4. Linear representations of a group as modules for the group ring

Fix a commutative ring k with identity. It is called the *base ring* or just the *base*.

4.1. **Associative algebras with identity.**

A k-module A is a *k-algebra* if we are given a k-linear map $\mu : A \otimes_k A \to A$, or, what amounts to the same, a k-bilinear map $A \times A \to A$. We call μ the *multiplication*. It is *associative* if $\mu(a \otimes \mu(b \otimes c)) = \mu(\mu(a \otimes b) \otimes c)$, in which case it is convenient to write just ab for $\mu(a, b)$. An *identity* for an associative algebra A is an element 1 of A such that $1a = a1 = a$ for all a in A. We can talk about units in an associative algebra with identity: a in A is a *unit* if there is an element b of A such that $ab = ba = 1$.[5] Units form a group under multiplication.

A *map of algebras* is a k-linear map respecting multiplication. A *map of associative algebras with identity* is a map of algebras respecting also the identity. The restriction to the group of units of such a map is a group homomorphism into the group of units.

The prototypical example of an associative k-algebra with identity is $\mathrm{End}_k V$, the set of all k-linear endomorphisms of a k-module V: multiplication is composition and identity the identity endomorphism of V. Rings with identity are precisely associative $\mathbb{Z}$-algebras with identity. Prototypical examples of rings with identity are therefore rings of endomorphisms of abelian groups.

Precomposing the multiplication of an algebra by the flip, we get its *opposite*: $\mu^{\mathrm{opp}}(a \otimes b) := \mu(b \otimes a)$. The k-module A with this new multiplication μ^{opp} is the *opposite algebra* A^{opp} of A. If A is associative with identity then so is A^{opp}. An *anti-homomorphism* from an algebra A to an algebra B is a homomorphism from A to B^{opp} (or, equivalently, from A^{opp} to B).

The space $M_n(k)$ of $n \times n$ matrices is an associative k-algebra with identity under matrix multiplication. The transpose map is an anti-endomorphism of $M_n(k)$.

4.1.1. Modules.

Let A be an associative k-algebra with identity. An *A-module* or *representation* of A is a homomorphism $\rho : A \to \mathrm{End}_k V$ of associative algebras with identity, where V is a k-module. We often just say that V is an A-module, the homomorphism ρ being tacitly understood.

Analogous to the case for the case of groups acting on sets discussed in §1, modules are either *left* or *right* depending upon the choice of direction for endomorphisms to act. We indicate the direction by writing A as a subscript: ${}_AV$ if V is a left module and V_A if it is a right module. A left A-module is naturally a right A^{opp}-module (and vice-versa): we need only define $va := av$. Thus, if there exists a natural choice of an isomorphism $a \mapsto a^\star$ from A to A^{opp}, we can convert left A-modules to right A-modules and vice-versa by the rule: $va := a^\star v$ and $av := va^\star$.

A *homomorphism* of A-modules is a k-linear map that commutes with multiplication by elements of A. In particular, the set $\mathrm{End}_A V$ of A-endomorphisms of an A-module V is the centralizer in $\mathrm{End}_k V$ of the image of A under the map

[5] If l and r are elements in an associative algebra with identity such that $lr = 1$, then l is a *left inverse* for r and r is a *right inverse* for l. An element a could have a left inverse but no right inverse and vice-versa. A *two-sided inverse* for a is an element b such that $ab = ba = 1$. Units are precisely elements with two-sided inverses. If a has both a left inverse l and a right inverse r, then $l = r$, so a is a unit: $l = l1 = l(ar) = (la)r = 1r = r$.

$A \to \mathrm{End}_k V$ defining the A-module structure on V. It is an associative subalgebra with identity of $\mathrm{End}_k V$.[6]

4.1.2. Remarks. A k-module V is tautologically a module for $\mathrm{End}_k V$. It is called the *defining representation* of $\mathrm{End}_k V$.

4.1.3. Left and right regular representations. Let A be an associative k-algebra with identity. Then A has naturally the structure of a left A-module and also that of a right A-module: these are called the *left regular* and the *right regular* representations respectively. Indeed, for a in A, the maps $\lambda_a : b \mapsto ab$ and $\rho_a : b \mapsto ba$ are k-linear endomorphisms of A; and, under the convention that $\mathrm{End}_k A$ acts on the left on A, the map $\lambda : a \mapsto \lambda_a$ (respectively $\rho : a \mapsto \rho_a$) is a homomorphism (respectively anti-homomorphism) into $\mathrm{End}_k A$ respecting identity. If $\mathrm{End}_k A$ acts on the right on A, then λ would be an anti-homomorphism and ρ a homomorphism. The images of λ and ρ are both in either case subalgebras of $\mathrm{End}_k A$.

Proposition 4.1. *The maps $\lambda : a \mapsto \lambda_a$ and $\rho : a \mapsto \rho_a$ are monomorphisms. The centralizer in $\mathrm{End}_k A$ of the subalgebra $\lambda(A)$ is $\rho(A)$ and vice-versa.*

Proof. We can recover a from λ_a (respectively ρ_a) as the image of 1 under it, which proves the first assertion. For the second, first observe that $\lambda_a\rho_b(x) = a(xb) = (ax)b = \rho_p\lambda_a(x)$, so $\lambda(A)$ and $\rho(A)$ centralize each other. Now suppose φ in $\mathrm{End}_k A$ commutes with all of $\lambda(A)$. Setting $b := \varphi(1)$, we have $\varphi(a) = \varphi(a1) = a\varphi(1) = ab = \rho_b(a)$, so $\varphi = \rho_b$. The proof of the other part is similar. □

Corollary 4.2. *The algebra $\mathrm{End}_A A$ of endomorphisms of an associatve algebra A with identity as a module over itself (whether right or left) is isomorphic to the opposite A^{opp} of A: $\boxed{\mathrm{End}_A A \simeq A^{opp}}$.*

4.2. **The group ring.** Let G be a group. Denote by kG the free k-module with basis G. We identify G with its image in kG. Extending k-bilinearly the multiplication map on G, we get a multiplication on kG. This multiplication is associative and has identity (namely the identity 1 of the group). Thus kG is an associative k-algebra with identity. It is the *group ring*.

A routine verification proves the following:

Proposition 4.3. *The natural injection $G \to kG$ has the following properties:*

1. *It identifies G as a subgroup of the group of units of kG.*
2. *Its image spans k-linearly the group ring.*
3. *Given an associative k-algebra A with identity and a homomorphism φ of groups from G into the group of units of A, there is a unique map of k-algebras $\tilde{\varphi} : kG \to A$ that extends φ.*

The algebra kG comes equipped with further structure:

- there is a natural map $kG \to k$ defined by $g \mapsto 1$ for all g in G.

---

[6]If V is a left A-module, it is convenient to let $\mathrm{End}_A V$ act on the right, so that V becomes an A-$\mathrm{End}_A V$ bimodule: for associative k-algebras C and D with identity, a *C-D bimodule*, denoted suggestively by ${}_C V_D$, is a k-module V that is simultaneously a left C-module and a right D-module and satisfies $(cv)d = c(vd)$.

Applying the above to the speical case $A = k$, every left k-module V is naturally a k-$\mathrm{End}_k V$ bimodule. Now if V is also an A-module, it is natural to write the action of A on the right, so that V becomes a k-A bimodule. This explains the notation is older treatises: the base ring acts on the left and the algebra or ring on the right.

- the map $g \mapsto g^{-1}$ defines an isomorphism of kG with its opposite kG^{opp}.

4.3. **Linear representations of groups.** Let G be a group and X be a G-set. It is interesting to consider situations in which X has some additional structure and the image of the given group homomorphism $G \to \operatorname{Bij} X$ lands in the subgroup of bijections preserving the structure. We are especially interested in a particular such situation: namely when X is a k-module V. We call V a *linear representation* or just a *representation* of G in such a case. Sometimes we use the term *G-module* for a linear representation. To summarise: a k-module V is a G-module if we are given a group homomorphism from G to the group $\mathrm{GL}_k V$ of k-linear bijections of V.

A linear map $f : V \to W$ of G-modules is a *G-map* if it is a map of G-sets, or, in other words, if it "commutes with the G-action": $f(gv) = g(fv)$.

4.4. **Group representations as modules for the group ring.** Let V be a representation of G and $\rho : G \to \mathrm{GL}_k V$ its defining group homomorphism. Since $\mathrm{GL}_k V$ is the group of units in the algebra $\operatorname{End}_k V$, there is a unique lift of ρ to a map $\tilde{\rho} : kG \to \operatorname{End}_k V$ of associative algebras with identity (Proposition 4.3(3)). Thus a G-module is naturally a kG-module. Under this identification, G-module maps are kG-module maps (Proposition 4.3(2)).

There is also a natural way to regard kG-modules as G-modules, which is a 'two-sided inverse' to the above procedure. Indeed, the algebra homomorphism $kG \to \operatorname{End}_k W$ defining the kG-module structure on a k-module W, on restriction to G, gives a group homomorphism into $\mathrm{GL}_k V$ (Proposition 4.3(1)).