Let $\phi \in \mathrm{End}_R(M)$ and $x \in M$. Let $r \in R$ be such that $sx = rx$ and $s\phi(x) = r\phi(x)$ (apply the hypothesis to $X = \{x, \phi(x)\}$). Then $s\phi(x) = r\phi(x) = \phi(rx) = \phi(sx)$. Hence $s\phi = \phi s$ (as elements of $\mathrm{End}_{\mathbb{Z}}(M)$) for every $\phi \in \mathrm{End}_R(M)$, i.e., $s \in R''$.

'Only if': Let $X = \{x_1, \ldots, x_n\}$, $n \geq 1$. Write $x = (x_1, \ldots, x_n) \in M^n$. Consider the R''-homothety $(y_1, \ldots, y_n) \mapsto (sy_1, \ldots, sy_n)$ of M. By Proposition 4.21(1) there exists an element $\tilde{s}$ of the bicommutant of the R-module M^n such that $\tilde{s}((y_1, \ldots, y_n)) = (sy_1, \ldots, sy_n)$. Note that M^n is a semisimple R-module. By Proposition 4.21(2) there exists $r \in R$ such that $(sx_1, \ldots, sx_n) = \tilde{s}x = rx = (rx_1, \ldots, rx_n)$, i.e., $sx = rx$ for every $x \in X$. □

4.23. **Definition.** Let S be a simple R-module and M an R-module. Say that M is *isotypic of type* S if $M \simeq S^{(I)}$ for some set I. Say that M is *isotypic* if there exists a simple R-module T such that M is isotypic of type T.

4.24. **Remark.** Every isotypic R-module is semisimple. If $M_\lambda, \lambda \in \Lambda$ is a family of R-modules with M_λ isotypic of type S (where S is a simple R-module), for every $\lambda \in \Lambda$, then $\bigoplus_{\lambda \in \Lambda} M_\lambda$ is isotypic of type S. If S is a simple R-module, I a set and M a submodule of $S^{(I)}$, then M is isotypic of type S: for, if M' is a submodule of $S^{(I)}$ with $M + M' = S^{(I)}$ and $M \cap M' = 0$, then $M \simeq S/M' \simeq S^{(I_1)}$ for some $I_1 \subseteq I$ (Proposition 4.12).

4.25. **Definition.** R is said to be a *semisimple ring* if ${}_RR$ is a semisimple R-module. R is said to be a *simple ring* if it is a semisimple ring and there is a unique simple R-module up to isomorphism.

4.26. **Remark.** Let R be a ring.

(1) Suppose that R is semisimple. Then it has finitely many simple modules, up to isomorphism. For, write ${}_RR$ as the (direct) sum of a family $S_\lambda, \lambda \in \Lambda$ of R-modules. Let T be a simple R-module. Let $0 \neq x \in T$. The R-morphism map ${}_RR \longrightarrow T$, $1 \mapsto x$ is surjective. Therefore there exists $\mu \in \Lambda$ such that $T \simeq S_\mu$ (Remark 4.16(1)). Hence each simple R-module is isomorphic to a submodule of ${}_RR$. Let $S_i, i \in \mathcal{I}$ be all the distinct simple R-modules, up to isomorphism. Write ${}_RR \simeq \bigoplus_{i \in \mathcal{I}} M_i$ where, for every $i \in \mathcal{I}$, M_i is a direct sum of copies of S_i.

Since ${}_RR$ is a finitely-generated R-module, $\mathcal{I}$ must be a finite set and for each $i \in \mathcal{I}$, M_i must be a direct sum of finitely many copies of S_i.

(2) Suppose that R is semisimple. Then every R-module is semisimple, since every R-module is a quotient of ${}_RR^{(I)}$ for some I, which is semisimple.

(3) If R is a simple ring, then, for some set I, ${}_RR \simeq S^{(I)}$ where S the unique (up to isomorphism) simple R-module; hence ${}_RR$ is isotypic. Conversely, if ${}_RR$ is isotypic of type S, then (a) ${}_RR$ is semisimple; (b) if T is a simple R-module, then $T \simeq S$ (as in Remark 4.26(1), using Remark 4.16(1)). Hence R is a simple ring.

4.27. **Proposition.** *Let R be a simple ring. Then:*

(1) The only two-sided ideals of R are 0 and R.

(2) Every simple module over R is faithful.

Proof. (1): Let I be any simple left R-ideal. If J is any other simple left ideal then it is isomorphic to J (as a left R-module). Both I and J are direct summands of ${}_RR$. Thus we get an R-endomorphism of ${}_RR$ as the composite ${}_RR \twoheadrightarrow I \simeq J \hookrightarrow {}_RR$. Every endomorphism f of ${}_RR$ is given by multiplication by $f(1)$ on the right. Thus we see that for every simple left ideal J, there exists $\alpha_J \in R$ such that the map $I \longrightarrow J$, $x \mapsto x\alpha_J$ is an isomorphism. Since R is a direct sum of simple left ideals, $IR = R$. Hence the only non-zero two-sided ideal is R.

(2): The annihilator of any non-zero left R-module is a two-sided proper ideal of R. Now use (1). □

4.28. **Proposition.** *Let D be division ring and M a finitely generated D-module. Write $R = \operatorname{End}_D(M)$. Then R is a simple ring, M a simple and faithful R-module and $D \simeq \operatorname{End}_R(M)$.*

Proof. Write $R = \operatorname{End}_D(M)$. That M is simple over R was established in Example 4.2(2). Since $R \subseteq \operatorname{End}_{\mathbb{Z}}(M)$, the map $R \longrightarrow R_M$ is an isomorphism, so M is a faithful R-module.

Write $S = \operatorname{End}_R(M)$ the bicommutant of M. We have maps $D \longrightarrow D_M \subseteq S$ (where D_M denotes the ring of homotheties). Since D is a division ring, the map $D \longrightarrow D_M$ is an isomorphism. Let $s \in S$. We want to show that there exists $a \in D$ such that $s = h_a$, the homothety $x \mapsto rx$. Fix $x \in M$. Note that M is a semisimple D-module. By the density theorem (Theorem 4.22) (in fact, Proposition 4.21(2) is enough) there exists $a \in D$ such that $sx = h_a x$. Let $y \in M$; there exists $\phi \in R$ such that $\phi(x) = y$; see Example 4.2(2). Then $sy = s(\phi(x)) = \phi(sx) = \phi(h_a x) = h_a\phi(x) = h_a y$. This is true for every $y \in M$, so $s = h_a$.

Define a map ${}_RR \longrightarrow M^n$ by $\phi \mapsto (\phi(x_i))$. This is a map of left R-modules. If $\phi(x_i) = 0$ for every i, then for every $y = \sum_i a_i x_i$ (with $a_i \in D$ for every i) $\phi(y) = \sum_i \phi(a_i x_i) = \sum_i a_i \phi(x_i) = 0$, so $\phi = 0$, since M is a faithful R-module. Hence ${}_RR$ is an R-submodule of M^n, which is isotypic. Hence R is simple by Remarks 4.24 and 4.26(3). □

4.29. **Theorem** (Wedderburn)**.** *Let R be a ring. Then R is simple if and only if it is isomorphic to $M_n(D)$ for some division ring D and a positive integer n.*

Proof. 'If' is a corollary of Proposition 4.28. Conversely, suppose that R is simple. Let S be the unique (up to isomorphism) simple R-module and $D = \operatorname{End}_R(S)$. Note that the commutant of S (as an R-module) is D. The bicommutant of S (as an R-module) is $\operatorname{End}_D(S)$, so we have a natural ring map $R \longrightarrow R_S \subseteq \operatorname{End}_D(S)$. The map $R \longrightarrow R_S$ is an isomorphism since S is a faithful R-module (Proposition 4.27(2)).

Let $v_1, \dots, v_n$ be a basis of S as a D-module. Let $\phi \in \operatorname{End}_D(S)$. By the density theorem (Theorem 4.22) there exists $r \in R$ such that $\phi(v_i) = rv_i$ for every $1 \leq i \leq n$. Hence $\phi(\sum_i d_i v_i) = \sum_i (d_i r) v_i = \sum_i (r d_i) v_i = r(\sum_i d_i v_i)$ for every collection $d_1, \dots, d_n \in D$. Hence the map $R \longrightarrow R_S \subseteq \operatorname{End}_D(S)$ is surjective, and an isomorphism. □

4.30. **Lemma.** *Let $\phi : R \longrightarrow R'$ be an isomorphism of rings. Let I be a left R-ideal. Then*

(1) $I' := \phi(I)$ is a left R'-ideal and the induced map $\phi|_I : I \longrightarrow I'$ is an isomorphism of R-modules, where R acts on I' through ϕ.

(2) *The ring map $\Phi : \mathrm{End}_{\mathbb{Z}}(I) \longrightarrow \mathrm{End}_{\mathbb{Z}}(I')$, $f \mapsto \phi|_I \circ f \circ \phi|_I^{-1}$ is an isomorphism. Moreover, for every $r \in R$, $\Phi(h_r) = h_{\phi(r)}$ (where h_r denotes the homethety $x \mapsto rx$ of I).*

(3) *Write S and S' for the commutants of I and I' respectively. Then $\Phi(S) = S'$; this gives a ring isomorphism $\Phi|_S : S \longrightarrow S'$.*

Proof. (1): Since I' is an abelian group, it suffices to show that for every $r' \in R'$ and $x \in I'$, $r'x' \in I'$. This indeed is true since $r'x' = \phi(\phi^{-1}(r')\phi^{-1}(x'))$. To show that $\phi|_I : I \longrightarrow I'$ is an isomorphism of R-modules, it suffices to check that it is also an R-morphism, since it is an isomorphism of abelian groups; this is immediate.

(2): It is straightforward to check that the ring map $\mathrm{End}_{\mathbb{Z}}(I') \longrightarrow \mathrm{End}_{\mathbb{Z}}(I), g \mapsto \phi|_I^{-1} \circ g \circ \phi|_I$ is the inverse of Φ. Let $y \in I'$ and $r \in R$. We want to show that $(\phi|_I \circ h_r \circ \phi|_I^{-1})(y) = h_{\phi(r)}(y)$. This follows immediately from the definitions.

(3): '$\subseteq$': Let $s \in S$, $r' \in R'$ and $y \in I'$; we want to show that $\Phi(s)(h_{r'}(y)) = h_{r'}(\Phi(s)(y))$. Write $r' = \phi(r)$ and $y = \phi(x)$. Then $\Phi(s)(h_{r'}(y)) = \phi(s(h_r(x)))$ and $h_{r'}(\Phi(s)(y)) = \phi(h_r(s(x)))$. Since $s \in S$, we have that $h_r(s(x)) = s(h_r(x))$.

'$\supseteq$': Let $s' \in S'$. Write $s' = \Phi(s)$ with $s \in \mathrm{End}_{\mathbb{Z}}(I)$. We need to show that $s \in S$. Let $r \in R$ and $x \in I$; we want to show that $s(h_r(x)) = h_r(s(x))$. This follows from noting that $\phi(s(h_r(x))) = s'(h_{\phi(r)}(\phi(x))) = h_{\phi(r)}(s'(\phi(x))) = \phi(h_r(s(x)))$. □

4.31. **Proposition.** *Let D_1 and D_2 be division rings and n_1 and n_2 positive integers. Then $M_{n_1}(D_1) \simeq M_{n_2}(D_2)$ if and only if $D_1 \simeq D_2$ and $n_1 = n_2$.*

Proof. 'If' is immediate. Conversely, first, by looking at Jordan-Hölder sequences, we conclude that $n_1 = n_2$ which we call n. Let $\phi : M_n(D_1) \longrightarrow M_n(D_2)$ be an isomorphism. Apply Lemma 4.30 with $R = M_n(D_1)$ and $R' = M_n(D_2)$ and I any simple left ideal of $M_n(D_1)$. Then, in the notation of that Lemma, $I \simeq D_1^n$ (as $M_n(D_1)$-modules), $I' \simeq D_2^n$ (as $M_n(D_2)$-modules) $S \simeq D_1$ and $S' \simeq D_2$ (as rings, in both the cases). □

4.32. **Theorem** (Wedderburn). *Let R be a semisimple ring and ${}_RR = \bigoplus_{i=1}^m I_i$ the isotypic decomposition of ${}_RR$ (into left R-ideals). Write $1 = e_1 + \cdots + e_m$ with $e_i \in I_i$ for every i. Then:*

(1) *For each $1 \le i \le m$, I_i is a two-sided R-ideal.*

(2) *For each $1 \le i \le m$, I_i is a simple ring with the operations induced from R and with e_i as the multiplicative identity.*

(3) *$R = \prod_{i=1}^m I_i$ as rings.*

4.33. **Lemma.** *Let R be a ring, I a simple left R-ideal and M a simple R-module. If I is not isomorphic to M, then $IM = 0$.*

Proof. IM is a submodule of M, so $IM = 0$ or $IM = M$. If $IM = M$, then there exists $x \in M$ such that $Ix \neq 0$, so $Ix = M$. Hence the map $I \longrightarrow M, r \mapsto rx$ is an R-isomorphism. □

Proof of Theorem 4.32. (1): Note that for $j \neq i$, $I_iI_j = 0$ by Lemma 4.33. Hence $I_i \subseteq I_iR = I_iI_i \subseteq I_i$, so $I_iR = I_iI_i = I_i$, i.e., I_i is a two-sided ideal.

(2): We already checked that I_i is closed under the multiplication induced from R. For every $r \in I_i$, $r = r(e_1 + \cdots + e_m) = re_i$.

(3): For $1 \le i \le n$, write $J_i = \bigoplus_{\substack{1 \le j \le m \\ j \neq i}} I_i$; The natural projection map $R \longrightarrow I_i$ is a ring homomorphism, with kernel J_i. Therefore it suffices to show that the natural map $R \longrightarrow \prod_{i=1}^m R/J_i$ is an isomorphism, for which we will use Theorem 1.16. Let $r \in R$. Write $r = \sum_{i=1}^n r_i$, with $r_i \in I_i$ for every i. Then $re_i = r_ie_i = r_i(\sum_{j=1}^n e_j)(\sum_{j=1}^n e_j)r_i = e_ir_i$, so e_i is a central idempotent for every i. Since $I_iI_j = 0$ for every $i \neq j$, $e_ie_j = 0$ for every $i \neq j$. Note that $I_i = Re_i$ and that $J_i = R(1 - e_i)$. Hence by Theorem 1.16 the natural map $R \longrightarrow \prod_{i=1}^m R/J_i$ is an isomorphism. □

4.34. **Corollary.** *Let R be a ring. Then R is semisimple if and only if it is of the form $\prod_{i=1}^m M_{n_i}(D_i)$ for some division rings $D_1, \ldots, D_n$ and positive integers $n_1, \ldots, n_m$.*

Proof. ‘Only if’: Use Theorems 4.32 and 4.29. ‘If’: see Exercise below. □

EXERCISES

(1) Let R and S be rings and M and N a semisimple R-module and a semisimple S-module respectively. Show that $M \oplus N$ is a semisimple $(R \times S)$-module.

(2) Let R be a ring and M a semisimple R-module. Let N be a simple R-module. Let M' be a submodule of M. Then the following are equivalent:

(a) M' is the largest isotypic submodule of M of type N, i.e., M' is isotypic of type N and if N' is a simple submodule of M isomorphic to N, then $N' \subseteq M'$.

(b) M' is the (direct) sum of all the simple submodules of M that are isomorphic to N.

(c) $M' = \operatorname{Hom}_R(N, M)$.

Let $N_\lambda, \lambda \in \Lambda$ be all the distinct (up to isomorphism) simple R-modules. Then $M = \bigoplus_{\lambda\in\Lambda} \operatorname{Hom}_R(N_\lambda, M)$. This is called the *isotypic decomposition* of M.

5. INTRODUCTION TO REPRESENTATION THEORY

Throughout this section $\Bbbk$ denotes a commutative ring. A $\Bbbk$-*algebra* is a ring R with a ring homomorphism $\Bbbk \longrightarrow R$ (often understood from the context and not stated explicitly) whose image is inside the centre of R. (That is, for us, a $\Bbbk$-algebra is unital and associative.) If $\Bbbk$ is field, then a $\Bbbk$-algebra R is said to be *finite-dimensional* if $\dim_\Bbbk R$ is finite. (Note that the ring map $\Bbbk \longrightarrow R$ makes R into a $\Bbbk$-vector-space.)

5.1. **Discussion.** Let G be a group. We make the free $\Bbbk$-module $\Bbbk^{(G)}$ into a $\Bbbk$-algebra as follows. Let $e_g, g \in G$ denote the standard basis for $\Bbbk^{(G)}$. Then set $e_g e_h = e_{gh}$; now extend it to $\Bbbk^{(G)}$ by setting $(\sum_{i=1}^n a_i e_{g_i})(\sum_{j=1}^m b_j e_{h_j}) = \sum_{i,j} a_i b_j e_{g_i h_j}$. This gives a ring with identity element e_1. The map $\Bbbk \longrightarrow \Bbbk^{(G)}$, $a \mapsto a e_1$ is a ring homomorphism; its image is inside the centre of $\Bbbk^{(G)}$. Thus we get a $\Bbbk$-algebra structure on $\Bbbk^{(G)}$; we denote it by $\Bbbk[G]$. We will write 1 for the element e_1. □

5.2. **Remark.** Let G be a group. $\Bbbk[G]$ is commutative if and only if $e_g e_h = e_h e_g$ for all $g, h \in G$ which holds if and only if G is an abelian group. For a positive integer r, $\Bbbk[\mathbb{Z}^r] = \Bbbk[x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_n, x_n^{-1}]$ and $\Bbbk[\mathbb{Z}/r] \simeq \Bbbk[x]/(x^r - 1)$. If $\Bbbk$ is a field, then $\Bbbk[G]$ is a finite-dimensional $\Bbbk$-algebra if and only if G is a finite group.

5.3. **Definition.** Let G be a group and M a $\Bbbk$-module. A *(linear) representation* of G on M is a group homomorphism $\rho : G \longrightarrow \operatorname{Aut}_\Bbbk(M)$, the group of invertible $\Bbbk$-endomorphisms of M. We denote this representation by (M, ρ); if the map ρ is understood from the context, we omit it from the notation and say that M is a representation of G. Moreover, when no confusion is likely to occur, we will write g for the automorphism $\rho(g) : M \longrightarrow M$.

5.4. **Example.** In these examples assume that M is free $\Bbbk$-module of rank n with basis $\{v_1, \ldots, v_n\}$. However, no generality is lost if one further assumes that $\Bbbk$ is a field.

(1) Identify $\operatorname{Aut}_\Bbbk(M)$ with $\operatorname{GL}_n(\Bbbk)$ (the group of invertible $n \times n$ matrices over $\Bbbk$) using the given basis. The cyclic group $\mathbb{Z}/n$ acts on $\{v_1, \ldots, v_n\}$ by cyclically permuting its elements. This gives a representation of $\mathbb{Z}/n$ on M which is given by the group homomorphism $\mathbb{Z}/n \longrightarrow \operatorname{GL}_n(\Bbbk)$

$$\overline{1} \mapsto \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

(2) More generally, every subgroup of the permutation group S_n has a *permutation representation* on M by $\sigma : v_i \mapsto v_{\sigma(i)}$. The image of σ in $\mathrm{GL}_n(\Bbbk)$ is the *permutation matrix* A_σ associated to σ, which is given by

$$(A_\sigma)_{i,j} = \begin{cases} 1, & \text{if } i = \sigma(j); \\ 0, & \text{otherwise.} \end{cases}$$

(3) Even more generally, if X is a set on which G acts on the left (as permutations), then we get a permutation representation of G on the free module $\Bbbk^{(X)}$ by $g : e_x \mapsto e_{g(x)}$. An important example of this is the *regular representation* of G: G acts on itself by left multiplication; this extends to a representation of G on $\Bbbk[G]$ satisfying $g : e_h \mapsto e_{gh}$.

5.5. **Discussion.** Let G be a group, and M, N representations of G. A *homomorphism of G-representations* (or a G-homomorphism) $\phi : M \longrightarrow N$ is is a $\Bbbk$-homomorphism $\phi : M \longrightarrow N$ satisfying $\phi(gx) = g(\phi(x))$ for every $x \in M$ and $g \in G$. Thus we can talk of the *category of G-representations*. We say that N is a *G-subrepresentation* of M if it is $\Bbbk$-submodule of M and the inclusion map is a G-homomorphism; in this case, for every $g \in G$, the $\Bbbk$-automorphism g of M induces a $\Bbbk$-automorphism of the quotient $\Bbbk$-module M/N, so M/N has a natural G-representation structure such that the quotiet map $M \longrightarrow M/N$ is a G-homomorphism. Therefore the kernel, the image and the cokernel of a G-homomorphism are G-representations. Moreover if $M_\lambda, \lambda \in \Lambda$ is a family of G-representations, then the $\Bbbk$-module $\bigoplus_{\lambda\in\Lambda} M_\lambda$ has a natural G-action, and is the direct sum in the category of G-representations. Similarly, the $\Bbbk$-module $\prod_{\lambda\in\Lambda} M_\lambda$ has a natural G-action, and is the product in the category of G-representations. □

5.6. **Discussion.** Let $\rho : G \longrightarrow \mathrm{Aut}_{\Bbbk}(M)$ be a representation of G on M. This extends to a homomorphism of $\Bbbk$-algebras $\overline{\rho} : \Bbbk[G] \longrightarrow \mathrm{End}_{\Bbbk}(M)$ determined (uniquely) by $\overline{\rho}(e_g) = \rho(g)$. Conversely, if $\sigma : \Bbbk[G] \longrightarrow \mathrm{End}_{\Bbbk}(M)$ is a homomorphism of $\Bbbk$-algebras, then we get a group homomorphism $\sigma' : G \longrightarrow \mathrm{Aut}_{\Bbbk}(M)$, by $\sigma'(g) = \sigma(e_g)$, since the elements e_g are invertible in $\Bbbk[G]$. The operations are inverses of each other: $(\overline{\rho})' = \rho$ and $\overline{(\sigma')} = \sigma$. Hence defining a G-representation on a $\Bbbk$-module M is equivalent to defining a $\Bbbk[G]$-module structure on M (compatible with the given $\Bbbk$-module structure). For G-representations M and N, a $\Bbbk$-homomorphism $\phi : M \longrightarrow N$ is a G-homomorphism) precisely when it is a $\Bbbk[G]$-homomorphism. Therefore the categories of G-representations and of $\Bbbk[G]$-modules is equivalent. The notions defined in Discussion 5.5 match the corresponding notions for $\Bbbk[G]$-modules. Therefore we will interchangeably use 'G-representations' and '$\Bbbk[G]$-modules' (and sometimes, merely, 'G-modules'). □

5.7. **Theorem.** *Let G be a finite group with $|G|$ invertible in $\Bbbk$. Let M be a $\Bbbk[G]$-module, and N a $\Bbbk[G]$-submodule of M that is a direct summand of M as a $\Bbbk$-module. Then N is a direct summand as a $\Bbbk[G]$-module.*

Proof. Let $p \in \mathrm{End}_{\Bbbk}(M)$ be a projection with image N. Define a $\Bbbk$-endomorphism $q : M \longrightarrow M$ by

$$x \mapsto \frac{1}{|G|} \sum_{g\in G} gp(g^{-1}x).$$

The image of q is N and, for every $x \in N$, $q(x) = x$. Hence $M = N \oplus (\ker q)$ as $\Bbbk$-modules. Moreover, $q(gx) = \frac{1}{|G|}\sum_{h\in G} hp(h^{-1}gx) = g\frac{1}{|G|}\sum_{h\in G} g^{-1}hp(h^{-1}gx) = g\frac{1}{|G|}\sum_{h\in G} hp(h^{-1}x) = gq(x)$ for every $g \in G$, so $(\ker q)$ is a $\Bbbk[G]$-module. Hence N is a direct summand of M as a $\Bbbk[G]$-module. □

5.8. **Corollary** (Maschke)**.** *Let $\Bbbk$ be a field and G a finite group with $|G|$ invertible in $\Bbbk$. Then $\Bbbk[G]$ is a semisimple ring.*

Proof. For every $\Bbbk[G]$-module M and $\Bbbk[G]$-submodule N of M, N is a direct summand of M as a $\Bbbk$-module. By Theorem 5.7, N is a direct summand of M as a $\Bbbk[G]$-module; now apply Corollary 4.34. □

5.9. **Remark.** The assertion of the Corollary 5.8 fails if $|G|$ is not invertible in $\Bbbk$. Consider the element $\epsilon = \sum_{g \in G} g \in \Bbbk[G]$. For every $g \in G$, $g\epsilon = \epsilon = \epsilon g$, so $\epsilon^2 = |G|\epsilon = 0$ and $\epsilon \in \Bbbk[G]g$, the left ideal generated by g. Hence the left module $\Bbbk[G]\epsilon$ is not a direct summand of the left module $\Bbbk[G]$. In particular $\Bbbk[G]$ is not a semisimple ring.

5.10. **Corollary.** *Let G be a finite group with $|G|$ invertible in $\Bbbk$. An exact sequence of $\Bbbk[G]$-modules is split if and only if it is split as an exact sequence of $\Bbbk$-modules.*

Proof. 'If' is immediate. 'Only if': Let $0 \longrightarrow M_1 \xrightarrow{f} M_2 \longrightarrow M_3 \longrightarrow 0$ be an exact sequence of $\Bbbk[G]$-modules. If it is split as a sequence of $\Bbbk$-modules, then $\operatorname{Im}(f)$ is a direct summand of M_2 as a $\Bbbk$-module, so by Theorem 5.7, it is a direct summand also as a $\Bbbk[G]$-module, i.e., the sequence is split as a sequence of of $\Bbbk[G]$-modules. □

5.11. **Corollary.** *Let G be a finite group with $|G|$ invertible in $\Bbbk$. A $\Bbbk[G]$-module is projective if and only if it is projective as a $\Bbbk$-module. In particular, if $\Bbbk$ is a field, then every $\Bbbk[G]$-module is projective.*

Proof. Let M be a $\Bbbk[G]$-module and F a free $\Bbbk[G]$-module with a surjective $\Bbbk[G]$-morphism $\phi : F \longrightarrow M$. If M is projective as a $\Bbbk[G]$-module, then ϕ is split as a $\Bbbk[G]$-morphism, and, *a fortiori*, as a $\Bbbk$-morphism. Hence M is a projective $\Bbbk$-module. Conversely, if M is a projective a $\Bbbk$-module, then ϕ is split as a $\Bbbk$-morphism. By Theorem 5.7, $\ker \phi$ is a direct summand of F as a $\Bbbk[G]$-module, so ϕ is split as a $\Bbbk[G]$-morphism. Hence M is a projective $\Bbbk[G]$-module. □

5.12. **Discussion** (Frobenius reciprocity)**.** Let H be a subgroup of G, and denote the inclusion map $\Bbbk[H] \longrightarrow \Bbbk[G]$ by ρ. The functor ρ_* (from the category of $\Bbbk[G]$-modules to the category of $\Bbbk[H]$-modules, treating a a $\Bbbk[G]$-module as $\Bbbk[H]$-module through restriction of scalars) is called the *restriction functor* and is denoted Res_H^G. The functor $\rho^*(-) = \Bbbk[G] \otimes_{\Bbbk[H]} -$ (from $\Bbbk[H]$-modules to the category of $\Bbbk[G]$-modules, treating $\Bbbk[G]$ as a right $\Bbbk[H]$-module) is called the *induction functor* and is denoted Ind_H^G; for a $\Bbbk[G]$-module M, $\operatorname{Ind}_H^G(M)$ is called the representation of G induced from M. Hom-$\otimes$ adjunction (Proposition 3.2) gives

$$\operatorname{Hom}_{\Bbbk[H]}(M, \operatorname{Res}_H^G N) = \operatorname{Hom}_{\Bbbk[G]}(\operatorname{Ind}_H^G M, N)$$

for every H-module M and G-module M. □

5.13. **Setup.** For the remainder of this section, let $\Bbbk$ be a field and G a finite group with $|G|$ invertible in $\Bbbk$. Let

$$\Bbbk[G] = \prod_{i=1}^{c} R_i$$

be the decomposition as the product of simple rings R_i. Let $1 \leq i \leq c$. Write e_i for the identity element of R_i. Let M_i be a simple R_i-module and $D_i = \operatorname{End}_{R_i}(M_i)$. Write $d_i = \dim_\Bbbk M_i$. Denote the simple characters (defined below) by $\chi_1, \ldots, \chi_c$.

5.14. **Definition.** Let $\rho : G \longrightarrow \operatorname{Aut}_\Bbbk(M)$ be representation. The *character* of ρ, denoted χ_ρ, is the function $G \longrightarrow \Bbbk$, $g \mapsto \operatorname{Trace}(\rho(g))$. Its $\Bbbk$-linear extension to $\Bbbk[G]$ will also be denoted by χ_ρ. A *simple* (or *irreducible*) character of G is the character of a simple G-module.

Note that the number of simple characters equals the number c of the factors in the decomposition of $\Bbbk[G]$ as a product of simple rings in Setup 5.13, since every simple $\Bbbk[G]$-module is a simple module over R_j for some j.

5.15. **Lemma.** *For all $1 \leq i, j \leq c$,*

$$\chi_j(e_i) = \begin{cases} d_i, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Note that M_j is a summand of R_j for every j. Thus $e_i : M_j \longrightarrow M_j$ is the identity map of M_i if $j = i$ and the zero map otherwise. Therefore

$$\chi_j(e_i) = \operatorname{Trace}(M_j \xrightarrow{e_i} M_j) = \begin{cases} d_i, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases} \qquad \square$$

5.16. **Proposition.** *Let χ_{reg} denote the character of the regular representation. Then $\chi_{\mathrm{reg}}(1) = |G|$ and for every $g \in G, g \neq 1$, $\chi_{\mathrm{reg}}(g) = 0$.*

Proof. For any finite-dimensional representation ρ of G on M, $\chi_\rho(1) = \dim_{\Bbbk} M$ so $\chi_{\mathrm{reg}}(1) = |G|$. On the other hand, for every $g \neq 1$, g permutes the natural basis of $\Bbbk[G]$ given by G without fixed points, so, with respect to this basis, the matrix of g is a permutation matrix with zeros on the diagonal. Hence for every $g \in G, g \neq 1$, $\chi_{\mathrm{reg}}(g) = 0$. $\square$

5.17. **Definition.** The *prime subring* of $\Bbbk$ is the image of the map $\mathbb{Z} \longrightarrow \Bbbk$.

5.18. **Proposition.** *Let $\chi_1, \ldots, \chi_c$ be the distinct simple characters of G. Let $\rho : G \longrightarrow \operatorname{Aut}_{\Bbbk}(M)$ be a representation. Then there exist $n_1, \ldots, n_c$ in the prime subring of $\Bbbk$ such that $\chi_\rho = \sum_{i=1}^c n_i\chi_i$. Now suppose that* $\operatorname{char} \Bbbk = 0$*. Then the n_i are uniquely determined non-negative integers, and, moreover, if ρ' is a representation such that $\chi_{\rho'} = \chi_\rho$ then ρ and ρ' are isomorphic to each other.*

Proof. Since M is a finite-dimensional $\Bbbk$-vector-space, there exist non-negative integers $n_1, \ldots, n_c$ such that $M = \bigoplus_{i=1}^{c} M_i^{\oplus n_i}$ as $\Bbbk[G]$-modules. Note that if $\phi : \bigoplus_{i=1}^{c} M_i^{\oplus n_i} \longrightarrow \bigoplus_{i=1}^{c} M_i^{\oplus n_i'}$ is a $\Bbbk[G]$-isomorphism, then for each i, $\operatorname{Im}(\phi|_{M_i^{\oplus n_i}}) \subseteq M_i^{\oplus n_i'}$, and $\phi|_{M_i^{\oplus n_i}}$ is an isomorphism, from which, after comparing ranks over $\Bbbk$, it follows that $n_i = n_i'$. Therefore the integers n_i (in the decomposition of M) are unique. Denoting the images of the integers n_i in $\Bbbk$ again by n_i, we see that $\chi_\rho = \sum_{i=1}^c n_i\chi_i$. Now suppose that $\operatorname{char} \Bbbk = 0$. Since the map $\mathbb{Z} \longrightarrow \Bbbk$ is injective, the uniqueness is preserved in the expression $\chi_\rho = \sum_{i=1}^c n_i\chi_i$. Further, if $\chi_{\rho'} = \chi_\rho = \sum_{i=1}^c n_i\chi_i$, where $\rho : G \longrightarrow \operatorname{Aut}_{\Bbbk}(M)$ and $\rho' : G \longrightarrow \operatorname{Aut}_{\Bbbk}(M')$, then $M \simeq M' \simeq \bigoplus_{i=1}^{c} M_i^{\oplus n_i'}$. $\square$

5.19. **Remark.** We see tht the set of characters of G is a $\Bbbk$-vector-space, spanned by the simple characters χ_i. If the dimensions d_i (over $\Bbbk$) of the simple $\Bbbk[G]$-modules M_i are invertible in $\Bbbk$ (e.g., if $\operatorname{char} \Bbbk = 0$), then the χ_i form a basis. To see this, suppose that $\sum_i \alpha_i\chi_i = 0$, with $\alpha_i \in \Bbbk$. Then $0 = (\sum_i \alpha_i\chi_i)(e_j) = \alpha_j\chi_j(e_j) = \alpha_j d_j$, so $\alpha_j = 0$. $\square$

5.20. **Notation.** For $g \in G$, denote its conjugacy class $\{hgh^{-1} \mid h \in G\}$ by C_g. Let $\mathcal{C} \subseteq G$ be a set of representatives for the conjugacy classes of G, i.e., $G = \bigsqcup_{g \in \mathcal{C}} C_g$. For $g \in G$, write $s_g = \sum_{h \in C_g} h$. $\square$

5.21. **Proposition.** *Let $a \in \Bbbk[G]$. Then the following are equivalent:*
 (1) a is a central element of $\Bbbk[G]$;
 (2) $ag = ga$ for every $g \in G$ (thought of as a subset of $\Bbbk[G]$);
 (3) a is a $\Bbbk$-linear combination of $\{s_g \mid g \in \mathcal{C}\}$.

Proof. (1) implies (2): Immediate.

(2) implies (3): Write $a = \sum_{\tau \in G} a_\tau \tau$. Then $\sum_{\tau \in G} a_\tau \tau = a = gag^{-1} \sum_{\tau \in G} a_\tau g\tau g^{-1} = \sum_{\tau \in G} a_{g^{-1}\tau g}\tau$. Since G is a $\Bbbk$-basis of $\Bbbk[G]$, we see that for every $\tau \in G$, $a_\tau = a_\sigma$ for every $\sigma \in C_\tau$.

(3) implies (1): For every $h \in G$, $hs_gh^{-1} = s_g$, so s_g is a central element for every $g \in \mathcal{C}$. $\square$

5.22. **Corollary.** *$\{s_g \mid g \in \mathcal{C}\}$ is a $\Bbbk$-basis for the centre of $\Bbbk[G]$.*

Proof. This follows from Proposition 5.21, after noting that $\{s_g \mid g \in \mathcal{C}\}$ is linearly independent over $\Bbbk$. $\square$

5.23. **Remark.** A function $f : G \longrightarrow \Bbbk$ is said to be a *class function* if $f(ghg^{-1}) = f(h)$ for every $g, h \in G$, or equivalently, $f(ghg^{-1}) = f(h)$ for every $g, h \in G$. Characters are class functions, since for two matrices A and B, $\operatorname{Trace}(AB) = \operatorname{Trace}(BA)$.

5.24. **Theorem.** *Suppose that $\Bbbk$ is algebraically closed. Let*

$$\Bbbk[G] = \prod_{i=1}^{c} R_i$$

be a decomposition as the product of simple rings R_i. Then:

(1) *G has exactly c conjugacy classes.*
(2) *$\{s_g \mid g \in \mathcal{C}\}$ and $\{e_1, \ldots, e_c\}$ are bases for the centre of $\Bbbk[G]$.*
(3) *$\chi_{\text{reg}} = \sum_{i=1}^{c} d_i \chi_i$.*
(4) *$|G| = \sum_{i=1}^{c} d_i^2$.*

Proof. Each R_i is a simple finite-dimensional $\Bbbk$-algebra, so $R_i = \operatorname{End}_{D_i}(M_i)$ for a finite-dimensional division ring D_i over $\Bbbk$ and free D_i-module M_i. Since $\Bbbk$ is algebraically closed, $D_i = \Bbbk$. Hence the centre of R_i is $\Bbbk_i := \Bbbk e_i$; thus the centre of $\Bbbk[G]$ is $\prod_{i=1}^{c} \Bbbk_i$. This proves (1) and (2). Note that as R-modules, $R_i = M_i^{\oplus d_i}$, so $\chi_{\text{reg}} = \sum_{i=1}^{c} d_i \chi_i$, proving (3). Hence $\dim_{\Bbbk} R_i = d_i^2$, so $|G| = \dim_{\Bbbk} \Bbbk[G] = \sum_{i=1}^{c} d_i^2$ proving (4). $\square$

5.25. **Observation.** Suppose that $\Bbbk$ is algebraically closed. Let $g \in G$ and $1 \leq i \leq c$. For any $a \in \Bbbk[G]$, $e_i a \in R_i$. Thus

$$\chi_{\text{reg}}(e_i g) = \sum_{j=1}^{c} d_j \chi_j(e_i g) = d_i \chi_i(e_i g) = d_i \chi_i(g).$$

Let $g \in G$ be such that it appears in e_i with a non-zero coefficient. Then by Proposition 5.16 $\chi_{\text{reg}}(e_i g^{-1}) \neq 0$, so d_i is non-zero in $\Bbbk$. In particular, the χ_i are linearly independent over $\Bbbk$ (Remark 5.19).

5.26. **Proposition.** *Suppose that $\Bbbk$ is algebraically closed. Then for every $1 \leq i \leq c$,*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \left(\chi_{\text{reg}}(e_i g^{-1}) \right) g = \frac{d_i}{|G|} \sum_{g \in G} \left(\chi_i(g^{-1}) \right) g$$

Proof. The second equality follows from Observation 5.25. To prove the first, write $e_i = \sum_{h \in G} a_i h$. Then $\chi_{\text{reg}}(e_i g^{-1}) = \sum_{h \in G} a_h \chi_{\text{reg}}(hg^{-1}) = a_g |G|$. $\square$

5.27. **Notation.** Let $X_{\Bbbk}(G)$ denote the set of characters of G and $Z_{\Bbbk}(G)$ the centre of $\Bbbk[G]$. $\square$

5.28. **Proposition.** *Suppose that $\Bbbk$ is algebraically closed. Then the pairing*

$$X_{\Bbbk}(G) \times Z_{\Bbbk}(G) \longrightarrow \Bbbk, (\chi, a) \mapsto \chi(a)$$

is non-degenerate. In particular, $X_{\Bbbk}(G)$ and $Z_{\Bbbk}(G)$ are dual to each other under this pairing.

Proof. Let $\chi = \sum_i \alpha_i \chi_i \neq 0$. Pick i such that $\alpha_i \neq 0$; then (use Lemma 5.15 and Observation 5.25) $\chi(e_i) = \alpha_i \chi_i(e_i) = \alpha_i d_i \neq 0$. Now let $a \neq 0 \in Z_{\Bbbk}(G)$. Write $a = \sum_i \beta_i e_i$ (Theorem 5.24(2)). Pick i such that $\beta_i \neq 0$; then $\chi_i(a) = \chi_i(\beta_i(e_i)) = \beta_i d_i \neq 0$. $\square$

5.29. **Proposition.** *Suppose that $\Bbbk$ is algebraically closed. Then we have a bilinear map*

$$\langle\ ,\ \rangle : X_{\Bbbk}(G) \times X_{\Bbbk}(G) \longrightarrow \Bbbk, (\chi, \chi') \mapsto \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'(g).$$

The χ_i form an orthonormal basis for $X_{\Bbbk}(G)$ with respect to this pairing, i.e.,

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 1, & \textit{if } i = j; \\ 0, & \textit{otherwise.} \end{cases}$$

CHENNAI MATHEMATICAL INSTITUTE, SIRUSERI, TAMILNADU 603103. INDIA
E-mail address: mkummini@cmi.ac.in