Appendix: Complements on Algebraic Structures

This appendix provides a short recap / introduction to some of the basic notions of module theory used in this lecture. Tensor products of vector spaces and algebraic integers are also recapped.

Reference:

[Rot10] J. J. Rotman. *Advanced modern algebra. 2nd ed.* Providence, RI: American Mathematical Society (AMS), 2010.

A Modules

Notation: Throughout this section we let $R = (R, +, \cdot)$ denote a unital associative ring.

Definition A.1 (*Left R-module*)

A **left** R**-module** is an ordered triple $(M, +, \cdot)$, where M is a set endowed with an **internal composition law**

$$\begin{array}{rccc} +: & M \times M & \longrightarrow & M \\ & (m_1, m_2) & \mapsto & m_1 + m_2 \end{array}$$

and an **external composition law** (or **scalar multiplication**)

$$\begin{array}{rccc} \cdot: & R \times M & \longrightarrow & M \\ & (r, m) & \mapsto & r \cdot m \end{array}$$

satisfying the following axioms:

(M1) $(M, +)$ is an abelian group;

(M2) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for every $r_1, r_2 \in R$ and every $m \in M$;

(M3) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for every $r \in R$ and every $m_1, m_2 \in M$;

(M4) $(rs) \cdot m = r \cdot (s \cdot m)$ for every $r, s \in R$ and every $m \in M$.

(M5) $1_R \cdot m = m$ for every $m \in M$.

Remark A.2

(a) Note that in this definition both the addition in the ring R and in the module M are denoted with the same symbol. Similarly both the internal multiplication in the ring R and the external multiplication in the module M are denoted with the same symbol. This is standard practice and should not lead to confusion.

(b) **Right R-modules** can be defined analogously using a *right* external composition law $\cdot : M \times R \longrightarrow R, (m, r) \mapsto m \cdot r$.

(c) Unless otherwise stated, in this lecture we always work with left modules. Hence we simply write "R-module" to mean "left R-module", and as usual with algebraic structures, we simply denote R-modules by their underlying sets.

(d) We often write rm instead of $r \cdot m$.

Example A.3

(a) Modules over rings satisfy the same axioms as vector spaces over fields. Hence:
vector spaces over a field K are K-modules, and conversely.

(b) Abelian groups are $\mathbb{Z}$-modules, and conversely.
(Check it! What is the external composition law?)

(c) If the ring R is commutative, then any right module can be made into a left module by setting $r \cdot m := m \cdot r \ \forall\, r \in R, \forall\, m \in M$, and conversely.
(Check it! Where does the commutativity come into play?)

Definition A.4 (*R-submodule*)

An R-**submodule** of an R-module M is a subgroup $U \leqslant M$ such that $r \cdot u \in U \ \forall\, r \in R, \forall\, u \in U$.

Properties A.5 (*Direct sum of R-submodules*)

If U_1, U_2 are R-submodules of an R-module M, then so is $U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$.
Such a sum $U_1 + U_2$ is called a **direct sum** if $U_1 \cap U_2 = \{0\}$ and in this case we write $U_1 \oplus U_2$.

Definition A.6 (*Morphisms*)

Let M, N be R-modules. A **(homo)morphism** of R-modules (or an R-**linear map**, or an R-**homomorphism**) is a map $\varphi : M \longrightarrow N$ such that:

(i) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \ \forall\, m_1, m_2 \in M$; and

(ii) $\varphi(r \cdot m) = r \cdot \varphi(m) \ \forall\, r \in R, \forall\, m \in M$.

A bijective morphism of R-modules is called an R-**isomorphism** (or simply an **isomorphism**), and we write $M \cong N$ if there exists an R-isomorphism between M and N.

A morphism from an R-module to itself is called an **endomorphism** and a bijective endomorphism is called an **automorphism**.

Properties A.7

If $\varphi : M \longrightarrow N$ is a morphism of R-modules, then the kernel

$$\ker(\varphi) := \{m \in M \mid \varphi(m) = 0_N\}$$

of φ is an R-submodule of M and the image

$$\mathrm{Im}(\varphi) := \varphi(M) = \{\varphi(m) \mid m \in M\}$$

of φ is an R-submodule of N. If $M = N$ and φ is invertible, then the inverse is the usual set-theoretic *inverse map* φ^{-1} and is also an R-homomorphism.

Notation A.8

Given R-modules M and N, we set $\mathrm{Hom}_R(M, N) := \{\varphi : M \longrightarrow N \mid \varphi \text{ is an } R\text{-homomorphism}\}$. This is an abelian group for the pointwise addition of maps:

$$\begin{array}{rccl} + : & \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N) & \longrightarrow & \mathrm{Hom}_R(M, N) \\ & (\varphi, \psi) & \mapsto & \varphi + \psi : M \longrightarrow N, m \mapsto \varphi(m) + \psi(m)\,. \end{array}$$

In case $N = M$, we write $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ for the set of endomorphisms of M. This is a ring for the pointwise addition of maps and the usual composition of maps.

Lemma-Definition A.9 (*Quotients of modules*)

Let U be an R-submodule of an R-module M. The quotient group M/U can be endowed with the structure of an R-module in a natural way via the external composition law

$$\begin{aligned} R \times M/U &\longrightarrow M/U \\ \big(r, m + U\big) &\longmapsto r \cdot m + U\,. \end{aligned}$$

The canonical map $\pi : M \longrightarrow M/U, m \mapsto m + U$ is R-linear and we call it the **canonical** (or **natural**) **homomorphism** or the **quotient homomorphism**.

Proof: Similar proof as for groups/rings/vector spaces/... ■

Theorem A.10 (*The universal property of the quotient and the isomorphism theorems*)

(a) **Universal property of the quotient**: Let $\varphi : M \longrightarrow N$ be a homomorphism of R-modules. If U is an R-submodule of M such that $U \subseteq \ker(\varphi)$, then there exists a unique R-module homomorphism $\overline{\varphi} : M/U \longrightarrow N$ such that $\overline{\varphi} \circ \pi = \varphi$, or in other words such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & N \\ M/U \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] & \end{tikzcd}$$

Concretely, $\overline{\varphi}(m + U) = \varphi(m)\ \forall\ m + U \in M/U\,.$

(b) **1st isomorphism theorem**: With the notation of (a), if $U = \ker(\varphi)$, then

$$\overline{\varphi} : M/\ker(\varphi) \longrightarrow \operatorname{Im}(\varphi)$$

is an isomorphism of R-modules.

(c) **2nd isomorphism theorem**: If U_1, U_2 are R-submodules of M, then so are $U_1 \cap U_2$ and $U_1 + U_2$, and there is an isomorphism of R-modules

$$(U_1 + U_2)/U_2 \cong U_1/(U_1 \cap U_2)\,.$$

(d) **3rd isomorphism theorem**: If $U_1 \subseteq U_2$ are R-submodules of M, then there is an isomorphism of R-modules

$$(M/U_1)\,/\,(U_2/U_1) \cong M/U_2\,.$$

(e) **Correspondence theorem**: If U is an R-submodule of M, then there is a bijection

$$\begin{array}{ccc} \{R\text{-submodules } X \text{ of } M \mid U \subseteq X\} & \longleftrightarrow & \{R\text{-submodules of } M/U\} \\ X & \mapsto & X/U \\ \pi^{-1}(Z) & \leftarrow\!\shortmid & Z\,. \end{array}$$

Proof: Similar proof as for groups/rings/vector spaces/... ■

Definition A.11 (*Irreducible/reducible/completely reducible module*)

An R-module M is called:

(a) **simple** (or **irreducible**) if it has exactly two submodules, namely the zero submodule 0 and itself;

(b) **reducible** if it admits a non-zero proper submodule $0 \subsetneq U \subsetneq M$;

(c) **semisimple** (or **completely reducible**) if it admits a direct sum decomposition into simple submodules.

Notice that the zero R-module 0 is neither reducible, nor irreducible, but it is completely reducible.

B Algebras

In this lecture we aim at studying modules over *the group algebra*, which are specific rings.

Definition B.1 (*Algebra*)

Let R be a commutative ring.

(a) An R-**algebra** is an ordered quadruple $(A, +, \cdot, *)$ such that the following axioms hold:

(A1) $(A, +, \cdot)$ is a ring;

(A2) $(A, +, *)$ is a left R-module; and

(A3) $r * (a \cdot b) = (r * a) \cdot b = a \cdot (r * b)\ \forall\ a, b \in A, \forall\ r \in R$.

(b) A map $f : A \to B$ between two R-algebras is called an **algebra homomorphism** iff:

(i) f is a homomorphism of R-modules; and

(ii) f is a ring homomorphism.

Example 3

(a) A commutative ring R itself is an R-algebra.
[The internal composition law "$\cdot$" and the external composition law "$*$" coincide in this case.]

(b) For each $n \in \mathbb{Z}_{\geqslant 1}$ the set $M_n(R)$ of $n \times n$-matrices with coefficients in a commutative ring R is an R-algebra for its usual R-module and ring structures.
[Note: in particular R-algebras need not be commutative rings in general!]

(c) Let K be a field. Then for each $n \in \mathbb{Z}_{\geqslant 1}$ the polynom ring $K[X_1, \dots, X_n]$ is a K-algebra for its usual K-vector space and ring structure.

(d) If K is a field and V a finite-dimensional K-vector space, then $\mathrm{End}_K(V)$ is a K-algebra.

(e) $\mathbb{R}$ and $\mathbb{C}$ are $\mathbb{Q}$-algebras, $\mathbb{C}$ is an $\mathbb{R}$-algebra, ...

(f) Rings are $\mathbb{Z}$-algebras.

Definition B.2 (*Centre*)

The **centre** of an R-algebra $(A, +, \cdot, *)$ is $Z(A) := \{a \in A \mid a \cdot b = b \cdot a \ \ \forall\, b \in A\}$.