RAPPELS D'ALGÈBRE GÉNÉRALE

par

Boyer Pascal

Table des matières

1. Groupes

1.1. Définitions. —

Définition 1.1. — On appelle *groupe* un couple $(G, *)$ formé d'un ensemble G et d'une loi de composition

$$(x, y) \in G^2 \mapsto x * y \in G$$

telle que les trois conditions suivantes soient vérifiées :

— *associativité* : pour tous $x, y, z \in G$, on a $x * (y * z) = (x * y) * z$;
— *élément neutre* : il existe $e \in G$ tel que pour tout $x \in G$, on a $e * x = x * e = x$; [1]
— *symétrique* : pour tout $x \in G$ il existe $y \in G$ tel que $x * y = y * x$.

Remarque : si de plus quels que soient $x, y \in G$, on a $x * y = y * x$ on dit que G est un groupe *commutatif* ou *abélien*.
Remarque : un groupe peut être fini ou infini, s'il est fini son cardinal et appelé *son ordre*.
Remarque : habituellement si la loi est commutative on la note avec un $+$ en lieu et place de $*$; sinon on préfère utiliser la notation multiplicative xy plus courte à écrire que $x * y$ et son symétrique est communément appelé son *inverse* que l'on note sous la forme x^{-1}. En ce qui concerne l'élément neutre on le note 0 dans le cas commutatif et 1 sinon.
Exercice : montrer qu'un groupe G tel que pour tout $x \in G$, on a $x^2 = e$, est nécessairement commutatif.
Exemples :

— l'ensemble $\mathbb{Z}$ des entiers relatifs muni de l'addition est un groupe abélien d'élément neutre 0. En remplaçant $\mathbb{Z}$ par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on obtient le groupe additif des nombres rationnels, réels ou complexes.
— L'ensemble $\mathbb{Q}^\times$ des nombres rationnels non nuls muni de la multiplication est un groupe abélien d'élément neutre 1 ; c'est le groupe multiplicatif des nombres rationnels. On définit de même $\mathbb{R}^\times$ et $\mathbb{C}^\times$.
— Si X est un ensemble, on note $\mathfrak{S}(X)$ l'ensemble des bijections de X muni de la loi de composition ; on définit ainsi un groupe non commutatif d'élément neutre l'identité que l'on appelle le groupe symétrique de X.
— Si dans l'exemple précédent, X est un $\mathbb{R}$-espace vectoriel de dimension n, et que l'on considère les bijections *linéaires* de X, on obtient le groupe linéaire $GL(X)$ isomorphe à $GL_n(\mathbb{R})$ une fois une base de X choisie.
— Si $G_1, \cdots, G_n$ sont des groupes, le produit cartésien $G = G_1 \times \cdots \times G_n$ muni de la loi produit

$$(x_1, \cdots, x_n) * (y_1, \cdots, y_n) = (x_1 y_1, \cdots, x_n y_n)$$

est un groupe appelé *le produit direct* de $G_1, \cdots, G_n$. Son élément neutre est $(1, \cdots, 1)$ et l'inverse de $(x_1, \cdots, x_n)$ est $(x_1^{-1}, \cdots, x_n^{-1})$.

1. un élément neutre est nécessairement unique comme le montre les relations $e_1 * e_2 = e_1 = e_2$.

Définition 1.2. — Pour G un groupe et X un ensemble quelconque, on note G^X l'ensemble des applications de X dans G ; la loi de groupe de G muni G^X d'une structure de groupe. Plus généralement on note $G^{(X)}$ le sous-ensemble de G^X des applications à support fini, i.e. celles telle que l'ensemble des x avec $f(x) \neq e$ est fini.

Remarque : par exemple $\mathbb{Z}^{\mathbb{N}}$ (resp. $\mathbb{Z}^{(\mathbb{N})}$) désigne l'ensemble des suites $(u_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{Z}$ (resp. telles que l'ensemble des n tels que $u_n \neq 0$ est fini).

Définition 1.3. — On dit qu'un sous-ensemble H d'un groupe $(G, *)$ est *sous-groupe* si les conditions suivantes sont réalisées :
- l'élément neutre e appartient à H ;
- pour tous $x, y \in H$, l'élément xy est dans H ;
- pour tout $x \in H$, l'inverse x^{-1} est dans H.

Remarque : on peut remplacer les deux dernières conditions par une seule : pour tous $x, y \in H$ alors $xy^{-1} \in H$. Les conditions de la définition précédente sont faites pour que H muni de la loi $*$ soit un groupe. Habituellement pour montrer qu'un ensemble muni d'une loi interne est un groupe, on essaie de montrer qu'il s'agit d'un sous-groupe d'un groupe déjà connu.
Exemples :
- les sous-ensembles G et $\{e\}$ de G sont clairement des sous-groupes que l'on qualifie habituellement de *triviaux* ;
- le sous-ensemble $\mathbb{R}_+^\times$ des réels strictement positifs ainsi que $\{\pm 1\}$ sont des sous-groupes de $\mathbb{R}^\times$;
- l'ensemble des nombres complexes de module 1 est un sous-groupe de $\mathbb{C}^\times$.

Remarque : l'intersection quelconque d'une famille de sous-groupes de G est aussi un sous-groupe de G ce qui permet de définir *le plus petit* sous-groupe contenant une partie X quelconque de G ; on le note $< X >$ et on l'appelle le sous-groupe engendré par X.
Exercice : montrer que pour H, K des sous-groupes de G, $HK = \{hk : \ (h, k) \in H \times K\}$ est égal à KH si et seulement si HK est un sous-groupe de G.

Définition 1.4. — Pour $g \in G$ si le sous-groupe $< g >= \{g^k : \ k \in \mathbb{Z}\}$ engendré par g est de cardinal fini, ce cardinal est appelé *l'ordre* de g ; sinon on dit que g est d'ordre infini.

Définition 1.5. — Pour G un groupe et H un sous-groupe de G, on associe la relation binaire $\mathcal{R}_H$ sur G définie par

$$x\mathcal{R}_H y \Leftrightarrow x^{-1}y \in H.$$

Cette relation est une relation d'équivalence ; l'ensemble des classes d'équivalence est noté G/H et s'appelle l'ensemble des classes à gauche modulo H.

Remarque : la classe d'équivalence d'un élément $x \in G$ est le sous-ensemble $xH = \{xh : \ h \in H\}$.
Remarque : on peut aussi définir la relation d'équivalence par $xy^{-1} \in H$ auquel cas les classes sont dites à droite et on note $H\backslash G$ l'ensemble des classes d'équivalence. La classe de x est alors $Hx = \{hx : \ h \in H\}$. On notera que la classe à gauche xH est égale à la classe à droite Hx si et seulement si $xHx^{-1} = H$; en particulier c'est toujours le cas si G est abélien.

Théorème 1.6. — ***(de Lagrange)***
Si G est fini alors on a $|G| = |H| \times |G/H|$ et en particulier l'ordre de H divise celui de G.

Preuve : Il suffit de dénombrer les éléments de G en utilisant la partition définie par les classes à gauche de G modulo H. Comme chacune de ces classes ont le même cardinal égal à l'ordre de H, la relation s'en déduit.
Remarque : si G est de cardinal un nombre premier alors ses seuls sous-groupes sont les sous-groupes triviaux $\{e\}$ et G.
Remarque : l'ordre d'un élément est toujours un diviseur du cardinal du groupe.
Exercice : soit G un groupe fini de cardinal n ; montrer que pour tout $g \in G$, on a $g^n = 1$.

On voudrait que la loi de G induise sur l'ensemble G/H une structure de groupe, i.e. on voudrait définir $(xH) * (yH) = xyH$; pour cela il faut vérifier que la formule ne dépend pas des choix de x et y, i.e. que pour $x' = xh_1$ et $y' = yh_2$ on a bien $x'y'H = xyH$ autrement dit pour tout $h_1, h_2 \in H$, il existe $h \in H$ tel que $xh_1yh_2 = xyh$ que l'on peut écrire encore sous la forme $yHy^{-1} \subset H$. On introduit alors la notion suivante.

Définition 1.7. — Un sous-groupe H de G est dit *distingué* si pour tout $g \in G$, on a $gHg^{-1} \subset H$. Un groupe est dit *simple* si ses seuls sous-groupes distingués sont ses sous-groupes triviaux.

Proposition 1.8. — *La loi de G induit sur G/H une structure de groupe si et seulement si H est un sous-groupe distingué de G.*

Remarque : en particulier si G est abélien alors tout sous-groupe est automatiquement distingué et G/H est, via la loi de G, muni d'une structure de groupe.
Exemple fondamental : reprenons la construction précédente pour le sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$. Ainsi la relation d'équivalence s'écrit :

$$x \sim_n y \Leftrightarrow n|x-y$$

et on dit que x et y sont *congruents modulo* n ; on écrit $x \equiv y \mod n$. L'ensemble quotient est $\mathbb{Z}/n\mathbb{Z}$ dont les éléments sont $\bar{x} = \{x + kn : \ k \in \mathbb{Z}\}$. On peut ainsi écrire, par exemple, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$, où un élément x appartient à $\bar{r}$ pour r le reste de la division euclidienne de x par n. On vérifie alors aisément que la définition suivante est cohérente : $\bar{x} + \bar{y} = \overline{x_0 + y_0}$ où x_0 et y_0 sont des éléments quelconques de $\bar{x}$ et $\bar{y}$ respectivement.

1.2. Morphismes. —

Définition 1.9. — *Un morphisme de groupe $f : G \to G'$* est une application telle que pour tous $x, y \in G$ on a $f(xy) = f(x)f(y)$.

Remarque : l'élément neutre de G s'envoie nécessairement sur l'élément neutre de G' ; par ailleurs on a $f(x^{-1}) = f(x)^{-1}$.
Exemples :

- la fonction logarithme népérien : $\ln : \mathbb{R}_+^\times \to \mathbb{R}$ définit un morphisme de $(\mathbb{R}_+^\times, \times)$ dans $(\mathbb{R}, +)$. De même la fonction exponentielle définit un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^\times, \times)$.
- Pour $g \in G$ l'application $k \in \mathbb{Z} \mapsto g^k \in G$ est un morphisme dont l'image est $< g >$ le sous-groupe de G engendré par g.
- Pour $n \geq 1$, la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme. Plus généralement si H est un sous-groupe distingué de G, l'application qui à g associe sa classe $\bar{g}$ modulo H, est un morphisme surjectif.

La composée de deux morphismes est évidemment un morphisme ; en outre si le morphisme f est bijectif, on dit alors que f est *un isomorphisme* ou que G et G' sont isomorphes via f, alors son application inverse f^{-1} est aussi un morphisme. Dans le cas où $G' = G$, on dit que f est *un automorphisme* ; l'ensemble des automorphismes de g est par ailleurs un groupe pour la loi de composition.

Lemme 1.10. — *Soit f un morphisme de G vers G'.*
- *Pour tout sous-groupe H de G, l'image $f(H)$ est un sous-groupe de G'.*
- *Pour tout sous-groupe H' de G', l'image réciproque $f^{-1}(H') := \{h \in G : \ f(h) \in H'\}$ est un sous-groupe de G.*

Remarque : on se méfiera de la notation $f^{-1}(H)$ qui laisserait à penser que l'application f^{-1} existerait ce qui n'est à priori pas le cas sauf si f était un isomorphisme.

Définition 1.11. — On appelle noyau d'un morphisme $f : G \to G'$ et on note $\operatorname{Ker} f$ l'ensemble $f^{-1}(\{e'\}) := \{g \in G : \ f(g) = e'\}$. L'image de f est notée $\operatorname{Im} f$.

Remarque : $\operatorname{Ker} f$ est un sous-groupe distingué de G.

Lemme 1.12. — *Le morphisme $f : G \to G'$ est injectif si et seulement si* $\operatorname{Ker} f$ *est réduit à l'élément neutre.*

Théorème 1.13. — ***(de factorisation)***
Soit $f : G \to G'$ un morphisme de groupe. Alors le groupe quotient f induit un isomorphisme de $G/\operatorname{Ker} f$ sur $\operatorname{Im} f$.

Remarque : pour π un morphisme $G \to H$, on dit que f se factorise par H ou par π s'il existe $\bar{f} : H \to G'$ tel que $f = \bar{f} \circ \pi$. On notera que f se factorise toujours par un quotient G/H où $H \subset \operatorname{Ker} f$: en effet il suffit de poser $\bar{f}(\bar{g}) := f(g)$ puisque $f(gh) = f(g)$ pour tout $h \in H \subset \operatorname{Ker} f$.
Exemple : reprenons l'application $\mathbb{Z} \to G$ qui à k associe g^k pour $g \in G$. L'image est $< g >$ et son noyau est un sous-groupe de la forme $n\mathbb{Z}$ de sorte que $< g > \simeq \mathbb{Z}/n\mathbb{Z}$ où n est l'ordre de g. On peut ainsi voir cet ordre comme le plus petit entier strictement positif m tel que $g^m = 1$.

Définition 1.14. — Une application surjective $f : G \to G'$ de noyau $H = \operatorname{Ker} f$ se présente habituellement sous la forme *d'une suite exacte courte* :

$$1 \to H \to G \to G' \to 1.$$

Exercice : montrer que tout sous-groupe distingué est le noyau d'un morphisme.

1.3. Groupes résolubles. —

Définition 1.15. — Un groupe G est dit *résoluble* s'il possède une filtration croissante par des sous-groupes

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

avec G_i distingué dans G_{i+1} et G_{i+1}/G_i commutatif.

Remarque : moralement tout ce qu'on sait faire pour un groupe commutatif, on devrait pouvoir l'étendre au cas des groupes résolubles.

Définition 1.16. — *Le groupe dérivé* $D(G)$ d'un groupe G est le groupe engendré par les commutateurs $[a,b] := aba^{-1}b^{-1}$ pour $a, b \in G$.

Remarque : de la formule $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$, on en déduit que G est un groupe distingué. En outre $G/D(G)$ est commutatif et vérifie la propriété universelle suivante : tout morphisme $G \to H$ avec H commutatif se factorise par $G \twoheadrightarrow G/D(G)$.

Définition 1.17. — On définit par récurrence $D^0 = G$ et $D^{n+1}(G) = D(D^n(G))$ pour $n \geq 0$.

Lemme 1.18. — *Le groupe G est résoluble si et seulement si $D^n(G)$ est trivial pour n assez grand.*

Preuve : Supposons G résoluble et soit $G_0 \subset \cdots \subset G_n = G$ une filtration comme dans la définition 1.15. D'après la propriété universelle de $D(G)$, la surjection canonique $G \twoheadrightarrow G_n/G_{n-1}$ se factorise par $G/D(G)$ et donc $D(G) \subset G_{n-1}$. Par récurrence simple, on montre que $D^i(G) \subset G_{n-i}$ et donc $D^n(G)$ est trivial.

Réciproquement si $D^n(G)$ est trivial on pose $G_{n-i} = D^i(G)$ et la filtration obtenue convient.

Proposition 1.19. — *Si*

$$1 \to G_1 \longrightarrow G_2 \longrightarrow G_3 \to 1$$

est exacte alors G_2 est résoluble si et seulement si G_1 e G_3 le sont.

Preuve : On a d'une part $D^n(G_2) \longrightarrow D^n(G_3)$ surjectif et $D^n(G_1) \longrightarrow D^n(G_2)$ injectif de sorte que G_2 résoluble implique que G_1 et G_3 le sont. Inversement si $D^n(G_3)$ est trivial, l'image de $D^n(G_2)$ dans G_3 est nul et donc $D^n(G_2)$ est contenu dans G_1. Si en outre $D^m(G_1)$ est trivial alors $D^{m+n}(G_2) \subset D^m(G_1) = 1$ d'où le résultat.
Remarque : en itérant le résultat précédent on obtient le corollaire suivant qui dit que la classe des groupes résolubles est stable par extension.

Corollaire 1.20. — *Si G possède une filtration croissante de sous-groupes*

$$1 = G_0 \subset \cdots \subset G_n = G$$

avec G_i distingué dans G_{i+1} et G_{i+1}/G_i résoluble alors G est résoluble.

1.4. Sur le groupe symétrique. —

Définition 1.21. — L'ensemble des bijections de l'ensemble $\{1, \cdots, n\}$ muni de la loi de composition est un groupe noté $\mathfrak{S}_n$ appelé le groupe symétrique d'ordre n ; ses éléments sont appelés des permutations.

Remarque : pour E un ensemble fini de cardinal, toute bijection de E sur $\{1, \cdots, n\}$, induit un isomorphisme du groupe $\mathfrak{S}(E)$ des bijections de E dans E, sur $\mathfrak{S}_n$.

Lemme 1.22. — *Le cardinal de $\mathfrak{S}_n$ est égal à $n!$.*

Remarque : il n'est pas raisonnable d'espérer comprendre « parfaitement » le groupe $\mathfrak{S}_n$; en effet d'après le théorème de Cayley, en faisant, avec le vocabulaire du paragraphe suivant, opérer tout groupe G sur lui-même par translation à gauche, G s'identifie à un sous groupe de $\mathfrak{S}_{|G|}$. Un argument plus convaincant pour justifier l'étude plus précise des $\mathfrak{S}_n$ est l'heuristique suivante : pour comprendre un groupe G, il est en général très instructif de le faire agir sur

un ensemble E, i.e. de construire un morphisme $G \to \mathfrak{S}(E)$ c'est même parfois seulement comme cela que le groupe G est défini.

Définition 1.23. — Les orbites de l'action du groupe engendré par σ sur $\{1, \cdots, n\}$, sont appelés ses cycles ; si $1 \leq k \leq n$ appartient à un cycle de longueur > 1, on dit qu'il appartient au support de σ. Si le support de σ est constitué d'un unique cycle de cardinal m, on dit que σ est un m-cycle.

Remarque : autrement dit le support d'une permutation σ est l'ensemble des k tels que $\sigma(k) \neq k$. Les dérangements sont les permutations de support maximal, i.e. $\{1, \cdots, n\}$; ce sont en quelque sorte les permutations les plus compliquées celles que l'on ne peut pas identifier avec une permutation d'ordre strictement plus petit. A l'opposé, les permutations les plus simples sont les 2-cycles que l'on appelle les transpositions.

Théorème 1.24. — *Toute permutation $\sigma \in \mathfrak{S}_n$ peut s'écrire comme la composée de cycles à supports disjoints. Cette décomposition est unique au sens où l'ordre de composition de ces cycles est indifférent. Les supports de ces cycles correspondent aux orbites de σ.*

Remarque : le résultat précédent s'appelle *la décomposition à supports disjoints* d'une permutation. En particulier en utilisant que l'ordre d'un m-cycle est m et la commutation de deux cycles à supports disjoints, on en déduit que l'ordre de σ est égal au ppcm des cardinaux de ses orbites.

Proposition 1.25. — *Soit $c \in \mathfrak{S}_n$ un m-cycle ; pour tout $r \in \mathbb{N}$, la décomposition à support disjoints de c^r admet $m \wedge r$-cycles tous de longueur $\frac{m}{m \wedge r}$. Une permutation $\sigma \in \mathfrak{S}_n$ commute avec c si et seulement elle s'écrit sous la forme $c^r \circ \sigma'$ où le support de σ' est disjoints de celui de c.*

Remarque : le commutant de c en tant que sous-groupe de $\mathfrak{S}_n$ est ainsi isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathfrak{S}_{n-m}$.

Si on cherche les générateurs les plus simples possibles, on se tourne vers les transpositions et on peut montrer les résultats suivants :

(i) les transpositions engendrent $\mathfrak{S}_n$;

(ii) les transpositions $(i\ i+1)$ engendrent $\mathfrak{S}_n$;

(iii) les transpositions $(1\ i)$ engendrent $\mathfrak{S}_n$.

Dans les deux derniers cas, on remarque qu'on ne peut pas enlever des transpositions : si (iii) on enlève $(1\ k)$ alors toute permutation dans le groupe engendré par les autres laisse k invariant ; dans (ii) ce sont les sous-ensembles $[1, k]$ et $[k+1, n]$ qui sont stables. On peut en fait montrer le résultat suivant.

Proposition 1.26. — *Soit $\{\tau_1, \cdots, \tau_r\}$ un ensemble de transpositions qui engendrent $\mathfrak{S}_n$, alors $r \geq n-1$.*

Remarque : si on s'autorise à prendre d'autres permutations, on note que $(1\ 2)$ et $(1\ 2 \cdots n)$ engendrent $\mathfrak{S}_n$; évidemment comme $\mathfrak{S}_n$ n'est pas commutatif pour $n \geq 3$, on ne peut pas trouver un seul générateur.

Une question usuelle dans l'étude d'un groupe est de comprendre ses classes de conjugaison, autrement dit en language savant, les orbites de l'action du groupe sur lui-même par

conjugaison. Dans le cas du groupe symétrique la question est réglée par la décomposition en cycles à support disjoints via la formule

$$\sigma \circ (a_1 \ \cdots \ a_r) \circ \sigma^{-1} = (\sigma(a_1) \ \cdots \ \sigma(a_r)).$$

Proposition 1.27. — *Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même nombre de cycles de longueur donnée, dans l'écriture de leur décomposition en cycles à supports disjoints*

Remarque : la formule précédente permet de montrer aisément que, pour $n \geq 3$, le centre de $\mathfrak{S}_n$ est réduit à l'identité. Selon le même principe si f est un morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$ alors toutes les transpositions ont même image car elles sont toutes conjuguées, ainsi il y a au plus un caractère non trivial, i.e. une représentation de dimension 1, $\mathfrak{S}_n \to GL_1(\mathbb{C})$. Il reste alors à la construire.
Construction de la signature : il y a essentiellement trois façons de la définir.

- la première en imposant $\epsilon(\tau) = -1$ pour toute transposition τ puis $\epsilon(\sigma) = (-1)^r$ où σ peut s'écrire en produit de r transpositions. Il s'agit alors de vérifier que la parité de r ne dépend que de σ, par contre ainsi définie ϵ est clairement un morphisme.
- La deuxième est d'utiliser la décomposition en cycles à supports disjoints et d'imposer $\epsilon(\sigma) = (-1)^{n-L(\sigma)}$ où $L(\sigma)$ est le nombre d'orbites : cette fois ci ϵ est bien définie par contre il faut vérifier que c'est bien un morphisme.
- Enfin la troisième et la meilleure est de poser $\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$ (parfois on dit que $\epsilon(\sigma) = (-1)^s$ où s est le nombre d'inversions i.e. de couples $i < j$ tels que $\sigma(i) > \sigma(j)$) : ϵ est bien définie et clairement un morphisme.

Définition 1.28. — Le noyau de la signature est un sous-groupe distingué $\mathcal{A}_n$ dit alterné ; il est de cardinal $\frac{n!}{2}$.

Proposition 1.29. — *La classe de conjugaison dans $\mathfrak{S}_n$ d'un élément $\sigma \in \mathcal{A}_n$ donne deux classes de conjugaison de $\mathcal{A}_n$ (resp. une unique classe de conjugaison) si et seulement si le commutateur de σ est contenu dans $\mathcal{A}_n$ (resp. sinon).*

Preuve : Tout repose sur la remarque triviale suivante : soient $\tau \in \mathfrak{S}_n - \mathcal{A}_n$ avec $\sigma' = \tau \circ \sigma \circ \tau^{-1}$. Alors il existe $\rho \in \mathcal{A}_n$ tel que $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ si et seulement si $\tau^{-1} \circ \rho$ appartient au commutant de σ ; on conclut alors aisément.
Remarque : le commutateur de $\sigma \in \mathcal{A}_n$ est contenu dans $\mathcal{A}_n$ si et seulement si les longueurs des cycles dans la décomposition en cycles à supports disjoints sont tous impairs sans multiplicité. En effet si c est un tel cycle de longueur paire alors il appartient au commutant et n'appartient pas à $\mathcal{A}_n$; si $c_1 = (a_1 \cdots a_{2r+1})$ et $c_2 = (b_1 \cdots b_{2r+1})$ sont deux tels cycles distincts alors $(a_1 b_1) \circ \cdots \circ (a_{2r+1} b_{2r+1})$ appartient au commutant et pas à $\mathcal{A}_n$.

Proposition 1.30. — *Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.*

Corollaire 1.31. — *Le centre de $\mathcal{A}_n$ est réduit à l'identité pour $n \geq 3$.*

Théorème 1.32. — *Pour $n \geq 5$, $\mathcal{A}_n$ est simple.*

Remarque : il y a plusieurs preuves possibles : soit on se ramène au cas $n = 5$, soit en considérant le nombre minimal d'éléments « dérangés ». Dans tous les cas, il s'agit, étant donné un sous-groupe distingué H non trivial de $\mathcal{A}_n$, de construire un 3-cycle dans H de sorte que comme les 3-cycles sont conjugués dans $\mathcal{A}_n$, il les contient tous et est donc égal à $\mathcal{A}_n$. La

technique comme d'habitude en théorie des groupes consiste à étudier des commutateurs, i.e. les $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$.
Remarque : via les théorèmes de Sylow, on peut aussi montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

Corollaire 1.33. — *Le groupe dérivée de $\mathcal{A}_n$ est égal à $\mathcal{A}_n$ pour $n \geq 5$.*

Remarque : $\mathcal{A}_n$ n'est donc pas résoluble, fait qui à une application spectaculaire sur la non résolution par radicaux des équations polynomiales de degré ≥ 5 ;

De la simplicité de $\mathcal{A}_n$ pour $n \geq 5$, on montre que $\mathcal{A}_n$ est le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$. Le théorème de Sylow nous apprend que $\mathfrak{S}_n$ contient tous les groupes d'ordre n qui sont donc d'indice $(n-1)!$ ce qui est très gros. En ce qui concerne les gros sous-groupes citons le résultat suivant :

Proposition 1.34. — *Si G est un sous-groupe d'indice $1 \leq k \leq n$ de $\mathfrak{S}_n$ avec $n \geq 5$, alors $k = 1, 2, n$ et G est isomorphe à $\mathfrak{S}_n$, $\mathcal{A}_n$ ou $\mathfrak{S}_{n-1}$.*

1.5. Opération d'un groupe sur un ensemble. —

Définition 1.35. — Une action d'un groupe G sur un ensemble E est un morphisme de groupes

$$\phi : G \longrightarrow \mathfrak{S}(E).$$

Remarque : concrètement cela signifie que pour tout $g \in G$, $\phi(g) \in \mathfrak{S}(E)$ est une bijection de E telle que $\phi(gg') = \phi(g) \circ \phi(g')$; en particulier $\phi(1) = Id_E$.
Remarque : on dit parfois que la définition précédente définit une action à gauche, une action à droite étant alors définie comme un morphisme de $G^{op} \to \mathfrak{S}(E)$ où G^{op} est l'ensemble G muni de la loi $g * h = hg$.

Définitions 1.36. — *On considère l'action d'un groupe G sur un ensemble E.*
- *L'orbite d'un élément $e \in E$ est par définition le sous-ensemble $\mathcal{O}_G(e) = \{g.e \ / \ g \in G\}$; évidemment si $e' \in \mathcal{O}_G(e)$ alors $\mathcal{O}_G(e) = \mathcal{O}_G(e')$. On dit que E est* G-homogène*, ou que G agit* transitivement *s'il n'y a qu'une seule orbite.*
- *Le stabilisateur de $e \in E$ est par définition le sous-groupe* $\mathrm{Stab}_G(e) = \{g \in G \ / \ g.e = e\}$ *; si $e' = g.e$ alors* $\mathrm{Stab}_G(e') = g\mathrm{Stab}_G(e)g^{-1}$. *On dit que G opère* fidèlement *si tous les stabilisateurs sont réduits à l'élément neutre.*

Remarque : on dit que G opère n-transitivement si pour tout $(x_i)_{1 \leq i \leq n}$ (resp. $(y_i)_{1 \leq i \leq n}$) distincts deux à deux, il existe $g \in G$ tel que pour tout $i = 1, \cdots, n$, $gx_i = y_i$.

Proposition 1.37. — *Pour tout $e \in E$ dont l'orbite est fini, on a $|\mathcal{O}_G(e)| = [G : \mathrm{Stab}_G(e)]$.*

Preuve : Il suffit de noter que l'application qui à $\bar{g}$ associe ge est une bijection d'image $\mathcal{O}_G(e)$.
Remarque : en particulier si G est fini, on peut écrire $|G| = |\mathcal{O}_G(e)|.|\mathrm{Stab}_G(e)|$.
Remarque : la version topologique de l'égalité numérique de la proposition précédente, consiste à dire qu'un ensemble G-homogène est isomorphe à un quotient G/H pour l'action de G par translation à gauche.

Corollaire 1.38. — ***(équations aux classes)***
Pour une action de G sur un ensemble E, on a

$$|E| = |E^G| + \sum_{\mathcal{O}_G(e)\in\mathcal{O} \ / \ |\mathcal{O}_G(e)|\neq 1} |\mathcal{O}_G(e)|$$

où $\mathcal{O}$ est l'ensemble des orbites et E^G désigne l'ensemble des points fixes.

Remarque : plus intéressante est *la formule de Burnside* qui permet de compter le nombre d'orbites :

$$\sum_{g\in G} |\mathrm{Fix}(g)| = |\mathcal{O}|.|G|.$$

Exemples :
- $E = G$: il y a 3 actions classiques, translation à gauche, à droite par g^{-1} et par conjugaison. Dans ce dernier cas, les orbites sont appelées *les classes de conjugaison.*
- E est un sous-groupe distingué de G : on peut alors faire opérer G par conjugaison
- E est un quotient de G : on fait alors agir G par translation à gauche.
- E est un ensemble de sous-groupe de G, par exemple ses sous-groupes de Sylow
- E est un autre groupe : on peut demander que $G \to \mathfrak{S}(E)$ s'envoie sur $\mathrm{aut}(E)$ ce qui permet de définir la notion de *produit semi-direct* et définir par exemple le groupe diédral.
- E est un espace vectoriel : on peut demander que l'image de G soit contenue dans les applications linéaires. On arrive alors à la notion de *représentations linéaires des groupes*, thème qui sera abordé au second semestre.

1.6. Caractères des groupes abéliens finis. — Soit G un groupe abélien fini noté multiplicativement.

Définition 1.39. — On appelle *caractère* de G, tout morphisme de groupes de G dans $\mathbb{C}^\times$. On note $\widehat{G}$ l'ensemble des caractères de G ; c'est un sous- groupe de l'ensemble des fonctions de G dans $\mathbb{C}^\times$.

Remarque : comme G est fini, d'après le théorème de Lagrange pour tout $g \in G$, on a $g^{\sharp G} = 1_G$. Ainsi pour tout caractère χ de G, on a $\chi(g)^{\sharp G} = 1$ i.e. les valeurs prises par χ sont des racines de l'unité. En particulier le conjugué $\overline{\chi}$ d'un caractère χ de G est égal à χ^{-1}.

Lemme 1.40. — *Soit G un groupe cyclique d'ordre n. Alors $\widehat{G}$ est isomorphe à G.*

Preuve : Notons g un générateur de G ; tout caractère $\chi \in \widehat{G}$ est déterminé par $\chi(g)$ qui est une racine n-ième de l'unité de sorte que $\widehat{G}$ s'identifie à un sous-groupe de $\mathbb{U}_n$, le groupe des racines n-ième de l'unité dans $\mathbb{C}$.

Inversement si $\xi \in \mathbb{U}_n$ alors l'application $g^i \mapsto \xi^i$ définit un élément de $\widehat{G}$. Ainsi G s'identifie à $\mathbb{U}_n$ lequel est bien isomorphe à G.

Proposition 1.41. — *Pour tout groupe abélien fini, $\widehat{G}$ est isomorphe à G.*

Preuve : D'après la remarque de la fin du paragraphe 5.3, G est un produit direct de groupe cyclique. Le résultat découle alors directement du lemme précédent.

Remarque : pour tout $g \in G$, l'application $\chi \mapsto \chi(g)$ définit un élément de $\widehat{\widehat{G}}$ et donc une identification canonique

$$G = \widehat{\widehat{G}}.$$

Proposition 1.42. — *Soit G un groupe abélien fini. Pour tout caractère χ de G, on a*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & si\ \chi \neq 1, \\ \sharp G & si\ \chi = 1. \end{cases}$$

Remarque : d'après la remarque précédente on a aussi

$$\sum_{\chi\in \widehat{G}} \chi(g) = \begin{cases} 0 & \text{si } g \neq 1, \\ \sharp G & \text{si } g = 1. \end{cases}$$

Preuve : Le cas $\chi = 1$ est évident. Supposons donc $\chi \neq 1$ et soit $h \in G$ tel que $\chi(h) \neq 1$. Comme $g \mapsto hg$ est une permutation de g, on a

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g)$$

et donc, comme $\chi(h) \neq 1$, il vient nécessairement $\sum_{g\in G} \chi(g) = 0$.

2. Polynômes

2.1. Généralités sur les anneaux, corps et algèbres. —

Définition 2.1. — On appelle *anneau* un triplet formé d'un ensemble A et de deux lois de composition interne, une addition $(x, y) \mapsto x + y$ et une multiplication $(x, y) \mapsto xy$, tels que :

- $(A, +)$ est un groupe commutatif d'élément neutre noté 0 ;
- la multiplication est associative et possède un élément neutre noté 1 ;
- la multiplication est distributive par rapport à l'addition, i.e.

$$x(y + z) = xy + xz \text{ et } (x + y)z = xz + yz \quad \forall x, y, z \in A.$$

Remarque : dans certains ouvrages, on en demande pas à A de posséder un élément neutre pour la multiplication et on parle d'anneau unitaire dans le cas où elle en possède un.
Remarque : si la multiplication est commutative, on dit que A est *un anneau commutatif.*
Exemples :

- l'ensemble $\mathbb{Z}$ des entiers relatifs muni de l'addition et de la multiplication est un anneau commutatif ; de même $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs.
- Pour X un ensemble et A un anneau, l'ensemble des applications de X à valeurs dans A est un anneau.
- Pour A un anneau et $n \geq 1$ un entier, l'ensemble $\mathbb{M}_n(A)$ des matrices carrées de taille n à coefficients dans A est un anneau non commutatif.
- Pour A un anneau, l'ensemble $A[X]$ des polynômes à coefficients dans A est un anneau.
- Pour $A_1, \cdots, A_n$ des anneaux, le produit cartésien $A = A_1 \times \cdots \times A_n$ muni de l'addition et de la multiplication composante par composante, est un anneau dit *anneau produit* des A_i.

Remarque : comme dans le paragraphe précédent, habituellement pour montrer qu'un triplet $(A, +, \times)$ est un anneau, on essaie de montrer qu'il s'agit d'un sous-anneau d'un anneau déjà construit, *un sous-anneau* étant un sous-groupe contenant l'élément neutre pour la multiplication et stable par produit.

Définition 2.2. — Un corps est un anneau commutatif dont tous les éléments non nuls sont inversibles.

Remarque : un anneau non commutatif dont tous les éléments admettent des inverses à gauche et à droite est généralement appelé *une algèbre à division* : le lecteur pourra alors vérifier que les inverses à gauche et à droite coïncident forcément.

Définition 2.3. — *Un idéal* à gauche (resp. à droite) I d'un anneau A est un sous-groupe de $(A, +)$ tel que pour tout $a \in A$ et pour tout $i \in I$, l'élément ai (resp. ia) de A appartienne à I. Un idéal est dit *bilatère* si c'est un idéal à gauche et à droite.

Remarque : si l'anneau A est commutatif alors tout idéal à gauche ou à droite est bilatère.
Exemples :
- les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$;
- pour X un ensemble et Y un sous-ensemble, le sous-ensemble de $F(X, \mathbb{R})$ formé des applications qui s'annulent sur Y est un idéal ;
- pour $a \in A$, l'ensemble aA (resp. Aa) est un idéal à droite (resp. à gauche) ; c'est *l'idéal principal* engendré par a que l'on note (a) dans le cas où A est commutatif.
- Si A est un corps alors ses seuls idéaux sont (0) et lui même : en effet dès qu'un idéal contient un inversible il est égal à tout l'anneau.

Remarque : pour I un idéal d'un anneau A on définit comme précédemment le quotient A/I qui est donc muni d'une loi de groupe induite par celle de A. La propriété de stabilité par multiplication à gauche par les éléments de A est alors juste celle qui est nécessaire pour que la multiplication de A induise sur A/I une structure d'anneau.

Définition 2.4. — Un morphisme d'anneau $f : A \to A'$ est un morphisme de groupe qui envoie l'élément neutre 1 de A sur celui de A' et tel que pour tout $x, y \in A$, on ait $f(xy) = f(x)f(y)$.

Remarque : la surjection canonique $A \twoheadrightarrow A/I$ est un morphisme d'anneau.

Lemme 2.5. — *Soit $f : A \to B$ un morphisme d'anneaux et A', B' des sous-anneaux de A et B respectivement.*
- *L'image $f(A')$ est un sous-anneau de B.*
- *L'image réciproque $f^{-1}(B')$ est un sous-anneau de A.*

Si J est un idéal de B alors $f^{-1}(J)$ est un idéal de A.

Remarque : en revanche l'image d'un idéal n'est pas nécessairement un idéal ; considérer par exemple l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$. En revanche si f est surjective alors l'image de tout idéal de A est un idéal de B.
Remarque : on a aussi une version du théorème de factorisation pour les morphismes d'anneaux puisque $\operatorname{Ker} f$ est clairement un idéal.

Définitions 2.6. — *On dira d'un anneau A qu'il est :*
- intègre *si l'égalité $xy = 0$ avec $x \neq 0$ implique $y = 0$;*
- principal *si tous ses idéaux sont principaux ;*

— noethérien *si toute chaine croissante* $I_1 \subset I_2 \subset \cdots$ *d'idéaux est stationnaire, i.e. il existe* $n \geq 1$ *tel que pour tout* $r \geq 0$, $I_{n+r} = I_n$;
— artinien *si toute chaine décroissante* $\cdots \subset I_2 \subset I_1$ *d'idéaux est stationnaire, i.e. il existe* $n \geq 1$ *tel que pour tout* $r \geq 0$, $I_{n+r} = I_n$;
— euclidien *s'il est intègre et qu'il existe* $\nu : A - \{0\} \to \mathbb{N}$ *tel que pour tout* $a, b \neq 0 \in A$ *il existe* $(q, r) \in A^2$ *tel que* $a = bq + r$ *avec* $r = 0$ *ou* $\nu(r) < \nu(b)$.

Définitions 2.7. — *On dira d'un idéal* I *de* A *qu'il est :*
— maximal *s'il est pour l'inclusion, i.e.* $I \subset J$ *alors soit* $J = I$ *soit* $J = A$;
— premier *si* $xy \in I$ *avec* $x \notin I$ *implique* $y \in I$;
— primaire *si* $xy \in I$ *avec* $x^n \notin I$ *pour tout* $n \geq 1$ *implique qu'il existe* $n \geq 1$ *tel que* $y^n \in I$.

Définitions 2.8. — *Un élément* $a \in A$ *est dit :*
— inversible *s'il possède un inverse pour la multiplication ; on note* $A^\times$ *l'ensemble des éléments inversibles de* A *qui est alors un groupe pour la multiplication appelé* le groupe des inversibles *de* A ;
— un diviseur de zéro, *s'il existe* $b \in A$ *non nul tel que* $ab = 0$;
— nilpotent *s'il existe* n *tel que* $a^n = 0$.

Définition 2.9. — Si $A^\times = A - \{0\}$ alors on dit que A est un corps.

Exercice : montrer que I est maximal (resp. premier, resp. primaire) si et seulement si A/I est un corps (resp. intègre, resp. ses diviseurs de zéro sont nilpotents).

Définition 2.10. — On dit qu'un ensemble E est inductif si toute partie non vide totalement ordonnée admet un majorant dans E.

Remarque : $\mathbb{R}$ muni de la relation d'ordre usuelle n'est pas inductif ; en revanche l'ensemble des parties d'un ensemble ordonné par l'inclusion est inductif.

Lemme 2.11. — ***(dit de Zorn)***
Tout ensemble non vide inductif admet un élément maximal.

Remarque : ce lemme peut être vu comme un axiome de la théorie des ensembles ; il est en fait équivalent à *l'axiome du choix* qui affirme que si $(E_i)_{i \in I}$ est une famille d'ensembles non vide alors $\prod_{i \in I} E_i$ est non vide.

Proposition 2.12. — *Tout anneau non nul admet un élément maximal.*

Preuve : Soit E la famille des idéaux propres de A ; comme A est non nul, $\{0\}$ est dans E qui est donc non nul. L'ensemble E est inductif : en effet la réunion d'une famille totalement ordonnée d'idéaux propres est encore un idéal propre qui est un majorant. On conclut alors en invoquant le lemme de Zorn.

2.2. Généralités sur les polynômes. — Dans ce qui suit $\mathbb{K}$ désigne un corps quelconque que l'on pourra dans un premier temps supposé égal à $\mathbb{R}$ ou $\mathbb{C}$.

Définitions 2.13. — *Rappelons qu'un polynôme* $P \in \mathbb{K}[X]$ *est par définition une suite* $(a_i)_{i \geq 0}$ *à support fini, i.e. il existe* n *tel que pour tout* $m > n$, $a_m = 0$. *Si le polynôme est non nul, il existe alors un tel* n *tel que* $a_n \neq 0$ *que l'on appelle* le degré *de* P *que l'on note* $\deg(P)$. *Il est dit* unitaire *si* le coefficient dominant $a_{\deg(P)}$ *est égal à* 1.

Remarque : ainsi $\mathbb{K}[X]$ s'identifie avec $\mathbb{K}^{(\mathbb{N})}$.
Remarque : par convention le degré du polynôme nul est posé égal à $-\infty$; on ordonne alors $\mathbb{N} \cup \{-\infty\}$ en rendant $-\infty$ plus petit que tout élément de $\mathbb{N}$. On prolonge ensuite l'addition de $\mathbb{N}$ en posant $(-\infty)+n = -\infty$ et $(-\infty)+(-\infty) = -\infty$. Avec ces conventions on a le lemme suivant.

Lemme 2.14. — *Soient $P, Q \in \mathbb{K}[X]$ alors*
— $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$ *avec égalité si* $\deg(P) \neq \deg(Q)$ *;*
— $\deg(PQ) = \deg(P) + \deg(Q)$.

Remarque : en particulier on en déduit que $\mathbb{K}[X]$ est un anneau intègre dont les éléments inversibles sont les polynômes constants non nuls que l'on identifie à $\mathbb{K}^\times$.
Remarque : on peut aussi définir *la valuation* d'un polynôme comme étant le plus petit m tel que $a_m \neq 0$ et on définit la valuation du polynôme nul comme étant égale à $+\infty$.

L'anneau $K[X]$ possède exactement les mêmes propriétés arithmétiques que $\mathbb{Z}$ et même plus. Les questions difficiles sur $\mathbb{Z}$ ont aussi un intérêt en remplaçant $\mathbb{Z}$ par $K[X]$; en utilisant la dérivation le plus souvent on parvient à avancer et les résultats sont une source d'inspiration pour les questions sur $\mathbb{Z}$.

Théorème 2.15. — *Soient A et B des polynômes de $K[X]$ avec $B \neq 0$. Il existe alors un unique couple $(Q, R) \in K[X]$ tel que*

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Remarque : Q s'appelle le quotient et R le reste de *la division euclidienne* de A par B.
Preuve : Elle est basée sur le fait élémentaire suivant : soient $U, V \in K[X]$ avec $k = \deg(U) \geq \deg(V) = q$ si a_k (resp. b_q) désigne le coefficient dominant de U (resp. de V) alors pour $Q = \frac{a_k}{b_q} X^{k-q}$ on a $\deg(U - VQ) < \deg(U)$.
Existence : soit $\mathcal{A} = \{A - BQ : \ Q \in K[X]\}$ et notons r le plus petit des degrés de ses éléments. Si on avait $r \geq \deg(B) \geq 0$ alors en appliquant ce qui précède, on construit un monôme Q' tel que $A - B(Q+Q') \in \mathcal{A}$ et de degré $< r$ d'où la contradiction.
Unicité : soient Q_1, Q_2 tels que $\deg(A - Q_i B) < \deg(B)$ pour $i = 1, 2$. On en déduit que

$$\deg(B) > \deg\Big((a - BQ_1) - (A - BQ_2)\Big) = \deg(B(Q_2 - Q_1))$$

et donc $Q_1 = Q_2$.
Muni de cette division euclidienne, on peut reprendre les énoncés sur $\mathbb{Z}$ et on obtient que :
— les idéaux de $K[X]$ sont principaux, i.e. engendrés par un unique polynôme ;
— notion de pgcd, ppcm ;
— relation de Bezout que l'on peut calculer via l'algorithme d'Euclide ;
— les lemmes d'Euclide et de Gauss sont vérifiés ;
— les éléments premiers sont les polynômes irréductibles et tout polynôme se décompose de manière unique aux inversibles près, comme un produit de polynômes premiers ;
— le quotient $K[X]/(P)$ est par définition l'ensemble des classes d'équivalence pour la relation d'équivalence

$$Q \sim Q' \Leftrightarrow P | (Q - Q').$$

Remarque : les lois $+, \times$ et la multiplication par un scalaire de K, munissent alors ce quotient d'une structure d'algèbre : comme dans le cas de $\mathbb{Z}$, on remarque les calculs dans le quotient sont indépendants du choix des représentants dans $K[X]$.

Toute classe d'équivalence possède un unique représentant dont le degré est strictement inférieur à celui de P : il se calcule comme le reste de la division euclidienne par P.

Proposition 2.16. — *Soit P un polynôme non constant ; la classe $\bar{A}$ d'un polynôme $A \in K[X]$ est inversible dans $K[X]/(P)$ si et seulement si A est premier avec P.*

Preuve : Si $\bar{A}$ est inversible alors il existe $\bar{B}$ tel que $\bar{A}.\bar{B} = \bar{1}$, autrement dit il existe Q tel que $AB + PQ = 1$ et donc $A \wedge P = 1$. Réciproquement si $A \wedge P = 1$, on considère une relation de Bezout $AB + PQ = 1$ de sorte que $\bar{B}$ est l'inverse de $\bar{A}$ dans $K[X]/(P)$.

2.3. Théorème de Gauss. — Dans ce qui suit A désigne un anneau factoriel, et donc intègre, de corps des fractions K.

Définition 2.17. — On dit qu'un polynôme $P \in A[X]$ est *irréductible* si
- $P \notin A[X]^* = A^*$,
- $\forall Q, R \in A[X]$ tels que $P = QR$, on a $Q \in A^*$ ou $R \in A^*$.

Remarque : L'hypothèse de factorialité de l'anneau A implique que $A[X]$ est factoriel. Par ailleurs, lorsque k est un corps, $k[X]$ est euclidien, donc factoriel. Ainsi, on se place toujours dans un cadre qui assure l'existence et l'unicité de la décomposition d'un polynôme en produits de facteurs irréductibles.

Exemples :
- Sur un corps algébriquement clos, les seuls polynômes irréductibles sont les polynômes de degré 1.
- Sur $\mathbb{R}$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 de la forme $aX^2 + bX + c$, avec $a \neq 0$ et $b^2 - 4ac < 0$.
- Nous verrons plus loin que sur $\mathbb{Q}$ ou sur un corps fini, il existe des polynômes irréductibles de n'importe quel degré.

Définition 2.18. — Soit $P \in A[X]$. On appelle *contenu* de P le pgcd de ses coefficients. On le note $c(P)$. On dit que P est *primitif* lorsque $c(P) = 1$.

Lemme 2.19. — ***Gauss*** *Pour tous $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Lemme 2.20. — *Soient $P, Q \in A[X]$ tel que P soit unitaire et PQ soit unitaire et à coefficients entiers. Alors Q est unitaire et P et Q sont à coefficients entiers.*

Preuve : Le fait que Q est unitaire est évident. Écrivons maintenant $P = X^\alpha + \frac{1}{\mu}\sum_{i=0}^{\alpha-1} p_i X^i$, où les entiers $\mu, p_0, \ldots, p_{\alpha-1}$ sont premiers entre eux dans leur ensemble (pour cela, il suffit de choisir pour μ le ppcm des dénominateurs des coefficients de P). On écrit de même $Q = X^\beta + \frac{1}{\nu}\sum_{i=0}^{\beta-1} q_i X^i$, avec $\nu, q_0, \ldots, q_\nu$ premiers entre eux dans leur ensemble. On sait alors que les polynômes μP et νQ sont à coefficients entiers et de contenu 1. On a doncv1 $= c(\mu P)c(\nu Q) = c(\mu P.\nu Q) = \mu\nu.c(PQ) = \mu\nu$, ce qui implique que $\mu = \nu = 1$, i.e. que P et Q sont à coefficients entiers.

Proposition 2.21. — *Soit A un anneau factoriel et* $\mathrm{frac}(A)$ *son corps des fractions. Les polynômes irréductibles de $A[X]$ sont :*

— *les constantes irréductibles dans* A,
— *les polynômes non constants primitifs et irréductibles dans* $\mathrm{frac}(A)$.

Remarque : Le polynôme $2X$ et irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$.
Preuve :

2.4. Racines. — Rappelons qu'à un polynôme on associe habituellement sa fonction polynôme et que dans le cas où $\mathbb{K}$ est infini, cette dernière détermine le polynôme dont on est parti ; dans ce qui suit on cèdera à la facilité de cette identification.

Définition 2.22. — On dit que $a \in \mathbb{K}$ est une racine de P si $P(a) = 0$.

Lemme 2.23. — *Soit* $P \in \mathbb{K}[X]$ *; alors* $P(a) = 0$ *si et seulement si* $X - a$ *divise* $P(X)$.

Preuve : Le résultat découle immédiatement de la division euclidienne $P = (X-a)Q+P(a)$.
Remarque : ainsi un polynôme irréductible n'a pas de racines. La réciproque est bien entendue fausse en général ; il faut en fait regarder les racines de P dans toutes les extensions de degré $\leq \deg P$, résultat qui sera abordé cette année.

Définition 2.24. — La multiplicité dans P de $a \in \mathbb{K}$ est le plus grand entier $r \geq 0$ tel que $(X - a)^r$ divise P.

Remarque : la multiplicité est non nulle si et seulement si a est une racine de P ; si $r = 1$ on dit que a est *une racine simple* et sinon *une racine multiple.*

Proposition 2.25. — *La multiplicité de la racine* a *de* P *est l'entier* $r \geq 1$ *tel que* $P(a) = P'(a) = P^{(r-1)}(a) = 0$ *et* $P^{(r)}(a) \neq 0$.

Preuve : Il suffit d'appliquer la formule de Taylor en a.
Remarque : en appliquant le lemme de Gauss, si $a_1, \cdots, a_n$ sont des racines de P de multiplicité $r_1, \cdots, r_n$ alors P est divisible par $\prod_{i=1}^{n}(X - a_i)^{r_i}$. En particulier on en déduit qu'un polynôme possède au plus $\deg P$ racines comptées avec multiplicités.
Remarque : un polynôme ne possède que des racines simples si et seulement si P et P' sont premiers entre eux.

Définition 2.26. — Un polynôme P pouvant s'écrire sous la forme $\lambda \prod_{i=1}^{n}(X - a_i)^{r_i}$ avec $\lambda \in \mathbb{K}$ est dit *totalement décomposé.*

Remarque : un corps $\mathbb{K}$ dans lequel tous les polynômes sont totalement décomposé est dit *algébriquement clos.* Le théorème de d'Alembert-Gauss affirme que $\mathbb{C}$ est algébriquement clos : c'est un résultat d'analyse qui repose de manière essentielle sur le théorème des valeurs intermédaires.

2.5. Polynômes symétriques. —

Définition 2.27. — Pour $a_1, \cdots, a_n \in \mathbb{K}$ on définit pour $1 \leq k \leq n$:

$$\sigma_k(a_1, \cdots, a_n) := \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} a_{i_1} a_{i_2} \cdots a_{i_k}.$$

Remarque : ainsi pour $k = 1$ (resp. $k = n$) on obtient $a_1 + \cdots + a_n$ (resp. $a_1 \cdots a_n$).

Proposition 2.28. — *Pour $a_1, \cdots, a_n \in \mathbb{K}$, on a l'égalité*

$$\prod_{i=1}^{n}(X - a_i) = X^n - \sigma_1(a_1, \cdots, a_n)X^{n-1} + \sigma_2(a_1, \cdots, a_n)X^{n-2} + \cdots + (-1)^n\sigma_n(a_1, \cdots, a_n).$$

Remarque : ainsi pour $n = 2$ on trouve $(X - a)(X - b) = X^2 - (a + b)X + ab$.

Pour $\underline{i} = (i_1, \cdots, i_n)$, on note $X^{\underline{i}} = X_{i_1} \cdots X_{i_n}$; ce monôme est dit *de degré n* et *de poids* $i_1 + 2i_2 + \cdots + ni_n$; le degré (resp. le poids) d'un polynôme est le maximum du degré (resp. du poids) de ses monômes. Le résultat fondamental est le suivant.

Théorème 2.29. — *(i) La sous-algèbre $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$ des polynômes symétriques, est engendrée sur $\mathbb{Z}$ par les polynômes symétriques élémentaires*

$$\sigma_1 = X_1 + \cdots + X_n, \qquad \sigma_k = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k}, \quad \sigma_n = X_1 \cdots X_n.$$

(ii) Les $\sigma_1, \cdots, \sigma_n$ son algébriquement indépendants sur $\mathbb{Z}$ de sorte que tout $P \in K[X_1, \cdots, X_n]^{\Sigma_n}$ s'écrit de façon unique comme un polynôme $Q(\sigma_1, \cdots, \sigma_n)$; le poids de Q est inférieur ou égal au degré de P.

(iii) La famille des monômes $X^{\underline{m}} = X_1^{m_1} \cdots X_n^{m_n}$ tels que $0 \le m_i < i$ pour $1 \le i \le n$, est une base de $\mathbb{Z}[X_1, \cdots, X_n]$ comme module sur le sous-anneau $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$; c'est donc un $\mathbb{Z}[X_1, \cdots, X_n]^{\Sigma_n}$-module libre de rang $n!$.

Remarque : en ce qui concerne les fractions rationnelles, on a encore

$$\mathbb{K}(X_1, \cdots, X_n)^{\mathfrak{S}_n} = \mathbb{K}(\sigma_1, \cdots, \sigma_n).$$

Comme conséquence important, on obtient que $\mathfrak{S}_n$ est le groupe de Galois de l'équation générale d'ordre n, i.e. si $\mathbb{L}$ désigne le corps de décomposition sur $K = k(a_1, \cdots, a_n)$ du polynôme $X^n - a_1X^{n-1} + \cdots + (-1)^n a_n$ alors $\mathbb{L}/\mathbb{K}$ est galoisienne de groupe de Galois $\mathfrak{S}_n$ vu comme le groupe des permutations des solutions $x_1, \cdots, x_n$ du polynôme ci-dessus.

2.6. Résultant et discriminant. — Soient

$$P(X) = a_0 + a_1X + \cdots + a_pX^p, \quad a_p \neq 0$$
$$Q(X) = b_0 + b_1X + \cdots + b_qX^q, \quad b_q \neq= 0$$

deux polynômes à coefficients dans un anneau A.

Définition 2.30. — On appelle *matrice de Sylvester* de P et Q la matrice suivante :

$$S(P,Q) = \begin{pmatrix} a_p & \cdots & \cdots & & a_0 & & \\ & \ddots & & & & \ddots & \\ & & a_p & \cdots & \cdots & & a_0 \\ b_q & \cdots & & b_0 & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & & \\ & & & b_q & & \cdots & b_0 \end{pmatrix} \begin{matrix} -- \\ q \\ -- \\ -- \\ \\ p \\ \\ -- \end{matrix} \begin{matrix} \\ \textit{lignes} \\ \\ \\ \\ \textit{lignes} \\ \\ \\ \end{matrix} \tag{1}$$

Le résultant de P et Q, noté $R(P, Q)$ est le déterminant de $S(P, Q)$.

Remarque : en échangeant les q premières lignes avec les p dernières, on voit que :

$$R(P,Q) = (-1)^{pq}R(Q,P). \tag{2}$$

Lemme 2.31. — *Supposons P et Q à coefficients dans un corps K.*

1. Si Q divise P, on a $R(P,Q)=0$;

2. si Q ne divise pas P, soient R le reste de la division de P par Q, r le degré de R. Alors

$$R(P,Q) = (-1)^{pq} b_q^{p-r} R(Q,R). \tag{3}$$

Preuve : Multiplions la i-ième colonne de la matrice $S(P,Q)$ par X^{p+q-i}. On obtient la matrice $\tilde{S}(P,Q)(X)$ suivante :

$$\left(\begin{array}{ccccccc}
a_pX^{p+q-1} & \dots & & & a_0X^{q-1} & 0 & \dots \\
 & \ddots & & & & \ddots & \\
0 & \dots & a_pX^p & \dots & & & a_0 \\
b_qX^{p+q-1} & \dots & & b_0X^{p-1} & 0 & \dots & 0 \\
0 & \ddots & & & \ddots & & \\
\vdots & & \ddots & & & & \\
0 & \dots & & b_qX^q & \dots & & b_0
\end{array}\right) \begin{array}{c} -- \\ q \\ -- \\ -- \\ \\ p \\ \\ -- \end{array} \begin{array}{l} \\ lignes \\ \\ \\ \\ lignes \\ \\ \end{array} \tag{4}$$

telle que $\tilde{S}(P,Q)(1) = S(P,Q)$. Remarquons que dans la matrice $\tilde{S}(P,Q)(X)$, la ligne l_i est formée des monômes du polynôme $X^{q-i}P(X)$ pour $1 \le i \le q$, et des monômes du polynôme $X^{p+q-i}Q(X)$ pour $q+1 \le i \le p+q$.
Montrons maintenant (3). Si $q > p$, on a $R = P$, et le lemme est vrai par la formule (2).
Si $p \ge q$, considérons la division euclidienne :

$$P = QA + R, \quad \deg(R) < \deg(Q) \text{ ou } R = 0. \tag{5}$$

Posons :

$$A(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-q}X^{p-q}\,;$$

on a donc :

$$QA = \alpha_0 Q + \alpha_1(XQ) + \cdots + \alpha_{p-q}(X^{p-q}Q). \tag{6}$$

1. Si Q divise P, on voit ainsi en utilisant (6) que la relation $P = QA$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est une combinaison linéaire des lignes $l_{p+q}, l_{p+q-1}, \dots, l_{2q}$ avec coefficients $\alpha_0, \dots, \alpha_{p-q}$. Le déterminant de la matrice $\tilde{S}(P,Q)(X)$ est donc nul, ce qui implique que $R(P,Q) = 0$.
2. Dans le cas général, posons

$$R(X) = c_0 + c_1X + \cdots + c_rX^r$$

avec $c_r \neq 0$. On voit alors en utilisant (6) que la relation $P = QA + R$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est la somme de la ligne $(0, \dots, 0, c_rX^r, \dots, c_0)$ correspondant au polynôme $R(X)$, et d'une combinaison linéaire des lignes $l_{p+q}, l_{p+q-1}, \dots, l_{2q}$ avec coefficients $\alpha_0, \dots, \alpha_{p-q}$.
On peut donc remplacer la ligne l_q de $\tilde{S}(P,Q)(X)$ par la ligne $(0, \dots, 0, c_rX^r, \dots, c_0)$ sans changer son déterminant.
En procédant de même avec les relations

$$X^iP = X^iQA + X^iR$$

pour $0 \le i \le q-1$, on voit que l'on peut remplacer les q premières lignes de $\tilde{S}(P,Q)(X)$ par les lignes formées de zéros et des monômes des polynômes X^iR, $0 \le i \le q-1$, la ligne l_{q-i} étant

remplacée par la ligne $(0,\dots,0,c_rX^{r+i},\dots,c_0X^i,0,\dots,0)$, ceci sans changer le déterminant. En faisant $X=1$ on voit alors que le déterminant de $S(P,Q)$ est égal au déterminant de la matrice :

$$\left(\begin{array}{ccccccc} 0 & \dots & c_r & \dots & c_0 & 0 & \dots \\ & & & \ddots & & \ddots & \\ 0 & \dots & & & c_r & \dots & c_0 \\ b_q & \dots & & b_0 & 0 & \dots & \\ 0 & \ddots & & & \ddots & & \\ \vdots & & \ddots & & & & \\ 0 & \dots & & b_q & \dots & & b_0 \end{array}\right) \begin{array}{l} -- \\ q \\ -- \\ -- \\ \\ p \\ \\ -- \end{array} \begin{array}{l} \\ lignes \\ \\ \\ \\ lignes \\ \\ \end{array}$$

d'où la relation (3).
Remarque : on peut ainsi calculer le résultant en utilisant l'algorithme d'Euclide.

Corollaire 2.32. — *Soit K un corps. Avec les notations ci-dessus, les conditions suivantes sont équivalentes :*

1. *$R(P,Q)=0$;*
2. *les polynômes P et Q ont un facteur commun de degré >0 dans $K[X]$.*

Preuve : 1) $\Rightarrow$ 2) : supposons que 2) soit faux, i.e. que P et Q n'aient pas de facteur commun dans $K[X]$. Le PGCD de P et Q est alors une constante $c\neq 0$. Le lemme précédent appliqué récursivement donne

$$R(P,Q)=\alpha R(R_s,c)$$

avec $\alpha\neq 0$, $c\neq 0$ et R_s un reste de degré $r_s>0$. Mais alors $R(R_s,c)=c^{r_s}\neq 0$, et donc que $R(P,Q)\neq 0$.

2. $\Rightarrow$ 1. Si P et Q ont un facteur commun non trivial A dans $K[X]$, supposons d'abord que $P=QA$ avec A de degré $p-q>0$. Alors le lemme précédent montre que $R(P,Q)=0$. Dans le cas général, on se retrouve dans la situation ci-dessus en considérant le dernier reste non nul dans l'algorithme d'Euclide.

Proposition 2.33. — *Supposons que dans $K[X]$, on ait :*

$$P=a_p(X-\alpha_1)\dots(X-\alpha_p)$$
$$Q=b_q(X-\beta_1)\dots(X-\beta_q).$$

Alors

$$R(P,Q)=a_p^qb_q^p\prod_{i,j}(\alpha_i-\beta_j)=a_p^q\prod_{1\leq i\leq p}Q(\alpha_i)=(-1)^{pq}b_q^p\prod_{1\leq j\leq q}P(\beta_j) \tag{7}$$

Preuve : Les égalités :

$$a_p^qb_q^p\prod(\alpha_i-\beta_j)=a_p^q\prod Q(\alpha_i)=(-1)^{pq}b_q^p\prod P(\beta_j)$$

sont immédiates.
Posons $R_2(P,Q)=a_p^q\prod Q(\alpha_i)=(-1)^{pq}b_q^p\prod P(\beta_j)$. Pour montrer que $R_2(P,Q)=R(P,Q)$, il suffit de montrer que R_2 satisfait à la même relation de récurrence (3) que $R(P,Q)$. On peut supposer $p\geq q>0$ (car on a évidemment $R(P,Q)=R_2(P,Q)=b_q^p$ si $q=0$). Si $P=QA+R$, on a $P(\beta_j)=R(\beta_j)$ pour toute racine β_j de Q, et donc :

$$R_2(P,Q)=(-1)^{pq}b_q^p\prod P(\beta_j)=(-1)^{pq}b_q^p\prod R(\beta_j)=(-1)^{pq}b_q^{p-r}R_2(Q,R),$$

ce qui est bien la même relation que (3).

Définition 2.34. — Soit A un anneau intègre et $P = a_pX^p + \cdots + a_0 \in A[X]$ tel que $a_p \neq= 0$. Alors on définit *le discriminant* $D(P)$ par la formule :

$$D(P) = \frac{(-1)^{p(p-1)/2}}{a_p} R(P, P').$$

Remarque : cette définition a bien un sens quel que soit l'anneau intègre A, car dans la matrice de Sylvester $R(P, P')$, la première colonne est divisible par a_p, puisque $P' = pa_pX^{p-1} + \cdots + a_1$.

Proposition 2.35. — *Si* $P(X) = a_p(X - \alpha_1)\dots(X - \alpha_p)$, *alors :*

$$D(P) = (-1)^{p(p-1)/2} a_p^{2p-2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_p^{2p-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Preuve : On a

$$P'(X) = a_p \sum_{i=1}^{p} (X - \alpha_1)\dots(\widehat{X - \alpha_i})\dots(X - \alpha_p),$$

la notation $(\widehat{X - \alpha_i})$ signifiant que l'on omet le terme $(X - \alpha_i)$ dans le produit. D'après **??**, on a $R(P, P') = (-1)^{p(p-1)/2} a_p^{p-1} \prod_{i=1}^{p} P'(\alpha_i)$ et le résultat découle de l'égalité $P'(\alpha_i) = a_p(\alpha_i - \alpha_1)\dots(\alpha_i - \alpha_p)$, où le terme $(\alpha_i - \alpha_i))$ n'apparait pas.
Exemples :

1. Si $P = aX^2 + bX + c$, $P' = 2aX + b$, on a :

$$R(P, P') = (-1) \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix},$$

   d'où $D(P) = b^2 - 4ac$.

2. $P = X^3 + pX + q$, $P' = 3X^2 + p$, un petit calcul de déterminant montre facilement que $D(P) = -4p^3 - 27q^2$.

Remarque : les résultants permettent d'éliminer des variables dans des systèmes d'équations algébriques. Par exemple, notons C la courbe algébrique paramétrée par

$$\begin{cases} x = \frac{2t}{1+t^2} \\ y = \frac{1-t^2}{1+t^2} \end{cases}$$

L'ensemble des points de $C \subset \mathbb{C}^2$ de corrdonnées (x, y) sont ceux pour lesquels il existe $t \in \mathbb{C} - \{\pm i\}$ solution commune des deux équations

$$\begin{cases} (1 + t^2)x = 2t \\ (1 + t^2)y = 1 - t^2 \end{cases}$$

Comme pour $t = \pm i$, il n'y a pas de solutions, on peut enlever la restriction précédente. Or d'après ce que l'on a vu, pour $P_{x,y} := xT^2 - 2T + x$ et $Q_{x,y} = (y+1)T^2 + y - 1$, l'annulation de $R(P_{x,y}, Q_{x,y})$ équivaut soit à $(x, y) = (0, -1)$ ou bien à $P_{x,y}$ et $Q_{x,y}$ ont une racine commune, i.e. $(x, y) \in C$. Le calcul du résultant en question donne $R = 4(x^2 + y^2 - 1)$ ce qui confirme que C est le cercle unité privé du point $(0, -1)$.

2.7. Polynômes cyclotomiques. — Soit $m \in \mathbb{N}^*$. On note $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$ l'ensemble des *racines m-ièmes de l'unité* dans $\mathbb{C}$. On rappelle que $\mathbb{U}_m$ est un groupe cyclique, et on appelle *racine primitive m-ième de l'unité* tout générateur de $\mathbb{U}_m$. On note $\mathbb{P}_m$ l'ensemble des racines primitives m-ième de l'unité.

Définition 2.36. — On appelle *m-ième polynôme cyclotomique* le polynôme

$$\Phi_m = \prod_{z \in \mathbb{P}_m} (X - z).$$

Proposition 2.37. — *(i) Le polynôme Φ_m est unitaire de degré $\phi(m)$.*
(ii) $X^m - 1 = \prod_{d|m} \Phi_d$.
(iii) Φ_m est à coefficients dans $\mathbb{Z}$.

Preuve : Les points (i) et (ii) découlent directement des propriétés de structure de $\mathbb{Z}/n\mathbb{Z}$. Montrons le point (iii) par récurrence :

- le résultat est immédiat pour $m = 1$ puisque $\Phi_1 = X - 1$.
- en supposant le résultat vrai pour tous les entiers inférieurs à m, on obtient que $U = \prod_{d|m, d \neq m} \Phi_d$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$. On peut donc effectuer dans $\mathbb{Z}[X]$ la division euclidienne de $X^m - 1$ par U : il existe $Q, R \in \mathbb{Z}[X]$ tels que $X^m - 1 = UQ + R$ et $deg(R) < deg(U)$. L'unicité de la division euclidienne dans $\mathbb{C}[X]$ permet de conclure que $Q = \Phi_m$ et $R = 0$, ce qui implique que Φ_m est bien à coefficients entiers.

Théorème 2.38. — *Le polynôme Φ_m est irréductible dans $\mathbb{Q}[X]$.*

Preuve : Pour montrer ce théorème, il suffit de montrer que Φ_m est le polynôme minimal de l'une de ses racines. Soit $z \in \mathbb{P}_m$ et $\pi \in \mathbb{Q}[X]$ son polynôme minimal (unitaire). On va montrer que π s'annule sur toutes les racines primitives m-ièmes de l'unité, ce qui impliquera que $\Phi_m = \pi$.

Commençons par remarquer que comme $X^m - 1$ s'annule en z, π le divise, donc il existe $R \in \mathbb{Q}[X]$ tel que $\pi R = X^m - 1$. Le lemme 2.20 affirme alors que π et R sont à coefficients entiers.

Considérons maintenant une racine ω de π et un nombre premier p ne divisant pas m, et supposons que ω^p n'est pas une racine de π. Tout d'abord, comme π divise $X^m - 1$, on sait que $\omega \in \mathbb{U}_m$, et donc que $\omega^p \in \mathbb{U}_m$. On a donc $0 = (\omega^p)^m - 1 = \pi(\omega^p)R(\omega^p)$. Comme on a supposé que ω^p n'est pas une racine de π, on obtient $R(\omega^p) = 0$. Le polynôme π étant irréductible, unitaire et s'annulant en ω, c'est le polynôme minimal de ω, donc il divise $R(X^p)$. Soit $S \in \mathbb{Q}[X]$ tel que $R(X^p) = \pi(X)S(X)$. À nouveau d'après le lemme 2.20, S est unitaire et à coefficients entiers.

Ainsi, l'égalité $R(X^p) = \pi(X)S(X)$ est une égalité dans $\mathbb{Z}[X]$, et on peut la passer modulo p : $\bar{R}(X)^p = \overline{R(X^p)} = \bar{\pi}(X)\bar{S}(X)$. Cette égalité nous assure que si T est un facteur irréductible de $\bar{\pi}$, alors T divise $\bar{R}(X)^p$, donc $\bar{R}(X)$. Par conséquent, T^2 divise $\bar{R}\bar{\pi} = \overline{X^m - 1} = X^m - 1$. Ceci est impossible car $X^m - 1$ et sa dérivée mX^{m-1} sont premiers entre eux : en effet, comme m est premier avec p, on peut l'inverser dans $\mathbb{Z}/p\mathbb{Z}$ et $\left(\frac{1}{m}X\right) mX^{m-1} - (X^m - 1) = 1$.

On obtient ainsi une contradiction ce qui montre que si ω est une racine de π et p un nombre premier ne divisant pas m, alors ω^p est aussi une racine de π.

Considérons maintenant une racine primitive m-ième de l'unité z'. On sait qu'il existe un entier n premier avec m et tel que $z' = z^n$. On écrit $n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$ où les p_i sont des entiers premiers ne divisant pas m. D'après la discussion précédente, et comme z est une racine de π, il est facile de montrer que z' est aussi une racine de π, ce qui termine la preuve du théorème.

Le théorème suivant, du à Kronecker, donne une caractérisation intéressante des polynômes cyclotomiques par les modules de leurs racines :

Théorème 2.39. — ***(de Kronecker)***
Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible dans $\mathbb{Q}[X]$ de degré supérieur ou égal à 1. On suppose que toutes ses racines sont de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Preuve : Soient $a_1, \dots, a_n$ les racines de P et p_0 son terme constant. D'après les relations racines-coefficients, $p_o = \prod a_i$. On a alors deux cas :

- soit l'une des racines est de module strictement inférieur à 1. Alors $|p_0| = \prod |a_i| < 1$, donc $p_0 = 0$. L'irréductibilité de P entraine donc que $P = X$.
- soit toutes les racines de P sont de module 1. Pour tout entier k, on pose $\mu_k = \prod_{i=1}^n (a_i^k - 1)$. C'est un polynôme symétrique en les racines de P, donc μ_k s'exprime comme un polynôme en les $\Sigma_{i,n}(a_1, \dots, a_n)$, i.e. en les coefficients de P. Par conséquent, μ_k est un entier pour tout k.

  Supposons maintenant que pour tout k, μ_k soit non nul. Alors

$$|a_1^k - 1| = \frac{\mu_k}{\prod_{i\neq 1} |\alpha_i - 1|} \geq \frac{1}{\prod_{i\neq 1} |a_i|^k + 1} = \frac{1}{2^{n-1}},$$

  donc le sous-groupe de $\mathbb{U}$ engendré par a_1 n'est pas dense. Il existe donc un rationel p/q tel que $a_1 = e^{2ip\pi/q}$. Mais alors $a_1^q = 1$ et $\mu_q = 0$, ce qui contredit notre hypothèse.

  On en déduit donc que μ_k s'annule pour un certain k, et donc qu'il existe i tel que $a_i^k = 0$. Comme P est le polynôme minimal de a_i, on en déduit qu'il divise $X^k - 1$, donc c'est un polynôme cyclotomique.

3. Espaces vectoriels

Dans ce qui suit $\mathbb{K}$ est un corps que l'on pourra supposer dans un premier temps égal à $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

3.1. Généralités. —

Définition 3.1. — Un $\mathbb{K}$-espace vectoriel est un triplet $(E, +, .)$ où

- $(E, +)$ est un groupe commutatif,
- muni d'une loi externe $(\lambda, e) \in \mathbb{K} \times E \mapsto \lambda.e \in E$ qui vérifie les propriétés suivantes :
  - pour tout $\lambda, \mu \in \mathbb{K}$ et pour tout $e \in E$, on a $(\lambda + \mu).e = \lambda.e + \mu.e$;
  - pour tout $\lambda \in \mathbb{K}$ et $e, f \in E$, on a $\lambda.(e + f) = \lambda.e + \lambda.f$;
  - pour tout $\lambda, \mu \in \mathbb{K}$ et $e \in E$, on a $(\lambda\mu).e = \lambda.(\mu.e)$;
  - pour tout $e \in E$ on a $1.e = e$.

Remarque : ces définitions prennent aussi sens dans le cas où $\mathbb{K}$ est simplement un anneau unitaire A, on parle alors de A-module : ce sujet sera abordé au premier semestre.
Exemples :

- $\mathbb{K}$ et plus généralement $\mathbb{K}^n$, $\mathbb{K}^{\mathbb{N}}$ ou $\mathbb{K}^{(\mathbb{N})}$;

— $\mathbb{M}_{m,n}(\mathbb{K})$ et $\mathbb{K}[X]$;
— les fonctions de X dans $\mathbb{K}$ où X est un ensemble quelconque ;
— le produit quelconque d'une famille d'espaces vectoriels est un espace vectoriel.

Définition 3.2. — Soit E un $\mathbb{K}$-espace vectoriel ; un sous-ensemble $F \subset E$ est *un sous-espace vectoriel* si et seulement si c'est un sous-groupe stable par la loi externe, i.e. si et seulement si pour tout $f_1, f_2 \in F$ et pour tout $\lambda \in \mathbb{K}$, on a : $f_1 + \lambda f_2 \in F$.

Exemples :
— $\mathbb{K}_n[X] \subset \mathbb{K}[X]$ le sous-ensemble des polynômes de degré $\leq n$;
— l'ensemble des suites convergentes de $\mathbb{K}^{\mathbb{N}}$;
— $\mathbb{R} \subset \mathbb{C}$ est un sous-$\mathbb{R}$-espace vectoriel mais n'est pas un sous-$\mathbb{C}$-espace vectoriel.
Remarque : comme précédemment un sous-espace vectoriel est un espace vectoriel et habituellement on se sert de cette remarque pour tester si on est en présence d'un espace vectoriel.
Remarque : l'intersection quelconque d'une famille de sous-espaces vectoriels est un espace vectoriel ce qui permet de définir le sous-espace vectoriel engendré par un sous-ensemble $A \subset E$ que l'on note $< A >$.
Remarque : si $\mathbb{K}$ est un corps infini, toute réunion finie de sous-espaces vectoriels est un sous-espace vectoriel si et seulement s'ils sont tous contenus dans un seul. En particulier une réunion finie d'hyperplans distincts n'est pas un sous-espace vectoriel. Que se passe-t-il dans le cas où $\mathbb{K}$ est fini ?
Exemple fondamental : soit $(e_i)_{i\in I}$ une famille *quelconque* d'éléments de E alors $< \{e_i : \ i \in I\} >$ est l'ensemble *des combinaisons linéaires* $\sum_{i\in I} \lambda_i e_i$ *à support fini.*

Définition 3.3. — Soient F, G des sous-espaces vectoriels d'un espace vectoriel E. *La somme* $F + G$ est le sous-espace $< F \cup G >$ engendré par F et G. On dit que F et G sont *en somme directe* et on écrit $F \oplus G$ si $F \cap G = \{0\}$.

Remarque : on vérifie aisément que $F + G = \{f + g : \ f \in F \text{ et } g \in G\}$; en outre F et G sont en somme directe si et seulement si l'écriture d'un élément $e \in F + G$ sous-la forme $f + g$ est unique.

Définition 3.4. — On dit que F et G sont *supplémentaires* si $E = F \oplus G$, i.e. si la somme $F + G$ est tout l'espace et qu'ils sont en somme directe.

Remarque : on veillera bien à ne pas confondre *supplémentaires* et *complémentaires* ; rappelons que le complémentaire d'un sous-espace vectoriel n'est jamais un sous-espace puisqu'il ne contient pas le vecteur nul !
Exercice : montrer que des sous-espaces $E_1, \cdots, E_n$ sont en somme directe si et seulement si pour tout $i = 1, \cdots, n$

$$E_i \cap \Big(\sum_{1\leq k\neq i\leq n} E_i \Big) = \{0\}.$$

3.2. Théorie de la dimension. —

Définition 3.5. — Une famille $\{(e_i)_{i\in I}\}$ de vecteurs d'un espace vectoriel E est dit *libre* si pour tout famille $(\lambda_i)_{i\in I} \in \mathbb{K}^{(I)}$ à support fini

$$\sum_{i\in I} \lambda_i e_i = 0 \Rightarrow \forall i \in I, \ \lambda_i = 0.$$

Elle est dite *génératrice* si $< \{e_i : \ i \in I\} >= E$, i.e. si tout vecteur de E peut s'écrire comme une combinaison linéaire à support fini des e_i.

Remarque : la famille $(X^i)_{i\in\mathbb{N}} \in \mathbb{K}[X]$ est libre et génératrice.
Remarque : la famille $(e_i)_{i\in I}$ est dite *liée* si elle n'est pas libre, i.e. s'il existe une famille $(\lambda_i)_{i\in I} \in \mathbb{K}^{(I)}$ non nulle telle que $\sum_{i\in I} \lambda_i e_i = 0$.

Définition 3.6. — Une famille $(e_i)_{i\in I}$ de vecteurs de E est *une base* si elle est libre et génératrice.

Remarque : la théorie de la dimension repose entière sur le résultat suivant dit *de la base incomplète.*

Théorème 3.7. — *Soient $\{f_1, \cdots, f_p\}$ une famille libre de vecteurs et $\{g_1, \cdots, g_q\}$ une famille génératrice de E. Il existe alors un entier $n \geq p$ et une base $\{e_1, \cdots, e_n\}$ de E telle que $e_i = f_i$ pour $1 \leq i \leq p$ et $e_j \in \{g_1, \cdots, g_q\}$ pour $p+1 \leq j \leq n$.*

Remarque : ainsi tout espace contenant une famille génératrice finie admet une base.

Corollaire 3.8. — *Soit E un espace vectoriel muni d'une base de cardinal n. Alors toute famille de cardinal strictement supérieur à n est liée.*

Remarque : on en déduit alors que le cardinal de toute base de E est toujours le même ; on l'appelle *la dimension* de E.

Corollaire 3.9. — *Tout sous-espace vectoriel F de E est de dimension inférieure ou égale à celle de E avec égalité si et seulement si $F = E$.*

Définition 3.10. — On appelle hyperplan d'un espace vectoriel E de dimension finie, tout sous-espace de dimension $n-1$.

Remarque : en dimension infinie, un hyperplan est un sous-espace tel que E/F est de dimension 1. La dimension de l'espace quotient E/F s'appelle *la codimension* de F dans E.
Remarque : la dimension de $E \times F$ est le produit des dimensions de E et F.
Remarque : toute famille libre est de cardinal $\leq n$ avec égalité si et seulement si c'est une base.
Remarque : la dimension de $F+G$ est inférieure ou égale à $\dim F + \dim G$ avec égalité si et seulement si F et G sont en somme directe. Plus précisément on a la formule du rang.

Théorème 3.11. — *Soient F, G deux sous-espace de E alors*

$$\dim(F+G) = \dim F + \dim G - \dim(F \cap G).$$

Finissons ce paragraphe par un court mot sur la dimension infinie.

Proposition 3.12. — *Soit E un $\mathbb{K}$-espace vectoriel et V, W_1, W_2 des sous-espaces tels que $V \cap W_1 = \{0\}$ et $V + W_2 = E$. Il existe alors un supplémentaire W de V contenu dans W_2 et contenant W_1.*

Preuve : Considérons l'ensemble $\mathcal{E}$ des sous-espaces de E contenant W_1 et contenus dans W_2 ; $\mathcal{E}$ n'est pas vide car $W_1 \in \mathcal{E}$. En outre $\mathcal{E}$ est partiellement ordonné par la relation d'inclusion et est inductif. Rappelons que cela signifie que toute chaine totalement ordonnée admet un majorant : ici pour une telle chaine, un majorant est simplement donné par la réunion qui est clairement un sous-espace.

D'après le lemme de Zorn, $\mathcal{E}$ admet un élément maximal, notons le W. Par définition on a donc $W \cap V = \{0\}$ et $W_1 \subset W \subset W_2$. Il reste alors à prouver que $V + W = E$; tout élément $x \in E$ s'écrit $x = v + w_2$ avec $v \in V$ et $w_2 \in W_2$. Si $w_2 \in W$ alors c'est gagné, sinon on considère le sous-espace engendré X par W et w_2. Par maximalité de W, X $\mathcal{E}$ de sorte qu'il existe $0 \neq y \in X \cap V$; ainsi $y = w + \lambda w_2 \in V$ et donc $y \in W \cap V$ ce qui n'est pas.
Remarque : le lecteur notera bien l'utilisation essentielle du lemme de Zorn qui rappelons le est équivalent à l'axiome du choix. Ainsi notre preuve n'est pas du tout constructive.

Corollaire 3.13. — *Tout sous-espace V de E admet un supplémentaire.*

Corollaire 3.14. — *Tout espace vectoriel non nul admet une base.*

Preuve : Considérons l'ensemble $\mathcal{A}$ des familles libres de E ; c'est clairement un ensemble non vide, partiellement ordonné par l'inclusion et inductif. D'après le lemme de Zorn, il possède un élément maximal qui est donc une famille libre maximal c'est donc nécessairement une famille génératrice et donc une base.
Remarque : le lecteur pourra s'exercer sur $\mathbb{K}^{\mathbb{N}}$ en vérifiant que toute base est nécessairement non dénombrable.

Corollaire 3.15. — ***(Théorème de la base incomplète)***
Soit $(e_i)_{i\in I}$ une partie génératrice de E. Soit $J \subset I$ tel que $(e_i)_{i\in J}$ est libre, il existe alors $J \subset K \subset I$ tel que $(e_i)_{i\in K}$ soit une base.

Preuve : On considère l'ensemble $\mathcal{A}$ des familles libres $(e_i)_{i\in A}$ pour $A \subset I$. C'est un ensemble non vide partiellement ordonné par l'inclusion et clairement inductif. D'après le lemme de Zorn, $\mathcal{A}$ possède une élément maximal K ; comme précédement $(e_i)_{i\in K}$ est libre et génératrice par maximalité de K.
Remarque : citons enfin le cas des espaces de Hilbert, i.e. des espaces hermitiens, au sens du paragraphe sur l'algèbre bilinéaire, qui sont complets, i.e. toutes les suites de Cauchy sont convergentes.

Définition 3.16. — On dit que $(e_i)_{i\in I}$ est *une base de Hilbert* d'un espace de Hilbert H si et seulement si :
- c'est une base orthonormée, i.e. $< e_i, e_j >= \delta_{i,j}$;
- la famille est complète au sens que pour tout $x \in H$ il existe $(\lambda_i)_{i\in I}$ telle que $\sum_{i\in I} \lambda_i e_i = x$, i.e. la série correspondante dans H est convergente de limite x.

Remarque : le lecteur vérifiera aisément qu'une base au sens de Hilbert n'est pas une base au sens classique, cf. par exemple les espaces L^2.

3.3. Application linéaires.—

Définition 3.17. — *Une application linéaire* ou *un morphisme* f d'un espace vectoriel E dans un espace F est une application telle que pour tous $\lambda \in \mathbb{K}$ et $x, y \in E$ on a $f(x + \lambda y) = f(x) + \lambda f(y)$.

Remarque : une application linéaire de E dans E est appelée un endomorphisme. Dans le cas où $F = \mathbb{K}$, on parle de *forme linéaire*.

Remarque : pour toute application linéaire $f : E \to F$ vérifie $f(0) = 0$ et

$$f(\sum_{i=1}^{n} \lambda_i e_i) = \sum_{i=1}^{n} \lambda_i f(e_i).$$

Notation 3.18. — *On note $\mathcal{L}(E, F)$ (resp. $\mathcal{L}(E) = \mathcal{L}(E, E)$), l'ensemble des morphismes de E dans F (resp. des endomorphismes de E) ; c'est un espace vectoriel de dimension* $\dim E . \dim F$.

En ce qui concerne l'existence des applications linéaires, on a le résultat suivant.

Proposition 3.19. — *Soit $(e_i)_{1 \leq i \leq n}$ une base de E. Pour n'importe quel ensemble de n vecteurs $\{f_1, \cdots, f_n\}$ de F, il existe une unique application linéaire telle que pour tout $i = 1, \cdots, n$, on ait $f(e_i) = f_i$.*

Remarque : ainsi deux applications linéaires sont égales si et seulement si elles coincident sur une base.

Définition 3.20. — Pour $f \in \mathcal{L}(E, F)$, on note $\operatorname{Ker} f$ l'ensemble des $e \in E$ tels que $f(e) = 0$; c'est un sous-espace vectoriel de E que l'on appelle *le noyau* de f.

Remarque : l'image de f est aussi un sous-espace de F que l'on note $\operatorname{Im} f$. Plus généralement l'image directe ou réciproque d'un sous-espace est un sous-espace vectoriel.

Proposition 3.21. — *Une application linéaire f est injective si et seulement si* $\operatorname{Ker} f = \{0\}$.

Remarque : f es surjective si et seulement si l'image d'une base de E est une famille génératrice de F. Ainsi f est bijective, et on dit que f est *un isomorphisme*, si l'image d'une base est une base : c'est alors vrai pour toute base.
Remarque : une application linéaire $f : E \to F$ où $\dim E = \dim F$ est injective si et seulement si elle est surjective.

Notation 3.22. — *On note $GL(E)$ l'ensemble des isomorphismes de E, on dit aussi* automorphisme. *C'est un groupe pour la composition.*

Remarque : pour $E = \mathbb{K}^n$ les vecteurs $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ définissent une base dite *canonique*. Tout espace vectoriel muni d'une base $(e_i)_{1 \leq i \leq n}$ de cardinal n est isomorphe à $\mathbb{K}^n$ où $f : \mathbb{K}^n \to E$ est défini par $f(x_1, \cdots, x_n) = \sum_{i=1}^{n} x_i e_i$. En particulier deux espaces vectoriels de même dimension sont toujours isomorphes.

Théorème 3.23. — *Soit $f \in \mathcal{L}(E, F)$ alors*

$$\dim E = \dim \operatorname{Ker} f + \dim \operatorname{Im}(f).$$

Définition 3.24. — La dimension de $\operatorname{Im} f$ s'appelle *le rang* de f ; on le note $\operatorname{rg} f$.

3.4. Matrices. —

Définition 3.25. — *Une matrice à coefficients dans* $\mathbb{K}$ *de taille* $m \times n$ est un tableau $(a_{i,j})_{\substack{1\leq i\leq m\\ 1\leq i\leq n}}$ de scalaires $a_{i,j} \in \mathbb{K}$ placé sur la i-ème ligne et la j-ème colonne. On note $\mathbb{M}_{m,n}(\mathbb{K})$ l'ensemble de ces matrices que l'on muni d'une structure d'espace vectoriel en l'identifiant avec $\mathbb{K}^{nm}$, i.e. coefficient par coefficient.

Remarque : une matrice ligne (resp. colonne) correspond au cas où $n = 1$ (resp. $m = 1$) ; on dit aussi vecteur ligne (resp. colonne). Les lignes (resp. les colonnes) d'une matrice sont appelées ses vecteurs lignes (resp. colonnes).
Remarque : les matrices $E_{i,j}$ dont les coefficients sont tous nuls sauf celui d'indice (i, j) égal à 1, forment une base de $\mathbb{M}_{m,n}(\mathbb{K})$.
Remarque : la matrice $(b_{i,j} = a_{j,i})_{i,j} \in \mathbb{M}_{n,m}(\mathbb{K})$ s'appelle *la matrice transposée*, on la note $B = {}^tA$ si $A = (a_{i,j})_{i,j}$.
Remarque : dans le cas où $m = n$, on parle de matrices carrées et on note $\mathbb{M}_n(\mathbb{K})$ pour $\mathbb{M}_{n,n}(\mathbb{K})$. Les éléments $a_{i,i}$ de $A = (a_{i,j})_{i,j}$ sont dits *diagonaux*. Ainsi une matrice est dite :

- *diagonale* si tous ses coefficients diagonaux sont nuls ; on parle aussi de matrice *anti-diagonale* si $a_{i,j} = 0$ sauf pour $i + j = n + 1$.
- *triangulaire* supérieure (resp. inférieure) si tous les $a_{i,j}$ sont nuls pour $i > j$ (resp. $j > i$).
- *tridiagonale* si $a_{i,j} = 0$ pour tout $|j - i| > 1$.

Les matrices ne sont pas de simples tableaux de chiffres mais doivent leur introduction en ce qu'ils permettent :

- d'étudier les systèmes linéaires ;
- de manipuler les endomorphismes des espaces vectoriels.

Ainsi pour $f : E \to F$ un endomorphisme entre deux espaces vectoriels munis des bases respectives $(e_i)_{1\leq i\leq n}$ et $(f_j) =_{1\leq j\leq m}$, on lui associe la matrice $A(f) = (a_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ telle que pour tout $1 \leq i \leq n$ on a

$$f(e_i) = \sum_{j=1}^{m} a_{i,j} f_j.$$

Autrement dit les vecteurs colonnes de A sont les $f(e_i)$ exprimés dans la base $(f_j)_j$.
Remarque : d'après ce qui précède, f est déterminé par sa matrice $A(f)$ de sorte que l'on doit pouvoir exprimer l'image $f(x)$ de tout vecteur $x = \sum_{i=1}^{n} x_i e_i$.

Définition 3.26. — Pour toute matrice $A \in \mathbb{M}_{m,n}(\mathbb{K})$ et tout vecteur colonne $X \in \mathbb{M}_{n,1}(\mathbb{K})$ on définit le vecteur colonne $Y = AX \in \mathbb{M}_{m,1}(\mathbb{K})$ par la formule :

$$y_j = \sum_{k=1}^{n} a_{j,k} x_k.$$

Pour une matrice $B \in \mathbb{M}_{n,r}$ dont on note $C_1, \cdots, C_r$ les vecteurs colonnes, on définit la matrice $M = AB \in \mathbb{M}_{m,r}(\mathbb{K})$ dont les vecteurs colonnes sont les AC_i pour $i = 1, \cdots, r$.

Proposition 3.27. — *Soit* $f : E \to F$ *et* $A(f)$ *sa matrice relativement à des bases* $(e_i)_{1\ \leq i\leq n}$ *et* $(f_j)_{1\leq j\leq m}$ *de respectivement* E *et* F. *Pour tout* $x = \sum_{i=1}^{n} x_i e_i$, *on note* X *le vecteur colonne* $(x_{i,1})_{1\leq i\leq n}$. *Alors les coordonnées de* $f(x)$ *dans la base* $(f_j)_{1\leq j\leq m}$ *sont les coordonnées* $(y_{j,1})_{1\leq j\leq m}$ *du vecteur colonne* $A(f)X$, *i.e.* $f(x) = \sum_{j=1}^{m} y_j f_j$.

Corollaire 3.28. — *Pour tout $f : E \to F$ et $g : F \to G$ des endomophismes ; on suppose E, F, G munis de base $(e_i)_{1\leq i\leq n}$, $(f_j)_{1\leq j\leq m}$ et $(g_k)_{1\leq k\leq r}$. On note $A(f), A(g)$ et $A(g\circ f)$ les matrices associées à f, g et $g\circ f$ relativement à ces bases. On a alors*

$$A(g\circ f) = A(g)A(f).$$

En particulier $\mathcal{L}(E)$ étant une algèbre on en déduit le corollaire suivant.

Corollaire 3.29. — *La multiplication des matrices définie plus haut, munit $\mathbb{M}_n(\mathbb{K})$ d'une structure d'algèbre.*

Définition 3.30. — Les matrices de $\mathbb{M}_n(\mathbb{K})$ qui s'identifient aux automorphismes de E sont dites *inversibles* ; l'ensemble de ces matrices inversibles est noté $GL_n(\mathbb{K})$.

Remarque : ainsi une matrice est inversible si et seulement si ses vecteurs colonnes forment une base.

Définition 3.31. — Étant donné un espace vectoriel E muni de deux bases $(e_i)_{1\leq i\leq n}$ et $(e'_i)_{1\leq i\leq n}$, on appelle matrice de passage de $(e_i)_i$ à $(e'_i)_i$ et on la note $P_{e_i\leftarrow e'_i}$, la matrice de $\mathbb{M}_n(\mathbb{K})$ dont la j-ème colonne est donnée par les coordonnées de e'_j dans la base $(e_i)_i$, i.e. $e'_j = \sum_{i=1}^n p_{i,j}e_i$.

Remarque : la matrice $P_{e_i\leftarrow e'_i}$ peut aussi se voir comme la matrice de l'application de l'identité de $E \to E$ où l'espace de départ est muni de la base $(e_i)_i$ et l'espace d'arrivée de la base $(e'_i)_i$. On en déduit alors que :

- $P_{e_i\leftarrow e'_i}$ est inversible, d'inverse $P_{e'_i\leftarrow e_i}$;
- si X' est le vecteur colonne des coordonnées d'un vecteur e de E dans la base $(e'_i)_i$, alors $X = P_{e_i\leftarrow e'_i}X'$ est celui de e dans la base $(e_i)_i$;
- si $A(f)$ est la matrice de $f : E \to F$ muni des bases $(e_i)_i$ et $(f_j)_j$ de respectivement E et F alors, pour des bases $(e'_i)_i$ et $(f'_j)_j$, la matrice $A'(f)$ relativement à ces bases est $P^{-1}_{e_i\leftarrow e'_i}A(f)P_{f_j\leftarrow f'_j}$. Dans le cas particulier où $E = F$ et où $A(f)$ et $A'(f)$ représentent la matrice de f dans respectivement les bases $(e_i)_i$ et $(e'_i)_i$ alors $A'(f) = P^{-1}_{e_i\leftarrow e'_i}A(f)P_{e_i\leftarrow e'_i}$.

Exemples : étant donnée une matrice $A \in \mathbb{M}_{m,n}(\mathbb{K})$, la multiplication à gauche (resp. à droite) par la matrice

- $T_{i,j}(\lambda)$ dont les coefficients diagonaux sont égaux à 1, tous les autres étant nuls sauf $t_{i,j} = \lambda$, correspond à modifier les lignes (resp. les colonnes) de A selon la règle $L_i \to L_i + \lambda L_j$ (resp. $C_i \to C_i + \lambda C_j$) ;
- $D_i(\lambda)$ matrice diagonale dont les coefficients diagonaux sont égaux à 1 sauf $d_{i,i} = \lambda$ correspond à modifier les lignes (resp. les colonnes) de A selon la règle $L_i \to \lambda L_i$ (resp. $C_i \to \lambda C_i$) ;
- $P_{i,j} = I - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, correspond à modifier les lignes (resp. les colonnes) de A selon la règle $L_i \leftrightarrow L_j$ (resp. $C_i \leftrightarrow C_j$).

Remarque : pour $i \neq j$, les matrices $T_{i,j}(\lambda)$ (resp. $D_i(\lambda)$) sont des matrices dites de transvections (resp. de dilatations) élémentaires relativement à la base canonique. Les matrices $P_{i,j}$ sont des cas particuliers des matrices de permutation. Ces trois types de matrices permettent d'effecteur les opérations élémentaires sur les lignes et les colonnes d'une matrice. Nous reviendrons sur ce point lors de l'étude des systèmes linéaires.

3.5. Réduction des endomorphismes. — Comme on l'a vu dans le paragraphe précédent, à chaque endomorphisme f, on associe des matrices qui dépendent du choix des bases. On cherche alors à trouver des bases pour que la matrice soit la plus simple possible.

Définition 3.32. — Deux matrices $A, A' \in \mathbb{M}_{m,n}(\mathbb{K})$ (resp. de $\mathbb{M}_n(\mathbb{K})$) sont dites *équivalentes* (resp. *semblables*) s'il existe deux matrices $P \in GL_m(\mathbb{K})$ et $Q \in GL_n(\mathbb{K})$ (resp. $P \in GL_n(\mathbb{K})$) telles que $A' = PAQ$ (resp. $A' = P^{-1}AP$).

Remarque : A et A' sont équivalentes (resp. semblables) si elles représentent le même morphisme $f : E \to F$ (resp. $f : E \to E$) relativement à des bases différentes au départ et à l'arrivée (resp. des bases différentes mais les mêmes au départ et à l'arrivée).

Proposition 3.33. — *Toute matrice $A \in \mathbb{M}_{m,n}(\mathbb{K})$ est équivalente à une matrice de la forme*

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & \ddots & 0 & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & 0 \end{pmatrix},$$

où le nombre de 1 *est égal au rang de f.*

Remarque : ainsi les classes d'équivalence dans $\mathcal{L}(E, F)$ sont données par le rang. En ce qui concerne les classes de similitude, la théorie bien que complète est plus complexe.

Définition 3.34. — Un vecteur $v \in E$ est dit *propre* par un endomorphisme f s'il est non nul et s'il existe un scalaire $\lambda \in \mathbb{K}$ tel que $f(v) = \lambda v$; le scalaire λ est alors appelé *une valeur propre.*

Remarque : un vecteur propre définie une droite stable par f ; plus généralement un sous-espace F de E est dit *stable* par f si $f(F) \subset F$. Si on prend une base de F que l'on complète par en une base de E, la matrice de f dans cette base sera triangulaire par blocs, i.e. de la forme $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ avec $A \in \mathbb{M}_{n_1}(K)$ et $B \in \mathbb{M}_{n_2}(K)$ avec $n_1 + n_2 = n$.
Exemples : le noyau $\operatorname{Ker} f$ et l'image $\operatorname{Im} f$ sont des sous-espaces stables par f.

Définition 3.35. — Un endomorphisme est dit *trigonalisable* s'il existe une base dans laquelle sa matrice est triangulaire supérieure.

La théorie de la réduction d'un endomorphisme est totalement contrôlée par une série de polynôme qu'on lui associe, appelés *ses invariants de similitude.* Le plus connu d'entre eux, le polynôme caractéristique se calcule au moyen d'un déterminant.

Proposition 3.36. — *Soit E un espace vectoriel muni d'une base $(e_i)_{1 \leq i \leq n}$. Il existe alors une unique application* $\det_{(e_i)_i} : E^n \to \mathbb{K}$ *qui soit* multilinéaire alternée *et telle que* $\det_{(e_i)_i}(e_1, \cdots, e_n) = 1$.

Remarque : pour $E = \mathbb{K}^n$ muni de la base canonique et $\mathbb{M}_n(\mathbb{K})$ identifié via ses vecteurs colonnes à E^n, l'application de la proposition précédente définie $\det : \mathbb{M}_n(\mathbb{K}) \to \mathbb{K}$ et s'appelle *le déterminant.*
Remarque : par opération élémentaires sur les vecteurs colonnes d'une matrice, on montre que $\det A \neq 0$ si et seulement si $A \in GL_n(\mathbb{K})$ ainsi que le corollaire suivant.

Corollaire 3.37. — *Pour $A, B \in \mathbb{M}_n(\mathbb{K})$ on a $\det(AB) = \det A . \det B$.*

Définition 3.38. — *Le polynôme caractéristique* d'un endomorphisme $f \in \mathcal{L}(E)$ est le déterminant $\chi_A(X) := \det(A(f) - XI_n) \in \mathbb{K}[X]$ où $A(f)$ est la matrice de f dans une base de E quelconque.

Remarque : le fait que χ_A soit indépendant de la base provient du fait que $\det(P^{-1}AP) = \det A$ d'après le corollaire précédent.

Théorème 3.39. — *Un endomorphisme f est triangularisable si et seulement si χ_f est scindé sur $\mathbb{K}$.*

Remarque : ainsi si K est algébriquement clos tous les endomorphismes sont trigonalisables.
Exercice : montrer, par des opérations élémentaires sur les lignes et les colonnes, que pour tout corps $\mathbb{K}$, toute matrice est semblable à une matrice de Hessenberg, c'est à dire de la forme

$$\begin{pmatrix} * & * & \cdots & \cdots & * \\ * & * & \ddots & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & * & * \end{pmatrix}$$

.

Le premier des invariants de similitude est donné par la définition suivante où l'on rappelle qu'étant donné un endomorphisme f et un polynôme $P(X) = \sum_i a_i X^i \in \mathbb{K}[X]$, $P(f)$ désigne l'endomorphisme $\sum_i a_i f^i$ où f^i désigne $f \circ \cdots \circ f$.

Définition 3.40. — Pour $f \in \mathcal{L}(E)$, l'ensemble I_f des polynôme $P \in \mathbb{K}[X]$ tels que $P(f)$ est l'endomorphisme nul, est un idéal de $\mathbb{K}[X]$; cet anneau étant principal, il existe un unique polynôme unitaire μ_f, appelé *polynôme minimal* de f, tel que $I_f =< \mu_f >$.

Remarque : comme E est de dimension finie, la famille $\mathrm{Id}, f, f^2, \cdots, f^{n^2+1}$ est liée de sorte que I_f n'est pas l'idéal nul et donc μ_f n'est pas le polynôme nul.

Théorème 3.41. — ***(de Cayley-Hamilton)***
Le polynôme caractéristique χ_f appartient à I_f, i.e. $\chi_f(f)$ est l'endomorphisme nul.

Revenons à présent à la problématique du début de ce paragraphe. Une fois un sous-espace stable F trouvé, on aimerait lui trouver un supplémentaire stable G de sorte que dans une base adaptée à la décomposition $E = F \oplus G$, la matrice de f soit diagonale par blocs, i.e. de la forme $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ avec $A \in \mathbb{M}_{n_1}(K)$ et $B \in \mathbb{M}_{n_2}(K)$ avec $n_1 + n_2 = n$.

Définition 3.42. — Un endomorphisme est dit *indécomposable* si on ne peut pas décomposer l'espace en une somme directe de deux sous-espaces stables stricts. Il est dit *semi-simple* si tout sous-espace stable admet un supplémentaire stable.

Proposition 3.43. — *Un endomorphisme f est indécomposable si et seulement si son polynôme caractéristique est la puissance d'un irréductible. Il est semi-simple si et seulement si son polynôme minimal est premier avec sa dérivée.*

Remarque : sur un corps algébriquement clos, semi-simple est équivalent à la notion plus classique d'endomorphisme diagonalisable au sens de la définition suivante.

Définition 3.44. — Un endomorphisme est dit *diagonalisable* s'il existe une base de vecteurs propres, i.e. s'il existe une base dans laquelle sa matrice est diagonale.

Remarque : sur $\mathbb{R}$ un endomorphisme semi-simple est semblable à une matrice diagonale par blocs dont les blocs sont soient de dimension 1 soit de dimension 2 de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.
Remarque : en ce qui concerne la définition des autres invariants de similitude, nous renvoyons le lecteur au cours d'algèbre du premier semestre.

Théorème 3.45. — *L'endomorphisme f est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples.*

Remarque : par exemple si le polynôme caractéristique est scindé à racines simples alors μ_f aussi ; plus généralement si P est un polynôme annulateur de f scindé à racines simples alors μ_f le sera aussi, puis que μ_f divise tout polynôme annulateur.

Définition 3.46. — Le sous-espace propre (resp. caractéristique) associée à une valeur propre λ est $\mathrm{Ker}(f - \lambda \mathrm{Id})$ (resp. $\mathrm{Ker}(f - \lambda \mathrm{Id})^n$ où n est la dimension de E, ou plus simplement la multiplicité de λ dans le polynôme minimal μ_f).

Remarque : la dimension du sous-espace caractéristique est égale à la multiplicité de λ dans le polynôme caractéristique.

Lemme 3.47. — ***dit des noyaux***
Si $P = P_1 P_2$ est un polynôme annulateur de f avec $P_1 \wedge P_2 = 1$ alors $E = \mathrm{Ker}\, P_1(f) \oplus \mathrm{Ker}\, P_2(f)$.

Remarque : on peut même montrer que les projecteurs sur chacun de ces sous-espaces stables parallèlement à l'autre, est un polynôme en f.

3.6. Rappels sur la dualité. —

Définition 3.48. — Étant donné un espace vectoriel E, l'ensemble des formes linéaires sur E est un espace vectoriel noté E^* et dit *le dual* de E.

Remarque : une base $(e_i)_{1 \leq i \leq n}$ de E étant fixée, l'application linéaire $e_i^* \in E^*$ définie par $e_i^*(e_j) = \delta_{i,j}$ est une base de E^* dite la base duale de $(e_i)_i$. On se méfiera de la notation car e_i^* dépend de toute la base $(e_i)_i$ et pas seulement du seul vecteur e_i.

Proposition 3.49. — *Étant donné un sous-espace $F \subset E$, le sous-ensemble $F^\perp \subset E^*$ des formes linéaires s'annulant sur F est un sous-espace de dimension $\dim E - \dim F$, i.e. la dimension de $F^\perp$ est égale à la codimension de F.*

Définition 3.50. — Soit $f \in \mathcal{L}(E,F)$, on lui associe alors son *application adjointe* notée $f^* \in \mathcal{L}(F^*,E^*)$ définie par la formule

$$y^* \in F_* \mapsto f^*(y^*) = y^* \circ f$$

au sens où $f^*(y^*)$ est la forme linéaire sur E définie par $x \mapsto y^*(f(x))$.

Proposition 3.51. — *Si E,F sont munies de bases respectives $(e_i)_i$ et $(f_j)_j$ alors la matrice de f^* dans les bases duales associées de F^* et E^* est la transposée de la matrice de f dans les bases $(e_i)_i$ et $(f_j)_j$.*

Remarque : on notera en particulier que f et f^* ont le même rang.

Proposition 3.52. — *Soit E un espace vectoriel de dimension finie ; alors le bidual $(E^*)^*$ s'identifie canoniquement à E.*

Remarque : l'application $E \to (E^*)^*$ est donnée par $x \mapsto (f \mapsto f(x))$.

3.7. Systèmes linéaires.—

Définition 3.53. — *Une équation linéaire* en les variables $x_1, \cdots, x_n$ est une expression de la forme

$$L(x_1, \cdots, x_n) = b \text{ où } L(x_1, \cdots, x_n) = a_1x_1 + \cdots + a_nx_n$$

dont on cherche les solutions dans $\mathbb{K}^n$. On dit que l'équation est *homogène* lorsque $b = 0$.

Remarque : on peut et on doit interpréter $L(x_1, \cdots, x_n)$ comme une forme linéaire sur $\mathbb{K}^n$ écrite dans la base canonique.

Définition 3.54. — *Un système linéaire* de m équations à n variables est une collection de m équations linéaires

$$(S) = \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n = b_2 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_n \end{cases}$$

que l'on cherche à résoudre simultanément. Il est dit *incompatible* s'il ne possède pas de solutions, *compatible* sinon.

Remarque : comme suggéré par les notations, on introduit la matrice $A_S = (a_{i,j}) \in \mathbb{M}_{m,n}(\mathbb{K})$ et on écrit le système précédent sous la forme $A_SX = B$ où X (resp. B) est le vecteur colonne de coordonnées les x_i (resp. les b_i).

Définition 3.55. — Deux systèmes linéaires (S) et (S') sont dit *équivalents* s'ils ont le même ensemble de solutions.

Proposition 3.56. — *Deux systèmes linéaires (S) et (S') sont équivalents si et seulement s'il existe une matrice inversible $P \in GL_m(\mathbb{K})$ telle que $A_S = PA_{S'}$ et $B = PB'$.*

Remarque : en utilisant que $GL_n(\mathbb{K})$ est engendré par les matrices de transvections et de dilatations (en général, par commodité, on rajoute aussi les matrices de permutation $P_{i,j}$), on doit pouvoir manipuler le système (S) pour arriver au système (S') qui lui est équivalent, encore faut-il que ce processus soit constructif, ce qui est assuré par l'algorithme de Gauss.

Définition 3.57. — Soit (S) un système linéaire non nécessairement homogène que l'on écrit sous forme matricielle $A_S X = B$. On introduit alors la matrice $\tilde{A}_S$ en rajoutant la colonne B à la matrice A_S.

Définition 3.58. — Une matrice $M \in \mathbb{M}_{m,n}(\mathbb{K})$ est dite *échelonnée* si en dessous du premier élément non nul de chaque ligne, il n'y a que des zéros. Elle est dite en outre *échelonnée réduite* si tout premier élément non nul de chaque ligne, appelé *pivot*, est égal à 1, et que chaque pivot est le seul élément non nul de sa colonne.

Proposition 3.59. — *Pour toute matrice $M \in \mathbb{M}_{m,n}(\mathbb{K})$, il existe une unique matrice $P \in GL_m(\mathbb{K})$ telle que PM est échelonnée réduite.*

Remarque : la mise en place pratique de ce résultat est ce que l'on appelle, **l'algorithme de Gauss**.

Ainsi étant donné un système linéaire (S) de matrice augmentée $\tilde{A}_S$, on lui applique l'algorithme de Gauss pour obtenir l'échelonnée réduite associée, par exemple de la forme

$$\begin{pmatrix} 0 & \cdots & \mathbf{1} & \bullet & \cdots & \bullet & \cdots & \bullet & \bullet & \bullet & \bullet & \bullet \\ 0 & \cdots & 0 & 0 & \cdots & \mathbf{1} & \bullet & 0 & 0 & \bullet & 0 & \bullet \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \mathbf{1} & 0 & \bullet & 0 & \bullet \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \mathbf{1} & \bullet & 0 & \bullet \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \bullet \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \alpha \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- Si la dernière colonne contient un pivot, alors le système est incompatible, ce qui dans l'exemple précédent correspond au cas $\alpha \neq 0$.
- Sinon, les positions des pivots fournissent les indices des variables dites *principales* alors que les autres sont dites *secondaires*. L'ensemble des solutions est alors un sous-espace affine de dimension le nombre de variables secondaires ; autrement dit quelles que soient les valeurs prises par ces variables secondaires, on obtient une unique solution pour les variables principales que l'on obtient en résolvant ce système du bas vers le haut.

Définition 3.60. — Le système (S) est dit *de Cramer* s'il possède une unique solution.

Remarque : autrement dit, (S) est de Cramer s'il est compatible sans variable secondaire, ce qui permet de prouver la proposition suivante.

Proposition 3.61. — *(S) est de Cramer si et seulement si A_S est une matrice inversible, ce qui impose en particulier que $m = n$.*

Remarque : on utilise des systèmes linéaires et leur résolution via l'algorithme de Gauss, par exemple pour trouver l'inverse d'une matrice, pour donner des équations linéaires d'un sous-espace dont on connait une famille génératrice...

4. Algèbre bilinéaire

4.1. Formes sesquilinéaires : généralités. — Rappelons qu'étant donné un automorphisme σ du corps $\mathbb{K}$, par exemple la conjugaison complexe de $\mathbb{C}$, *une application semi-linéaire* est une application θ telle que pour tout $x, y \in E$ et $\lambda \in \mathbb{K}$ on a

$$\theta(x + \lambda y) = \theta(x) + \lambda^\sigma \theta(y)$$

où par convention on note λ^σ pour $\sigma(\lambda)$.

Définition 4.1. — On appelle *forme σ-sesquilinéaire* toute application $\phi : E \times E \to \mathbb{K}$ vérifiant les conditions suivantes :
— pour tout $x \in E$, l'application $\phi_x : y \in E \mapsto \phi(x, y)$ est linéaire ;
— pour tout $y \in E$ l'application $\phi_y : x \in E \mapsto \phi(x, y)$ est σ-linéaire.

Remarque : les notations ϕ_x et ϕ_y ne sont pas exemplaires, on veillera à ne pas se mélanger.

Proposition 4.2. — *Soit E un espace vectoriel muni d'une base $(e_i)_{1\leq i\leq n}$. On note $A_\phi = \big(\phi(e_i, e_j)\big) \in \mathbb{M}_n(\mathbb{K})$ la matrice associée à la forme sesquilinéaire ϕ, relativement à la base $(e_i)_i$. Pour tous vecteurs $x, y \in E$ de vecteur colonne coordonnées X et Y, on a alors*

$$\phi(x, y) = {}^tX^\sigma A_\phi Y.$$

Remarque : si $P_{(e_i)\leftarrow(e'_i)}$ est la matrice de changement de base de $(e_i)_i$ à $(e'_i)_i$ alors la matrice A'_ϕ relativement à cette nouvelle base est telle que

$$A'_\phi = {}^tP^\sigma_{(e_i)\leftarrow(e'_i)_i} A_\phi P_{(e_i)\leftarrow(e'_i)_i}.$$

En particulier le déterminant de A_ϕ, qu'on appelle le discriminant de ϕ, n'est défini que comme élément de $\mathbb{K}/N(\mathbb{K})$ où $N(\mathbb{K}) = \{\lambda\lambda^\sigma,\ \lambda \in \mathbb{K}\}$.

Définition 4.3. — Pour M une partie de E, on note

$$M^\perp = \{y \in E,\ \phi(M, y) = 0\}, \qquad {}^\perp M = \{x \in E,\ \phi(x, M) = 0\}.$$

On dit que $M^\perp$ (resp. ${}^\perp M$) est l'orthogonal à droite (resp. à gauche) de M.

Remarque : $M^\perp$ et ${}^\perp M$ sont clairement des sous-espaces de E. En outre $E^\perp = \operatorname{Ker}\phi_y$ et ${}^\perp E = \operatorname{Ker}\phi_x$.

Définition 4.4. — On dit que ϕ est *non dégénérée* si $E^\perp = \{0\}$ (resp. ${}^\perp E = \{0\}$. Le rang de A_ϕ est appelé *le rang* de ϕ, il est égal à la codimension de $E^\perp$ et ${}^\perp E$.

Remarque : pour M un sous-espace de E on a

$$\dim M + \dim M^\perp = \dim E + \dim(M \cap {}^\perp E).$$

On a aussi que ${}^\perp(M^\perp) = M + {}^\perp E$ et donc pour ϕ non dégénérée on retrouve la propriété habituelle ${}^\perp(M^\perp) = M$.

Définition 4.5. — Une forme σ-sesquilinéaire est dite *réflexive* si pour tout $x, y \in E$, $\phi(x, y) = 0$ équivaut à $\phi(y, x) = 0$.. Elle est dite hermitienne (resp. antihermitienne) si $\phi(x, y) = \epsilon\Big(\phi(y, x)\Big)^\sigma$ avec $\epsilon = 1$ (resp. $\epsilon = -1$).

Remarque : pour une forme hermitienne ou antihermitienne, σ est nécessairement une involution ; dans le cas antihermitien en caractéristique différente de 2, on a même $\sigma = \mathrm{Id}$ et on dit simplement que ϕ est *anti-symétrique*.

Proposition 4.6. — *On suppose que ϕ est une forme hermitienne ou antihermitienne non dégénérée. Pour tout $u \in \mathcal{L}(E)$, il existe un unique endomorphisme $u^* \in \mathcal{L}(E)$, appelé* adjoint *de u, tel que pour tous $x, y \in E$:*

$$\phi(u(x), y) = \phi(x, u(y)).$$

En outre on a aussi $\phi(x, u(y)) = \phi(u^*(x), y)$.

Remarque : la donnée d'une forme σ-sesquilinéaire non dégénérée, induit un isomorphisme canonique entre E et E^* de sorte que l'adjoint habituel d'un endomorphisme vu dans $\mathcal{L}(E^*)$ se voit désormais comme un endomorphisme de E.

On suppose à présent que ϕ est une forme hermitienne ou antihermitienne, auquel cas la caractéristique est en outre supposée différente de 2.

Définitions 4.7. — — *Un vecteur x de E est dit* isotrope *si $\phi(x,x)=0$.*
— *Un sous-espace F de E est dit* isotrope *si $F\cap F^\perp \neq \{0\}$.*
— *Un sous-espace F de E est dit* totalement isotrope *et on écrit* séti*, si $F\subset F^\perp$.*
— *Un séti est dit maximal et on écrit* sétim*, si pour tout séti G contenant F alors $G=F$.*

Remarque : comme on est en dimension finie, tout séti est contenu dans un sétim.
Remarque : si F est non isotrope alors $E=F\oplus F^\perp$; dans le cas où ϕ est non dégénéré c'est même une équivalence.

Proposition 4.8. — *Si ϕ est non dégénéré il existe alors une décomposition dite de Witt de l'espace $E=F\oplus F'\oplus G$ avec F,F' des sétim et G un sous- espace non isotrope telle que la matrice de ϕ dans une base adaptée soit de la forme*

$$\begin{pmatrix} 0 & I_r & 0 \\ \epsilon I_r & 0 & 0 \\ 0 & 0 & B \end{pmatrix}.$$

Remarque : sous-entendu dans l'énoncé précédent est que toute les sétim ont la même dimension appelée *l'indice* de ϕ.

Définition 4.9. — Un automorphisme u de E est dit *unitaire* si pour tous $x,y\in E$:

$$\phi(u(x),u(y))=\phi(x,y).$$

L'ensemble des automorphismes unitaires est un sous-groupe de $GL(E)$ noté U_ϕ et appelé *le groupe unitaire* de ϕ. Le noyau du morphisme déterminant d'image $\mathbb{H}=\{\lambda\in\mathbb{K}:\ \lambda\lambda^\sigma=1\}$, est noté SU_ϕ et s'appelle *le groupe spécial unitaire* de ϕ.

Remarque : u est unitaire si et seulement si $u^{-1}=u^*$. Matriciellement la matrice U de u est unitaire si et seulement si ${}^tU^\sigma A_\phi U=A_\phi$. Dans le cas où $A_\phi=I_n$, on retrouve la condition usuelle ${}^tU^\sigma U=I_n$.

Définition 4.10. — Une similitude de rapport $\lambda\in\mathbb{K}^\times$ est un automorphisme tel que pour tous $x,y\in E$:

$$\phi\big(u(x),u(y)\big)=\lambda\phi(x,y).$$

Le groupe des similitudes se note GU_ϕ.

Remarque : une définition classique d'une similitude consiste à demander :

$$\phi(x,y)=0\Rightarrow\phi\big(u(x),u(y)\big)=0.$$

4.2. Le cas réel. — Dans ce cas $\sigma = \mathrm{Id}$ et on parle alors de forme bilinéaire symétrique et antisymétrique.

Définition 4.11. — Une forme bilinéaire symétrique est dite :
- positive (resp. négative) si pour tout $x \in E$, on a $\phi(x,x) \geq 0$ (resp. $\phi(x,x) \leq 0$) ;
- définie positive (resp. définie négative) si elle est positive (resp. négative) et que $\phi(x,x) = 0$ si et seulement si x est le vecteur nul.

Théorème 4.12. — ***(Loi d'inertie de Sylvester)***
Soit ϕ une forme bilinéaire symétrique.
- *Il existe alors une décomposition*

$$E = E^{\perp} \oplus E^{+} \oplus E^{-}$$

telle que la restriction de ϕ à E^{+} (resp. E^{-}) est définie positive (resp. définie négative). Une telle décomposition n'est pas unique mais les dimensions s de E^{+} et t de E^{-} sont les mêmes pour toute telle décomposition et sont respectivement égale au maximum des dimensions des sous-espaces F de E tels que la restriction de ϕ y soit définie positive (resp. négative). On dit que le couple (s,t) est la signature *de ϕ.*
- *Il existe une base $(e_i)_{1\leq i\leq n}$ de E telle que*

$$\phi(\sum_{i=1}^{n} \lambda_i e_i,\ \sum_{j=1}^{n} \mu_j e_j) = \sum_{i=1}^{s} \lambda_i \lambda_i \mu_i - \sum_{i=s+1}^{s+t} \lambda_i \mu_i.$$

- *Le rang de ϕ est égal à $s+t$ et son indice est égal à $(n - \mathrm{rg}\phi) + \min\{s,t\}$.*

Définition 4.13. — Une application $q : E \to \mathbb{R}$ est appelée *une forme quadratique* sur E si elle vérifie les conditions suivantes :
- $q(\lambda x) = \lambda^2 q(x)$ pour tout $\lambda \in \mathbb{R}$;
- l'application

$$\phi : E \times E \to \mathbb{R}, \quad (x,y) \mapsto \frac{1}{2}\Big(q(x+y) - q(x) - q(y)\Big)$$

est une forme bilinéaire (symétrique) appelée *la forme polaire de q.*

Remarque : l'application qui à une forme quadratique associe sa forme polaire est un isomorphisme linéaire entre l'espace des formes quadratiques et l'espace des formes bilinéaires symétriques. Parfois on utilise l'un ou l'autre des langages. Par exemple on dit que q est non dégénérée pour dire que sa forme polaire l'est.
Remarque : soit $(e_i)_i$ une base orthogonale pour une forme bilinéaire symétrique ϕ de rang r ; quitte à réindexer on suppose que $q(e_i) = a_i \neq 0$ pour $1 \leq i \leq r$. On note $(e_i^*)_i$ la base duale de sorte que pour $x \in E$:

$$q(x) = a_1[e_1^*(x)]^2 + \cdots + a_r[e_r^*(x)]^2.$$

Il existe un algorithme pour obtenir une décomposition $q(x) = \sum_{i=1}^{r} \lambda_i f_i(x)^2$ avec $(f_1, \cdots, f_r)$ une famille **libre** de formes linéaires ; il s'agit du procédé d'orthogonalisation de Gauss. En effet pour une telle décomposition, en complétant la famille des f_i en une base de E^*, la base duale dans $(E^*)^* \simeq E$, est une base orthogonale pour la forme polaire de q.
Remarque : on note aussi $O(q)$ le groupe O_ϕ pour ϕ la forme polaire de q. Dans notre situation, $O(q)$ s'appelle *le groupe orthogonal* de q.

Définition 4.14. — Soit F un sous-espace non isotrope de E ; l'unique involution unitaire u telle que $F = \mathrm{Im}(u + \mathrm{Id})$ s'appelle *la symétrie orthogonale par rapport au sous-espace non isotrope* F. Si F est un hyperplan, on dit que u est *une réflexion* ; si F est de codimension 2 on dit que u est *un retournement* ou *un renversement.*

Remarque : si v est un vecteur normé orthogonal à un hyperplan H non isotrope, alors la réflexion par rapport à H est l'application $x \mapsto x - 2\phi(x, v)v$.

Théorème 4.15. — ***(de Cartan-Dieudonné)***
Soit q une forme quadratique non dégénérée sur E. Tout élément de $O(q)$ est produit de p réflexions avec $p \leq \dim E$. En dimension ≥ 3, tout élément de $SO(q)$ est produit de q retournements avec $q \leq \dim E$.

Remarque : rappelons que l'espace E muni d'une forme quadratique q est dit *euclidien* si q est définie positive. En dimension 2, on a un isomorphisme de groupes $\mathbb{R}/2\pi\mathbb{Z} \to SO(2)$ qui à θ associe la matrice

$$R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

En dimension 3 toute matrice de $SO(3)$ est semblable à une matrice de la forme

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On a aussi un isomorphisme de groupes entre $SO(3)$ et le groupe des quaternions de norme 1 quotienté par $\{\pm 1\}$. Cette description est particulièrement utile quand il s'agit de composer des rotations de l'espace ; pour plus de détails on renvoie le lecteur au cours d'algèbre du premier semestre.

4.3. Le cas hermitien. — Dans ce paragraphe on considère le cas $\mathbb{K} = \mathbb{C}$ et σ égal à la conjugaison complexe. Pour $A \in GL_n(\mathbb{C})$, on note A^* pour ${}^t\overline{A}$. Notons en particulier que tout forme hermitienne ϕ vérifie $\phi(x, x) \in \mathbb{R}$. On dit alors qu'elle est *positive* (resp. négative) si $\phi(x, x) \geq 0$ (resp. ≤ 0) pour tout $x \in E$ et on dit qu'elle est en outre *définie* si $\phi(x, x) = 0 \Rightarrow x = 0$.
Remarque : si E est muni d'une forme hermitienne définie positive on dit que E est *un espace hermitien.*

Proposition 4.16. — *Si ϕ est positive alors*

$$\phi(x, y)\overline{\phi(x, y)} \leq q(x)q(y).$$

Théorème 4.17. — *Comme dans le cas réel,*
- *il existe une décomposition $E = E^\perp \oplus E^+ \oplus E^-$ telle que la restriction de ϕ à E^+ (resp. E^-) est définie positive (resp. négative). En outre la dimension s de E^+ et t de E^- sont indépendantes de cette décomposition et le couple (s, t) s'appelle* la signature *de ϕ.*
- *Il existe une base $(e_i)_{1 \leq i \leq n}$ telle que*

$$\phi\Big(\sum_{i=1}^{n} \lambda_i e_i, \sum_{j=1}^{n} \mu_j e_j\Big) = \sum_{i=1}^{s} \lambda_i \overline{\mu_i} - \sum_{i=s+1}^{s+t} \lambda_i \overline{\mu_i}.$$

- *Le rang de ϕ est $s + t$ et son indice $n - (s + t) + \min\{s, t\}$.*

On définit de même le groupe unitaire qui matriciellement s'écrit $U^*A_\phi U = A_\phi$, ce qui dans une base orthonormée pour ϕ s'écrit $U^*U = I_n$.

Définition 4.18. — Un endomorphisme u d'un espace hermitien est dit *normal* si $u \circ u^* = u^* \circ u$.

Remarque : u est normal si et seulement si $||u(x)|| = ||u^*(x)||$ pour tout $x \in E$.

Théorème 4.19. — *Un endomorphisme est normal si et seulement s'il est diagonalisable dans une base orthonormée.*

Remarque : la preuve de ce résultat repose sur l'observation suivante : pour tout sous-espace stable F de E par u, alors $F^\perp$ est stable par u. Ce résultat recouvre par ailleurs un certain nombre de résultat de diagonalisation.

Corollaire 4.20. — *Un endomorphisme d'un espace hermitien est unitaire si et seulement s'il possède une base orthonormée de vecteurs propres pour des valeurs propres de norme* 1.

Définition 4.21. — Un endomorphisme u d'un espace euclidien est *hermitien* ou *auto-adjoint* s'il vérifie $u = u^*$.

Corollaire 4.22. — *Un endomorphisme d'un espace hermitien est hermitien si et seulement s'il est diagonalisable dans une base orthonormée pour des valeurs propres réelles.*

Corollaire 4.23. — *Une endomorphisme symétrique d'un espace euclidien est diagonalisable en base orthonormée.*

Corollaire 4.24. — *Soit A une matrice hermitienne définie positive et B une matrice hermitienne, toutes deux de taille n. Il existe alors $P \in GL_n(\mathbb{C})$ telle que*

$$P^*AP = I_n \text{ et } P^*BP \text{ est diagonale.}$$

Théorème 4.25. — ***(Décomposition polaire)***
Soit f un endomorphisme d'un espace hermitien. Il existe alors un unique couple (u, h) avec u unitaire et h hermitien tel que $f = u \circ h$.

Remarque : on obtient u en prenant la racine carrée positive de $f^* \circ f$. Cette décomposition est une généralisation de l'écriture d'un nombre complexe z sous la forme $\rho e^{i\theta}$. On peut aussi écrire $f = h' \circ u'$ avec cette fois-ci u' qui est la racine carrée positive de $f \circ f^*$.
Remarque : dans le cas réel, on écrit $f = o \circ s$ avec o orthogonale et s symétrique.

Terminons ces rappels algébriques par un exemple fondamental de matrice hermitienne.

Définition 4.26. — Soit $(x_1, \cdots, x_m)$ une famille de vecteurs d'un espace hermitien E. *La matrice de Gram* définie par

$$Gram(x_1, \cdots, x_m) = \Big(\phi(x_i, x_j)\Big)_{1 \leq i,j \leq m}$$

est une matrice hermitienne dont on note $G(x_1, \cdots, x_m)$ le déterminant.

Proposition 4.27. — *Pour tout $(x_1, \cdots, x_m)$, le déterminant de Gram $G(x_1, \cdots, x_m)$ appartient aux réel positifs ; il est non nul si et seulement si la famille $(x_1, \cdots, x_m)$ est libre.*

Corollaire 4.28. — *Soient $x \in E$ et F un sous-espace de E ; si $(x_1, \cdots, x_m)$ est une base de F alors la distance $d(x, F)$ de x à F est donnée par*

$$d(x, F)^2 = \frac{G(x, x_1, \cdots, x_m)}{G(x_1, \cdots, x_m)}.$$

5. Modules

Dans la suite A désignera un anneau commutatif que l'on supposera rapidement principal. Le lecteur est vivement encouragé, dans un premier temps, à le considérer égal à $\mathbb{Z}$ puis $K[X]$ pour K un corps.

5.1. Généralités. — Dans ce paragraphe A est un anneau commutatif quelconque.

Définition 5.1. — - Un A-module est un groupe commutatif $(M, +)$ muni d'une application $A \times M \to M$, où l'on note ax l'image de (a, x), telle que :

1. $\forall a \in A$ et $x, y \in M$, $a(x + y) = ax + ay$;
2. $\forall a, b \in A$ et $x \in M$, $(a + b)x = ax + bx$;
3. $\forall a, b \in A$ et $x \in M$, $1x = 1$ et $a(bx) = (ab)x$.

- Un sous-module d'un A-module M est un sous-groupe N de M stable par l'action de A.
- Un morphisme de A-modules $M \to N$ est un morphisme des groupes additifs $(M, +) \to (N, +)$ qui est de plus A-linéaire.

Remarque : la notion de A-module est formellement identique à celle de K-espace vectoriel sauf que l'action externe est relative à un anneau A plutôt qu'à un corps K.
Exemples : les constructions habituelles sur les espaces vectoriels se généralisent au cas des A-modules (quotient, somme, intersection, A-module engendré...). On utilisera dans la suite plus spécifiquement les exemples suivants.
- Si $(G, +)$ est un groupe commutatif, il est canoniquement muni d'une structure de $\mathbb{Z}$-module, en définissant, pour $n \geq 0$, ng comme $\overbrace{g + g + \cdots + g}^{n}$, et $(-1)g$ comme $-g$.
- Si V est un K-espace vectoriel et $u \in \mathcal{L}(V)$ un endomorphisme de V, on munit V d'une structure de $K[X]$-module en posant pour tout $P \in K[X]$ et pour tout $\overrightarrow{v} \in V$, $P.\overrightarrow{v} := P(u)(\overrightarrow{v})$.
- L'anneau A est lui-même un A-module. Les sous-A-modules de A sont ses idéaux.

Définition 5.2. — Un sous-ensemble S d'un A-module M est dit

- *libre* si l'égalité $\sum_{s \in S} a_s s = 0$ où la famille $(a_s)_{s \in S}$ est supposée à support fini, implique que pour tout $s \in S$, on a $a_s = 0$.
- *générateur* si tout élément $m \in M$ peut s'écrire sous la forme $\sum_{s \in S} a_s s$ où la famille $(a_s)_{s \in S}$ est à support fini.
- *une base* si S est à la fois libre et générateur.

On dit que M est

- *libre* si M admet une base.
- *de type fini* s'il admet un sous-ensemble fini S générateur.
- *de torsion* si l'ensemble des éléments $\lambda \in A$ qui annulent M i.e. tels que $\forall m \in M$ on ait $\lambda m = 0$, est un idéal non nul de A. Cet idéal est appelé *annulateur* de M et noté $\mathrm{Ann}(M)$.

Exemple : l'annulateur de $M = A/I$ est l'idéal I.
Remarque : la donnée d'une base d'un A-module libre de type fini est équivalent à la donnée d'un isomorphisme $A^n \longrightarrow M$.

Proposition 5.3. — *Soit M un A-module libre de type fini. Alors toutes ses bases ont le même cardinal.*

Preuve : Soient $(e_1, \cdots, e_n)$ une base de M et $\mathcal{M} \in A$ un idéal maximal de sorte que le quotient $A/\mathcal{M}$ est un corps k. On note $\mathcal{M}M = \{\sum_{i=1}^n m_i e_i : \ m_i \in \mathcal{M}\}$ de sorte que $V := M/\mathcal{M}M$ est un k-espace vectoriel, i.e. un groupe muni d'une action externe de $A/\mathcal{M}$. Notons par ailleurs que $(\bar{e}_i)_{i=1,\cdots,n}$ est une base de V. C'est clairement une famille génératrice. Pour la liberté, $\sum_{i=1}^n \lambda_i \bar{e}_i = 0$ s'écrit aussi $\sum_{i=1}^n \mu_i e_i = \sum_{i=1}^n m_i e_i$ où $\bar{\mu}_i = \lambda_i$ et les $m_i \in I$. La famille $(e_i)_{i=1,\cdots,e_n}$ étant libre, on en déduit que $\mu_i = m_i$ et donc $\lambda_i = \bar{\mu}_i = 0$.

Ainsi n est la dimension de l'espace vectoriel $M/\mathcal{M}M$ et est donc le cardinal de toute base du A-module M.

Proposition 5.4. — *Un sous-module d'un module de type fini est de type fini.*

Preuve : Soit $f : A^n \twoheadrightarrow M$ définie par la donnée d'une famille génératrice de cardinal n de M. Pour un sous-module N de M, il suffit de montrer que $f^{-1}(N)$ est de type fini, i.e. on est ramené au cas où $M = A^n$. On raisonne alors par récurrence sur n : dans le cas $n = 1$, un sous-module de A est un idéal qui est donc principal et donc libre de rang 1.
Supposons alors le résultat acquis jusqu'au rang $n-1$ et traitons le cas de n. Considérons alors l'application $g : N \hookrightarrow A^n \twoheadrightarrow A$ où la deuxième flèche est donnée par la première projection $(a_1, \cdots, a_n) \mapsto a_1$. L'image de g est de la forme $a_1 A$ et notons $n_1 \in N$ un antécédent puis $N' = N \cap A^{n-1}$ où A^{n-1} est le noyau de la première projection. Notons que $n_1 A \cap N' = (0)$ puisque si $g(\lambda n_1) = 0$ alors $\lambda = 0$. En outre pour $n \in N$, on peut écrire $n = \lambda n_1 + (n - \lambda n_1)$ où $f(n) = \lambda a_1 = f(\lambda n_1)$ et donc $n - \lambda n_1 \in N'$. Autrement dit on a $N = An_1 \oplus N'$ avec $N' \subset A^{n-1}$. Par récurrence N' est de type fini et donc N aussi.

5.2. Calculs matriciels dans un anneau principal. — Rappelons que $\mathbb{M}_n(A)$ désigne l'ensemble des matrices carré de taille n à coefficients dans A.

Lemme 5.5. — *La matrice $M \in \mathbb{M}_n(A)$ est inversible si et seulement si* $\det M \in A^\times$.

Preuve : Si la matrice M est inversible, alors en appliquant le déterminant à l'égalité $M.M^{-1} = I_n$ on obtient que l'inverse de $\det M$ est $\det(M^{-1})$. Inversement, notons $\tilde{M}$ la transposée de la matrice des cofacteurs de M. De l'égalité $\tilde{M}.M = \det M$ on en déduit que si $\det M \in A^\times$ alors $(\det M)^{-1}\tilde{M}$ est l'inverse de M.

Le lemme suivant est l'ingrédient calculatoire essentiel pour les calculs matriciels de la suite.

Lemme 5.6. — *Soient $x, y \in A$ non tous deux nuls, z un pgcd de x et $ux + vy = z$ une relation de Bézout. Alors la matrice $M := \begin{pmatrix} u & v \\ -y/z & x/z \end{pmatrix}$ de déterminant* 1 *vérifie l'équation*

$$M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix}.$$

Nous utiliserons la matrice de taille (n,n) suivante :

$$L_{j,k}(x,y) = \begin{pmatrix} 1 & 0 & \dots & & & & & & \dots & 0 \\ 0 & \ddots & & & & & & & 0 & \vdots \\ & & 1 & & & & & & & \\ \vdots & 0 & \dots & u & 0 & \dots & & v & \vdots & \\ & \vdots & & & 1 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 1 & & & \\ & & & -y/z & 0 & \dots & & x/z & & \\ & & & & & & & & 1 & \\ & & & & & & & & \ddots & \\ 0 & \dots & & & & & & & & 1 \end{pmatrix}$$

u étant en (j,j), v en (j,k), $-y/z$ en (k,j) et x/z en (k,k).
Remarque : comme d'habitude, en notant l_i la ligne d'indice i d'une matrice M, la multiplication à gauche d'une matrice $M \in \mathbb{M}_{n,m}(A)$ par la matrice $L_{j,k}(x,y)$ remplace l_j et l_k par respectivement $\alpha l_j + \beta l_k$ et $\gamma l_j + \delta l_k$.

Proposition 5.7. — *Soit $M \in \mathbb{M}_{n,m}(A)$. Il existe alors une matrice $L \in SL_n(A)$ telle que LM soit triangulaire supérieure.*

Preuve : La démonstration consiste à appliquer plusieurs fois le lemme 5.6 pour faire apparaître des zéros sous la diagonale principale.
a) Soit $M = (a_{ij})$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$. Multiplions M à gauche par la matrice $L_1 = L_{1,2}(a_{1,1}, a_{2,1})$ de sorte que la première colonne de $M_1 = L_1 M$ commence par $\begin{pmatrix} d \\ 0 \end{pmatrix}$ avec $d = a_{11} \wedge a_{21}$.
b) On multiplie ensuite M_1 à gauche par une matrice $L_2 = L_{1,3}(d, a_{3,1})$ de façon à faire apparaître un zéro à la place $(3,1)$ et à remplacer d par $d_1 = a_{1,1} \wedge a_{2,1} \wedge a_{3,1}$. On continue ainsi jusqu'à ce que l'on obtienne la matrice $M_{n-1} = L_{n-1} \cdots L_1 M$ dont la première colonne est $(d_{n-1}, 0 \dots 0)$ avec d_{n-1} le pgcd des éléments de la première colonne de M.
c) On continue de même avec la seconde colonne, en commençant par multiplier à gauche par une matrice $L_{2,3}$ de façon à laisser la première ligne inchangée et à ne manipuler que les lignes $l_2, \dots, l_n$. En procédant ainsi on obtient une deuxième colonne de la forme $(a, b, 0, \cdots, 0)$. En continuant ainsi pour toutes les colonnes, on obtient une matrice triangulaire supérieure.

Définition 5.8. — Une matrice $M \in \mathbb{M}_{n,m}(A)$ est dite *réduite* si

$$M = \begin{pmatrix} a_{1,1} & 0 & \dots & & 0 \\ 0 & a_{2,2} & 0 & \dots & \vdots \\ \vdots & & \ddots & & \\ & & & a_{n,n} & \dots & 0 \end{pmatrix}$$

avec

$$a_{i,i} \mid a_{i+1,i+1}, \quad 1 \leq i \leq \inf(n,m) - 1.$$

Remarque : on a représenté une matrice M avec $n < m$. Il est à noter que les derniers $a_{i,i}$ peuvent être nuls et que tous les éléments non sur la diagonale sont nuls.

Théorème 5.9. — *Soit $M \in \mathbb{M}_{n,m}(A)$. Il existe alors $L \in SL_nA$ et $R \in SL_m(A)$ telles que $M' = LMR$ soit réduite.*

Remarque : l'énoncé analogue sur un corps K est que toute matrice $M \in \mathbb{M}_{n,m}(K)$ est équivalente à une matrice de la forme $M' = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Preuve : Nous avons vu comment en manipulant les lignes, on faisait remonter le pgcd de chaque colonne sur la première ligne. On commence donc par faire cela pour chacune des colonnes. Puis, comme on a opéré sur les lignes, on opère sur les colonnes de sorte à ramener le pgcd de la première ligne, et donc celui de tous les coefficients de la matrice, en position $(1, 1)$.

À ce stade, le coefficient $a_{1,1}$ est le pgcd de tous les $a_{i,j}$. On recommence alors à opérer sur les lignes de façon à obtenir la première colonne égale à $(a_{1,1}, 0, \cdots, 0)$: on note en particulier que la première ligne n'est pas modifiée. On opère ensuite de même sur les colonnes pour que la première ligne soit égale à $(a_{1,1}, 0, \cdots, 0)$. Comme précédemment, on ne modifie pas la première ligne de sorte qu'à ce stade la matrice est diagonale par blocs avec un premier bloc de taille 1 et le deuxième de taille $(n-1, m-1)$.

On conclut alors par récurrence.

5.3. Théorème de la base adaptée. —

Théorème 5.10. — *Soit N un sous-module d'un A-module L libre de type fini. Alors N est un sous-module libre de type fini et il existe une base, dite* adaptée, *$(f_1, \ldots, f_n)$ de L ainsi que des éléments $a_i \in A$, $1 \leq i \leq n$ tels que :*

$$\begin{cases} a_1 \mid a_2 \mid \cdots \mid a_n, \\ \text{les } (a_i f_i) \text{ tels que } a_i \neq 0 \text{ forment une base de } N. \end{cases}$$

De plus, la suite des idéaux (a_i) satisfaisant ces conditions est unique.

Preuve : D'après la proposition 5.4, N est de type fini, notons alors $(g_1, \ldots, g_m)$ une famille génératrice de N et écrivons la matrice de passage M des g_i pour $1 \leq i \leq m$ dans une base $(e_1, \cdots, e_n)$ de L. D'après 5.9, il existe $P \in SL_nA$ et $Q \in SL_m(A)$ telles que $M' = PMQ$ soit réduite avec des éléments $a_{i,i}$ sur la diagonale que l'on note simplement a_i.
La matrice P (resp. Q) s'interprète comme une matrice de changement de base de L (resp. de changement de famille génératrice de N). Notons $(f_1, \cdots, f_n)$ la nouvelle base de L ; l'écriture matricielle de M' s'interprète alors en disant que $(a_1 f_1, \cdots, a_r f_r)$ est une famille génératrice de N, où on a noté a_r le dernier des a_i non nuls. On note alors que cette nouvelle famille génératrice de N est libre, i.e. N est aussi libre avec $M/N \simeq A/(a_1) \times \cdots \times A/(a_r) \times A^{n-r}$. Montrons alors l'unicité des (a_i). Notons tout d'abord que $n - r$ ne dépend que de N. Pour ce faire considérons un irréductible p ne divisant pas a_r de sorte que pour tout $1 \leq i \leq n$, a_i est inversible modulo p et donc pour $M_i = A/(a_i)$ on a M_i/pM_i est nul. On voit ainsi que $n - r$ est la dimension du $A/(p)$ espace vectoriel $(M/N)/p(M/N)$. Considérons alors

$$\frac{A}{(a_1)} \times \cdots \times \frac{A}{(a_q)} \simeq \frac{A}{(a'_1)} \times \cdots \times \frac{A}{(a'_s)},$$

les (a_i) et les (a'_i) vérifiant les propriétés de divisibilité de l'énoncé et sont tous non nuls. Alors $(a_r) = \mathrm{Ann}(M/N) = (a'_s)$ et donc $\frac{A}{(a_1)} \times \cdots \times \frac{A}{(a_{q-1})} \simeq \frac{A}{(a'_1)} \times \cdots \times \frac{A}{(a'_{s-1})}$. En procédant de même de manière, on identifie de proche en proche les a_{q-i} avec les a'_{s-i} jusque obtenir $s = q$.

Définition 5.11. — On dit que $m \in M$ est un *élément de torsion* si $m \neq 0$ et s'il existe $\lambda \in A, \lambda \neq 0$, tel que $\lambda m = 0$. L'ensemble des éléments de torsion de M est noté M_t. Si $M_t = \{0\}$, on dit que M est *sans torsion.*

Remarque : M_t est un sous-module de M. Par ailleurs M est de torsion si et seulement si $M = M_t$. Avec ces notions la preuve du théorème précédent se réécrit.

Corollaire 5.12. — *Soit M un A-module de type fini, M_t son sous-module de torsion. Alors il existe un sous-module $L \subset M$ libre de rang r tel que $M = M_t \oplus L$.*

Définition 5.13. — Le rang de la partie libre de M s'appelle le *rang* de M. Les idéaux non nuls (a_i) pour $1 \leq i \leq q$ sont les *facteurs invariants* de M.

Remarque : le corps des rationnels $\mathbb{Q}$ est un exemple de $\mathbb{Z}$-module sans torsion et non libre (si $q_1 = a/b$ et $q_2 = c/d$, sont deux rationnels non nuls, on a la relation $bcq_1 - adq_2 = 0$). Ainsi $\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module de type fini.

Définition 5.14. — Un A-module M est dit *indécomposable* s'il n'est pas isomorphe à la somme directe de deux A-modules non nuls.

Proposition 5.15. — *Soit M un A-module de type fini. Les conditions suivantes sont équivalentes :*

1. *le module M est indécomposable ;*
2. *$M \simeq A$, ou il existe un élément irréductible $p \in A$, un entier $\alpha > 0$ tels que $M \simeq A/(p^\alpha)$.*

Preuve : 1. $\Rightarrow$ 2.
D'après le théorème 5.12 on peut supposer $M = A/(a)$. Si l'élément a a au moins deux facteurs irréductibles, il résulte du lemme chinois que M n'est pas indécomposable.
2. $\Rightarrow$ 1.
L'anneau A étant intègre, il est clair que le A-module A est indécomposable.
Si $\alpha > 0$, les sous-modules de $\tilde{M} = A/(p^\alpha)$ sont engendrés par les images dans $\tilde{M}$ des éléments p^γ pour $\gamma \leq \alpha$. Si M_1 et M_2 sont deux tels sous-modules, on a toujours $M_1 \subset M_2$ ou $M_2 \subset M_1$; ils ne peuvent donc pas être en somme directe.

Définition 5.16. — Soient M un A-module, $p \in \mathcal{P}$ un élément irréductible. On note $M(p)$ l'ensemble des éléments $x \in M$ de p-trosion, i.e. annulés par une puissance de p.

Remarque : en appliquant le théorème chinois au théorème 5.12, on obtient la décomposition canonique en indécomposable donnée par le théorème suivant.

Théorème 5.17. — *Soit M un A-module de torsion de type fini, $(a) = \mathrm{Ann}(M)$ son annulateur. Alors :*

1. *$M = \bigoplus_{p_i \in \mathcal{P},\, p_i | a} M(p_i)$ et $M(p_i) \neq (0)$ pour chaque élément irréductible p_i tel que $p_i | a$*

2. *pour chaque élément irréductible $p_i \in \mathcal{P}$, $p_i|a$, il existe une suite d'entiers $\nu_{i1} \leq \nu_{i2} \leq \cdots \leq \nu_{ik}$ unique telle que :*

$$M(p_i) \simeq \prod_{j=1}^{k} A/(p_i^{\nu_{ij}})).$$

3. *la décomposition $M \simeq \prod_{i,j} A/(p_i^{\nu_{ij}})$ est l'unique décomposition de M en produit de modules indécomposables.*

Exemple : prenons $A = \mathbb{Z}$, $M = M_t = \mathbb{Z}/96\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. On a $96 = 2^5 \times 3$, $72 = 2^3 \times 3^2$, d'où :

$$M \simeq \mathbb{Z}/32\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

par le théorème chinois. On a donc

$$\begin{array}{lcccccc} M(2) & \simeq & \mathbb{Z}/32\mathbb{Z} & \times & \mathbb{Z}/8\mathbb{Z} & \times & \mathbb{Z}/2\mathbb{Z} \\ M(3) & \simeq & \mathbb{Z}/9\mathbb{Z} & \times & \mathbb{Z}/3\mathbb{Z} & & \\ M(5) & \simeq & \mathbb{Z}/5\mathbb{Z}. & & & & \end{array} \tag{8}$$

Pour trouver la décomposition en indécomposable (resp. en facteurs invariants), on lit le tableau ci-dessus en lignes (resp. en colonnes), et on trouve $M = M(2) \oplus M(3) \oplus M(5)$ (resp. $a_3 = 32 \times 9 \times 5 = 1440$, $a_2 = 8 \times 3 = 24$, $a_1 = 2$, d'où la décomposition $M \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/1440\mathbb{Z}$.
Remarque : en considérant un groupe abélien comme un $\mathbb{Z}$-module, on peut donner la classification des groupes abéliens finis d'ordre n donné. On procède de la manière suivante. Soit G un groupe d'ordre n.

1. On écrit $n = p_1^{\nu_1} \dots p_s^{\nu_s}$ avec p_i premiers, ν_i entiers ;
2. on a alors $G \simeq G(p_1) \oplus \cdots \oplus G(p_s)$;
3. pour chaque entier i, $1 \leq i \leq s$ il existe une suite (ν_{ij}) unique d'entiers > 0 tels que $\sum_j \nu_{ij} = \nu_i$ et $G(p_i) \simeq \bigoplus_j \mathbb{Z}/p_i^{\nu_{ij}}\mathbb{Z}$;
4. deux groupes d'ordre n sont isomorphes si et seulement si tous les p_i et les entiers ν_{ij} sont les mêmes.

Exemple : donnons à isomorphisme près tous les groupes abéliens d'ordre $108 = 2^2 \times 3^3$. Soit $G = G(2) \oplus G(3)$ avec $G(2)$ d'ordre 4 et $G(3)$ d'ordre 27. Il y a à isomorphisme près deux possibilités pour $G(2)$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et trois pour $G(3)$, $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^3$. Il y a donc à isomorphisme près six groupes abéliens d'ordre 108.

5.4. Sous-groupes de $\mathbb{R}^n$. — Parmi les sous-groupes de $\mathbb{R}$, les exemples les plus simples sont d'une part $\{0\}$, $\mathbb{Z}$ et plus généralement $\delta\mathbb{Z}$ pour $\delta \in \mathbb{R}$, et d'autre part $\mathbb{Z} + \sqrt{2}\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Les premiers sont *discrets* au sens où pour tout compact K de $\mathbb{R}$ l'intersection $K \cap G$ est finie, alors que les deuxièmes sont denses. Par ailleurs étant donnés deux sous-groupes G_1 et G_2 de respectivement $\mathbb{R}^{n_1}$ et $\mathbb{R}^{n_2}$, le groupe produit $G_1 \times G_2$ est un sous-groupe de $\mathbb{R}^{n_1+n_2}$. Nous allons voir dans une certaine mesure qu'on obtient ainsi tous les sous-groupes de $\mathbb{R}^n$.

Lemme 5.18. — *Un sous-groupe G de $\mathbb{R}^n$ est discret dans $\mathbb{R}^n$ si et seulement s'il existe un ouvert U de $\mathbb{R}^n$ contenant 0 tel que $G \cap U$ soit discret.*

Preuve : Si G est discret on peut prendre $U = \mathbb{R}^n$. Réciproquement si G n'est pas discret alors il existe $z \in \mathbb{R}^n$ qui est un point d'accumulation d'éléments de G, i.e. pour tout $\epsilon > 0$, il existe $x_1 \neq x_2 \in G$ tel que $0 \leq |z - x_i| < \epsilon$ pour $i = 1, 2$ et donc $0 < |x_1 - x_2| < 2\epsilon$ ce qui montre que 0 est un point d'accumulation de G car $x_1 - x_2 \in G$.
Remarque : en particulier un sous-groupe non discret de $\mathbb{R}$ est partout dense.

Définition 5.19. — Un sous-groupe discret d'un espace vectoriel est appelé un *sous-réseau* de V ; s'il engendre V on dit que c'est *un réseau*.

Voici une caractérisation des réseaux parmi les sous-réseaux.

Lemme 5.20. — *Soit G un sous-réseau de V. Pour que G engendre V, il faut et il suffit qu'il existe un ensemble borné B de V tel que*

$$V = \bigcup_{g \in G} (B + g).$$

Preuve : Si G contient une base $(e_1, \cdots, e_n)$ de V alors

$$B = \{\sum_{i=1}^{n} x_i e_i,\ 0 \leq x_i < 1\}$$

convient. Réciproquement si G est contenu dans un sous-espace strict V' de V, notons $p : V \longrightarrow W$ la projection de V sur un supplémentaire W de V' dans V. Alors

$$p\Big(\bigcup_{g \in G} (B + g)\Big) = p(B).$$

Comme B est borné et que $W = p(V)$ est de dimension ≥ 1, on a $p(B) \neq p(V)$ et donc

$$\bigcup_{g \in G} (B + g) \neq V.$$

Proposition 5.21. — *Soit G un sous-groupe discret de $\mathbb{R}^n$. Il existe alors $1 \leq t \leq n$ et des éléments $e_1, \cdots, e_t \in G$ linéairement indépendants tels que $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_t$.*

Preuve : Soit $f_1, \cdots, f_t$ une base de l'espace vectoriel V engendré par G de sorte que $G' = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_t$ est un sous-groupe de G. Montrons que G' est d'indice fini dans G. Considérons le compact $K = \big\{u_1 f_1 + \cdots + u_t f_t :\ 0 \leq u_i \leq 1\big\}$. Soit $g \in G \subset V$ que l'on écrit sous la forme

$$g = x_1 f_1 + \cdots + x_t f_t = \sum_{i=1}^{t} \lfloor x_i \rfloor f_i + k$$

avec $k \in G \cap K$. Comme G est supposé discret $G \cap K$ est fini de sorte que G/G' l'est aussi. Notons $s := [G : G']$ et soit $f_i' = \frac{1}{s} f_i$. On a alors

$$\mathbb{Z}f_1 + \cdots + \mathbb{Z}f_1 \subset G \subset \mathbb{Z}f_1' + \cdots + \mathbb{Z}f_t',$$

et le résultat découle du théorème de la base adaptée 5.10.

Théorème 5.22. — *Soit G un sous-groupe additif de $\mathbb{R}^n$. Il existe alors un plus grand sous-espace vectoriel V de $\mathbb{R}^n$ contenu dans l'adhérence de G et il existe un sous-groupe discret G' de G tel que G soit la somme directe*

$$G = (G \cap V) \oplus G'.$$

Si t désigne le rang de G' et d la dimension de V alors $d+t$ est la dimension de l'espace vectoriel engendré par G.

Preuve : Pour $\rho > 0$, notons $B(0,\rho) = \{x \in \mathbb{R}^n,\ ||x|| \leq \rho\}$ et soit V_ρ le $\mathbb{R}$-espace vectoriel engendré par $G \cap B(0,\rho)$. L'application $\rho \mapsto \dim V_\rho$ est croissante à valeurs entières positives de sorte qu'il existe $\rho_0 > 0$ tel que pour tout $0 < \rho \leq \rho_0$, $V_\rho = V_{\rho_0}$. Posons $V := V_{\rho_0}$ et montrons que $G' = G \cap V$ est dense dans V. Soit $\epsilon > 0$ et soit $x \in V$. Posons $\rho = \min\{\epsilon/d, \rho_0\}$ et soit $(e_1, \cdots, e_d)$ une base de V avec $e_i \in G \cap B(0,\rho)$. Pour $x = x_1e_1 + \cdots + x_de_d$, on pose $m_i = \lfloor x_i \rfloor$ et $y = m_1e_1 + \cdots + m_de_d$. Alors $y \in G'$ vérifie $||x - y|| \leq \epsilon$.
Soit W le sous-espace engendré par G ; comme il contient V sa dimension est $d+t$ avec $t \geq 0$. Notons V' un supplémentaire de V dans W et soit $p : W \longrightarrow V'$ la projection de noyau V. Montrons que $p(G)$ est un sous-groupe discret de V'. Dans le cas contraire il existerait $z \in p(G)$ tel que $0 < ||z|| < \epsilon$ avec $\epsilon = \rho_0/2$. Soit $w \in G$ tel que $z = p(w)$; on a $u = z - w \in V$. Comme G' est dense dans V, il existe $w' \in G'$ tel que $||u - w'|| < \epsilon$ et $||w - w'|| < \rho_0$ puis $p(w - w') = z \neq 0$, i.e. $w - w' \in G$ vérifie $w - w' \notin V$ ce qui contredit le fait que $V = V_{\rho_0}$.

Alors $p(G)$ est un sous-groupe discret de V' de rang t, donc un réseau de V'. On en prend une base $p(y_1), \cdots, p(y_t)$ et on pose $G'' = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_t$ de sorte que $G = G' \oplus G''$. Enfin comme G'' est discret, V est bien le plus grand sous-espace vectoriel de $\mathbb{R}^n$ contenu dans l'adhérence de G.

6. Questions

Exercice 6.1. — *Soient G un groupe et H, K deux sous-groupes. On suppose que soit H soit K est distingué, montrer alors que $HK = \{hk,\ h \in H \text{ et } k \in K\}$ est un sous-groupe de G.*

Exercice 6.2. — *(cf. [?]) Notons D_n le nombre de dérangements de $\mathfrak{S}_n$ c'est à dire l'ensemble des permutations de $\mathfrak{S}_n$ sans point fixe. Montrer les propriétés suivantes :*

1. $\sum_{k=0}^{n} \binom{k}{n} D_{n-k} = n!$;
2. $D_n = n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$;
3. *la série génératrice* $\sum_{k\geq 0} \frac{D_k z^k}{k!}$ *est égale à* $\frac{e^{-z}}{1-z}$, *son rayon de convergence est* e ;
4. $D_k = \lfloor \frac{k!}{e} + \frac{1}{2} \rfloor$;
5. $D_{n+1} = n(D_n + D_{n-1})$;
6. $D_n = nD_{n-1} + (-1)^n$.

Exercice 6.3. — *Un paysan a $2n+1$ vaches telles, l'une quelconque de ses vaches étant mises de côté, il peut répartir les $2n$ restantes en deux sous-troupeaux de même poids total. Montrez que toutes les vaches ont le même poids.*

Exercice 6.4. — *Une fonction $f : \mathbb{Z} \to \mathbb{Z}$ est appelée un quasi-endomorphisme s'il existe une constante C_f telle que*

$$\forall m, n \in \mathbb{Z},\ |f(n+m) - f(n) - f(m)| \leq C_f.$$

On note $\mathcal{Q}$ l'ensemble des quasi-endomorphismes de $\mathbb{Z}$.

1. *Montrer que l'addition usuelle des fonctions munie $\mathcal{Q}$ d'une loi de groupe abélien.*
2. *Montrer que $\mathcal{Q}$ est stable par la composition des fonctions ; $(\mathcal{Q}, +, \circ)$ est-il un anneau ?*

3. *Montrer que pour tout $k \geq 2$, on a*
$$\left| f(n_1 + \cdots + n_k) - f(n_1) - \cdots - f(n_k) \right| \leq (k-1)C_f.$$
4. *Montrer que la suite $\left(\frac{f(n)}{n}\right)_{n\geq 1}$ est convergente dans $\mathbb{R}$.*
Indication : on pourra utiliser une majoration de $\left|\frac{f(nm)}{nm} - \frac{f(n)}{n}\right|$ afin de montrer que la suite $\left(\frac{f(n)}{n}\right)_{n\geq 1}$ est de Cauchy.
5. *Soit $l : \mathcal{Q} \to \mathbb{R}$ qui à f associe $\lim_{n\to\infty} \frac{f(n)}{n}$. Montrer que l est un morphisme surjectif de groupes dont le noyau $\mathcal{K}$ est l'ensemble des quasi-endomorphismes bornés.*
6. *Montrer que pour tout $f, g \in \mathcal{Q}$, on a $l(g \circ f) = l(g)l(f)$.*

Remarque : le quotient $\mathcal{Q}/\mathcal{K}$ est donc isomorphe à $\mathbb{R}$. Notons qu'il est possible de construire $\mathbb{R}$ en utilisant les quasi-endomorphismes de $\mathbb{Z}$. Il s'agit alors de montrer que le quotient $\mathcal{Q}/\mathcal{K}$ muni de $\circ$ est un anneau que l'on peut munir d'une relation d'ordre total : $f \leq g$ si et seulement si $f - g$ est borné. On montre enfin que $\mathcal{Q}/\mathcal{K}$ est un corps satisfaisant la propriété de la borne supérieure. Pour une preuve complète on renvoie le lecteur à http ://www.math.mq.edu.au/∼street/EffR.pdf

Exercice 6.5. — *Soient G un groupe fini, d'élément neutre e, et x un élément de G d'ordre m.*

1. *Montrer que pour tout entier k, l'ordre de x^k est $\frac{m}{(m\wedge k)}$.*
2. *Soit n un entier ≥ 1. Montrer que les conditions suivantes sont équivalentes :*
   — *on a $m = n$.*
   — *On a $x^n = e$ et pour tout diviseur premier p de n, on a $x^{\frac{n}{p}} \neq e$.*

Exercice 6.6. — 1. *Montrer que dans un groupe fini d'ordre impair, tout élément est un carré.*
2. *Soient G un groupe cyclique d'ordre n pair, d'élément neutre e. Montrer que G possède exactement $\frac{n}{2}$ éléments qui sont des carrés.*
3. *Soit a un élément de G. Montrer l'équivalence*
$$a \text{ est un carré dans } G \iff a^{\frac{n}{2}} = e.$$
4. *Supposons que n soit une puissance de 2. Montrer que l'ensemble des générateurs de G est l'ensemble des éléments qui ne sont pas des carrés.*

Exercice 6.7. — ***Puissances dans un groupe cyclique*** *Soient G un groupe cyclique d'ordre n, d'élément neutre e, et a un élément de G.*

1. *Soit k un entier naturel. Montrer que pour qu'il existe $x \in G$ tel que $x^k = a$ il faut et il suffit que l'on ait*
$$a^{\frac{n}{d}} = e \quad \text{où} \quad d = (k \wedge n). \tag{1}$$
2. *Soit k un entier naturel tel que la condition (1) soit satisfaite. Soit x_0 un élément de G tel que $x_0^k = a$. Montrer que l'ensemble des éléments $x \in G$ tels que $x^k = a$ est*
$$\Big\{ x_0 z \;\Big|\; z \in G \text{ et } z^d = e \Big\},$$
et que son cardinal est d.

3. *On prend pour G le groupe additif $\mathbb{Z}/25\mathbb{Z}$. Déterminer dans G l'ensemble des solutions de l'équation $5x = \overline{15}$.*

Exercice 6.8. — *Soit A un anneau intègre.*

1. *Montrer qu'un idéal $\mathcal{P}$ de A est premier si et seulement s'il vérifie la propriété suivante :*
$$xy \in \mathcal{P} \text{ et } x \notin \mathcal{P} \Rightarrow y \in \mathcal{P}.$$
2. *Soient $\mathcal{P}$ un idéal premier de A et $I_1, \cdots, I_r$ des idéaux tels que $I_1.\cdots.I_r \subset \mathcal{P}$. Montrez que $\mathcal{P}$ contient l'un des I_k.*
3. *Soit I un idéal non premier de A, montrez qu'il existe deux idéaux I_1 et I_2 tels que $I \subset I_1$, $I \subset I_2$ et $I_1.I_2 \subset I$.*
En utilisant le lemme de Zorn, montrez l'existence d'idéaux premiers minimaux pour l'inclusion. En supposant A noethérien, montrez qu'il existe un nombre fini d'idéaux premiers minimaux.
4. *Un idéal $\mathcal{Q}$ sera dit primaire s'il vérifie :*
$$\forall x, y \in A \; xy \in \mathcal{Q}, \; x \notin \mathcal{Q} \Rightarrow \exists n \; y^n \in \mathcal{Q}.$$
Si $\mathcal{Q}$ est primaire que peut-on dire de $A/\mathcal{Q}$? Pour tout idéal I de A, on pose
$$\sqrt{I} = \{x \in A \; / \; \exists n \; x^n \in I\}.$$
Montrer que Q primaire entraine que sa racine est un idéal premier. Réciproquement : soit $I = (X), \; n > 1 \; J = (X, Y)^n$ dans $A = \mathbb{C}[X, Y]$. Montrer que $Q = I \cap J$ n'est pas primaire bien que son radical soit premier.

Exercice 6.9. — *Soient $\mathfrak{A}$ et $\mathfrak{B}$ des idéaux d'un anneau A. On définit alors*
$$\mathfrak{A} : \mathfrak{B} = \{a \in A : \; ab \in \mathfrak{A} \; \forall b \in \mathfrak{B}\}$$
Montrez que $\mathfrak{A} : \mathfrak{B}$ est un idéal de A tel que :

1. $(\mathfrak{A} : \mathfrak{C}) + (\mathfrak{B} : \mathfrak{C}) \subset (\mathfrak{A} + \mathfrak{B}) : \mathfrak{C}$;
2. $\mathfrak{A} : (\mathfrak{B} + \mathfrak{C}) = (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$;

$(\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} = \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$;

Exercice 6.10. — *Quels sont les idéaux bilatères de $\mathcal{L}(E)$?*

Exercice 6.11. — *Quels sont les idéaux à gauche de $\mathcal{L}(E)$?*

Exercice 6.12. — *Quels sont les idéaux à droite de $\mathcal{L}(E)$?*

Exercice 6.13. — *Soit k un corps et $A = k[[X]]$ l'algèbre des séries formelles à coefficients dans k.*

1. *Montrez que A est intègre et déterminez $A^\times$.*
2. *Montrez que tout idéal non nul de A est de la forme $X^n A$, $n \in \mathbb{N}$. En déduire que A est principal et déterminez ses éléments irréductibles.*
3. *Montrez que A est euclidien.*

7. Solutions

6.1 Soient h_1k_1 et h_2k_2 des éléments de KH ; si H (resp. K) est distingué, pour tout $h \in H$ et $k \in K$ on a $hk = kh'$ (resp. $hk = k'h$) pour $h' \in H$ (resp. $k' \in K$) de sorte que $h_1k_1h_2k_2 \in HK$. En ce qui concerne l'inverse on écrit $k^{-1}h^{-1}$ sous la forme $h'k^{-1}$ (resp. $h^{-1}k'$) et donc HK est un sous-groupe de G.

6.2 1) La formule découle directement de la partition de $\mathfrak{S}_n$ selon le cardinal du support

2) La relation découle directement de la première question ou se prouve en utilisant la formule du crible à l'égalité

$$D_n = n! - \sharp\Big(\bigcup_{i=1}^{n} U_i\Big)$$

où U_i désigne le sous-ensemble de $\mathfrak{S}_n$ des permutations fixant i.

3) La formule se prouve en utilisant la première question ou alors directement par une preuve purement de combinatoire algébrique.

4) L'égalité découle de

$$\frac{k!}{e} + \frac{1}{2} = D_k + \frac{1}{2} + k!R_k, \qquad R_k = \sum_{n=k+1}^{+\infty} \frac{(-1)^n}{n!}$$

et de la minoration des séries alternées $|R_k| \leq \frac{1}{(k+1)!}$.

5) La relation de récurrence (v) se prouve comme suit : soit l'orbite de $n+1$ est de cardinal 2 ce qui donne nD_{n-1} possibilité pour un tel dérangement et sinon nD_n.

6) La relation se prouve à partir de la question précédente par récurrence ou peut se montrer purement combinatoirement mais de manière détournée pour l'instant.

6.3 L'énoncé se traduit matriciellement comme suit : il existe une matrice $A \in \mathbb{M}_{2n+1}(\mathbb{R})$ telle que

- $a_{i,i} = 0$ (on met la i-ème vache de côté) ;
- $a_{i,j} = \pm 1$ si $j \neq i$ (le signe dépend dans quel sous-troupeau on met la j-ème vache quand la i-ème est de côté) ;
- $\sum_{j=1}^{2n+1} a_{i,j} = 0$ (les deux sous-troupeaux sont de même cardinal) ;
- $\sum_{j=1}^{2n+1} a_{i,j}p_j = 0$, où p_j est le poids de la j-ème vache (les deux sous-troupeaux ont même poids total).

Le résultat découle alors directement du fait suivant : toute matrice $A \in \mathbb{M}_{2n+1}(\mathbb{R})$ à coefficients diagonaux nuls, les autres étant égaux à ± 1 est de rang $2n$. En effet comme le vecteur n'ayant que des 1 est dans le noyau, le vecteur des p_i qui est aussi dans le noyau lui sera proportionnel et donc tous les p_i seront égaux. Considérons la matrice extraite B obtenue en ôtant la dernière ligne et colonne et montrons qu'elle est inversible. Son déterminant est

$$\delta = \sum_{\sigma \in \mathfrak{S}_{2n}} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{2n,\sigma(2n)}.$$

Les termes diagonaux étant nuls, les seuls termes non nuls sont ceux pour lesquels σ est un dérangement. Par ailleurs chacun de ces termes étant égal à ± 1, il suffit de montrer que $D_n \equiv 1 \mod 2$. Comme $D_{2n-1} = (2n-2)(D_{2n-2} + D_{2n-3})$ il est pair et $D_{2n} = (2n-1)(D_{2n-1} + D_{2n-2})$ est de la même parité que D_{2n-2} ; on conclut par récurrence.

6.4 1) C'est clair en posant $C_{f+g} = C_f + C_g$ et en utilisant l'inégalité triangulaire.

2) On écrit

$$\Big|g\circ f(m+n)-g\circ f(n)-g\circ f(m)\Big|\leq$$
$$\Big|g\circ f(n+m)-g\big(f(n)+f(m)\big)\Big|+\Big|g\big(f(n)+f(m)\big)-g(f(n))-g(f(m))\Big|$$

Le deuxième terme du membre de droite est majoré par C_g et quant au premier en écrivant $f(n+m)=f(n)+f(m)+\delta$ avec $|\delta|\leq C_f$ et en notant $M=\max_{|i|\leq M}|g(i)|$, on obtient

$$\Big|g\circ f(n+m)-g\big(f(n)+f(m)\big)\Big|\leq M+C_g$$

et donc en posant $C_{g\circ f}=M+2C_g$, on a bien $g\circ f\in\mathcal{Q}$.
Remarque : comme $\circ$ n'est pas distributive par rapport à l'addition, $(\mathcal{Q},+,\circ)$ n'est pas un anneau.

3) Par récurrence sur k ; supposons le résultat acquis jusqu'au rang $k-1$, on écrit alors

$$f(n_1+\cdots+n_k)-f(n_1)-\cdots-f(n_k)=f(n_1+\cdots+n_k)-f(n_1+\cdots+n_{k-1})-f(n_k)+f(n_1+\cdots+n_{k-1})-f(n_1)-\cdots-$$

de sorte que le résultat découle de l'inégalité triangulaire.

6.4 D'après la question précédente, on a $|f(nm)-mf(n)|\leq mC_f$ et $|f(nm)-nf(m)|\leq C_f$, de sorte que

$$\Big|\frac{f(nm}{nm}-\frac{f(n)}{n}\Big|\leq\frac{C_f}{n}\text{ et }\Big|\frac{f(nm)}{nm}-\frac{f(m)}{m}\Big|\leq\frac{C_f}{n}$$

et par inégalité triangulaire on obtient

$$\Big|\frac{f(m}{m}-\frac{f(n)}{n}\Big|\leq\frac{C_f}{n}+\frac{C_f}{m}$$

et donc $\Big(\frac{f(n)}{n}\Big)_{n\geq1}$ est de Cauchy.

4) Pour la surjectivité prendre par exemple $f(x)=\lfloor nx\rfloor$ pour $x\in\mathbb{R}$. Par ailleurs l est clairement un morphisme de groupe ; soit $f\in\mathcal{K}$, on va montrer que $|f(n)|\leq C_f$, pour tout $n\geq0$, ce qui est déjà le cas pour $n=0$. On raisonne par l'absurde en considérant $n_0>0$ tel que $|f(n_0)|>C_f$; on a alors $|f(kn_0)-kf(n_0)|\leq(k-1)C_f$ et donc

$$|f(kn_0)|\geq|f(n_0)|+(k-1)\Big(|f(n_0)|-C_f\Big).$$

Ainsi la suite extraite $\Big(\frac{f(kn_0)}{kn_0}\Big)_{k\geq1}$ ne converge pas vers 0 ce qui n'est pas. Pour les $n<0$, on écrit $f(0)-f(n)-f(-n)|\leq C_f$ et donc $|f(n)|\leq|f(0)|+|f(-n)|+C_f$ et donc $|f(n)|\leq3C_f$.

5) Si $l(f)=0$ alors f est bornée et donc $g\circ f$ aussi et donc $l(g\circ f)=0=l(g)l(f)$. Si $l(f)>0$ alors comme $f(n)\to+\infty$, il existe n_0 tel que pour tout $n\geq n_0$, $f(n)>0$ de sorte que le résultat découle de l'égalité suivante que l'on passe à la limite :

$$\frac{g\circ f(n)}{n}=\frac{g\circ f(n)}{f(n)}\frac{f(n)}{n}.$$

Finalement le raisonnement est identique si $l(f)<0$ en remarquant que $f(n)/n$ tend vers $l(f)$ quand $n\to-\infty$, car $|f(n)+f(-n)|\leq|f(0)|+C_f$.

6.5 1) Soit d le plus grand commun diviseur de m et k. On a d'abord $(x^k)^{\frac{m}{d}}=(x^m)^{\frac{k}{d}}=e$, où e est l'élément neutre de G (car $x^m=e$). Considérons alors un entier u tel que $(x^k)^u=e$. L'entier m divise uk (car m est l'ordre de x) et donc m/d divise aussi uk/d. Les entiers m/d et k/d étant premiers entre eux, il en résulte que m/d divise u, ce qui prouve notre assertion.

2) La première condition entraîne la seconde car m est le plus petit entier $k \geq 1$ tel que $x^k = e$. Inversement, supposons la condition 2 réalisée. Il existe un entier $k \geq 1$ tel que l'on ait $n = mk$: on a $n = mk + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < m$, d'où $x^r = e$ puis $r = 0$. Supposons $k \geq 2$. Soit p un diviseur premier de k. On a alors les égalités

$$x^{\frac{n}{p}} = \left(x^m\right)^{\frac{k}{p}} = e,$$

ce qui contredit l'hypothèse faite. Par suite, on a $k = 1$, puis $m = n$.

6.6 1) Soit G un groupe fini d'ordre $2n - 1$. Pour tout élément $x \in G$, on a $x^{2n-1} = e$ (e est l'élément neutre de G), d'où $x = x^{2n} = (x^n)^2$.

2) Soit $f : G \to G$ l'application définie par $f(x) = x^2$. C'est un morphisme de groupes. Puisque G est cyclique, G a un unique élément d'ordre 2, et le noyau de f est donc d'ordre 2. Par suite, l'ensemble G^2 des carrés de G est un groupe d'ordre $\frac{n}{2}$.

3) Soit H le sous-groupe de G formé des éléments x tels que $x^{\frac{n}{2}} = e$. Puisque G est cyclique, H est l'unique sous-groupe d'ordre $\frac{n}{2}$ de G. D'après la question précédente, G^2 et H ont le même ordre. On en déduit que $G^2 = H$, d'où l'équivalence annoncée.

Remarque. Si x est un élément de G qui ne soit pas un carré, $x^{\frac{n}{2}}$ est l'unique élément d'ordre 2 de G.

4) Supposons $n = 2^t$ avec $t \geq 1$. Dans ce cas, G^2 est de cardinal 2^{t-1} et son complémentaire aussi. Par ailleurs, il y a exactement $\varphi(2^t) = 2^{t-1}$ générateurs dans G (φ est la fonction indicatrice d'Euler). De plus, un générateur de G n'est évidemment pas un carré. Cela entraîne le résultat. [On peut aussi procéder comme suit : soit x un élément de G qui n'est pas un carré dans G. Si y est un générateur de G, il existe m tel que $x = y^m$. D'après l'hypothèse faite, m est impair, donc x est un générateur, car les générateurs de G sont précisément les éléments de la forme y^k avec k impair (ce sont les entiers k premiers avec l'ordre de G)].

6.7 1) Considérons le morphisme de groupes $\psi : G \to G$ défini par $\psi(x) = x^k$. Vérifions que son noyau est d'ordre d. Soit x un élément de $\mathrm{Ker}(\psi)$. On a $x^k = e$ et $x^n = e$, d'où en utilisant le théorème de Bézout, $x^d = e$. On en déduit que les éléments de $\mathrm{Ker}(\psi)$ sont exactement les éléments $x \in G$ pour lesquels on a $x^d = e$. Puisque G est cyclique, on a donc $|\mathrm{Ker}(\psi)| = d$ et l'ordre de l'image de ψ est n/d. Par suite, si a est dans l'image de ψ, on a $a^{n/d} = e$. Inversement, si on a l'égalité $a^{n/d} = e$, puisque G est cyclique, a appartient à l'unique sous-groupe de G d'ordre n/d, qui est précisément l'image de ψ, d'où la condition (1) de l'énoncé.

2) Si $x \in G$ vérifie l'égalité $x^k = a$, on a $(xx_0^{-1})^k = e$, d'où $x = x_0 z$ avec $z^k = e$, et comme on l'a constaté ci-dessus, on a alors $z^d = e$. Inversement, pour tout $z \in G$ tel que $z^d = e$, on a $(x_0 z)^k = a$ car d divise k, d'où l'ensemble des solutions annoncé. Par ailleurs, G étant cyclique, il y a exactement d éléments $z \in G$ tels que $z^d = e$. Cela établit le résultat.

3) On remarque que $x_0 = \overline{3}$ est une solution particulière. Par ailleurs, les éléments $x \in G$ qui vérifient $5x = \overline{0}$ sont les classes de 0, 5, 10, 15 et 20. L'ensemble des solutions cherché est donc $\left\{\overline{3}, \overline{8}, \overline{13}, \overline{18}, \overline{23}\right\}$.

6.8 1) La traduction est immédiate : la relation $\bar{x}\bar{y} = \bar{0}$ est équivalente à $xy \in \mathcal{P}$ pour $x \in \bar{x}$ et $y \in \bar{y}$; ainsi si $\mathcal{P}$ est premier on a x ou y appartient à $\mathcal{P}$ soit $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$. Réciproquement si $xy \in \mathcal{P}$ alors si $A/\mathcal{P}$ est intègre, on a $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$ et donc x ou y appartient à $\mathcal{P}$.

2) Soit $\mathcal{P}$ premier et $I_1 \cdots I_r \subset \mathcal{P}$, et supposons que pour tout $1 \leq k \leq r$, $I_k \not\subset \mathcal{P}$; on fixe ainsi pour tout k, un élément $x_k \in I_k$ et $x_k \notin \mathcal{P}$. Par hypothèse $x_1 \cdots x_r \in \mathcal{P}$ avec $x_1 \notin \mathcal{P}$ soit $x_2 \cdots x_r \in \mathcal{P}$ et par récurrence $x_r \in \mathcal{P}$ d'où la contradiction.

3) Soit I non premier, et soit $x, y \in A\backslash I$ avec $xy \in I$. On pose $I_1 = (I \cup \{x\})$ et $I_2 = (I \cup \{y\})$; on a $I_1 I_2 \subset I$ avec $I \subset I_1 \cap I_2$.

On considère la relation d'ordre sur l'ensemble $\mathcal{I}$ des idéaux premiers, donnée par la contenance, i.e. $I \leq J \Leftrightarrow J \subset I$; cette relation d'ordre est à nouveau inductive, un majorant d'une chaîne totalement ordonnée C étant donné par l'intersection $M = \cap_{I \in C} I$; en effet on vérifie comme précédemment que M est un idéal, le fait qu'il soit premier se montre aisément : soit $xy \in M$ et donc $xy \in I$ pour tout $I \in C$; comme I est premier, x ou y appartient à I ; supposons que $y \notin I$, alors pour tout $J \subset I \in C$, on a $y \notin J$ et donc $x \in J$ soit $x \in M$. Le lemme de Zorn donne alors l'existence d'éléments maximaux qui sont donc des idéaux premiers minimaux pour l'inclusion.

On suppose A noethérien et on considère l'idéal (0) ; s'il est premier alors c'est le seul idéal premier minimal, sinon soit I_1 et I_2 comme ci-dessus. Si I_1 et I_2 sont premiers, ceux sont les seuls idéaux premiers minimaux ; en effet soit $\mathcal{P}$ un idéal premier ; on a $(0) = I_1 I_2 \subset \mathcal{P}$ et donc $I_i \subset \mathcal{P}$ pour $i = 1$ ou 2, d'après ce qui précède. Si I_1 n'est pas premier, soit $I_{1,1}$ et $I_{1,2}$ comme ci-dessus ; on construit ainsi un arbre binaire dont la racine est l'idéal (0), tous les sommets sont des idéaux qui contiennent le produit des idéaux de ses deux fils et tel que tout chemin filial défini une chaîne totalement ordonnée pour l'inclusion. Si on suppose A noethérien, l'arbre est fini et les idéaux premiers minimaux sont les feuilles.

4) La traduction dans $A/\mathbb{Q}$ est à nouveau immédiate : $\mathbb{Q}$ est primaire si et seulement si dans $A/\mathbb{Q}$ les seuls diviseurs de 0 sont les éléments nilpotents, i.e. ceux tels qu'il existe n tels qu'élevés à la puissance n, ils donnent 0.
Montrons en premier lieu que $\sqrt{I}$ est un idéal : soient donc $x, y \in \sqrt{I}$ et n, m des entiers tels que $x^n \in I$ et $y^m \in I$. On a alors $(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} C_{n+m-1}^k x^k (-y)^{n+m-1-k}$; or $k < n$ si et seulement si $n + m - 1 - k \geq m$ et donc pour tout $0 \leq k \leq n + m - 1$, au moins un parmi x^k et $y^{n+m-1-k}$ appartient à I et donc $x - y \in \sqrt{I}$. Si $a \in A$ alors $(ax)^n \in I$ et donc $ax \in \sqrt{I}$ et donc finalement $\sqrt{I}$ est un idéal de A.
Exemple : dans $\mathbb{Z}$, la racine de l'idéal $n\mathbb{Z}$ avec $n = \prod_i p_i^{\alpha_i}$ est l'idéal engendré par $\prod_i p_i$.

Soit $\mathbb{Q}$ un idéal primaire et $\mathcal{P} = \sqrt{\mathbb{Q}}$; soit $x, y \in A$ tels que $xy \in \mathcal{P}$ et $x \notin \mathcal{P}$. Soit donc un entier n tel que $x^n y^n \in \mathbb{Q}$; comme $x \notin \mathcal{P}$ alors $x^n \notin \mathbb{Q}$ et donc $\mathbb{Q}$ étant primaire, soit m un entier tel que $(y^n)^m \in \mathbb{Q}$ soit $y \in \mathcal{P}$, et donc $\mathcal{P}$ est un idéal premier.

On considère $A = \mathbb{C}[X, Y]$ l'anneau des polynômes en deux variables à coefficients dans $\mathbb{C}$ et soit $I = (X)$ et $J = (X, Y)^n$ avec $n > 1$. On pose $\mathbb{Q} = I \cap J$ qui est l'idéal engendré par $X^n, X^{n-1}Y, \cdots, XY^{n-1}$; on a $\sqrt{\mathbb{Q}} = (X)$ qui est premier alors que $\mathbb{Q}$ n'est pas primaire car $X^{n-1}Y \in \mathbb{Q}$ avec $X^{n-1} \notin \mathbb{Q}$ et $Y^m \notin \mathbb{Q}$ pour tout entier m.

6.9 1) Vérifions tout d'abord que $\mathfrak{A} : \mathfrak{B}$ est un idéal de A : soient $a_1, a_2 \in \mathfrak{A} : \mathfrak{B}$ et $a \in A$, pour tout $b \in \mathfrak{B}$ on a $(r_1 + ar_2)b = r_1 + ar_2 b \in \mathfrak{A}$, d'où le résultat. Soit alors $a = a_1 + a_2 \in \mathfrak{A} : \mathfrak{C} + \mathfrak{B} : \mathfrak{C}$ de sorte que pour tout $c \in \mathfrak{C}$, $a_1 c \in \mathfrak{A}$ et $a_2 c \in \mathfrak{B}$ et donc $ac \in \mathfrak{A} + \mathfrak{B}$ pour tout $c \in \mathfrak{C}$ soit $a \in (\mathfrak{A} + \mathfrak{B}) : \mathfrak{C}$.

2) Soit $a \in \mathfrak{A} : (\mathfrak{B} + \mathfrak{C})$ alors $a(b+c) \in \mathfrak{A}$ pour tout $b \in \mathfrak{B}$ et $c \in \mathfrak{C}$. En particulier en prenant $c = 0$, on a $ab \in \mathfrak{A}$ pour tout $b \in \mathfrak{B}$ et donc $a \in \mathfrak{A} : \mathfrak{B}$. En procédant de même avec $\mathfrak{C}$, on obtient l'inclusion $\mathfrak{A} : (\mathfrak{B} + \mathfrak{C}) \subset (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$. Réciproquement soit $a \in (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$ alors $ab \in \mathfrak{A}$ pour tout $b \in \mathfrak{G}$ et $ac \in \mathfrak{A}$ pour tout $c \in \mathfrak{C}$ de sorte que $a(b + c) \in \mathfrak{A}$, ce qui donne l'inclusion réciproque.

6.9 Soit $a \in (\mathfrak{A} : \mathfrak{B}) : \mathfrak{C}$ de sorte que pour tout $c \in \mathfrak{C}$, $ac \in \mathfrak{A} : \mathfrak{B}$ et donc pour tout $b \in \mathfrak{B}$, on a $acb \in \mathfrak{A}$. Comme $\mathfrak{A}$ est stable par l'addition, on en déduit donc que $ad \in \mathfrak{A}$ pour tout $d \in \mathfrak{B}\mathfrak{C}$ et donc $(\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} \subset \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$. Réciproquement soit $a \in \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$ de sorte que pour

tout $d \in \mathfrak{BC}$, on a $ad \in \mathfrak{A}$. En particulier pour $d = bc$, c fixé et b décrivant $\mathfrak{C}$, on obtient que $ac \in \mathfrak{A} : \mathfrak{B}$. Comme ce fait est vrai pour tout c, on en déduit que $a \in (AF : \mathfrak{B}) : \mathfrak{C}$.

6.10 On se ramène à $\mathbb{M}_n(K)$; soit I un idéal bilatère de $\mathbb{M}_n(K)$ et $M = (m_{i,j})_{1\leq i,j\leq n} \in I$ non nulle. Soit (i_0, j_0) tel que $m_{i_0,j_0} \neq 0$. On a

$$E_{i,i_0} M E_{j_0,j} = \sum_{1\leq k,l\leq n} m_{k,l} E_{i,i_0} E_{k,l} E_{j_0,j} = \sum_{k=1}^{n} m_{k,j_0} E_{i,i_0} E_{k,l} = m_{i_0,j_0} E_{i,j}$$

de sorte que pour tout (i, j), $E_{i,j} \in I$ et donc $I = \mathbb{M}_n(K)$.

6.11 Soit I un idéal de $\mathbb{M}_n(\mathbb{C})$, on va montrer que $I = \mathbb{M}_n(\mathbb{C})A = \{M \in \mathbb{M}_n(\mathbb{C}) \ / \ \operatorname{Ker} A \subset \operatorname{Ker} M\}$. Soit $M = PI_rQ \in I$, on a alors $Q^{-1}P^{-1}M \in I$ et donc I contient un projecteur. Pour tout f, on note I_f l'ensemble des endomorphismes qui s'annulent sur $\operatorname{Ker} f$: $I_f = \mathbb{M}_n(\mathbb{C})f$. De l'écriture $I = p + (Id - p)$, on en déduit que $\mathbb{M}_n(\mathbb{C}) = I_p \oplus I_{Id-p}$.

Soit alors p un projecteur de rang maximal dans I, alors $I \cap I_{Id-p} = 0$. En effet il suffit de montrer que l'intersection ne contient aucun projecteur q. Soit donc un projecteur q qui s'annule sur $\operatorname{Ker}(Id - p) = \operatorname{Im} p$. Dans une base convenable on a $p = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ er $q = \begin{pmatrix} 0 & B \\ 0 & D \end{pmatrix}$. Le projecteur $r = \begin{pmatrix} 0 & 0 \\ 0 & D \end{pmatrix}$ appartient évidemment à I ainsi donc que $p + r$ de sorte que $D = 0$ et donc $\operatorname{tr} q = 0$ soit $q = 0$.

Ainsi on a $I = I_p$ d'où le résultat.

6.12 La réponse est $\{M \in \mathbb{M}_n(\mathbb{C}) \ / \ \operatorname{Im} M \subset \operatorname{Im} A\}$, la démonstration est parallèle à la précédente.

6.13 1) Soit ν la valuation sur $k[[X]]$ définie par $\nu(\sum_{i=0}^{+\infty} a_i X^i) = \min\{i \in \mathbb{N},\ a_i \neq 0\}$ avec la convention $\nu(0) = +\infty$. Ainsi si $a = \sum_i a_i X^i$ et $b = \sum_i b_i X^i$ sont de valuations respectives α, β, alors ab est de valuation $\alpha + \beta$ car $a_\alpha b_\beta \neq 0$.
Montrons que $a = \sum_i a_i X^i$ est inversible si et seulement si $a_0 \neq 0$; supposons $a_0 \neq 0$, la recherche d'un inverse se ramène à la résolution du système triangulaire suivant : $a_0 b_0 = 1$ et pour tout $k \geq 1$, $\sum_{i=0}^{k} a_i b_{k-i} = 0$; une solution se calculant facilement par récurrence sur k. Réciproquement si a a pour inverse $b = \sum_i b_i X^i$, on a alors $a_0 b_0 = 1$ et donc $a_0 \neq 0$.

2) Soit I un idéal non nul de A et soient $n = \min_{x\in I} \nu(x)$ et $a \in I$ tel que $\nu(a) = n$; $a = X^n b$ avec $\nu(b) = 0$ de sorte que b est inversible soit $X^n \in I$ et donc $(X^n) \subset I$; l'inclusion réciproque étant évidente, on en déduit $I = (X^n)$.
L'anneau A est donc principal, donc factoriel. Soit $p \in A$ un élément irréductible, l'idéal (p) est alors premier et maximal. Or tout idéal I est contenu dans (X) qui est maximal car si $b \notin (X)$ alors b est inversible ; ainsi on a $(a) = (X)$ et a est associé à X de sorte qu'aux inversibles près, il n'y a qu'un seul irréductible, à savoir X.

3) Montrons que A est euclidien pour le stathme ν. Soient donc $(a, b) \in A \times A^\times$; $b = X^n \beta$ avec $\beta \in A^\times$. On écrit $a\beta^{-1} = X^\beta q + c$ avec $\deg c < \beta$, et donc $a = c\beta + bq$ avec $c\beta = 0$ ou $\nu(c\beta) < \nu(b) = \beta$, d'où le résultat.

Boyer Pascal