Chapitre 2 – Modules

§1 Premières définitions

Définition 1. Soit A un anneau et V un groupe abélien. Une *structure de A-module* sur V est une application

$$A \times V \longrightarrow V\,,$$

notée $(a, v) \mapsto a \cdot v$, avec les propriétés suivantes :

- l'opération est *bilinéaire*, c'est-à-dire que l'on a

$$(a+b)\cdot v = a\cdot v + b\cdot v\,, \qquad a\cdot(v+w) = a\cdot v + a\cdot w\,,$$

  pour $a, b \in A$ et $v, w \in V$;
- l'opération est associative, dans le sens où

$$a\cdot(b\cdot v) = (ab)\cdot v$$

  pour $a, b \in A$ et $v \in V$, en écrivant bien sûr ab pour la multiplication dans A ;
- $1 \cdot v = v$ pour tout $v \in V$.

La première chose à remarquer, et c'est capital, c'est que dans la situation où A est un corps, noté disons $\mathbb{K}$, dire que V possède une structure de $\mathbb{K}$-module revient exactement à dire que V est un espace vectoriel sur $\mathbb{K}$. C'est donc quelque chose que vous connaissez bien ! Le but de ce chapitre, et plus généralement du cours d'algèbre de ce semestre, est de voir si l'on peut « faire de l'algèbre linéaire » avec d'autres anneaux, qui ne sont pas des corps. Nous verrons que certaines notions se généralisent bien, mais dans l'ensemble le cas des corps est très particulier...

Voyons donc d'autres exemples. Pour cela, il sera utile de reformuler un peu la définition ci-dessus, car elle n'est pas toujours la plus pratique, selon les situations. Rappelons que, au cours des exercices sur le chapitre précédent, nous avons vu que pour tout groupe abélien V, l'ensemble $\mathrm{End}(V)$ des endomorphismes de V est naturellement muni d'une structure d'anneau, la multiplication étant la composition $\circ$, et l'élément neutre de cette multiplication étant l'identité I.

Lemme 2. *Soit V un groupe abélien et A un anneau. Se donner une structure de A-module sur V revient exactement à se donner un homomorphisme d'anneaux $\rho\colon A \longrightarrow \mathrm{End}(V)$.*

Démonstration. Supposons que V est un A-module au sens précédent. Pour chaque $a \in A$, notons

$$\begin{aligned}\rho(a)\colon V &\longrightarrow V\\ v &\mapsto a\cdot v\,.\end{aligned}$$

Ainsi $\rho(a)$ est un élément de $\mathrm{End}(V)$, et $a \mapsto \rho(a)$ est un homomorphisme d'anneaux : ces deux affirmations découlent des propriétés ci-dessus des A-modules (vérifiez-le).

Réciproquement, supposons donné $\rho\colon A \longrightarrow \mathrm{End}(V)$. Pour éviter les lourdeurs, nous écrirons $a \mapsto \rho_a$ (et non pas $\rho(a)$). Il suffit alors de poser, pour $a \in A$ et $v \in V$:

$$a \cdot v := \rho_a(v)\,.$$

Vous vérifierez (c'est le même calcul que ci-dessus, mais à l'envers) que $(a, v) \mapsto a \cdot v$ est bien une structure de A-module.

Enfin, il est immédiat que ces deux constructions sont inverses l'une de l'autre. □

Exemple 3. Qu'est-ce qu'un $\mathbb{Z}$-module ? Il faut prendre un groupe abélien V, et trouver un homomorphisme $\mathbb{Z} \longrightarrow \mathrm{End}(V)$. Or, nous avons vu ça dans les exercices du chapitre précédent, pour tout anneau A il existe un *unique* homomorphisme $\mathbb{Z} \longrightarrow A$; ici pour $A = \mathrm{End}(V)$, il s'agit de $n \mapsto nI$. Donc V est automatiquement un $\mathbb{Z}$-module, de manière unique. En bref, *un $\mathbb{Z}$-module n'est rien d'autre qu'un groupe abélien*.

Encore quelques préliminaires avant un autre exemple important.

Définition 4. Soient V et W des A-modules. Une application $f\colon V \longrightarrow W$ est appelée *homomorphisme de A-modules* lorsque c'est un homomorphisme de groupes abéliens et que $f(a \cdot v) = a \cdot f(v)$ pour $a \in A$ et $v \in V$. On dit que f est *A-linéaire*. Lorsque $V = W$, on dit que f est un *endomorphisme* du A-module V. Enfin, on dit que f est un *isomorphisme de A-modules* lorsque c'est un homomorphisme et une bijection.

Comme prévu, dans le cas où A est un corps, vous retrouvez une notion familière.

Lemme 5. *Soit V un A-module, et soit $\mathrm{End}_A(V)$ l'ensemble de ses endomorphismes de A-module. Alors $\mathrm{End}_A(V)$ est un sous-anneau de $\mathrm{End}(V)$. Lorsque $A = \mathbb{K}$ est un corps commutatif, $\mathrm{End}_{\mathbb{K}}(V)$ est même une algèbre sur $\mathbb{K}$.*

Démonstration. C'est très simple : il faut prendre $f, g \in \mathrm{End}_A(V)$ et écrire que

$$f \circ g(a \cdot v) = f(g(a \cdot v)) = f(a \cdot g(v)) = a \cdot f(g(v)) = a \cdot f \circ g(v)\,,$$

ce qui montre bien que $f \circ g \in \mathrm{End}_A(V)$.

Supposons maintenant que $A = \mathbb{K}$ est un corps commutatif (on parle donc d'espaces vectoriels ici). Écrivons I pour l'identité de V, et pour $\lambda \in \mathbb{K}$ écrivons sans surprise λI pour l'application $v \mapsto \lambda \cdot v$. L'ensemble des λI avec $\lambda \in \mathbb{K}$ est un anneau, et même un sous-anneau de $\mathrm{End}_{\mathbb{K}}(V)$ (car $\mathbb{K}$ est commutatif !) que l'on peut identifier avec $\mathbb{K}$. Ceci donne bien à $\mathrm{End}_{\mathbb{K}}(V)$ une structure d'algèbre sur $\mathbb{K}$: en effet il faut vérifier que $\lambda I \circ f = f \circ \lambda I$ pour $f \in \mathrm{End}_{\mathbb{K}}(V)$, mais cette condition revient exactement à dire que f est $\mathbb{K}$-linéaire. □

Tournons-nous vers le cas des algèbres, et commençons par une remarque. Lorsque B est un sous-anneau de A, tout A-module peut être considéré comme un B-module, si l'on veut : par exemple un espace vectoriel sur $\mathbb{C}$ est aussi un espace vectoriel sur $\mathbb{R}$. Prenons alors un

corps commutatif $\mathbb{K}$ et une algèbre sur $\mathbb{K}$, notée A. Puisque A possède un sous-anneau que l'on identifie à $\mathbb{K}$, la remarque précédente montre que tout A-module est en particulier un espace vectoriel sur $\mathbb{K}$. On peut alors énoncer le résultat suivant, qui est la variante pour les algèbres du lemme 2.

Lemme 6. *Soit A une algèbre sur $\mathbb{K}$, et soit V un groupe abélien. Se donner une structure de A-module sur V revient exactement à se donner une structure de $\mathbb{K}$-espace vectoriel sur V ainsi qu'un homomorphisme d'algèbres $\rho\colon A \longrightarrow \mathrm{End}_{\mathbb{K}}(V)$.*

Démonstration. On vous le laisse à titre d'exercice. C'est une variante de la démonstration du lemme 2. Attention à une chose : la définition de $\mathrm{End}_{\mathbb{K}}(V)$ dépend bel et bien de la structure de $\mathbb{K}$-espace vectoriel choisie. □

Exemple 7. Qu'est-ce qu'un $\mathbb{K}[X]$-module ? D'après le lemme, il s'agit d'un $\mathbb{K}$-espace vectoriel V muni d'un homomorphisme $\rho\colon \mathbb{K}[X] \longrightarrow \mathrm{End}_{\mathbb{K}}(V)$. Mais une proposition du chapitre précédent nous dit qu'un tel homomorphisme d'algèbre est de la forme $P \mapsto P(f)$, où $f \in \mathrm{End}_{\mathbb{K}}(A)$, et qu'il suffit de nous donner f. En bref, *un $\mathbb{K}[X]$-module est une paire (V, f) où V est un espace vectoriel sur $\mathbb{K}$ et $f\colon V \longrightarrow V$ est un $\mathbb{K}$-endomorphisme.* Pour être tout-à-fait clair, pour $v \in V$ on a

$$X \cdot v = f(v)\,.$$

Pour $P \in \mathbb{K}[X]$ quelconque, on a alors

$$P \cdot v = P(f)(v)\,;$$

ces parenthèses sont bien pénibles, mais $P(f)$ est un endomorphisme de V, on peut donc l'appliquer à v pour obtenir $P(f)(v)$. Voir l'exemple suivant.

Exemple 8. Soyons très concrets, et définissons un $\mathbb{R}[X]$-module. On prend $V = \mathbb{R}^2$ (dans tout ce cours, les éléments de $\mathbb{K}^n$ sont vus comme des matrices-colonnes, au fait). Il nous faut un endomorphisme $f\colon V \longrightarrow V$. Comme on le sait bien, il doit être de la forme $f(v) = Fv$, où F est la matrice de f dans la base canonique ; c'est une matrice 2×2, et ici Fv désigne bien le produit matriciel. (Note : la lettre F est plutôt rare pour une matrice, mais dans ce cours on va essayer, dans la mesure du possible, d'appeler F la matrice de f, puis G la matrice de g etc.) Pour continuer à être concret, on peut prendre par exemple

$$F = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Si on prend un polynôme, disons $P = X^3 - 4$, alors la matrice de l'endomorphisme $P(f)$ est tout simplement $P(F) = F^3 - 4I$. De sorte que si l'on prend un vecteur v, on a

$$P \cdot v = (X^3 - 4) \cdot v = (F^3 - 4I)v \qquad (= P(f)(v))\,.$$

Ici

$$F^3 - 4I = \begin{pmatrix} -3 & 3 \\ 0 & -3 \end{pmatrix},$$

donc si on prend disons $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, alors

$$P \cdot v = \begin{pmatrix} 3 \\ -3 \end{pmatrix}.$$

Maintenant que nous pouvons penser aux $\mathbb{K}[X]$-modules comme à des paires (V, f), nous pouvons « traduire » la notion d'homomorphisme :

Lemme 9. *Soient (V, f) et (W, g) deux $\mathbb{K}[X]$-modules, et soit $\phi\colon V \longrightarrow W$. Alors ϕ est un homomorphisme de $\mathbb{K}[X]$-modules si et seulement si ϕ est $\mathbb{K}$-linéaire et vérifie $\phi \circ f = g \circ \phi$.*

La situation est comme sur le diagramme suivant :

$$\begin{array}{ccc} V & \xrightarrow{f} & V \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ W & \xrightarrow{g} & W \end{array}$$

Démonstration. Si ϕ est $\mathbb{K}[X]$-linéaire, alors elle est certainement $\mathbb{K}$-linéaire ; et de plus, on doit avoir pour $v \in V$ la relation

$$\phi(X \cdot v) = X \cdot \phi(v).$$

Mais ici on a $X \cdot v = f(v)$, et pour tout $w \in W$ on a $X \cdot w = g(w)$, donc finalement

$$\phi(f(v)) = g(\phi(v)),$$

comme on le souhaitait.

Pour la réciproque, on suppose que ϕ est $\mathbb{K}$-linéaire et vérifie $\phi \circ f = g \circ \phi$, et on doit montrer pour tout polynôme $P \in \mathbb{K}[X]$ que $\phi(P \cdot v) = P \cdot \phi(v)$ pour tout v. C'est certainement vrai pour $P = X$, puisque la condition $\phi(X \cdot v) = X \cdot \phi(v)$ n'est que la traduction de $\phi \circ f = g \circ \phi$. Or l'ensemble

$$R = \{P \in \mathbb{K}[X] \mid \phi(P \cdot v) = P \cdot \phi(v)\}$$

est, à l'évidence, un sous-anneau de $\mathbb{K}[X]$. Puisque $X \in R$, on en déduit que $R = \mathbb{K}[X]$ en entier. □

Exemple 10. Pour $W = V$ et $g = f$, la condition est que $\phi \circ f = f \circ \phi$, c'est-à-dire que ϕ et f commutent. Reprenons l'exemple 8. Si Φ est la matrice de $\phi\colon V \longrightarrow V$, alors la condition pour que ϕ soit un endomorphisme de (V, f) peut s'écrire $\Phi F = F\Phi$. Si

$$\Phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

alors en écrivant séparément ΦF et $F\Phi$ on voit que la condition équivaut à $c = 0$ et $a = d$. En d'autres termes, nous avons une description de l'anneau $\mathrm{End}_{\mathbb{R}[X]}(V)$ des endomorphismes de (V, f) comme $\mathbb{R}[X]$-module :

$$\mathrm{End}_{\mathbb{R}[X]}(V) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \text{ avec } a, b \in \mathbb{R} \right\}.$$

C'est une algèbre sur $\mathbb{R}$, et comme espace vectoriel réel, elle est de dimension 2.

Nous pouvons maintenant annoncer plus clairement nos intentions dans ce cours. Nous allons parler de modules tout le long du semestre. Pour chaque résultat ou concept, ou presque, concernant les A-modules :

- lorsque A est un corps, on retrouvera quelque chose de connu d'algèbre linéaire, et en général on pourra réduire l'énoncé à quelque chose de beaucoup plus simple ;
- lorsque $A = \mathbb{Z}$, les choses seront immédiatement plus subtiles : on aura besoin des « vrais » énoncés généralisés, car si on s'attendait à ce que l'algèbre linéaire fonctionne « de la même manière » sur $\mathbb{Z}$, on aurait bien tort, les contre-exemples étant abondants ;
- lorsque $A = \mathbb{K}[X]$, les questions naturelles sur les modules se traduisent en questions que vous avez déjà un peu étudiées en cours de « réduction des endomorphismes » ; comme vous le savez, certaines de ces questions sont sophistiquées.

Nous étudierons souvent les A-modules sans hypothèse sur A, mais ce sont les 3 situations ci-dessus que nous allons systématiquement examiner dans les exemples. Puis, arrivera un chapitre où l'on montrera que $\mathbb{Z}$ et $\mathbb{K}[X]$ ne sont pas si différents (ce sont des « anneaux euclidiens »), et que leurs modules ne sont pas si compliqués, après tout !

La dernière partie du cours va étudier les « G-modules », où G est un groupe. Ceux-ci sont très bien compris, et avec la théorie des « caractères » on peut même rendre les choses très concrètes.

§2 Sous-modules

Dans cette partie, A est un anneau quelconque, et $\mathbb{K}$ est un corps commutatif.

Définition 11. Soit V un A-module, et $U \subset V$. On dit que U est un *sous-A-module de V* (ou sous-module de V pour faire court) lorsque c'est un sous-groupe de V, et que pour $u \in U$ et $a \in A$ on a $a \cdot u \in U$. (En d'autres termes, U est « stable par combinaisons linéaires à coefficients dans A ».)

Dans ce cas U est lui-même un A-module.

Exemple 12. Pour $A = \mathbb{K}$, on retrouve la notion de sous-espace vectoriel. Pour $A = \mathbb{Z}$, on retrouve la notion de sous-groupe (abélien). Lorsque $A = \mathbb{K}[X]$, et que (V, f) est donc un $\mathbb{K}[X]$-module, dire que $U \subset V$ est un sous-$\mathbb{K}[X]$-module de V signifie exactement que $f(U) \subset U$, autrement dit que U est stable par f. En écrivant $f|_U$ pour la restriction de f à U, on a bien un $\mathbb{K}[X]$-module $(U, f|_U)$.

Définition 13. Soient U_1 et U_2 deux sous-modules de V. La *somme* $U_1 + U_2$ est par définition

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}.$$

C'est un sous-module de V. On dit que V est *la somme directe* de U_1 et U_2, et on écrit $V = U_1 \oplus U_2$, lorsque $V = U_1 + U_2$ et $U_1 \cap U_2 = \{0\}$.

Avant même de donner des exemples, nous pouvons rappeler le fait suivant, qui vous est familier dans le cas $A = \mathbb{K}$ et qui n'est pas plus compliqué en général :

Lemme 14. *Soient U_1 et U_2 deux sous-modules de V. Alors $V = U_1 \oplus U_2$ est équivalent au fait que tout $v \in V$ peut s'écrire $v = u_1 + u_2$ avec $u_i \in U_i$, et ceci de manière unique.*

Démonstration. Exercice. Comme dans le cas $A = \mathbb{K}$ que vous connaissez. □

Exemple 15. Pour $A = \mathbb{K}$, on retrouve la notion de somme directe que vous connaissez depuis longtemps. Regardons un peu $A = \mathbb{Z}$. Prenons $V = \mathbb{Z}$, qui est bien un groupe abélien. Tout sous-module (= sous-groupe, ici) de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un entier $n \geq 0$. Si $U_1 = n\mathbb{Z}$ et $U_2 = m\mathbb{Z}$, avec n et m tous les deux > 0, alors $U_1 \cap U_2$ n'est jamais réduit à $\{0\}$, puisqu'il contient toujours $nm \neq 0$ par exemple. Donc on ne peut pas écrire V comme une somme directe, à part si U_1 ou U_2 est nul. (Dans les exercices nous étudierons $U_1 + U_2$ et $U_1 \cap U_2$.)

Enfin, soit (V, f) un $\mathbb{K}[X]$-module, avec V de dimension finie sur $\mathbb{K}$. Supposons que $V = U_1 \oplus U_2$, où U_i est un sous-$\mathbb{K}[X]$-module. Prenons une base de U_1, disons $e_1, \ldots, e_d$, et une base de U_2, disons $\varepsilon_1, \ldots, \varepsilon_r$. Alors la réunion $e_1, \ldots, e_d, \varepsilon_1, \ldots, \varepsilon_r$ est une base de V. Dans cette base, la matrice de f est de la forme

$$\begin{pmatrix} F_1 & 0 \\ 0 & F_2 \end{pmatrix}$$

où F_1 est une matrice $d \times d$ et F_2 est une matrice $r \times r$; en fait F_i est la matrice de $f|_{U_i}$. Autrement dit *il existe une base dans laquelle la matrice de f est diagonale par blocks*. Réciproquement, s'il existe une telle base, il est clair que V peut s'exprimer comme une somme directe.

Définition 16. Un A-module V est dit *indécomposable* lorsqu'on ne peut pas trouver de sous-modules U_1 et U_2, tous les deux non-nuls, tels que $V = U_1 \oplus U_2$.

L'exemple précédent montre que $\mathbb{Z}$, comme $\mathbb{Z}$-module, est indécomposable. Voyons un autre exemple.

Exemple 17. Revenons à la situation de l'exemple 8, et montrons que V est indécomposable. Supposons donc que $V = U_1 \oplus U_2$. Comme espace vectoriel sur $\mathbb{K}$, nous savons que V est de dimension 2 ; si les deux U_i sont non-nuls, on doit donc avoir $\dim U_1 = \dim U_2 = 1$. Mais alors, tout vecteur non-nul $u_i \in U_i$ est un *vecteur propre* de f, puisque $f(u_i) \in U_i =$

$\mathcal{V}ect(u_i)$. On aurait donc une base u_1, u_2 de vecteurs propres de f, ou autrement dit, f serait diagonalisable. Or, rappelons que la matrice de f est

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

son polynôme caractèristique est $(X-1)^2$, la seule valeur propre est 1, et l'espace propre $\ker(f-I)$ est de dimension 1, donc f n'est pas diagonalisable. (Ou encore : avec une seule valeur propre, si f était diagonalisable, elle serait déjà diagonale, comme on le sait bien.) Cette contradiction montre que V est indécomposable.

Dans le cas $A = \mathbb{K}$, c'est-à-dire dans le cas des espaces vectoriels, quels sont les modules indécomposables ? Il y en a très peu, en conséquence de la proposition suivante :

Proposition 18. *Soit V un espace vectoriel [de dimension finie pour simplifier], et soit U un sous-espace de V. Alors il existe un sous-espace U' tel que $V = U \oplus U'$.*

Ici, et dans le reste de cette partie, nous ferons des hypothèses de dimension finie, qui ne sont pas nécessaires : le résultat est vrai en toute généralité, mais il faut l'axiome du choix et diverses choses que nous préférons éviter... On va essayer d'en rester à des résultats que vous avez vus en L1.

Démonstration. Soit $e_1, \dots, e_d$ une base de U – il en existe, d'après votre cours d'algèbre linéaire de L1. On utilise le théorème de la base incomplète, qui nous affirme que l'on peut trouver des vecteurs $e_{d+1}, \dots, e_n$ tels que $e_1, \dots, e_n$ est une base de V. Si l'on pose $U' = \mathcal{V}ect(e_{d+1}, \dots, e_n)$, alors il est clair que $V = U \oplus U'$. □

Dans cette situation, dès lors que V possède un sous-espace U qui est non-nul, et tel que $U \neq V$, alors $V = U \oplus U'$ montre que V n'est pas indécomposable. On sent qu'il ne va pas y avoir beaucoup de modules indécomposables !

Le vocabulaire suivant va être utile :

Définition 19. Un module V non-nul est dit *simple* lorsque, pour tout sous-module $U \subset V$, on a ou bien $U = V$ ou bien $U = \{0\}$.

On a donc toujours :

Lemme 20. *Si V est un A-module simple, alors V est indécomposable.*

Démonstration. En effet, si on a $V = U_1 \oplus U_2$, alors par simplicité de V, on doit avoir ou bien $U_1 = V$ (et donc $U_2 = \{0\}$) ou bien $U_1 = \{0\}$ (et $U_2 = V$) ; on voit que U_1 et U_2 ne peuvent pas être tous les deux non-nuls, et donc que V est bel et bien indécomposable. □

Pour $A = \mathbb{K}$, la situation est complètement sous-contrôle :

Proposition 21. *Soit V un espace vectoriel sur $\mathbb{K}$ non-nul [de dimension finie pour simplifier]. Alors les trois propriétés ci-dessous sont équivalentes :*

1. *V est simple,*
2. *V est indécomposable,*
3. *V est de dimension 1.*

Démonstration. D'après le dernier lemme, on a toujours $(1) \implies (2)$. Supposons (2), et soit $v \in V$, $v \neq 0$ et $U = \mathcal{V}ect(v)$. D'après la proposition, on peut trouver U' tel que $V = U \oplus U'$. Mais comme V est indécomposable, ceci n'est possible que si $U' = \{0\}$. On en déduit que $V = U = \mathcal{V}ect(v)$, et en particulier la dimension de V est (1).

Enfin, supposons (3). Un sous-espace U de V doit être de dimension inférieure à 1, donc soit $\dim U = 0$ et $U = \{0\}$, soit $\dim U = 1$ et $U = V$. On a bien montré (1). □

On comprend bien pourquoi, dans vos cours d'algèbre linéaire, on ne vous a pas embêtés avec les notions de « module indécomposable » et « module simple » ! Mais sur un anneau quelconque, les choses sont plus délicates.

Exemple 22. Pour $A = \mathbb{Z}$, nous avons vu ci-dessus que $V = \mathbb{Z}$ est indécomposable. Mais il n'est pas simple : pour tout $n > 0$, le sous-groupe $U = n\mathbb{Z}$ est non-nul, et $U \neq V$ (il y a donc une infinité de sous-modules qui contredisent la simplicité de V).

Voyons des $\mathbb{Z}$-modules simples. Si p est un entier, alors les sous-groupes de $V = \mathbb{Z}/p\mathbb{Z}$ sont en bijection avec les diviseurs de p ; plus précisément, si $p = dk$, alors $U = \{v \in V \mid dv = 0\}$ est l'unique sous-groupe de V d'ordre d. Par conséquent, si p est un nombre premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un module simple (on dit aussi un groupe simple, ici).

Il y a donc une infinité de modules simples (un pour chaque nombre premier), qui ne sont pas isomorphes les uns aux autres (alors que dans le cas des corps, les modules simples, ie les modules de dimension 1, sont bien sûr tous isomorphes les uns aux autres). On verra plus loin qu'il n'y a pas d'autres $\mathbb{Z}$-modules simples.

Exemple 23. Voyons maintenant le cas de $A = \mathbb{K}[X]$. Retournons encore une fois à l'exemple 8. Nous venons de voir que ce module est indécomposable. Par contre, il n'est pas simple : si e_1, e_2 est la base canonique de V comme $\mathbb{R}$-espace vectoriel, alors $U = \mathcal{V}ect(e_1)$ est stable par f, visiblement, donc U est un sous-$\mathbb{K}[X]$-module de V.

Pour produire un exemple de $\mathbb{K}[X]$-module simple, il suffit de prendre V de dimension 1, avec f donné par une matrice 1×1 (bref un scalaire λ). En effet, un sous-module U d'un tel V doit être en particulier un sous-espace vectoriel, mais puisque V est alors simple comme $\mathbb{K}$-module (par la proposition), on a certainement $U = V$ ou $U = \{0\}$. En faisant varier λ, on obtient une collection de modules simples qui ne sont pas isomorphes les uns aux autres.

Plus loin dans ce cours, nous donnerons une classification des $\mathbb{Z}$-modules et des $\mathbb{K}[X]$-modules (avec un seul théorème !), et nous pourrons alors décrire complètement les indécomposables et les simples.

Terminons cette partie avec la définition du produit de deux modules :

Définition 24. Soient V et W deux modules sur A. Alors leur produit cartésien $V \times W$ est vu comme un A-module avec la structure

$$a \cdot (v, w) = (a \cdot v, a \cdot w)$$

pour $a \in A$, $v \in V$, $w \in W$ (et avec la structure naturelle de groupe abélien sur $V \times W$). On l'appelle tout naturellement le produit de V et W.

La notation $V \times W$ va être abusée presque tout de suite (dans ce cours, on va essayer de faire attention, mais c'est vrai que c'est tentant). En effet, le sous-module

$$V \times \{0\} = \{(v, 0) \mid v \in V\}$$

peut être sans danger identifié à V, et de même on identifie $\{0\} \times W$ à W. Ayant fait ceci, on voit V et W comme des sous-modules de $V \times W$, et ils sont alors en somme directe : $V \times W = V \oplus W$. Voilà pourquoi on trouve souvent la notation $V \oplus W$ là où il serait plus juste d'écrire $V \times W$.

Ajoutons enfin qu'il existe des définitions de la somme directe $\bigoplus_{i \in I} U_i$ d'une famille quelconque de modules U_i indexés par l'ensemble I, ainsi que du produit $\prod_{i \in I} U_i$ de ces mêmes modules : nous n'en dirons rien dans ce cours, mais sachez que ces deux constructions sont bien distinctes. (Alors que pour deux modules, ou même pour un nombre fini de modules, on vient de voir que confondre produit et somme directe n'est pas dramatique.)

§3 Modules libres

A désigne un anneau, et $\mathbb{K}$ est un corps commutatif.

Généralités

Définition 25. Pour tout entier $n \geq 1$, on écrit A^n pour le produit de n copies de A, c'est-à-dire le produit cartésien formé des n-uplets $(a_1, \ldots, a_n)$ avec $a_i \in A$; c'est un A-module avec

$$a \cdot (a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)\,.$$

On dit qu'un module V est *libre de rang* n s'il est isomorphe à A^n.

Pour $n = 1$, le module A^1 n'est autre que A, vu comme module sur lui-même (!), en utilisant la multiplication. On l'appelle parfois le *module régulier* de A. Il sera parfois utile de garder la notation A^1 pour le module régulier, quand on veut le distinguer de l'anneau A. Noter que A^n est le produit de n copies du module A^1.

Voici des concepts qui vous sont familiers :

Définition 26. Soit V un A-module, et $v_1, \ldots, v_n$ une famille d'éléments de V.

1. On dit que $v_1, \ldots, v_n$ est une *famille génératrice* lorsque l'application

$$\begin{aligned} A^n &\longrightarrow V \\ (a_1, \ldots, a_n) &\mapsto a_1 v_1 + \cdots + a_n v_n \end{aligned}$$

   est surjective.

2. On dit que $v_1, \ldots, v_n$ est une *famille libre* lorsque l'application ci-dessus est injective.

3. On dit que $v_1, \ldots, v_n$ est une *base* de V lorsque c'est une famille à la fois libre et génératrice, ou en d'autres termes lorsque l'application ci-dessus est un isomorphisme.

Prenez le temps de bien vérifier que ceci correspond à la façon dont vous avez vu ces concepts dans le cadre de l'algèbre linéaire. Par exemple, pour le deuxième point, rappelez-vous bien que l'application que l'on regarde est injective $\iff$ son noyau est réduit à $\{0\}$, c'est-à-dire si et seulement si la seule façon d'avoir une combinaison linéaire nulle

$$a_1 v_1 + \cdots + a_n v_n = 0$$

est de prendre tous les a_i nuls. (L'élément neutre 0 dans le module A^n est $(0, 0, \ldots, 0)$, évidemment !)

Vérifions que nous comprenons bien ce vocabulaire :

Lemme 27. *Soit V un A-module. Alors V est libre de rang n si et seulement s'il possède une base formée de n éléments.*

Démonstration. Si V possède une base avec n éléments, par définition il est isomorphe à A^n, donc libre. Pour la réciproque, dans le module A^n on peut utiliser les éléments

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

avec le 1 en i-ième position. La famille $e_1, \ldots, e_n$ est une base de A^n, évidemment. Si $\phi\colon A^n \longrightarrow V$ est un isomorphisme, alors la famille $\phi(e_1), \ldots, \phi(e_n)$ est une base de V. □

Définition 28. Un A-module V est dit *de type fini* lorsqu'il possède une famille génératrice (finie).

Lorsque $A = \mathbb{K}$, on dit plutôt que V est de *dimension finie* plutôt que de type fini, comme vous le savez. Un résultat très fort d'algèbre linéaire est le suivant :

Proposition 29. *Tout espace vectoriel de dimension finie possède une base.* □

Là encore, la vérité est qu'on n'a pas besoin de supposer que l'espace vectoriel est de dimension finie, mais vous n'avez sans doute pas vu la version plus générale. La moralité est que *sur un corps, tous les modules sont libres*.

Comme d'habitude, c'est loin d'être le cas avec les autres anneaux. Avec $A = \mathbb{Z}$, il suffit de prendre $V = \mathbb{Z}/2\mathbb{Z}$, qui ne risque pas d'être libre, c'est-à-dire isomorphe à $\mathbb{Z}^n$ pour un certain n, puisqu'il n'est même pas infini ! Et dans la même veine, avec $\mathbb{K}[X]$ il suffit de prendre une paire (V, f) avec V de dimension finie sur $\mathbb{K}$: il n'a alors aucune chance d'être isomorphe à $\mathbb{K}[X]^n$, qui est de dimension infinie sur $\mathbb{K}$.

Idéaux

Puisque nous venons d'introduire le module régulier A^1, nous pouvons parler des *idéaux*, qui fournissent de bons exemples de modules :

Définition 30. Les sous-modules de A^1 sont appelés les *idéaux* de A (ou parfois les *idéaux à gauche*, pour être plus précis). En clair, un idéal de A est un sous-groupe $I \subset A$ ayant la propriété que, pour $a \in A$ et $x \in I$, on a toujours $ax \in I$.

Exemple 31. Fixons $x_0 \in A$. Alors on note

$$(x_0) = \{ax_0 \mid a \in A\},$$

l'ensemble des multiples de x_0 (à gauche). C'est un idéal de A, et on dit que c'est *l'idéal principal engendré par* x_0. C'est donc un module de type fini (l'élément x_0 est une famille génératrice à lui tout seul). On le note aussi parfois Ax_0 ou, dans le cas où A est commutatif, x_0A.

Exemple 32. Prenons $A = \mathbb{Z}$. Alors chaque sous-groupe (= sous-module = idéal) de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un $n \geq 1$; c'est donc un idéal principal. Vous savez peut-être que la même chose est vraie avec $A = \mathbb{K}[X]$: tout idéal de cet anneau est principal, et nous reviendrons sur ce phénomène dans le chapitre suivant.

Il y a des anneaux qui n'ont pas cette propriété. Par exemple, prenons $A = \mathbb{Z}[X]$, et

$$I = A \cdot 5 + A \cdot X\,;$$

c'est une somme de deux idéaux principaux, donc en clair

$$I = \{a \cdot 5 + b \cdot X \mid a, b \in A\}.$$

Alors c'est un exercice facile que de montrer que I n'est pas principal.

Si I et J sont deux idéaux de l'anneau A, alors on peut parler de l'idéal $I + J$ (comme dans l'exemple précédent d'ailleurs), puisqu'on connait les sommes de sous-modules. Mais on peut aussi parler de IJ :

Définition 33. Le *produit* IJ des idéaux I et J est par définition l'idéal *engendré par* les éléments de la forme xy avec $x \in I$ et $y \in J$, c'est-à-dire que c'est le plus petit idéal qui contient ces éléments. Plus concrètement, IJ est l'ensemble des éléments de la forme

$$\sum_{k=1}^{m} x_k y_k$$

où m est un entier, et avec $x_k \in I$ et $y_k \in J$ pour k entre 1 et m.

Exemple 34. Si $I = (x)$ et $J = (y)$ sont des idéaux principaux, avec A commutatif, alors par définition on a $IJ = (xy)$ (vérifiez-le).

Plus généralement, si I est un idéal et M est un A-module quelconque, on peut définir IM, et on vous laisse deviner.

§4 Quotients

Introduction

Nous allons donner la définition du quotient V/U lorsque V est un A-module, et $U \subset V$ un sous-module. Avec $V = \mathbb{Z}$ et $U = n\mathbb{Z}$, nous retrouverons bel et bien $\mathbb{Z}/n\mathbb{Z}$! Commençons par une approche informelle, car la version définitive est un peu technique.

Nous allons voir qu'il y a un homomorphisme *surjectif* $V \longrightarrow V/U$ dont le noyau *est précisément* U. Ainsi, les éléments de U ont « disparu » du nouveau module V/U.

Premier exemple informel. Par exemple, supposons que $A = \mathbb{K}[X] = V$, et

$$U = X^3A = \{ \text{ les multiples de } X^3 \ \}$$

$$= \{a_3X^3 + a_4X^4 + \cdots + a_nX^n \mid a_i \in \mathbb{K}, n \geq 3\}\,.$$

Alors U est bien un sous-module de V (vérifiez-le !). Admettons que le module V/U existe avec les propriétés ci-dessus, et écrivons $P \mapsto \overline{P}$ pour le morphisme $V \longrightarrow V/U$. Dans ce cas $\overline{X^k} = 0$ pour $k \geq 3$ puisque $X^k \in U$ dans ce cas. On en déduit que tout élément de V/U est de la forme

$$\overline{a_0 + a_1X + \cdots + a_nX^n} = a_0\overline{1} + a_1\overline{X} + a_2\overline{X^2}\,.$$

Il semblerait intuitif que V/U soit un espace vectoriel de dimension 3 sur $\mathbb{K}$, avec pour base $\overline{1}, \overline{X}, \overline{X^2}$. Nous verrons que c'est effectivement le cas, lorsque nous aurons donné une définition rigoureuse des quotients. On peut imaginer des situations, dans lesquelles on travaille avec des polynômes, et où l'on se rend compte que seuls les termes de degré ≤ 2 sont « importants » pour les calculs que l'on mène ; il peut alors être plus agréable de travailler dans V/U, qui est de dimension finie, plutôt que dans V.

Deuxième exemple informel. Cette fois-ci, prenons $\mathbb{K} = \mathbb{R}$ et $V = \mathbb{R}^2$. Pour U, prenons une droite vectorielle quelconque. Comment peut-on espérer construire un module V/U avec une application linéaire $V \longrightarrow V/U$ dont le noyau serait U ? Dans ce cas précis, c'est facile. On peut prendre un U' tel que $V = U \oplus U'$ (cf chapitre précédent). On considère alors la projection

$$p\colon V = U \oplus U' \longrightarrow U'$$

$$p(u + u') = u'\,,$$

ce qui a un sens car tout vecteur de V s'écrit de manière unique $u+u'$ avec $u \in U,\ u' \in U'$. Il est alors immédiat que le noyau de p est bien U. Donc U' peut être pris comme modèle pour V/U, avec l'homomorphisme $p\colon V \longrightarrow U'$. Par contre, U' n'est pas unique du tout, et c'est un peu curieux.

Or, il y a une remarque « géométrique » à faire. Faisons un dessin. [à insérer]. On a pris une droite U' arbitraire. Ce qui se voit bien, c'est que chaque droite (affine) parallèle à U coupe U' en un point et un seul ; en fait si $u' \in U'$, la droite

$$u' + U = \{u + u' \mid u \in U\}$$

est parallèle à U, et coupe U' en u'. *Il y a ainsi une bijection entre les éléments de U' et les droites parallèle à U.*

Pour donner une définition de V/U sans avoir à choisir une droite U', nous allons *considérer l'ensemble des droites parallèles à U, et mettre une structure d'espace vectoriel dessus.*

Passons à la version rigoureuse.

Définition des quotients

Dans cette partie, A désigne toujours un anneau, et $\mathbb{K}$ un corps commutatif.

Définition 35. Soit V un A-module et $U \subset V$ un sous-module. Pour $v \in V$, on note

$$v + U := \{v + u \mid u \in U\}.$$

De plus, on note

$$V/U := \{v + U \mid v \in V\}.$$

(Formellement V/U est un donc un ensemble d'ensembles, chacun de la forme $v + U$, de même que ci-dessus on avait vu que V/U, sur un exemple, était identifié avec un ensemble de droites.)

Enfin, lorsque V et U sont fixés une fois pour toutes, on peut employer la notation

$$\overline{v} = v + U.$$

Avec cette notation

$$V/U = \{\overline{v} \mid v \in V\}.$$

Lemme 36. *Il existe un structure de A-module sur V/U, et une seule, telle que l'application*

$$p\colon V \longrightarrow V/U$$

définie par $p(v) = \overline{v}$ est un homomorphisme de A-modules.

De plus, $\ker(p) = U$.

Démonstration. Si X et Y sont des parties de V, définissons

$$X + Y = \{x + y \mid x \in X, y \in Y\}.$$

Examinons ceci dans le cas où $X = v + U$ et $Y = w + U$. On constate rapidement que

$$X + Y = (v + U) + (w + U) = (v + w) + U.$$

Ceci nous donne une opération $+$ sur V/U, et il est immédiat que $\overline{v} + \overline{w} = \overline{v + w}$. De plus, puisque p est surjective, il est très simple de vérifier que $+$ donne bien une structure de groupe abélien sur V/U. Par exemple, admettons que l'on veuille vérifier la commutativité,

c'est-à-dire que $x+y=y+x$ pour $x,y\in V/U$. Choisissons $v\in V$ tel que $\overline{v}=x$, et de même prenons w tel que $\overline{w}=y$, alors

$$x+y=\overline{v}+\overline{w}=\overline{v+w}=\overline{w+v}=\overline{w}+\overline{v}=y+x\,.$$

Nous avons utilisé la commutativité de la loi $+$ sur V. Notons que l'élément neutre est $\overline{0}=U$.

On fait pareil avec les autres propriétés à vérifier (associativité...). Et sur le même modèle, on définit, pour $a\in A$ et X une partie de V, la partie aX par

$$aX=\{ax\mid x\in X\}\,.$$

Si $X=v+U$ alors $aX=av+U$. Ceci nous donne une opération $A\times V/U\longrightarrow V/U$ qui complète la structure de A-module (les vérifications étant là encore très simples). On a $\overline{av}=a\overline{v}$, par définition.

L'unicité provient du fait que p est surjective (on vous laisse vérifier ceci).

Nous devons maintenant examiner le noyau de p. Il s'agit des $v\in V$ tels que $p(v)=\overline{0}=\overline{v}$, ce qui par définition signifie $U=v+U$. Clairement, ceci arrive si et seulement si $v\in U$. □

Proposition 37. *Soit U,V comme ci-dessus et $p\colon V\longrightarrow V/U$ l'application quotient. Soit W un autre A-module et $f\colon V\longrightarrow W$ un homomorphisme. On suppose que $f(u)=0$ pour tous les $u\in U$.*

Alors il existe un unique homomorphisme $\overline{f}\colon V/U\longrightarrow W$ tel que $f=\overline{f}\circ p$. Ou ce qui revient au même : pour $v\in V$ on a $f(v)=\overline{f}(\overline{v})$.

Démonstration. Soit $x\in V/U$. On peut choisir un $v\in V$ tel que $x=p(v)=\overline{v}$. Ce v n'est pas unique, mais par contre, l'élément $f(v)$ ne dépend pas du choix : en effet, si $p(v')=p(v)=x$, alors $u=v-v'\in\ker(p)=U$, donc $f(u)=0=f(v)-f(v')$. On peut donc poser $\overline{f}(x)=f(v)$ pour un v quelconque tel que $x=p(v)$, et ceci est bien défini. On a $f(v)=\overline{f}(p(v))$ par définition.

Il faut vérifier que $\overline{f}$ est un homomorphisme, mais c'est très facile, par exemple si $x=\overline{v}$ et $y=\overline{w}$ alors $x+y=\overline{v+w}$ de sorte que

$$\overline{f}(x+y)=\overline{f}(\overline{v+w})=f(v+w)=f(v)+f(w)=\overline{f}(\overline{v})+\overline{f}(\overline{w})=\overline{f}(x)+\overline{f}(y)\,.$$

Et ainsi de suite. □

Corollaire 38. *Soit $f\colon V\longrightarrow W$ un homomorphisme surjectif entre A-modules, et soit $U=\ker f$. Alors l'application induite $\overline{f}\colon V/U\longrightarrow W$ est un isomorphisme.*

On résume parfois ce corollaire en écrivant

$$V/\ker f\cong\mathrm{Im}(f)\,.$$

Démonstration. Puisque f est surjective, tout $w\in W$ est de la forme $w=f(v)=\overline{f}(\overline{v})$, donc $\overline{f}$ est surjective. De plus, si $x\in\ker\overline{f}$, alors en prenant $v\in V$ tel que $x=\overline{v}$ on a $\overline{f}(x)=f(v)=0$, d'où $v\in U$ et $\overline{v}=\overline{0}=x$. On a bien $\ker\overline{f}=\{\overline{0}\}$, donc $\overline{f}$ est également injective. □

Exemple 39. Nous avons promis que pour $V = \mathbb{Z}$ et $U = n\mathbb{Z}$ on retrouvait $\mathbb{Z}/n\mathbb{Z}$ comme on le connaît. Montrons-le : soit M le groupe abélien que vous avez appelé $\mathbb{Z}/n\mathbb{Z}$ les années précédentes ; tout le monde n'a peut-être pas eu la même définition, mais vous nous accorderez qu'il y a un homomorphisme surjectif $f\colon \mathbb{Z} \longrightarrow M$ dont le noyau est $n\mathbb{Z}$. Par le corollaire, $M \cong \mathbb{Z}/n\mathbb{Z}$, où l'écriture $\mathbb{Z}/n\mathbb{Z}$ désigne bien la nouvelle notion introduite dans ce chapitre.

Avant de donner d'autres exemples :

Définition 40. Soit U un sous-module de V, et soit $E \subset V$ un sous-ensemble – on ne suppose pas que E est un sous-module, en général. On dit que U et E sont *supplémentaires* lorsque tout $v \in V$ peut s'écrire de manière unique $v = u + e$ avec $u \in U$ et $e \in E$.

Bien sûr, si $V = U \oplus U'$, alors $E = U'$ est un supplémentaire de U, mais il y a d'autres exemples. Par exemple, si $A = V = \mathbb{Z}$, $U = n\mathbb{Z}$, et $E = \{0, 1, 2, \ldots, n-1\}$.

Lemme 41. *Soit U un sous-module de V, et soit E un supplémentaire de U. Alors l'application quotient*

$$p\colon V \longrightarrow V/U$$

donne une bijection entre E et V/U. Si E est un sous-module, alors p est un isomorphisme de modules ; si A est une algèbre sur $\mathbb{K}$ et si E est un $\mathbb{K}$-espace vectoriel, alors p est un isomorphisme d'espaces vectoriels.

Démonstration. La définition même de « supplémentaire » rend évident le fait que tout $x \in V/U$ s'écrit $x = p(e)$ pour un $e \in E$ unique. Le reste provient du fait que p est un homomorphisme de modules, donc sa restriction à E (si E est aussi un module) est encore un homomorphisme. □

Exemple 42. On retrouve bien sûr le fait que

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

(et le fait que les n éléments à droite sont distincts). Voici un autre exemple : prenons $A = \mathbb{K}[X] = V$, et $U =$ les multiples de X^3 comme dans l'introduction. On pose alors $E = \mathcal{V}ect(1, X, X^2)$. C'est un sous-espace vectoriel de V, mais pas un sous-module (si on multiplie un élément de E par X, on ne tombe pas forcément dans E !). Le lemme s'applique, car U et E sont supplémentaires. Ceci montre que V/U est isomorphe comme espace vectoriel à E, donc il est bien de dimension 3 avec pour base $\overline{1}, \overline{X}, \overline{X^2}$.

Quotient d'un anneau par un idéal

Nous venons de voir les quotients de modules. Voyons les quotients dans le monde des anneaux (dans un autre chapitre, nous verrons les quotients de groupes non-commutatifs).

Lemme 43. *Soit I un idéal de l'anneau A. On suppose que A est commutatif. Alors le A-module A/I est également un anneau commutatif, et l'application naturelle $p\colon A \longrightarrow A/I$ est un homomorphisme d'anneaux.*

Enfin, si A est une $\mathbb{K}$-algèbre, où $\mathbb{K}$ est un corps commutatif, alors A/I aussi, et l'application p est un homomorphisme d'algèbres.

Démonstration. Soient $x, y \in A/I$. On choisit $a, b \in A$ tels que $p(a) = x$ et $p(b) = y$; montrons que l'élément $p(ab) = ab + I \in A/I$ ne dépend pas du choix de a ou b, mais seulement de x et y.

En effet, si $p(a') = p(a) = x$ et $p(b') = p(b) = y$, alors $i = a' - a \in \ker(p) = I$ et de même $j = b' - b \in I$. Par suite

$$a'b' + I = ab + (ib' + aj + ij) + I = ab + I\,,$$

la dernière égalité provenant du fait que $ib' + aj + ij \in I$, car I est un idéal, et A est commutatif (c'est crucial !), donc $ib' = b'i \in I$.

On peut donc définir $xy = ab + I$, et ceci a un sens. Ceci donne une multiplication sur A/I, et $p(a)p(b) = p(ab)$ par définition. On en déduit facilement que A/I est un anneau commutatif.

La démonstration du « enfin » vous est laissée en exercice. □

Exemple 44. On retrouve le fait que $\mathbb{Z}/n\mathbb{Z}$ est un anneau, ainsi que la formule $\overline{ab} = \overline{a}\overline{b}$.

Lemme 45. *Soit $f\colon A \longrightarrow B$ un homomorphisme d'anneaux, et I un idéal de A tel que $f(I) = \{0\}$. Alors l'application induite $\overline{f}\colon A/I \longrightarrow B$ est un homomorphisme d'anneaux.*

De plus, si f est surjective et $I = \ker f$, alors l'isomorphisme $A/I \cong B$ induit par f est un isomorphisme d'anneaux.

Démonstration. Exercice. □

Dans la suite, nous allons nous concentrer sur un type d'exemple très important : on prend un corps commutatif $\mathbb{K}$, l'anneau $A = \mathbb{K}[X]$, et l'idéal $I = (D)$ principal engendré par le polynôme non-nul $D = a_0 + a_1X + \cdots + a_dX^d$. En tant que A-module, le cas de A/I est crucial, comme nous le verrons dans le chapitre suivant (en gros : tout $\mathbb{K}[X]$-module finiment engendré est un produit de modules de la forme $\mathbb{K}[X]/(D)$). En tant qu'anneau, le cas de A/I sera étudié à la loupe au second semestre.

Posons donc

$$E = \{P \in \mathbb{K}[X] \mid \deg(P) < d\}\,.$$

Comme vous le savez, dans $\mathbb{K}[X]$ on peut faire des divisions euclidiennes, c'est-à-dire que pour tout $P \in \mathbb{K}[X]$, on peut écrire

$$P = DQ + R$$

avec $\deg(R) < d$, et ceci de manière unique. Ceci revient à dire que (D) et E sont supplémentaires dans $\mathbb{K}[X]$ (pensez-y !). D'après un lemme ci-dessus, on en déduit que A/I est isomorphe, comme $\mathbb{K}$-espace vectoriel, à E. Plus précisément, en écrivant comme d'habitude $P \mapsto \overline{P}$ pour l'application $A \longrightarrow A/I$, les éléments $\overline{1}, \overline{X}, \ldots, \overline{X^{d-1}}$ forment une base de A/I.

Nous allons poser $x = \overline{X}$. On a $\overline{X^k} = x^k$ puisque l'application $A \longrightarrow A/I$ est un homomorphisme d'anneaux. Finalement, tout élément de A/I peut s'écrire de manière unique

$$\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_{d-1} x^{d-1}\,.$$

Et enfin, pour faire des calculs dans A/I, il suffit de se rappeler que $D(x) = 0$. En effet $D(x) = \overline{D(X)}$, et bien sûr $D \in (D)$ donc $\overline{D} = 0$. Nous avons tout ce qu'il nous faut pour travailler dans cet anneau quotient.

Exemple 46. Prenons $\mathbb{K} = \mathbb{R}$ et $D = X^2 + 1$. Appelons $K = \mathbb{R}[X]/(X^2+1)$. Comme espace vectoriel sur $\mathbb{R}$, cet anneau est de dimension 2, avec comme base $1, x$. De plus, on a la relation $x^2 + 1 = 0$. En écrivant ça $x^2 = -1$, on peut s'amuser à multiplier $z = a + bx$ par $w = a' + b'x$:

$$zw = aa' - bb' + (ab' + a'b)x\,.$$

Évidemment on se dit qu'on a probablement $K \cong \mathbb{C}$, et il est très facile de le montrer. Soit $\phi\colon \mathbb{R}[X] \longrightarrow \mathbb{C}$ l'homomorphisme $P \mapsto P(i)$. Alors ϕ est nul sur l'idéal $I = (X^2+1)$, puisque

$$\phi((X^2+1)\cdot P) = (i^2+1)\phi(P) = 0\,.$$

On a donc un homomorphisme de $\mathbb{R}$-algèbres induit $\overline{\phi}\colon \mathbb{R}[X]/(X^2+1) \longrightarrow \mathbb{C}$, qui est évidemment surjectif, et puisqu'il est $\mathbb{R}$-linéaire entre deux espaces de même dimension, c'est un isomorphisme (qui envoie x sur i) On a bien $K \cong \mathbb{C}$.

Au passage, on a même un peu plus. Soit $\phi_-\colon \mathbb{R}[X] \longrightarrow \mathbb{C}$ défini par $P \mapsto P(-i)$. Comme ci-dessus, on démontre que $\overline{\phi}_-$ est un isomorphisme entre K et $\mathbb{C}$. On voit alors que $\overline{\phi}_- \circ \overline{\phi}^{-1}\colon \mathbb{C} \longrightarrow \mathbb{C}$ est un automorphisme (de $\mathbb{R}$-algèbres) qui envoie i sur $-i$. Il s'agit bien sûr de la conjugaison complexe.

Exemple 47. Essayons avec $\mathbb{K} = \mathbb{C}$ et $D = X^2 + 1$. On a maintenant $X^2 + 1 = (X + i)(X - i)$, et

$$\frac{1}{2i}(X+i) - \frac{1}{2i}(X-i) = 1\,.$$

Les idéaux $I = (X + i)$ et $J = (X - i)$ vérifient donc $I + J = \mathbb{K}[X]$. D'après le lemme chinois (cf les exercices), on a

$$\mathbb{C}[X]/(X^2+1) \cong \mathbb{C}[X]/(X+i) \times \mathbb{C}[X]/(X-i)\,.$$

Par ailleurs, l'anneau $\mathbb{C}[X]/(P)$, avec P quelconque de degré 1, est une algèbre sur $\mathbb{C}$ de dimension 1 : c'est donc simplement $\mathbb{C}$! Finalement $\mathbb{C}[X]/(X^2+1) \cong \mathbb{C} \times \mathbb{C}$. Ce n'est pas un corps.

Exemple 48. Et maintenant, prenons $\mathbb{K} = \mathbb{Q}$ et $D = X^2 - 2$. L'anneau $K = \mathbb{Q}[X]/(X^2-2)$ est une algèbre de dimension 2 sur $\mathbb{Q}$, avec pour base $1, x$, et $x^2 - 2 = 0$, donc $x^2 = 2$. Les calculs dans K sont du type :

$$(a + bx)(a' + b'x) = aa' + 2bb' + (ab' + a'b)x\,.$$

Montrons que $K \cong \mathbb{Q}[\sqrt{2}]$ (cf les exercices de la feuille 1 pour la notation). On note $\phi_\pm : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt{2}]$ l'homomorphisme $P \mapsto P(\pm\sqrt{2})$. Alors $\phi_\pm$ vaut 0 sur l'idéal engendré par $X^2 - 2$, et on a donc un homomorphisme induit $\overline{\phi}_\pm : \mathbb{Q}[X]/(X^2-2) \longrightarrow \mathbb{Q}[\sqrt{2}]$; ce dernier est surjectif, et en comparant les dimensions, on constate que $\overline{\phi}_\pm$ est un isomorphisme. Il envoie x sur $\pm\sqrt{2}$.

On note que $\overline{\phi}_- \circ \overline{\phi}_+^{-1}$ est un automorphisme de $\mathbb{Q}[\sqrt{2}]$ qui envoie $\sqrt{2}$ sur $-\sqrt{2}$. Il n'est pas du tout trivial qu'un tel automorphisme existe !