§3 Rings and fields

<u>Definition</u> Let A be a set equipped with two composition laws

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array} \quad \text{and} \quad \begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & ab \end{array}$$

additive law — multiplicative law

If (1) $(A,+)$ is a commutative group (whose zero element is denoted by 0)

(2) $(A,\cdot)$ is a monoid (whose unit element is denoted by 1)

(3) distributivity: $\forall a,b,c \in A$, $(a+b)c = ac+bc$

$c(a+b) = ca+cb$

we say that A is a ring. If in addition the multiplicative law is commutative, we say that A is a commutative ring.

Let K be a commutative ring. If any non-zero element in K is invertible with respect to the multiplicative law, we say that K is a field.

<u>Example</u>. · $\mathbb{Z}$ is a commutative ring

· $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

· $\mathbb{Z}$ is not a field (2 is not invertible in $\mathbb{Z}$).

§4 Modules, vector spaces

In this section we fix a commutative ring A.

<u>Definition</u> We call A-module any set M equipped with two maps:

$$\begin{array}{ccc} M \times M & \longrightarrow & M \\ (x,y) & \longmapsto & x+y \end{array} \quad \text{and} \quad \begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,x) & \longmapsto & ax \end{array}$$

additive law — multiplication by a scalar

such that (1) $(M,+)$ is a commutative group

(2) distributivity: $\forall a,b \in A$, $x,y \in M$ $\quad (a+b)x = ax+bx$

$a(x+y) = ax+ay$

(3) $\forall a,b \in A$, $x \in M$, $(ab)x = a(bx)$

(4) $\forall x \in M$, $1 \cdot x = x$.

<u>Examples</u> ① $M = A^n \quad (n \in \mathbb{N},\ n \geq 1)$

$$= \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \;\middle|\; \forall i \in \{1, \dots, n\},\ x_i \in A \right\}$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

For $a \in A$ $\quad a \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} ax_1 \\ \vdots \\ ax_n \end{pmatrix}$

② $(A^n)^\vee := \{ (x_1, \dots, x_n) \mid \forall i \in \{1, \dots, n\},\ x_i \in A \}$

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$$

⚠ A^n and $(A^n)^\vee$ are NOT the same A-module

<u>Proposition</u> Let M be an A-module and $\underline{0}$ be the zero element of M. Then (1) for any $x \in M$ one has $0 \cdot x = \underline{0}$
the zero element of A

(2) for any $a \in A$ one has $a\underline{0} = \underline{0}$

<u>Proof</u> $0x = (0+0)x = 0x + 0x \overset{\text{cancel out}}{\Longrightarrow} 0x = \underline{0}$

$a\underline{0} = a(\underline{0} + \underline{0}) = a\underline{0} + a\underline{0} \Rightarrow a\underline{0} = \underline{0}$

※

<u>Definition</u> Let M be an A-module. We call <u>sub-A-module</u> of M any subgroup M' of $(M, +)$ such that

$$\forall a \in A,\ x \in M',\quad ax \in M'.$$

(Thus M' becomes an A-module)

<u>Proposition</u> Let M be an A-module and M' be a sub-A-module of M. Then $x \sim y \iff x - y \in M'$ define an equivalence relation on the set M.
$(:= x + (-y))$

<u>Proof</u>. For any $x \in M$, one has $x - x = 0 \in M'$, so $x \sim x$

- If $x, y \in M$ are such that $x \sim y$ (i.e $x - y \in M'$) then $y - x = -(x-y) \in M'$, so $y \sim x$
- If $x, y, z \in M$ are such that $x - y \in M'$, $y - z \in M'$, then $x - z = (x-y) + (y-z) \in M' \Rightarrow x \sim z$. ※

We denote by M/M' the quotient space. We claim that the structure of A-module on M induces a structure of A-module on M/M'.

- If $[x]$ and $[y]$ are two equivalence classes in M/M', let
$$[x] + [y] := [x+y]$$
- If $[x] \in M/M'$ and $a \in A$, let $a[x] := [ax]$

These maps are well defined:

If $x \sim x'$ $(x - x' \in M')$ and $y \sim y'$ $(y - y' \in M')$, then
$$(x+y) - (x'+y') = (x-x') + (y-y') \in M',$$
so $[x+y] = [x'+y']$.

Similarly $a(x-x') = ax - ax' \in M'$, so $[ax] = [ax']$.

<u>Definition</u> Let M be an A-module and M' be a sub-A-module of M. The A-module M/M' constructed above is called the quotient A-module of M by M'.

<u>Convention</u> If K is a field. A K-module is also called
sub-K-module
quotient K-module

a K-vector space
K-vector subspace
quotient K-vector space.

§ 5 Linear maps

We also fix a commutative ring A.

<u>Definition</u> Let M and N be two A-modules. We call A-linear map from M to N any map $f: M \to N$ such that

$$\forall\, a, b \in A,\ x, y \in M, \quad f(ax+by) = af(x) + bf(y).$$

(Namely, f is a morphism of additive groups which preserves the multiplication by a scalar)

An A-linear map from an A-module M to itself is called an A-linear endomorphism.

<u>Example</u> ① Let M be an A-module and M' be a sub-A-module of M. Then the inclusion map $i: M' \to M$ and the projection map $\pi: M \to M/M'$ are A-linear maps.

② If $M \xrightarrow{f} N \xrightarrow{g} P$ are A-linear maps, then $g \circ f: M \to P$ is an A-linear maps.

<u>Definition</u> Let M and N be two A-modules. $f: M \to N$ be an A linear map. We define $\mathrm{Ker}(f) := \{x \in M \mid f(x) = 0\} \subset M$

$$\mathrm{Im}(f) := \{f(x) \mid x \in M\} \subset N$$

called the kernel and the image of f respectively

<u>Proposition</u> With the notation of the definition

(1) $\mathrm{Ker}(f)$ is a sub-A-module of M. It reduces to $\{0\}$ if and only if f is injective

(2) $\mathrm{Im}(f)$ is a sub-A-module of N. It equals N if and only if f is surjective

<u>Proof</u> (1) If $x, y \in \mathrm{Ker}(f)$ then $f(x-y) = f(x) - f(y) = 0$

So $x - y \in \mathrm{Ker}(f) \rightsquigarrow \mathrm{Ker} f$ is a subgroup.

If $x \in \mathrm{Ker}(f)$ and $a \in A$ then $f(ax) = af(x) = 0 \Rightarrow ax \in \mathrm{Ker}(f)$

Assume that f is injective. Then for any $x \in \mathrm{Ker}(f)$ one has $x=0$ since $f(x)=0=f(0)$

Conversely, if $\mathrm{Ker}(f)=\{0\}$, then for all $x, y \in M$ such that $f(x)=f(y)$ one has $x-y=0$ since $f(x-y)=f(x)-f(y)=0$. So f is injective

(2) If $u=f(x)$ and $v=f(y)$ are in $\mathrm{Im}(f)$, then $u-v=f(x-y) \in \mathrm{Im}(f)$. So $\mathrm{Im}(f)$ is a subgroup.
Moreover for $a \in A$ one has $au = af(x) = f(ax) \in \mathrm{Im}(f)$.

<u>Definition</u> Let M and N be two A-modules, and $f: M \to N$ be an A-linear map. If f is a bijection, then we say that f is an A-linear isomorphism. In this case, the inverse map $f^{-1}: N \to M$ is also an A-linear isomorphism. (M is isomorphic to N) ※

<u>Theorem</u> Let M and N be two A-modules and $f: M \to N$ be an A-linear map. Then there exists a unique A-linear map $\tilde{f}: M/\mathrm{Ker}(f) \to N$ such that $f = \tilde{f} \circ \pi$ (where $\pi: M \to M/\mathrm{Ker}(f)$ is the projection map). Moreover $\tilde{f}$ defines an A-linear isomorphism from $M/\mathrm{Ker}(f)$ to $\mathrm{Im}(f)$.

<u>Proof</u> If $x \sim y$ (namly $x-y \in \mathrm{Ker}(f)$), then $f(x)-f(y)=f(x-y)$
$=0$
So $f(x)=f(y)$. Therefore, there exists a unique map $\tilde{f}: M/\mathrm{Ker}(f) \to N$ such that $\tilde{f} \circ \pi = f$, namely $\tilde{f}([x])=f(x)$ for any $x \in M$.

Moreover, for $a, b \in A$ and $x, y \in M$. $\tilde{f}(a[x]+b[y]) = \tilde{f}([ax+by])$
$= f(ax+by) = af(x)+bf(y) = a\tilde{f}([x]) + b\tilde{f}([y])$.
So $\tilde{f}$ is an A-linear map.

<u>Moreover</u>, by definition $\tilde{f}$ and f have the same image. So

$$\tilde{f} : M/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f) \text{ is surjective.}$$

If $\tilde{f}([x]) = 0$, then $f(x) = 0$ so $x \in \mathrm{Ker}(f) \Rightarrow [x] = 0$ (in $M/\mathrm{Ker}(f)$)

Therefore $\tilde{f}$ is also injective $\Rightarrow$ It is an A-linear isomorphism. ※

<u>Example</u> Let M be an A-module and $\{e_1, \dots, e_n\}$ be elements of M, then one obtains an A-linear map $A^n \longrightarrow M$ sending $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ to $a_1 e_1 + \dots + a_n e_n$

- If this map is injective, we call $\{e_1, \dots, e_n\}$ a free family
- If this map is surjective, we call $\{e_1, \dots, e_n\}$ a system of generators
- If this map is an A-linear isomorphism, we call $\{e_1, \dots, e_n\}$ a basis of M.

<u>Definition</u> If an A-module M admits a finite system of generators we say that it is of finite type.

<u>Theorem</u> Let K be a field and V be a K-vector space of finite type. Then V admits a basis. Moreover, all bases of V have the same cardinal ($\mathrm{rk}_K(V)$), which is equal to the minimal cardinal of systems of generators of V and the maximal cardinal of free families in V. (This cardinal is called the rank of V over K, denoted by $\mathrm{rk}_K(V)$).

<u>Corollary</u> Let V be a K-vector space of finite type and V' be a K-vector subspace. Then V' and V/V' are K-vector spaces of finite type. Moreover, if $\{x_1, \dots x_n\}$ is a basis of V' and $\{[y_1], \dots [y_m]\}$ is a basis of V/V', then $\{x_1, \dots, x_n, y_1, \dots, y_m\}$ is a basis of V. In particular, $\mathrm{rk}(V) = \mathrm{rk}_K(V') + \mathrm{rk}_K(V/V')$