– Chapter 0: Recapitulation on algebraic structures –

A Lie algebra is primarily an algebra, but in general its multiplication is neither associative, nor commutative, nor does it possess an identity element. In this respect, we recall here elementary definitions and constructions of rings, fields, modules, vector spaces, algebras and their substructures, morphisms and factor structures.

Nothing in this note should be new. If you have never formally encountered a *module* before, replace the words *K-module*, by *K-vector space* throughout. Similarly, if you have never formally encountered an *algebra* before, see it as a set, endowed with both the structure of a *K-vector space* and the structure of a ring.

1. RINGS

DEFINITION 1.1 (Rings).
A **ring** is an ordered triple $(R, +, \cdot)$, where R is a set endowed with two internal composition laws $+ : R \times R \longrightarrow R$ and $\cdot : R \times R \longrightarrow R$ called respectively **addition** and **multiplication**, satisfying the following axioms:

(RI) $(R, +)$ is an abelian group.

(RII) The multiplication is **distributive** with respect to addition, i.e.

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

for all $a, b, c \in R$.

Moreover:

(i) The ring R is said to be **associative** if its multiplication is associative, i.e. $\forall\, a, b, c \in R$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(ii) The ring R is said to be **commutative** if its multiplication is commutative, i.e. $\forall\, a, b \in R$:

$$a \cdot b = a \cdot b$$

(iii) The ring R is said to be **unital**, or a **ring with 1**, if its multiplication has an identity element, denoted 1_R, i.e. $1_R \cdot a = a = a \cdot 1_R \ \forall\, a \in R$.

For ease of notation we denote rings simply by their underlying set, the usual convention also being to omit the $\cdot$ symbol if desired when multiplying two elements.

DEFINITION 1.2 (Ring homomorphisms).
Let R and S be two rings.

(a) A **ring homomorphism**, or **morphism of rings**, of R into S is a map $f : R \longrightarrow S$ such that, for all $a, b \in R$:
  (i) $f(a + b) = f(a) + f(b)$;
  (ii) $f(a \cdot b) = f(a) \cdot f(b)$.

(b) If, moreover, R and S are unital rings, then we call **homomorphism of rings** of R into S a ring homomorphism $f : R \longrightarrow S$ in the sense of (a) satisfying the supplementary assumption that $f(1_A) = 1_B$.

Definition 1.3 (Substructures).
Let $(R, +, \cdot)$ be a ring.

(a) A subset $S \subseteq R$ is called a **subring of** R if it is subgroup for the addition and is closed under multiplication.

(b) If R is a unital ring, then a **subring** S of R is a subring in the sense of (a) and $1_R \in S$.

(c) A subset $I \subseteq R$ is called an **ideal of** R (or a **two-sided ideal**) provided:
  (i) $(I, +) \leq (R, +)$;
  (ii) $a \cdot x \in R$ and $x \cdot a \in R$ for all $a \in R$, $x \in I$.
  We shall use the notation $I \triangleleft R$.

Remark 1.4. If $\varphi : R \longrightarrow S$ is a ring homomorphism, then $\ker(\varphi)$ is an ideal of R and $\mathrm{Im}(\varphi)$ is a subring of S.

Recall that given a group $(R, +)$ and a normal subgroup $I \trianglelefteq R$, the set $R/I := \{a + I \,|\, a \in R\}$ of cosets of R modulo I endowed with the induced composition law

$$+ : R/I \times R/I \longrightarrow R/I,\ (a + I, b + I) \mapsto (a + b) + I$$

$$\begin{array}{rccc} \cdot : & R/I \times R/I & \longrightarrow & R/I \\ & (a + I, b + I) & \mapsto & (a + b) + I \end{array}$$

(also denoted by the symbol +) is a group, called the **quotient group of** R **modulo** I (or also the **factor group** R **modulo** I).

Proposition 1.5 (Quotient rings).
Let $(R, +, \cdot)$ be a ring and $I \triangleleft R$ be an ideal. Then the quotient group $(R/I, +)$ (as above) endowed with the induced multiplication (also denoted by the symbol $\cdot$)

$$\begin{array}{rccc} \cdot : & R/I \times R/I & \longrightarrow & R/I \\ & (a + I, b + I) & \mapsto & (a \cdot b) + I \end{array}$$

*is a ring called the **quotient ring of** R **modulo** I (or also the **factor ring** R **modulo** I).*

Proposition 1.6 (Universal property of the quotient ring).
Let R be a ring and let $I \triangleleft R$ be an ideal. Let $\pi : R \longrightarrow R/I, a \mapsto a + I$ be the associated quotient map (this is a ring homomorphism). If $f : R \longrightarrow S$ is a ring homomorphism such that $f(I) = \{0_S\}$, then there exists a unique ring homomorphism $\overline{f} : R/I \longrightarrow S$ such that $\overline{f} \circ \pi = f$.

Theorem 1.7 (The isomorphism theorems).
Let R be a ring, $I, J \triangleleft R$ be ideals, and H be a subring of R. Then the following hold:

(a) *If $f : R \longrightarrow S$ is a ring homomorphism, then there is a ring isomorphism:*

$$R/ker f \cong \mathrm{Im}(f)$$

(b) *$H + I$ is a subring of R, I is an ideal of $H + I$, $H \cap I$ is an ideal of H and there is an isomorphism of rings:*

$$(H + I)/I \cong H/H \cap I$$

(c) *If $J \subseteq I$, then there is an isomorphism of rings:*

$$R/I \cong R/J \Big/ I/J$$

(d) *(Two-step quotient)*

$$R/(I + J) \cong R/I \Big/ (I + J)/I \cong R/J \Big/ (I + J)/J$$

Theorem 1.8 (Correspondence theorem).
Let R/I be the factor ring of a ring R modulo an ideal I. Then the quotient homomorphism $\pi : R \longrightarrow R/I$ induces a bijection:

$$\begin{array}{rccc} \Pi: & \{\, \text{Ideals } J \triangleleft R \mid J \supseteq I \,\} & \xrightarrow{\sim} & \{\, \text{Ideals of } R/I \,\} \\ & J & \mapsto & J/I \end{array}$$

with inverse map given by $\Pi^{-1}(X) = \pi^{-1}(X)$ for every ideal $X \triangleleft R/I$.

2. Fields

Definition 2.1 (Skew fields, fields).
A **skew field** is an associative unital ring $(K, +, \cdot)$ satisfying the following axioms:

(KI) $K \neq \{0_K\}$.
(KII) Every non-zero element of K is invertible, i.e. $K^\times = K \setminus \{0_K\}$.

Moreover, a skew-field K is simply called a **field** if it satisfies the following axiom:

(KIII) K is a commutative ring.

Notice that some authors use the terminology *field* to mean *skew-field*, and *commutative field* to mean *field*.

3. Modules and vector spaces

Fix K an associative ring with 1.

Definition 3.1 (Modules).
A **left K-module** (or **left module over** K) is an ordered triple $(M, +, *)$, where M is a set endowed with an internal composition law $+ : M \times M \longrightarrow M$ and an external composition law

$$* : K \times M \longrightarrow M$$

satisfying the following axioms:

(MI) $(M, +)$ is an abelian group.
(MII) The external law $*$ is distributive with respect to the internal composition law $+$.
(MIII) $(a + b) * x = a * x + b * x$ for all $a, b \in K$, $x \in M$.
(MIV) $a * (b * x) = (ab) * x$ for $a, b \in K$, $x \in M$.
(MV) $1_K * x = x$ for all $x \in M$.

The elements of the ring K are called the **scalars**.

A **right** K**-module** can be defined in a similar fashion, replacing the external composition law on the left with a external composition law on the right. If the ring K is commutative, then the notions of a left K-module and a right K-module coincide. In this case we talk about a K-module.

Definition 3.2 (Vector spaces).
A left K-module is called a K**-vector space** provided the ring K is a field.

Definition 3.3 (Submodules).
Let $(M, +, *)$ be a K-module. A subset $N \subseteq M$ is called an K**-submodule of** R provided:

(i) $(N, +) \leq (M, +)$;
(ii) $a \cdot m \in M$ for all $a \in K$, $m \in M$.

Definition 3.4 (K-homomorphisms).
Let M and N be two K-modules. A **homomorphism of** K**-modules**, or a K**-homomorphism**, or K**-linear map**, of M into N is a map $f : M \longrightarrow M'$ such that, for all $m, n \in M$ and all $a \in K$:

(i) $f(m + n) = f(m) + f(n)$;
(ii) $f(a * m) = a * f(m)$.

Proposition 3.5 (Quotient modules).
Let $(M, +, *)$ be a K-module and $N \supseteq M$ be a submodule. Then the quotient group $(M/N, +)$ endowed with the induced external law (also denoted by the symbol $*$)

$$\begin{array}{rccc} * : & K \times M/N & \longrightarrow & M/N \\ & (a, m + I) & \mapsto & (a * m) + N \end{array}$$

is a K-module called the ***quotient module of*** *M* ***modulo*** *N (or also the* ***factor module*** *of M modulo N).*

Proposition 3.6 (Universal property of the quotient module).
Let M be a K-module and let $N \subseteq M$ be a submodule. Let $\pi : M \longrightarrow M/N, m \mapsto m + N$ be the associated quotient map (this is a K-linear map). If $f : M \longrightarrow M'$ is a K-homomorphism such that $f(N) = \{0_{M'}\}$, then there exists a unique K-homomorphism $\overline{f} : M/N \longrightarrow L$ such that $\overline{f} \circ \pi = f$.

Theorem 3.7 (The isomorphism theorems).
Let M be a K-module, $L, N \subseteq M$ be K-submodules. Then the following hold:

(a) *If $f : M \longrightarrow M'$ is a K-homomorphism, then there is a K-isomorphism $M/\ker f \cong \mathrm{Im}(f)$.*
(b) *There is an isomorphism of K-modules:*

$$(L + N)/N \cong L/L \cap N$$

(c) *If $L \subseteq N$, then*

$$M/L \cong M/N \Big/ N/L$$

as K-modules.

Theorem 3.8 (Correspondence theorem).
Let M/N be the factor module of a K-module M modulo a K-submodule N. Then the quotient homomorphism $\pi : M \longrightarrow M/N$ induces a bijection:

$$\begin{array}{rccc} \Pi: & \{\, K\text{-submodules } L \subseteq M \,|\, L \supseteq N \,\} & \xrightarrow{\sim} & \{\, K\text{-submodules of } M/N \,\} \\ & L & \mapsto & L/N \end{array}$$

with inverse map given by $\Pi^{-1}(X) = \pi^{-1}(X)$ *for every ideal* $X \subseteq M/N$.

4. Algebras

Fix K a commutative, associative ring with 1.

Definition 4.1.
A K**-algebra**, or an **algebra over** K, is an ordered quadruple $(A, +, \cdot, *)$ satisfying the following conditions:

(AI) $(A, +, *)$ is a K-module.
(AII) $(A, +, \cdot)$ is a ring.
(AIII) $r * (a \cdot b) = (r * a) = a \cdot (r * b)$ for all $a, b \in A$, $r \in K$.

Equivalently, a K-algebra A is a K-module together with an internal composition law $\cdot : A \times A \longrightarrow A$, which is K-bilinear.
The K-algebra A is called **associative (resp. commutative)** if the ring $(A, +, \cdot)$ is associative (resp. commutative).
The K-algebra A is called **unital** (or **an algebra with 1**) if $(A, +, \cdot)$ is a ring with 1.

Definition 4.2 (Algebra homomorphisms).
Let A and B be two K-algebras. A K-homomorphism $f : A \longrightarrow B$ is called an **algebra homomorphism**, or a **homomorphism of** K**-algebras**, provided it is also a ring homomorphism, i.e. $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in A$.

Definition 4.3 (Bases of an algebra / structure constants).

(a) A *basis* of K-algebra A is a basis of A for its K-module structure.
(b) If $\{a_i\}_{i \in I}$ is a basis of K-algebra $(A, +, \cdot, *)$, then there exists a unique family $\{\gamma_{ij}^k\}_{(i,j,k) \in I \times I \times I}$ of elements of K such that for every $(i, j) \in I \times I$, the $|\{k \in I \,|\, \gamma_{i,j}^k \neq 0\}| < \infty$ and

$$a_i \cdot a_j = \sum_{k \in I} \gamma_{i,j}^k * a_k$$

The scalars $\gamma_{i,j}^k$ are called the **structure constants** of the algebra A with respect to the basis $\{a_i\}_{i \in I}$.

Definition 4.4 (Substructures).
Let A be a K-algebra.

(a) A submodule $B \subseteq A$ is called a **subalgebra of** A provided it is a subring of A.
(b) If A is a unital algebra, then a **subalgebra** B of A is a subalgebra in the sense of (a) and $1_A \in B$.
(c) A submodule $I \subseteq A$ is called an **ideal of** R provided I is an ideal of the ring A. As for rings, we shall use the notation $I \triangleleft A$.

Clearly, the quotient A/I of a K-algebra A by an ideal I is again a K-algebra.

Theorem 4.5 (The isomorphism theorems).
Let A be a K-algebra, $I, J \triangleleft R$ be ideals, and B be a subalgebra of A. Then the following hold:

(a) *If $f : A \longrightarrow A'$ is a K-algebra homomorphism, then there is a K-algebra isomorphism:*
$$A/ker f \cong \mathrm{Im}(f)$$

(b) *$H + I$ is a subalgebra of A, I is an ideal of $H + I$, $H \cap I$ is an ideal of H and there is an isomorphism of K-algebras:*
$$(H + I)/I \cong H/H \cap I$$

(c) *If $J \subseteq I$, then there is an isomorphism of K-algebras:*
$$R/I \cong R/J\Big/I/J$$

Theorem 4.6 (Correspondence theorem).
Let A/I be the factor algebra of a K-algebra A modulo an ideal I. Then the quotient homomorphism $\pi : A \longrightarrow A/I$ induces a bijection:
$$\begin{array}{rccc} \Pi : & \{ \text{Ideals } J \triangleleft A \mid J \supseteq I \} & \xrightarrow{\sim} & \{ \text{Ideals of } A/I \} \\ & J & \mapsto & J/I \end{array}$$
with inverse map given by $\Pi^{-1}(X) = \pi^{-1}(X)$ for every ideal $X \triangleleft A/I$.