Résumé du cours d'algèbre 1, 2013-2014

Sandra Rozensztajn

UMPA, ENS de Lyon, sandra.rozensztajn@ens-lyon.fr

CHAPITRE 0

Relations d'équivalence et classes d'équivalence

1. Relation d'équivalence

DÉFINITION 1.1. *Soit X un ensemble. Une relation R sur X est une partie de $R \subset X \times X$. On dit que x est en relation avec y pour la relation R, et on note $x \sim y$, si $(x, y) \in R$.*

Une relation d'équivalence est une relation sur X qui est :

(1) réflexive : pour tout x, $x \sim x$

(2) symétrique : $x \sim y$ si et seulement si $y \sim x$

(3) transitive : si $x \sim y$ et $y \sim z$ alors $x \sim z$

2. Classes d'équivalence, quotient

DÉFINITION 2.1. *Soit X muni de la relation d'équivalence R, et $x \in X$. La classe d'équivalence de X est l'ensemble $\{y \in X, xRy\}$. On la note $Cl(x)$, ou $\overline{x}$, ou $[x]$.*

Une classe d'équivalence est une partie de X qui est la classe d'équivalence d'un $x \in X$. Un élément d'une classe d'équivalence est appelé représentant de cette classe d'équivalence.

DÉFINITION 2.2. *Une partition d'un ensemble X est une famille (X_i) de sous-ensembles de X qui sont disjoints et dont la réunion est X. On note $X = \sqcup_i X_i$.*

PROPOSITION 2.3. *Il y a une bijection entre les relations d'équivalences sur X et les partitions de X : l'ensemble des classes d'équivalence pour une relation d'équivalence forme une partition de X, et réciproquement, toute partition de X définit une relation d'équivalence.*

On note X/R l'ensemble des classes d'équivalence de X pour R, et on l'appelle quotient de X par la relation R. On a une projection canonique $\pi : X \to X/R$ qui à x associe sa classe d'équivalence, c'est une surjection.

3. Exemples

La relation d'égalité est une relation d'équivalence. Chaque classe d'équivalence contient exactement un élément, X est la même chose que $X/=$.

Soit n un entier. La relation définie sur $\mathbb{Z}$ par $x \sim y$ si et seulement si n divise $x - y$ est une relation d'équivalence. L'ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$.

CHAPITRE 1

Groupes

1. Bases

1.1. Définitions.

DÉFINITION 1.1. *Un groupe est un triplet $(G, \star, e)$ où G est un ensemble, e un élément de G, et $\star$ une application $G \times G \to G$ (loi de composition interne), vérifiant :*

(1) la loi $\star$ est associative : on a $(a \star b) \star c = a \star (b \star c)$

(2) e est élément neutre : on a $a \star e = e \star a = a$ pour tout a.

(3) tout élément a un inverse : pour tout a il existe b tel que $a \star b = b \star a = e$.

On vérifie qu'un groupe a un unique élément neutre, et que l'inverse est uniquement défini, on note a^{-1} l'inverse de a.

Un groupe est dit commutatif, ou abélien, si $a \star b = b \star a$ pour tous a, b.

On appelle ordre du groupe le cardinal du groupe.

1.2. Sous-groupe.

DÉFINITION 1.2. *Un sous-groupe de G est une partie H de G vérifiant :*

(1) $e \in H$

(2) pour tous $a, b \in H$ on a $a \star b \in H$

(3) pour tout $a \in H$ on a $a^{-1} \in H$.

On a alors que $(H, \star, e)$ est un groupe.

DÉFINITION 1.3. *Soit $X \subset G$. On appelle sous-groupe engendré par X, et on note $\langle X \rangle$, le plus petit sous-groupe de G contenant X. C'est aussi l'ensemble des produits d'éléments de X et de leurs inverses.*

Un groupe est dit monogène s'il peut être engendré par un seul élément. Il est dit cyclique s'il est monogène et fini. Exemples : $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ (ce sont les seuls).

L'ordre d'un élément est l'ordre du sous-groupe qu'il engendre (éventuellement infini).

1.3. Morphismes de groupes.

DÉFINITION 1.4. *Un morphisme de groupes de G vers G' est une application $f : G \to G'$ vérifiant :*

(1) $f(e) = e'$

(2) pour tous a, b, $f(a \star b) = f(a) \star' f(b)$

(3) $f(a^{-1}) = f(a)^{-1}$

On note $\operatorname{Im} f = \{x \in G', \exists y \in G, f(y) = x\}$ et $\ker f = \{x \in G, f(x) = e'\}$. Ce sont des sous-groupes de G' et G respectivement.

f est injective si et seulement si $\ker f = \{e\}$ et f est surjective si et seulement si $\operatorname{Im} f = G'$.

2. Classes définies par un sous-groupe, sous-groupe distingué, quotient

2.1. Classes définies par un sous-groupe.

PROPOSITION 2.1. *Soit H un sous-groupe de G. Alors la relation définie par $x \sim y$ si et seulement si il existe $h \in H$ tel que $x = yh$ est une relation d'équivalence.*

On note xH la classe d'équivalence de x, G/H l'ensemble quotient pour cette relation d'équivalence, c'est l'ensemble des classes à gauche pour H.

On définit de même une relation d'équivalence à droite, et $H\backslash G$ l'ensemble des classes à droite, Hx la classe de x.

DÉFINITION 2.2. *Si l'ensemble G/H est fini, on dit que H est d'indice fini dans G, et le cardinal de G/H est l'indice de H dans G, noté $[G : H]$. Sinon on dit que H est d'indice infini.*

Par exemple, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ d'indice fini $|n|$ si $n \neq 0$.

EXERCICE 1. *Montrer que G/H est fini si et seulement si $H\backslash G$ l'est, et qu'ils ont même cardinal : il n'y a donc rien de particulier à choisir les classes à gauche plutôt que les classes à droite dans la définition.*

PROPOSITION 2.3. *Soit G un groupe fini et H un sous-groupe de G. Toutes les classes à gauche pour H ont même cardinal.*

COROLLAIRE 2.4. *Soit G fini, alors $[G : H] = |G|/|H|$.*

Une application de la proposition 2.3 est le théorème de Lagrange :

THÉORÈME 2.5 (Théorème de Lagrange). *Soit G un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

DÉMONSTRATION. On considère sur G la relation d'équivalence à gauche définie par H : les classes d'équivalence sont les aH, $a \in G$. Nous allons montrer que toutes les classes d'équivalence ont même cardinal. Soit $a \in G$, on a plus précisément que la multiplication à gauche par a induit une bijection de H sur aH. Ainsi chaque classe est de cardinal $|H|$, et on a donc l'égalité $|G| = [G : H]|H|$ ce qui prouve le théorème. □

COROLLAIRE 2.6. *Soit G un groupe fini, et $x \in G$. Alors l'ordre de x divise le cardinal de G.*

2.2. Sous-groupe distingué.

DÉFINITION 2.7. *Un sous-groupe H de G est dit distingué (ou normal) si pour tout $a \in G$, on a $aH = Ha$.*

Si G est abélien, tout sous-groupe est distingué.

Le sous-groupe $\{e\}$ est distingué, G aussi (ce sont les sous-groupes distingués dits triviaux).

DÉFINITION 2.8. *On dit que G est simple s'il n'a pas de sous-groupe distingué non trivial.*

Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est simple.

EXERCICE 2. *Si G est abélien fini et simple, alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

PROPOSITION 2.9. *Soit G un groupe, et $f : G \to G'$ un morphisme de groupes. Alors* $\ker f$ *est distingué.*

$\mathrm{SL}_n(k)$ est un sous-groupe distingué de $\mathrm{GL}_n(k)$. $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$.

EXERCICE 3. *Soit G un groupe, et H un sous-groupe d'indice 2, alors H est distingué.*

DÉFINITION 2.10. *Soit G un groupe, et H un sous-groupe de G. On dit que x normalise H si $xH = Hx$. On appelle normalisateur de H dans G, et on note $N_G(H)$, l'ensemble des éléments de G qui normalisent H. C'est un sous-groupe de G, et c'est le plus grand dans lequel H est distingué.*

2.3. Groupes quotients.

THÉORÈME 2.11. *Soit H un sous-groupe distingué de G. Alors il existe une unique structure de groupe sur G/H telle que la projection canonique $\pi : G \to G/H$ soit un morphisme de groupe. Le noyau de π est H.*

DÉMONSTRATION. Soit $\alpha, \beta \in G/H$, et $a, b \in G$ tels que $\pi(a) = \alpha$ et $\pi(b) = \beta$. Si π est un morphisme de groupe, on a nécessairement $\alpha\beta = \pi(ab)$. Montrons qu'on définit bien une loi de composition interne sur G/H par cette formule, c'est-à-dire que le résultat ne dépend pas du choix de a et b. Prenons donc a', b' tels que $\pi(a') = \alpha$ et $\pi(b') = \beta$. Il existe x et y dans H tels que $a' = ax$ et $b' = by$. On a alors $a'b' = axby$. On a $xb \in Hb$, donc comme H est distingué, $xb \in bH$, donc peut s'écrire $xb = bz$ avec $z \in H$. Cela donne $a'b' = abzy$, avec $zy \in H$, donc $\pi(ab) = \pi(a'b')$.

Une fois cette loi définie, le fait que c'est une loi de groupe provient de la loi de groupe sur G. □

COROLLAIRE 2.12. *Un sous-groupe H de G est distingué si et seulement si il existe un groupe G', et un morphisme de groupes $f : G \to G'$ tels que $H = \ker f$.*

PROPOSITION 2.13. *Il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H, donnée par $K \mapsto \pi^{-1}(K)$.*

THÉORÈME 2.14 (Factorisation par le quotient). *Soit G un groupe, H un sous-groupe distingué, $\pi : G \to G/H$ la projection canonique. Soit $f : G \to G'$ un morphisme de groupes. Alors il existe un morphisme de groupes $f' : G/H \to G'$ tel que $f = f' \circ \pi$ si et seulement si $H \subset \ker f$, et f' est alors unique.*

DÉMONSTRATION. Supposons d'abord qu'une telle factorisation existe. Alors $\ker \pi \subset \ker f$ donc $H \subset \ker f$.

Supposons maintenant que $H \subset \ker f$. Soit $x \in G$, alors $f(x)$ ne dépend que de l'image de x dans G/H, on peut donc définir une fonction $f' : G/H \to G'$ par $f'(\xi) = f(x)$ où x est une représentant de ξ. Alors f' est automatiquement un morphisme de groupes. La factorisation dit que f' est définie de façon unique sur l'image de π, or π est surjective, donc f' est définie de façon unique. □

COROLLAIRE 2.15 (Formule d'isomorphisme). *Soit $f : G \to G'$ un morphisme de groupes. Alors la factorisation précédente induit un isomorphisme $f' : G/(\ker f) \to \mathrm{Im}\, f$.*

Exemple : $\mathrm{GL}_n(k)/\mathrm{SL}_n(k)$ est isomorphe à k^*.

3. Actions de groupes

3.1. Définitions.

DÉFINITION 3.1. *Soit G un groupe et X un ensemble. Une action (à gauche) de G sur X est la donnée d'une application $\cdot : G \times X \to X$ vérifiant les propriétés suivantes :*

(1) pour tout $a, b \in G$ et $x \in X$ on a $a \cdot (b \cdot x) = (ab) \cdot x$

(2) $e \cdot x = x$.

On appelle aussi cela une opération.

PROPOSITION 3.2. *Une action de groupe de G sur X est la même chose qu'un morphisme de groupes de G dans Bij(X), la correspondance étant donnée par $a \mapsto (\phi_a : x \mapsto a \cdot x)$.*

On dit que l'action est fidèle si le morphisme précédent est injectif.
Si $X = \{1, \dots, n\}$, on note $\mathfrak{S}_n$ pour Bij(X).

PROPOSITION 3.3. *On suppose que G agit sur X et X', et que H est un sous-groupe de G. Alors ces actions induisent :*

(1) H agit sur X

(2) G agit sur $X \times X'$

(3) G agit sur $\mathcal{P}(X)$ l'ensemble des parties de X

(4) si $Y \subset X$ vérifie : pour tout $a \in G, x \in Y, a \cdot x \in Y$, alors G agit sur Y

Exemples : Bij(X) agit sur X, $GL_n(k)$ agit sur k^n, mais aussi sur l'ensemble des droites de k^n, l'ensemble des ses sous-espaces vectoriels, l'ensemble de ses bases, $GL_n(k)$ agit sur $M_n(k)$ par conjugaison, $GL_n(k) \times GL_n(k)$ agit sur $M_n(k)$ par $(P, Q) \cdot M = PMQ^{-1}$.

G agit sur lui-même par conjugaison, par translation, il agit par conjugaison sur l'ensemble de ses sous-groupes, et si H est un sous-groupe de G, G agit sur G/H par $g \cdot aH = gaH$.

Le groupe Γ des isométries du plan préservant un triangle équilatéral agit sur l'ensemble des sommets de ce triangle. Cette action est fidèle, et donne un isomorphisme $\Gamma \to \mathfrak{S}_3$.

EXERCICE 4. *Le groupe des isométries préservant un tétraètre régulier est isomorphe à $\mathfrak{S}_4$. Le groupe des isométries directes préservant un cube est isomorphe à $\mathfrak{S}_4$. Le groupe des isométries directes préservant un icosaèdre régulier est isomorphe à $\mathfrak{A}_5$ (difficile !).*

DÉFINITION 3.4. *Le stabilisateur de x, noté G_x ou Stab(x), est l'ensemble $\{g \in G, g \cdot x = x\}$. C'est un sous-groupe de G.*

DÉFINITION 3.5. *L'orbite de x, notée $G \cdot x$, est l'ensemble des $\{g \cdot x, g \in G\}$.*

On note X^G l'ensemble des éléments de X fixés par G.

On définit une relation d'équivalence sur X en posant $x \sim y$ si et seulement si il existe $g \in G$ tel que $g \cdot x = y$. Les orbites sont les classes d'équivalence pour cette relation. Deux éléments équivalents pour cette relation sont dits conjugués. Si $y = g \cdot x$, alors $\mathrm{Stab}(y) = g\mathrm{Stab}(x)g^{-1}$. On dit que l'action est transitive s'il n'y a qu'une seule orbite.

Un exemple : l'action de G sur lui-même par conjugaison. On appelle classe de conjugaison de x son orbite pour cette action. On note $Z(x)$ pour Stab(x) (centralisateur de

x). On note $Z(G)$ le noyau de $G \to \mathrm{Bij}(G)$ donné par cette action (centre de G), c'est aussi G^G.

Action de G sur G/H à gauche par translation : cette action est transitive. Le stabilisateur de H est H, et le stabilisateur de aH est aHa^{-1}.

G agit fidèlement (et transitivement) sur lui-même par translation, d'où un morphisme injective $G \to \mathrm{Bij}(G)$, et $\mathrm{Bij}(G)$ est isomorphe à $\mathfrak{S}_n$ avec $n = |G|$. D'où :

THÉORÈME 3.6 (théorème de Cayley). *Si G est de cardinal n, il s'identifie à un sous-groupe fini de $\mathfrak{S}_n$.*

3.2. La formule des classes.

PROPOSITION 3.7. *L'application $f : G/Stab(x) \to G \cdot x$, $g \mapsto g \cdot x$ est bien définie et est une bijection.*

En particulier, l'orbite de x est finie si et seulement si $\mathrm{Stab}(x)$ est d'indice fini dans G, et alors $|G \cdot x| = [G : \mathrm{Stab}(x)]$. En particulier, le cardinal de l'orbite divise l'ordre de G.

PROPOSITION 3.8 (Formule des classes). *Si X est fini alors $|X| = \sum_{x \in C} [G : Stab(x)]$ où C comprend un représentant de chaque orbite de l'action de G sur X.*

3.3. Le cas des p-groupes. Soit p un nombre premier. Un groupe G est appelé un p-groupe si c'est un groupe fini de cardinal une puissance de p.

THÉORÈME 3.9. *Soit G un p-groupe agissant sur un ensemble fini X. Alors $|X| = |X^G|$ modulo p.*

THÉORÈME 3.10 (Lemme de Cauchy). *Soit G un groupe fini, et p un nombre premier divisant le cardinal de G. Alors il existe un élément dans G d'ordre exactement p.*

DÉMONSTRATION. Soit $X = \{(x_1, \dots, x_p) \in G^p, x_1 \dots x_p = e\}$. Alors X est un ensemble de cardinal $|G|^{p-1}$: en effet, pour tout $x_1, \dots, x_{p-1} \in G^{p-1}$, il existe un unique x_p qui complète le p-uplet en un élément de X. En particulier, $p||X|$.

Le p-groupe $\mathbb{Z}/p\mathbb{Z}$ agit sur X par $(j, (x_1, \dots, x_p)) \mapsto (x_{1+j}, \dots, x_{p+j})$, les indices étant pris modulo p. Pour cette action, on a $X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, \dots, x), x = e$ ou x est d'ordre exactement $p\}$. Comme $p||X^{\mathbb{Z}/p\mathbb{Z}}|$, il existe bien au moins un x d'ordre exactement p. □

THÉORÈME 3.11. *Soit G un p-groupe. Alors $Z(G)$ est non trivial.*

DÉMONSTRATION. On regarde l'action de G sur lui-même par conjugaison. Comme G est un p-groupe, on a $|G| = |G^G|$ modulo p, donc p divise $|G^G| = |Z(G)|$. Comme $|Z(G)|$ n'est pas l'ensemble vide (il contient l'élément neutre), c'est que $Z(G)$ contient au moins p éléments. □

EXERCICE 5. *Un groupe d'ordre p^2 est abélien.*

3.4. Les théorèmes de Sylow. Soit p un nombre premier, et G un groupe fini. Si le cardinal de G est de la forme $n = p^a m$, avec m premier à p, on dit qu'un sous-groupe H de G est un p-Sylow de G si son cardinal est p^a. De façon équivalence, H est un p-Sylow de G si H est un p-groupe et p ne divise pas $[G : H]$.

THÉORÈME 3.12. *Soit G un groupe fini. Alors :*

(1) G admet au moins un p-Sylow.

(2) tous les p-Sylow de G sont conjugués.

(3) soit $n_p(G)$ le nombre de p-Sylow de G, alors $n_p(G)$ divise l'ordre de G, et $n_p(G) = 1$ modulo p.

La preuve repose sur les deux résultats suivants :

Proposition 3.13. *Soit G un groupe fini, P un p-Sylow de G, H un sous-groupe de G. Alors il existe $a \in G$ tel que $aPa^{-1} \cap H$ est un p-Sylow de H.*

et :

Lemme 3.14. *Tout groupe fini G peut-être plongé dans un groupe fini admettant un p-Sylow.*

Preuve de la proposition 3.13. On fait agir H par translation à gauche sur G/P. Le stabilisateur de aP est $aPa^{-1} \cap H$. Le cardinal de l'orbite de aP est donc $|H|/|aPa^{-1} \cap H|$. Toutes les orbites ne peuvent être de cardinal divisible par p, sinon p diviserait $|G/P|$ ce qui n'est pas le cas. Il existe donc a tel que p ne divise pas $|H|/|aPa^{-1} \cap H|$, ce qui dit exactement que $aPa^{-1} \cap H$ est un p-Sylow de H. □

En appliquant ceci à $H = P$ un p-Sylow de G, on en déduit que tous les p-Sylow de G sont conjugués. Supposons que G admette au moins un p-Sylow, alors $n_p(G)$ est le cardinal de l'orbite de l'action de G sur ses p-Sylow par conjugaison, donc divise $|G|$.

Preuve du lemme 3.14. On sait que G s'injecte dans $\mathfrak{S}_n$, où n est l'ordre de G. Il suffit donc de montrer que $\mathfrak{S}_n$ admet un p-Sylow. Pour cela on utilise :

Proposition 3.15. *Pour tout corps k, il existe un plongement de $\mathfrak{S}_n$ dans $GL_n(k)$.*

Ce plongement est donné par $\sigma \mapsto u_\sigma$, où u_σ est l'application linéaire définie par son action sur la base canonique : $u_\sigma(e_i) = e_{\sigma(i)}$.

Choisissons maintenant $k = \mathbb{Z}/p\mathbb{Z}$, alors $GL_n(\mathbb{Z}/p\mathbb{Z})$ admet un p-Sylow, en effet il est d'ordre $p^{n(n-1)/2} \prod_{i=1}^{n} (p^i - 1)$, et contient comme sous-groupe l'ensemble U des matrices triangulaires supérieures avec des 1 sur la diagonale, de cardinal $p^{n(n-1)/2}$. □

Reste à prouver le dernier point sur $n_p(G)$. Soit P un p-Sylow de G, on le fait agir sur l'ensemble X des p-Sylow de G par conjugaison. Alors $n_p(G) = |X|$ est congru à $|X^P|$ modulo p. Reste à voir que le seul point fixe de cette action est P. Soit donc Q un p-Sylow fixé par l'action de P par conjugaison. Soit H le sous-groupe engendré par P et Q, alors P et Q sont des p-Sylow de H. Par ailleurs Q est distingué dans H, donc c'est le seul p-Sylow de H, donc $P = Q$.

Corollaire 3.16 (Corollaire de la proposition 3.13). *Soit H un sous-groupe de G qui est un p-groupe, alors H est contenu dans un p-Sylow de G.*

4. Le groupe symétrique

On note $\mathfrak{S}_n$ le groupe des bijections de l'ensemble $\{1, \ldots, n\}$ vers lui-même, muni de la composition. $\mathfrak{S}_n$ est de cardinal $n!$.

4.1. Cycles et classes de conjugaison. Un cycle de longueur r, ou r-cycle, est une permutation de la forme suivante : soit $i_1, \dots, i_r$ des éléments distincts de $\{1, \dots, n\}$, alors $\sigma(i_j) = i_{j+1}$ si $j < r$ et $\sigma(i_r) = i_1$, et les autres éléments de $\{1, \dots, n\}$ sont fixés par σ. On note cette permutation $[i_1 \dots i_r]$ ou $(i_1 \dots i_r)$. L'ensemble $\{i_1, \dots, i_r\}$ est appelé le support du cycle. Deux cycles à support disjoint commutent entre eux. On appelle transposition un 2-cycle.

THÉORÈME 4.1. *Une permutation σ s'écrit de façon unique (à l'ordre près) comme produit de cycles à supports disjoints.*

ESQUISSE DE DÉMONSTRATION. Soit H le sous-groupe de $\mathfrak{S}_n$ engendré par σ. On écrit $\{1, \dots, n\} = \sqcup_{j=1}^{s} X_j$ la décomposition en orbites. Le groupe H envoie donc chaque X_j vers lui-même. Fixons $i_1 \in X_j$, alors les autres éléments de X_j sont de la forme $\sigma^k(i_1)$, et les $\sigma^k(i_1)$ sont distincts pour $0 \leq k < r$ où r est le cardinal de X_j. On note $\sigma^k(i_1) = i_{k+1}$, alors σ agit sur X_j comme le cycle $[i_1 \dots i_r]$. Ce qui donne l'écriture de σ comme produit de cycles à supports disjoints.

Réciproquement, si on écrit σ comme produit de cycles à supports disjoints, alors les supports des cycles sont exactement les orbites sous l'action de H, ce qui prouve l'unicité. □

COROLLAIRE 4.2. *Les transpositions engendrent $\mathfrak{S}_n$, et tout $\sigma \in \mathfrak{S}_n$ peut s'écrire comme le produit d'au plus $n-1$ transpositions.*

DÉMONSTRATION. Il suffit de prouver que chaque cycle $[i_1 \dots i_r]$ est produit de transpositions. Or $[i_1 \dots i_r] = [i_1 i_2] \dots [i_{r-1} i_r]$. □

PROPOSITION 4.3. *L'ordre d'une permutation σ est le ppcm des cardinaux des supports des cycles à supports disjoints apparaissant dans σ.*

PROPOSITION 4.4. *Soit $\sigma = [i_1 \dots i_r]$ un cycle, et $\tau \in \mathfrak{S}_n$. Alors $\tau\sigma\tau^{-1} = [\tau(i_1) \dots \tau(i_r)]$*

COROLLAIRE 4.5. *$Z(\mathfrak{S}_n) = \{Id\}$ si $n > 2$, et $\mathfrak{S}_n$ est commutatif si $n \leq 2$.*

DÉMONSTRATION. Soit $n > 2$, et $\sigma \in \mathfrak{S}_n$, $\sigma \neq \mathrm{Id}$. Trouvons τ tel que $\tau\sigma\tau^{-1} \neq \sigma$. Supposons d'abord que σ contienne dans sa décomposition en cycles un cycle $[i_1 \dots i_r]$ avec $r > 2$. Posons alors $\tau = [i_1 i_2]$. Si ce n'est pas le cas, alors σ contient dans sa décomposition en cycles deux cyles distincts, disons $[i_1 \dots i_r]$ et $[j_1 \dots j_s]$, avec $r > 1$. On pose alors $\tau = [i_1 j_1]$. □

On appelle partition de l'entier n la donnée d'entiers > 0 $k_1 \geq \dots \geq k_s$ tels que $n = k_1 + \dots + k_s$. Soit $\sigma \in \mathfrak{S}_n$, on lui associe une partition de n par les longueurs des cycles à supports disjoints qui interviennent, rangées par ordres décroissants.

THÉORÈME 4.6. *L'application ainsi définie induit une bijection entre les classes de conjugaison de $\mathfrak{S}_n$ et les partitions de n.*

4.2. Signature et groupe alterné.

THÉORÈME 4.7. *Il existe un unique morphisme de groupes non trivial $\mathfrak{S}_n \to \mathbb{C}^*$. Son image est égale à $\{1, -1\}$, on l'appelle signature et on le note ε.*

DÉMONSTRATION. On commence par montrer qu'il existe au plus un tel morphisme et que son image est alors $\{1, -1\}$. Soit $\tau = [12]$ une transposition. Alors $\varepsilon(\tau)^2 = \varepsilon(\tau^2) = 1$, donc $\varepsilon(\tau) = \pm 1$. D'autre part, toutes les transpositions sont conjuguées, donc elles

ont toutes même image par ε. De plus, les transpositions engendrent $\mathfrak{S}_n$, donc ε est entièrement déterminé par $\varepsilon(\tau)$. Si $\varepsilon(\tau) = 1$, alors ε est le morphisme trivial. Si $\varepsilon(\tau) = -1$, alors l'image de ε est $\{1, -1\}$.

Reste à montrer l'existence d'un ε tel que $\varepsilon(\tau) = -1$. On pose $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$.

Ensuite, ε est non trivial. Posons $\sigma = (12)$ et calculons $\varepsilon(\sigma)$: pour toute paire $\{i, j\} \neq \{1, 2\}$ la quantité $\frac{\sigma(i)-\sigma(j)}{i-j}$ est > 0, et $\frac{\sigma(2)-\sigma(1)}{2-1} < 0$, donc $\varepsilon(\sigma) < 0$.

Enfin, c'est un morphisme de groupes. Calculons $\varepsilon(\sigma\tau)$. C'est $\prod_{i>j} \frac{\sigma\tau(i)-\sigma\tau(j)}{i-j}$ qui vaut $\prod_{i<j} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)} \prod_{i<j} \frac{\tau(i)-\tau(j)}{i-j}$. D'autre part $\prod_{i<j} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)} = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$, d'où finalement $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. □

PROPOSITION 4.8. *La signature vérifie les propriétés suivantes :*

(1) si σ est un r-cycle, alors $\varepsilon(\sigma) = (-1)^{r+1}$

(2) si σ s'écrit comme produit de k transpositions, alors $\varepsilon(\sigma) = (-1)^k$.

DÉFINITION 4.9. *On appelle groupe alterné, et on note $\mathfrak{A}_n$, le noyau de ε.*

PROPOSITION 4.10. *C'est un sous-groupe distingué de $\mathfrak{S}_n$, et son unique sous-groupe d'indice 2.*

DÉMONSTRATION. C'est un sous-groupe distingué comme noyau d'un morphisme. Il est d'indice 2 car ε induit un isomorphsme $\mathfrak{S}_n/\mathfrak{A}_n \to \operatorname{Im}\varepsilon$ et $\operatorname{Im}\varepsilon$ est de cardinal 2. Soit H un sous-groupe d'indice 2 de $\mathfrak{S}_n$, alors il est distingué, donc induit un morphisme $\psi : \mathfrak{S}_n \to \mathfrak{S}_n/H$ surjectif. Comme $\mathfrak{S}_n/H$ est canoniquement isomorphe au groupe $\{1, -1\}$, on en déduit que $\psi = \varepsilon$ par unicité du morphisme signature, donc $H = \mathfrak{A}_n$. □

EXERCICE 6. *$\mathfrak{A}_n$ est engendré par les 3-cycles. On utilisera que $\mathfrak{A}_n$ est formé des éléments qui sont produit d'un nombre pair de transpositions.*

THÉORÈME 4.11. *Si $n \geq 5$, alors $\mathfrak{A}_n$ est simple.*

5. Représentations linéaires des groupes finis

Dans tout ce chapitre, G est un groupe fini. On fixe un corps K (après quelques définitions initiales on prendra $K = \mathbb{C}$).

5.1. Représentations, sous-représentations, morphismes.

5.1.1. *Définition.* On a deux définitions équivalentes :

DÉFINITION 5.1. *Une représentation linéaire de G est la donnée d'un K-espace vectoriel de dimension finie G, et d'une action de G sur V telle que pour tout g, l'application $V \to V$, $x \mapsto g \cdot x$ soit K-linéaire.*

DÉFINITION 5.2. *Une représentation linéaire de G est la donnée de (ρ, V), où V est un K-espace vectoriel de dimension finie, appelé espace sous-jacent de la représentation, et ρ un morphisme de groupes $G \to GL(V)$. On abrégera parfois en ρ ou V au lieu de (ρ, V). On notera aussi $g \cdot v$ pour $\rho(g)(v)$. On appelle degré de la représentation la dimension de V.*

La première définition revient à se donner un morphisme de groupes $G \to \mathrm{Bij}(V)$ tel que l'image soit contenue dans $\mathrm{GL}(V)$.

On dit que la représentation est fidèle si ρ est injectif.

5.1.2. *Construction de représentations.* Soit $\phi : G \to K^*$ un morphisme de groupes, alors ϕ définit une représentation de dimension 1 de G, donnée par $\psi(g) \in GL_1(K) = K^*$. Lorsque ψ est le morphisme trivial, on obtient la représentation triviale de G, notée $\mathbf{1}$.

Soit $\psi : G \to K^*$ un morphisme de groupes, et (ρ, V) une représentation. On définit la représentation tordue par ψ $(\rho(\psi), V(\psi))$, d'espace sous-jacent V, définie par $g \mapsto \psi(g)\rho(g)$.

Soit (ρ, V) et (ρ', V') deux représentations du groupe G. On petu définir la représentation somme $(\rho \oplus \rho', V \oplus V')$, d'espace sous-jacent $V \oplus V'$, et où $r = \rho \oplus \rho'$ est donné par l'inclusion de $GL(V) \times GL(V') \to GL(V \oplus V')$.

On définit aussi une représentation $\mathrm{Hom}(V, V')$ en faisant agir G sur $f : V \to V'$ par $(g \cdot f) = g \cdot (f(g^{-1} \cdot x))$. Lorsque $V' = \mathbf{1}$ on note V^* la représentation obtenue, appelée représentation duale de V.

Si G agit sur un ensemble fini X, on définit la représentation de permutation associée à X : on pose $V_X = \oplus_{x \in X} \mathbb{C}e_x$, et on définit $\rho_X(g)(e_x) = e_{g \cdot x}$. Lorsque X est G muni de son action de translation à gauche, on appelle cette représentation la représentation régulière. Si l'action de G sur X est fidèle, la représentation associée l'est aussi. On retrouve l'inclusion $\mathfrak{S}_n \to \mathrm{GL}_n(k)$ définie précédemment.

Définition 5.3. *Un sous-espace stable par G de la représentation (ρ, V) est un sous-espace vectoriel W de V tel que $\rho(g)(W) \subset W$ pour tout $g \in G$. On dit alors que $(\rho_{|W}, W)$ est une sous-représentation de V.*

On note V^G l'ensemble $\{v \in V, g \cdot v = v \forall g \in G\}$. C'est l'espace des invariants de la représentation, c'est une sous-représentation de V.

Exemple : soit (ρ, k^n) la représentation de permutation associée à l'action de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$. La droite $D = k(e_1 + \cdots + e_n)$ est un sous-espace stable. L'hyperplan $H_n = \{x = \sum x_i e_i, \sum x_i = 0\} = \langle e_i - e_j, 1 \leq i, j \leq n \rangle$ est un sous-espace stable (on l'appelle la représentation standard de $\mathfrak{S}_n$).

5.1.3. *Morphismes de représentations.*

Définition 5.4. *Soit (ρ, V) et (σ, W) deux représentations de G. Un morphisme de représentations de V vers W est une application linéaire $f : V \to W$ telle que pour tout $g \in G$, pour tout $x \in V$ on a $g \cdot f(x) = f(g \cdot x)$. On note $\mathrm{Hom}_G(V, W)$ le $\mathbb{C}$-espace vectoriel des morphismes de représentations de V vers W. On dit aussi que f est G-équivariante.*

Un isomorphisme de représentations est un morphisme de représentations qui est un isomorphisme d'espaces vectoriels.

Proposition 5.5. *Soit ρ et ρ' deux représentations isomorphes du groupe G. Alors il existe $u : V \to V'$ linéaire inversible telle que $\rho'(g) = u \circ \rho(g) \circ u^{-1}$ pour tout $g \in G$.*

Proposition 5.6. $\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G$.

Démonstration. Soit $f \in \mathrm{Hom}(V, W)$. Alors $f \in \mathrm{Hom}(V, W)^G$ si et seulement si pour tout $g \in G$ et pour tout $x \in V$ on a $(g \cdot f)(x) = f(x)$, c'est-à-dire $g \cdot f(g^{-1} \cdot x) = x$, c'est-à-dire $f(g^{-1} \cdot x) = g^{-1} \cdot x$ pour tout $g \in G$, $x \in V$, ce qui est bien équivalent à dire que f est G-équivariant. □

5.1.4. *Sous-espaces stables.* **À partir de maintenant on suppose $K = \mathbb{C}$.**

Théorème 5.7. *Tout sous-espace stable par G admet un supplémentaire stable.*

Exemple : H_n est un supplémentaire de D (en caractéristique 0 seulement !).

Corollaire 5.8. *Soit W un sous-espace stable et U un supplémentaire stable. Alors (ρ, V) est isomorphe à $(\rho_{|W}, W) \oplus (\rho_{|U}, U)$.*

Définition 5.9. *Un produit scalaire hermitien invariant par G sur V est la donnée d'un produit scalaire hermitien $(,)$ tel que $(g \cdot v, g \cdot w) = (v, w)$ pour tous $v, w \in V$.*

Proposition 5.10. *Il existe un produit scalaire hermitien invariant par G sur V.*

Démonstration. Soit $[,]$ un produit scalaire hermitien quelconque. On pose $(v, w) = \sum_{g\in G}(g \cdot v, g \cdot w)$. □

Première preuve du théorème 5.7. Fixons un produit scalaire hermitien invariant par G sur V. Comme W est stable par G, alors $W^\perp$ aussi, on a donc trouvé un supplémentaire stable. □

Deuxième preuve du théorème 5.7. Soit p un projecteur quelconque d'image W. On pose $\pi = \frac{1}{|G|}\sum_{g\in G} \rho(g) \circ p \circ \rho(g)^{-1}$. Alors π est un projecteur G-équivariant d'image W, et son noyau fournit le supplémentaire cherché. En effet : il est clair que $\rho(g)\circ\pi = \pi\circ\rho(g)$ pour tout g. De plus $\pi\circ p = p$. D'où $\pi\circ\pi = \frac{1}{|G|}\sum_{g\in G} \pi\circ\rho(g)\circ p\circ\rho(g)^{-1} = \frac{1}{|G|}\sum_{g\in G} \rho(g) \circ \pi \circ p \circ \rho(g)^{-1} = \pi$. De plus, W est contenu dans l'image de π, et enfin π et p ont même rang puisque même trace, donc $\operatorname{Im} p = \operatorname{Im} \pi = W$. □

Proposition 5.11. *Soit $\pi_G = \frac{1}{|G|}\sum_{g\in G} \rho(g)$. Alors π_G est un projecteur sur V^G et il définit un morphisme G-équivariant $V \to V^G$.*

Démonstration. On vérifie facilement que $\pi_G^2 = \pi_G$. On a $\rho(g) \circ \pi_G = \pi_G$, donc l'image de π_G est contenue dans V^G, et clairement $\pi_G(x) = x$ pour tout $x \in V^G$ donc l'image de π_G est V^G. La formule $\pi_G \circ \rho(g) = \pi_G$ s'interprète alors en disant que π_G est G-équivariant de V sur V^G (sur lequel G agit trivialement). □

5.1.5. *Représentations irréductibles.*

Définition 5.12. *Une représentation est dite irréductible si elle n'a pas de sous-espace stable non trivial, c'est-à-dire différent de $\{0\}$ et V.*

On note $\mathcal{I}_G$ l'ensemble des classes d'isomorphismes de représentations irréductibles de G.

Proposition 5.13. *H_n est une représentation irréductible de $\mathfrak{S}_n$.*

Démonstration. Il suffit de montrer que si $x \in H_n$, $x \neq 0$, alors le sous-espace vectoriel V_x de H_n engendré par les $\sigma \cdot x$ est H_n entier. Soit donc un tel x, $x = \sum x_i e_i$. Il existe i et j tels que $x_i \neq x_j$. On pose $\tau = (ij)$, alors $x - \tau \cdot x = (x_i - x_j)(e_i - e_j)$, donc $e_i - e_j \in V_x$. Soit $k, \ell \in \{1, \dots, n\}$, et σ tel que $\sigma(i) = k$ et $\sigma(j) = \ell$, on a $\sigma \cdot (e_i - e_j) = e_k - e_\ell$, ce qui montre que $V_x = H_n$. □

Théorème 5.14 (Lemme de Maschke). *Toute représentation est somme directe de sous-représentations irréductibles.*

Exemple : $\mathbb{C}^n$ est isomorphe à $\mathbf{1} \oplus H_n$.

Démonstration. La preuve se fait par récurrence sur le degré de la représentation : si elle n'est pas irréductible, il existe une décomposition non triviale $V = U \oplus W$ en sous-représentations, qui sont sommes de représentations irréductibles par hypothèses de récurrence. □

Remarquons que la décomposition n'est pas unique (prendre par exemple V avec l'action triviale de G, n'importe quelle décomposition de V en somme directe de droites convient).

Théorème 5.15 (Lemme de Schur). *Soit V et W deux représentations irréductibles. Alors soit $\mathrm{Hom}_G(V,W) = \mathbb{C}$, si V et W sont isomorphes, soit $\mathrm{Hom}_G(V,W) = \{0\}$.*

Démonstration. Soit $f \in \mathrm{Hom}_G(V,W)$. Si f n'est pas nulle, alors f est un isomorphisme. En effet, comme f est G-équivariante, $\ker f$ et $\mathrm{Im}\, f$ sont des sous-espaces stables par G. L'irréductibilité de V et W dit alors que ces espaces sont nuls ou V ou W tout entier. Donc : si $\mathrm{Hom}_G(V,W) \neq 0$, alors V et W sont isomorphes. Supposons maintenant V et W' isomorphes, alors on peut supposer $W = V$. Soit $f \in \mathrm{Hom}_G(V,V)$, alors $f - \lambda\,\mathrm{Id}$ est aussi G-équivariant pour tout λ. Choisissons λ une valeur propre de f, on voit qu'alors $f = \lambda\,\mathrm{Id}$ par le même raisonnement. □

Proposition 5.16. *Si G est abélien, toute représentation irréductible est de dimension 1.*

Démonstration. Soit V une représentation de G, de dimension > 1. Si pour tout $g \in G$, $\rho(g)$ est une homothétie, alors V n'est pas irréductible : n'importe quel sous-espace de V est stable par G. Sinon, soit g tel que $\rho(g)$ n'est pas une homothétie, et λ une valeur propre de $\rho(g)$. Posons $W = \ker(\rho(g) - \lambda\,\mathrm{Id})$. C'est un sous-espace stable par G car G est abélien. Il est non trivial car λ est une valeur propre de $\rho(g)$ et $\rho(g)$ n'est pas une homothétie. □

5.1.6. *Critère d'isomorphisme.* Soit V une représentation de G. On suppose V isomorphe à $\oplus_i V_i$, avec V_i irréductible. Soit $W \in \mathcal{I}_G$. On note $n_W = |\{i, V_i \simeq W\}|$.

Proposition 5.17. *Deux représentations V et V' sont isomorphes si et seulement si $n_W = n'_W$ pour tout $W \in \mathcal{I}_G$. En particulier, n_W ne dépend pas de la décomposition choisie.*

Démonstration. Soit $f : V \to V'$ un isomorphisme. Soit $V_W = \oplus_{i, V_i \simeq W} V_i$. Le lemme de Schur dit que $f(V_W) \subset V'_W$, et si $f_{|V_W}$ est un isomorphisme alors ces deux espaces ont même dimension $n_W \dim W = n'_W \dim W$ et donc $n_W = n'_W$. □

5.2. Caractères et fonctions centrales.

5.2.1. *Caractères.*

Définition 5.18. *Soit V une représentation de G. On appelle caractère de V la fonction $\chi_V : G \to \mathbb{C}$, $g \mapsto \mathrm{tr}\, \rho_V(g)$.*

Proposition 5.19. *Si deux représentations sont isomorphes, elles ont même caractère.*

Démonstration. Soit $\rho, \rho' : G \to \mathrm{GL}_n(\mathbb{C})$ isomorphes. Il existe donc $A \in \mathrm{GL}_n(\mathbb{C})$ tel que $A\rho(g)A^{-1} = \rho'(g)$ pour tout $g \in G$, d'où l'égalité des caractères. □

Lorsque V est de dimension 1, le caractère de la représentation se confond avec la représentation elle-même. On dit que χ_V est un caractère linéaire.

PROPOSITION 5.20. *Pour tout $g \in G$, on a $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.*

DÉMONSTRATION. Soit $\lambda_1, \ldots, \lambda_n$ les valeurs propres de $\rho(g)$, de sorte que $\chi_V(g) = \sum \lambda_i$. Chaque λ_i est un complexe de module 1, puisque $g^{|G|} = e$ donc $\rho(g)$ est annulé par le polynôme $X^{|G|} - 1$, les valeurs propres de $\rho(g)$ sont donc parmi les racines de ce polynôme, donc des racines de l'unité. En particulier, $\lambda_i^{-1} = \overline{\lambda_i}$, et $\chi_V(g^{-1}) = \sum \lambda_i^{-1} = \sum \overline{\lambda_i} = \overline{\chi_V(g)}$. □

Nous avons prouvé au passage :

PROPOSITION 5.21. *$\rho(g)$ est diagonalisable pour tout g.*

PROPOSITION 5.22. *$\chi_{V\oplus W} = \chi_V + \chi_W$. $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$. $\chi_{V^*} = \overline{\chi_V}$.*

DÉMONSTRATION. On prouve la formule pour $\mathrm{Hom}(V, W)$. Soit $g \in G$, on fixe une base (e_i) de V et une base (f_j) de W qui sont des bases de diagonalisations de g de valeurs propres (λ_i) et (μ_j) respectivement. On note $(u_{i,j})$ la base de $\mathrm{Hom}(V, W)$ telle que $u_{i,j}(e_k) = 0$ si $i \neq k$, et f_j si $i = k$. Alors c'est une base de diagonalisation de g sur $\mathrm{Hom}(V, W)$, de valeurs propres $\lambda_i^{-1}\mu_j$, ce qui donne le résultat. □

PROPOSITION 5.23. $\dim V^G = \frac{1}{|G|} \sum_{g\in G} \chi_V(g)$.

DÉMONSTRATION. On a $\dim V^G = \mathrm{tr}\, \pi_G$, or $\pi_G = \frac{1}{|G|} \sum_{g\in G} \rho_V(g)$. □

PROPOSITION 5.24. *Soit (ρ_X, V_X) la représentation de permutation associée à l'action de G sur un ensemble fini X. $\chi_X(g)$ est le nombre de points fixes de l'action de g sur X.*

5.2.2. *Fonctions centrales.*

DÉFINITION 5.25. *Une fonction centrale sur G est une fonction $f : G \to \mathbb{C}$ telle que pour tous $g, h \in G$ on a $f(gh) = f(hg)$, ou de façon équivalente $f(ghg^{-1}) = f(h)$. On note $R(G)$ l'espace des fonctions centrales sur G.*

$R(G)$ est un espace vectoriel de dimension le nombre de classes de conjugaison de G. Tout caractère d'une représentation est une fonction centrale. Remarquons que si une fonction centrale est un caractère, son conjugué aussi (en regardant la représentation duale).

On définit un produit scalaire hermitien sur $R(G)$ par :

$$\langle u, v\rangle = \frac{1}{|G|} \sum_{g\in G} \overline{u(g)}v(g)$$

PROPOSITION 5.26. *Soit V et W des représentations de G, alors $\langle \chi_W, \chi_V\rangle = \dim \mathrm{Hom}_G(W, V)$. Si V et W sont irréductibles, alors $\langle \chi_W, \chi_V\rangle = 1$ si V et W sont isomorphes et 0 sinon. En particulier, la famille des $(\chi_V)_{V\in\mathcal{I}_G}$ forme une partie libre de $R(G)$.*

DÉMONSTRATION. On a $\mathrm{Hom}_G(W, V) = \mathrm{Hom}(W, V)^G$, donc $\dim \mathrm{Hom}_G(W, V) = \frac{1}{|G|} \sum_g \chi_{\mathrm{Hom}(W,V)}(g) = \frac{1}{|G|} \sum_g \overline{\chi_W(g)}\chi_V(g) = \langle W, V\rangle$. □

5.2.3. *Décomposition de représentations.*

PROPOSITION 5.27. *Soit V une représentation de G, et $V = \oplus_i V_i$ une décomposition de V en somme directe de représentations irréductibles. Soit W une représentation irréductible de G. Alors le nombre n_W de V_i qui sont isomorphes à W vaut $\langle \chi_W, \chi_V \rangle$.*

COROLLAIRE 5.28. *Si deux représentations ont même caractère, elles sont isomorphes.*

COROLLAIRE 5.29. *Soit n_W la multiplicité de $W \in \mathcal{I}_G$ dans V. Alors $\langle \chi_V, \chi_V \rangle = \sum_{W \in \mathcal{I}} n_W^2$. En particulier, V est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.*

On appelle caractère irréductible le caractère d'une représentation irréductible. Alors le conjugué d'un caractère irréductible est un caractère irréductible.

Prenons l'exemple de la représentation régulière gauche V_G de G sur lui-même.

PROPOSITION 5.30. *Soit $W \in \mathcal{I}_G$, alors W apparaît dans V_G avec multiplicité* $\dim W$. *En particulier, $\sum_{W \in \mathcal{I}_G} (\dim W)^2 = |G|$.*

DÉMONSTRATION. Calculons $\langle \chi_W, \chi_{V_G} \rangle = \frac{1}{|G|} \sum_g \overline{\chi_W(g)} \chi_{V_G}(g) = \frac{1}{|G|} \overline{\chi_W(1)} \chi_{V_G}(1) = \dim W$, puisque g agit sans point fixe sur V_G pour $g \neq 1$ donc $\chi_{V_G}(g) = 0$ si $g \neq 1$. □

5.2.4. *Base de $R(G)$.*

THÉORÈME 5.31. *La famille des $\{\chi_V\}$ pour V parcourant $\mathcal{I}_G$ est une base orthonormée de $R(G)$.*

COROLLAIRE 5.32. *Le cardinal de $\mathcal{I}_G$ est le nombre de classes de conjugaison de G.*

DÉMONSTRATION. On sait déjà que c'est une famille orthonormée. Reste à voir qu'elle est génératrice.

Soit $\alpha \in R(G)$ tel que $\langle \alpha, \chi_V \rangle = 0$ pour toute représentation irréductible V. Pour toute représentation (ρ, V) de G, on peut définir $f_{V,\alpha} : V \to V$ par la formule $f_{V,\alpha} = \sum_g \overline{\alpha(g)} \rho(g)$. Alors $f_{V,\alpha}$ est G-équivariante : en effet, $\rho(g) \circ f_{V,\alpha} = \sum_h \overline{\alpha(g^{-1}h)} \rho(h)$, et $f_{V,\alpha} \circ \rho(g) = \sum_h \overline{\alpha(hg^{-1})} \rho(h)$. Les deux quantités sont égales car α est une fonction centrale.

Supposons maintenant que V est irréductible, alors $f_{V,\alpha}$ est une homothétie par le lemme de Schur. Par ailleurs, $\mathrm{tr}(f) = |G| \langle \alpha, \chi_V \rangle = 0$ donc $f_{V,\alpha} = 0$. On en déduit que $f_{V,\alpha}$ est nul pour tout V, puisque toute représentation est somme de représentations irréductibles. On applique cela à la représentation régulière, alors $f_{V,\alpha}(e_1) = \sum_g \overline{\alpha(g)} e_g = 0$ ce qui donne $\alpha(g) = 0$ pour tout $g \in G$. □

5.3. Table des caractères.

5.3.1. *Définition.* La table de caractères d'un groupe fini G est un tableau donnant la valeur des caractères des représentations irréductibles de G. Les lignes du tableau sont indexées par les représentations irréductibles, et les colonnes par les classes de conjugaison $(\mathcal{C}_i)$ dans G, données par un de leur représentant (puisque les caractères sont des fonctions centrales). C'est donc un tableau carré, et la case en position (i, j) contient $\chi_i(\mathcal{C}_j)$.

On met en première ligne le caractère trivial, et en première colonne la classe de conjugaison de l'élément neutre. On écrit parfois le cardinal de chaque classe de conjugaison au-dessus de la description de la classe.

5.3.2. *Propriétés.* On lit sur la colonne de la classe de conjugaison de 1 la dimension de la représentation, puisque $\chi_V(1) = \dim V$.

La somme des carrés des dimensions des représentations fait $|G|$.

Notons X la matrice des $\chi_i(\mathcal{C}_j)$, et K la matrice diagonale ayant pour coefficients les $k_i = |\mathcal{C}_i|$.

PROPOSITION 5.33. *On a* $\overline{X}K{}^tX = |G|\,\mathrm{Id}$, *et* ${}^tX\overline{X} = |G|K^{-1}$.

DÉMONSTRATION. La première égalité est une réécriture du fait que les caractères irréductibles forment une famille orthonormée. La deuxième suit formellement. □

COROLLAIRE 5.34. *Les colonnes sont orthogonales pour le produit scalaire hermitien usuel, et la norme de la colonne associée à* $\mathcal{C}_i$ *est* $|G|/k_i$.

5.3.3. *Exemple : le cas de* $\mathfrak{S}_3$. C'est un tableau 3×3. Les classes de conjugaison sont celles de Id (cardinal 1), (12) (cardinal 3), et (123) (cardinal 2).

On connaît déjà trois représentations irréductibles de $\mathfrak{S}_3$: $\mathbf{1}$, ε, et H_3. D'où la table :

	1	3	2
	Id	(12)	(123)
$\mathbf{1}$	1	1	1
ε	1	-1	1
H_3	2	0	-1

5.3.4. *Exemple : le cas de* $\mathfrak{S}_4$. On a 5 classes de conjugaison : Id (cardinal 1), (12) (cardinal 6), (123) (cardinal 8), (12)(34) (cardinal 3), et (1234) (cardinal 6).

On commence par mettre dans le tableau la représentation triviale, la signature et H_4. On observe ensuite que $H_4(\varepsilon)$ est différent de H_4, on le rajoute encore dans le tableau. Il manque une représentation, de dimension n vérifiant $1 + 1 + 9 + 9 + n^2 = 24$ ce qui nous donne $n = 2$. On peut compléter par orthogonalité des colonnes, ou bien utiliser le fait que $\mathfrak{S}_4/V$ est isomorphe à $\mathfrak{S}_3$, où V est le sous-groupe de cardinal 4 contenant les produits de deux transpositions à supports disjoints. Donc toute représentation irréductible de $\mathfrak{S}_3$ donne une représentation irréductible de $\mathfrak{S}_4$, et la représentation cherchée provient de H_3.

	1	6	8	3	6
	Id	(12)	(123)	(12)(34)	(1234)
$\mathbf{1}$	1	1	1	1	1
ε	1	-1	1	1	-1
H_4	3	1	0	-1	-1
$H_4(\varepsilon)$	3	-1	0	-1	1
H_3	2	0	-1	2	0

CHAPITRE 2

Anneaux

1. Généralités

1.1. Définitions.

DÉFINITION 1.1. *Un anneau est la donnée de $(A, +, \star, 0_A, 1_A)$, où :*

(1) $(A, +, 0_A)$ est un groupe abélien (on appelle + l'addition de A)

(2) $\star$ est une loi de composition interne associative $A \times A \to A$ (on appelle $\star$ la multiplication de A)

(3) 1_A est un élément de A tel que pour tout $a \in A$, on a $a \star 1_A = 1_A \star a = a$ (c'est l'unité de A).

(4) pour tout $a \in A$, on a $0_A \star a = a \star 0_A = 0_A$.

(5) la multiplication est distributive par rapport à l'addition : pour tous a, b, c on a $a \star (b + c) = a \star b + a \star c$, et $(a + b) \star c = a \star c + b \star c$.

On appelle opposé de $a \in A$ son inverse pour +, et on le note $-a$. On a $-a = (-1) \star a$.

On dit que A est commutatif si $\star$ est commutative.

Exemples d'anneaux : $\mathbb{Z}$, $\mathbb{C}[X]$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}$, $M_n(\mathbb{C})$, l'anneau nul (l'unique anneau tel que $0_A = 1_A$).

DÉFINITION 1.2. *Un sous-anneau de $(A, +, \star, 0_A, 1_A)$ est une partie A' de A avec $0_A \in A$ et $1_A \in A$ et $(A', +, \star, 0_A, 1_A)$ est un anneau.*

DÉFINITION 1.3. *Soit $(A, +, \star, 0_A, 1_A)$ et $(B, +, \star, 0_B, 1_B)$ deux anneaux. Un morphisme d'anneau est une application $f : A \to B$ vérifiant :*

(1) $f(0_A) = 0_B$ et $f(1_A) = 1_B$

(2) pour tous $a, b \in A$, $f(a + b) = f(a) + f(b)$ et $f(a \star b) = f(a) \star f(b)$.

On appelle noyau de f, et on note $\ker f$, l'ensemble des $\{x \in A, f(x) = 0_B\}$, et image de f, noté $\operatorname{Im} f$ l'ensemble $f(A)$.

En particulier, f induit un morphisme de groupes $(A, +, 0_A) \to (B, +, 0_B)$. De plus, $\operatorname{Im} f$ est un sous-anneau de B. $\ker f$ n'est pas un sous-anneau de A (sauf si B est nul).

Pour tout anneau A, il existe un unique morphisme d'anneaux $\mathbb{Z} \to A$, et un unique morphisme d'anneaux $A \to$ AnneauNul. Il n'existe aucun morphisme d'anneaux AnneauNul $\to A$ si A n'est pas l'anneau nul aussi.

On dit que A est intègre s'il n'est pas nul et si pour tous $a, b \in A$, on a $ab \neq 0$ si $a \neq 0$ et $b \neq 0$.

Exemples : $\mathbb{Z}$ est intègre, $M_n(\mathbb{C})$ ne l'est pas si $n > 1$, $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.

On appelle unité de A un élément a inversible pour $\star$, et on note A^* l'ensemble des unités de A. Un anneau commutatif non nul tel que $A^* = A \setminus \{0\}$ est appelé un corps. Un corps est un anneau intègre.

PROPOSITION 1.4. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $n = 0$ ou n est premier. $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

1.2. Idéaux et quotients. À partir de maintenant tous les anneaux considérés sont commutatifs

1.2.1. *Idéaux.*

DÉFINITION 1.5. *Un idéal de A est une partie I de A telle que :*

(1) I est un sous-groupe de $(A, +, 0)$

(2) pour tout $a \in A$ et $x \in I$, on a $ax \in I$.

Exemple : $\{0\}$, A sont des idéaux. Idéal principal : $Ax = (x) = \{ax, a \in A\}$. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, les idéaux de $\mathbb{C}[X]$ sont les $P\mathbb{C}[X]$. Plus généralement on a la notion d'idéal engendré par une partie de A : $I = \langle X \rangle$ est l'ensemble des éléments de la forme $\sum_i a_i x_i$, avec $a_i \in A$ et $x_i \in X$.

Un idéal est dit propre s'il n'est pas A tout entier.

PROPOSITION 1.6. *Soit $f : A \to B$ un morphisme d'anneaux, alors* $\ker f$ *est un idéal de A. Si I est un idéal de B, $f^{-1}(I)$ est un idéal de A.*

1.2.2. *Quotients.* Soit A un anneau et I un idéal, on définit une relation d'équivalence sur A par $a \sim b$ si et seulement si $a - b \in I$. On note A/I l'ensemble des classes d'équivalence.

THÉORÈME 1.7. *Il existe une unique structure d'anneau sur A/I qui fait de la projection canonique $\pi : A \to A/I$ un morphisme d'anneaux.*

DÉMONSTRATION. Observons que I est un sous-groupe distingué de $(A, +, 0)$, ce qui traite la partie additive de la structure d'anneau de A/I. Pour la multiplication, il faut vérifier que si $\alpha, \beta \in A/I$, et a, a' et b, b' sont des représentants de α et β, alors $ab \sim a'b'$. Si $a' = a + x$, $b' = b + y$, $x, y \in I$, on a $a'b' = ab + ay + xb + xy \in ab + I$. □

Exemple : $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}[X]/(X^2 + 1) = \mathbb{C}$.

On a la propriété de factorisation :

PROPOSITION 1.8. *Soit $f : A \to B$ un morphisme d'anneaux, I un idéal de A. Alors f se factorise par A/I si et seulement si $I \subset \ker f$.*

et la propriété d'isomorphisme :

PROPOSITION 1.9. *Soit $f : A \to B$ un morphisme d'anneaux, alors f induit un isomorphisme $A/\ker f \to \operatorname{Im} f$.*

1.2.3. *Opération sur les idéaux.* Soit I et J deux idéaux de A, on note $I + J$ l'ensemble des $\{x + y, x \in I, y \in J\}$. C'est un idéal de A. On dit que I et J sont premiers entre eux si $I + J = A$.

Soit I et J deux idéaux de A, on note IJ l'ensemble des $\{\sum_i x_i y_i, x_i \in I, y_i \in J\}$. C'est un idéal de A. Il n'est en général pas égal à $\{xy, x \in I, y \in J\}$.

Si I et J sont des idéaux, $I \cap J$ est un idéal. On a $IJ \subset I \cap J$ mais n'y est pas forcément égal.

PROPOSITION 1.10 (Lemme chinois). *Soit $I_1, \ldots, I_n$ des idéaux de A qui sont deux à deux premiers entre eux. Alors $A/I_1 \ldots I_n \to A/I_1 \times \cdots \times A/I_n$ est un isomorphisme.*

DÉMONSTRATION. Commençons par définir le morphisme : on a un morphisme d'anneaux $A \to A/I_1 \times \cdots \times A/I_n$, dont le noyau contient $I_1 \dots I_n$ d'où $u : A/I_1 \dots I_n \to A/I_1 \times \cdots \times A/I_n$. On raisonne par récurrence sur n, en observant que I_1 et $I_2 \dots I_n$ sont premiers entre eux.

Il suffit donc de travailler avec I, J premiers entre eux. Soit $a \in I$, $b \in J$ avec $a + b = 1$. Observons que $\ker u = I \cap J$. Montrons que $I \cap J = IJ$: soit $x \in I \cap J$, alors $x = x(a + b) \in IJ$. Soit maintenant $(\overline{x}, \overline{y}) \in A/I \times A/J$, alors $u(bx + ay) = (\overline{x}, \overline{y})$ donc u est surjective. □

1.2.4. *Propriétés des idéaux.* Un idéal I est de type fini s'il peut être engendré par un nombre fini d'éléments. On note alors $I = (x_1, \dots, x_n)$. Il est principal s'il peut être engendré par un seul élément. Tout idéal de $\mathbb{Z}$ est principal.

Un idéal I de A est dit premier s'il est propre et si $ab \in I$ implique que $a \in I$ ou $b \in I$.

Un idéal I de A est dit maximal s'il est propre et s'il n'existe pas d'idéal propre de A contenant strictement I.

PROPOSITION 1.11. *Un idéal I est premier si et seulement si A/I est intègre. Un idéal I est maximal si et seulement si A/I est un corps.*

COROLLAIRE 1.12. *Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les (p), p premier. Les idéaux maximaux de $\mathbb{Z}$ sont les (p), p premier.*

On a le résultat suivant dont la preuve utilise le lemme de Zorn :

PROPOSITION 1.13 (Théorème de Krull). *Tout idéal propre de A est contenu dans un idéal maximal.*

1.2.5. *Caractéristique d'un anneau.*

DÉFINITION 1.14. *Soit A un anneau, et n le générateur ≥ 0 du morphisme d'anneaux $\mathbb{Z} \to A$. On appelle n la caractéristique de A et on le note* $\operatorname{car}(A)$.

A contient alors comme sous-anneau $\mathbb{Z}/\operatorname{car}(A)\mathbb{Z}$. A est de caractéristique 0 si et seulement si $n1_A \neq 0$ pour tout $n > 0$. $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. Si A est intègre, alors $\operatorname{car}(A) = 0$ ou est premier.

PROPOSITION 1.15. *Soit $A \to B$ un morphisme d'anneaux. S'il est injectif, on a* $\operatorname{car}(A) = \operatorname{car}(B)$. *En général, on a soit* $\operatorname{car}(A) = \operatorname{car}(B) = 0$, *soit* $\operatorname{car}(B) \mid \operatorname{car}(A)$.

1.3. Corps des fractions d'un anneau intègre.

THÉORÈME 1.16. *Soit A un anneau intègre. Il existe un unique corps K, appelé corps des fractions de A et noté* $\operatorname{Frac}(A)$, *tel que $A \hookrightarrow K$, et tel que tout morphisme injectif $A \to F$ où F est un corps se prolonge de façon unique en $K \to F$.*

ESQUISSE DE DÉMONSTRATION. Soit $X = A \times (A \setminus \{0\})$. On munit X d'une relation d'équivalence par $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$. On note K l'ensemble des classes d'équivalence. On définit une addition sur K par $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$ et une multiplication par $\overline{(a, b)}\overline{(c, d)} = \overline{(ac, bd)}$. Cela munit K d'une structure d'anneau, et A s'injecte dans K par $a \mapsto (a, 1)$. Si $\overline{(a, b)}$ est non nul, son inverse est $\overline{(b, a)}$, K est donc un corps.

Soit $u : A \to F$ injectif, on le prolonge à $K \to F$ par $u(\overline{(a, b)}) = u(a)u(b)^{-1}$. □

Notons que K a la même caractéristique que A.
Exemple : $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\mathrm{Frac}(\mathbb{C}[X]) = \mathbb{C}(X)$.

2. Anneaux de polynômes

2.1. Définitions.

DÉFINITION 2.1. *L'anneau des polynômes en une variable sur A, noté $A[X]$ est l'ensemble des sommes formelles $\sum_{n\geq 0} a_n X^n$ avec tous les a_i nuls sauf un nombre fini, muni de l'addition $(\sum_{n\geq 0} a_n X^n) + (\sum_{n\geq 0} b_n X^n) = \sum_{n\geq 0}(a_n + b_n)X^n$, de la multiplication $(\sum_{n\geq 0} a_n X^n)(\sum_{n\geq 0} b_n X^n) = \sum_{n\geq 0}\sum_{k=0}^{n}(a_k b_{n-k})X^n$, de l'élément nul 0_A et de l'élément unité 1_A.*

On a une inclusion $A \to A[X]$, $a \mapsto (a_0 = a, a_i = 0 \forall i > 0)$ qui est un morphisme d'anneaux.
On a $\mathrm{car}(A[X]) = \mathrm{car}(A)$.

DÉFINITION 2.2. *L'anneau des polynômes en n variable sur A, noté $A[X_1, \ldots, X_n]$ est l'ensemble des sommes formelles $\sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha$ où $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, avec tous les α nuls sauf un nombre fini, muni de l'addition $(\sum_\alpha a_\alpha X^\alpha) + (\sum_\alpha b_\alpha X^\alpha) = \sum_\alpha (a_\alpha + b_\alpha)X^\alpha$, de la multiplication $(\sum_\alpha a_\alpha X^\alpha)(\sum_\alpha b_\alpha X^\alpha) = \sum_\alpha \sum_{\beta+\gamma=\alpha}(a_\beta b_\gamma)X^\alpha$, de l'élément nul 0_A et de l'élément unité 1_A.*

On a que $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$.

2.2. Degré.

DÉFINITION 2.3. *Le degré de $P(X) = \sum_n a_n X^n$ est $\deg(P) = \sup\{n, a_n \neq 0\}$. Si $P = 0$ on pose $\deg(P) = -\infty$.*

DÉFINITION 2.4. *On appelle coefficient dominant de P le coefficient non nul d'indice le plus grand. P est dit unitaire si son coefficient dominant est 1.*

On a toujours $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.

PROPOSITION 2.5. *Si A est intègre, alors $\deg(PQ) = \deg(P) + \deg(Q)$.*

Notons que ce n'est pas forcément vrai si A n'est pas intègre. Dans $\mathbb{Z}/6\mathbb{Z}[X]$, on a $\deg(2X) = 1$, $\deg(3X + 1) = 1$, et $\deg(2X(3X + 1)) = 1$.

COROLLAIRE 2.6. *Si A est intègre alors $A[X]$ aussi, et on a $A[X]^* = A^*$.*

2.3. Division euclidienne par un polynôme unitaire.

THÉORÈME 2.7. *Soit $P \in A[X]$, $Q \in A[X]$ unitaire. Il existe un couple unique (U, R) de polynômes tels que $P = UQ + R$ et $\deg(R) < \deg(Q)$.*

2.4. Morphismes d'évaluation. Soit A un anneau et $u : A \to B$ un morphisme d'anneaux. On dit que B est muni par u d'une structure de A-algèbre. Si $v : A \to C$ est un autre morphisme d'anneaux, on dit que $f : B \to C$ est un morphisme de A-algèbre si $f \circ u = v$. Exemple : $\mathbb{C}[X]$ est une $\mathbb{C}$-algèbre. L'application $\mathbb{C}[X] \to \mathbb{C}$, $P \mapsto P(1)$ est un morphisme de $\mathbb{C}$-algèbres.

Soit B une A-algèbre. On a une bijection entre B et $\mathrm{Hom}_A(A[X], B)$, où b correspond à $P \mapsto P(b)$ qui est le morphisme d'évaluation en b. On a une bijection entre B^n

et $\mathrm{Hom}_A(A[X_1,\dots,X_n],B)$, où $(b_1,\dots,b_n)$ correspond à $P \mapsto P(b_1,\dots,b_n)$ qui est le morphisme d'évaluation du polynôme en $(b_1,\dots,b_n)$.

Un polynôme $P \in A[X_1,\dots,X_n]$ définit donc une fonction polynomiale $A^n \to A$.

Soit $a \in A$. On dit que a est une racine de $P \in A[X]$ si $P(a) = 0$.

PROPOSITION 2.8. *Pour tout polynôme P, il existe un polynôme Q tel que $(P(X) - P(a)) = (X-a)Q(X)$. En particulier, si a est une racine de P, alors il existe $Q(X)$ tel que $P(X) = (X-a)Q(X)$.*

COROLLAIRE 2.9. *Le noyau du morphisme d'évaluation en a est l'idéal engendré par $(X-a)$. Le morphisme d'évaluation en a induit un isomorphisme $A[X]/(X-a) \to A$.*

COROLLAIRE 2.10. *Si A est intègre, un polynôme de degré n a au plus n racines.*

Ce n'est pas vrai si A n'est pas intègre : $2X$ a deux racines dans $\mathbb{Z}/4\mathbb{Z}$.

COROLLAIRE 2.11. *Si A est infini, toute fonction polynomiale détermine entièrement le polynôme dont elle provient.*

Ce n'est pas vrai si A est fini : dans $\mathbb{Z}/p\mathbb{Z}$, 0 et $X^p - X$ définissent la même fonction.

EXERCICE 7. *Un anneau A est un corps fini si et seulement si toute fonction $A \to A$ est polynomiale.*

On dit que a est une racine d'ordre $k \geq 1$ de P s'il existe Q tel que $P(X) = (X-a)^k Q(X)$. Si $k > 1$ on dit que a est une racine multiple de P.

EXERCICE 8. *Si A est intègre, P de degré n a au plus n racines en comptant la multiplicité.*

2.5. Dérivation. Soit $P = \sum a_n X^n \in A[X]$. Le polynôme dérivé de P, noté P', est $P'(X) = \sum_{n\geq 1} n a_n X^{n-1}$.

PROPOSITION 2.12. *Supposons A intègre. Alors a est racine multiple de P si et seulement si a est racine de P et de P'.*

EXERCICE 9. *Si $\mathrm{car}(A) \neq 0$ on ne peut pas lire la multiplicité de la racine sur les dérivées successives !*

2.6. Corps des fractions.

PROPOSITION 2.13. *Supposons A intègre, et $K = \mathrm{Frac}(A)$. Alors $\mathrm{Frac}(A[X]) = K(X)$.*

3. Questions de factorisation

Dans cette section, tous les anneaux sont intègres.

3.1. Vocabulaire.

DÉFINITION 3.1. *On dit que a divise b, et que b est divisible par a, s'il existe c tel que $b = ac$. C'est équivalent à dire que $(b) \subset (a)$.*

On dit que a et b sont associés si a divise b et b divise a, ce qui est équivalent à dire qu'il existe une unité u telle que $b = au$, ou que $(a) = (b)$. La relation d'association est une relation d'équivalence.

On dit que a non nul est irréductible si ce n'est pas une unité et s'il n'est divisible que par les éléments qui lui sont associés et les unités.

On dit que a est premier si $a|bc$ implique $a|b$ ou $a|c$, ou de façon équivalente, si l'idéal engendré par a est premier.

On dit que a et b sont premiers entre eux si les seuls éléments divisant à la fois a et b sont des unités.

Exemple : dans $\mathbb{Z}$, les irréductibles sont les nombres premiers. Dans $k[X]$, les irréductibles sont les polynômes irréductibles.

PROPOSITION 3.2. *Tout élément premier est irréductible.*

DÉMONSTRATION. Soit a un élément premier. Supposons $a = bc$. On a donc $bc \in (a)$. Comme a est premier, cela veut dire que $b \in (a)$ ou $c \in (a)$, donc a est associé à b ou c. □

EXERCICE 10. *La réciproque n'est pas forcément vraie, par exemple $2 \times 3 = (1 + \sqrt{5})(1 - \sqrt{5})$ dans $\mathbb{Z}[\sqrt{-5}]$.*

PROPOSITION 3.3. *Soit a et b tels que (a) et (b) sont premiers entre eux. Alors a et b sont premiers entre eux.*

EXERCICE 11. *La réciproque n'est pas forcément vraie, par exemple X et Y dans $\mathbb{C}[X, Y]$.*

3.2. Anneaux principaux.

DÉFINITION 3.4. *Un anneau A est dit principal s'il est intègre et si tout idéal est principal.*

DÉFINITION 3.5. *Soit a, b des éléments de A principal. On appelle pgcd de a et b tout générateur de $(a) + (b)$ et ppcm de a et b tout générateur de $(a) \cap (b)$. On appelle relation de Bézout tout relation de la forme $ax + by = d$ pour le pgcd d et a et b.*

Le pgcd et ppcm sont donc définis à une unité près.

PROPOSITION 3.6. *Un pgcd d de a et b est caractérisé (à association près) par la propriété suivante : x divise a et b si et seulement si x divise d.*

DÉMONSTRATION. Supposons $(d) = (a) + (b)$. Soit x divisant d, alors $(d) \subset (x)$, donc $(a) \subset (x)$ et $(b) \subset (x)$ donc x divise a et b. Si x divise a et b alors $(a) \subset (x)$ et $(b) \subset (x)$ donc $(d) \subset (x)$ d'où x divise d. Soit maintenant un autre d' avec cette propriété, alors il divise a b donc d, et il est divisible par d donc associé à d. □

THÉORÈME 3.7 (Relation de Bézout). *a et b sont premiers entre eux si et seulement si (a) et (b) sont premiers entre eux. En particulier, si a et b sont premiers entre eux alors il existe x et y tels que $ax + by = 1$.*

DÉMONSTRATION. Soit a et b premiers entre eux et soit d un pgcd de a et b. Alors d divise a et b donc d est une unité donc $(a) + (b) = A$. Réciproquement, si 1 est un pgcd de a et b alors tout élément qui divise a et b est une unité, donc a et b sont premiers entre eux. □

PROPOSITION 3.8. *Dans un anneau principal, tout élément irréductible est premier.*

DÉMONSTRATION. Un élément a irréductible est premier si et seulement si il vérifie le lemmme d'Euclide : si $a \mid bc$ alors $a \mid b$ ou $a \mid c$.

Montrons que le lemme d'Euclide est vrai dans un anneau principal. Soit a irréductible, et b et c tels que $a \mid bc$. Supposons que a ne divise pas b. Alors a et b sont premiers entre eux. Il existe donc une relation de Bézout $ax + by = 1$, d'où $acx + bcy = c$, d'où $a \mid c$ puisque $a \mid bc$. □

3.3. Anneaux euclidiens.

DÉFINITION 3.9. *Un stathme euclidien sur A est la donnée d'une fonction $v : A \setminus \{0\} \to \mathbb{N}$ vérifiant la condition suivante : pour tout a et b dans A, b non nul, il existe q et r tels que $a = bq + r$, et soit $r = 0$, soit $v(r) < v(b)$. On dit alors que q est un quotient et r un reste de la division euclidienne de a par b.*

Par exemple, $\mathbb{Z}$ muni de $v(x) = |x|$, ou $k[X]$ muni de $v(P) = \deg P$. Attention, (q, r) n'est en général pas unique.

THÉORÈME 3.10. *Tout anneau euclidien est principal.*

DÉMONSTRATION. Soit I un idéal non nul de A. On regarde $\{v(x), x \in I \setminus \{0\}\}$. C'est une partie non vide de $\mathbb{N}$, donc admet un élément minimal, disons $v(x_0)$. Montrons que $I = (x_0)$. On a déjà $(x_0) \subset I$. Soit $x \in I$, on écrit la division euclidienne de x par x_0 : $x = qx_0 + r$. On a $r \in I$, et soit $r = 0$ soit $v(r) < v(x_0)$, donc $r = 0$ par choix de x_0, ce qui montre que $x \in (x_0)$. □

Il existe des anneaux principaux non euclidiens.

THÉORÈME 3.11. *Il existe un algorithme, appelé algorithme d'Euclide étendu, qui permet de calculer le pgcd de deux éléments, ainsi qu'une relation de Bézout.*

DÉMONSTRATION. Soit a et b deux éléments de A. On définit trois suites d'éléments de A de la façon suivante : $x_0 = a$, $x_1 = b$, $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$.

Ensuite, si $x_n \neq 0$, on effectue la division euclidienne de x_{n-1} par x_n : $x_{n-1} = q_n x_n + r_n$. On pose alors $x_{n+1} = r_n$, $u_{n+1} = u_{n-1} - q_n u_n$, $v_{n+1} = v_{n-1} - q_n v_n$. Si $x_n = 0$ on s'arrête.

On a pour tout n tel que les termes sont définis, $u_n a + v_n b = x_n$, et $\operatorname{pgcd}(x_{n-1}, x_n) = \operatorname{pgcd}(x_n, x_{n+1}) = \operatorname{pgcd}(a, b)$.

Par ailleurs, il existe un n tel que $x_{n+1} = 0$ puisque $v(x_n)$ décroît strictement pour $n \geq 1$. Alors $x_n = d$ est un pgcd de a et b. □

3.4. Anneaux factoriels.

3.4.1. *Définition.* Soit A un anneau intègre. On note $\mathcal{I}(A)$ un ensemble de représentants des éléments irréductibles de A pour la relation d'association.

DÉFINITION 3.12. *On dit que A vérifie la propriété (E) si pour tout $a \in A$ non nul, il existe une unité u, et des entiers $\alpha_\pi \geq 0$ pour $\pi \in \mathcal{I}(A)$, nuls sauf un nombre fini, tels que $a = u \prod_{\pi \in \mathcal{I}(A)} \pi^{\alpha_\pi}$. On dit que A vérifie la propriété (U) si l'écriture précédente est unique.*

EXERCICE 12. *Cette définition ne dépend pas du choix de représentants qu'on a pris pour $\mathcal{I}(A)$.*

DÉFINITION 3.13. *Un anneau factoriel est un anneau intègre vérifiant (E) et (U).*

Exemple : $\mathbb{Z}[\sqrt{-5}]$ n'est pas un anneau factoriel.

Écrivons $a = u\prod_{\pi\in\mathcal{I}(A)}\pi^{\alpha_\pi}$. On note $\alpha_\pi = v_\pi(a)$ (valuation π-adique de a). On a $v_\pi(ab) = v_\pi(a) + v_\pi(b)$.

Soit a et b non nuls dans A factoriel. Alors a divise b si et seulement si $v_\pi(a) \leq v_\pi(b)$ pour tout π, et a et b sont premiers entre eux si et seulement si pour tout π on a soit $v_\pi(a) = 0$ soit $v_\pi(b) = 0$.

3.4.2. *Propriétés.*

Proposition 3.14. *Dans un anneau factoriel, les propriétés suivantes sont vérifiées :*

(1) on a le lemme d'Euclide : si a est irréductible, alors $a|bc$ implique $a|b$ ou $a|c$.

(2) on a le théorème de Gauss : si $a|bc$ et a est premier à b alors a divise c.

Autrement dit, dans un anneau factoriel, tout élément irréductible est premier.

Démonstration. Montrons la première. $a \mid bc$ dit que $v_a(bc) \geq 1$, donc $v_a(b) \geq 1$ ou $v_a(c) \geq 1$ ce qui donne bien $a \mid b$ ou $a \mid c$.

Montrons la seconde : si $a \mid bc$ alors $v_\pi(a) \leq v_\pi(b) + v_\pi(c)$ pour tout irréductible π. Comme a est premier à b, on a $v_\pi(b) = 0$ pour tout π tel que $v_\pi(a) > 0$, d'où $v_\pi(a) \leq v_\pi(c)$ pour tout π, d'où a divise c. □

On peut définir une notion de pgcd et de ppcm dans un anneau factoriel. Le pgcd d de a et b est défini par $v_\pi(d) = \min(v_\pi(a), v_\pi(b))$ et le ppcm m par $v_\pi(m) = \max(v_\pi(a), v_\pi(b))$.

Proposition 3.15. $(m) = (a) \cap (b)$.
d est caractérisé par le fait que $x \mid a$ et $x \mid b$ si et seulement si $x \mid d$.

En revanche, on n'a pas forcément $(d) = (a) + (b)$. Considérer par exemple X et Y dans $k[X, Y]$.

Proposition 3.16. *Soit K le corps des fractions de A. Tout élément x non nul de K peut s'écrire $x = a/b$ avec a et b premiers entre eux (écriture réduit d'une fraction), et pour tout autre écriture $x = a'/b'$ on a que $a \mid a'$ et $b \mid b'$.*

3.4.3. *Anneaux principaux et factorialité.*

Théorème 3.17. *Tout anneau principal est factoriel.*

Proposition 3.18. *Soit A un anneau intègre vérifiant (E) et dans lequel tout élément irréductible est premier. Alors A est factoriel.*

Démonstration. Prouvons que A a la propriété (U). Nous devons montrer que s'il existe une égalité $a = b$ avec $a = u\prod_{\pi\in\mathcal{I}(A)}\pi^{\alpha_\pi}$ et $b = v\prod_{\pi\in\mathcal{I}(A)}\pi^{\beta_\pi}$ alors $u = v$ et $\alpha_\pi = \beta_\pi$ pour tout π. On raisonne par récurrence sur $\min(\sum\alpha_\pi, \sum\beta_\pi)$. Si cette quantité est nulle, l'un des côté est une unité, donc l'autre aussi, donc les deux sommes sont nulles. Supposons maintenant $\sum\alpha_\pi > 0$. Soit π_0 tel que $\alpha_{\pi_0} > 0$. Alors $\pi_0 \mid a$, donc $\pi_0 \mid b$. Le lemme d'Euclide est vrai dans A puisque tout élément irréductible est premier. On en déduit que π_0 divise l'un des π^{β_π}. Si $\pi \neq \pi_0$, pour tout n, π_0 ne divise pas π^n. Donc $\pi_0 \mid \pi_0^{\beta_{\pi_0}}$, donc $\beta_{\pi_0} > 0$, donc on peut diviser par π_0 des deux côtés et appliquer l'hypothèse de récurrence. □

Démonstration du théorème 3.17. Pour la propriété (E) : voir preuve dans le cas noethérien. Par ailleurs, dans un anneau principal, tout élément irréductible est premier (proposition 3.8). Il ne reste plus qu'à appliquer la proposition 3.18. □

PROPOSITION 3.19. *Les notions de pgcd et de ppcm de A vu comme anneau principal ou comme anneau factoriel coïncident.*

DÉMONSTRATION. On a déjà vu que les notions de ppcm étaient les mêmes.

Pour le pgcd, on utilise la caractérisation de d comme l'élément tel que $x \mid d$ si et seulement si $x \mid a$ et $x \mid b$. □

3.5. Anneaux de polynômes et factorialité.

THÉORÈME 3.20. *Soit A un anneau factoriel. Alors $A[X]$ est factoriel.*

COROLLAIRE 3.21. *Si A est factoriel, $A[X_1, \ldots, X_n]$ est factoriel pour tout n. En particulier, si k est un corps, $k[X_1, \ldots, X_n]$ est factoriel pour tout n.*

EXERCICE 13. *En revanche, si A est principal, $A[X]$ ne l'est en général pas. En fait $A[X]$ est principal si et seulement si A est un corps.*

DÉFINITION 3.22. *Soit $P \in A[X]$ non nul. On appelle contenu de P, et on note $C(P)$, le pgcd de ses coefficients, qui est défini modulo A^*. On dit que P est primitif si $C(P) = 1$.*

Tout polynôme peut s'écrire $P = cQ$ avec Q primitif.

PROPOSITION 3.23. *Si P et Q sont non nuls alors $C(PQ) = C(P)C(Q)$ modulo A^*.*

DÉMONSTRATION. Il est clair que $C(P)C(Q) \mid C(PQ)$. Montrons que si $C(P) = C(Q) = 1$ alors $C(PQ) = 1$. Soit π un irréductible de A, et regardons l'image de P et Q dans l'anneau quotient $B = A/(\pi)$, qui est intègre car un irréductible est premier. L'image de P et Q est non nulle, puisque leurs coefficients ne sont pas tous divisibles par π, donc l'image de PQ est aussi non nulle. Donc tous les coefficients de PQ ne sont pas divisibles par π, donc π ne divise pas $C(PQ)$. Comme c'est vrai pour tout π, on en déduit que $C(PQ) = 1$. □

Notons K le corps des fractions de A.

LEMME 3.24.
1. *Soit $P \in K[X]$. Il existe $a \in K^*$ tel que $aP \in A[X]$ et $C(aP) = 1$.*
2. *Soit $P \in A[X]$ primitif, et $P = QR$ dans $K[X]$. Alors il existe a et b dans K^* avec $ab = 1$, $aQ \in A[X]$ et $bR \in A[X]$ et $C(aQ) = 1$ et $C(bR) = 1$.*

DÉMONSTRATION. Prenons pour a un ppcm des dénominateurs des coefficients de P. On obtient $aP \in A[X]$, il ne reste plus qu'à diviser par $C(aP)$.

Écrivons $Q = (a/b)Q'$, $R = (c/d)R'$ avec $a, b, c, d \in A$ et $Q', R' \in A[X]$ primitifs. On a alors $bdP = acQ'R'$, d'où $(ac)/(bc) \in A^*$ en considérant le contenu. □

PROPOSITION 3.25. *Les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes non constants de contenu 1 qui sont irréductibles dans $K[X]$.*

DÉMONSTRATION. Il est clair que les irréductibles de A sont irréductibles dans $A[X]$, car leurs seuls diviseurs possible sont des constantes. De même, tout élément de A qui est irréductible dans $A[X]$ est un irréductible de A.

Soit $P \in A[X]$ non constant, $C(P) = 1$ et P irréductible dans $K[X]$. On écrit $P = QR$ avec Q, R dans $A[X]$. Alors l'un des deux est une constante par irréductibilité de P dans $K[X]$, disons Q. On a $C(Q) \mid C(P)$, donc $C(Q) = 1$, donc Q est une unité. D'où l'irréductibilité de P dans $A[X]$.

Réciproquement, soit P non constant, irréductible dans $A[X]$. On a $C(P) = 1$ puisque $C(P) \mid P$. Supposons $P = QR$ dans $K[X]$. On écrit $P = (aQ)(bR)$ comme dans le lemme 3.24. Par irréductibilité de P, P divise aQ ou bR, donc par considération du degré, Q ou R est une unité de $K[X]$, donc P est irréductible dans $K[X]$. □

Démonstration du théorème 3.20. Montrons l'existence d'une décomposition. Soit $P \in A[X]$ non nul. Si P est constant, on utilise la factorialité de A. Sinon, on écrit dans $K[X]$ que $P = u \prod P_i^{n_i}$, avec $u \in K^*$ et les P_i parcourant des polynômes irréductibles de $K[X]$. On peut supposer que les P_i sont dans $A[X]$ et de contenu 1. Dans ce cas on a forcément $u = C(P) \in A$ ce qui permet de finir la décomposition.

Pour l'unicité, il suffit de montrer que tout P irréductible est premier. Supposons $P \in A$, c'est donc un élément premier de A puisque A est factoriel. On a $A[X]/(P) = (A/P)[X]$ qui est donc bien intègre. Soit maintenant P irréductible non constant, et $u : A[X]/(P) \to K[X]/(P)$. Il suffit de montrer que u est injective, puisque $K[X]/(P)$ est intègre. Il faut voir que $PK[X] \cap A[X] = PA[X]$. Soit $Q \in PK[X] \cap A[X]$, on peut supposer $C(Q) = 1$ et on écrit $Q = PR$, $R \in K[X]$. Soit a tel que $aR \in A[X]$ primitif comme dans le lemme 3.24, alors $aQ = PaR$ d'où $aC(Q) = C(aQ) = C(P)C(aR) = 1$ modulo A^*, donc $a \in A^*$. □

4. Anneaux noethériens

4.1. Définitions et premières propriétés.

Définition 4.1. *Un anneau A (pas nécessairement intègre) est dit noethérien si tout idéal de A est de type fini.*

Exemple : tout anneau principal est noethérien. Il existe des anneaux non noethériens : considérer $A = k[(X_n)_{n\in\mathbb{N}}]$. Un anneau noethérien peut avoir un sous-anneau non noethérien : regarder $A \subset \mathrm{Frac}(A)$ pour l'anneau A précédent.

Proposition 4.2. *Si A est noethérien, tout quotient de A par un idéal aussi.*

Proposition 4.3. *On a équivalence entre les trois propriétés suivantes :*

(1) tout idéal de A est de type fini

(2) toute famille croissante d'idéaux est stationnaire

(3) toute famille non vide d'idéaux admet un élément maximal

Démonstration. 1 ⇒ 2. Soit (I_n) une famille croissante d'idéaux. Alors $I = \cup I_n$ est un idéal. Il est de type fini, engendré par $x_1, \ldots, x_r$. Il existe N tel que I_N contient tous les x_i, alors $I = I_N = I_n$ pour tout $n \geq N$.

2 ⇒ 3. Considérons $(I_x)_{x\in X}$ une famille non vide d'idéaux ne contenant pas d'élément maximal, et construisons une famille croissante d'idéaux non stationnaire. On prend $I_0 \in X$ quelconque, et si $I_n \in X$ est construit, il n'est pas maximal, donc il existe $I_{n+1} \in X$ contenant strictement I_n.

3 ⇒ 1. Soit I un idéal de A. On considère la famille des idéaux de type fini contenus dans I. Soit J un élément maximal, alors $I = J$. Sinon, soit $x \in I$, $x \notin J$, alors (J, x) est contenu dans I, contient strictement J et est de type fini, contradiction.

□

On en déduit une preuve du théorème de Krull dans le cas des anneaux noethériens : soit I un idéal propre de A, considérer la famille de tous les idéaux propres de A contenant I et appliquer la propriété 3.

4.2. Anneaux noethériens et polynômes.

THÉORÈME 4.4 (Théorème de Hilbert). *Soit A un anneau noethérien. Alors $A[X]$ est aussi noethérien.*

DÉMONSTRATION. Soit I un idéal de $A[X]$. Construisons une partie génératrice finie de I.

Pour tout entier n on note J_n la partie de A formée par les coefficients dominants des éléments de I de degré $\leq n$. Alors J_n est un idéal de A. Montrons que si a, b sont dans J_n alors $a+b$ aussi. Soit P, Q dans I de degré $\leq n$ de coefficients dominants a et b respectivement. Supposons par exemple $\deg P \geq \deg Q$, alors $a+b$ est le coefficient dominant de $P + X^{\deg P - \deg Q}Q$. De plus J_n est aussi la réunion de $\{0\}$ et de l'ensemble des coefficients dominants des polynômes de I de degré exactement n.

On a une suite croissante d'idéaux de A qui devient donc stationnaire : il existe N tel que $J_N = J_n$ pour tout $n \geq N$.

Pour tout $n \leq N$, il existe une partie finie E_n de I formée de polynômes de degré n dont les coefficients dominants engendrent J_n. Notons $E = \cup_{n \leq N} E_n$, et montrons que E est une partie génératrice (finie) de I. On raisonne par récurrence sur le degré de $P \in I$. Soit $P \in I$ de degré n. Son coefficient dominant a peut s'écrire $\sum x_i a_i$ avec x_i dans A et a_i le coefficient dominant de $P_i \in E_n$. Alors $Q = P - \sum_i x_i P_i$ est un élément de I de degré $< n$, ce qui permet de conclure. □

4.3. Existence de décomposition en irréductibles.

THÉORÈME 4.5. *Soit A noethérien intègre. Alors la propriété (E) est vérifiée.*

DÉMONSTRATION. Soit $a \in A$ non nul. Montrons qu'il est produit d'irréductibles. Si ce n'est pas le cas, $a = bc$ avec b et c non inversibles, et b ou c n'est pas produit d'irréductibles, disons b. Posons $a_0 = a$, $a_1 = b$, on construit ainsi par récurrence une famille (a_i) d'éléments qui ne sont pas produits d'irréductibles, et $(a_i) \subset (a_{i+1})$ et l'inclusion est stricte. C'est impossible par la propriété des familles croissantes d'idéaux. □

CHAPITRE 3

Modules

Dans tout ce chapitre, A désigne un anneau commutatif.

1. Généralités

1.1. Définitions.

Définition 1.1. *Un A-module est un ensemble M muni de $(+, 0_M)$ de sorte que $(M, +, 0_M)$ est un groupe abélien, et d'une application $A \times M \to M$ vérifiant :*

(1) Pour tout m dans M, $0_A \cdot m = 0_M$ et $1_A \cdot m = m$

(2) Pour tous a, b dans A, m dans M, $(a + b) \cdot m = a \cdot m + b \cdot m$

(3) Pour tout a dans A, m, n dans M, $a \cdot (m + n) = a \cdot m + a \cdot n$.

(4) Pour tous a, b dans A, m dans M, $(ab) \cdot m = a \cdot (b \cdot m)$

Définition 1.2. *Soit M et M' deux A-modules. Une application A-linéaire de M dans M' est une fonction $f : M \to M'$ telle que f est un morphisme de groupes de $(M, +)$ vers $(M', +)$, et de plus $f(a \cdot m) = a \cdot f(m)$ pour tous $m \in M$, $a \in A$. On note* $\mathrm{Hom}_A(M, M')$*, ou simplement* $\mathrm{Hom}(M, M')$*, l'ensemble des applicactions A-linéaires de M dans M'.*

Exemple : si A est un corps, un A-module est exactement la même chose qu'un espace vectoriel sur A, et une application A-linéaire est la même chose que les applications linéaires pour un corps.

Exemple : si $A = \mathbb{Z}$, un $\mathbb{Z}$-module est la même chose qu'un groupe abélien et un morphisme de $\mathbb{Z}$-modules est la même chose qu'un morphisme de groupes. Par exemple $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module.

Exemple : pour tout $a \in \mathbb{C}$, on peut définir une structure de $\mathbb{C}[X]$-module sur $\mathbb{C}$ par $P \cdot z = P(a)z$.

Exemple : pour tout anneau A, A^n est un A-module, et pour tout idéal I de A, I et A/I sont des A-modules.

Définition 1.3. *Soit M un A-module, un sous-module de M est un sous-groupe de N tel que pour tout $a \in A$, $a \cdot N \subset N$.*

Exemple : on considère A comme un A-module. Alors ses sous-modules sont exactement ses idéaux. Si M est un A-module et I un idéal de A, IM est un sous-module de M.

Si $f \in \mathrm{Hom}(M, M')$, on note $\ker f = \{x \in M, f(x) = 0\}$. C'est un sous-module de M, et $\ker f = 0$ si et seulement si f est injective. On note $\mathrm{Im}\, f = \{f(x), x \in M\}$. C'est un sous-module de M'. On dit que f est un isomorphisme si c'est une bijection. Dans ce cas la bijection réciproque f^{-1} est automatiquement une application linéaire.

1.2. Quotients, supplémentaires. Soit M un module et N un sous-module. On définit une relation d'équivalence sur M par : $m \sim m'$ si et seulement si $m - m' \in N$. On note M/N l'ensemble quotient, et $\pi : M \to M/N$ la projection canonique.

THÉORÈME 1.4. *Il existe une unique structure de A-module sur M/N telle que π est une application linéaire.*

Pour tout $f : M \to M'$, il existe u tel que $f = u \circ \pi$ si et seulement si $N \subset \ker f$, et u est alors unique.

Pour tout $f : M \to M'$, la factorisation précédente donne un isomorphisme $u : M/\ker f \to \operatorname{Im} f$.

On introduit la notion de suite exacte : soit $M \xrightarrow{f} N \xrightarrow{g} P$ deux applications linéaires. On dit que c'est une suite exacte en N si $\ker g = \operatorname{Im} f$.

On dit que la suite $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ est exacte si elle est exacte en M, N et P, c'est-à-dire que f est injective, g surjective, et $\ker g = \operatorname{Im} g$. Dans ce cas, M s'identifie à un sous-module de N, et P à N/M.

DÉFINITION 1.5. *Soit M un A-module, P et Q deux sous-modules de M. On dit que P et Q sont en somme directe dans M, et on note $M = P \oplus Q$, si tout $m \in M$ s'écrit de façon unique $m = p + q$, $p \in P$ et $q \in Q$.*

Soit N un sous-module de M, on dit que le sous-module P est un supplémentaire de N si $N \oplus P = M$.

Tout sous-module n'admet pas forcément de supplémentaire. Exemple : $2\mathbb{Z} \subset \mathbb{Z}$.

PROPOSITION 1.6. *Soit N, P deux sous-modules de M. Alors $N \oplus P = M$ si et seulement si la projection canonique : $\pi : M \to M/N$ induit un isomorphisme de P sur M/N.*

1.3. Générateurs.

DÉFINITION 1.7. *Soit X une partie de M. Le sous-module engendré par M est le plus petit sous-module de M contenant X, c'est aussi l'ensemble des $\sum a_i x_i$, $a_i \in A$ et $x_i \in X$.*

La somme de deux sous-modules P et Q, notée $P + Q$, est le sous-module engendré par P et Q.

On dit que M est de type fini s'il existe une partie finie X de M telle que M est engendré par X.

Tout quotient d'un module de type fini est de type fini. En revanche, tout sous-module d'un module de type fini n'est pas forcément de type fini. Un module est de type fini si et seulement si c'est un quotient de A^n.

On dit qu'un module est libre de type fini s'il existe n tel que M est isomorphe à A^n.

On appelle base de M une famille X qui est libre, c'est-à-dire que pour toute relation $\sum_{x \in X} a_x x = 0$, on a $a_x = 0$ pour tout x, et qui est génératrice. Le choix d'une base donne un isomorphisme entre M et A^X.

Tout module n'admet pas forcément de base, toute famille libre ne se prolonge pas forcément en une base, toute famille génératrice ne contient pas forcément de base. Un module admet une base finie si et seulement si il est libre de type fini.

PROPOSITION 1.8. *Soit M un module libre de type fini. Alors toutes les bases de M ont même cardinal, qu'on appelle rang de M. De façon équivalente, il existe un unique n tel que M est isomorphe à A^n.*

DÉMONSTRATION. Soit I un idéal maximal de A. Le module quotient M/IM est un A/I-espace vectoriel, et l'image d'une base de M sur A est une base de M/IM sur A/I. On utilise alors les résultats connus sur les espaces vectoriels. □

Exemple : $\mathbb{Z}/n\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module libre si $n \neq 0$. La famille $\{2, 3\}$ de $\mathbb{Z}$ est génératrice comme $\mathbb{Z}$ module, mais ne contient pas de base. La famille $\{2\}$ de $\mathbb{Z}$ est libre, mais ne se prolonge pas en une base de $\mathbb{Z}$ comme $\mathbb{Z}$-module.

On définit le produit (ou la somme) de deux modules : $M \oplus N = M \times N$.

1.4. Modules noethériens.

DÉFINITION 1.9. *Un module est dit noethérien si tout sous-module de M est de type fini.*

En particulier, M lui-même est de type fini. Si A est un anneau noethérien, c'est un A-module noethérien.

PROPOSITION 1.10. *Soit $0 \to N \to M \to Q \to 0$ une suite exacte. Alors M est noethérien si et seulement si N et Q le sont.*

DÉMONSTRATION. Si M est noethérien, tout sous-module de N est noethérien, car un sous-module de N est un sous-module de M. Le quotient est aussi noethérien : si $P' \subset P$, l'image par π d'une famille génératrice de $\pi^{-1}(P')$ est une famille génératrice de P'.

Supposons maintenant N et Q noethériens, et soit M' un sous-module de M. Alors $M' \cap N$ est de type fini, engendré par $x_1, \ldots, x_n$. $\pi(M')$ est de type fini, engendré par $y_1, \ldots, y_m$. Soit $z_1, \ldots, z_m$ dans M' relevant $y_1, \ldots, y_m$. Montrons que M' est engendré par $x_1, \ldots, x_n, z_1, \ldots, z_m$. Soit $x \in M'$. Il existe des a_i tels que $\pi(x) = \sum a_i y_i$. Alors $x - \sum a_i z_i \in N$, donc s'écrit $\sum b_j x_j$. □

Soit A un anneau noethérien. On a le résultat suivant :

THÉORÈME 1.11. *Soit M un module de type fini sur A. Alors M est noethérien.*

DÉMONSTRATION. En appliquant récursivement la proposition 1.10, on voit que A^n est noethérien pour tout n. Comme M est de type fini, il existe n et une suite exacte $0 \to N \to A^n \to M \to 0$. On applique alors de nouveau la proposition 1.10. □

2. Algèbre linéaire

Soit M et N deux modules libres de rang fini sur A.

PROPOSITION 2.1. *Étant donné un choix de bases $(e_i)_{1 \leq i \leq m}$ de M et $(f_i)_{1 \leq i \leq n}$ de N, il existe une bijection canonique entre* $\mathrm{Hom}_A(M, N)$ *et* $M_{m,n}(A)$.

DÉMONSTRATION. Si $C \in M_{m,n}(A)$, on définit $u_C : M \to N$ par $u(e_i) = \sum_j c_{i,j} f_j$. Comme e est une base de M, cette définition se prolonge de façon unique par linéarité à M entier. (on utilise le fait que e est libre pour l'existence du prolongement au sous-espace engendré par e, et le fait que e est génératrice pour le fait que cela définit u sur M entier)

Réciproquement, soit $u : M \to N$, on définit C_u la matrice dont le coefficient $c_{i,j}$ est la coordonnée de $u(e_i)$ sur f_j dans la base f (on utilise le fait que f est génératrice pour l'existence de $c_{i,j}$). □

Définition 2.2. *Soit $C \in M_n(A)$. On définit* $\mathrm{tr}(C)$ *par la formule* $\sum_i c_{i,i}$ *et* $\det(C)$ *par la formule* $\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\prod_i c_{i,\sigma(i)}$.

On peut calculer le déterminant comme dans le cas des corps en développant par rapport à une ligne, une colonne.

Proposition 2.3. *(1)* $\mathrm{tr}(CD) = \mathrm{tr}(DC)$ *pour tous* $C, D \in M_n(A)$.

(2) $\det(CD) = \det(C)\det(D)$ *pour tous* $C, D \in M_n(A)$.

Démonstration. Le (1) est un calcul simple.

Montrons comment déduire (2) du résultat analogue sur les corps. Soit $R = \mathbb{Z}[X_{i,j}, Y_{i,j}, 1 \leq i, j \leq n]$ l'anneau de polynômes à $2n^2$ variables sur $\mathbb{Z}$. Soit $X, Y \in M_n(R)$ les matrices de coefficients $X_{i,j}$ et $Y_{i,j}$ respectivement. On a $\det(XY) = \det(X)\det(Y)$ car on peut considérer toutes ces matrices comme des éléments de $M_n(\mathrm{Frac}\, R)$.

Soit maintenant A un anneau, et $C, D \in M_n(A)$. On définit $u : R \to A$ par $u(X_{i,j}) = c_{i,j}$ et $u(Y_{i,j}) = d_{i,j}$. Alors $C = u(X)$, $D = u(Y)$, $CD = u(XY)$, $\det(C) = u(\det(X))$, $\det(D) = u(\det(Y))$ et $\det(CD) = u(\det(XY))$, de sorte que le résultat se déduit du résultat sur R. □

Soit $f \in \mathrm{Hom}_A(M, M)$. On définit son déterminant $\det(f)$ dans une base. Alors comme dans le cas des corps, il ne dépend pas du choix de la base (par l'égalité (2) de la proposition 2.3, et $\det(fg) = \det(f)\det(g)$. En particulier, si f est inversible, $\det(f) \in A^*$.

Définition 2.4. *Soit $C \in M_n(A)$. On définit la comatrice de C, ou matrice des cofacteurs, notée* $\mathrm{co}(C)$*, comme la matrice dont le coefficient en position (i, j) est $(-1)^{i+j}$ fois le déterminant obtenu en enlevant de C la i-ième ligne et la j-ième colonne.*

Proposition 2.5. $C \cdot {}^t\mathrm{co}(C) = {}^t\mathrm{co}(C) \cdot C = (\det(C))\,\mathrm{Id}$.

Corollaire 2.6. *f est inversible si et seulement si* $\det(f) \in A^*$.

On peut donc définir un groupe $\mathrm{GL}_n(A)$ comme l'ensemble des éléments de $M_n(A)$ de déterminant inversible.

f est surjective si et seulement f est bijective. En revanche f peut-être injective sans être bijective (et on a f injective si et seulement si $\det(f)$ n'est pas diviseur de 0, mais ce n'est pas très facile).

Définition 2.7. *Soit $C \in M_n(A)$. On considère $X\,\mathrm{Id} - C \in M_n(A[X])$, et on pose $\chi_C = \det(X\,\mathrm{Id} - C) \in A[X]$, c'est le polynôme caractéristique de C. Deux matrices semblables ont même polynôme caractéristique, on peut donc définir aussi χ_u pour $u \in \mathrm{End}_A(M)$, M libre de rang n.*

Théorème 2.8 (Cayley-Hamilton). $\chi_C(C) = 0$.

Démonstration. Deux méthodes : on peut utiliser la technique de la preuve de la proposition 2.3 pour se ramener au cas des corps. On peut aussi faire une preuve directe vraie dans tout anneau, qu'on explique maintenant.

Soit $M = A^n$, et $(e_1, \ldots, e_n)$ la base canonique de M. On munit M d'une structure de $A[X]$-module par $X \cdot m = Cm$.

Par ailleurs, on a une action naturelle de $M_n(A[X])$ sur M^n : si $B \in M_n(A[X])$, on pose $u_B(m_1, \ldots, m_n) = (\sum_j b_{1,j} \cdot m_j, \ldots, \sum_j b_{n,j} \cdot m_j)$, et u induit un morphisme d'anneaux (non commutatifs) $M_n(A[X]) \to \mathrm{End}_A(M^n)$, en particulier $u_{B+B'} = u_B + u_{B'}$, et $u_{BB'} = u_B \circ u_{B'}$.

De plus, pour tout $P \in A[X]$, $u_{P\,\mathrm{Id}}(m_1, \dots, m_n) = (P(X) \cdot m_1, \dots, P(X) \cdot m_n) = (P(C)m_1, \dots, P(C)m_n)$.

On considère C comme un élément de $M_n(A[X])$ par l'inclusion de A dans $A[X]$, et on observe alors que $u_C(e) = u_{X\,\mathrm{Id}}(e) = (X \cdot e_1, \dots, X \cdot e_n)$, où $e = (e_1, \dots, e_n)$ (mais on n'a pas l'égalité d'opérateurs $u_C = u_{X\,\mathrm{Id}}$).

Considérons la matrice $X\,\mathrm{Id} - C \in M_n(A[X])$. Alors $u_{X\,\mathrm{Id}-C}(e) = 0$, donc $u_{{}^t\mathrm{co}(X\,\mathrm{Id}-C)(X\,\mathrm{Id}-C)}(e) = 0$, d'où $u_{\det(X\,\mathrm{Id}-C)\,\mathrm{Id}}(e) = 0$, et finalement $u_{\chi_C(C)\,\mathrm{Id}}(e) = 0$, donc $(\chi_C(C)e_1, \dots, \chi_C(C)e_n) = 0$. En particulier, $\chi_C(C)e_i = 0$ pour tout i, donc $\chi_C(C) = 0$. □

3. Modules de type fini sur un anneau principal

Dans toute la suite on fixe un anneau principal A.

3.1. Sous-modules.

THÉORÈME 3.1. *Soit M un module libre de type fini sur A, et N un sous-module de M. Alors N est libre de rang inférieur ou égal au rang de M.*

DÉMONSTRATION. Soit $(e_1, \dots, e_n)$ une base de M, et (e_i^*) la base duale associée. On note $N_i = N \cap (Ae_1 + \cdots + Ae_i)$ pour $i \leq n$. On va montrer par récurrence sur i que N_i est libre de rang $\leq i$. Le cas $i = 1$ est la propriété d'être un anneau principal, qui revient à dire que tout sous-module d'un module libre de rang 1 est libre de rang 0 ou 1. Supposons la propriété vraie au rang i. On regarde $e_{i+1}^*(N_{i+1})$: c'est un idéal de A, engendré par un élément disons a. Si $a = 0$, cela signifie que $N_i = N_{i+1}$ donc la propriété est vraie aussi au rang $i + 1$. Sinon soit $z \in N_{i+1}$ tel que $e_{i+1}^*(z) = a$. Alors $N_{i+1} = N_i \oplus Az$. En effet, pour tout $x \in N_{i+1}$, il existe $b \in A$ tel que $e_{i+1}^*(x) = ab$, alors $x - bz \in N_i$, et il est clair que $N_i \cap Az = \{0\}$. □

Ceci n'est pas vrai si on ne suppose pas A principal : regarder par exemple le sous-module (X, Y) de $\mathbb{C}[X, Y]$.

COROLLAIRE 3.2. *Tout sous-module d'un module de type fini est de type fini et peut être engendré par moins d'éléments (ou autant) que le module de départ.*

3.2. Théorèmes de structure.

THÉORÈME 3.3. *Soit $M \in M_{r,s}(A)$ une matrice. Alors il existe des matrices inversibles P et Q de taille r et s respectivement telles que PMQ soit de la forme $\mathrm{diag}(d_1, \dots, d_{\min(r,s)})$ avec $d_1 | d_2 \dots | d_{\min(r,s)}$. De plus les (d_i) sont entièrement déterminés, et (d_1) est le pgcd des coefficients de la matrice.*

Les (d_i) sont appelés facteurs invariants de la matrice M, et la matrice ainsi obtenue est la forme normale de Smith. On commence par observer :

PROPOSITION 3.4. *Soit $M \in M_{r,s}(A)$. Pour tout $n \leq \min(r, s)$, on note I_n l'idéal engendré par les mineurs de taille n de M. Alors I_n ne dépend que de la classe d'équivalence de M.*

DÉMONSTRATION DU THÉORÈME 3.3. L'unicité des (d_i) provient de ce que dans une telle décomposition, on a nécessairement $I_n = (d_1 \dots d_n)$. On note $\mathrm{pgcd}(M)$ pour I_1.

Pour montrer le théorème il suffit de prouver qu'il existe P et Q inversibles telles que PMQ est de la forme $\begin{pmatrix} d_1 & 0 \\ 0 & M' \end{pmatrix}$ avec $d_1 = \mathrm{pgcd}(M)$ et donc divisant tous les coefficients de M' et ensuite raisonner par récurrence sur la taille de la matrice.

Soit $i > 1$. Alors il existe une matrice inversible telle que la multiplication à gauche (resp. à droite) par cette matrice change $m_{1,1}$ en un générateur de $\mathrm{pgcd}(m_{1,1}, m_{1,i})$ (resp de $\mathrm{pgcd}(m_{1,1}, m_{i,1})$). Montrons-le pour les matrices 2×2. Soit $u = m_{1,1}$ et $v = m_{1,2}$ et d un pgcd de u et v. Il existe a et b tels que $au + bv = d$, alors la matrice $\begin{pmatrix} a & b \\ -v/d & u/d \end{pmatrix}$ convient. De plus, si $m_{1,1} \mid m_{i,1}$ (resp. $_{1,1} \mid m_{1,i}$), on peut faire en sorte que la première ligne (resp. la première colonne) ne soit pas modifiée.

Par applications successives de cette méthode, on se ramène au cas où $m_{1,1}$ divise tous les coefficients de la première ligne et de la première colonne. Précisément, les idéaux engendrés par $(m_{1,1})$ forment une suite croissante, et strictement croissante à chaque fois qu'on applique la méthode avec $m_{1,1} \not| m_{i,1}$ ou $m_{1,i}$, et comme elle devient stationnaire c'est qu'au bout d'un moment $m_{1,1}$ divise tous les $m_{i,1}$ et $m_{1,i}$.

Ensuite par opérations élémentaires sur les lignes et les colonnes, on se ramène au cas où M est de la forme $\begin{pmatrix} d & 0 \\ 0 & M' \end{pmatrix}$.

Si d divise $\mathrm{pgcd}(M')$ on a fini. Sinon, par opération élémentaire sur les lignes ou les colonnes on met sur la première ligne ou la première colonne un élément non divisible par d, et on recommence la méthode précédente.

L'algorithme finit par terminer, car les idéaux engendrés par $m_{1,1}$ à chaque étape forment une suite croissante, qui ne peut donc être strictement croissante et infinie. □

Remarque 3.5. *Lorsque l'anneau est euclidien, la phase de remplacement de $m_{1,1}$ par un générateur de $\mathrm{pgcd}(m_{1,1}, m_{1,i})$ peut se faire par opérations élémentaires sur les lignes et les colonnes.*

On peut exprimer ce résultat en termes d'endomorphismes :

Théorème 3.6 (Théorème de la base adaptée). *Soit M un module libre de rang m, et N un module libre de rang n, et $u \in \mathrm{Hom}_A(M, N)$. Il existe une base $(e_1, \ldots, e_m)$ de M, et une base $(f_1, \ldots, f_n)$ de N, et des éléments $d_1, \ldots, d_m$ de A avec $d_1 | \ldots | d_m$ tels que $u(e_i) = d_i f_i$ (avec $d_i = 0$ si $i > n$ de sorte que $u(e_i)$ est bien défini même pour les $i > n$).*

Corollaire 3.7. *Soit N un sous-module du module libre M de rang m. Il existe une base $(e_1, \ldots, e_m)$ de M, $n \leq m$, et $d_1 \mid \cdots \mid d_n$ non nuls tels que les $d_i e_i$, $1 \leq i \leq n$, forment une base de N.*

On déduit aussi du théorème 3.3 le théorème de structure des modules de type fini sur un anneau principal :

Théorème 3.8. *Soit M un module de type fini. Alors il existe un entier $n \geq 0$, des éléments $d_1 | \ldots | d_r$ de A non nuls et non inversibles, tels que M est isomorphe à $A^n \oplus (\oplus_{i=1}^r A/(d_i))$. De plus n et les (d_i) sont uniquement déterminés.*

Démonstration de l'existence. M étant de type fini, c'est un quotient de A^s pour un $s \geq 0$. Le noyau de la projection $p : A^s \to M$ est un module libre, isomorphe à un A^r. On applique alors le théorème 3.6 au morphisme $A^r \to A^s$, ce qui montre l'existence. □

Proposition 3.9. *Soit $M = \oplus_{i=1}^n A/(d_i)$, avec les d_i non nuls et non inversibles et $d_1 \mid \cdots \mid d_n$. Alors il existe des éléments irréductibles non associés $p_1, \ldots, p_r$, et des entiers $n_{i,j}$ avec $1 \leq i \leq r$, $1 \leq j \leq m_i$, et $1 \leq n_{i,1} \leq \ldots n_{i,m_i}$ pour tout i, tels que M est*

isomorphe à $\oplus_{i=1}^{r}(\oplus_{j=1}^{m_i}A/(p_i^{n_{i,j}})$. *De plus les* (p_i) *et les* $n_{i,j}$ *sont uniquement déterminés par* M.

Soit $M = \oplus_{i=1}^{r}(\oplus_{j=1}^{m_i}A/(p_i^{n_{i,j}})$, *où les* p_i *sont des irréductibles non associés, et* $1 \leq n_{i,1} \leq \dots n_{i,m_i}$ *pour tout* i. *Alors il existe* $d_1, \dots, d_n$ *des éléments non nuls et non inversibles avec* $d_1 \mid \cdots \mid d_n$, *et* M *est isomorphe à* $\oplus_{i=1}^{n}A/(d_i)$. *De plus les* (d_i) *sont uniquement déterminés par* M.

Démonstration. Il s'agit essentiellement du lemme chinois : si $d = u\prod_{i=1}^{r}p_i^{n_i}$, alors $A/(d)$ est isomorphe à $\oplus_{i=1}^{r}A/(p_i^{n_i})$. □

Proposition 3.10. *Soit* $M = A^n \oplus (\oplus_{i=1}^{r}(\oplus_{j=1}^{m_i}A/(p_i^{n_{i,j}}))$. *Soit* p *un élément premier, et* $k = A/(p)$. *Alors* $\dim_k(p^rM/p^{r+1}M) = 0$ *si aucun des* p_i *n'est associé à* p, *et* $\dim_k(p^rM/p^{r+1}M) = n + \#\{j, n_{i,j} > r\}$ *si* p *est associé à* p_i.

Démonstration. Si p ne divise pas d, alors la multiplication par p est un automorphisme de $A/(d)$. Par ailleurs, $p^rA/p^{r+1}A$ est isomorphe à A/pA. □

On en déduit la preuve de l'unicité :

Corollaire 3.11. *Supposons* $M = A^n \oplus (\oplus_{i=1}^{r}(\oplus_{j=1}^{m_i}A/(p_i^{n_{i,j}}))$. *Alors* n, *les* (p_i) *et les* $n_{i,j}$ *sont entièrement déterminés par* M.

Corollaire 3.12. *Dans le théorème 3.3, les* (d_i) *sont uniquement déterminés.*

Démonstration. Soit $M \in M_{r,s}(A)$ comme dans l'énoncé, et soit $u : A^r \to A^s$ donné par la matrice M dans la base canonique. Alors $A^s/u(A^r)$ est isomorphe à $\oplus A/(d_i)$ si $s \leq r$, et à $A^{s-r} \oplus (\oplus A/(d_i))$ si $s \geq r$, donc on peut lire les d_i sur le quotient. On utilise alors l'unicité dans le théorème 3.8. □

Remarque 3.13. *On a* $n = 0$ *si et seulement si* M *est de torsion.*

Corollaire 3.14. *Soit* M *un module de type fini sans torsion. Alors* M *est libre.*

Définition 3.15. *Si* p *est un élément irréductible, et* M *un* A*-module, on note* $M(p) = \{m \in M, \exists n \in \mathbb{N}, p^nm = 0\}$. *On l'appelle partie* p*-primaire de* M, *et c'est un sous-module de* M.

Proposition 3.16. *Soit* M *un module de type fini qui est* p*-primaire. Alors* M *est isomorphe à* $\oplus_i A/(p^{n_i})$ *où les* n_i *sont uniquement déterminés.*

On peut reformuler le théorème 3.8 en termes de modules p-primaires :

Théorème 3.17. *Soit* M *un module de type fini de torsion. Alors* M *est isomorphe à* $\oplus_p M(p)$, *et les* $M(p)$ *sont nuls sauf un nombre fini. De plus* $M(p)$ *est isomorphe à* $\oplus_i A/(p^{n_{p,i}})$ *où les* $n_{p,i}$ *sont uniquement déterminés par* M.

3.3. Applications aux groupes abéliens de type fini.

Théorème 3.18. *Soit* G *un groupe abélien de type fini. Il existe* $n \geq 0$, *des entiers* $d_1 \mid \cdots \mid d_m$ *strictement positifs avec* $d_1 > 1$ *définis uniquement par* G, *tels que* $G \simeq \mathbb{Z}^n \oplus (\oplus_{i=1}^{m}\mathbb{Z}/d_i\mathbb{Z})$.

G est fini si et seulement si $n = 0$. Si G est fini, d_m est l'exposant de G (c'est-à-dire le plus petit entier annulant G).

3.4. Applications à l'algèbre linéaire.

Dans cette section on fixe un corps k.

3.4.1. *Généralités.* Soit V un k-ev de dimension finie, et $u \in \mathrm{End}(V)$. On munit V d'une structure de $k[X]$-module par $X \cdot x = u(x)$. On note $[V, u]$ le $k[X]$-module ainsi obtenu.

PROPOSITION 3.19. *Le $k[X]$-module $[V, u]$ est de type fini et de torsion.*

DÉMONSTRATION. Toute famille génératrice de V comme k-ev est une famille génératrice du $k[X]$-module $[V, u]$. V étant supposé de dimension finie, $[V, u]$ est de type fini.

Comme $\mathrm{End}(V)$ est de dimension finie, il existe un polynôme P non nul tel que $P(u) = 0$. Alors P annule $[V, u]$, qui est donc de torsion. □

PROPOSITION 3.20. *Tout $k[X]$-module de type fini de torsion est de la forme $[V, u]$.*

DÉMONSTRATION. Soit M un $k[X]$-module de type fini de torsion. Il existe un polynôme P non nul tel que P annule M, de sorte que M est un $k[X]/(P)$-module. Il est de type fini, donc c'est un quotient de $(k[X]/(P))^n$ pour un certain n. Notons V le k-ev sous-jacent à M, il est de dimension finie. L'action de X est un endomorphisme k-linéaire de V, qu'on note u, alors $M = [V, u]$. □

PROPOSITION 3.21. *Les morphismes de $k[X]$-modules entre $[V, u]$ et $[V', u']$ correspondent naturellement aux applications linéaires $f : V \to V'$ vérifiant $f \circ u = u' \circ f$. En particulier, les $k[X]$-modules $[V, u]$ et $[V, u']$ sont isomorphes si et seulement si u et u' sont conjugués.*

Les sous-$k[X]$-modules de $[V, u]$ correspondent naturellement aux sous-espaces vectoriels de V stables par u.

DÉFINITION 3.22. *On dit que u est cyclique (de polynôme P) si $[V, u]$ est isomorphe à $k[X]/(P)$ pour un certain polynôme P. De façon équivalente, u est cyclique si et seulement si il existe $x \in V$ tel que V est engendré par les $u^n(x), n \geq 0$.*

PROPOSITION 3.23. *Soit $[V, u] = \oplus_{i=1}^m k[X]/(P_i)$ un $k[X]$-module. Alors le polynôme minimal de u est le ppcm des P_i.*

Si u est cyclique de polynôme P, alors $\mu_u = \chi_u = P$.

3.4.2. *Calcul des facteurs invariants.*

THÉORÈME 3.24. *Soit $u \in \mathrm{End}(V)$. Alors les facteurs invariants de $[V, u]$ sont les facteurs invariants non constants de la matrice $X\,\mathrm{Id} - M$, où M est la matrice de u dans une base quelconque de V.*

Comme on l'a vu à la proposition 3.8, pour calculer les facteurs invariants de $[V, u]$ il suffit de trouver une application surjective $\pi : k[X]^r \to [V, u]$ et une application surjective $\phi : k[X]^s \to \ker \pi$.

Notons $(e_1, \ldots, e_n)$ une base de V, et $(f_1, \ldots, f_n)$ la base canonique de $k[X]^n$. On définit une surjection $\pi : k[X]^n \to [V, u]$ par $\pi(f_i) = e_i$.

Soit $M = \mathrm{Mat}_e(u)$, et soit $\tilde{u}$ l'endomorphisme de $k[X]^n$ tel que $\mathrm{Mat}_f(\tilde{u}) = M$. Il vérifie la propriété : pour tout i, $\pi(\tilde{u}(f_i)) = u(e_i)$.

Soit $\phi = X\,\mathrm{Id} - \tilde{u} \in \mathrm{End}(k[X]^n)$. Alors ϕ a pour matrice $X\,\mathrm{Id} - M$ dans la base $(f_1, \ldots, f_n)$.

PROPOSITION 3.25. $\mathrm{Im}\,\phi = \ker \pi$.

DÉMONSTRATION. Le sous-module $\operatorname{Im}\phi$ est engendré par les $\phi(f_i)$. On a $\pi(\phi(f_i)) = \pi(Xf_i - \tilde{u}(f_i)) = 0$. D'où $\operatorname{Im}\phi \subset \ker\pi$.

Soit $m \geq 0$ un entier et $t \in k[X]^n$. Alors $X^m t - \tilde{u}^m(t) \in \operatorname{Im}\phi$. En effet, $X^m \operatorname{Id} - \tilde{u}^m = \phi \circ (\sum_{i=0}^{m-1} X^i \tilde{u}^{m-1-i})$. Soit maintenant $x \in \ker\pi$. On peut écrire $x = \sum_{i=1}^n P_i(X) f_i$. Posons $x_0 = \sum_{i=1}^n P_i(\tilde{u})(f_i)$. D'après le résultat précédent, $x - x_0 \in \operatorname{Im}\phi$.

Soit $V_0 \subset k[X]^n$ le sous-k-ev formé des $\sum \lambda_i f_i$ avec λ_i dans k. Alors π induit un isomorphisme de k-ev entre V_0 et V, et V_0 est stable par $\tilde{u}$. On en déduit que $x_0 = 0$. En effet, $x_0 \in V_0$, et $\pi(x_0) = 0$ puisque on a supposé $x \in \ker\pi$.

Finalement, $x = x - x_0$ est bien dans $\operatorname{Im}\phi$. □

On peut donc utiliser la suite exacte $k[X]^n \xrightarrow{\phi} k[X]^n \xrightarrow{\pi} [V,u] \to 0$ pour calculer les facteurs invariants de $[V,u]$.

3.4.3. *Applications de la classification.* Soit $P_1, \ldots, P_m$ les polynômes unitaires non constants qui sont les facteurs invariants de $[V,u]$. La classification nous donne :

PROPOSITION 3.26. *$[V,u]$ est isomorphe à $\oplus_{i=1}^m k[X]/(P_i)$ comme $k[X]$-module. Il existe une décomposition de V en $\oplus_{i=1}^m V_i$ des sous-espaces stables par u, tels que $u_i = u|_{V_i}$ est cyclique de polynôme P_i.*

COROLLAIRE 3.27. *$\mu_u = P_m$, et $\chi_u = P_1 \ldots P_m$.*

DÉMONSTRATION. La relation sur χ_u vient du fait que $P_1 \ldots P_m = \det\phi$ (à une unité près), où ϕ est défini au paragraphe précédent. □

On remarque qu'on a encore redémontré le théorème de Cayley-Hamilton.

PROPOSITION 3.28. *Soit A et B dans $M_n(k)$. Alors A et B sont semblables si et seulement si $X\operatorname{Id} - A$ et $X\operatorname{Id} - B$ sont équivalentes comme éléments de $M_n(k[X])$.*

3.4.4. *Le cas des corps algébriquement clos.* On suppose maintenant que k est algébriquement clos. Les éléments premiers de $k[X]$ sont alors exactement les $(X - \lambda)$ pour $\lambda \in k$.

On note V_λ la composante $(X-\lambda)$-primaire de $[V,u]$. Alors le corollaire 3.17 donne que $V = \oplus_\lambda V_\lambda$. De plus, $V_\lambda = \oplus_{i=1}^m k[X]/(X-\lambda)^{n_i}$. Le $k[X]$-module $k[X]/(X-\lambda)^n$ correspond à $[V_{\lambda,n}, u_{\lambda,n}]$ où $u_{\lambda,n}$ a pour matrice :

$$\begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

Cela donne donc le :

THÉORÈME 3.29. *Sur un corps algébriquement clos, tout endomorphisme admet une unique décomposition de Jordan.*