Modules et groupes finis

Anna Cadoret

Cours de 3ème année à l'Ecole Polytechnique - version 2018/2019

Préambule

On supposera connues ici les définitions de base concernant les groupes, anneaux, corps et algèbres. Les anneaux considérés seront toujours *associatifs* et *unitaires*.

Les trois premiers cours seront consacrés aux modules sur les anneaux (non nécessairement commutatifs) et les deux cours suivants aux groupes finis. Dans les quatre derniers cours, nous nous intéresserons à la classification des modules sur les algèbres semisimples de dimension finie sur un corps (parfait) et en donnerons plusieurs applications à la théorie des représentations des groupes finis.

Ce cours doit beaucoup aux notes d'un cours de M2 donné par P. Baumann à l'Université de Strasbourg [B09].

Tout au long du cours, nous utiliserons informellement le langage catégoriel (dont le lecteur trouvera un petit lexique en appendice de ce cours) afin d'introduire progressivement ce formalisme qui est devenu le language quotidien de l'algébriste moderne.

Commençons par un petit exemple, illustrant comment les notions d'algèbre et de groupe fini sont intimement liées. Etant donné un anneau commutatif A, à tout groupe fini G on peut associer une A-algèbre $A[G]$ comme suit. La structure de A-module est donnée par

$$A[G] = \bigoplus_{g \in G} Ag$$

et la structure multiplicative est donnée par le 'produit de convolution' :

$$\sum_{g \in G} a(g)g * \sum_{g \in G} a'(g)g = \sum_{g \in G} (\sum_{\gamma \in G} a(\gamma)a'(\gamma^{-1}g))g.$$

$A[G]$ est un anneau associatif unitaire d'élément neutre $1 \cdot e_G$ pour la multiplication (e_G désignant l'élément neutre de G). Notons que l'application

$$\begin{array}{rccc} \iota_G : & G & \to & A[G]^\times \\ & g & \to & 1_A \cdot g \end{array}$$

est un morphisme de groupes injectif.
Si $f : G \to G'$ est un morphisme de groupes, on vérifie que le morphisme de A-modules induit

$$A[f] : A[G] \to A[G']$$

est un morphisme d'anneaux et que si $G \xrightarrow{f} G' \xrightarrow{f'} G''$ sont des morphismes de groupes, on a $A[f' \circ f] = A[f'] \circ A[f]$. Autrement dit

$$A[-] : Grp \to Alg_{/A}$$

est un *foncteur* de la catégorie Grp des groupes finis sur la catégorie $Alg_{/A}$ des A-algèbre. En outre, ce foncteur est *fidèle*, c'est à dire que pour tous groupes finis G, G', l'application

$$A[-] : \mathrm{Hom}_{Grp}(G, G') \to \mathrm{Hom}_{Alg_{/A}}(A[G], A[G'])$$

est injective (on notera qu'elle n'est pas surjective en général, comme le montre l'exemple $G = \mathbb{Z}/2$, $A = \mathbb{Z}/4$ donc que ce foncteur n'est pas *plein*).

Le morphisme de groupes $\iota_G : G \to A[G]^\times$ introduit ci-dessus satisfait la propriété universelle suivante : pour toute A-algèbre B et morphisme de groupe $\phi : G \to B^\times$ il existe un unique morphisme de A-algèbres $\Phi : A[G] \to B$ tel que $\Phi \circ \iota_G = \phi$. Inversement, tout morphisme de A-algèbres $\Phi : A[G] \to B$ induit un morphisme de groupes $\phi := \Phi \circ \iota_G|^{B^\times} : G \to B^\times$. Ces constructions sont inverses l'une de l'autre et définissent une bijection fonctorielle en B :

$$\mathrm{Hom}_{Grp}(G, B^\times) \tilde{\to} \mathrm{Hom}_{Alg_{/A}}(A[G], B).$$

En termes catégoriels, on dit que les foncteurs $A[-] : Grp \to Alg_{/A}$ et $(-)^\times : Alg_{/A} \to Grps$ sont adjoints. Dans le cas particulier où $A = k$ est un corps et $B = M_n(k)$, on obtient par exemple :

$$\mathrm{Hom}_{Grp}(G, \mathrm{GL}_n(k)) \tilde{\to} \mathrm{Hom}_{Alg_{/k}}(k[G], M_n(k)),$$

ce qui montre que les représentations linéaires de dimension n de G sur k correspondent bijectivement aux $k[G]$-modules de k-dimension n.

Le foncteur $A[-] : Grp \to Alg_{/A}$ va plus généralement permettre de ramener les problèmes de théorie des groupes finis (par exemple la classification de leurs représentations, le calcul de leurs groupes de cohomologie) à des problèmes sur les A-algèbres, de type fini comme A-module (par exemple, la classification de leurs modules, le calcul de leur groupes de cohomologie), en général plus facile à traiter grâce à la structure A-linéaire. C'est un exemple du 'principe de linéarisation'.

Table des matières

1 Modules sur un anneau **7**
- 1.1 Définition et premiers exemples . . . 7
- 1.2 Opérations sur les modules . . . 9
  - 1.2.1 Sous A-module, intersection, module engendré par une partie . . . 9
  - 1.2.2 Limites . . . 9
  - 1.2.3 Produits tensoriels . . . 13
- 1.3 Conditions de finitude . . . 18
- 1.4 Atomisation d'un A-modules I : Modules indécomposables . . . 19
  - 1.4.1 Modules indécomposables . . . 19
  - 1.4.2 Théorème de Krull-Schmidt . . . 19
  - 1.4.3 Modules de type fini sur les anneaux principaux . . . 21
- 1.5 Atomisation II : Modules simples . . . 27
  - 1.5.1 A-modules simples et semisimples . . . 27
  - 1.5.2 Suites de composition et théorème de Jordan-Holder . . . 29
  - 1.5.3 Extensions . . . 31

2 Groupes finis - compléments **35**
- 2.1 Echauffement : le groupe symétrique . . . 35
- 2.2 Théorèmes de Sylow, p-groupes . . . 36
  - 2.2.1 Théorèmes de Sylow . . . 36
  - 2.2.2 p-groupes . . . 38
- 2.3 Extensions . . . 39
  - 2.3.1 Atomisation d'un groupe (fini) . . . 39
  - 2.3.2 Groupes finis simples . . . 39
  - 2.3.3 Extensions, produits semidirects . . . 40

3 Représentations linéaires des groupes finis **47**
- 3.1 Anneaux semisimples . . . 47
  - 3.1.1 Anneaux semisimples . . . 47
  - 3.1.2 Théorèmes de structure . . . 48
- 3.2 Récoltes : représentations linéaires des groupes finis . . . 52
  - 3.2.1 K-algèbres semisimples de dimension finie (résumé) . . . 52
  - 3.2.2 Applications à $K[G]$ . . . 52
  - 3.2.3 Une application à la théorie des groupes finis : le théorème de Burnside . . . 59
- 3.3 $K[G]$-modules induits . . . 61
  - 3.3.1 Foncteurs de restriction et d'induction . . . 61
  - 3.3.2 Restriction des représentations induites . . . 62
  - 3.3.3 Caractère d'une représentation induite et critère d'irréductibilité de Mackey . . . 63
  - 3.3.4 Représentations linéaires irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$ ($2 \not| q$) . . . 66

4 Indications / Corrections de (la plupart des) exercices **69**
- 4.1 Chapitre 1 . . . 69
- 4.2 Chapitre 2 . . . 75
- 4.3 Chapitre 3 . . . 79

5 Annales 2014/2019 **89**
5.1 Examen 2014/2015 . . . 89
5.1.1 Enoncé . . . 89
5.1.2 Corrigé . . . 91
5.2 Examen 2015/2016 . . . 95
5.2.1 Enoncé . . . 95
5.2.2 Corrigé . . . 101
5.3 Examen 2016/2017 . . . 105
5.3.1 Enoncé . . . 105
5.3.2 Corrigé . . . 108
5.4 Examen 2017/2018 . . . 112
5.4.1 Enoncé . . . 112
5.4.2 Corrigé . . . 114

6 Appendice : Un peu de vocabulaire catégoriel **119**

Chapitre 1

Modules sur un anneau

Ce chapitre constitue une introduction modeste à la notion de modules sur des anneaux (non nécessairement commutatifs). Ces objets sont au coeur de l'algèbre moderne : géométrie algébrique, théorie des nombres, topologie algébrique et, bien sûr, théorie des représentations. Dans un premier temps, on passera en revue quelques définitions/constructions élémentaires (section 2). On commencera ensuite (section 3) à s'intéresser de plus près à la classification des modules sur un anneau sous certaines conditions de finitude. L'idée consiste à se ramener à des modules les plus petits possible et à tenter de reconstruire tous les modules à partir de ceux-ci. En général, cette intuition est trop naive : les petits modules auxquels on réussit à se ramener sont encore trop gros (les modules indécomposables du théorème de Krull-Schmidt) pour pouvoir être classifiés. On dispose cependant d'une classe de modules encore plus petits que les modules indécomposables et que l'on sait souvent assez bien classifier (les modules simples du théorème de Jordan-Holder). Mais là le problème c'est que la connaissance des modules simples ne suffit pas en général à reconstruire tous les modules car deux modules simples peuvent parfois se combiner de nombreuses façons différentes ; c'est le problème de la détermination des extensions derrière lequel se profilent les méthodes d'algèbre homologique. Lorsque l'anneau A a suffisamment de bonnes propriétés l'idée marche cependant bien. On le verra par exemple pour les modules de type finis sur les anneaux principaux (section 4).

Nous reviendrons sur le problème de la classification dans le chapitre 3, où nous étudierons le cas des anneaux semisimples (là, l'idée marche parfaitement !) et des algèbres de dimension finies sur un corps.

1.1 Définition et premiers exemples

Soit M un groupe abélien. L'ensemble $\mathrm{End}(M)$ des endomorphismes de M comme groupe abélien, muni de l'addition induite par l'addition de M et de la composition est un anneau associatif unitaire (d'unité l'identité Id_M de M).

Soit A un anneau. On appelle *A-module à gauche* (ou module à gauche sur A) tout couple (M, θ) où M est un groupe abélien et

$$\theta : A \to \mathrm{End}(M)$$

est un morphisme d'anneaux. Dans la pratique, s'il n'y a pas de confusion possible, on notera simplement $a \cdot m := \theta(a)(m)$, $a \in A$, $m \in M$. On peut définir de façon équivalente un A-module à gauche comme un couple (M, α), où M est un groupe abélien et

$$\alpha : A \times M \to M$$

une application vérifiant les propriétés suivantes :

- (Distributivité) $\alpha(a, m + m') = \alpha(a, m) + \alpha(a, m')$, $a \in A$, $m, m' \in M$ et $\alpha(a + a', m) = \alpha(a, m) + \alpha(a', m)$, $a, a' \in A$, $m \in M$;
- (Associativité) $\alpha(aa', m) = \alpha(a, \alpha(a', m))$, $a, a' \in A$, $m \in M$;
- (Neutre) $\alpha(1, m) = m$

Là encore, s'il n'y a pas de confusion possible, on notera simplement $a \cdot m := \alpha(a, m)$, $a \in A$, $m \in M$.

On a une définition analogue de A-module à droite. Un A-module à droite M définit un A^{op}-module à gauche (où A^{op} est l'anneau ayant la même structure additive $(A, +)$ que A et dont la structure multiplicative est donnée par $a \cdot_{A^{op}} a' = a' \cdot_A a$, $a, a' \in A$). Et inversement. Ces deux notions sont donc équivalentes. Lorsqu'on ne précisera pas, un

A-module sera toujours un A-module à gauche.

Soit M, M' deux A-modules. On appelle morphisme de A-modules tout morphisme de groupes abéliens $f : M \to M'$ qui est A-linéaire *i.e.* vérifie

$$f(a \cdot m) = a \cdot f(m),\ a \in A,\ m \in M.$$

On notera $\mathrm{Hom}_A(M, M')$ l'ensemble des morphismes de A-modules de M dans M'. C'est encore un A-module. Lorsque $M' = A$, on note $M^\vee :=\mathrm{Hom}_A(M, A)$ et on dit que c'est le *A-module dual* de M. Lorsque $M' = M$ on note $\mathrm{End}_A(M) :=\mathrm{Hom}_A(M, M)$.

Etant donnés M, M', M'' des A-modules, on dispose d'une loi de composition

$$\begin{array}{rccc} \circ : & \mathrm{Hom}_A(M', M'')\times\ \mathrm{Hom}_A(M, M') & \to & \mathrm{Hom}_A(M, M'') \\ & (f', f) & \to & f' \circ f \end{array}$$

qui est A-bilinéaire, associative, possède des identités à gauche et à droite. En particulier, les A-modules forment une *catégorie* (*cf.* appendice), que l'on notera parfois $\mathrm{Mod}_{/A}$.

Exemple 1.1.1

1. Soit A un anneau. Tout idéal à gauche (resp. à droite) est un A-module à gauche (resp. à droite). En particulier, on a
   — le A-module régulier A ;
   — le A-module trivial $\{0\}$, qui est caractérisé par les propriétes suivantes :
   (i) Pour tout A-module M on a $|\mathrm{Hom}_A(M, 0)| = 1$;
   (ii) Pour tout A-module M on a $|\mathrm{Hom}_A(0, M)| = 1$.
   En termes catégoriels, (i) dit que 0 est un objet terminal dans la catégorie des A-modules et (ii) dit que c'est un objet initial. On appelle 0-objet un objet qui est à la fois terminal et initial.
2. Lorsque $A = k$ est un corps commutatif, la notion de k-module coincide avec celle de k-espace vectoriel rencontrée dans les petites classes.
3. La catégorie des $\mathbb{Z}$-modules et celle des groupes abéliens sont équivalentes.
4. Par définition, tout A-module est un groupe abélien et tout morphisme de A-modules est un morphisme de groupes abéliens. en termes catégoriels, on a un foncteur d'oubli naturel
   $$Oub : \mathrm{Mod}_{/A} \to \mathrm{Mod}_{/\mathbb{Z}}$$
   qui consiste à 'oublier' la structure de A-module sur A. Ce foncteur est essentiellement surjectif si A est de caractéristique 0 ou si M est annulé par la caractéristique de A. Il est également *fidèle* mais il est loin d'être *plein* : entre deux A-modules M et M', il y a en général beaucoup moins de morphismes de A-modules que de morphismes de groupes abéliens et, partant, beaucoup plus de (classes d'isomorphismes de) A-modules que de classes d'isomorphismes de groupes abéliens.
5. Un A-module M est toujours muni d'une structure de $\mathrm{End}(M)$-module (et de $\mathrm{End}_A(M) \subset \mathrm{End}(M)$ module) par $\phi \cdot m = \phi(m)$. On utilisera souvent cette observation dans les preuves conceptuelles.
6. Soit $f : A' \to A$ un morphisme d'anneaux alors tout A-module M est muni d'une structure de A'-module définie par la composition
   $$A' \xrightarrow{f} A \to \mathrm{End}(M).$$
   On notera $f_*(M)$ le A'-module ainsi obtenu, que l'on appelle la *restriction de M à A'*. En fait,
   $$f_* : \mathrm{Mod}_{/A} \to \mathrm{Mod}_{/A'}$$
   définit un *foncteur* (*cf.* appendice).
7. Soit A un anneau commutatif. Par la propriété universelle de l'anneau des polynômes [1], la donnée d'un $A[X_1, \ldots, X_n]$-module est équivalente à la donnée d'un couple $(M, \underline{\phi})$, où M est un A-module et $\underline{\phi} := (\phi_1, \ldots, \phi_n)$ est un n-uplet d'endomorphismes A-linéaires de M qui commutent deux à deux. Par exemple, si V est un k-espace vectoriel de dimension finie, et $u \in \mathrm{End}_k(V)$, on peut munir V de la structure V_u de $k[X]$-module définie par $P(X) \cdot v = P(u)(v)$. Si $u, u' \in \mathrm{End}_k(V)$, on a
   $$\mathrm{Hom}_{k[X]}(V_u, V_{u'}) = \{\varphi : V \to V \mid \varphi \circ u = u' \circ \varphi\}.$$
   Un certain nombre de résultats d'algèbre linŕaire s'interprètent (et deviennent bien plus naturels) en termes de $k[X]$-modules.

1. Rappelons que la A-algèbre $\iota : A \hookrightarrow A[X]$ vérifie la propriété universelle suivante : pour toute A-algèbre $\phi : A \to B$ et pour tous $b_1, \ldots, b_n \in B$ commutant deux à deux, il existe un unique morphisme de A-algèbres $f : A[X_1, \ldots, X_n] \to B$ tel que $f(X_i) = b_i$. De façon équivalente, pour toute A-algèbre $\phi : A \to B$, l'application canonique
$$\mathrm{Hom}_{A-Alg}(A[X_1, \ldots, X_n], B) \to B^n,\ f \to (f(X_1), \ldots, f(X_n))$$
est bijective.

1.2 Opérations sur les modules

Soit A un anneau. Nous allons passer ici en revue quelques opérations classiques sur les A-modules. Sans le dire, on est en fait en train de vérifier que la catégorie des A-modules est abélienne et que lorsque A est commutatif, elle est aussi tensorielle. Les preuves sont purement formelles et laissées en exercices au lecteur. Le titre de la section 1.2.2 vient de ce que les noyaux, conoyaux, produits, sommes directes *etc.* sont des cas particuliers de ce qu'en termes catégoriels on appelle des limites. Par manque de temps, nous n'aborderons pas cette notion dans sa généralité mais nous invitons le lecteur à se reporter par exemple au chapitre 2 de [S10].

1.2.1 Sous A-module, intersection, module engendré par une partie

Si M est un A-module, on appelle *sous A-module* de M tout couple (M', i), où M' est un A-module et $i : M' \hookrightarrow M$ un morphisme injectif de A-modules. Dans la pratique, on identifiera M' et son image $i(M') \subset M$.

Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on vérifie immédiatement que l'intersection

$$\bigcap_{i\in I} M_i \subset M$$

est encore un sous-A-module de M.

Si $X \subset M$ est un sous-ensemble, on note $\langle X\rangle$ l'intersection de tous les sous A-modules $M' \subset M$ contenant X. D'après ce qui précède, c'est encore un sous A-module de M et, par construction, c'est le plus petit sous A-module de M contenant X. On dit que $\langle X\rangle$ est le *sous A-module* engendré par X et on vérifie qu'il coincide avec l'ensemble des éléments de la forme $\sum_{x\in X} a(x)x$, où $a : X \to A$ est une application à support fini. Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on note

$$\sum_{i\in I} M_i = \langle \bigcup_{i\in I} M_i\rangle \subset M.$$

1.2.2 Limites

1.2.2.1 Produits et sommes directes

Soit M_i, $i \in I$ une famille de A-modules.

On munit le groupe abélien produit $\prod_{i\in I} M_i$ de la structure de A-module

$$\begin{array}{ccc} A \times \prod_{i\in I} M_i & \to & \prod_{i\in I} M_i \\ (a, \underline{m} = (m_i)_{i\in I}) & \to & a \cdot \underline{m} = (a \cdot m_i)_{i\in I}. \end{array}$$

Avec cette structure de A-module, les projections canoniques $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ deviennent des morphismes de A-modules.

On note $\bigoplus_{i\in I} M_i \subset \prod_{i\in I} M_i$ le sous A-module des $\underline{m} = (m_i)_{i\in I}$ tels que

$$|\{i \in I \mid m_i \neq 0\}| < +\infty.$$

Les injections canoniques $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ sont des morphismes de A-modules. Si I est fini, on a tautologiquement $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$

Lemme 1.2.1

- *(1.2.1.1) Pour toute famille de morphismes de A-modules $f_i : M \to M_i$, $i \in I$ il existe un unique morphisme de A-modules $f : M \to \prod_{i\in I} M_i$ tel que $p_i \circ f = f_i$, $i \in I$.*
- *(1.2.1.2) Pour toute famille de morphismes de A-modules $f_i : M_i \to M$, $i \in I$ il existe un unique morphisme de A-modules $f : \bigoplus_{i\in I} M_i \to M$ tel que $f \circ \iota_i = f_i$, $i \in I$.*

Preuve On procède par analyse-synthèse. (1.2.1.1) Si f existe, les relations $p_i \circ f = f_i$, $i \in I$ imposent $f(m) = (f_i(m))_{i\in I}$. On vérifie immédiatement que cela définit bien un morphisme de A-modules. (1.2.1.2) Si f existe, les relations $f \circ \iota_i = f_i$, $i \in I$ imposent $f((m_i)_{i\in I}) = \sum_{i\in I} f_i(m_i)$ (qui est bien défini puisque seuls un nombre fini de m_i

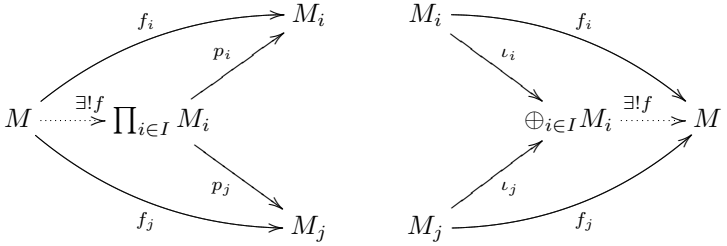
sont non-nuls). On vérifie immédiatement que cela définit bien un morphisme de A-modules. □

On peut aussi réécrire 1.2.1 en disant que, pour tout A-module M les morphismes canoniques

$$\mathrm{Hom}_A(M, \prod_{i\in I} M_i) \to \prod_{i\in I} \mathrm{Hom}_A(M, M_i),\ f \to (p_i \circ f)_{i\in I}$$

$$\mathrm{Hom}_A(\oplus_{i\in I} M_i, M) \to \prod_{i\in I} \mathrm{Hom}_A(, M_i M),\ f \to (f \circ \iota_i)_{i\in I}$$

sont des isomorphismes ou encore, plus visuellement :



En termes catégoriels, le Lemme 1.2.1 dit que les $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ représentent le foncteur

$$\prod_{i\in I} \mathrm{Hom}_A(-, M_i) : \mathrm{Mod}_{/A} \to \mathrm{Mod}_{/A}$$

et que les $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ représentent le foncteur

$$\prod_{i\in I} \mathrm{Hom}_A(M_i, -) : \mathrm{Mod}_{/A} \to \mathrm{Mod}_{/A},$$

Remarque 1.2.2 (Unicité des objets universels) Lorsqu'un foncteur $F : \mathcal{C} \to Ens$ est représentable, l'objet qui le représente est toujours unique à unique isomorphisme près ; c'est une conséquence du lemme de Yoneda (*cf.* appendice). Ainsi les $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ et les $\iota_j : M_j \hookrightarrow \oplus_{i\in I} M_i$, $j \in I$ sont uniques à unique isomorphisme près. On peut bien sûr aussi le vérifier à la main en utilisant l'existence et l'unicité de f dans le lemme 1.2.1. Donnons l'argument pour le produit : supposons qu'il existe deux familles de morphismes de A-module $p_i : \Pi \to M_i$, $i \in I$ et $p'_i : \Pi' \to M'_i$, $i \in I$ qui vérifient (1.2.1.1). En appliquant (1.2.1.1)

- (1.2.2.1) pour les $p'_i : \Pi \to M'_i$, $i \in I$ avec $f_i := p_i$: il existe un unique morphisme de A-modules $f : \Pi \to \Pi'$ tel que $p'_i \circ f = p_i$, $i \in I$.
- (1.2.2.2) pour les $p_i : \Pi \to M_i$, $i \in I$ avec $f_i := p'_i$: il existe un unique morphisme de A-modules $g : \Pi' \to \Pi$ tel que $p_i \circ f = p'_i$, $i \in I$.
- (1.2.2.3) pour les $p'_i : \Pi \to M'_i$, $i \in I$ avec $f_i := p'_i$: il existe un unique morphisme de A-modules $f : \Pi \to \Pi'$ tel que $p'_i \circ f = p'_i$, $i \in I$.
- (1.2.2.4) pour les $p_i : \Pi \to M_i$, $i \in I$ avec $f_i := p_i$: il existe un unique morphisme de A-modules $g : \Pi' \to \Pi$ tel que $p_i \circ f = p_i$, $i \in I$.

Dans (1.2.2.3), $g \circ f$ et Id_Π conviennent donc $g \circ f = Id_\Pi$. De même, dans (1.2.2.4), $f \circ g$ et $Id_{\Pi'}$ conviennent donc $f \circ g = Id_{\Pi'}$. Cela montre que f, g sont des isomorphismes inverses l'un de l'autre.
Dans la suite du cours, nous ne le mentionnerons plus, mais, en vertu de ce principe général, tous les objets universels qui apparaitront (noyaux, conoyaux, produits tensoriels *etc.*) sont toujours uniques à unique isomorphisme près.

Si $M_i = M$ pour tout $i \in I$, on notera $M^I := \prod_{i\in I} M_i$ et $M^{(I)} := \oplus_{i\in I} M_i$. Par construction, on a des isomorphismes de foncteurs canoniques

$$\mathrm{Hom}(A^{(I)}, -) \simeq \prod_{i\in I} \mathrm{Hom}(A, -) \simeq (-)^I$$

et on dit que $A^{(I)}$ est le *A-module libre de base I*.

Soit $f_i : M_i \to N_i$, $i \in I$ une famille de morphismes de A-modules. En appliquant la propriété universelle des $p_j : \prod_{i\in I} N_i \to N_j$, $j \in I$ à la famille de morphismes de A-modules

$$\prod_{i\in I} M_i \xrightarrow{p_j} M_j \xrightarrow{f_j} N_j,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \prod_{i\in I} f_i : \prod_{i\in I} M_i \to \prod_{i\in I} N_i$ tel que $p_i \circ f = f \circ p_i$, $i \in I$. On vérifie qu'on obtient ainsi un foncteur

$$\prod_{i\in I} : (Mod_{/A})^I \to Mod_{/A}.$$

De même, en appliquant la propriété universelle des $\iota_j : M_j \to \oplus_{i\in I} M_i$, $j \in I$ à la famille de morphismes de A-modules

$$M_j \xrightarrow{f_j} N_j \xrightarrow{\iota_j} \oplus_{i\in I} M_i,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \oplus_{i\in I} f_i : \oplus_{i\in I} M_i \to \oplus_{i\in I} N_i$ tel que $f \circ \iota_i = \iota_i \circ f$, $i \in I$. On vérifie qu'on obtient ainsi un foncteur

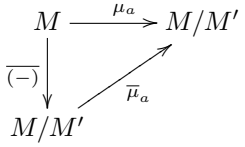
$$\oplus_{i\in I} : (Mod_{/A})^I \to Mod_{/A}.$$

1.2.2.2 Noyaux, conoyaux

Soit $M' \subset M$ un sous A-module. C'est en particulier un sous groupe abélien et on dispose donc du quotient $\overline{(-)} : M \to M/M'$ dans la catégorie des groupes abéliens. On peut munir M/M' d'une structure de A-module comme suit. Pour tout $a \in A$, l'application

$$\begin{array}{rccc} \mu_a : & M & \to & M/M' \\ & m & \to & \overline{a \cdot m} \end{array}$$

est un morphisme de groupes abéliens tel que $M' \subset \ker(\mu_a)$; il se factorise donc en



On pose alors

$$\begin{array}{ccc} A \times M/M' & \to & M/M' \\ (a, \overline{m}) & \to & a \cdot \overline{m} := \overline{\mu}_a(m) (= \overline{a \cdot m}). \end{array}$$

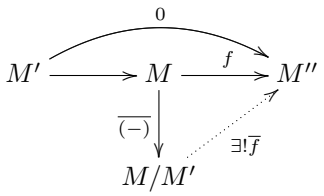
On vérifie immédiatement que cela définit bien une structure de A-module sur M/M' et que c'est l'unique structure de A-module sur M/M' qui fait de $\overline{(-)} : M \to M/M'$ un morphisme de A-modules. De plus,

Lemme 1.2.3 *Pour tout morphisme de A-modules $f : M \to M''$ tels que $M' \subset \ker(f)$, il existe unique morphisme de A-modules $\overline{f} : M/M' \to M''$ tel que $\overline{f} \circ \overline{(-)} = f$.*

On peut aussi réécrire 1.2.3 en disant que, pour tout A-module M'' le morphisme canonique

$$\mathrm{Hom}_A(M/M', M'') \to \{M \xrightarrow{f} M'' \mid M' \subset \ker(f)\},\ \overline{f} \to \overline{f} \circ \overline{(-)}$$

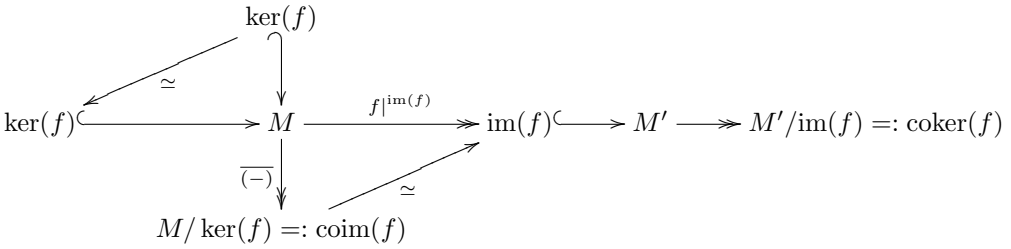
est un isomorphisme ou encore, plus visuellement :



En termes catégoriels, le Lemme 1.2.3 dit que $\overline{(-)} : M \to M/M'$ représente le foncteur

$$\begin{array}{rccc} F : & Mod_{/A} & \to & Mod_{/A} \\ & M'' & \to & F(M'') := \{M \xrightarrow{f} M'' \mid M' \subset \ker(f)\}. \end{array}$$

On observera que $M' = \ker(\overline{(-)})$ et $M/M' = \mathrm{im}(\overline{(-)})$. Inversement, si $f : M \to M'$ est un morphisme de A-modules, on vérifie immédiatement que $\ker(f) \subset M$ et $\mathrm{im}(f) \subset M'$ sont des sous A-modules [2] et qu'on a un diagramme commutatif canonique de morphismes de A-modules



On a donc une correspondance bijective entre sous A-modules et noyaux de morphismes de A-modules d'une part et A-modules quotients et images de morphismes de A-modules d'autre part. Même si les A-modules $\mathrm{im}(f)$ et $M/\ker(f)$ sont isomorphes, on notera parfois $\mathrm{coim}(f) := M/\ker(f)$ (coimage). On note $\mathrm{coker}(f) := M'/\mathrm{im}(f)$ (conoyaux).

1.2.2.3 Suites exactes, lemme du serpent et lemme des cinq

On dit qu'une suite de morphismes de A-modules

$$M_0 \overset{u_0}{\to} M_1 \overset{u_1}{\to} M_2 \overset{u_2}{\to} \cdots \overset{u_n}{\to} M_{n+1}$$

est exacte si $\mathrm{im}(u_i) = \ker(u_{i+1})$ pour tout $0 \leq i \leq n-1$. Une suite exacte courte est une suite exacte de la forme :

$$0 \to M' \to M \to M'' \to 0.$$

La notion de suite exacte est au coeur de l'étude des catégories abéliennes. La raison première est que c'est l'outil qui permet de 'dévisser' un objet compliqué (M) en deux objets plus simples (M' et M'').

Exercice 1.2.4 *Soit*

$$0 \to M' \overset{u}{\to} M \overset{v}{\to} M'' \to 0$$

une suite exacte courte de A-modules. Montrer que les propriétés suivantes sont équivalentes :

1. *il existe un morphisme de A-modules $s : M'' \to M$ tel que $v \circ s = Id_{M''}$;*
2. *il existe un morphisme de A-modules $s : M' \to M'$ tel que $s \circ u = Id_{M'}$;*
3. *il existe un isomorphisme de A modules $f : M \tilde{\to} M' \oplus M''$ tel que $\iota_{M'} = f \circ u$ et $p_{M''} \circ f = v$.*

On dit qu'une suite exacte courte vérifiant les conditions équivalente de l'exercice 1.2.4 est *scindée*.

Exemple 1.2.5

1. *Si $n \geq 2$ est un entier, la suite de $\mathbb{Z}$-modules $0 \to \mathbb{Z} \overset{n\cdot}{\to} \mathbb{Z} \to \mathbb{Z}/n \to 0$ n'est pas scindée.*
2. *On consid'ere les structure de $\mathbb{Z}[X]$-modules suivantes sur $\mathbb{Z}^2$*
   (a) $X \cdot (a,b) = (b,a)$
   (b) $X \cdot (a,b) = (a+b,b)$

   Dans le cas (a), la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \overset{a \to (a,a)}{\to} \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

   est-elle scindée ? Même question avec dans le cas (b), la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \overset{a \to (a,0)}{\to} \mathbb{Z}^2 \to \mathbb{Z} \to 0.$$

2. Et plus généralement que les images directes et images inverses de sous A-modules par des morphismes de A-modules sont encore des sous A-modules.

L'exercice suivant est le point de départ de l'étude cohomologique des suites exactes.

Exercice 1.2.6 *1. Soit*

$$\begin{array}{ccc} M' & \xrightarrow{u'} & M \\ {\scriptstyle\alpha'}\downarrow & & \downarrow{\scriptstyle\alpha} \\ N' & \xrightarrow[v']{} & N \end{array}$$

un diagramme commutatif de morphismes de A-modules. Montrer que $u' : M' \to M$ induit un morphisme canonique $\ker(\alpha') \to \ker(\alpha)$ *et que $v' : N' \to N$ induit un morphisme canonique* $\operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha)$.

2. Soit

$$\begin{array}{ccccccc} & & M' & \xrightarrow{u'} & M & \xrightarrow{u} & M'' \longrightarrow 0 \\ & & {\scriptstyle\alpha'}\downarrow & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha''} \\ 0 & \longrightarrow & N' & \xrightarrow[v']{} & N & \xrightarrow[v]{} & N'' \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

(a) Construire un morphisme 'naturel' $\delta : \ker(\alpha'') \to \operatorname{coker}(\alpha')$ *;*

(b) Montrer que la suite de morphismes

$$\ker(\alpha') \to \ker(\alpha) \to \ker(\alpha'') \xrightarrow{\delta} \operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\alpha'')$$

est exacte.

(c) Montrer que si α', α'' sont injectives (resp. surjectives) alors α est injective (resp. surjective).

(d) On suppose de plus que $u' : M' \to M$ est injective et $v : N \to N''$ est surjective. Montrer que si deux des trois morphismes α, α', α'' sont des isomorphismes alors le troisième l'est aussi.

3. Soit

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \downarrow{\scriptstyle\alpha_3} & & \downarrow{\scriptstyle\alpha_4} & & \downarrow{\scriptstyle\alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

(a) Montrer que si α_1 est surjective et α_2, α_4 sont injectives alors α_3 est injective.

(b) Montrer que si α_5 est injective et α_2, α_4 sont surjectives alors α_3 est surjective.

1.2.3 Produits tensoriels

Nous introduisons ici la notion fondamentale de produit tensoriel. On va distinguer le cas où l'anneau de base est commutatif du cas général.

1.2.3.1 Produit tensoriel de A-modules - A commutatif

Soit $M_1, \ldots, M_r$ et M des A-modules. Notons

$$L_{r,A}(M_1 \times \cdots \times M_r, M)$$

l'ensemble des applications $f : M_1 \times \cdots \times M_r \to M$ qui sont r-A-linéaires *i.e.* telles que $f \circ \iota_i : M_i \to M$ est un morphisme de A-modules, $i = 1, \ldots, r$. La structure de A-module sur M induit une structure de A-module sur $L_{r,A}(M_1 \times \cdots \times M_r, M)$ et on vérifie immédiatement que

$$L_{r,A}(M_1 \times \cdots \times M_r, -) : Mod_{/A} \to Mod_{/A}$$

est un foncteur.

Proposition-Définition 1.2.7 *Il existe un A-module $M_1 \otimes_A \cdots \otimes_A M_r$ et une application r-A-linéaire $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ (uniques à unique isomorphisme près) tels que pour tout A-module M et application r-A-linéaire $f : M_1 \times \cdots \times M_r \to M$ il existe un unique morphisme de A-module $\overline{f} : M_1 \otimes_A \cdots \otimes_A M_r \to M$ vérifiant $\overline{f} \circ p = f$. On traduit cela par le diagramme commutatif :*

$$\begin{array}{ccc} M_1 \times \cdots \times M_r & \xrightarrow{\forall f} & M \\ {\scriptstyle p}\downarrow & \nearrow_{\exists ! \overline{f}} & \\ M_1 \otimes_A \cdots \otimes_A M_r & & \end{array}$$

En termes catégoriels, la Proposition 1.2.7 dit que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ représente le foncteur $L_{r,A}(M_1 \times \cdots \times M_r, -) : Mod_{/A} \to Mod_{/A}$. On dit que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ est 'le' *produit tensoriel* sur A des $M_1, \ldots, M_r$.

Preuve (esq.) Nous allons juste donner la construction de $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$. Notons

$$M_0 := A^{(M_1 \times \cdots \times M_r)},$$

le A-module libre engendré par $M_1 \times \cdots \times M_r$, $(m_1, \ldots, m_r) \in M_0$ l'élément correspondant au terme avec des 0 partout sauf en l'indice $(m_1, \ldots, m_r)$ et $M_{00} \subset M_0$ le sous A-module engendré par les éléments de la forme

$$(m_1, \ldots, a_i m_i + a_i' m_i', \ldots, m_r) - a_i(m_1, \ldots, m_i, \ldots, m_r) - a_i'(m_1, \ldots, m_i', \ldots, m_r).$$

En posant $M := M_0/M_{00}$ et

$$\begin{array}{rccccc} p : & M_1 \times \cdots \times M_r & \to & A^{(M_1 \times \cdots \times M_r)} & \to & M \\ & (m_1, \ldots, m_r) & \to & 1 \cdot (m_1, \ldots, m_r) & \to & (m_1, \ldots, m_r) \mathrm{mod} M_{00} =: m_1 \otimes \cdots \otimes m_r \end{array}$$

on vérifie facilement que $p : M_1 \times \cdots \times M_r \to M$ est une application A-r-linéaire et que (M, p) est 'le' produit tensoriel sur A des $M_1, \ldots, M_r$. □

On note $p(m_1, \ldots, m_r) = m_1 \otimes \cdots \otimes m_r$. La construction ci-dessus montre que $M_1 \otimes_A \cdots \otimes_A M_r$ est engendré comme A-module par les éléments de la forme $m_1 \otimes \cdots \otimes m_r$. Par contre, attention, les éléments de $M_1 \otimes_A \cdots \otimes_A M_r$ ne sont pas tous de cette forme ! !

Si $f_i : M_i \to N_i$, $i = 1, \ldots, r$ sont r morphismes de A-modules, l'application

$$\begin{array}{rccc} (f_1, \ldots, f_r) & M_1 \times \ldots \times M_r & \to & N_1 \otimes_A \ldots \otimes_A N_r \\ & (m_1, \ldots, m_r) & \to & f_1(m_1) \otimes \ldots \otimes f_r(m_r) \end{array}$$

est r-A-linéaire donc se factorise en un morphisme de A-modules $f_1 \otimes_A \ldots \otimes_A f_r : M_1 \otimes_A \ldots \otimes_A M_r \to N_1 \otimes_A \ldots \otimes_A N_r$ tel que $f_1 \otimes_A \ldots \otimes_A f_r(m_1 \otimes \ldots m_r) = (f_1, \ldots, f_r)(m_1, \ldots, m_r) = f_1(m_1) \otimes \ldots \otimes f_r(m_r)$. On vérifie qu'on obtient ainsi un foncteur

$$(Mod_{/A})^r \to Mod_{/A}.$$

Les preuves des deux paragraphes suivants sont purement formelles et, là encore, laissées en exercices.

1.2.3.1.1 Propriétés élémentaires

Lemme 1.2.8 (Le produit tensoriel 'commute' aux sommes directes) *Soit $M_1, \ldots, M_r$ et M des A-modules. On a un isomorphisme canonique*

$$\begin{array}{rccc} M \otimes_A (\bigoplus_{1 \leq i \leq r} M_i) & \tilde{\to} & \bigoplus_{1 \leq i \leq r} (M \otimes_A M_i) \\ m \otimes (m_1 \oplus \cdots \oplus m_r) & \to & (m \otimes m_1) \oplus \cdots \oplus (m \otimes m_r) \end{array}$$

En particulier, si $A = k$ est un corps, et $M_1, \ldots, M_r$ sont de k-dimension finie, $M_1 \otimes_k \cdots \otimes_k M_r$ est de k-dimension $\dim_k(M_1) \cdots \dim_k(M_r)$.

Lemme 1.2.9 (Commutativité et associativité) *On a un isomorphisme (de A-modules) canoniques*

$$\begin{array}{ccc} L \otimes_A (M \otimes_A N) & \tilde{\to} & (L \otimes_A M) \otimes_A N \\ l \otimes (m \otimes n) & \to & (l \otimes m) \otimes n \end{array}$$

$$\begin{array}{ccc} M \otimes_A N & \tilde{\to} & N \otimes_A M \\ m \otimes n & \to & n \otimes m \end{array}$$

Proposition 1.2.10 (Adjonction-1) *On a des isomorphismes (de A-modules) canoniques, fonctoriels en L, M, N*

$$\mathrm{Hom}_A(L, \mathrm{Hom}_A(M, N)) \tilde{\to} L_{r,A}(L \times M, N) \tilde{\to} \mathrm{Hom}_A(L \otimes_A M, N).$$

En termes catégoriels, la Proposition 1.2.10 dit que les foncteurs $- \otimes_A M : Mod_{/A} \to Mod_{/A}$ et $\mathrm{Hom}_A(M, -) : Mod_{/A} \to Mod_{/A}$ sont adjoints.

Exercice 1.2.11

1. *Soit M un A-module. Montrer que le foncteur $\mathrm{Hom}_A(M, -) : Mod_{/A} \to Mod_{/A}$ est exact à gauche i.e. que pour toute suite exacte courte de A-modules*
$$0 \to N' \stackrel{u}{\to} N \stackrel{v}{\to} N'' \to 0$$
la suite
$$0 \to \mathrm{Hom}_A(M, N') \stackrel{u\circ}{\to} \mathrm{Hom}_A(M, N) \stackrel{v\circ}{\to} \mathrm{Hom}_A(M, N'')$$
est exacte. Même question pour le foncteur $\mathrm{Hom}_A(-, M) : Mod^{op}_{/A} \to Mod_{/A}$.
2. *Soit M un A-module. Montrer que le foncteur $- \otimes_A M : Mod_{/A} \to Mod_{/A}$ est exact à droite (on pourra le montrer directement ou utiliser (1)).*
3. *Soit M un A-module et $\mathfrak{i} \subset A$ un idéal. Montrer que $M/\mathfrak{i}M \tilde{\to} M \otimes_A A/\mathfrak{i}$.*
4. *Soit $0 \to M' \stackrel{u}{\to} M \stackrel{v}{\to} M'' \to 0$ une suite exacte courte de $\mathbb{Z}$-modules et p un nombre premier. Montrer qu'on a une suite exacte de $\mathbb{Z}$-modules*
$$M'[p] \stackrel{u}{\to} M[p] \stackrel{v}{\to} M''[p] \stackrel{\delta}{\to} M'/p \stackrel{u}{\to} M/p \stackrel{v}{\to} M''/p \to 0$$
et en déduire une condition suffisante pour que $0 \to M'/p \stackrel{u}{\to} M/p \stackrel{v}{\to} M''/p \to 0$ soit une suite exacte courte de $\mathbb{Z}$-modules.

Proposition 1.2.12 *Supposons que $A = k$ est un corps. On a des isomorphismes canoniques, fonctoriels en M et N*

$$\begin{array}{ccc} M^\vee \otimes_k N & \tilde{\to} & \mathrm{Hom}_k(M, N) \\ f \otimes n & \to & f(-)n\,; \end{array} \quad , \quad \begin{array}{ccc} M^\vee \otimes_k N^\vee & \tilde{\to} & (M \otimes_k N)^\vee \\ f \otimes g & \to & m \otimes n \to f(m)g(n). \end{array}$$

et

$$\begin{array}{ccc} \mathrm{End}_k(M) \otimes_k \mathrm{End}_k(N) & \tilde{\to} & \mathrm{End}_k(M \otimes_k N) \\ f \otimes g & \to & m \otimes n \to f(m) \otimes g(n)\,; \end{array}$$

1.2.3.1.2 Extension/Restriction des scalaires Soit $f : A \to B$ un morphisme d'anneaux commutatifs. L'application

$$\begin{array}{ccc} A \times B & \to & B \\ (a, b) & \to & f(a)b \end{array}$$

munit B d'une structure de A-module.

— Soit M un A-module. L'application

$$\begin{array}{ccc} B \times B \otimes_A M & \to & B \otimes_A M \\ (b_0, b \otimes m) & \to & (b_0 b) \otimes m \end{array}$$

est bien définie et munit $B \otimes_A M$ d'une structure de B-module. Plus précisément, cela définit un foncteur

$$f^* := B \otimes_A - : Mod_{/A} \to Mod_{/B}$$

(qui envoie un A-module M sur le B-module $B \otimes_A M$ et un morphisme de A-module $\phi : M \to M'$ sur le morphisme de B-modules $Id_B \otimes \phi : B \otimes_A M \to B \otimes_A M'$).

— Inversement, on a vu qu'on disposait du foncteur de restriction (exemple 1.1.1 (5))

$$f_* : Mod_{/B} \to Mod_{/A}.$$

Proposition 1.2.13 (Adjonction-2) *Soit M un A-module et N un B-module. On a un isomorphisme canonique (de $\mathbb{Z}$-modules) fonctoriel en M, N*

$$\mathrm{Hom}_A(M, f_*N) \tilde{\to} \mathrm{Hom}_B(f^*M, N).$$

En termes catégoriels, la Proposition 1.2.13 dit que les foncteurs $f_* : Mod_{/B} \to Mod_{/A}$ et $f^* : Mod_{/A} \to Mod_{/B}$ sont adjoints.

Exercice 1.2.14

1. *Soit $A \to B$ et $A \to C$ deux morphismes d'anneaux commutatifs. Montrer que le produit tensoriel $B \otimes_A C$ est canoniquement muni d'une structure de A-algèbre.*
2. *Soit $I, J \subset A$ deux idéaux. Montrer qu'on a un isomorphisme canonique de A-algèbres*

   $$(A/I) \otimes_A (A/J) \tilde{\to} A/(I + J).$$

   Par exemple, si m, n sont deux entiers, calculer

   $$\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n.$$

3. *Si $\varphi : A \to B$ est un morphisme d'anneaux et $P \in A[X]$, montrer qu'on a un isomorphisme canonique de B-algèbres*

   $$B \otimes_A (A[X]/P) \tilde{\to} B[X]/\varphi(P)$$

   (on note encore $\varphi : A[X] \to B[X]$ le morphisme obtenu en appliquant φ aux coefficients).
   Calculer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Est-ce un corps ? Même question avec $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

1.2.3.2 Produits tensoriels de A-modules - A quelconque

Soit A un anneau associatif unitaire. On aimerait définir un foncteur produit tensoriel $- \otimes - : Mod_{/A} \times Mod_{/A} \to Mod_{/A}$ possédant les mêmes propriétés que dans le cas des anneaux commutatifs. La construction dans le cas des anneaux commutatifs ne se généralise pas telle quelle (pourquoi ?) mais en ajustant les définitions, on peut s'en sortir.

Soit M un A-module à droite, N un A-module (à gauche) et Z un $\mathbb{Z}$-module. On dit qu'un morphisme $\mathbb{Z}$-bilinéaire $\phi : M \times N \to Z$ est *A-équilibré* si pour tout $m \in M$, $n \in N$ et $a \in A$ on a

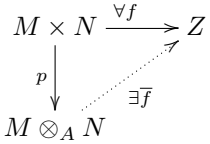
$$\phi(ma, n) = \phi(m, an).$$

On note $\mathrm{Hom}_{A-eq}(M \times N, Z)$ l'ensemble des morphismes A-équilibrés. La structure de $\mathbb{Z}$-module sur Z induit une structure de $\mathbb{Z}$-module sur $\mathrm{Hom}_{A-eq}(M \times N, Z)$ et on vérifie immédiatement que

$$\mathrm{Hom}_{A-eq}(M \times N, -) : Mod_{/\mathbb{Z}} \to Mod_{/\mathbb{Z}}$$

est un foncteur.

Proposition-Définition 1.2.15 *Il existe un $\mathbb{Z}$-module $M \otimes_A N$ et un morphisme A-équilibré $p : M \times N \to M \otimes_A N$ (uniques à unique isomorphisme près) tels que pour tout $\mathbb{Z}$-module Z et morphisme A-équilibré $f : M \times N \to Z$ il existe un unique morphisme de $\mathbb{Z}$-modules $\overline{f} : M \otimes_A N \to Z$ vérifiant $\overline{f} \circ p = f$. On traduit cela par le diagramme commutatif :*



En termes catégoriels, la Proposition 1.2.15 dit que $p : M \times N \to M \otimes_A N$ représente le foncteur $\mathrm{Hom}_{A-eq}(M \times N, -) : Mod_{/\mathbb{Z}} \to Mod_{/\mathbb{Z}}$. On dit que $p : M \times N \to M \otimes_A N$ est 'le' *produit tensoriel* sur A de M et N.

On construit $M \otimes_A N$ exactement comme dans la preuve de la proposition 1.2.7. En particulier, $M \otimes_A N$ est engendré, comme $\mathbb{Z}$-module, par les éléments de la forme $p(m,n) =: m \otimes n$.

Avec cette construction, on obtient les propriétés escomptées.

Proposition 1.2.16 (Adjonction-1) *On a des isomorphismes (de $\mathbb{Z}$-modules) canoniques, fonctoriels en M, N et Z*

$$\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbb{Z}}(N,Z)) \tilde{\to} \mathrm{Hom}_{A-eq}(M \times N, Z) \tilde{\to} \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, Z).$$

(On a muni ici $\mathrm{Hom}_{\mathbb{Z}}(N,Z)$ de la structure de A-module à droite définie par $f \cdot a := f(- \cdot a) : N \to Z$)).

Remarquons que $M \otimes_A N$ est un $\mathbb{Z}$-module mais pas un A-module en général. Cependant, si $f : A \to B$ est un morphisme d'anneaux, l'application

$$\begin{array}{ccc} B \times A & \to & B \\ (b,a) & \to & bf(a) \end{array}$$

munit B d'une structure de A-module à droite.

— Pour tout A-module M, l'application

$$\begin{array}{ccc} B \times B \otimes_A M & \to & B \otimes_A M \\ (b_0, b \otimes m) & \to & (b_0 b) \otimes m \end{array}$$

est bien définie et munit $B \otimes_A M$ d'une structure de B-module. Plus précisément, cela définit un foncteur

$$f^* := B \otimes - : Mod_{/A} \to Mod_{/B}$$

(qui envoie un A-module M sur le B-module $B \otimes_A M$ et un morphisme de A-module $\phi : M \to M'$ sur le morphisme de B-modules $Id_B \otimes \phi : B \otimes_A M \to B \otimes_A M'$).

— Inversement, on dispose toujours du foncteur de restriction

$$f_* : Mod_{/B} \to Mod_{/A}$$

Proposition 1.2.17 (Adjonction-2) *Soit M un A-module et N un B-module. On a un isomorphisme canonique, fonctoriel en M, N de $\mathbb{Z}$-modules*

$$\mathrm{Hom}_A(M, f_*N) \tilde{\to} \mathrm{Hom}_B(f^*M, N).$$

En termes catégoriels, la proposition 1.2.17 dit que les foncteurs $f^* : Mod_{/A} \to Mod_{/B}$ et $f_* : Mod_{/B} \to Mod_{/A}$ sont adjoints.

On retrouve également les propriétés suivantes (qui se démontrent exactement comme dans le cas du produit tensoriel de A-modules - A abélien en utilisant les propriétés universelles pour construire l'application et son inverse).

Lemme 1.2.18 *1. Soit M un A-module à droite et M_i, $i \in I$ des A-modules à gauche. On a un isomorphisme canonique de $\mathbb{Z}$-modules*

$$M \otimes_A (\oplus_{i \in I} M_i) \tilde{\to} \oplus_{i \in I} (M \otimes_A M_i).$$

2. Soit M_i, $i \in I$ des A-modules à droite et M un A-module un A-module à gauche. On a un isomorphisme canonique de $\mathbb{Z}$-modules

$$(\oplus_{i \in I} M_i) \otimes_A M \tilde{\to} \oplus_{i \in I} (M_i \otimes_A M).$$

3. Soit $A \xrightarrow{f} B \xrightarrow{g}$ des morphismes d'anneaux. On a un isomorphisme canonique de C-modules

$$C \otimes_B (B \otimes_A M) \tilde{\to} C \otimes_A M.$$

1.3 Conditions de finitude

Soit A un anneau.

Un A-module M est *de type fini* s'il existe un sous-ensemble fini $X \subset M$ tel que $M = \langle X \rangle$. De façon équivalente, un A-module M est de type fini s'il existe un morphisme surjectif de A-modules $A^n \twoheadrightarrow M$. Un A-module M est de *presentation finie* s'il existe une suite exacte

$$A^{m'} \to A^m \to M \to 0$$

(autrement dit, on demande non seulement que M n'ait qu'un nombre fini de générateurs mais aussi que ces générateurs ne vérifient qu'un nombre fini de relations).

Lemme 1.3.1 *Soit M un A-module. Les conditions suivantes sont équivalentes.*

1. *Toute suite croissante de sous A-modules*

$$M_0 \subset M_1 \subset \ldots \subset M_n \subset M_{n+1} \subset \ldots \subset M$$

   est stationnaire à partir d'un certain rang ;
2. *Tout ensemble non vide de sous A-modules de M possède un élément maximal pour l'inclusion ;*
3. *Tout sous A-module de M est de type fini.*

Un A-module M vérifiant les conditions équivalentes du Lemme 1.3.1 est dit *noetherien*.

Preuve. (1) $\Rightarrow$ (2) : Si (2) n'était pas vrai, il existerait un ensemble non vide $\mathcal{E}$ de sous A-modules de M ne contenant aucun élément maximal pour l'inclusion. Soit $M_0 \in \mathcal{E}$. Comme M_0 n'est pas maximal pour l'inclusion, il existe $M_1 \in \mathcal{E}$ tel que $M_0 \subsetneq M_1$. On itère l'argument avec M_1 et on construit ainsi une suite strictement croissante infinie de sous A-modules de M, ce qui contredit (1).
(2) $\Rightarrow$ (3) : Soit $M' \subset M$ un sous A-module et $\mathcal{E}$ l'ensemble des sous A-modules de type fini de M'. Comme le module trivial $\{0\}$ est dans $\mathcal{E}$, $\mathcal{E}$ est non-vide donc admet un élément M'' maximal pour l'inclusion. Pour tout $m \in M'$, le A-module $M'' + Am$ est dans $\mathcal{E}$ et contient M''. Par maximalité de M'', on a $M'' + Am = M''$ donc $m \in M''$.
(3) $\Rightarrow$ (1) : Soit

$$M_0 \subset M_1 \subset \ldots \subset M_n \subset M_{n+1} \subset \ldots \subset M$$

une suite croissante de sous A-modules. La réunion

$$U := \bigcup_{n \geq 0} M_n \subset M$$

est un sous A-module. Soit $m_1, \ldots, m_r$ une famille de générateurs de U. Chaque m_i est dans M_{n_i} pour un certain $n_i \geq 0$. Avec

$$N := \max\{n_i \mid i = 1, \ldots, r\}$$

on a $M_n = M_N$, $n \geq N$. □

Lemme 1.3.2 *Soit M un A-module. Les conditions suivantes sont équivalentes.*

1. *Toute suite décroissante de sous A-modules*

$$M \supset \ldots \supset M_0 \supset M_1 \supset \ldots \supset M_n \supset M_{n+1} \supset \ldots$$

   est stationnaire à partir d'un certain rang ;
2. *Tout ensemble non vide de sous A-modules de M possède un élément minimal pour l'inclusion.*

Un A-module M vérifiant les conditions équivalentes du Lemme 1.3.2 est dit *artinien*.

Exemple 1.3.3

1. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est ni noetherien ni artinien.

2. Le $\mathbb{Z}$-module régulier est noetherien mais pas artinien.
3. Le $\mathbb{Z}$-module $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ est artinien mais pas noetherien (observer que les sous $\mathbb{Z}$-modules de $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ sont les $(\mathbb{Z}\frac{1}{p^n} + \mathbb{Z})/\mathbb{Z}$, $n \geq 0$).
4. Tout $\mathbb{Z}$-module fini est à la fois noetherien et artinien. Si A est une algèbre sur un corps k, tout A-module de k-dimension finie est à la fois noetherien et artinien.

Exercice 1.3.4

1. *Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de A-modules. Montrer que M est noetherien (resp. artinien) si et seulement si M' et M'' sont noetheriens (resp. artininens).*
2. *Montrer qu'une somme directe finie de A-modules noetheriens (resp. artiniens) est encore noetherien (resp. artinien).*
3. *On dit qu'un anneau A est noetherien (resp. artinien) si le A-module régulier l'est. Montrer que tout module de type fini sur un anneau noethérien (resp. artinien) est noetherien (resp. artinien). Montrer que tout module de type fini sur un anneau noethérien est de présentation finie.*

Exercice 1.3.5 *Soit $f : M \to M$ un endomorphisme de A-module. Montrer que*

1. *Si M est noetherien et f surjectif alors f est un isomorphisme.*
2. *Si M est artinien et f injectif alors f est un isomorphisme.*
3. *(Lemme de 'Fitting') Si M est artinien et noetherien alors il existe une décomposition $M = f^\infty(M) \oplus f^{-\infty}(0)$ en somme directe de deux sous A-modules f-stables tels que la restriction de f à $f^\infty(M)$ soit un automorphisme et la restriction de f à $f^{-\infty}(0)$ soit nilpotente.*

1.4 Atomisation d'un A-modules I : Modules indécomposables

1.4.1 Modules indécomposables

Un A-module M est dit *indécomposable* s'il est non nul et ne peut s'écrire sous la forme $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Un A-module M est dit *totalement décomposable* s'il peut s'écrire sous la forme $M = M_1 \oplus \ldots \oplus M_r$ avec $M_1, \ldots, M_r \subset M$ des sous A-modules indécomposables.

Un anneau E est dit *local* si $E \setminus E^\times$ est un idéal ; auquel cas, $E \setminus E^\times$ est l'unique idéal bilatère maximal de E.

Lemme 1.4.1 *Soit M un A-module. Si $E := \mathrm{End}_A(M)$ est local, M est indécomposable. Réciproquement, si M est artinien et noetherien, E est local.*

Preuve. Supposons E local et qu'on puisse écrire $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Notons $e := \iota_{M'} \circ p_{M'} \in E$ la projection de M sur M' parallèlement à M''. On a $e, 1-e \in E \setminus E^\times$. Mais si E est local, $E \setminus E^\times$ est un idéal donc $1 = e + (1-e) \in E \setminus E^\times$: contradiction. Supposons maintenant que M est un A-module artinien et noetherien indécomposable, d'après l'Exercice 1.3.5 (3), tout élément non nul de E est soit inversible soit nilpotent. En particulier $J := E \setminus E^\times$ est l'ensemble des éléments nilpotents de E. Il suffit de montrer que J est un idéal bilatère. Soit donc $j \in J$ et $e \in E$. Comme j est nilpotent on a $\ker(j) \neq 0$ et $\mathrm{im}(j) \neq M$ (exercice 1.3.5 (1), (2)). Donc aussi $\ker(ej) \neq 0$ et $\mathrm{im}(je) \neq M$, ce qui montre que $ej, je \in E \setminus E^\times = J$. Donc $EJ = JE = J$. Il reste à voir que J est stable par addition. Soit $j, j' \in J$, si $j + j' \in E^\times$ il existerait $e \in E$ tel que $ej = 1 - ej'$. Comme $ej' \in J$, on a forcément $1 - ej' \in E^\times$ (d'inverse $\sum_{n\geq 0}(ej')^n$), ce qui contredit le fait que $j \in J$. □

1.4.2 Théorème de Krull-Schmidt

Notons $Ind(A)$ l'ensemble des classes d'isomorphismes de A-modules indécomposables.

Théorème 1.4.2 (Krull-Schmidt) *Soit M un A-module artinien ou noetherien. Alors il existe une application à support finie $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ telle que*

$$M = \bigoplus_{N \in Ind(A)} N^{\oplus \kappa(N)}.$$

Si M est à la fois artinien et noetherien alors $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ est unique ; on la notera $\kappa_M : Ind(A) \to \mathbb{Z}_{\geq 0}$.

Preuve. Commençons par montrer l'existence de la décomposition. Raisonnons par l'absurde. Si M n'est pas totalement décomposable, M n'est en particulier pas indécomposable donc

$$M = M_1^{(0)} \oplus M_2^{(0)}$$

avec $0 \neq M_1^{(0)}, M_2^{(0)} \subset M$ deux sous A-modules dont l'un au moins des deux - disons $M_1^{(0)}$ n'est pas totalement décomposable. On itère l'argument pour obtenir une suite de décompositions en sommes directes de sous A-modules non nuls

$$M = M_1^{(1)} \oplus M_2^{(1)} \oplus M_2^{(0)}$$
$$\cdots$$
$$M = M_1^{(n+1)} \oplus M_2^{(n+1)} \oplus M_2^{(n)} \oplus M_2^{(n-1)} \oplus \cdots \oplus M_2^{(1)} \oplus M_2^{(0)}$$

avec, à chaque fois, $M_1^{(n)}$ qui n'est pas totalement décomposable. On obtient en particulier une suite strictement croissante de sous A-modules

$$\{0\} \subset M_2^{(0)} \subset M_2^{(1)} \oplus M_2^{(0)} \subset \cdots \subset M_2^{(n)} \oplus \cdots M_2^{(1)} \oplus M_2^{(0)} \subset \cdots$$

et une suite strictement décroissante de sous A-modules

$$M \supset M_1^{(0)} \supset M_1^{(0)} \supset \cdots \supset M_1^{(n)} \supset M_1^{(n+1)} \supset \cdots$$

Supposons maintenant que M est artinien et noetherien et montrons l'unicité de la décomposition. D'après le Lemme 1.4.1 et par récurrence, il suffit de montrer que si on a un isomorphisme de A-modules noetherien et artinien

$$M \oplus M' \simeq N_1 \oplus \ldots \oplus N_s =: N$$

avec $E := \mathrm{End}_A(M)$ local et les $N_1, \ldots, N_s$ indécomposables alors il existe $1 \leq i \leq s$ tel que $M \simeq N_i$ et $M' \simeq \oplus_{j \neq i} N_j$. Soit $\Phi = (\phi\ \phi') : M \oplus M' \tilde{\to} N$ un isomorphisme de A-modules d'inverse

$$\Psi = \begin{pmatrix} \psi \\ \psi' \end{pmatrix} : N \tilde{\to} M \oplus M'.$$

Par le lemme 1.4.1, $E \setminus E^\times$ est un idéal bilatère et l'égalité

$$Id_M = \psi \circ \phi = \sum_{1 \leq i \leq s} \psi \circ \iota_i \circ p_i \circ \phi$$

implique que $\chi_i := \psi \circ \iota_i \circ p_i \circ \phi \in E^\times$ pour au moins un $i = 1, \ldots, s$. On a alors $p_i \circ \phi : M \hookrightarrow N_i$ injectif, $\psi \circ \iota_i : N_i \twoheadrightarrow M$ surjectif et

$$0 \longrightarrow \ker(\psi \circ \iota_i) \longrightarrow N_i \underset{p_i \circ \phi \circ \chi_i^{-1}}{\overset{\psi \circ \iota_i}{\rightleftarrows}} \mathrm{im}(\psi \circ \iota_i) \longrightarrow 0$$

donc

$$N_i = \ker(\psi \circ \iota_i) \oplus \mathrm{im}(p_i \circ \phi).$$

Comme par hypothèse N_i est indécomposable on a forcément $\ker(\psi \circ \iota_i) = 0$ et $\mathrm{im}(p_i \circ \phi) = N_i$. Donc $p_i \circ \phi : M \tilde{\to} N_i$ et $\psi \circ \iota_i : N_i \tilde{\to} M$ sont des isomorphismes. Il reste à voir que $M' \simeq \oplus_{j \neq i} N_j$. Pour cela, considérons les suites exactes courtes de A-modules :

$$0 \to M \overset{\iota}{\to} M \oplus M' \overset{p}{\to} M' \to 0$$
$$0 \to \bigoplus_{i \neq j} N_j \overset{\Psi \circ \iota_i'}{\to} M \oplus M' \overset{p_i \circ \Phi}{\to} N_i \to 0.$$

On sait que $p_i \circ \Phi \circ \iota = p_i \circ \phi : M \tilde{\to} N_i$ est un isomorphisme et on voudrait montrer que $p \circ \Psi \circ \iota_i' : \bigoplus_{i \neq j} N_j \to M'$ en est un aussi. Cela découle du petit lemme suivant, dont on laisse la preuve en exercice au lecteur. □

Lemme 1.4.3

1. *Soit* $0 \to K \overset{\alpha}{\to} M \overset{\beta}{\to} Q$ *et* $0 \to K' \overset{\alpha'}{\to} M \overset{\beta'}{\to} Q'$ *deux suites exactes de* A*-modules. Alors* $\beta'\alpha$ *est injectif si et seulement si* $\beta\alpha'$ *est injectif.*
2. *Soit* $K \overset{\alpha}{\to} M \overset{\beta}{\to} Q \to 0$ *et* $K' \overset{\alpha'}{\to} M \overset{\beta'}{\to} Q' \to 0$ *deux suites exactes de* A*-modules. Alors* $\beta'\alpha$ *est surjectif si et seulement si* $\beta\alpha'$ *est surjectif.*

1.4.3 Modules de type fini sur les anneaux principaux

Rappelons qu'un anneau commutatif intègre A est dit *principal* si tous ses idéaux sont de la forme Aa, $a \in A$. Rappelons aussi que dans un anneau principal tout idéal premier est maximal et que les éléments irréductibles sont premiers.

Exemple 1.4.4

- Tout corps commutatif.
- Tout anneau de valuation discrète, par exemple, l'anneau $k[[T]]$ des séries formelles sur un corps commutatif k, l'anneau des entiers p-adiques $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n$, le localisé $A_{\mathfrak{p}}$ d'un anneau intégralement clos A en un idéal premier $\mathfrak{p}$ de hauteur 1. On rappelle qu'un anneau de valuation discrète est un anneau commutatif intègre A de corps des fractions k et vérifiant les propriétés équivalentes suivantes.
  1. Il existe un morphisme surjectif de groupes $v : (k^\times, \times) \to (\mathbb{Z}, +)$ tel que $v(x+y) \geq \inf\{vx), v(y)\}$ et $A \setminus \{0\} = v^{-1}([0, +\infty[)$;
  2. A est principal et possède un unique idéal premier non nul ;
  3. A est noetherien, local et son unique idéal maximal est engendré par un élément non nilpotent.
- Tout anneau euclidien *i.e.* muni d'une application (= sthasme) $\nu : A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ telle que pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ avec $a = bq + r$ et $\nu(r) < \nu(b)$. Les anneaux de valuations discrètes sont euclidiens. L'anneau $\mathbb{Z}$ et l'anneau $k[T]$ des polynômes à une indéterminée sur un corps commutatif k sont euclidiens.
- Les anneaux d'entiers quadratiques fournissent aussi des exemples d'anneaux (noetheriens) qui peuvent être euclidiens ($\mathbb{Z}[\sqrt{d}]$ avec $d = -1, -2$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ avec $d = -7, -8, -11$), principaux non euclidiens ($\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ avec $d = -19, -43, -69, -163$), factoriels non principaux ($\mathbb{Z}[\sqrt{3}]$), non factoriel ($\mathbb{Z}[i\sqrt{5}]$) *etc.* Rappelons plus généralement qu'on a les implications suivantes :

$$\begin{array}{ccccc} \text{Euclidien} & \Rightarrow & \text{Principal} & \Rightarrow & \text{Factoriel} \\ & & \Downarrow & & \Downarrow \\ & & \text{noetherien} & \Rightarrow & \text{Existence factorisation en produit d'irréductibles.} \end{array}$$

Soit M un A-module. Un élément $m \in M$ est dit *de torsion* s'il existe $0 \neq a \in A$ tel que $am = 0$. On note $T_M \subset M$ l'ensemble des éléments de torsion de M. On vérifie immédiatement que c'est un sous A-module et que le A-module M/T_M est sans torsion. Le A-module M s'insère donc dans la suite exacte courte

$$(*) \quad 0 \to T_M \to M \to M/T_M \to 0,$$

où T_M est de torsion et M/T_M est sans torsion. Cela indique la voie pour classifier les A-modules de type fini : montrer que la suite exacte courte $(*)$ se scinde, ce qui par l'Exercice 1.2.4 impliquera automatiquement que

$$M \tilde{\to} T_M \oplus M/T_M$$

et réduit donc le problème de la classification des A-modules de type fini à

- la classification des A-modules de type fini sans torsion ;
- la classification des A-modules de type fini de torsion.

En fait, on va plutôt procéder dans l'ordre suivant. Notons que comme A est noterien et M de type fini, M est noetherien. Donc T_M et M/T_M sont aussi noetheriens donc de type fini.

1. Tout d'abord, la raison pour laquelle on se restreint aux A-modules de type fini provient du lemme suivant.

   Lemme 1.4.5 *Un A-module de type fini est noetherien. Un A-module de type fini et de torsion est noetherien et artinien.*

   Preuve. Comme A est principal, tous ses sous A-modules (=idéaux) sont de type fini donc A est noetherien ; la première partie de l'énoncé résulte donc de l'Exercice 1.3.4. Supposons M de torsion. Soit $m_1, \ldots, m_r \in M$ un

système de générateurs. Pour chaque $i = 1, \dots, r$ on peut trouver un élément $0 \neq a_i \in A$ tel que $a_i m_i = 0$. On a donc une factorisation

$$\begin{array}{ccc} A^r & \xrightarrow{(m_1,\dots,m_r)} & M \\ \downarrow & \nearrow & \\ A/Aa_1 \times \cdots \times A/Aa_r & & \end{array}$$

D'après l'Exercice 1.3.4, il suffit donc de montrer que les A-module de la forme A/Aa avec $0 \neq a \in A$ sont artiniens. Soit

$$A/Aa =: M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} \supset \cdots$$

une suite décroissante de sous A-modules. Notons $\pi : A \to A/Aa$ la projection canonique et posons :

$$I_n := \pi^{-1}(M_n),\ n \geq 0.$$

Par construction on obtient une suite décroissante d'idéaux

$$A = I_0 \supset I_1 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots Aa.$$

Chacun de ces idéaux est de la forme $I_n = Aa_n$ avec $0 \neq a_n \in A$ et $a_n | a$. Mais comme un anneau principal est factoriel, a n'a qu'un nombre fini de diviseurs deux à deux non associés. Il n'y a donc qu'un nombre fini d'idéaux dans la suite I_n, $n \geq 0$. □

2. On va ensuite montrer que tout A-modules libre (sur un anneau intègre) est classifié par son rang et qu'un A-module de type fini sans torsion sur un anneau principal est libre de rang fini. Cela permettra aussi d'appliquer l'observation suivante.

   Lemme 1.4.6 *Si M'' est un A-module libre alors toute suite exacte courte de A-modules $0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ ests scindée.*

   Preuve. On construit une section en utilisant la propriété universelle de la somme directe. Plus précisément, quitte à composer v par un isomorphisme, on peut supposer que $M'' = A^{(I)}$. Pour chaque $i \in I$ notons $e_i = (\delta_{i,j})_{j \in I} \in A^{(I)}$ et choisissons $m_i \in I$ tel que $v(m_i) = e_i$. Le choix de m_i définit un morphisme de A-module $s_i : Ae_i \xrightarrow{e_i \to m_i} Am_i \hookrightarrow M$. Par propriété universelle des $\iota_i : Ae_i \to A^{(I)}$, $i \in I$, on en déduit un unique morphisme $s : A^{(I)} \to M$ tel que $s \circ \iota_i = s_i$, $i \in I$. Par construction $v \circ s = Id$. On conclut par l'Exercice 1.2.4. □
3. D'après le Lemme 1.4.5 et le Théorème de Krull-Schmidt 1.4.2, T_M est totalement décomposable ; le point sera donc de classifier les modules indécomposables de torsion sur un anneau principal A. On montrera que ce sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier (=maximal) de A et $n \geq 0$.

1.4.3.1 Classification des A-modules de type fini sans torsion

Supposons d'abord que A est seulement un anneau commutatif intègre.

Lemme 1.4.7 *Un A-module de type fini sans torsion est isomorphe à un sous A-module d'un A-module libre de type fini.*

Preuve. Soit $m_1, \dots m_r \in M$ un système de générateur. L'ensemble

$$\mathcal{S} := \{I \subset \{1, \dots, r\} \mid A^I \overset{(m_i)_{i \in I}}{\hookrightarrow} M\}$$

est non vide puisque M est sans torsion donc contient un élément $I \subset \{1, \dots, r\}$ maximal pour l'inclusion. Notons

$$N := \sum_{i \in I} Am_i \simeq A^I.$$

Par maximalité de I, pour chaque $j \in I^c := \{1, \dots, r\} \setminus I$ il existe $0 \neq a_j \in A$ tel que $a_j m_j \in N$. Notons $a := \prod_{j \in I^c} a_j \in A$; c'est un élément non nul de A puisque A est intègre. On en déduit que le morphisme de A-module

$$\begin{array}{ccc} M & \to & N \\ m & \to & am \end{array}$$

est injectif, puisque M est sans torsion. □

Lemme 1.4.8 (Classification des A-modules libres de type fini par le rang)

1. *Le A-module libre $A^{(I)}$ est de type fini si et seulement si $|I| < +\infty$.*
2. *Soit I, J deux ensembles finis. Alors $A^{(I)}$ et $A^{(J)}$ sont isomorphes comme A-modules si et seulement si $|I| = |J|$.*

Preuve. L'idée est de se ramener au cas des espaces vectoriels sur un corps pour lesquels le lemme est connu. Soit donc M un A-module libre de type fini et $\mathfrak{m} \subset A$ un idéal maximal. Comme M est de type fini, le $k := A/\mathfrak{m}$ espace vectoriel $M/\mathfrak{m}M = M \otimes_A A/\mathfrak{m}$ est de dimension finie - disons r - sur k. Soit I un ensemble pour lequel on a un isomorphisme de A-modules

$$f : A^{(I)} \tilde{\to} M.$$

Posons $m_i := f(e_i)$, où e_i est le 'i-ème vecteur de la base canonique', $i \in I$. On va montrer que $|I| = r$. Pour cela, il suffit de montrer que les images $\overline{m}_i$, $i \in I$ des m_i, $i \in I$ dans $M/\mathfrak{m}M$ forment une k-base de $M/\mathfrak{m}M$. Puisque f est surjective, les $\overline{m}_i$, $i \in I$ forment une famille génératrice. Montrons qu'elle est libre. Soit $a : I \to A$ à support fini telle que

$$\sum_{i \in I} a(i) m_i \in \mathfrak{m}M.$$

Comme $M = \oplus_{i \in I} A m_i$ et $A \tilde{\to} A m_i$, $a \to a m_i$, $i \in I$, cela implique $a(i) \in \mathfrak{m}$ donc $\overline{a}_i = 0$, $i \in I$. □

Le Lemme 1.4.8 montre en particulier que si M est un A-module libre de type fini il existe un unique entier $r \geq 1$ tel que $M \simeq A^{\oplus r}$. On appelle cet entier le *rang* du A-module libre M.

Supposons maintenant que A *est principal.*

Lemme 1.4.9 *Un sous A-module d'un A-module libre de rang fini r est un A-module libre de rang $\leq r$.*

Preuve. On procède par récurrence sur r. Si $r = 1$, cela résulte du fait que A est principal. Supposons que l'énoncé du Lemme 1.4.9 est vérifié pour tout A-module libre de rang $\leq r$. Soit $M \subset A^{\oplus(r+1)}$ un sous A-module. Notons $p_{r+1} : A^{\oplus(r+1)} \twoheadrightarrow A$ la $r+1$-ième projection canonique. Comme $\ker(p_{r+1}) \simeq A^{\oplus r} \subset A^{\oplus(r+1)}$ est un A-module libre de rang r, par hypothèse de récurrence, le sous A-module $M \cap \ker(p_{r+1}) \subset \ker(p_{r+1})$ est un A-module libre de rang $s \leq r$. Comme $p_{r+1}(M) \subset A$ est un idéal et que A est principal, il existe $d_0 \in A$ et $m_0 \in M$ tel que $p_{r+1}(M) = A d_0 \overset{\cdot d_0}{\tilde{\leftarrow}} A$ et on conclut par le Lemme 1.4.6. □

Exercice 1.4.10

1. *Soit A un anneau commutatif et $f : A^{\oplus r} \to A^{\oplus s}$ un morphisme de A-modules. Montrer que si f est injectif alors $r \leq s$.*
2. *Donner un contre-exemple au Lemme 1.4.9 lorsque A n'est pas principal.*

On vient donc de montrer

Corollaire 1.4.11 *Un A-module de type fini sans torsion est libre de rang fini. Plus précisément, l'application $\mathbb{Z}_{\geq 0} \to \mathrm{Mod}_{/A}$, $r \to A^{\oplus r}$ induit une bijection de $\mathbb{Z}_{\geq 0}$ sur l'ensemble des classes d'isomorphismes de A-modules de type fini sans torsion.*

En particulier, M/T_M est un A-module libre de rang fini - disons r - donc, par le Lemme 1.4.6 on a

$$M \simeq T_M \oplus M/T_M \simeq T_M \oplus A^{\oplus r}.$$

Il reste à classifier les A-modules de type fini qui sont de torsion.

1.4.3.2 Classification des A-modules de type fini de torsion

Soit A un anneau principal.

Théorème 1.4.12 *Les A-modules de type fini de torsion qui sont indécomposables sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p} \subset A$ est un idéal premier non nul et $n \in \mathbb{Z}_{\geq 0}$.*

Preuve. Vérifions d'abord qu'un A-module de la forme $A/\mathfrak{p}^n$ est indécomposable. Observons (c'est par exemple la factorialité de A) que

$$\mathrm{End}_A(A/\mathfrak{p}^n) \simeq \mathrm{End}_{A/\mathfrak{p}^n}(A/\mathfrak{p}^n) \simeq A/\mathfrak{p}^n$$

a un unique idéal maximal - $\mathfrak{p}/\mathfrak{p}^n$, donc est local. Le fait que $A/\mathfrak{p}^n$ est indécomposable résulte alors du lemme 1.4.1. Montrons maintenant que tout A-module indécomposable est de cette forme. Soit M un A-module. Pour tout $m \in M$, on note

$$Ann_A(m) := \{a \in A \mid am = 0\} \subset A$$

l'idéal annulateur de m et on se fixe un générateur $a_m \in Ann_A(m)$. On note également

$$Ann_A(M) := \bigcap_{m \in M} Ann_A(m) \subset A$$

l'idéal annulateur de M.

Lemme 1.4.13 *Il existe $m \in M$ tel que $Ann_A(m) = Ann_A(M)$.*

Preuve du lemme 1.4.13. Soit $m_1, \ldots, m_r$ un système de générateurs de M comme A-module. On a

$$Ann_A(M) = \cap_{1 \leq i \leq r} Ann_A(m_i).$$

Il suffit donc de montrer que pour tout $m_1, m_2 \in M$ il existe $m_3 \in M$ tel que

$$Ann_A(m_1) \cap Ann_A(m_2) = Ann_A(m_3).$$

Ecrivons $Ann_A(m_i) = Aa_i$, $i = 1, 2$. Comme A est factoriel, en utilisant la décomposition en produit de facteurs irréductibles de a_1 et a_2, on peut écrire $a_1 = \alpha_1\beta_1$ et $a_2 = \alpha_2\beta_2$ avec α_1, α_2 premier entre eux de produit 'le' plus petit commun multiple de a_1 et a_2. Posons $m_3 := \beta_1 m_1 + \beta_2 m_2$ et vérifions que m_3 convient. On a clairement $Ann_A(m_1) \cap Ann_A(m_2) \subset Ann_A(m_3)$. Pour l'inclusion réciproque, soit $a \in Ann_A(m_3)$. On a $a\beta_1 m_1 = -a\beta_2 m_2$. Par Bézout, il existe $u, v \in A$ tels que $u\alpha_1 + v\alpha_2 = 1$. On a donc

$$a\beta_1 m_1 = (u\alpha_1 + v\alpha_2)a\beta_1 m_1 = au\underbrace{a_1 m_1}_{=0} + v\alpha_2 a\beta_1 m_1 = -av\underbrace{a_2 m_2}_{=0} = 0.$$

Donc $a\beta_1 \in Ann_A(m_1) = Aa_1$ et $a\beta_2 \in Ann_A(m_2) = Aa_2$ en particulier a est un multiple commun de α_1 et α_2 donc de $\alpha_1\alpha_2 = ppcm(a_1, a_2)$. Donc $a \in Ann_A(m_1) \cap Ann_A(m_2)$. □

Notons $B := A/Ann_A(m) = A/Ann_A(M)$ et considérons la suite exacte courte

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0.$$

On notera que comme $Ann_A(M)$ annnule M, cette suite est également une suite de B-modules.

Lemme 1.4.14 *La suite exacte courte de B-modules*

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0$$

est scindée.

Elle est donc *a fortiori* scindée comme suite exacte courte de A-modules *i.e.*

$$M \simeq A/Ann_A(M) \oplus M/Am$$

comme A-module. Mais comme M est indécomposable (et non nul), on en déduit $M = Am \simeq A/Ann_A(M) = A/Aa_m$. On conclut par la factorialité de A, le lemme 1.4.15 et l'indécomposabilité de M. □

Preuve du lemme 1.4.14. On peut la déduire directement du lemme 1.5.13 et de l'exercice 1.5.14. Mais donnons-en un argument 'self-contained'. Introduisons l'ensemble $\mathcal{E}$ des couples (u, N) où $m \in N \subset M$ est un sous-B-module et $u : N \to B$ un morphisme de B-modules tel que $u(m) = 1$. On munit $\mathcal{E}$ de la relation d'ordre $\leq$ définie par $(u_1, N_1) \leq (u_2, N_2)$ si $N_1 \subset N_2$ et $u_2|_{N_1} = u_1$. $\mathcal{E}$ est non-vide : par définition $B = A/Ann_A(m)$ donc on a un isomorphisme $v : B \tilde{\to} Bm$ et $(Am, v^{-1}) \in \mathcal{E}$. Par définition, $\mathcal{E}$ est un ensemble ordonné inductif donc admet un élément maximal (u, N) (en fait, ici, on peut invoquer le fait que M est noetherien, ce qui permet d'éviter le Lemme

de Zorn). Montrons que $N = M$. Sinon, soit $\mu \in M \backslash N$ et montrons qu'on peut étendre $u : N \to B$ en $u_1 : N + B\mu \to B$. Pour cela, il faut 'deviner' la bonne valeur de $u_1(\mu)$. Introduisons l'idéal

$$\mathfrak{i} := \{b \in B \mid b\mu \in N\} \subset B.$$

Ecrivons $Ann_A(M) = Aa$. Comme B est quotient de l'anneau principal A, $\mathfrak{i} = Ab/Aa$ avec $Aa \subset Ab$ *i.e.* $a = \alpha b$ pour un certain $\alpha \in A$. Notons $u(b\mu) = \overline{c}$ (on note $\overline{\ }$ les classes modulo Aa). On a $u(a\mu) = 0 = \alpha\overline{c}$ donc $\alpha c = qa = q\alpha b$ dans A. Mais comme A est intègre $c = qb$. On a donc envie de poser $u_1(\mu) = \overline{q}$. Définissons $u_0 : N \oplus B \to B$ par $u_0(n \oplus \lambda) = u(n) + \lambda\overline{q}$. On a

$$\ker(N \oplus B \twoheadrightarrow N + B\mu, n \oplus \lambda \to n + \lambda\mu) = \{\beta b\mu \oplus -\beta b \mid \beta \in B\} \subset \ker(u_0)$$

En effet, $u_0(\beta b\mu \oplus -\beta b) = u(\beta b\mu) - \beta b\overline{q} = \beta u(b\mu) - \beta b\overline{q} = \beta\overline{c} - \beta b\overline{q} = 0$. Donc $u_0 : N \oplus B \to B$ passe au quotient en $u_1 : N + B\mu \to B$ avec $u_1|_N = u$. Cela contredit la maximalité de (u, N). □

Soit $I_1, \ldots, I_r \subset A$ des idéaux et considérons le produit des projections canoniques $p := \prod_{1\leq i\leq r} p_{I_i} : A \to \prod_{1\leq i\leq r} A/I_i$; c'est un morphisme d'anneaux de noyau $\cap_{1\leq i\leq r} I_i$. De plus

Lemme 1.4.15 (Restes chinois) *Si $I_i + I_j = A$, $1 \leq i \neq j \leq r$ alors $\cap_{1\leq i\leq r} I_i = I_1 \cdots I_r$ et $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective. Inversement, si $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective alors $I_i + I_j = A$, $1 \leq i \neq j \leq r$.*

Preuve. Supposons d'abord que $I_i + I_j = A$, $1 \leq i \neq j \leq r$. On a toujours $\cap_{1\leq i\leq r} I_i \supset I_1 \cdots I_r$. Pour l'inclusion inverse et la surjectivité de $p := \prod_{1\leq i\leq r} p_{I_i} : A \to \prod_{1\leq i\leq r} A/I_i$, on procède par récurrence sur r. Si $r = 2$, il existe $a_i \in I_i$, $i = 1, 2$ tels que $1 = a_1 + a_2$. En particulier,
— Pour tout $x \in I_1 \cap I_2$, $x = x1 = x(a_1 + a_2) = xa_1 + xa_2 = a_1x + xa_2 \in I_1 \cdot I_2$.
— Soit $x_1, x_2 \in A$ arbitraires. En posant $x = a_1x_2 + a_2x_1$ on a bien $p_{I_1}(x) = p_{I_1}(a_2)p_{I_1}(x_1) = p_{I_1}(x_1)$ et $p_{I_2}(x) = p_{I_2}(a_1)p_{I_2}(x_2) = p_{I_2}(x_2)$.
Si $r \geq 3$, on a par hypothèse de récurrence $I_2 \cap \cdots \cap I_r = I_2 \cdots I_r$ et $A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow \prod_{2\leq i\leq r} A/I_i$. Il suffit de montrer que $I_1 + I_2 \cdots I_r = A$. En effet, le cas $r = 2$ (et l'hypothèse de récurrence) nous donnera alors
— $I_1 \cap (I_2 \cap \cdots \cap I_r) = I_1 \cap (I_1 \cdots I_r) = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r$.
— $A \twoheadrightarrow A/I_1 \times A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow A/I_1 \times \prod_{2\leq i\leq r} A/I_i \twoheadrightarrow \prod_{1\leq i\leq r} A/I_i$
Mais pour $i = 2, \ldots, r$ il existe $a_i \in I_1$, $b_i \in I_i$ tels que $a_i + b_i = 1$. On a donc $1 = \prod_{2\leq i\leq r}(a_i + b_i) = \prod_{2\leq i\leq r} a_i + \cdots \in I_1 + I_2 \cdots I_r$.
Inversement, si $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective, pour tout $1 \leq i \neq j \leq r$, il existe $x \in A$ tel que $p(x) = (\delta_{i,k})_{1\leq k\leq r} \in \prod_{1\leq i\leq r} A/I_i$ *i.e.* $x \in 1 + I_i$ et $x \in I_j$. Donc $1 = (1 - x) + x \in I_i + I_j$. □

Corollaire 1.4.16 *Soit M un A-module de type fini de torsion. Il existe une unique suite décroissante d'idéaux*

$$A \supsetneq I_1 \supset I_2 \supset \ldots \supset I_r \supsetneq 0$$

telle que

$$M \simeq A/I_1 \oplus \ldots \oplus A/I_r.$$

Preuve. Comme M est artinien et noetherien, d'après le Théorème de Krull-Schmidt 1.4.2, M se décompose de façon unique comme somme directe de modules indécomposables. D'après le Théorème 1.4.12, cette décomposition s'écrit

$$M \simeq \bigoplus_{\mathfrak{p}} \bigoplus_{n\geq 0} A/\mathfrak{p}^{\alpha_{M,\mathfrak{p}}(n)},$$

où la première somme est indexée par l'ensemble $\mathrm{spec}(A)$ des idéaux premiers non nuls de A et

$$\alpha_{M,-} : \mathrm{spec}(A) \to \mathbb{Z}_{\geq 0}^{(\mathbb{Z}_{\geq 0})}$$

est une application à support fini telle que $\alpha_{M,\mathfrak{p}} = (\alpha_{M,\mathfrak{p}}(n))_{n\geq 0}$ est une suite décroissante dont les termes sont nuls pour $n \gg 0$. Pour chaque $\mathfrak{p} \in \mathrm{spec}(A)$ choisissons un générateur p de $\mathfrak{p}$ comme A-module. Soit $n \geq 0$ le plus grand des entiers tels qu'il existe $\mathfrak{p} \in \mathrm{spec}(A)$ pour lequel $\alpha_{M,\mathfrak{p}}(n) \neq 0$ et posons

$$a_{n+1-j} := \prod_{\mathfrak{p}} p^{\alpha_{M,\mathfrak{p}}(j)},\ j = 1, \ldots, n.$$

La suite d'idéaux $I_i := Aa_j$, $j = 1, \ldots, n$ vérifie alors la propriété de l'énoncé. Leur unicité résulte de l'unicité dans le théorème de Krull-Schmidt. □

On dit que la suite $A \supsetneq I_1 \supset I_2 \supset \ldots \supset I_r \supsetneq 0$ est la *suite des invariants* du A-module M.

1.4.3.3 Applications

On peut appliquer la classification des A-modules de type fini sur un anneau principal à l'anneau $\mathbb{Z}$ pour obtenir le classique théorème de classification des groupes finis.

Corollaire 1.4.17 *Soit M un groupe abélien de type fini. Il existe un unique $r \in \mathbb{Z}_{\geq 0}$ et une unique suite d'entiers positifs $d_1|d_2|\dots|d_s$ tels que*

$$M \simeq \mathbb{Z}^r \oplus (\oplus_{1\leq i\leq s}\mathbb{Z}/d_i).$$

Exercice 1.4.18 *Donner la liste des groupes abéliens d'ordre 6, 18, 24 et 36.*

On peut également appliquer la classification à l'anneau $k[T]$ des polynômes à une indéterminée sur le corps k pour obtenir la classification des classes de conjugaison des endomorphisme d'un k-espace vectoriel de dimension finie par les invariants de similitude. Plus précisément, si V est un k-espace vectoriel de dimension finie tout endomorphisme $u : V \to V$ définit une structure de $k[T]$ module V_u sur V par $P(T)v = P(u)(v)$, $P \in k[T]$, $v \in V$. Le $k[T]$-module V_u est évidemment de type fini et de torsion. Il existe donc une unique suite de polynômes $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ telle que

$$V_u \simeq k[T]/P_{u,1} \oplus \cdots \oplus k[T]/P_{u,r_u}.$$

On dit que la suite $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ est la suite des *invariants de similitude* de l'endomorphisme u.

Exercice 1.4.19 (Classification des classes de conjugaison par les invariants de similitude)

1. *Soit $u, u' : V \to V$ deux endomorphismes. Montrer qu'il existe $\phi \in \mathrm{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ si et seulement si u et u' ont mêmes invariants de similitude.*
2. *Calculer le polynôme minimal et le polynôme caractéristique de u en fonction de sa suite d'invariants de similitude. Montrer plus précisément qu'il existe une base du k-espace vectoriel V dans laquelle u a pour matrice la matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des $P_{u,i}$.*
3. *Calculer le nombre de classes de conjugaison (sous $\mathrm{GL}_n(\mathbb{F}_q)$) dans $M_n(\mathbb{F}_q)$, dans $\mathrm{GL}_n(\mathbb{F}_q)$.*

Exercice 1.4.20 (Théorème de la base adaptée) *Soit A un anneau principal, M un A-module libre de rang r et $N \subset M$ un sous-A-module. L'objectif de cet exercice est de montrer qu'il existe un unique entier $0 \leq s \leq r$, une unique suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ d'idéaux de A et $m_1, \dots, m_r \in M$ tels que*

$$N = \bigoplus_{1\leq i\leq s} Ad_i m_i \subset \bigoplus_{1\leq i\leq r} Am_i = M.$$

1. *Justifier l'unicité (sous réserve d'existence).*
2. *Notons $\mathcal{E}$ l'ensemble des $\lambda(N)$, $\lambda \in \mathrm{Hom}_A(M, A)$. Montrer que $\mathcal{E}$ possède un unique élément maximal $\mathcal{I}$ pour l'inclusion.*
3. *Fixons $f \in \mathrm{Hom}_A(M, A)$ tel que $\mathcal{I} = f(N) = Ad_1$ et $n_1 \in N$ tel que $f(n_1) = d_1$. Montrer qu'il existe $m_1 \in M$ tel que $n_1 = d_1 m_1$. En déduire que $M = Am_1 \oplus \ker(f)$ et $N = Ad_1 m_1 \oplus \ker(f) \cap N$.*
4. *Conclure par récurrence sur le rang de M.*

Exercice 1.4.21 (Classes d'équivalence) *On considère l'action de $\mathrm{GL}_n(A)\times\mathrm{GL}_m(A)$ sur $M_{n,m}(A)$ donnée par $(P, Q)\cdot M = PMQ^{-1}$. Montrer que l'ensemble des classes d'équivalence $M_{n,m}(A)/\mathrm{GL}_n(A)\times\mathrm{GL}_m(A)$ est classifié par les suites $Ad_1 \supset Ad_2 \supset \dots \supset Ad_n$ d'idéaux de A. Noter que dans le cas où $A = k$ est un corps commutatif, on retrouve le thèorème de classification des classes d'équivalence par le rang de la matrice.*

Exercice 1.4.22 *Soit M un $\mathbb{Z}$-module libre de rang fini m et $\phi \in \mathrm{End}_{\mathbb{Z}}(M)$ tel que $\phi \otimes \mathbb{Q} \in \mathrm{Aut}_{\mathbb{Q}}(M \otimes \mathbb{Q})$ est inversible. Montrer que $\phi(M) \subset M$ est d'indice fini et calculer $[M : \Phi(M)$.*

Le théorème de Krull-Schmidt dit essentiellement que les briques de base des A-modules artiniens et noetheriens sont les A-modules indécomposables. Mais le problème c'est qu'en général les A-modules indécomposables peuvent être très gros et, partant, difficiles à déterminer. Il y a certains cas cependant où on sait le faire. On a vu que c'est le cas lorsque A est un anneau principal (c'est vrai plus plus généralement si A est de Dedekind) et on verra que c'est aussi le cas lorsque A est un anneau semisimple. Dans ce second cas, les A-modules indécomposables coincident avec les A-modules simples. En général les A-modules simples sont beaucoup plus petits et donc plus faciles à déterminer que les A-modules indécomposables mais, malheureusement, on ne dispose pas d'un théorème de Krull-Schmidt avec 'simple' à la place de 'indécomposable'. Le théorème de Jordan-Holder sert de substitut (bien imparfait) au théorème de Krull-Schmidt.

1.5 Atomisation II : Modules simples

1.5.1 A-modules simples et semisimples

Un A-module M est dit *simple* (ou *irréductible*) s'il est non nul et si les seuls sous A-modules de M sont $\{0\}$ et M.

Si M est un A-module simple et $0 \neq m \in M$, le morphisme de A-modules

$$\begin{array}{ccc} A & \to & M \\ a & \to & am \end{array}$$

est surjectif et son noyau est un idéal à gauche maximal. Les A-modules simples sont donc exactement les A-modules de la forme $A/\mathfrak{m}$, avec $\mathfrak{m} \subset A$ idéal à gauche maximal. Dans la suite, on notera $\widehat{A}$ l'ensemble des classes d'isomorphismes de A-modules simples.

Un anneau A est dit *à division* si l'ensemble des éléments non nuls est un groupe *i.e.* si $A \setminus \{0\} = A^\times$. En particulier, un anneau à division est local (d'unique idéal maximal 0).

Exemple 1.5.1 *Tout corps commutatif est un anneau à division. Les premiers exemples d'anneaux à division non commutatifs sont fournis par les algèbres de quaternions. Si F est un corps commutatif et $a, b \in k^\times$, on note (a, b) la F-algèbre de dimension 4 sur k $(a, b) = F1 \oplus Fi \oplus Fj \oplus Fk$ et dont la multiplication est donnée par les relations*

$$ij = -ji = k,\ i^2 = a,\ j^2 = b.$$

On note $N : (a, b) \to F$ l'application définie par

$$N(x1 + yi + zj + wk) = (x1 + yi + zj + wk)(x1 - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2.$$

On peut alors montrer que (a, b) est une F-algèbre à division si et seulement si $N^{-1}(0) = 0$. C'est par exemple le cas pour $\mathbb{H} = (-1, -1)$ et $F \subset \mathbb{R}$ (quaternions de Hamilton).

Le lemme suivant est l'analogue du lemme 1.4.1 pour les A-modules simples.

Lemme 1.5.2 (Schur) *Si M, M' sont deux A-modules simples alors*

1. *Soit le seul morphisme de A-modules de M vers M' est le morphisme nul ;*
   Soit il existe un isomorphisme de A-modules $\phi : M \tilde{\to} M'$ induisant un isomorphisme (de A-modules)

   $$\phi^{-1} \circ - : \mathrm{Hom}_A(M, M') \tilde{\to} \mathrm{End}_A(M)$$

   et l'anneau $\mathrm{End}_A(M)$ est un anneau à division.
2. *En particulier, si A est une algèbre sur un corps k algébriquement clos et M est un A-module simple de k-dimension finie, on a $k \tilde{\to} \mathrm{End}_A(M)$.*

Preuve. Pour 1., il suffit d'observer que le noyau et l'image d'un morphisme de A-modules sont encore des A-modules. Pour 2., seule la surjectivité de $k \to \mathrm{End}_A(M)$ n'est pas tout à fait immédiate. Soit donc $\phi : M \tilde{\to} M$ un automorphisme de A-modules. Notons $k[\phi] \subset \mathrm{End}_A(M)$ la sous k-algèbre engendrée par ϕ et $P_\phi \in k[T]$ le polynome minimal de ϕ. On a un isomorphisme de k-algèbres $k[T]/P_\phi \tilde{\to} k[\phi]$. Mais comme $\mathrm{End}_A(M)$ est intègre, $k[\phi]$ l'est aussi. Donc $P_\phi \in k[T]$ est irréductible donc de degré 1 puisque k est algébriquement clos. □

Remark : La preuve de 1.5.2.2 montre que si k est un corps algébriquement clos, la seule k-algèbre à division de k-dimension finie est k.

Corollaire 1.5.3 *Pour tout A-modules simples M_i, $i = 1, \ldots, r$ deux à deux non-isomorphes et pour tout $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 1}$ on a un isomorphisme canonique d'anneaux*

$$\prod_{1 \leq i \leq r} M_{n_i}(\mathrm{End}_A(M_i)) \tilde{\to} \mathrm{End}_A(\bigoplus_{1 \leq i \leq r} M_i^{\oplus n_i}).$$

On retiendra que si M est un A-module artinien et noetherien, on a

$$\begin{array}{ccc} M \text{ indécomposable} & \Leftrightarrow & \mathrm{End}_A(M) \text{ local} \\ \Uparrow & & \Uparrow \\ M \text{ simple} & \Rightarrow & \mathrm{End}_A(M) \text{ anneau à division} \end{array}$$

Lemme 1.5.4 *Soit M un A-module. Les conditions suivantes sont équivalentes.*

1. *Il existe des sous A-modules simples M_i, $i \in I$ de M tels que*
$$M = \sum_{1 \in I} M_i;$$
2. *Il existe des sous A-modules simples M_i, $i \in I$ de M tels que*
$$M = \bigoplus_{i \in I} M_i;$$
3. *Pour tout sous A-module M' de M, il existe une sous-A-module M'' de M tel que*
$$M = M' \oplus M''.$$

On dit qu'un A-module M vérifiant les conditions équivalentes du lemme 1.5.4 est *semisimple*.

Preuve du lemme 1.5.4. (1) $\Rightarrow$ (2) Pour tout $J \subset I$ notons $M_J := \sum_{i \in J} M_i$. Soit $\mathcal{E}$ l'ensemble des sous-A-modules M_J, $J \subset I$ qui vérifient
$$M_J := \sum_{i \in J} M_i = \bigoplus_{i \in J} M_i.$$
Choisissons $M_J \in \mathcal{E}$ maximal* pour l'inclusion et montrons que $M = M_J$. En effet, pour tout $i \in I$, par maximalité de M_J on a $M_J \cap M_i \neq 0$. Or, comme M_i est simple, on a forcément $M_J \cap M_i = M_i \subset M_J$. Ceci étant vrai pour tout $i \in I$, on a $M = \sum_{1 \in I} M_i \subset M_J$.
(2) $\Rightarrow$ (3) Pour tout $J \subset I$ notons $M_J := \oplus_{i \in J} M_i$. Soit $\mathcal{E}$ l'ensemble des sous-A-module M_J, $J \subset I$ qui vérifient
$$M' \oplus M_J.$$
Choisissons $M_J \in \mathcal{E}$ maximal* pour l'inclusion et montrons que $M = M' \oplus M_J$. En effet, pour tout $i \in I$, par maximalité de M_J, $(M' \oplus M_J) \cap M_i \neq 0$. Or, comme M_i est simple, on a forcément $(M' \oplus M_J) \cap M_i = M_i \subset M' \oplus M_J$. Ceci étant vrai pour tout $i \in I$, on a $M = \sum_{1 \in I} M_i \subset M' \oplus M_J$.
(3) $\Rightarrow$ (1) Montrons d'abord :

Lemme 1.5.5 *Tout sous-A-module non nul de M contient un sous-A-module simple.*

Preuve du Lemme 1.5.5. Soit $0 \neq m \in M$. Alors le noyau du morphisme surjectif de A-modules
$$\begin{array}{rccc} \lambda_m : & A & \twoheadrightarrow & Am \\ & a & \to & am \end{array}$$
est un idéal à gauche de A. Il est donc contenu dans un idéal à gauche maximal* $\mathfrak{m}$ de A. En appliquant (3) à $\mathfrak{m}m \subset M$, on trouve un sous-A-module $N \subset M$ tel que $M = \mathfrak{m}m \oplus N$. Comme $\mathfrak{m}m \subset Am$, on a aussi $Am = \mathfrak{m}m \oplus (Am \cap N)$. Maintenant, si on considère le morphisme de A-module surjectif canonique
$$A \overset{a \to am}{\twoheadrightarrow} Am \overset{p_{Am \cap N}}{\twoheadrightarrow} Am \cap N \simeq Am/\mathfrak{m}m,$$
celui-ci se factorise en un morphisme surjectif non nul $A/\mathfrak{m} \twoheadrightarrow Am \cap N$, qui est automatiquement un isomorphisme puisque $A/\mathfrak{m}$ est simple. $\square$

Soit maintenant M_0 le sous-A-module de M somme de tous les sous A-modules simples de M. Si $M_0 \neq M$, d'après (3), il existe un sous A-module non nul M' de M tel que $M = M_0 \oplus M'$. Mais cela contredit la définition de M_0 puisque M' contient un sous-A-module simple de M. $\square$

* : utilise le lemme de Zorn (tout ensemble ordonné inductif admet un élément maximal).

Exercice 1.5.6 *1. Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de A-modules. Montrer que si M est semisimple alors M' et M'' le sont. La réciproque est-elle vraie ?*

2. Montrer que les conditions suivantes sont équivalentes :

(a) Le A-module régulier est semisimple ;

(b) Tout A-module est semisimple.

On dit alors que A est un anneau semisimple.

3. Soit A un anneau à division. Montrer que le seul A-module simple est le A-module régulier et en déduire que tout A-module est libre et semisimple.

4. Soit A un anneau principal. Soit $a_1, \ldots, a_r \in A$ des éléments irréductibles deux à deux non associés et $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 1}$. Montrer que le A-module $A/\langle a_1^{n_1} \cdots a_r^{n_r} \rangle$ est semisimple si et seulement si $n_1 = \ldots = n_r = 1$.

5. ('Théorème' de Maschke) Soit G un groupe fini et k un corps dont la caractéristique est première à l'ordre de G. Montrer que tout $k[G]$-module de k-dimension finie est semisimple. Cela reste-il vrai si on ne suppose plus que la caractéristique de k est première à l'ordre de G ?

1.5.2 Suites de composition et théorème de Jordan-Holder

Soit M un A-module. On appelle suite de composition pour M toute filtration *finie* de M par des sous A-modules

$$F_\bullet(M) \;\; M := F_0(M) \supset F_1(M) \supset \ldots \supset F_n(M) \supset F_{n+1}(M) = 0$$

telle que $F_i(M)/F_{i+1}(M)$ est un A-module simple, $i = 1, \ldots, n$. On dit que le A-module

$$Gr_F(M) = \bigoplus_{0 \leq i \leq n} F_i(M)/F_{i+1}(M)$$

est le *gradué associé* à la filtration $F_\bullet(M)$. Par construction, c'est un A-module semisimple. On associe à la filtration $F_\bullet(M)$ l'application à support fini :

$$I_F : \begin{array}{ccc} \widehat{A} & \to & \mathbb{Z}_{\geq 0} \\ S & \to & I_F(S) \end{array},$$

où pour tout A-module simple S, l'entier $I_F(S)$ est le nombre de $i \in \{1, \ldots, n\}$ tels que $F_i(M)/F_{i+1}(M) \simeq S$.

Lemme 1.5.7 (Papillon) *Soit M un A-module et $M_2 \subset M_1 \subset M$, $N_2 \subset N_1 \subset M$ des sous-A-modules. On a un isomorphisme canonique de A-modules*

$$\frac{M_2 + M_1 \cap N_1}{M_2 + M_1 \cap N_2} \xrightarrow{\sim} \frac{N_2 + N_1 \cap M_1}{N_2 + N_1 \cap M_2}.$$

Preuve. Considérons la restriction de la projection canonique

$$M \twoheadrightarrow \frac{M}{M_2 + M_1 \cap N_2}$$

à $M_1 \cap N_1$. L'image de ce morphisme est

$$\frac{M_1 \cap N_1 + M_2 + M_1 \cap N_2}{M_2 + M_1 \cap N_2} \xrightarrow{\sim} \frac{M_2 + M_1 \cap N_1}{M_2 + M_1 \cap N_2}$$

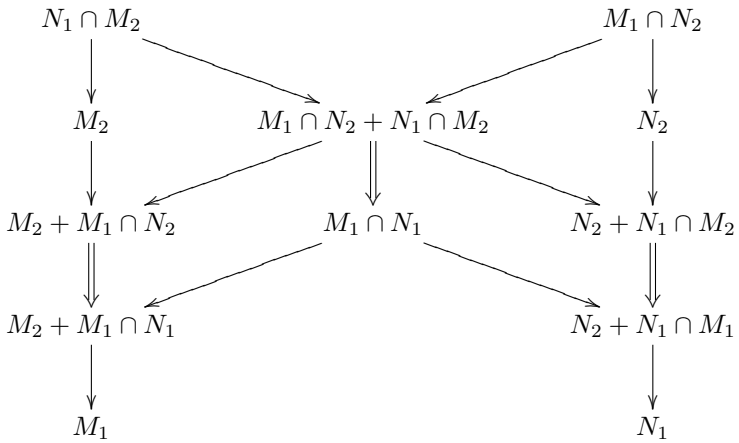
et le noyau est

$$M_1 \cap N_1 \cap (M_2 + M_1 \cap N_2) = M_2 \cap N_1 + M_1 \cap N_2.$$

On obtient donc un isomorphisme

$$\frac{M_1 \cap N_1}{M_2 \cap N_1 + M_1 \cap N_2} \xrightarrow{\sim} \frac{M_2 + M_1 \cap N_1}{M_2 + M_1 \cap N_2}.$$

On conclut en observant que la situation est symétrique en les M_i et les N_i. □



Dans le diagramme ci-dessus, les flèches $\Rightarrow$ correspondent à des quotients isomorphes.

Proposition 1.5.8 (Jordan-Holder) *Un A-module M artinien et noetherien possède une suite de composition. De plus, si $F_\bullet(M)$ et $F'_\bullet(M)$ sont deux suites de composition pour M on a $I_F = I_{F'}$.*

Preuve. Commençons par montrer l'existence d'une suite de composition. Notons $\mathcal{S}$ l'ensemble des sous A-modules de M possédant une suite de composition. L'ensemble $\mathcal{S}$ est non-vide puisqu'il contient 0. Comme M est noetherien, $\mathcal{S}$ possède donc un élément M', maximal pour l'inclusion. Supposons $M' \subsetneq M$. L'ensemble $\mathcal{S}'$ des sous A-modules de M contenant strictement M' est non-vide puisqu'il contient M. Comme M est artinien, $\mathcal{S}'$ possède donc un élément M'', minimal pour l'inclusion. Mais par construction M''/M' est un A-module simple donc, comme M' possède une suite de composition, M'' aussi : cela contredit la maximalité de M'.
Soit maintenant $F_\bullet(M)$ et $F'_\bullet(M)$ deux suites de composition pour M. Notons

$$F_{i,j} := F_i(M) \cap F'_j(M) + F_{i+1}(M),\ F'_{j,i} := F_i(M) \cap F'_j(M) + F'_{j+1}(M).$$

On a

$$\cdots \supset F_{i-1,n+1} = F_{i,0} = F_i(M) \supset F_{i,1} \supset \cdots \supset F_{i,j} \supset F_{i,j+1} \supset \cdots \supset F_{i,n'+1} = F_{i+1}(M) = F_{i+1,0} \supset \cdots,$$

$$\cdots \supset F'_{j-1,n+1} = F'_{j,0} = F'_j(M) \supset F'_{j,1} \supset \cdots \supset F'_{j,i} \supset F'_{j,i+1} \supset \cdots \supset F'_{j,n+1} = F'_{j+1}(M) = F'_{j+1,0} \supset \cdots$$

Les quotient de la première filtration sont les mêmes que ceux de $F_\bullet(M)$ et ceux de la seconde filtration sont les mêmes que ceux de $F'_\bullet(M)$. Plus précisément, comme $F_i(M)/F_{i+1}(M)$ est simple, il existe un unique $0 \leq j \leq n'$ tel que $F_{i,j}(M) \supsetneq F_{i,j+1}(M)$; auquel cas $F_i(M) = F_{i,j}(M)$, $F_{i,j+1}(M) = F_{i+1}(M)$. Et de même pour la seconde filtration. En outre, par le Lemme 1.5.7, on a

$$F_i(M)/F_{i+1}(M) \simeq F_{i,j}/F_{i,j+1} \simeq F'_{j,i}/F'_{j,i+1} \simeq F'_j/F'_{j+1}.\ \square$$

Puisque $I_F : \widehat{A} \to \mathbb{Z}_{\geq 0}$ ne dépend que de M et pas de la filtration $F_\bullet(M)$, on notera simplement $I_M : \widehat{A} \to \mathbb{Z}_{\geq 0}$ et $\mathrm{Gr}(M) := \mathrm{Gr}_F(M)$. On dit que

$$\ell(M) := \sum_{S \in \widehat{A}} I_M(S) \in \mathbb{Z}_{\geq 0}$$

est la *longueur* de M et $I_M(S) \in \mathbb{Z}_{\geq 0}$ la *multiplicité* de M en S, $S \in \widehat{A}$.

Remarque 1.5.9 *1.* Si M est un A-module semisimple, M est isomorphe à $\mathrm{Gr}(M)$. Lorsque M n'est pas semi-simple, on perd en général beaucoup d'information en passant de M à $\mathrm{Gr}(M)$. Par exemple, si on prend pour A le sous-anneau des matrices triangulaires supérieures dans $\mathrm{M}_n(k)$ et pour M le A-module tautologique $k^{\oplus n}$, on voit que $\mathrm{Gr}(M)$ est k^n sur lequel A opère par

$$X\underline{z} = (x_{1,1}z_1, \ldots, x_{n,n}z_n),\ X = (x_{i,j}) \in A, \underline{z} = (z_i) \in k^{\oplus n}$$

Autrement dit, on ne garde que l'information de la diagonale.
Dans le même ordre d'idée, on peut observer que les $\mathbb{Z}$-modules $\mathbb{Z}/9$ et $\mathbb{Z}/3 \oplus \mathbb{Z}/3$ ont le même gradués associés mais ne sont pas isomorphes.

2. On notera également l'importance des hypothèses de finitude. Par exemple le $\mathbb{Z}$-module $\mathbb{Z}$, qui n'est pas artinien, n'admet pas de suite de composition.

Exercice 1.5.10 (Semisimplification) *On a vu qu'à tout A-module artinien et noetherien M on pouvait associer un A-module semisimple $\mathrm{Gr}(M)$ mais telle quelle, cette construction n'est pas fonctorielle. Expliquer comment construire canoniquement la filtration $F_\bullet(M)$ de sorte que tout morphisme de A-modules $f : M \to M'$ induise un morphisme de A-modules $\mathrm{Gr}(f) : \mathrm{Gr}(M) \to \mathrm{Gr}(M')$ et que pour tout morphismes de A-modules $M \xrightarrow{f} M' \xrightarrow{f'} M''$, on ait*

$$\mathrm{Gr}(f' \circ f) = \mathrm{Gr}(f') \circ \mathrm{Gr}(f).$$

1.5.3 Extensions

Soit M' et M'' deux A-modules. On appelle *extension de M'' par M'* toute suite exacte courte de A-modules de la forme

$$(u', u)\ \ 0 \to M' \xrightarrow{u'} M \xrightarrow{u} M'' \to 0$$

et on dit que deux extensions $0 \to M' \xrightarrow{u_i} M_i \xrightarrow{v_i} M'' \to 0$, $i = 1, 2$ sont équivalentes s'il existe un isomorphisme de A-modules $\phi : M_1 \xrightarrow{\sim} M_2$ tel que $u_2 = \phi \circ u_1$ et $v_2 \circ \phi = v_1$. On note $\mathrm{Ext}^1_A(M'', M')$ l'ensemble des classes d'isomorphismes $[u', u]$ d'extensions (u', u) de M'' par M'.

'L'imperfection' du théorème de Jordan-Holder pose le problème de la classification des extensions. Si on connait à la fois les quotients simples successifs $M_i := F_i(M)/F_{i+1}(M)$ et les extensions successives

$$0 \to F_n(M) \to F_{n-1}(M) \to F_{n-1}(M)/F_n(M) \to 0$$

$$0 \to F_{n-1}(M) \to F_{n-2}(M) \to F_{n-2}(M)/F_{n-1}(M) \to 0$$

$$\dots$$

on peut reconstruire M.

Le problème de la détermination de l'ensemble $\mathrm{Ext}^1_A(M'', M')$ est en général difficile et fait appel à des techniques d'algèbre homologique. Faisons cependant quelques remarques simples.

1.5.3.1 Structure de groupe abélien sur $\mathrm{Ext}^1_A(M'', M')$

On peut munir $\mathrm{Ext}^1_A(M'', M')$ d'une structure de groupe abélien. A tout couple d'extensions

$$(u'_i, u_i)\ \ 0 \to M' \xrightarrow{u'_i} M_i \xrightarrow{u_i} M'' \to 0,\ i = 1, 2$$

on associe l'extension

$$(u', u)\ \ 0 \to M' \xrightarrow{u'} M \xrightarrow{u} M'' \to 0$$

définie comme suit. On considère les deux sous A-modules de $M_1 \oplus M_2$

$$K := \{(m_1, m_2) \in M_1 \oplus M_2 \mid u_1(m_1) = u_2(m_2)\},$$

$$D := \{(u'_1(m'), -u'_2(m')) \mid m' \in M'\}$$

On a $D \subset K$; posons $M := K/D$ et

$$u' : \begin{array}{ccc} M' & \to & \dfrac{M}{(u'_1(m'), 0)} \\ m' & \to & \end{array}, \quad u : \begin{array}{ccc} \dfrac{M}{(m_1, m_2)} & \to & M'' \\ & \to & u_1(m_1) \end{array}.$$

On vérifie que la suite

$$(u', u)\ \ 0 \to M' \xrightarrow{u'} M \xrightarrow{u} M'' \to 0$$

ainsi définie est exacte et que sa classe $[u', u]$ ne dépend que des classes $[u'_1, u_1]$, $[u'_2, u_2]$. On peut donc poser $[u', u] =: [u'_1, u_1] + [u'_2, u_2]$. Il faut encore vérifier que $+$ munit bien $\mathrm{Ext}^1_A(M'', M')$ d'une structure de groupe abélien (d'élément neutre la classe d'équivalence des suites exactes courtes scindées).

1.5.3.2 Fonctorialité

Donnons-nous maintenant des morphismes de A-modules $f' : M_1' \to M_2'$ et $f'' : M_1'' \to M_2''$. Ces morphismes induisent des morphismes de groupes

$$f^{''*} : \mathrm{Ext}^1_A(M_2'', M') \to \mathrm{Ext}^1_A(M_1'', M'), \quad f'_* : \mathrm{Ext}^1_A(M'', M_1') \to \mathrm{Ext}^1_A(M'', M_2').$$

par pullback et pushout respectivement. On vérifie qu'on définit ainsi deux foncteurs :

$$\begin{array}{lll} \mathrm{Ext}^1_A(M'', -) & Mod_{/A} & \to \quad Mod_{/\mathbb{Z}} \\ & M' & \to \quad \mathrm{Ext}^1_A(M'', M') \\ & f' : M_1' \to M_{2'} & \to \quad f'_* : \mathrm{Ext}^1_A(M'', M_1') \to \mathrm{Ext}^1_A(M'', M_2') \end{array}$$

$$\begin{array}{lll} \mathrm{Ext}^1_A(-, M') & Mod^{op}_{/A} & \to \quad Mod_{/\mathbb{Z}} \\ & M'' & \to \quad \mathrm{Ext}^1_A(M'', M') \\ & f'' : M_1'' \to M_2'' & \to \quad f^{''*} : \mathrm{Ext}^1_A(M_2'', M') \to \mathrm{Ext}^1_A(M_1'', M') \end{array}$$

Si l'on part d'une suite exacte courte

$$(u', u)\ 0 \to M' \xrightarrow{u'} M \xrightarrow{u} M'' \to 0$$

et qu'on lui applique le foncteur $\mathrm{Hom}_A(N, -)$ on peut montrer que la suite

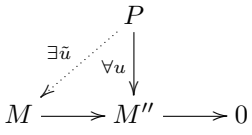
$$0 \to \mathrm{Hom}_A(N, M') \to \mathrm{Hom}_A(N, M) \to \mathrm{Hom}_A(N, M'') \xrightarrow{f \to f^*[u', u]} \mathrm{Ext}^1_A(N, M') \to \mathrm{Ext}^1_A(N, M) \to \mathrm{Ext}^1_A(N, M'')$$

est exacte. Cette suite exacte (qui est en fait le tout début de la suite exacte longue des Ext...) permet parfois de calculer les groupes $\mathrm{Ext}^1_A(M'', M')$ ou d'en démontrer certaines propriétés.

1.5.3.3 A-modules injectifs et projectifs

Il y a certains type de A-modules pour lesquels les Ext^1_A sont toujours nuls. Il s'agit des A-modules projectifs et des A-modules injectifs. Nous en donnons ci-dessous des caractérisations utiles. Ces modules jouent un rôle prépondérant en algèbre homologique (ils servent par exemple à construire les foncteurs dérivés).

Proposition-Définition 1.5.11 *Soit P un A-module. Les propriétés suivantes sont équivalentes*

1. *Le foncteur $\mathrm{Hom}_A(P, -) : Mod_{/A} \to Mod_{/A}$ envoie suites exactes courtes sur suites exactes courtes ;*
2. 

3. *toute suite exacte courte $0 \to M' \to M \to P \to 0$ est scindée ;*
4. *Pour tout A-module M' on a $Ext^1_A(P, M') = 0$*
5. *P est un facteur direct d'un A-module libre.*

Un A-module P qui vérifie les conditions de la Proposition 1.5.11 est dit *projectif*. Tout A-module libre est projectif et la réciproque est vraie pour certains anneaux (on le verra par exemple pour les anneaux principaux) mais pas en général, comme le montre le petit exercice suivant.

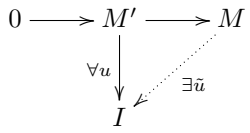
Exercice 1.5.12 *Soit V un espace vectoriel de dimension finie sur un corps k et soit $A := \mathrm{End}_k(V)$. Montrer que le A-module V est projectif mais pas libre.*

On a un énoncé dual :

Proposition-Définition 1.5.13 *Soit I un A-module. Les propriétés suivantes sont équivalentes*

1. *Le foncteur $\mathrm{Hom}_A(-, I) : Mod^{op}_{/A} \to Mod_{/A}$ envoie suites exactes courtes sur suites exactes courtes ;*

2.



3. *toute suite exacte courte* $0 \to I \to M \to M'' \to 0$ *est scindée ;*
4. *Pour tout* A*-module* M'' *on a* $Ext^1_A(M'', I) = 0$
5. I *vérifie la propriété (2) pour les morphismes de* A*-modules injectifs de la forme* $0 \to \mathfrak{i} \xrightarrow{\iota} A$*, où* $\mathfrak{i} \subset A$ *est un idéal et* $\mathfrak{i} \xhookrightarrow{\iota} A$ *l'inclusion canonique.*

Un A-module I qui vérifie les conditions de la Proposition 1.5.13 est dit *injectif*. On notera que la condition (5) est équivalente à

(5') Pour tout $a \in A$ et $x \in I$ il existe $y \in I$ tel que $x = ay$.

Par exemple $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$ sont des $\mathbb{Z}$-modules injectifs.

Preuve des propositions 1.5.11 et 1.5.13. L'équivalence des conditions (1), (2), (3), (4) se prouve de façon similaire dans les deux cas et n'est pas très difficile. Nous laissons cette partie de la preuve en exercice.

Cas projectif : (3) $\Rightarrow$ (5) résulte du fait que tout A-module (donc en particulier P) est quotient d'un A-module libre et de l'exercice 1.2.4. Montrons (5) $\Rightarrow$ (1). Cela résulte du fait que

— le A-module régulier est projectif (pourquoi ?) ;

— si M et N sont deux A-modules, on a par définition

$$\mathrm{Hom}_A(M \oplus N, -) = \mathrm{Hom}_A(M, -) \times \mathrm{Hom}_A(N, -)$$

Le deuxième point montre que $M \oplus N$ vérifie (1) si et seulement si M et N vérifient (1) et le premier point combiné à cette observation, que tout A-module libre vérifie (1).
Cas injectif : (2) $\Rightarrow$ (5) est immédiate. Montrons (5) $\Rightarrow$ (2). Avec les notations de (2), identifions M' et son image dans M de sorte que le morphisme $M' \to M$ soit simplement l'inclusion canonique. Notons $\mathcal{S}$ l'ensemble des couples (N, v), où $N \subset M$ est un sous A-module contenant M' et $v : N \to I$ est un morphisme de A-module tel que $v|_{M'} = u : M' \to I$. On ordonne $\mathcal{S}$ par

$$(N_1, v_1) \leq (N_2, v_2) \Longleftrightarrow N_1 \subset N_2 \text{ et } v_2|_{N_1} = v_1.$$

On vérifie facilement que $(\mathcal{S}, \leq)$ est un ensemble ordonné inductif non-vide (il contient (M', u)) donc possède* un élément (N, v) maximal pour $\leq$. Il reste à voir que $N = M$. Soit $m \in M$; introduisons l'idéal à gauche

$$\mathfrak{i} := \{a \in A \mid am \in N\} \subset A.$$

Par (5), le morphisme de A-module

$$\begin{array}{rccc} V : & \mathfrak{i} & \to & I \\ & a & \to & v(am) \end{array}$$

s'étend en un morphisme de A-module $\tilde{V} : A \to I$. Cela permet de construire un prolongement $\tilde{v} : N + Am \to I$ de $v : N \to I$. En effet, considérons l'e morphisme de A-modules

$$\begin{array}{rccc} \phi : & N \oplus A & \to & M \\ & n + a & \to & v(n) + \tilde{V}(a) \end{array}$$

et observons que pour tout $n + a \in K := \ker(N \oplus A \twoheadrightarrow N + Am)$ on a $am = -n \in N$ donc $a \in \mathfrak{i}$, ce qui implique

$$\phi(n + a) = v(n) + \tilde{V}(a) = v(n) + v(am) = 0.$$

Donc $\phi : N \oplus A \to M$ se factorise *via* $(N \oplus A)/K \simeq N + Am$ en $\tilde{v} : N + Am \to I$. Par maximalité de (N, v), on en déduit que $m \in N$. □

* :utilise le lemme de Zorn.

Exercice 1.5.14 *Soit* A *un anneau principal et* $\mathfrak{i} \subset A$ *un idéal non nul. Montrer que le* $A/\mathfrak{i}$*-module régulier* $A/\mathfrak{i}$ *est injectif.*

1.5.3.4 Exemples de calculs

1. Montrer que pour tout $\mathbb{Z}$-module M et entier $n \geq 1$ on a
$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, M) = M[n] := \ker(\cdot n : M \to M),\ \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, M) = M/n.$$
2. En déduire que
   (a) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = 0$, $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = \mathbb{Z}/n$;
   (b) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m) = \mathbb{Z}/d$, $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m) = \mathbb{Z}/d$, où d est le p.g.c.d. de m et n ;
   (c) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}) = 0$, $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}) = 0$.
3. Montrer que [3] $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}) = A/\mathbb{Q}$, où A est le groupe des adèles *i.e.* des suites $(x_p) \in \prod_p \mathbb{Q}_p$ telles que $x_p \in \mathbb{Z}_p$ pour tous sauf un nombre fini de premiers p et $\mathbb{Q} \subset A$ est l'inclusion diagonale. (Ind. : Considérer la suite exacte courte
$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$
et montrer que $A \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$).

3. Cet exercice demande de connaitre la définition de $\mathbb{Z}_p$ et $\mathbb{Q}_p$.

Chapitre 2

Groupes finis - compléments

L'objectif de ce chapitre est de manipuler un peu les groupes finis, dont nous étudierons les représentations linéaires de dimension finie dans le chapitre 3.

Nous commencerons par revoir rapidement les propriétés élémentaire du groupe symétrique (section 1) puis nous intéresserons à la structure des groupes finis (sections 2 et 3).

2.1 Echauffement : le groupe symétrique

Le groupe symétrique joue un rôle prépondérant dans l'étude des groupes finis, notamment *via* les actions de groupes. En effet, toute action d'un groupe fini G sur un ensemble fini X définit un morphisme de groupe

$$G \to \mathcal{S}(X)$$

à valeur dans le groupe symétrique $\mathcal{S}(X)$ sur X et inversement. Lorsque l'action considérée est fidèle (par exemple lorsqu'on fait opérer G sur lui-même par translation), ce morphisme est même injectif. Les groupes symétriques contiennent donc tous les groupes finis... Ce qui laisse augurer de leur complexité. Si l'on se fixe une bijection $X \xrightarrow{\sim} \{1, \dots, n\}$, on peut identifier $\mathcal{S}(X)$ et

$$\mathcal{S}_n := \mathcal{S}(\{1, \dots, n\}).$$

En dépit de la complexité de $\mathcal{S}_n$ on dispose sur celui-ci d'une description combinatoire particulièrement simple, qui permet d'y faire des calculs explicites. On suppose que le lecteur est familier de ces petites manipulations. Rappelons seulement la formule de conjugaison :

$$\sigma \circ (k_1, \dots, k_r) \circ \sigma^{-1} = (\sigma(k_1), \dots, \sigma(k_r)).$$

Voici quelques propriétés élémentaires de $\mathcal{S}_n$ qu'il faut connaitre (nous en verrons de plus évoluées dans la suite du cours).

1. (Cardinal) : $|\mathcal{S}_n| = n!$.
2. (Classes de conjugaison) : pour tout $\sigma \in \mathcal{S}_n$ il existe une unique famille de cycles $c_1, \dots, c_r \in \mathcal{S}_n$ à supports deux à deux disjoints tels que
$$\sigma = c_1 \circ \cdots \circ c_r.$$
Les supports de ces cycles sont les orbites de l'action tautologique de $\langle \sigma \rangle$ sur $\{1, \dots, n\}$. Notons $\ell_\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ l'application qui à un entier $1 \leq k \leq n$ associe le nombre de cycles de longueur k parmi les $c_1, \dots, c_r$. Deux permutations $\sigma, \tau \in \mathcal{S}_n$ sont conjuguées dans $\mathcal{S}_n$ si et seulement si
$$\ell_\sigma = \ell_\tau.$$
3. (Générateurs) : Les ensembles suivant forment des systèmes de générateurs de $\mathcal{S}_n$
   — Les transpositions $(i, i+1)$, $i = 1, \dots, n-1$;
   — Les transpositions $(1, i)$, $i = 2, \dots, n$;

— La transposition $(1,2)$ et le n-cycle $(1,2,\dots,n)$.

4. (Signature) : il existe un unique morphisme de groupe surjectif

$$\epsilon : \mathcal{S}_n \to \{\pm 1\}$$

appelée la *signature*. Pour tout $\sigma \in \mathcal{S}_n$, on a

$$\epsilon(\sigma) = \prod_{1\le i<j\le n} \frac{(\sigma(j)-\sigma(i))}{(j-i)} = (-1)^{\sum_{1\le k\le n}(k-1)\ell_\sigma(k)} = (-1)^{n-|\{1,\dots,n\}/\langle\sigma\rangle|}.$$

On appelle $\mathcal{A}_n := \ker(\epsilon) \lhd \mathcal{S}_n$ le *groupe alterné*. C'est l'unique sous-groupe d'indice 2 de $\mathcal{S}_n$.

Exercice 2.1.1

1. *Montrer que le centre de $\mathcal{S}_n$ est trivial pour $n \ge 3$.*
2. *Montrer que, si $n \ge 3$, $\mathcal{A}_n$ est engendré par les 3-cycles et que, si $n \ge 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$.*
3. *(a) Soit $c \in \mathcal{S}_n$ un cycle de longueur l. Montrer que pour tout entier $m \ge 1$, la permutation c^m se décompose en produit de $d = pgcd(l,m)$ cycles à support disjoint de longueur $\frac{l}{d}$.*
   (b) Rappelons qu'on peut plonger le groupe symétrique $\mathcal{S}_n$ dans le groupe linéaire $\mathrm{GL}_n(k)$ en associant à $\sigma \in \mathcal{S}_n$ la matrice $P_\sigma \in \mathrm{GL}_n(k)$ définie par $P_\sigma e_i = e_{\sigma(i)}$, $i = 1,\dots,n$ (où $e_1,\dots,e_n$ désigne la base canonique de k^n). Montrer que la k-dimension de $(k^n)^{P_\sigma}$ est le nombre de cycles à supports disjoints de σ.
   (c) Montrer que la matrice $(i \wedge j)_{1\le i,j\le n} \in \mathrm{M}_n(k)$ est inversible. En déduire que $\sigma, \tau \in \mathcal{S}_n$ sont conjuguées dans $\mathcal{S}_n$ si et seulement si P_σ, P_τ sont conjugués dans $\mathrm{GL}_n(k)$.

   Remarque : *Si on suppose k de caractéristique 0, on peut donner une preuve plus simple en utilisant l'égalité des polynomes caractéristiques.*
4. *Montrer qu'on a des isomorphismes $\mathcal{S}_3 \tilde{\to} \mathrm{GL}_2(\mathbb{F}_2)$ et $\mathcal{S}_4 \tilde{\to} \mathrm{PGL}_2(\mathbb{F}_3)$.*

2.2 Théorèmes de Sylow, p-groupes

2.2.1 Théorèmes de Sylow

Soit G un groupe fini et p un nombre premier divisant l'ordre de G. On écrit

$$|G| = mp^r,$$

avec $p \not| m$.
On appelle *p-Sylow* de G tout sous-groupe de G d'ordre p^r et on note $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G.

Exemple 2.2.1 Soit $G = \mathrm{GL}_r(\mathbb{F}_p)$. On a

$$|G| = (p^r-1)(p^r-p)\cdots(p^r-p^{r-1}) = p^{\frac{r(r-1)}{2}} \prod_{i=1}^{r}(p^i-1).$$

Le sous-groupe de $\mathrm{GL}_r(\mathbb{F}_p)$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_r(\mathbb{F}_p)$.

Théorème 2.2.2 (Sylow)

1. *$\mathcal{S}_p(G)$ est non vide ;*
2. *l'action de G par conjugaison sur $\mathcal{S}_p(G)$ est transitive ;*
3. *tout p sous-groupe de G est contenu dans un p-Sylow de G ;*
4. *$|\mathcal{S}_p(G)| \equiv 1 \bmod p$ et $|\mathcal{S}_p(G)||m$.*

Preuve. commençons par le lemme suivant.

Lemme 2.2.3 *Soit G un groupe fini, S un p-Sylow de G et H un sous-groupe de G d'ordre divisible par p. Alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Preuve du lemme 2.2.3. Notons

$$X := H \setminus G/S.$$

Comme

$$G = \bigsqcup_{x\in X} HxS = \bigsqcup_{x\in X} \bigsqcup_{h\in H/xSx^{-1}\cap H} hxS,$$

on a

$$|G| = \sum_{x\in X} |S|[H : xSx^{-1} \cap H]$$

donc

$$[G : S] = \sum_{x\in X} [H : xSx^{-1} \cap H].$$

Par hypothèse p ne divise pas $[G : S]$ donc il existe au moins un $x_0 \in X$ tel que p ne divise pas $[H : x_0Sx_0^{-1} \cap H]$. Mais $x_0Sx_0^{-1} \cap H$ est un p-groupe et, toujours par hypothèse, p divise $|H|$. On en déduit que $x_0Sx_0^{-1} \cap H$ est un p-Sylow de H. □

Montrons (1), (2) et (3). Notons $n = |G| = mp^r$ avec $p \not| m$. En faisant agir G sur lui même par translation, on définit un plongement de G dans le groupe des permutations $\mathcal{S}(G)$ de G. N'importe quelle bijection $G\tilde{\to}\{1, \ldots, n\}$ induit un isomorphisme de groupe $\mathcal{S}(G)\tilde{\to}\mathcal{S}_n$. Enfin, en faisant agir $\mathcal{S}_n$ par permutation sur les vecteurs de la base canonique de $\mathbb{F}_p^n$, on définit un plongement de $\mathcal{S}_n$ dans $\mathrm{GL}_n(\mathbb{F}_p)$. On vient donc de construire un plongement

$$G \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p),$$

ce qui permet de voir G comme un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ et d'appliquer le lemme 2.2.3 avec $G = \mathrm{GL}_n(\mathbb{F}_p)$, $H = G$ et, par exemple, S le sous-groupe des matrices triangulaires supérieures avec des 1 sur la diagonale. Cela donne (1). Pour (2) (resp. (3)), on applique le lemme 2.2.3 avec $G = G$, S et H des p-Sylow de G (resp. S un p-Sylow de G et H un p sous-groupe de G).
Montrons maintenant (4). Comme l'action de G par conjugaison sur $\mathcal{S}_p(G)$ est transitive, pour tout p-Sylow S de G on a :

$$G/S \twoheadrightarrow G/\mathrm{Nor}_G(S)\tilde{\to}\mathcal{S}_p(G),$$

on en déduit que $|\mathcal{S}_p(G)| = [G : \mathrm{Nor}_G(S)]$ divise $[G : S] = m$. Faisons maintenant agir S par conjugaison sur $\mathcal{S}_p(G)$. Pour tout p-Sylow S' de G, la bijection

$$S/\mathrm{Nor}_S(S')\tilde{\to}S \cdot S'$$

montre que les orbites de S agissant sur $\mathcal{S}_p(G)$ sont toutes d'ordre une puissance de p. Comme

$$|\mathcal{S}_p(G)| = \sum_{S'\in\mathcal{S}_p(G)/S} S \cdot S',$$

il suffit donc de montrer qu'il n'y a qu'une seule orbite de longueur 1, celle de S. Sinon, on aurait un p-Sylow $S' \neq S$ tel que $sS's^{-1} = S'$ pour tout $s \in S$. Mais dans ce cas SS' serait un p sous-groupe (observer que les fibre se l'application surjective $S \times S' \twoheadrightarrow SS'$ sont toutes en bijections avec $S \cap S'$) de G contenant strictement S et S' : une contradiction. □

Exercice 2.2.4 *Décrire les sous-groupes de Sylow de $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{A}_4$, $\mathcal{A}_5$.*

Exercice 2.2.5 *Soit G un groupe fini d'ordre 24 tel que $|\mathcal{S}_p(G)| > 1$, $p = 2, 3$. L'objectif de cet exercice est de montrer que G est isomorphe à $\mathcal{S}_4$.*

1. *Calculer $|\mathcal{S}_p(G)|$ et $|\mathrm{Nor}_G(S)|$, $S \in \mathcal{S}_p(G)$ pour $p = 2, 3$.*
2. *En faisant agir G par conjugaison sur ses 3-Sylow, montrer qu'on définit un morphisme*

$$\phi : G \to \mathcal{S}_4$$

   dont le noyau est d'ordre 1 ou 2.
3. *Conclure.*

2.2.2 p-groupes

Nous étudions ici quelques propriétés élémentaires des p-groupes qui, comme on vient de le voir, joue un rôle prépondérant dans l'étude de la structure des groupes finis.

Lemme 2.2.6 (Centre) *Soit G un p-groupe .*

1. *$1 \neq N \lhd G$ un sous-groupe distingué non nul. Alors $Z(G) \cap N \neq 1$. En particulier, $Z(G) \neq 0$;*
2. *Si $Z(G) \subsetneq G$ alors $[G : Z(G)] > p$.*

Preuve. (1) Faisons agir G par conjugaison sur $N \setminus \{1\}$. L'équation aux classes s'écrit :

$$|N \setminus \{1\}| = |N| - 1 = \sum_{n \in N\setminus\{1\}/G} \frac{|G|}{|\mathrm{Stab}_G(n)|}.$$

Comme G est un p-groupe, les termes $\frac{|G|}{|\mathrm{Stab}_G(n)|}$ valent 1 ou une puissance de p. Mais comme $|N|$ est aussi une puissance de p, le terme $|N| - 1$ est premier à p, ce qui montre qu'il existe au moins un $1 \neq n \in N$ tel que $G = \mathrm{Stab}_G(n)$ *i.e.* $n \in Z(G) \cap N$.
Si $[G : Z(G)] = p$ alors $G/Z(G)$ est cyclique. Mais, en général, un groupe fini G pour lequel $G/Z(G)$ est cyclique est abélien. En effet, il suffit d'observer que si $g \in G$ relève un générateur de $G/Z(G)$ alors l'application surjective

$$\begin{array}{lll} Z(G) \times \langle g \rangle & \twoheadrightarrow & G \\ (z, g^r) & \to & zg^r \end{array}$$

définit un morphisme de groupe, ce qui contredit le fait que G n'est pas abélien. □

Lemme 2.2.7 (Sous-groupes maximaux) *Tout sous-groupe maximal d'un p-groupe G est normal dans G et d'indice p dans G .*

Preuve. Pour la première partie de l'assertion, on procède par induction sur $|G|$. Si $|G| = 1, p$, c'est immédiat. Supposons donc $|G| > p$. Soit $M \subset G$ un sous-groupe maximal de G. Alors $MZ(G) \subset G$ est aussi un sous-groupe de G et, par maximalité de M soit $MZ(G) = G$ soit $MZ(G) = M$. Dans le premier cas, on a clairement $M \lhd G$. Dans le second, $M/Z(G)$ est un sous-groupe maximal de $G/Z(G)$. Mais par le lemme 2.2.6, on a $|G/Z(G)| < |G|$ donc, par induction $M/Z(G) \lhd G/Z(G)$, ce qui implique $M \lhd G$.
Pour la seconde partie de l'assertion, comme $M \lhd G$, le quotient G/M est un groupe. De plus, les sous-groupes de G/M sont en correspondance bijective avec les sous-groupe de G contenant M. Autrement dit, les seuls sous-groupes de G/M sont 1 et G/M, ce qui impose $G/M = \mathbb{Z}/p$. □

Corollaire 2.2.8 *Soit G un p-groupe d'ordre $|G| = p^r$. Alors il existe une suite de sous-groupes*

$$G = F_0(G) \supset F_1(G) \supset \cdots \supset F_{r-1}(G) \supset F_r(G) = 0$$

telle que $F_{i+1}(G) \lhd F_i(G)$ et $F_i(G)/F_{i+1}(G) \simeq \mathbb{Z}/p$, $i = 0, \ldots, r-1$.

Autrement dit, on a un 'théorème de Jordan-Holder' pour les p-groupes. On va voir que cela reste vrai pour les groupes finis généraux.

Exercice 2.2.9 (Groupes nilpotents) *Soit G un groupe fini.*

1. *Soit $N \lhd G$ un sous-groupe normal et $P \in \mathcal{S}_p(N)$. Montrer que*

$$G = \mathrm{Nor}_G(P)N.$$

2. *Montrer que les conditions suivantes sont équivalentes :*
   (a) G est le produit direct de ses p-Sylow ;
   (b) tout p-Sylow de G est normal dans G ;
   (c) tout sous-groupe maximal de G est normal dans G.

   Un groupe fini G vérifiant ces propriétés est dit nilpotent.

2.3 Extensions

2.3.1 Atomisation d'un groupe (fini)

Ce que nous avons vu pour les A-module admet un exact analogue pour les groupes. Plus précisément, on dit un groupe G vérifie la *condition DCC* (descending chain condition) (resp. la *condition ACC* - ascending chain condition) si toute suite croissante (resp. décroissante) :

$$G_0 \subset G_1 \subset \cdots \subset G \ \text{ (resp. } \ G \supset G_0 \supset G_1 \supset \cdots \text{)}$$

telle que $G_i \lhd G_{i+1}$, $i \geq 0$ (resp. $G_{i+1} \lhd G_i$, $i \geq 0$) est stationnaire à partir d'un certain rang. Ces conditions correspondent aux notions de module noetherien et artinien.

Un groupe fini vérifie bien sûr à la fois les conditions DCC et ACC.

On dit qu'un groupe est *indécomposable* s'il est non trivial et ne peut s'écrire comme produit direct de deux groupes non triviaux et qu'un groupe est *simple* s'il est non trivial et si ses seuls sous-groupes normaux sont le groupe trivial et lui-même. On a alors

— (Krull-Schmidt) *Soit G un groupe vérifiant les conditions DCC et ACC. Alors il existe une unique (à isomorphisme et permutation près) famille finie de groupes indécomposables $G_1, \ldots, G_r$ tels que*

$$G \simeq G_1 \times \cdots \times G_r.$$

— (Jordan-Holder) *Soit G un groupe vérifiant les conditions DCC et ACC. Alors il existe une filtration finie*

$$F_\bullet(G) \ \ G = F_0(G) \supset F_1(G) \supset \cdots \supset F_n(G) \supset F_{n+1}(G) = 1$$

telle que $F_{i+1}(G) \lhd F_i(G)$, $i = 0, \ldots, n$ et $F_i(G)/F_{i+1}(G)$ est simple, $i = 0, \ldots, n$. En outre, le gradué associé

$$Gr_F(G) := \prod_{0 \leq i \leq n} F_i(G)/F_{i+1}(G)$$

ne dépend pas, à isomorphisme près, de la filtration $F_\bullet(G)$.

Exemple 2.3.1 *Calculer le gradué associé des groupes $\mathcal{S}_4$, $\mathbb{H}_8$ et D_8.*

On est donc confronté pour les groupes finis au même problème (en plus compliqué) que pour les modules : d'un côté, les groupes finis indécomposables sont beaucoup trop gros pour être classifiés et, de l'autre, si l'on sait maintenant classifier les groupes finis simples (voir section 2.3.2), leurs extensions sont encore très mal comprises.

2.3.2 Groupes finis simples

Comme les modules simples, les groupes finis simples ont des propriétés élémentaires remarquables. Par exemple,

— si $\phi : G \to G'$ est un morphisme de groupes finis et si G est simple alors ϕ est soit le morphisme trivial soit injectif ;

— si G est simple et $1 \neq X \subset G$ est un sous-ensemble stable par conjugaison alors $G = \langle X \rangle$.

Exercice 2.3.2 *Soit G un groupe fini d'ordre pair. Montrer que si les 2-Sylow de G sont cycliques et $|G| > 2$ alors G n'est pas simple. En déduire qu'un groupe simple d'ordre pair est d'ordre divisible par 4.*

La classification des groupes finis simples (ou 'théorème énorme'), achevée vers le milieu des années 80, est considéré comme le résultat le plus impressionnant des mathématiques du vingtième siècle.

Théorème 2.3.3 *Tout groupe fini simple est de l'un des type suivant*

1. *Un groupe cyclique d'ordre premier ;*
2. *Un groupe alterné $\mathcal{A}_n$, $n \geq 5$;*

3. *Un groupe de type Lie classiques (pour presque toutes les valeurs de n et $q = p^r$) :* $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$, $\mathrm{P}\Omega^\epsilon_n(\mathbb{F}_q)$, $\mathrm{PSU}_n(\mathbb{F}_{q^2})$ *;*
4. *Un groupes de Lie exceptionnel (pour presque toutes les valeurs de n et $q = p^r$) :* $E_6(\mathbb{F}_q)$, $E_7(\mathbb{F}_q)$, $E_8(\mathbb{F}_q)$, $F_4(\mathbb{F}_q)$, $G_2(\mathbb{F}_q)$ *et certaines de leurs formes tordues ;*
5. *L'un des* 27 *groupes sporadiques.*

Montrons un tout petit bout de ce résultat.

Proposition 2.3.4 *Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$.*

preuve. Soit $1 \subsetneq N \lhd \mathcal{A}_n$. Comme $\mathcal{A}_n$ est engendré par les 3-cycles (exercice 2.1.1 (2)), il suffit de montrer que N contient les 3-cycles. Comme N est normal dans $\mathcal{A}_n$ et que les 3-cycles sont conjugués dans $\mathcal{A}_n$ (exercice 2.1.1 (2)), il suffit de montrer que N contient un 3-cycle. Pour cela, fixons $1 \neq \sigma \in N$ admettant un nombre maximal de points fixes et montrons que σ est un 3-cycle.
Supposons d'abord que toutes les orbites de $\langle\sigma\rangle$ opérant sur $\{1, \ldots, n\}$ sont de longueur 2. Comme $\sigma \in \mathcal{A}_n$, il y au moins deux telles orbites, disons $\{i, j\}$ et $\{k, l\}$. Comme $n \geq 5$, on peut choisir $r \in \{1, \ldots, n\} \setminus \{i, j, k, l\}$ et introduire le 3-cycle $\tau := (k, l, r) \in \mathcal{A}_n$. Comme N est normal dans $\mathcal{A}_n$, on a encore $[\tau, \sigma] \in N$. Mais $[\tau, \sigma]$ laisse invariant tous les points fixes de σ distincts de i, j, k, l, r. Il laisse également invariant i et j. Et il est non trivial : $[\tau, \sigma](k) = r$. Il a donc au moins un point fixe de plus que σ, ce qui contredit la définition de σ.
$\langle\sigma\rangle$ a donc au moins une orbite de longueur ≥ 3 contenant disons i, j, k avec $\sigma(i) = j$, $\sigma(j) = k$. Si σ n'est pas un 3-cycle, le support de σ possède deux autres éléments, disons l, r tels que $\sigma(l) = r$. Introduisons à nouveau le 3-cycle $\tau := (k, l, r)$. Comme ci-dessus $[\tau, \sigma] \in N$ et $[\tau, \sigma]$ laisse invariant j et tous les points fixes de σ distincts de k, l, r. Mais comme aucun des points i, j, k, l, r n'est fixés par σ, $[\tau, \sigma]$ a au moins un point fixe de plus que σ, ce qui contredit la définition de σ. □

Exercice 2.3.5 (Groupe fini simple d'ordre 60) *L'objectif de cet exercice est de montrer que tout groupe fini simple G d'ordre* 60 *est isomorphe à $\mathcal{A}_5$.*

1. *Montrer que G n'a pas de sous-groupe d'indice < 5 ;*
2. *Montrer que G contient un sous-groupe d'indice* 5 *(Ind : on pourra raisonner par l'absurde et montrer que si ce n'était pas le cas, G contiendrait* 15 2*-Sylow d'intersection deux à deux triviale).*
3. *En déduire que G se plonge dans $\mathcal{S}_5$ puis qu'il est isomorphe à $\mathcal{A}_5$.*

2.3.3 Extensions, produits semidirects

Nous allons maintenant nous intéresser un peu au problème de la classification des extensions d'un groupe G'' par un groupe G'. Comme nous l'avons déjà mentionné, c'est un problème difficile (encore beaucoup plus difficile que pour les modules) qu'on est loin de savoir résoudre complétement à l'heure actuelle. Tout d'abord, si on a une suite exacte courte de groupes finis

$$1 \to G' \stackrel{u'}{\to} G \stackrel{u}{\to} G'' \to 1$$

et que celle-ci se scinde (*i.e.* s'il existe un morphisme de groupe $s : G'' \to G$ tel que $u \circ s = Id_{G''}$), il n'est plus vrai que $G \simeq G' \times G''$. Cela conduit à la notion de produit semi-direct.

2.3.3.1 Produits semi-directs

2.3.3.1.1 Definition 'interne'

Lemme 2.3.6 *Soit $1 \to G' \stackrel{u'}{\to} G \stackrel{u}{\to} G'' \to 1$ une suite exacte courte de groupes. Les propriétés suivantes sont équivalentes :*

1. *il existe un sous-groupe $\tilde{G}'' \subset G$ tel que $G = G'\tilde{G}''$ et $G' \cap \tilde{G}'' = 1$;*
2. *il existe un morphisme de groupe $s : G'' \to G$ tel que $u \circ s = Id_{G''}$.*

On dit alors que G est produit semi-direct de G' par G'' et on note

$$G \simeq G' \rtimes G''.$$

Exemple 2.3.7

1. *Montrer que $\mathcal{S}_4$ se dévisse en produits semi-directs de groupes cycliques.*
2. *Montrer que $\mathbb{H}_8$ ne peut pas s'écrire comme produit semi-direct de deux groupes non triviaux.*

2.3.3.1.2 Definition 'externe' Si une extension de groupes finis $1 \to G' \overset{u'}{\to} G \overset{u}{\to} G'' \to 1$ se scinde, le choix d'une section $s : G'' \to G$ définit un morphisme de groupes

$$\begin{array}{rccc} \phi : & G'' & \to & \mathrm{Aut}_{Grp}(G') \\ & g'' & \to & g' \to s(g'')g's(g'')^{-1} \end{array}$$

Inversement, tout morphisme de groupe $\phi : G'' \to \mathrm{Aut}_{Grp}(G')$ définit une extension scindée de G'' par G'. Explicitement, on munit l'ensemble

$$G' \times G''$$

du produit tordu par ϕ :

$$(g', g'') \cdot_\phi (h', h'') = (g'\phi(g'')(h'), g''h'').$$

On vérifie que cela définit bien une loi de groupe sur $G' \times G''$; on note le groupe ainsi obtenu $G' \rtimes_\phi G''$ et on dit que c'est le produit semi-direct de G'' par G' relativement à ϕ. L'injection canonique $u' : G' \hookrightarrow G' \rtimes_\phi G''$, $g' \to (g', 1)$ et la surjection canonique $u : G' \rtimes_\phi G'' \twoheadrightarrow G''$, $(g', g'') \to g''$ sont des morphismes de groupes et on a une suite exacte courte de groupes

$$1 \to G' \overset{u'}{\to} G' \rtimes_\phi G'' \overset{u}{\to} G'' \to 1$$

scindée par l'injection canonique $s : G'' \to G' \rtimes_\phi G''$, $g'' \to (1, g'')$.

On prendra garde que deux morphismes $\phi_1, \phi_2 : G'' \to \mathrm{Aut}_{Grp}(G')$ peuvent induire des produits semi-directs non-isomorphes.

2.3.3.1.3 Produit semi-direct versus produit direct On vérifie aisément qu'un produit semi-direct est direct si et seulemet si

— (Définition interne) : on a les propriétés équivalentes suivantes :
  1. $\tilde{G}'' \lhd G$;
  2. il existe un morphisme de groupe $s : G \to G'$ tel que $s \circ u' = Id_{G'}$.

— (Définition externe) : $\phi : G'' \to \mathrm{Aut}_{Grp}(G')$ est le morphisme trivial.

Exercice 2.3.8 (Groupes d'ordre pq) *Soit p, q deux nombres premiers. Déterminer tous les groupes d'ordre pq à isomorphisme près.*

Exercice 2.3.9 *Montrer qu'un groupe d'ordre* 255 *est toujours cyclique.*

2.3.3.2 Extensions abéliennes, classification par le $\mathbf{H}^2$, théorème de Schur-Zassenhauss

Il y a cependant un cas où l'on dispose d'une méthode systématique pour classifier les extensions comme pour les modules : c'est lorsque G' est abélien. Sous cet angle, les groupes finis dont le gradué associé est abélien sont les plus faciles à appréhender.

2.3.3.2.1 Groupes résolubles et nilpotents Soit G un groupe et $H, K \subset G$ deux sous-groupes. On note $[H, K] \subset G$ le sous-groupe engendré par les éléments de la forme

$$[h, k] = hkh^{-1}k^{-1},\ h \in H, k \in K.$$

En particulier, si $H = K = G$, on note $D(G) := [G, G]$ le *sous-groupe dérivé* de G. C'est un sous-groupe caractéristique dont le quotient $p_{D(G)} : G \twoheadrightarrow G/D(G) =: G^{ab}$ est abélien, caractérisé par la propriété universelle suivante.

Lemme 2.3.10 *Pour tout morphisme de groupe $\phi : G \to A$ avec A abélien, $D(G) \subset \ker(\phi)$ donc il existe un unique morphisme de groupe $\overline{\phi} : G^{ab} \to A$ tel que $\overline{\phi} \circ p_{D(G)} = \phi$.*

Autrement dit, $p_{D(G)} : G \twoheadrightarrow G^{ab}$ représente le foncteur $\mathrm{Hom}_{Grp}(G, -) : \mathrm{Mod}_{/\mathbb{Z}} \to \mathrm{Mod}_{/\mathbb{Z}}$.

Exemple 2.3.11 Quels sont le sous-groupe dérivé et l'abélianisé de $\mathcal{A}_n$, $\mathcal{S}_n$, D_{2n}, $\mathbb{H}_8$?

On peut construire deux filtrations canoniques en utilisant l'opération $[-,-]$:

— La *série dérivée* : $D^0(G) = G$, $D^{n+1}(G) = D(D^n(G))$, $n \geq 0$;

— La *série centrale* : $C^0(G) = G$, $C^{n+1}(G) = [G, C^n(G)]$, $n \geq 0$.

Lemme 2.3.12 *Soit G un groupe. Les propriétés suivantes sont équivalentes.*

1. *$D^n(G) = 1$ pour $n \gg 0$;*
2. *Il existe une suite de sous-groupes normaux de G*
$$G = F_0(G) \supset F_1(G) \supset \cdots \supset F_n(G) \supset F_{n+1}(G) = 0$$
telle que $F_i(G)/F_{i+1}(G)$ soit abélien, $i = 0, \ldots, n$;
3. *Il existe une suite de sous-groupes de G*
$$G = F_0(G) \supset F_1(G) \supset \cdots \supset F_n(G) \supset F_{n+1}(G) = 0$$
telle que $F_{i+1}(G) \lhd F_i(G)$ et $F_i(G)/F_{i+1}(G)$ soit abélien, $i = 0, \ldots, n$;
4. *Si G est fini, le gradué associé à G est abélien.*

On dit qu'un groupe vérifiant les propriétés équivalentes du lemme 2.3.12 est *résoluble*.

Exemple 2.3.13

1. Soit $1 \to G' \to G \to G'' \to 1$ une suite exacte courte de groupes finis. Alors G est résoluble si et seulement si G' et G'' sont résolubles.
2. $\mathcal{S}_n$ est résoluble si et seulement si $n \leq 4$.
3. On verra dans la troisième partie du cour que tout groupe d'ordre $p^a q^b$ est résoluble (théorème de Burnside). Plus généralement, le (difficile !) théorème de Feit-Thomson dit que tout groupe fini d'ordre impair est résoluble.

Lemme 2.3.14 *Soit G un groupe. Les propriétés suivantes sont équivalentes.*

1. *$C^n(G) = 1$ pour $n \gg 0$;*
2. *il existe une suite de sous-groupes de G*
$$G = F_0(G) \supset F_1(G) \supset \cdots \supset F_n(G) \supset F_{n+1}(G) = 0$$
telle que $[G, F_i(G)] \subset F_{i+1}(G)$, $i = 0, \ldots, n$;
3. *il existe une suite de sous-groupes de G*
$$G = F_0(G) \supset F_1(G) \supset \cdots \supset F_n(G) \supset F_{n+1}(G) = 0$$
telle que $F_{i+1}(G) \lhd F_i(G)$ et $F_i(G)/F_{i+1}(G) \subset Z(G/F_{i+1}(G))$, $i = 0, \ldots, n$;
4. *Si G est fini, les propriétés ci-dessus sont également équivalentes à (cf. Exercice 2.2.9) :*
   (a) *Pour tout sous-groupe strict $H \subsetneq G$ on a $H \subsetneq \mathrm{Nor}_G(H)$;*
   (b) *G est le produit direct de ses p-Sylow ;*
   (c) *tout p-Sylow de G est normal dans G ;*
   (d) *tout sous-groupe maximal de G est normal dans G.*

On dit qu'un groupe vérifiant les propriétés équivalentes du lemme 2.3.14 est *nilpotent*.

Exemple 2.3.15

1. Soit $1 \to G' \to G \to G'' \to 1$ une suite exacte courte de groupes finis. Alors si G est nilpotent, G' et G'' sont nilpotents. Si G' est contenu dans le centre de G et G'' est nilpotent alors G est nilpotent. Par contre, il n'est pas vrai en général qu'une extension de groupes nilpotents est nilpotent. Contre-exemple ?
2. Tout p-groupe est nilpotent.

Exercice 2.3.16 (Sous-groupe de Frattini) *Soit G un groupe fini. On note $\Phi(G)$ l'intersection des sous-groupes maximaux de G. C'est un sous-groupe caractéristique de G, appelé sous-groupe de Frattini de G.*

1. *Soit $H \subset G$ un sous-groupe. Montrer que $H = G$ si et seulement si $H\Phi(G) = G$;*
2. *Montrer que $\Phi(G)$ est nilpotent ;*
3. *Soit G un p-groupe. Montrer que $\Phi(G)$ est le sous-groupe de G engendré par $D(G)$ et les puissances p-ièmes.*

2.3.3.2.2 Groupes de cohomologie de G à valeur dans un $\mathbb{Z}[G]$-module Nous allons maintenant associer à un groupe G et un $\mathbb{Z}[G]$-module A une suite de groupes

$$\mathrm{H}^n(G, A)$$

qui sont des invariants abéliens contenant énormément d'information sur le groupe G. On verra en particulier que pour $n = 2$ ces groupes classifient les extensions de G par A.

Commençons par la construction. On note $C^n(G, A)$ l'ensemble des applications $G^n \to A$. Ce sont des groupes abéliens et on peut considérer leur somme directe :

$$C^\bullet(G, A) := \bigoplus_{n\geq 0} C^n(G, A).$$

On peut munir $C^\bullet(G, A)$ d'une différentielle $d^\bullet : C^\bullet(G, A) \to C^{\bullet+1}(G, A)$ en posant

$$df(x_1, \ldots, x_{n+1}) = x_1 f(x_2, \ldots, x_{n+1}) + \sum_{1\leq i\leq n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n)$$

Exemple 2.3.17

— Si $a \in A = C^0(G, A)$ on a $da(x) = xa - a$ donc $da = 0$ si et seulement si $a \in A^G$.
— Si $f \in C^1(G, A)$ on a $df(x, y) = xf(y) - f(xy) + f(x)$.
— Si $f \in C^2(G, A)$ on a $df(x, y, z) = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y)$.

Lemme 2.3.18 *$d^\bullet : C^\bullet(G, A) \to C^{\bullet+1}(G, A)$ est un morphisme de groupes qui translate le degré de 1 et vérifie $d \circ d = 0$.*

En particulier $B^n(G, A) := \mathrm{im}(d^{n-1}) \subset \ker(d^n) =: Z^n(G, A)$, $n \geq 0$. Les éléments de $B^n(G, A)$ et $Z^n(G, A)$ sont appelés respectivement *n-cobords* et *n-cocycles*. Ce sont des groupes abéliens et on peut introduire leur quotient

$$\mathrm{H}^n(G, A) := Z^n(G, A)/B^n(G, A),$$

appelé *n-ième groupe de cohomologie de G à valeurs dans A.*

Exemple 2.3.19

— $\mathrm{H}^0(G, A) = A^G$.
— Supposons que G agisse trivialement sur A. Alors $B^1(G, A) = 0$ et $\mathrm{H}^1(G, A) = \mathrm{Hom}_{Grp}(G, A)$.

2.3.3.2.3 $H^1(G, A)$, $H^2(G, A)$ Considérons une suite exacte courte de groupes

$$1 \to A \to E \xrightarrow{p} G \to 1.$$

Puisque A est abélien pour tout $e, e' \in E$ tels que $p(e) = p(e')$ on a $eae^{-1} = e'ae'^{-1}$, $a \in A$. Cela montre que si $s : G \to E$ est une section ensembliste *i.e.* une application telle que $p \circ s = Id_G$, on a une action de groupe

$$\begin{array}{ccc} G \times A & \to & A \\ (g, a) & \to & g \cdot a = s(g)as(g)^{-1}, \end{array}$$

bien définie et indépendante de la section ensembliste $s : G \to E$. Le groupe $\mathrm{H}^2(G, A)$ classifie les classes d'isomorphismes d'extensions $1 \to A \to E \xrightarrow{p} G \to 1$ dont l'action associée $G \times A \to A$ induit la structure de $\mathbb{Z}[G]$-module donnée sur A. Nous n'allons pas vérifier tous les détails (cela ne présente aucune diffficulté mais est un peu fastidieux) mais expliquer 'comment ça marche'.

Partons d'une extension (ϵ) $1 \to A \to E \xrightarrow{p} G \to 1$ et fixons une section ensembliste $s : G \to E$. Cela définit une application

$$\begin{array}{rccc} c_s : & G \times G & \to & A \\ & (x, y) & \to & s(x)s(y)s(xy)^{-1}, \end{array}$$

qui mesure le 'défaut de compatibilité de $s : G \to E$ aux structures de groupe sur G et E'. On vérifie que $dc_s = 0$ *i.e.* $c_s \in Z^2(G, A)$. Par ailleurs, la donnée d'une autre section ensembliste $t : G \to E$ définit une application

$$\begin{array}{rccc} a_{s,t} : & G & \to & A \\ & x & \to & t(x)s(x)^{-1}. \end{array}$$

et on vérifie que $c_t(x, y) = a_{s,t}(x)x \cdot a_{s,t}(y)a_{s,t}(x, y)^{-1}c_s(x, y) = da_{s,t}(x, y)c_s(x, y)$, $x, y \in G$. Autrement dit les classes $[c_s]$ et $[c_t]$ de $c_s, c_t \in Z^2(G, A)$ coincident dans $\mathrm{H}^2(G, A)$; notons donc cette classe $[\epsilon]$. Soit $\mathcal{E}(A, G)^0$ l'ensemble des extensions de G par A et $\mathcal{E}(A, G) := \mathcal{E}(A, G)^0/\simeq$ l'ensemble des classes d'isomorphismes d'extensions de G par A. On dit que deux extensions

$$(\epsilon)\ \ 1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

$$(\epsilon')\ \ 1 \to A \xrightarrow{i'} E \xrightarrow{p'} G \to 1$$

sont isomorphes ($(\epsilon) \simeq (\epsilon')$) s'il existe un morphisme de groupes $\phi : E \to E'$ faisant commuter le diagramme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

$\phi : E \to E'$ est alors automatiquement un isomorphisme. On vient de construire une application

$$[-] : \mathcal{E}(A, G)^0 \to \mathrm{H}^2(G, A)$$

et là encore on peut vérifier que deux extensions isomorphes induisent la même classe de cohomologie donc que cette application se factorise en une application

$$[-] : \mathcal{E}(A, G) \to \mathrm{H}^2(G, A).$$

Proposition 2.3.20 *L'application*

$$[-] : \mathcal{E}(A, G) \to \mathrm{H}^2(G, A)$$

est bijective et envoie la classe du produit semi-direct $A \rtimes G$ (associé à $\phi : G \to \mathrm{Aut}_{Grp}(A)$, $g \to s(g) - s(g)^{-1}$) sur 0.

La preuve consiste à construire l'application inverse. Pour cela, on part de $c \in Z^2(G, A)$ et on lui associe l'ensemble $E = A \times G$ que l'on munit de la loi de composition interne

$$(a, g) *_c (a', g') = (a(g \cdot a')c(g, g'), gg'),\ a, a' \in A,\ g, g' \in G.$$

On vérifie $E_c = (E, *_f)$ est un groupe, que si l'on remplace c par un cocycle équivalent, l'extension résultante est isomorphe à E_c et que l'application $\mathrm{H}^2(G, A) \to \mathcal{E}(A, G)$ ainsi construite est bien inverse de $[-] : \mathcal{E}(A, G) \to \mathrm{H}^2(G, A)$.

Soit enfin $(\epsilon)\ \ 1 \to A \to E \xrightarrow{p} G \to 1$ une extension scindée et notons $S(\epsilon)$ l'ensemble des classes de conjugaison des sections de (ϵ). On va voir que le groupe $\mathrm{H}^1(G, A)$ est en bijection avec $S(\epsilon)$. En effet, si $s, t : G \to E$ sont deux morphismes de groupes tels que $p \circ s = p \circ t = Id_G$ alors l'application

$$\begin{array}{rccc} a_{s,t} : & G & \to & A \\ & x & \to & t(x)s(x)^{-1}. \end{array}$$

vérifie $da_{s,t} = 0$ et pour tout $a \in A = C^0(G, A)$ on a $a_{s,at(-)a^{-1}} = da + a_{s,t}$. Autrement dit, l'application qui à t associe la classe $[a_{s,t}]$ définit une application $\mathcal{S}(\epsilon) \to \mathrm{H}^1(G, A)$.

Proposition 2.3.21 *L'application*

$$[-] : S(\epsilon) \to \mathrm{H}^1(G, A)$$

est bijective et envoie la classe de conjugaison de s sur 0.

Là encore, la preuve consiste à construire l'application inverse. Pour tout $a \in Z^1(G, A)$, l'application

$$\begin{array}{rccc} t_a : & G & \to & A \\ & x & \to & a(x)s(x). \end{array}$$

est une section de (ϵ) d'où une application bien dfinie $t_- : Z^1(G, A) \to S(\epsilon)$. On a de plus $t_{adb} = bt_ab^{-1}$, $b \in A$, $a \in Z^1(G, A)$ donc $t_- : Z^1(G, A) \to S(\epsilon)$ se factorise en une application $t_- : H^1(G, A) \to S(\epsilon)$ qui, par construction, est inverse de $[-] : S(\epsilon) \to \mathrm{H}^1(G, A)$.

2.3.3.2.4 Théorème de Schur-Zassenhauss

Lemme 2.3.22 *Soit G un groupe fini d'ordre $|G| =: N$ et A un $\mathbb{Z}[G]$-module. Alors $N\mathrm{H}^n(G,A) = 0$, $n \geq 1$.*

Preuve. Soit $f \in Z^n(G,A)$. Posons

$$\begin{array}{rccc} F: & G^{n-1} & \to & A \\ & (x_1,\ldots,x_{n-1}) & \to & \sum_{g\in G} f(x_1,\ldots,x_{n-1},g). \end{array}$$

Par hypothèse on a

$$0 = df(x_1,\ldots,x_{n+1}) = x_1 f(x_2,\ldots,x_{n+1}) + \sum_{1\leq i\leq n} (-1)^i f(x_1,\ldots,x_{i-1},x_ix_{i+1},\ldots,x_{n+1}) + (-1)^{n+1} f(x_1,\ldots,x_n).$$

En sommant sur $x_{n+1} \in G$, on en déduit

$$0 = x_1 F(x_2,\ldots,x_n) + \sum_{1\leq i\leq n-1} (-1)^i F(x_1,\ldots,x_{i-1},x_ix_{i+1},\ldots,x_n) + (-1)^n F(x_1,\ldots,x_{n-1}) + (-1)^{n+1} Nf(x_1,\ldots,x_n),$$

d'où $Nf = d((-1)^n F)$. □

Corollaire 2.3.23 *Si $N : A \tilde{\to} A$ est un automorphisme alors $\mathrm{H}^n(G,A) = 0$, $n \geq 1$.*

Preuve. Il suffit d'observer que $N : A \tilde{\to} A$ induit un automorphisme $N : C^n(G,A) \tilde{\to} C^n(G,A)$ qui commute à la différentielle d donc induit encore par passage au quotient un automorphisme $N : \mathrm{H}^n(G,A) \tilde{\to} \mathrm{H}^n(G,A)$. □

En particulier, si A est fini et d'ordre premier à $|G|$, on déduit de $\mathrm{H}^2(G,A) = \mathrm{H}^1(G,A) = 0$ que

- Toute extension de G par A est scindée ;
- Si $(\epsilon)\ \ 1 \to A \to E \xrightarrow{p} G \to 1$ est une extension de G par A, deux sections sont toujours conjuguées par un élément de A.

Le théorème de Schur-Zassenhauss étend ce résultat aux extensions de G par des groupes finis qui ne sont plus nécessairement abéliens.

Théorème 2.3.24 (Schur-Zassenhauss) *Soit A, G deux groupes finis d'ordres premiers entre eux. Alors*

- *Toute extension de G par A est scindée ;*
- *Si A ou G est résoluble et si $(\epsilon)\ \ 1 \to A \to E \xrightarrow{p} G \to 1$ est une extension de G par A, deux sections sont toujours conjuguées par un élément de A.*

Remarque 2.3.25 D'après le théorème de Feit-Thompson, on peut supprimer l'hypothèse 'Si A ou G est résoluble' dans l'énoncé du théorème de Schur-Zassenhauss.

Preuve (d'après [Se79, §4.4]). On raisonne par récurrence sur l'ordre $|E|$ de l'extension

$$(\epsilon)\ \ 1 \to A \to E \xrightarrow{p} G \to 1$$

et se ramener au cas où A est abélien.

Nous utiliserons à plusieurs reprises l'observation suivante sur les groupes résolubles (c'est d'ailleurs la seule propriété des groupes résolubles que l'on utilise) : tout groupe résoluble fini non trivial contient un p-groupe abélien élémentaire non trivial caractéristique. (Considérer le dernier terme non trivial $D^n(G)$ de la série dérivée de G ; c'est un sous-groupe abélien caractéristique de G. Si p est un nombre premier divisant $|D^n(G)|$, on peut prendre le sous-groupe de $D^n(G)$ engendré par les éléments d'ordre p).

On va distinguer trois cas. L'ordre dans lequel on les prouve est important.

1. *A est résoluble.* D'après l'observation ci-dessus, A contient un p-groupe abélien élémentaire non trivial caractéristique disons A_1. Si $A = A_1$, on est dans la situation du corollaire 2.3.23. Sinon, comme A_1 est normal dans E on peut quotienter (ϵ) pour obtenir :

$$1 \to A/A_1 \to E/A_1 \to G \to 1.$$

Comme $|E/A_1| < |E|$, l'hypothèse de récurrence nous donne une section $s_1 : G \to E/A_1$. Notons $G_1 := s_1(G) \subset E/A_1$ et $E_1 \subset E$ l'image inverse de G_1 par $E \twoheadrightarrow E/A_1$. On a une suite exacte courte

$$1 \to A_1 \to E_1 \to G_1 \to 1.$$

Comme A_1 est abélien, le corollaire 2.3.23 nous donne une section $s_2 : G_1 \to E_1$. On en déduit une section $s := s_2 \circ (s_1|^{G_1})^{-1} : G \to E_1 \subset E$.
Montrons maintenant que deux sections $s, t : G \to E$ sont conjuguées par un élément de A. Notons $p_{A_1} : E \to E/A_1$ la projection canonique. L'hypothèse de récurrence appliquée à $1 \to A/A_1 \to E/A_1 \to G \to 1$ montre qu'il existe $a \in A$ tel que pour tout $g \in G$

$$s(g)(at(g)a^{-1})^{-1} \in A_1.$$

Donc quitte à remplacer t par $at(-)a^{-1}$, on peut supposer que $t(G) \subset t(G)A_1 = s(G)A_1 = E_1$ et on conclut par le corollaire 2.3.23 appliqué à

$$1 \to A_1 \to E_1 \to G \to 1.$$

2. *Première partie de l'assertion (sans hypothèse de résolubilité).* Soit p un nombre premier divisant $|A|$ et S un p-Sylow de A. On a $E = ANor_E(S)$ (cela résulte du fait que E agit transitivement sur $\mathcal{S}_p(A)$ donc que $E/Nor_E(S) \simeq A/Nor_A(S) \twoheadleftarrow A$). Posons $E' := Nor_E(S)$ et $A' = E' \cap A$. A' est un sous-groupe normal de E'. On dispose donc d'une suit exacte courte

$$1 \to A' \to E' \to G \to 1.$$

Si $|E'| < |E|$, l'hypothèse de récurrence donne une section $s : G \to E' \subset E$. Sinon, S est normal dans E et on peut considérer la suite exacte courte

$$1 \to A/S \to E/S \to G \to 1.$$

Comme $|E/S| < |E|$, l'hypothèse de récurrence donne une section $s_1 : G \to E/S$. Notons $G_1 := s_1(G) \subset E/S'$ et $E_1 \subset E$ l'image inverse de G_1 par $E \twoheadrightarrow E/S$. On a une suite exacte courte

$$1 \to S \to E_1 \to G_1 \to 1.$$

Comme S est résoluble, le cas (1) nous donne une section $s_2 : G_1 \to E_1$. On en déduit une section $s := s_2 \circ (s_1|^{G_1})^{-1} : G \to E_1 \subset E$.

3. *Deuxième partie de l'assertion lorsque G est résoluble.* Soit $s, t : G \to E$ deux sections et I un p-sous-groupe élémentaire caractéristique de G. Comme $s(G) \cap p^{-1}(I) = s(I)$ et $t(G) \cap p^{-1}(I) = t(I)$ sont des p-Sylow de $p^{-1}(I)$, il existe $x \in p^{-1}(I)$ tel que $s(I) = xt(I)x^{-1}$. En écrivant $x = s(i)a$ avec $i \in I$, on obtient $s(I) = at(I)a^{-1}$ (car I est abélien). Donc quitte à remplacer t par $at(-)a^{-1}$, on peut supposer que $s(I) = t(I) =: J$. Introduisons $N := \mathrm{Nor}_E(J)$. Puisque I est normal dans G, on a $s(G), t(G) \subset N$. Si $|N| < |E|$, on peut appliquer l'hypothèse de récurrence à

$$1 \to A \cap N \to N \to G \to 1.$$

Sinon, J est normal dans E donc l'hypothèse de récurrence appliquée à

$$1 \to A/J \cap A \to E/J \to G/I \to 1$$

montre qu'il existe $a \in A$ tel que pour tout $g \in G$

$$t(g)as(g)a^{-1} \in J \cap A = \{1\}. \ \square$$

Exercice 2.3.26 *Soit G un groupe fini et π un ensemble de nombres premiers divisant $|G|$. On dit qu'un sous-groupe $H \subset G$ est un sous-groupe de Hall si $gcd([G : H], |H|) = 1$ et que $H \subset G$ est un π-sous-groupe si les seuls premiers qui divisent $|H|$ sont dans π. On suppose G résoluble. Montrer par récurrence sur $|G|$ que*

1. *G contient toujours des π-sous-groupes de Hall.*
2. *Deux π-sous-groupes maximaux sont toujours conjugués dans G (et donc que ce sont des sous-groupes de Hall).*

Chapitre 3

Représentations linéaires des groupes finis

Soit G un groupe fini et K un corps algébriquement clos de caractéristique 0 ou première à l'ordre de G. Dans ce chapitre, nous allons nous intresser à la classification des $K[G]$-modules de K-dimension finie (ou K-représentations linéaires de G de K-dimension finie). Sous nos hypothèses sur K et G, $K[G]$ est une K-algèbre semi-simple. Or pour les anneaux semi-simples et leurs modules, on dispose de résultats de classification très précis (Section 3.1). En combinant ces résultats de classification aux propriétés de $K[G]$, on peut encore affiner la description de $K[G]$ et de ses modules (Section 3.2). On montre par exemple que le nombre de $K[G]$-modules simples est le nombre de classes de conjugaison de G, que l'ordre de G est la somme des carrés des K-dimensions des $K[G]$-modules simples *etc.* Comme tout $K[G]$-module est semisimple, classifier les $K[G]$-modules revient à classifier les $K[G]$-modules simples. A leur tour, ceux-ci sont uniquement déterminés par leur caractère. Comme on connait le nombre de caractères irréductibles, le problème auquel on est finalement confronté est celui de la détermination de *tous* les caractères irréductibles de G. Nous passerons d'abord en revue un certain nombre de techniques élémentaires permettant de déterminer ces caractères (représentations de l'abélianisé, torsion par les caractères de dimension 1, relations d'orthogonalité *etc.*). Celles-ci ne suffisent en général pas à construire toute la 'table des caractères' de groupes un peu compliqués. Pour aller plus loin, on a besoin de la notion de représentation induite (Section 3.3), qui donne accès à des techniques plus puissantes, permettant de construire des représentations irréductibles de G à partir des représentations irréductibles de ses sous-groupes. On verra aussi au passage une application de la théorie des caractères à la théorie des groupes (le théorème de Burnside, qui dit que tout groupe d'ordre $p^a q^b$ avec p, q premiers est résoluble).

3.1 Anneaux semisimples

Soit A un anneau associatif unitaire.

3.1.1 Anneaux semisimples

On rappelle que le A-module régulier est le groupe abélien A muni de la structure de A-module induite par la multiplication à gauche

$$\begin{array}{rccc} L: & A & \to & \mathrm{End}_{\mathbb{Z}}(A) \\ & a & \to & b \to ab \end{array}$$

et que les conditions suivantes sont équivalentes (Exercice 3.1.7.2).

1. Tout A-module est semisimple ;
2. Le A-module régulier (A, L) est semisimple.

On dit alors qu'un anneau A vérifiant les conditions équivalentes ci-dessus est *semisimple*.

L'exemple le plus important pour nous sera celui donné par le théorème de Maschke (Exercice 3.1.7.5) : si G est un groupe fini et K un corps de caractéristique $p \geq 0$ alors la K-algèbre $K[G]$ est semisimple si et seulement si $p \not| |G|$.

Une autre famille d'exemples est donnée par l'énoncé suivant.

Corollaire 3.1.1 *Soit M un A-module fidèle (i.e. $aM = 0$ si et seulement si $a = 0$) de type fini comme $A' := \mathrm{End}_A(M)$-module. Alors A est semisimple si et seulement si M est un A-module semisimple .*

Preuve. La condition nécessaire résulte de l'exercice 3.1.7. Pour la condition suffisante, fixons un système de générateurs $m_1, \ldots, m_r$ de M *comme A'-module* et considérons le morphisme de A-modules

$$\begin{array}{rccc} \phi: & A & \to & M^{\oplus r} \\ & a & \to & (am_i)_{1\leq i\leq r} \end{array}$$

Ce morphisme est injectif. En effet, comme

$$M = \sum_{1\leq i\leq r} A'm_i$$

pour tout $m \in M$ il existe $a'_{m,1}, \ldots, a'_{m,r} \in A'$ tel que $m = \sum_{1\leq i\leq r} a'_{m,i}m_i$. Mais alors, pour tout $a \in \ker(\phi)$ on a

$$a(m) = \sum_{1\leq i\leq r} aa'_{m,i}m_i = \sum_{1\leq i\leq r} a'_{m,i}am_i = 0$$

donc $a = 0$. La conclusion résulte alors du fait que tout sous-A-module d'un A-module semisimple est semisimple (Exercice 3.1.7.1). □

Exercice 3.1.2 (Lemme de densité) *Soit M un A-module semi-simple ; notons $A' := \mathrm{End}_A(M)$, $A'' := \mathrm{End}_{A'}(M)$.*

1. *Vérifier que la multiplication à gauche induit un morphisme d'anneaux $L : A \to A''$.*
2. *Montrer que pour tout $\phi \in A''$ et $m \in M$ il existe $a \in A$ telle que $\phi(m) = L_a(m)$.*
3. *Montrer que pour tout $\phi \in A''$ et $m_1, \ldots, m_r \in M$ il existe $a \in A$ telle que $\phi(m_i) = L_a(m_i)$, $i = 1, \ldots, r$. En déduire que si M est un A'-module de type fini alors $L : A \to A''$ est surjective.*

3.1.2 Théorèmes de structure

3.1.2.1 Anneaux semisimples

Par définition du A-module régulier (A, L), les sous-A-modules de (A, L) sont les idéaux à gauche de A.

Proposition 3.1.3 *Supposons que A est semisimple et soit $\mathcal{I}_i$, $i \in I$ un système de représentants des classes d'isomorphismes des idéaux à gauche de A, simples comme sous-A-modules de (A, L). Alors,*

1. *I est fini ;*
2. *Pour chaque $i \in I$, l'idéal à gauche A_i engendré par tous les idéaux à gauche de A isomorphes à $\mathcal{I}_i$ (comme A-modules) est un idéal bilatère et*
$$A = \bigoplus_{i\in I} A_i$$
comme A-modules.
3. *Décomposons 1_A sous la forme $1_A = \sum_{i\in I} e_i$ avec $e_i \in A_i$, $i \in I$. On a $e_i^2 = e_i$, $e_ie_j = \delta_{i,j}e_i$ et $e_ia = ae_i$, $a \in A$, $i, j \in I$. De plus, pour chaque $i \in I$, $A_i = Ae_i$, la structure d'anneau sur A induit une structure d'anneau sur l'idéal bilatère A_i d'unité e_i et*
$$A = \prod_{i\in I} A_i$$
comme anneaux.

Preuve. Observons d'abord que $\mathcal{I}_i\mathcal{I}_j = 0$ si $i \neq j$. En effet, puisque $\mathcal{I}_j$ est un idéal à gauche, tout élément $a_j \in \mathcal{I}_j$ induit par multiplication à droite un morphisme de A-modules $R_{a_j} : \mathcal{I}_i \to \mathcal{I}_j$, qui est nul, par le lemme de Schur.

On en déduit que $A_iA_j = 0$ si $i \neq j$. Par ailleurs, puisque A est semisimple, on a

$$A = \sum_{i\in I} A_i.$$

Donc en particulier

$$A_iA = A_iA_i \subset A_i,$$

ce qui montre que les A_i, $i \in I$ sont aussi des idéaux à droite. Ecrivons maintenant

$$1_A = \sum_{i \in I} e_i.$$

Le sous-ensemble $I' \subset I$ des $i \in I$ tels que $e_i \neq 0$ est fini. On vérifie immédiatement que le morphisme

$$\begin{array}{rccc} \phi : & \bigoplus_{i \in I'} A_i & \to & A \\ & (a_i)_{i \in I'} & \to & \sum_{i \in I'} a_i \end{array}$$

est un isomorphisme de A-modules d'inverse

$$\begin{array}{rccc} \psi : & A & \to & \bigoplus_{i \in I'} A_i \\ & a & \to & (ae_i)_{i \in I'} \end{array}$$

En particulier, $I = I'$ est fini. D'où (1) et (2). Des égalités

$$\begin{array}{l} 1_A^2 = 1_A \, ; \\ a1_A = a = 1_A a, \, a \in A, \end{array}$$

on déduit que les e_i, $i \in I'$ vérifient $e_i e_j = \delta_{i,j} e_i$ et $e_i a = a e_i$, $a \in A$. On vérifie également que A_i muni des lois $+$ et $\times$ héritées de A est un anneaux d'unité e_i, $i \in I$ et qu'avec ces structures d'anneaux sur les A_i, le morphisme ci-dessus est également un morphisme d'anneaux. □

3.1.2.2 Anneaux simples

On dit que A est *simple* si A est semisimple et si A ne contient qu'une classe d'isomorphisme (comme A-module) d'idéaux à gauche simples.

Lemme 3.1.4 *Soit A un anneau semisimple. Alors A est simple si et seulement si A ne contient pas d'autres idéaux bilatères que 0 et A.*

Preuve. Supposons d'abord que A est simple. Comme A est semisimple, A s'écrit comme somme directe d'idéaux à gauche simples

$$A = \bigoplus_{i \in I} \mathcal{I}_i$$

Comme tout idéal bilatère contient un idéal à gauche simple (rappelons que tout A-module semisimple non-nul contient un sous A-module simple (Lemme 1.5.5)), il suffit de montrer que si $\mathcal{I}$ est un idéal à gauche simple de A alors $\mathcal{I}A = A$.

1. Pour tout $\mathcal{I}'$ idéal à gauche simple de A, il existe $a \in A$ tel que $\mathcal{I}a = \mathcal{I}'$.

   En effet, comme A est semisimple on peut écrire $A = \mathcal{I} \oplus \mathcal{J}$ pour un certain idéal à gauche $\mathcal{J}$ de A. Notons $p : A \to \mathcal{I}$ la projection de A sur $\mathcal{I}$ parallèlement à $\mathcal{J}$. Par construction $p : A \to \mathcal{I}$ est un morphisme de A-modules. Fixons un isomorphisme de A-modules $\sigma : \mathcal{I} \tilde{\to} \mathcal{I}'$. Alors la composée

   $$A \stackrel{p}{\to} \mathcal{I} \stackrel{\sigma}{\tilde{\to}} \mathcal{I}' \hookrightarrow A$$

   est un endomorphisme du A-module A. Mais on a un isomorphisme canonique $A^{op} \tilde{\to} \mathrm{End}_A(A)$, $a \to R_a$ (d'inverse $\mathrm{End}_A(A) \tilde{\to} A^{op}$, $\alpha \to \alpha(1)$). Il existe donc $a \in A$ tel que $\sigma \circ p = R_a$. En particulier, pour tout $x \in \mathcal{I}$ on a $xa = \sigma \circ p(x) = \sigma(x) \in \mathcal{I}'$; on en déduit que $R_a : A \to A$ induit un morphisme non nul de A-modules $R_a : \mathcal{I} \to \mathcal{I}'$, qui est nécessairement un isomorphisme par le lemme de Schur. En particulier, on a $\mathcal{I}' = \mathcal{I}a$ comme annoncé.

2. D'après (1), pour tout $i \in I$ il existe $a_i \in A$ tel que $\mathcal{I}_i = \mathcal{I}a_i$. D'où

   $$A = \bigoplus_{i \in I} \mathcal{I}_i = \bigoplus_{i \in I} \mathcal{I}a_i = \mathcal{I}A.$$

La réciproque résulte directement de la la proposition 3.1.3. □

Lemme 3.1.5 *Supposons que A est simple et soit $\mathcal{I}$ un idéal à gauche non nul. Notons $A' := \mathrm{End}_A(\mathcal{I})$ et $A'' := \mathrm{End}_{A'}(\mathcal{I})$. Alors le morphisme canonique induit par la multiplication à gauche $L : A \tilde{\to} A''$ est un isomorphisme d'anneaux.*

Preuve. Commençons par observer que L est bien défini *i.e.* que pour tout $a \in A$ on a bien $L_a|_{\mathcal{I}} \in A''$. En effet, pour tout $\phi \in A'$ et pour tout $b \in \mathcal{I}$, comme $ab \in \mathcal{I}$ on a $\phi \circ L_a(b) = \phi(ab) = a\phi(b) = L_a \circ \phi(b)$.

En outre, par construction $\ker(L)$ est un idéal bilatère de A distinct de A donc (Lemme 3.1.4) $L : A \hookrightarrow A''$ est un morphisme injectif. Par ailleurs, comme $\mathcal{I}A$ est un idéal bilatère non nul de A, on a (Lemme 3.1.4) $A = \mathcal{I}A$ donc $L(A) = L(\mathcal{I}) \circ L(A)$. Supposons avoir montrer que $L(\mathcal{I})$ est un idéal à gauche de A''. On aura alors $A'' \circ L(\mathcal{I}) = L(\mathcal{I})$ et comme $L(A)$ contient $Id_I = L_{1_A}$,

$$A'' = A'' \circ L(A) = A'' \circ L(\mathcal{I}) \circ L(A) = L(\mathcal{I}) \circ L(A) = L(A).$$

Reste donc à voir que $L(\mathcal{I})$ est un idéal à gauche de A''. Soit donc $a \in \mathcal{I}$ et $\phi \in A''$. On doit montrer que $\phi \circ L_a \in L(\mathcal{I})$. Or, pour tout $b \in \mathcal{I}$, on a $R_b \in A'$ donc

$$\phi \circ L_a(b) = \phi(ab) = \phi \circ R_b(a) = R_b \circ \phi(a) = \phi(a)b = L_{\phi(a)}(b),$$

ce qui montre que $\phi \circ L_a = L_{\phi(a)} \in L(\mathcal{I})$. □

Exemple 3.1.6 Avec les notations de la proposition 3.1.3, les anneaux A_i sont simples, $i \in I$. En particulier, on a un isomorphisme d'anneaux

$$A \tilde{\to} \prod_{i \in I} \mathrm{End}_{A_i'}(\mathcal{I}_i),$$

où $A_i' := \mathrm{End}_A(\mathcal{I}_i)$, $i \in I$.

Exemple 3.1.7 *Soit A un anneau simple.*

1. *Montrer que $Z(A)$ est un corps commutatif.*
2. *Montrer que les seuls idéaux bilatères de $M_n(A)$ sont 0 et $M_n(A)$.*
3. *Montrer que si A est de dimension finie sur $Z(A)$ ou que si A est à division alors $M_n(A)$ est semisimple. Donner alors une décomposition explicite de $M_n(A)$ en somme directe d'idéaux à gauche simples tous isomorphes.*

Exercice 3.1.8 (Radical de Jacobson) *On dit qu'un idéal I de A est nilpotent s'il existe un entier $n \geq 1$ tel que $I^n = 0$ et que c'est un nilidéal si tous ses éléments sont nilpotents. Un idéal nilpotent est toujours un nilidéal mais la réciproque est fausse lorsque A n'est pas commutatif.*
Soit maintenant K un corps et A une K-algèbre de K-dimension finie. On appelle radical de Jacobson de A l'intersection $\mathcal{J}_A$ de tous les idéaux à gauche maximaux de A.

1. *Montrer que $\mathcal{J}_A$ est l'intersection des $Ann_A(M) := \{a \in A \mid aM = 0\}$, où M décrit l'ensemble des A-modules simples. En déduire que $\mathcal{J}_A$ est un idéal bilatère. Montrer que $\mathcal{J}_{A/\mathcal{J}_A} = 0$.*
2. *Montrer que $\mathcal{J}_A$ est nilpotent.*
3. *Montrer que pour un idéal à gauche I de A, les assertions suivantes sont équivalentes :*
   (a) *I est nilpotent ;*
   (b) *I est un nilidéal ;*
   (c) *I est contenu dans $\mathcal{J}_A$.*
4. *Montrer que A admet un plus petit idéal à gauche I_0 tel que A/I_0 est semisimple. Montrer que $\mathcal{J}_A = I_0$. En déduire que A est semisimple si et seulement si $\mathcal{J}_A = 0$ et qu'un A-module M est semi-simple si et seulement si $\mathcal{J}_A M = 0$. En déduire que si A est commutative alors A est semisimple si et seulement si A ne contient pas d'éléments nilpotents (non nuls) et que, dans ce cas, c'est un produit fini d'extensions de corps finies de K ;*
5. *(Utilise de la théorie de Galois) Supposons que A est semisimple. Montrer que pour toute extension de corps L/K séparable finie $L \otimes_K A$ est encore semisimple. Donner un contre-exemple lorsque L/K n'est plus supposée séparable.*

Exercice 3.1.9 *Soit G un groupe fini.*

1. *Soit k un corps de caractéristique première à $|G|$. Pour tout $x = \sum_{g\in G} x_g g \in k[G]$ et $g_0 \in G$, calculer la trace $T(xg_0)$ de la multiplication à gauche par xg_0 sur $k[G]$. En déduire que $\mathcal{J}_{k[G]} = 0$ donc que $k[G]$ est semi-simple.*
2. *Supposons maintenant que $|G| = p^r$ et que k est de caractéristique p. Calculer $\mathcal{J}_{k[G]}$.*

Exercice 3.1.10

1. *Soit A un anneau simple. Montrer que $Z(A)$ est un corps commutatif. On dit qu'une k-algèbre A de k-dimension finie est simple centrale si A est un anneau simple et $Z(A) = k$.*
2. *Soit A une k-algèbre simple centrale et B une k-algèbre simple. Montrer que $A \otimes_k B$ est une k-algèbre simple et que le morphisme canonique $Z(B) \simeq Z(A \otimes_k B)$, $b \to 1 \otimes b$ est un isomorphisme. En déduire que si A et B sont des k-algèbres simples centrales alors $A \otimes_k B$ est aussi une k-algèbre simple centrale.*
3. *Soit A une k-algèbre de k-dimension finie n. Montrer que A est une k-algèbre simple centrale si et seulement si le morphisme canonique*
$$A \otimes_k A^{op} \to \mathrm{End}_k(A)$$
est un isomorphisme. Montrer que $\mathrm{End}_k(A) = M_n(k)$.

3.1.2.3 Modules sur des anneaux semisimples

Notons $\widehat{A}$ l'ensemble des classes d'isomorphismes de A-modules simples.

Proposition 3.1.11 *Supposons que A est semisimple. Alors, avec les notations de la proposition 3.1.3, on a*

1. *Les $\mathcal{I}_i$, $i \in I$ forme un système de représentants des classes d'isomorphismes de A-modules simples. En particulier $|\widehat{A}| = |I|$;*
2. *Pour tout A-module M on a*
$$M = \bigoplus_{i\in I} A_i M = \bigoplus_{i\in I} e_i M.$$
En outre, pour chaque $i \in I$, le sous-A-module $A_iM = e_iM$ est le sous-A-module de M engendré par les sous-A-modules simples de M isomorphes à $\mathcal{I}_i$; il est donc isomorphe à une somme directe de copies de $\mathcal{I}_i$.
3. *Si, en outre, K est un corps et A est une K-algèbre de K-dimension fini alors tout A-module M de K-dimension finie se décompose de façon unique sous la forme*
$$M = \bigoplus_{i\in I} \mathcal{I}_i^{\oplus n_i}$$
et le uplet des multiplicités n_i, $i \in I$ détermine la classe d'isomorphisme de M comme A-module.

Preuve. Soit M un A-module simple. Tout $0 \neq m \in M$, définit alors un morphisme surjectif de A-modules $\lambda_m : A \twoheadrightarrow M$, $a \to am$. Comme A est semisimple, il existe un idéal à gauche $\mathcal{I}$ de A tel que $A = \ker(\lambda_m) \oplus \mathcal{I}$ et , par construction, le morphisme $\lambda_m : A \to M$ induit un isomorphisme $\lambda_m|_{\mathcal{I}} : \mathcal{I} \xrightarrow{\sim} M$. Ce qui montre que $\mathcal{I}$ est un idéal à gauche simple de A. D'où (1).
Soit maintenant M un A-module quelconque. On a $M = AM$ donc, d'après la proposition 3.1.3,
$$M = \sum_{i\in I} A_i M = \sum_{i\in I} e_i AM = \sum_{i\in I} e_i M$$
et cette somme est directe puisque pour tout $m_i \in M$, $i \in I$ la relation
$$\sum_{i\in I} e_i m_i = 0$$
implique, en multipliant à gauche par e_i, que $0 = e_i^2 m_i = e_i m_i$, $i \in I$. Enfin, notons M_i le sous-A-module de M engendré par les sous-A-modules simples de M isomorphes à $\mathcal{I}_i$. On a alors
$$e_i M = A_i M = \sum_{I\simeq I_i} IM = \sum_{I\simeq I_i,\, m\in M} Im.$$
Or pour tout $I \simeq I_i$ et $m \in M$, le morphisme de A-module $R_m : I \twoheadrightarrow Im$, $a \to am$ est soit nul soit un isomorphisme (lemme de Schur). Cela montre que $e_iM \subset M_i$. Inversement, on a
$$M_i = \sum_{N\simeq I_i} N$$

et pour tout sous-A-module $N \subset M$ tel que $N \simeq I_i$, pour tout $0 \neq n \in N$, le morphisme de A-module $R_n : A \to N$ est surjectif et, comme A est semisimple, il existe un idéal à gauche simple $I \subset A$ tel que $R_n : A \to N$ induise un isomorphisme $R_n|_I : I \xrightarrow{\sim} N$. Cela montre que $I \simeq I_i$ et que $N \subset IM \subset A_i M = e_i M$.
L'assertion (3) est l'unicité dans Jordan-Holder. □

3.2 Récoltes : représentations linéaires des groupes finis

3.2.1 K-algèbres semisimples de dimension finie (résumé)

Reprenons ce qui précède dans le cas particulier suivant : K est un corps et A est une K-algèbre semisimple de K-dimension finie. On a alors vu que $\widehat{A}$ est fini et coïncide avec les classes d'isomorphismed d'idéaux à gauche simples de A. En outre, pour tout $I \in \widehat{A}$, en notant $A_I := \sum_{I \simeq J \subset A} J$ et $1_A = \sum_{I \in \hat{A}} e_I$ avec $e_I \in A_I$, on a des isomorphismes canoniques

— de K-modules $A \xrightarrow{(1)}{\sim} \oplus_{I \in \widehat{A}} A_I$ donné explicitement par $a \to (ae_I)_{I \in \widehat{A}}$;

— de K-algèbres

$$A \xrightarrow{(2)}{\sim} \prod_{I \in \widehat{A}} A_I \xrightarrow{(3)}{\sim} \prod_{I \in \widehat{A}} \mathrm{End}_{D_I}(I),$$

où $D_I := \mathrm{End}_A(I)$ est une K-algèbre à division (lemme de Schur). (2) est donné explicitement par $a \to (ae_I)_{I \in \widehat{A}}$ et (3) par $(a_I)_{I \in \widehat{A}} \to (L_{a_I})_{I \in \widehat{A}}$.

En fixant pour chaque $I \in \widehat{A}$ une D_I bases $\underline{b}_I$ de I, on a également un morphisme de K-modules (non canonique)

$$A \xrightarrow{(4)}{\simeq} \prod_{I \in \widehat{A}} I^{\oplus \dim_{D_i}(I)}$$

donné explicitement par $a \to (L_a(\underline{b}_I))_{I \in \widehat{A}}$.

Lorsque K est algébriquement clos, on a de plus $D_I = K$.

En combinant cela avec l'observation de l'exemple 3.1.7, on obtient

Corollaire 3.2.1 *Soit A une K-algèbre de K-dimension finie. Alors*

1. *A est simple si et seulement si A est isomorphe comme K-algèbre à $M_n(D)$, pour une K-algèbre à division D. Si, de plus, K est algébriquement clos, alors A est simple si et seulement si A est isomorphe comme K-algèbre à $M_n(K)$;*
2. *A est semisimple si et seulement si A est isomorphe comme K-algèbre à*

$$\prod_{1 \leq i \leq r} M_{n_i}(D_i)$$

pour des K-algèbre à division D_i, $i = 1, \ldots, r$. Si, de plus, K est algébriquement clos, alors A est semisimple si et seulement si A est isomorphe comme K-algèbre à

$$\prod_{1 \leq i \leq r} M_{n_i}(K).$$

3.2.2 Applications à $K[G]$

On va maintenant appliquer ce qui précède à $A = K[G]$, où K est un corps *algébriquement clos de caractéristique $p \geq 0$ et G un groupe fini tel que, si $p > 0$, $p \not| |G|$*. Un $K[G]$-module signifiera toujours un $K[G]$-module de *K-dimension finie.*

3.2.2.1 Position du problème

Comme $K[G]$ est semisimple, classifier les $K[G]$-modules revient à classifier les $K[G]$-modules simples. On sait déjà que $|\widehat{K[G]}|$ est fini ; le problème consiste donc essentiellement à exhiber suffisamment de $K[G]$-modules simples non-isomorphes. Voici déjà deux façons élémentaires de construire des $K[G]$-modules simples. On en verra une plus sophistiquée au paragraphe 3.3.

1. Pour tout $p : G \twoheadrightarrow G'$ un morphisme surjectif de groupes finis, l'application
$$\begin{array}{ccc} \widehat{k[G']} & \to & \widehat{k[G]} \\ V' & \to & V'|_G \end{array}$$
est bien définie et injective.
2. Soit $(k, \chi) \in \widehat{k[G]}$ de dimension 1, l'application
$$\begin{array}{ccc} \widehat{k[G]} & \to & \widehat{k[G]} \\ V & \to & \chi \otimes_K V \end{array}$$
est bien définie et bijective. Par contre, elle peut avoir des points fixes...

3.2.2.2 Nombre et dimensions des $K[G]$-modules simples

Les résultats suivants se déduisent de
$$K[G] \simeq \prod_{I \in \widehat{K[G]}} \mathrm{End}_K(I)$$
en prenant les K-dimension de $K[G]$ et de son centre respectivement.

1. $|G| = \sum_{I \in \widehat{K[G]}} \dim_K(I)^2$;
2. Notons $Cl(G)$ l'ensemble des classes de conjugaison de G. On a $|\widehat{K[G]}| = |Cl(G)|$.

   En effet $Z(K[G]) = K^{|\widehat{K[G]}|}$ donc $|\widehat{K[G]}| = \dim_K(Z(K[G]))$. Mais, pour tout $\underline{a} = \sum_{g \in G} a(g)g \in K[G]$, on a $\underline{a} \in Z(K[G])$ si et seulement si $g_0\underline{a} = \underline{a}g_0$, $g_0 \in G$ *i.e.* si et seulement si $\sum_{g \in G} a(g_0^{-1}g)g = \sum_{g \in G} a(gg_0^{-1})g$, $g_0 \in G$. Mais cette dernière égalité équivaut à $a(g_0^{-1}gg_0) = a(g)$, $g,\ g_0 \in G$. Donc une K-base de $Z(K[G])$ est donnée par $(\epsilon_C := \sum_{g \in C} g)_{C \in Cl(G)}$.

3.2.2.3 Caractères

Lemme 3.2.2 *Soit K un corps de caractéristique $p \geq 0$, A une K-algèbre semisimple de K-dimension finie et M, N deux A-modules de K-dimension finie.*

1. *Si pour tout $a \in A$, $L_a|_M \in \mathrm{End}_K(M)$ et $L_a|_N \in \mathrm{End}_K(N)$ ont même polynôme caractéristique alors $M \simeq N$ comme A-modules.*
2. *Si $p = 0$ ou si $\dim_K(A) < p$ et si pour tout $a \in A$, $L_a|_M \in \mathrm{End}_K(M)$ et $L_a|_N \in \mathrm{End}_K(N)$ ont même trace alors $M \simeq N$ comme A-modules.*

Preuve. On écrit $M = \oplus_{I \in \widehat{A}} I^{\oplus \nu_I(M)}$, $N = \oplus_{I \in \widehat{A}} I^{\oplus \nu_I(N)}$ et le problème revient à montrer que $\nu_I(M) = \nu_I(N)$, $I \in \widehat{A}$. Or, pour (1) l'hypothèse pour $a = e_I$ nous dit que $(T-1)^{\nu_I(M)\dim_K(I)} = (T-1)^{\nu_I(N)\dim_K(I)}$ dans $K[T]$, $I \in \widehat{A}$. Pour (2), l'hypothèse pour $a = e_I$ dit seulement $\nu_I(M)\dim_K(I) = \nu_I(N)\dim_K(I)$ dans K. Mais comme $\dim_K(I) \leq \dim_K(A) < p$, cela implique bien $\nu_I(M) = \nu_I(N)$. □

A partir de maintenant, *on suppose de plus $p = 0$.*

Soit V un $K[G]$-module, le *caractère* de V est la forme K-linéaire

$$\begin{array}{rccl} \chi_V : & K[G] & \to & K \\ & a & \to & Tr(L_a|_V : V \to V), \end{array}$$

Notons que les données suivantes sont équivalentes :

1. la forme K-linéaire $\chi_V : K[G] \to K$;
2. l'application ensembliste $\chi_V|_G : G \to K$;
3. l'élément $\chi_V = \sum_{g\in G} \chi(g)g$ de $K[G]$.

On notera

$$\widehat{G} = \{\chi_I \mid I \in \widehat{K[G]}\}$$

l'ensemble des caractères des $K[G]$-modules simples. Explicitement,

$$\chi_I(a) = Tr_I(L_a|_I : I \to I = \frac{1}{\dim_K(I)} Tr_{K[G]}(L_{ae_I} : K[G] \to K[G]).$$

Il résulte directement du Lemme 3.2.2 que l'application

$$\begin{array}{ccc} \widehat{K[G]} & \to & \widehat{G} \\ I & \to & \chi_I \end{array}$$

est bijective donc en particulier que $|\widehat{G}| = |\widehat{K[G]}|$.

Exercice 3.2.3 *Soit V, V' deux $K[G]$-modules. Calculer, en fonction de χ_V et $\chi_{V'}$ les caractères de*

1. *$V \oplus V'$;*
2. *$V \otimes V'$. Ici $V \otimes V'$ est le $K[G]$-module défini comme le K-espace vectoriel $V \otimes_K V'$ muni de la structure de $K[G]$-module*
$$g \cdot v \otimes v' = (g \cdot v) \otimes (g' \cdot v');$$
3. *$V^\vee$. Ici $V^\vee$ est le $K[G]$-module défini comme le K-espace vectoriel $V^\vee = \mathrm{Hom}_K(V, K)$ muni de la structure de $K[G]$-module*
$$g \cdot f = f(g^{-1} \cdot -);$$
4. *$\mathrm{Hom}_{K[G]}(V, V')$. Ici $\mathrm{Hom}_{K[G]}(V, V')$ est le $K[G]$-module défini comme le K-espace vectoriel $\mathrm{Hom}_K(V, V')$ muni de la structure de $K[G]$-module*
$$g \cdot f = g \cdot f(g^{-1} \cdot -).$$

Notons $\mathrm{Mod}^\circ_{/K[G]}$ l'ensemble des classes d'isomorphismes de $k[G]$-modules. Les relations (1) et (2) montrent que $\mathrm{Mod}^\circ_{/K[G]}$ est un monoide commutatif pour $\oplus$ et $\otimes$ (quelles sont les éléments neutres ?). En déduire qu'il existe un unique anneau commutatif $R_K(G)$ muni d'un morphisme de monoides (pour l'addition et la multiplication) injectif $\mathrm{Mod}^\circ_{/K[G]} \hookrightarrow R_K(G)$ universel pour les morphismes de monoides de $\mathrm{Mod}^\circ_{/K[G]}$ à valeur dans un anneau commutatif. On dit que $R_K(G)$ est l'anneau des représentations virtuelles de G sur K.

3.2.2.4 Caractères et $K[G]$-module régulier

On notera $\chi_{reg} : K[G] \to K$ le caractère du $K[G]$-module régulier $(K[G], L)$.

Les résultats suivants se déduisent directement de

$$K[G] \simeq \bigoplus_{I\in\widehat{K[G]}} I^{\oplus \dim_K(I)}.$$

1.
$$\chi_{reg} = \sum_{I\in\widehat{K[G]}} \dim_K(I)\chi_I;$$

2.
$$\chi_{reg}(g) = \begin{array}{ll} |G| & \text{si } g = 1\,; \\ 0 & \text{sinon.} \end{array}$$

3. $\chi_I(e_J) = \delta_{I,J}\dim_K(I)$, $I, J \in \widehat{K[G]}$.
4. Par définition, les χ_I sont constants sur les classes de conjugaisons de G donc (*cf.* 2.1 (2)) ils sont dans $Z(K[G])$. En fait, les χ_I, $I \in \widehat{K[G]}$ forment une K-base de $Z(K[G])$.

   En effet, Comme $\dim_K(Z(K[G])) = |Cl(G)| = |\widehat{K[G]}|$, il suffit de montrer que les χ_I, $I \in \widehat{K[G]}$ sont K-libres. Or, pour tout $(\lambda_I)_{I\in\widehat{K[G]}} \in K^{|\widehat{K[G]}|}$ tels que
$$\sum_{I\in\widehat{K[G]}} \lambda_I\chi_I = 0,$$
   en évaluant en les e_I, $I \in \widehat{K[G]}$, on obtient $\lambda_I\dim_K(I) = 0$, $I \in \widehat{K[G]}$.
   En fait, en écrivant $e_I = \sum_{g\in G} e_I(g)g$, on a d'une part $\chi_{reg}(e_I g_0^{-1}) = \sum_{g\in G} e_I(g)\chi_{reg}(gg_0^{-1}) = e_I(g_0)|G|$ et d'autre part $\chi_{reg}(e_I g_0^{-1}) = \chi_{reg}(g_0^{-1}e_I) = \dim_K(I)Tr(L_{g_0^{-1}}|_I) = \dim_K(I)\chi_I(g_0^{-1})$. D'où
$$\dim_K(I)\chi_I(g_0^{-1}) = |G|e_I(g_0),\ g_0 \in G.$$
   A ce stade, on dispose donc de trois K-bases canoniques de $Z(K[G])$: χ_I, $I \in \widehat{K[G]}$, e_I, $I \in \widehat{K[G]}$, ϵ_C, $C \in Cl(G)$. On prendra garde que si les deux premières correspondent à la décomposition $Z(K[G]) = \oplus_{I\in\widehat{K[G]}} Z(K[G]_I)$, il n'en est pas de même de la dernière.

Exercice 3.2.4 (Dénombrement) *Soit G un groupe fini*

1. *Soit $(V,\theta) \in \widehat{K[G]}$.*
   (a) Montrer que pour tout $x \in G$
$$R_\theta(x) := \frac{1}{|G|}\sum_{g\in G} \theta(gxg^{-1}) = \frac{\chi_\theta(x)}{\chi_\theta(1)}Id.$$
   (b) Montrer que pour tout $x_1, \ldots, x_n, y \in G$
$$\frac{1}{|G|^n}\sum_{g_1,\ldots,g_n\in G} \chi_\theta(g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1}y) = \frac{\chi_\theta(x_1)\cdots\chi_\theta(x_n)\chi_\theta(y)}{\chi_\theta(1)^n}.$$
2. *Soit $C_1, \ldots, C_n$ n classes de conjugaison de G. Déduire de ce qui précède le nombre de solutions dans $C_1\times\cdots\times C_n$ de l'équation*
$$g_1\cdots g_n = 1$$
   en fonction des $\chi(C_i)$, $i = 1, \ldots, n$, $\chi \in \widehat{G}$, de $|G|$ et des $|C_i|$, $i = 1, \ldots, n$.

A noter que ce résultat est à l'origine des techniques dites de rigidité, qui ont permis de réaliser de nombreux groupes finis comme groupes de Galois d'extensions finis de $\mathbb{Q}$. Cf. [Se92, Chap. 7] pour plus de détails.

Exercice 3.2.5 (Caractères et sous-groupes normaux) *Soit G un groupe fini.*

1. *Soit (V,θ) un $\mathbb{C}[G]$-module. Montrer que*
$$N_\theta = \{g \in G \mid \chi_\theta(g) = \chi_\theta(1)\} = \ker(\theta).$$
2. *Montrer que tout sous-groupe normal de G est de la forme*
$$\bigcap_{(V,\theta)\in E} N_V,$$
   pour un sous-ensemble $E \subset \widehat{\mathbb{C}[G]}$.
3. *En déduire que G est simple si et seulement si pour tout $(V,\theta) \in \widehat{K[G]} \setminus \mathbb{I}$ on a $N_\theta = \{1\}$.*

Exercice 3.2.6 (Caractères des groupes abéliens finis)

1. *Soit G un groupe fini. Montrer que G est abélien si et seulement si $\dim_K(I) = 1$, $I \in \widehat{K[G]}$.*
2. *Soit G un groupe abélien fini. Montrer que l'ensemble $\widehat{G}$ des caractères des $K[G]$-modules simples est un groupe commutatif pour le produit et que le morphisme canonique*

$$\begin{array}{ccc} G & \to & \widehat{\widehat{G}} \\ g & \to & \chi \to \chi(g) \end{array}$$

est un isomorphisme.

Exercice 3.2.7 (Corps finis) *Soit $q = p^e$ avec p premier et $e \in \mathbb{Z}_{\geq 1}$. On note $\mathbb{F}_q$ le corps à q éléments et on se fixe $\omega_p \in \mathbb{C}$ racine primitive p-ième de l'unité.*

1. *On dit qu'une extension de corps algébrique K/k séparable si pour tout $x \in K$ le polynôme minimal de x sur k est séparable (i.e. à racines simples sur son corps de décomposition). Si K/k est une extension de corps finie, pour tout $x \in K$ on note $L_x : K \to K$, $y \to xy$ la multiplication à gauche par x, que l'on regarde comme un endomorphisme du k-espace vectoriel K et on note $tr_{K/k}(x)$ sa trace. Cela nous donne une forme linéaire $tr_{K/k} : K \to k$. Soit k un corps fini. On rappelle que toute extension finie K/k est monogène i.e. de la forme $K = k(x)/k$. Montrer que si K/k est séparable, $tr_{K/k} : K \to k$ est non nulle (on pourra par exemple observer qu'il suffit de montrer que $tr_{K/k} \otimes_k \overline{k} : K \otimes_k \overline{k} \to \overline{k}$ est non nulle).*
2. *On considère l'application*

$$\begin{array}{rccc} \tau : & \mathbb{F}_q & \to & \mathbb{C}^\times \\ & x & \to & \omega_p^{Tr_{\mathbb{F}_p}(L_x)}, \end{array}$$

où $L_x : \mathbb{F}_q \to \mathbb{F}_q$, $y \to xy$ est la multiplication à gauche par x vu comme élément de $\mathrm{End}_{\mathbb{F}_p}(\mathbb{F}_q)$. Montrer que $\tau \in \widehat{\mathbb{F}}_q$ et que $\tau \neq 1$.
3. *Déduire de ce qui précède que l'application*

$$\begin{array}{rccc} \tau \circ R_- : & \mathbb{F}_q & \to & \widehat{\mathbb{F}}_q \\ & y & \to & x \to \tau(xy) \end{array}$$

est un isomorphisme de groupes.

Le lemme 3.2.2 montre en particulier qu'un $K[G]$-module (simple) est entièrement déterminé par son caractère. Le problème de la détermination des $K[G]$-modules simples se ramène donc à celui de la construction de la 'table des caractères'. Pour cela, on dispose de relations numériques dites 'd'orthogonalité', qui permettent souvent de construire la table des caractères en n'ayant que peu d'informations sur le groupe G.

3.2.2.5 Orthogonalité

On veut munir $K[G]$ d'une forme bilinéaire symétrique non dégénérée. Pour cela, on utilise l'isomorphisme de K-algèbres

$$\begin{array}{rccc} \mathcal{F} : & K[G] & \tilde{\to} & \Pi_G \\ & a & \to & (L_a|_I : I \to I)_{I \in \widehat{K[G]}}, \end{array}$$

où l'on a noté :

$$\Pi_G := \prod_{I \in \widehat{K[G]}} \mathrm{End}_K(I).$$

Sur chaque $\mathrm{End}_K(I)$ on dispose d'une forme K-biliéaire symétrique non dégénérée

$$\begin{array}{rccc} (-,-) : & \mathrm{End}_K(I) \times \mathrm{End}_K(I) & \tilde{\to} & K \\ & (\phi, \psi) & \to & Tr_V(\phi \circ \psi). \end{array}$$

On peut munir $K[G]$ de la forme bilinéaire symétrique $(-,-)_G : K[G] \times K[G] \to K$ définie par

$$(a,b)_G = \frac{1}{|G|^2} \sum_{I \in \widehat{K[G]}} \dim_K(I) Tr_I(L_a|_I \circ L_b|_I) = \frac{1}{|G|^2} \sum_{I \in \widehat{K[G]}} \dim_K(I) Tr_I(L_{ab}) = \frac{1}{|G|^2} \sum_{I \in \widehat{K[G]}} Tr_{K[G]}(L_{abe_I}) = \frac{1}{|G|^2} Tr_{K[G]}(L_{ab}).$$

Donc, simplement

$$(a,b)_G = \frac{1}{|G|^2} \chi_{reg}(ab)$$

On peut expliciter un peu plus $(-,-)_G$ comme suit.

1. Pour tout $g, h \in G$ on a
$$(g,h)_G = \frac{1}{|G|^2} \chi_{reg}(gh) = \frac{1}{|G|} \delta_{g,h^{-1}},$$
d'où, par K-linéarité, pour tout $a, b \in K[G]$ on a
$$(a,b)_G = \frac{1}{|G|} \sum_{g \in G} a(g) b(g^{-1})$$
2. On voit aussi immédiatement que
$$(e_I, e_J)_G = \frac{1}{|G|^2} Tr_{K[G]}(L_{e_I e_J}) = \frac{\dim_K(I)^2}{|G|^2} \delta_{I,J}.$$
En particulier, comme les e_I, $I \in \widehat{K[G]}$ forme une K-base de $Z(K[G])$, on voit que la restriction à $Z(K[G])$ de $(-,-)_G$ est encore non-déénérée et que les e_I, $I \in \widehat{K[G]}$ sont une base orthogonale de $(Z(K[G], (-,-)_G)$.
3. De $\dim_K(I)\chi_I(g^{-1}) = |G| e_I(g)$, $g \in G$, on déduit également
$$(\chi_I, \chi_J)_G = \frac{1}{|G|^2} \sum_{g \in G} \frac{|G|^2}{\dim_K(I)\dim_K(J)} e_I(g^{-1}) e_J(g) = \frac{|G|^2}{\dim_K(I)\dim_K(J)} (e_I, e_J)_G = \delta_{I,J}.$$

i.e. les χ_I, $I \in \widehat{K[G]}$ forment une base orthonormale de $(Z(K[G]), (-,-)_G)$. En d'autres termes

Lemme 3.2.8 (Orthogonalité des lignes) *Pour tout $\chi, \chi' \in \widehat{G}$ on a*

$$(\chi, \chi')_G = \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'(g^{-1}) = \delta_{\chi,\chi'}.$$

Corollaire 3.2.9 *Pour tout $K[G]$-module V, en décomposant*

$$V = \bigoplus_{I) \in \widehat{K[G]}} I^{\oplus n_V(I)}$$

en somme directe de représentations simples, on a $(\chi_I, \chi_V)_G = n_V(I)$. En particulier, V est irréductible si et seulement si $(\chi_V, \chi_V)_G = 1$.

Exercice 3.2.10 *Soit G un groupe fini et V un $\mathbb{C}[G]$-module fidèle.*

1. *Montrer que pour tout $g \in G$ on a $\chi_V(g) = \chi_V(1)$ si et seulement si $g = 1$;*
2. *Soit $I \in \widehat{\mathbb{C}[G]}$, montrer que la série formelle*
$$\sum_{n \geq 0} (\chi_I, \chi_V^n)_G X^n$$
est un élément de $\mathbb{C}(X) \setminus \mathbb{C}[X]$;
3. *En déduire que I apparait dans une infinité de puissances tensorielles de V.*

Exercice 3.2.11 (Représentations simples d'un produit) *Soit G et G' deux groupes finis.*

1. *Etant donnés un $K[G]$-module V et un $K[G']$-module V', calculer $\chi_{V\otimes V'}$.*
2. *Etant donnés des $K[G]$-module V_i et des $K[G']$-module V_i', $i=1,2$ calculer $(\chi_{V_1\otimes V_1'},\chi_{V_2\otimes V_2'})_{G\times G'}$.*
3. *En déduire que $V\in\widehat{K[G]}$ et $V'\in\widehat{K[G']}$ si et seulement si $V\otimes V'\in\widehat{K[G\times G']}$ et que que pour tout $W\in\widehat{K[G\times G']}$ il existe $V\in\widehat{K[G]}$ et $V'\in\widehat{K[G']}$ tels que $W\simeq V\otimes V'$.*

Corollaire 3.2.12 (Orthogonalité des colonnes) *Pour tout $C,C'\in Cl(G)$, on a*

$$\sum_{\chi\in\widehat{G}}\chi(C)\chi(C'^{-1})=\frac{|G|}{|C|}\delta_{C,C'}.$$

Preuve. Notons $n:=|Cl(G)|$, $\chi_1,\dots,\chi_n$ les caractères simples de G, $C_1,\dots,C_n$ les classes de conjugaison de G et introduisons les matrices

$$\mathcal{X}=(\chi_i(C_j))_{1\le i,j\le n}\,,\ \mathcal{X}^\vee=\left(\chi_i(C_j^{-1})\right)_{1\le i,j\le n}\ \text{ et }\ \Delta=(\delta_{i,j}|C_i|))_{1\le i,j\le n}\,.$$

On vérifie immédiatement que

$$\mathcal{X}\Delta{}^t\mathcal{X}^\vee=|G|\,((\chi_i,\chi_j)_G)_{1\le i,j\le n}=|G|I_n.$$

En particulier $\Delta{}^t\mathcal{X}^\vee=|G|\mathcal{X}^{-1}$ commute avec $\mathcal{X}$. D'où

$$|G|Id_n=\mathcal{X}\Delta{}^t\mathcal{X}^\vee=\Delta{}^t\mathcal{X}^\vee\mathcal{X}=(|C_j|\sum_{1\le k\le n}\chi_k(C_i)\chi_k(C_j^{-1}))_{1\le i,j\le n}.\ \square$$

Exercice 3.2.13 *Supposons $K=\mathbb{C}$. Que vaut $\det(\mathcal{X})^2$?*

Exercice 3.2.14 (Représentations de permutation) *Soit G un groupe fini opérant non trivialement sur un ensemble fini X. On considère le K-espace vectoriel $V_X=\oplus_{x\in X}Kx$ qu'on munit de la structure de $K[G]$-module définie par l'action de G sur X.*

1. *En calculant de deux façons diffŕentes le nombre de couples $(g,x)\in G\times X$ tels que $gx=x$ montrer que*

$$|X/G|=\frac{1}{|G|}\sum_g|X^g|,$$

   où on note X^g l'ensemble des élémmens de X fixés par g.
2. *Montrer que la multiplicité de $\mathbb{I}$ dans V est $|X/G|$.*
3. *Soit $V_{X,0}$ le noyau du morphisme d'augmentation $V_X\to K$, $\sum_{x\in X}a_xx\to\sum_{x\in X}a_x$. On fait agir G sur $X\times X$ diagonalement. Si on note $\Delta_X\subset X\times X$ la diagonale, on observe que l'action de G sur $X\times X$ stabilise Δ_X (donc $X\times X\setminus\Delta_X$). Montrer que les conditions suivantes sont équivalentes :*
   (a) $V_{X,0}\in\widehat{K[G]}$;
   (b) $|X\times X/G|=2$;
   (c) $|X/G|=1$ et G opère doublement transitivement sur $X\times X$ i.e. transitivement sur $X\times X\setminus\Delta_X$.
4. *Déduire de ce qui précède que $\mathcal{S}_n$ possède toujours une représentation irréductible de K-dimension $n-1$.*

Exercice 3.2.15 (Quelques table des caractères) *Montrer qu'un groupe fini G est abélien si et seulement si les $K[G]$-modules simples sont de K-dimension 1. Calculer les tables des caractères lorsque G est*

1. *cyclique d'ordre n ;*
2. *le groupe alterné $\mathcal{A}_4$;*
3. *le groupe symétrique $\mathcal{S}_4$.*

Exercice 3.2.16 (Table des caractères des groupes non abéliens d'ordre 8) *Il y a deux classes d'isomorphismes de groupes non abéliens d'ordre 8, le groupe diédral D_8 et le groupe des quaternions $\mathbb{H}_8$. On va cependant voir que ces deux groupes ont la même table des caractères, ce qui montre que, si la table des caractères contient beaucoup d'information sur le groupe G, elle ne suffit pas à en caractériser la classe d'isomorphisme. Soit donc G un groupe non abélien d'ordre 8.*

1. *Montrer que $Z(G)=\mathbb{Z}/2$ et que $G/Z(G)=\mathbb{Z}/2\times\mathbb{Z}/2$.*

2. *En déduire que* $|\widehat{G}| = 5$. *Décrire toutes les représentations de degré* 1 *de* G.
3. *En déduire la table des caractères complète de* G

Remarque 3.2.17 Lorsque que $K = \mathbb{C}$, on a (exercice) pour tout $V \in \mathrm{Mod}_{\mathbb{C}}(\mathbb{C}[G])$ et pour tout $g \in G$

$$\chi_V(g^{-1}) = \overline{\chi_V(g)}.$$

Munissons $\mathbb{C}[G]$ de la forme bilinéaire symétrique

$$\begin{array}{rccc} \langle -,- \rangle_G : & \mathbb{C}[G] \otimes_{\mathbb{C}} \mathbb{C}[G] & \to & \mathbb{C} \\ & (\underline{a}, \underline{b}) & \to & \dfrac{1}{|G|} \displaystyle\sum_{g \in G} a(g)\overline{b(g)}. \end{array}$$

Notons que $\langle -,- \rangle_G$ et $(-,-)_G$ coincident sur $\mathbb{R}[\chi, \chi \in \widehat{G}] \subset \mathbb{C}[G]$. On vérifie immédiatement que $\langle -,- \rangle_G$ est un produit scalaire hermitien sur $\mathbb{C}[G]$ et le lemme 3.2.8 peut se reformuler en disant que les éléments de $\widehat{G}$ forment une $\mathbb{C}$-base orthonormale de $(Z(\mathbb{C}[G]), \langle -,- \rangle_G)$.

3.2.3 Une application à la théorie des groupes finis : le théorème de Burnside

Le théorème de Feit-Thompson - l'un des grands théorème de la théorie des groupes finis - affirme que tout groupe fini d'ordre impair est résoluble. Nous nous proposons ici d'en montrer un cas particulier, le théorème de Burnisde, dont la preuve repose sur des propriétés élémentaires d'intégralité des caractères.

Théorème 3.2.18 (Burnside) *Soit* p *et* q *des nombres premiers. Alors tout groupe d'ordre* $p^a q^b$ *est résoluble.*

Remarque 3.2.19 Comme le groupe $\mathcal{A}_5$ n'est pas résoluble, on voit que le théorème de Burnside est optimal.

3.2.3.1 Propriétés d'intégralité des caractères

Lemme 3.2.20 *Soit* R *un anneau commutatif et* $A \subset R$ *un sous-anneau. Pour tout* $x \in R$, *les propriétés suivantes sont équivalentes.*

1. *Il existe* $P_x \in A[T]$ *unitaire tel que* $P_x(x) = 0$;
2. $A[x]$ *est un* A*-module de type fini ;*
3. *Il existe un sous-anneau* $A[x] \subset B_x \subset R$ *qui est un* A*-module de type fini.*

Preuve. (1) $\Rightarrow$ (2) : utiliser la division euclidienne par P_x. (2) $\Rightarrow$ (3) : immédiat. (3) $\Rightarrow$ (1) : Soit $b_1, \ldots, b_n$ un système de générateur de B_x comme A-module. Comme B_x est un anneau, on a $xb_i \in B_x$, $i = 1, \ldots, n$ donc il existe $a_{i,1}, \ldots, a_{i,n} \in A$ tels que

$$xb_i = \sum_{1 \leq j \leq n} a_{i,j} b_j.$$

Notons $X := (a_{i,j})_{1 \leq i,j \leq n} \in M_n(A) \subset M_n(R)$ et $\underline{b} = (b_i)_{1 \leq i \leq n} \in R^n$. On a

$$(xId - X)\underline{b} = 0$$

donc

$${}^tCom(xId - X)(xId - X)\underline{b} = det(xId - X)\underline{b} = 0$$

Comme $1 \in B_x$, cela implique $det(xId - X) = 0$ donc $P_x = det(TId - X) \in A[T]$ convient. □

Les éléments $x \in R$ vérifiant les propriétés équivalentes du lemme 3.2.20 sont dit *entiers sur* A. L'ensembles des éléments de R entiers sur A est un sous-anneau de R. Lorsque $A = \mathbb{Z}$ et $R = \mathbb{C}$, on parle d'*entiers algébriques*. On vérifie facilement que si $x \in \mathbb{Q}$ est un entier algébrique alors $x \in \mathbb{Z}$.

On rappelle que si V est un $K[G]$-module, on note $\theta_V : G \to \mathrm{GL}(V)$ le morphisme de groupes sous-jacent.

Lemme 3.2.21 *Soit G un groupe fini, $V \in \widehat{\mathbb{C}[G]}$ et $\underline{a} \in Z(\mathbb{C}[G])$ tel que $a(g)$ soit un entier algébrique, $g \in G$. Alors*

$$\frac{1}{n_V}\sum_{g\in G} a(g)\chi_V(g)$$

est aussi un entier algébrique.

Preuve. Commençons par observer que pour tout $\mathbb{C}[G]$-module V, les $\chi_V(g)$, $g \in G$ sont des entiers algébriques. Notons $N := |G|$. Pour tout $g \in G$ on a $\theta_V(g)^N - Id = 0$ donc les valeurs propres de $\theta_V(g)$ sont des entiers algébriques. L'assertion résulte donc du fait que l'ensemble des entiers algébriques est stable par addition et que $\chi_V(g)$ est la somme des valeurs propres de $\theta_V(g)$ (comptées avec multiplicité).
Comme l'ensemble des entiers algébriques est un anneau, il suffit de considérer le cas où $a = g(C)$ pour $C \in Cl(G)$. On a

$$\frac{1}{n_V}\sum_{g\in G} g(C)(g)\chi_V(g) = \frac{1}{n_V}\sum_{g\in C}\chi_V(g) = \frac{|C|\chi_V(C)}{n_V}.$$

Pour tout $a \in Z(\mathbb{C}[G])$, comme a est invariant sur les classes de conjugaison de G, on vérifie que l'élément

$$\sum_{g\in G} a(g)\theta_V(g)$$

commute avec les $\theta_V(g_0)$, $g_0 \in G$ donc, par le lemme de Schur, est une homothétie de rapport disons $\lambda_V(\underline{a})$. En outre, l'application $\lambda_V : Z(\mathbb{C}[G]) \to \mathbb{C}$ est un morphisme d'anneaux donc $\lambda_V(Z(\mathbb{Z}[G])) \subset \mathbb{C}$ est un sous-anneau, contenant $\mathbb{Z}$ et qui est de type fini comme $\mathbb{Z}$-module (engendré par les $g(C)$, $C \in Cl(G)$). Par le lemme 3.2.20, l'anneau $\lambda(Z(\mathbb{Z}[G]))$ est en fait un sous-anneau de l'anneau des entiers algébriques. On conclut en observant que $\frac{|C|\chi_V(g)}{n_V} = \lambda_V(g(C))$. □

Corollaire 3.2.22 *Pour tout $V \in \widehat{\mathbb{C}[G]}$ l'entier $n_V := \dim_{\mathbb{C}}(V)$ divise $|G|$.*

Preuve. En effet, comme $\chi_V^\vee \in Z(\mathbb{C}[G])$, par le lemme 3.2.21,

$$\frac{1}{n_V}\sum_{g\in G}\chi_V(g^{-1})\chi_V(g)$$

est un entier algébrique. Mais comme $\frac{1}{n_V}\sum_{g\in G}\chi_V(g^{-1})\chi_V(g) = \frac{|G|}{n_V}||\chi_V||^2 = \frac{|G|}{n_V}$ est aussi dans $\mathbb{Q}$, on a $\frac{|G|}{n_V} \in \mathbb{Z}$. □

Exercice 3.2.23 *Déterminer le nombre et les dimensions des représentations irréductibles des groupes non abéliens d'ordre pq (p, q premiers).*

Corollaire 3.2.24 *Pour tout $V \in \widehat{\mathbb{C}[G]}$ et $C \in Cl(G)$. Si n_V et $|C|$ sont premiers entre eux alors $\frac{\chi_V(C)}{n_V}$ est un entier algébrique. Si de plus $\chi_V(C) \neq 0$ alors $\theta_V(g)$ est une homothétie, $g \in C$.*

Preuve. Pour la première assertion, par bézout il existe $a, b \in \mathbb{Z}$ tels que $an_V + b|C| = 1$ donc

$$\frac{\chi_V(C)}{n_V} = a\chi_V(C) + b\frac{|C|\chi_V(C)}{n_V}$$

est un entier algébrique par le lemme 3.2.21. Pour la seconde assertion, les valeurs propres $\zeta_1, \dots \zeta_{n_V}$ de g agissant sur V sont des racines de l'unité et

$$\frac{\chi_V(C)}{n_V} = \frac{\zeta_1 + \cdots + \zeta_{n_V}}{n_V}$$

est un entier algébrique. La conclusion résulte donc du lemme 3.2.25 ci-dessous. □

Lemme 3.2.25 *Soit $\zeta_1, \dots \zeta_n \in \mathbb{C}$ des racines de l'unité. Si*

$$\frac{\zeta_1 + \cdots + \zeta_n}{n}$$

est un entier algébrique alors soit $\zeta_1 + \cdots + \zeta_n = 0$ soit $\zeta_1 = \ldots = \zeta_n$.

Preuve. Notons $z := \frac{\zeta_1+\cdots+\zeta_n}{n}$. Pour tout $\sigma \in \Gamma_{\mathbb{Q}}$ et $1 \leq i \leq n$, $\sigma(\zeta_i)$ est encore une racine de l'unité. Donc $|\sigma(z)| \leq 1$. En outre, comme z est un entier algébrique, pour tout $\sigma \in \Gamma_{\mathbb{Q}}$ $\sigma(z)$ est aussi un entier algébrique. Notons Z le produit des conjugués de z sur $\mathbb{Q}$. Alors Z un entier algébrique comme produit d'entiers algébriques et $Z \in \mathbb{Q}$ puisqu'au signe près, c'est le terme constant du polynôme minimal de z sur $\mathbb{Q}$. Donc $Z \in \mathbb{Z}$. Mais $|Z| \leq 1$. Donc soit $Z = 0$ (auquel cas $z = 0$) soit $|Z| = 1$, auquel cas $|z| = 1$, ce qui implique $\zeta_1 = \ldots = \zeta_n$. □

3.2.3.2 Preuve du théorème de Burnside

On est maintenant en mesure de prouver le théorème 3.2.18.

On peut supposer $a, b > 0$ (puisque, sinon, G est nilpotent). On procède par récurrence sur $|G|$. Ce qui va permettre la récurrence est le lemme suivant.

Lemme 3.2.26 *Soit G un groupe fini et $e_G \neq g \in G$. Notons C_g la classe de conjugaison de g et supposons qu'il existe une nombre premier p tel que $|C_g|$ soit une puissance de p. Alors il existe un sous groupe $N \lhd G$, $N \subsetneq G$ tel que $p_N(g) \in Z(G/N)$.*

Preuve du Théorème 3.2.18. On a

$$p^a q^b = |G| = 1 + \sum_{C \in Cl(G) \setminus \{e_G\}} |C|$$

donc il existe $C \in Cl(G) \setminus \{e_G\}$ telle que $q \not| |C|$. Soit $g \in C$. On a $|C||\mathrm{Stab}_G(g)| = |G|$ donc $|C|$ divise $|G|$. Cela montre que $|C|$ est une puissance de p. Mais alors, d'après le lemme 3.2.26, il existe un sous groupe $N \lhd G$, $N \subsetneq G$ tel que $p_N(g) \in Z(G/N)$. Si $N \neq 1$, l'hypothèse de recurrence montre que N et G/N sont résolubles donc G aussi. Si $N = 1$, on a $e_G \neq g \in Z(G)$ et soit $G = Z(G)$, auquel cas G est évidemment résoluble, soit $Z(G) \subsetneq G$ et l'hypothèse de recurrence montre que $G/Z(G)$ est résoluble donc G aussi. □

Preuve du lemme 3.2.26. d'après l'orthogonalité selon les colonnes on a

$$1 + \sum_{V \in \widehat{\mathbb{C}[G]} \setminus \mathbb{I}} n_V \chi_V(g) = 0$$

donc

$$\sum_{V \in \widehat{\mathbb{C}[G]} \setminus \mathbb{I}} \frac{n_V \chi_V(g)}{p} = -\frac{1}{p},$$

qui n'est pas un entier algébrique. Il existe donc $V \in \widehat{\mathbb{C}[G]} \setminus \mathbb{I}$ tel que $\frac{n_V \chi_V(g)}{p}$ ne soit pas un entier algébrique. En particulier, $\chi_V(g) \neq 0$ et $p \not| n_V$. D'après le corollaire 3.2.24, $\theta_V(g)$ est donc une homothétie. Si l'on note $N_V := \ker(\theta_V) \lhd G$, on a bien $N_V \subsetneq G$ puisque $V \neq \mathbb{I}$. De plus $\theta_V : G \to \mathrm{GL}(V)$ se factorise en $\overline{\theta}_V : G/N_V \hookrightarrow \mathrm{GL}(V)$. Comme $\overline{\theta}_V(p_{N_V}(g))$ est une homothétie donc dans le centre de $\mathrm{GL}(V)$, on a *a fortiori* $p_{N_V}(g) \in Z(G/N_V)$. □

3.3 $K[G]$-modules induits

3.3.1 Foncteurs de restriction et d'induction

Soit G un groupe fini et $H \subset G$ un sous-groupe. On a alors une inclusion canonique de K-algèbres

$$K[H] \hookrightarrow K[G].$$

On munit $K[G]$ de la structure de $K[H]$-module à droite induite par la multiplication à droite ; pour cette structure, $K[G]$ est un $K[H]$-module à droite libre de rang $[G : H]$. On dispose alors du foncteur de restriction canonique

$$\begin{array}{rccc} |_{K[H]} =: \mathrm{Res}^H_G : & \mathrm{Mod}_{/K[G]} & \to & \mathrm{Mod}_{/K[H]} \\ & (V, \theta) & \to & (V, \theta|_{K[H]}) \end{array}$$

et de son adjoint à gauche, le foncteur d'induction

$$\begin{array}{rccc} K[G] \otimes_{K[H]} - =: \mathrm{Ind}^G_H : & \mathrm{Mod}_{/K[H]} & \to & \mathrm{Mod}_{/K[G]} \\ & w & \to & K[G] \otimes_{K[H]} W. \end{array}$$

Rappelons en particulier 1.2.17 que pour tout $K[G]$-module V et $K[H]$-module W on a un isomorphisme de K-modules canonique

$$\mathrm{Hom}_{K[H]}(W, \mathrm{Res}^H_G(V)) \tilde{\to} \mathrm{Hom}_{K[G]}(\mathrm{Ind}^G_H(W), V), \tag{3.1}$$

qui envoie un morphisme de $K[H]$-modules $\phi : W \to \mathrm{Res}^H_G(V)$ sur le morphisme de $K[G]$-modules $Id \otimes \phi : \mathrm{Ind}^G_H(W) \to V$.

Et que 1.2.18,

1. Pour tout tous sous-groupe $H \subset G$ et $K[H]$-modules $V_1, \ldots, V_r$ on a $\mathrm{Ind}^G_H(\oplus_{1\leq i\leq r} V_i) = \oplus_{1\leq i\leq r} \mathrm{Ind}^G_H(V_i)$.
2. Pour tout système de représentants $g_1, \ldots, g_{[G:H]}$ de G/H, la décomposition $K[G] = \oplus_{1\leq i\leq r} g_i K[H]$ comme $K[H]$-module à droite induit un isomorphisme de K-modules $\mathrm{Ind}^G_H(V) = \oplus_{1\leq i\leq r} \mathrm{Ind}^G_H(g_i \otimes V)$.
3. Pour tous sous-groupes $L \subset H \subset G$ on a
$$\mathrm{Ind}^G_L \simeq \mathrm{Ind}^G_H \circ \mathrm{Ind}^H_L.$$

Soit maintenant V un $K[G]$-module et W un sous-$K[H]$-module de $\mathrm{Res}^H_G(V)$. On dit que V est induit par W si le morphisme canonique $K[G] \otimes_{K[H]} W \to V$ est un isomorphisme ou, de façon équivalente, que pour tout système de représentants $g_1, \ldots, g_{[G:H]}$ de G/H, on a

$$V = \bigoplus_{1\leq i\leq [G:H]} g_i W.$$

Si $V \in \widehat{K[G]}$, cela équivaut aussi à

$$\dim_K(V) = [G : H] \dim_K(W).$$

Exercice 3.3.1 (Sous-groupes abéliens et dimension des $K[G]$-modules simples) *On rapelle (cf. Exercice 3.2.15) qu'un groupe fini G est abélien si et seulement si toute les représentations simples de $K[G]$ sont de K-dimension 1. En déduire que si G est un groupe fini, tout $K[G]$-module simple est de K-dimension inférieure ou égale au minimum des $[G : A]$ lorsque A décrit l'ensemble des sous-groupe abélien de G.*
Remarque : La borne

$$\inf\{[G : A] \mid A \subset G \text{ abélien}\}$$

n'est pas atteinte en général (cf. par exemple $\mathcal{S}_4$). En fait, on peut prouver que tout $K[G]$-module simple est de K-dimension divisant $[G : N]$, où N décrit l'ensemble des sous-groupes abéliens normaux de G.

Exercice 3.3.2 (Groupe des transformations affines de la droite) *Soit $\mathbb{F}_q$ un corps fini de caractéristique p et soit G le groupe des transformations affines de la droite sur $\mathbb{F}_q$ i.e. des applications $\mathbb{F}_q \to \mathbb{F}_q$, $x \to ax + b$, $a \in \mathbb{F}_q^\times$, $b \in \mathbb{F}_q$, que l'on peut aussi voir comme le sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$ des matrices de la forme*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q.$$

1. *Montrer que G contient un sous-groupe normal N isomorphe à $\mathbb{F}_q$. Quelle est la structure de G ?*
2. *Soit $\chi \in \widehat{K[N]}$, $\chi \neq \mathbb{I}$. Montrer que $Ind^G_N(\chi)$ ne dépend pas de χ et est un $K[G]$-module simple.*
3. *Construire la table des caractères de G.*

Exercice 3.3.3 (Table des caractères du groupe dihédral) *Construire la table des caractères du groupe dihédral d'ordre $2n$ (on distinguera les cas n pair et n impair).*

3.3.2 Restriction des représentations induites

Observons d'abord qu'on peut décrire explicitement $\mathrm{Ind}^G_H(W)$ comme suit. On se fixe un système $g_1, \ldots, g_{[G:H]}$ de représentants de G/H alors, on a

$$K[G] \otimes_{K[H]} W = \bigoplus_{1\leq i\leq [G:H]} K g_i \otimes W$$

Pour tout $g \in G$ et $1 \leq i \leq [G : H]$, il existe un unique $1 \leq i(g, i) \leq [G : H]$ tel que $g g_i H = g_{i(g,i)} H$. Posons $h(g, i) := g^{-1}_{i(g,i)} g g_i \in H$. On a alors

$$g \cdot (g_i \otimes w) = g_{i(g,i)} h(g, i) \otimes w = g_{i(g,i)} \otimes h(g, i) \cdot w.$$

On se fixe maintenant deux sous-groupes $H, L \subset G$ et un $K[H]$-module (W, τ). On cherche à décrire

$$\mathrm{Res}_G^L \mathrm{Ind}_H^G(W).$$

Pour cela, à tout $g \in G$, on associe le $K[L \cap gHg^{-1}]$-module $W^g := (W, \tau^g)$ défini par

$$\tau^g(h) = \tau(g^{-1}hg),\ h \in L \cap gHg^{-1}.$$

On peut interpréter $L \setminus G/H$ comme le quotient $L \setminus (G/H)$, où L agit par translation à gauche sur G/H. Pour tout $g \in G$ et $l \in L$, on a $lgH = gH$ si et seulement si $l \in L \cap gHg^{-1}$. On peut donc écrire

$$G/H = \bigsqcup_{\overline{g} \in L\setminus G/H} \bigsqcup_{\overline{l} \in L/L\cap gHg^{-1}} \{lgH\}.$$

Autrement dit, si on se fixe un système de représentants $g_1, \ldots, g_{|L\setminus G/H|}$ de $L\setminus G/H$ et, pour chaque $i = 1, \ldots, |L\setminus G/H|$ un système de représentants $l_{i,1}, \ldots, l_{i,[L:L\cap g_i H g_i^{-1}]}$ de $L/L \cap g_i H g_i^{-1}$, on obtient un système de représentants $l_{i,j}g_i$ de G/H. Avec ces notations, décomposons

$$\mathrm{Ind}_H^G(W) = \bigoplus_{1\le i\le |L\setminus G/H|} \bigoplus_{1\le j\le [L:L\cap g_i H g_i^{-1}]} K l_{i,j} g_i \otimes W.$$

Calculons l'action de $l \in L$ sur un élément de la forme $l_{i,j}g_i \otimes w$. Il existe un unique $1 \le j(l;i,j) \le [L/L \cap g_i H g_i^{-1}]$ tel que

$$l l_{i,j} L \cap g_i H g_i^{-1} = l_{i,j(l;i,j)} L \cap g_i H g_i^{-1}.$$

Notons

$$l(l;i,j) := l_{i,j(l;i,j)}^{-1} l l_{i,j} \in L \cap g_i H g_i^{-1}.$$

Comme $g_i^{-1} l(l;i,j) g_i \in H$, on obtient

$$l \cdot (l_{i,j}g_i \otimes w) = l_{i,j(l;i,j)} g_i g_i^{-1} l(l;i,j) g_i \otimes w = l_{i,j(l;i,j)} g_i \otimes \tau^{g_i}(l(l;i,j))w.$$

Cela montre que chaque

$$W_i := \bigoplus_{1\le j\le [L:L\cap g_i H g_i^{-1}]} K l_{i,j} g_i \otimes W$$

est L-stable et isomorphe, comme $K[L]$-module à $\mathrm{Ind}_{L\cap g_i H g_i^{-1}}^L (W, \tau^{g_i})$. Autrement dit, on a une décomposition canonique

$$\mathrm{Res}_G^L \mathrm{Ind}_H^G (W, \tau) = \bigoplus_{\overline{g} \in L\setminus G/H} \mathrm{Ind}_{L\cap gHg^{-1}}^L (W, \tau^g). \tag{3.2}$$

3.3.3 Caractère d'une représentation induite et critère d'irréductibilité de Mackey

En conservant les notations du paragraphe 3.3.1, on dispose également de morphismes de K-espaces vectoriels canoniques

$$\mathrm{Res}_G^H : K[G] \to K[H]$$

et

$$\mathrm{Ind}_H^G : K[H] \to K[G]$$

définis comme suit. Pour tout $a \in K[G]$,

$$\mathrm{Res}_G^H(a) = \sum_{h\in H} a(h)h$$

et, pour tout $a \in K[H]$,

$$\mathrm{Ind}_H^G(a) = \sum_{g\in G} \left(\frac{1}{|H|} \sum_{g' \in G \mid g'^{-1}gg' \in H} a(g'^{-1}gg') \right) g.$$

On peut restreindre ces

Lemme 3.3.4 *Avec les notations ci-dessus, pour tout $K[G]$-module (V,ρ)*

$$\chi_{\mathrm{Res}^H_G(V)} = \mathrm{Res}^H_G(\chi_V)$$

et pour tout $K[H]$-module (W,τ),

$$\chi_{\mathrm{Ind}^G_H(W)} = \mathrm{Ind}^G_H(\chi_W).$$

Preuve. La première partie de l'assertion est immédiate. Reprenons les notations du début du paragraphe 3.3.2. Fixons également une K-base $w_1,\dots,w_r$ de W, les $g_i\otimes w_j$, $1\le i\le [G:H]$, $1\le j\le r$ forment une K-base de $K[G]\otimes_{K[H]} W$. Avec ces notations, l'action de g sur $g_i\otimes w_j$ est donnée explicitement par

$$g\cdot(g_i\otimes w_j) = g_{i(g,i)}\otimes(h(g,i)w_j).$$

En particulier, seuls les $1\le i\le [G:H]$ tels que $i=i(g,i)$ *i.e.* $g_i^{-1}gg_i\in H$ interviennent dans le calcul de la trace. Et on a alors

$$\chi_{\mathrm{Ind}^G_H(W)}(g)) = \sum_{1\le i\le [G:H]\ |\ g_i^{-1}gg_i\in H} Tr_W(\tau(g_i^{-1}gg_i)) = \frac{1}{|H|}\sum_{g'\in G\ |\ g'^{-1}gg'\in H} Tr(\tau(g'^{-1}gg')).\ \square$$

Remarque 3.3.5 Comme les caractères forment une K-base de $Z(K[G])$, le Lemme 3.3.4 montre en particulier que les morphismes de K-espaces vectoriels $\mathrm{Res}^H_G : K[G]\to K[H]$ et $\mathrm{Ind}^G_H : K[H]\to K[G]$ se restreignent en des morphismes de K-espaces vectoriels $\mathrm{Res}^H_G : Z(K[G])\to Z(K[H])$ et $\mathrm{Ind}^G_H : Z(K[H])\to Z(K[G])$. On notera que comme pour tout $\chi,\chi'\in\widehat{G}$, $\chi\chi'\in\widehat{G}$ (Exercice 3.2.3) et que $\widehat{G}$ est une K-base de $Z(K[G])$, $Z(K[G])\subset K^G$ est un sous-k-algèbre (on a donc deux structures différentes de k-algèbre commutative sur $Z(K[G])$, celle induite par le produit de convolution de $K[G]$ et celle induite par le produit composante par composante de K^G). Avec la structure de sous-anneau de K^G, $\mathrm{Res}^H_G : Z(K[G])\to Z(K[H])$ est un morphisme de k-algèbres.

Lemme 3.3.6 *Pour tout $K[G]$-module V, on a*

$$\dim_K(V^G) = (\chi_V,\tilde{1})_G$$

En particulier, pour tout $K[G]$-modules V, V', on a

$$\dim_K(\mathrm{Hom}_{K[G]}(V,V')) = (\chi_V,\chi_{V'})_G.$$

Preuve. La K-dimension de V^G est la multiplicité de la représentation triviale $\mathbb{I}$ dans V. Or, le caractère de $\mathbb{I}$ est la fonction constante $\tilde{1}$. La première partie de l'énoncé résulte donc du corollaire 3.2.9.
La deuxième partie de l'énoncé découle de la première en observant que

$$\mathrm{Hom}_{K[G]}(V,V') = \mathrm{Hom}_K(V,V')^G = (V^\vee\otimes_K V')^G$$

et que

$$\chi_{V^\vee\otimes V'} = \chi_V^\vee\cdot\chi_{V'}.\ \square$$

Lemme 3.3.7 (Réciprocité de Frobenius) *Pour tout $\phi\in Z(K[G])$ and $\psi\in Z(K[H])$ on a*

$$(\psi,\mathrm{Res}^H_G(\phi))_H = (\mathrm{Ind}^G_H(\psi),\phi)_G.$$

Preuve. Comme les caractères des $K[G]$- (resp. de $K[H]$-)modules simples forment une K-base de $Z(K[G])$ (resp. de $Z(K[H])$), par K-linéarité il suffit de traiter le cas où $\phi=\chi_V$ et $\psi=\chi_W$ pour $V\in\widehat{K[G]}$, $W\in\widehat{K[H]}$. Or, dans ce cas, on a

$$(\chi_W,\mathrm{Res}^H_G(\chi_V))_H = \dim_K(\mathrm{Hom}_{K[H]}(W,\mathrm{Res}^H_G(V)))$$

et

$$(\mathrm{Ind}^G_H(\chi_W),\chi_V)_G = \dim_K(\mathrm{Hom}_{K[G]}(\mathrm{Ind}^G_H(W),V)).$$

La conclusion résulte donc de l'isomorphisme de K-espaces vectoriels (3.1). $\square$

Le critère d'irréductibilité ci-dessous ne fait intervenir que les représentations W^g des sous-groupes $H\cap gHg^{-1}\subset H$, $g\in G$ de H d'où son intérêt en pratique.

Proposition 3.3.8 (Critère d'irréductibilité de Mackey) *Pour tout $K[H]$-module (W,τ), on a $\mathrm{Ind}_H^G(W) \in \widehat{K[G]}$ si et seulement si*

1. *$W \in \widehat{K[H]}$;*
2. *Pour tout $g \in G \setminus H$, les représentations $\mathrm{Res}_H^{H\cap gHg^{-1}}(W)$, W^g sont disjointes i.e.*

$$(\chi_{\mathrm{Res}_H^{H\cap gHg^{-1}}(W)}, \chi_{W^g})_{H\cap gHg^{-1}} = 0.$$

Preuve. On sait que $\mathrm{Ind}_H^G(W) \in \widehat{K[G]}$ si et seulement si

$$(\chi_{\mathrm{Ind}_H^G(W)}, \chi_{\mathrm{Ind}_H^G(W)})_G = 1.$$

Mais d'après le lemme 3.3.7 et (3.2), on a

$$(\chi_{\mathrm{Ind}_H^G(W)}, \chi_{\mathrm{Ind}_H^G(W)})_G = (\mathrm{Ind}_H^G(\chi_W), \chi_{\mathrm{Ind}_H^G(W)})_G = (\chi_W, \mathrm{Res}_G^H \chi_{\mathrm{Ind}_H^G(W)})_H = (\chi_W, \chi_{\mathrm{Res}_G^H \mathrm{Ind}_H^G(W)})_H$$

Donc

$$(\chi_{\mathrm{Ind}_H^G(W)}, \chi_{\mathrm{Ind}_H^G(W)})_G = \sum_{\overline{g}\in H\backslash G/H} (\chi_W, \chi_{\mathrm{Ind}_{H\cap gHg^{-1}}^H(\tau^g)})_H.$$

Or pour $g = 1$ on a $(\chi_W, \chi_{\mathrm{Ind}_{H\cap gHg^{-1}}^H(\tau^g)})_H \geq 1$ et pour g quelconque on a toujours $(\chi_W, \chi_{\mathrm{Ind}_{H\cap gHg^{-1}}^H(\tau^g)})_H \geq 0$. On en déduit que $(\chi_{\mathrm{Ind}_H^G(W)}, \chi_{\mathrm{Ind}_H^G(W)})_G = 1$ si et seulement si $(\chi_W, \chi_W)_H = 1$ et $(\chi_W, \chi_{\mathrm{Ind}_{H\cap gHg^{-1}}^H(W^g)})_H = 0$ pour $g \in G \setminus H$. □

Remarque 3.3.9 Si H est distingué dans G, (2) devient simplement : pour tout $g \in G \setminus H$, $(W, W^g)_H = 0$.

Exercice 3.3.10 *Soit G un groupe fini et X un ensemble de sous-groupes de G stable par conjugaison. On note $R(G)$ la K-algèbre $Z(K[G])$ munie de la structure d'anneau induite par celle de K^G.*

1. *Montrer que l'image de $\oplus_{H\in X}\mathrm{Ind}_H^G : \oplus_{H\in X} R(H) \to R(G)$ est un idéal de $R(G)$.*
2. *Montrer que les propriétés suivantes sont équivalentes.*
   (i) G est la réunion de ses sous-groupes H, $H \in X$;
   (ii) Tout caractère de G est combinaison linéaire à coefficients dans $\mathbb{Q}$ des caractères induits $\mathrm{Ind}_H^G(\chi)$, $\chi \in \widehat{H}$, $H \in X$.
3. *En déduire que tout caractère de G est combinaison linéaire à coefficients dans $\mathbb{Q}$ des caractères induits de ses sous-groupes cycliques.*

Exercice 3.3.11 (p-groupes) *Soit p un nombre premier et G un groupe fini d'ordre p^t.*

1. *Rappeler pourquoi le centre $Z(G)$ de G est toujours nontrivial. Si on suppose G non abélien, montrer qu'il existe un sous-groupe abélien A, normal dans G, différent de G et contenant strictement $Z(G)$.*
2. *On suppose toujours que G est non abélien. Soit V un $K[G]$-module simple de K-dimension ≥ 2. Par semisimplicité, on peut décomposer $V|_A$ an somme directe de $K[A]$-modules simples*

$$V|_A = \bigoplus_{i=1}^{r} W_i^{\oplus m_i}$$

   (où W_i est un $K[A]$-module simple, $i = 1,\ldots,r$ et W_i, W_j sont non-isomorphes pour $1 \leq i \neq j \leq r$). Montrer que $r \geq 2$ et qu'il existe un sous-groupe $Z(G) \subsetneq H \subsetneq G$ et un $K[H]$-module simple $W \subset V$ tel que $V = K[G]\otimes_{K[H]} W$. On pourra d'abord traiter le cas où V est fidèle (i.e. $G \hookrightarrow \mathrm{GL}(V)$) puis s'y ramener.
3. *Déduire de ce qui précède que tout $K[G]$-module simple est de la forme $K[G]\otimes_{K[H]} W$ avec $H \subsetneq G$ un sous-groupe strict et $W \subset V$ un $K[H]$-module simple de K-dimension 1.*

Exercice 3.3.12 (Représentations simples des produit semidirect par un groupe abélien) *Soit G un groupe fini qui s'écrit comme produit semidirect $G = A \rtimes H$ avec A abélien. Comme A est normal dans G, G agit sur $\widehat{A}$ par la formule*

$$\begin{array}{lll} G \times \widehat{A} & \to & \widehat{A} \\ (g, \chi) & \to & g \cdot \chi = \chi(g^{-1} - g) \end{array}$$

et, comme A agit trivialement sur $\widehat{A}$, cette action se factorise via $G \twoheadrightarrow H = G/A$. Pour chaque $\chi \in \widehat{A}/H$, notons

$$H_\chi := \mathrm{Stab}_H(\chi) \subset H.$$

On va construire les représentations simples de G à partir de celles de A et des H_χ, $\chi \in \widehat{A}/H$. Pour chaque $\chi \in \widehat{A}/A$, notons aussi $G_\chi := AH_\chi \subset G$. Alors,

— *D'une part, le caractère $\chi \in \widehat{A}$ s'étend en un caractère $\tilde{\chi} \in \widehat{G}_\chi$ de degré 1 par la formule*

$$\tilde{\chi}(ah) = \chi(a),\ a \in A,\ h \in H_\chi.$$

— *D'autre part, tout $(V, \theta) \in \widehat{K[H_\chi]}$ se relève en $(V, \theta \circ p_\chi) \in \widehat{K[G_\chi]}$ via la projection $p_\chi : G_\chi \twoheadrightarrow H_\chi$.*

On obtient ainsi un $K[G]$-module

$$(V_{\chi,\theta}, \rho_{\chi,\theta}) = \mathrm{Ind}_{G_\chi}^G((k, \tilde{\chi}) \otimes_K (V, \theta \circ p_\chi)).$$

Montrer que

1. *Les $K[G]$-modules $(V_{\chi,\theta}, \rho_{\chi,\theta})$ ainsi construits sont simples.*
2. *$(V_{\chi,\theta}, \rho_{\chi,\theta})$ et $(V_{\chi',\theta'}, \rho_{\chi',\theta'})$ sont isomorphes si et seulement si $H \cdot \chi = H \cdot \chi'$ et (V, θ) est isomorphe à (V', θ').*
3. *Tout $K[G]$-module simple est de la forme $(V_{\chi,\theta}, \rho_{\chi,\theta})$.*

3.3.4 Représentations linéaires irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$ ($2 \not| q$)

Nous terminons ce chapitre par l'étude systématique des représentations linéaires irréductibles complexes de de $\mathrm{GL}_2(\mathbb{F}_q)$ pour $2 \not| q$.

3.3.4.1 Classes de conjugaison

Rappelons que $|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$. Le tableau ci-dessous décrit les classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_q)$. C'est le premier ingédient pour déterminer les représentations linéaires irréductibles de $\mathrm{GL}_2(\mathbb{F}_q)$

Invariants	Représentant	Cardinal	Nombre de classes
$(T-x),(T-x)$	$\begin{pmatrix} \mathrm{x} & 0 \\ 0 & \mathrm{x} \end{pmatrix}$	1	$q-1$
$(T-x)^2$	$\begin{pmatrix} \mathrm{x} & 1 \\ 0 & \mathrm{x} \end{pmatrix}$	q^2-1	$q-1$
$(T-x)(T-y),\ x \neq y$	$\begin{pmatrix} \mathrm{x} & 0 \\ 0 & \mathrm{x} \end{pmatrix}$	q^2+1	$\frac{(q-1)(q-2)}{2}$
$P(T) = (T-(x+\sqrt{\epsilon}y))(T-(x-\sqrt{\epsilon}y)),\ x,y \in \mathbb{F}_q,\ \epsilon \in \mathbb{F}_q \setminus \mathbb{F}_q^2$	$\begin{pmatrix} \mathrm{x} & \epsilon\,\mathrm{y} \\ \mathrm{y} & \mathrm{x} \end{pmatrix}$	q^2-q	$\frac{q(q-1)}{2}$

3.3.4.2 Représentations de dimension 1

Les représentations de dimension 1 de $\mathrm{GL}_2(\mathbb{F}_q)$ sont les représentations de son abélianisation. LE problème consiste donc à déterminer $[\mathrm{GL}_2(\mathbb{F}_q), \mathrm{GL}_2(\mathbb{F}_q)]$.

Lemme 3.3.13 *On a*

$$[\mathrm{GL}_2(\mathbb{F}_q), \mathrm{GL}_2(\mathbb{F}_q)] = \mathrm{SL}_2(\mathbb{F}_q)(:= \ker(\det)).$$

Preuve. Comme le déterminant est un morphisme de groupes, on a déjà $[\mathrm{GL}_2(\mathbb{F}_q), \mathrm{GL}_2(\mathbb{F}_q)] \subset \mathrm{SL}_2(\mathbb{F}_q)$. Inversement, il s'agit de voir que tout élément de $\mathrm{SL}_2(\mathbb{F}_q)$ s'écrit comme produit de commutateurs. Cela se fait en deux étapes :

1. $\mathrm{SL}_2(\mathbb{F}_q)$ est engendré par les matrices de la forme
$$X_u := \begin{pmatrix} 1 & \mathrm{u} \\ 0 & 1 \end{pmatrix},\ Y_v := \begin{pmatrix} 1 & 0 \\ \mathrm{v} & 1 \end{pmatrix}$$
Pour montrer cela, on part de
$$X = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}$$
telle que $ad - bc = 1$. Si $c \neq 0$, on montre que $X = X_u Y_v X_w$. En passant à la transposée, on obtient une décomposition similaire si $b \neq 0$. Si $b = c = 0$, on se ramène au cas précédent en observant par exemple que
$$XX_{a^{-1}} = \begin{pmatrix} a & 1 \\ 0 & a^{-1} \end{pmatrix}$$
2. On a
$$X_u = \left[X_{\frac{u}{2}}, \begin{pmatrix} 1 & 0 \\ 0 & \text{-1} \end{pmatrix} \right]$$
En passant à la transposée, on obtient de même que les Y_v sont des commutateurs.

Les représentations de dimension 1 de $\mathrm{GL}_2(\mathbb{F}_q)$ sont donc les représentations de la forme
$$\chi \circ \det : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{C},\ \chi \in \widehat{\mathbb{C}[\mathbb{F}_q^\times]}$$
Cela nous donne $q - 1$ représentations de dimension 1.

3.3.4.3 Série principale

Soit
$$B := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{F}_q)$$
On a
$$[B, B] = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$$
Et
$$B^{ab} = B/[B, B] = \mathbb{F}_q^\times \times \mathbb{F}_q^\times.$$
Donc B a $(q-1)^2$ représentations de dimension 1,
$$\underline{\lambda} = (\lambda_1, \lambda_2),\ \lambda_1, \lambda_2 \in \widehat{\mathbb{C}[\mathbb{F}_q^\times]}$$
(explicitement
$$\underline{\lambda}(\begin{pmatrix} \mathrm{a} & \mathrm{b} \\ 0 & \mathrm{d} \end{pmatrix}) = \lambda_1(a)\lambda_2(d)).$$
On note
$$V_{\underline{\lambda}} := \mathrm{Ind}_B^{\mathrm{GL}_2(\mathbb{F}_q)}(\underline{\lambda}).$$
1. Montrer que si $\lambda_1 \neq \lambda_2$ alors $V_{\underline{\lambda}}$ est irréductible.
2. Montrer que si $\lambda_1 = \lambda_2 =: \lambda$ alors
$$V_{\underline{\lambda}} = \lambda \circ \det \oplus W_{\underline{\lambda}},$$
où $W_{\underline{\lambda}}$ est une représentation irréductible de $\mathbb{C}$-dimension q.
3. Montrer que
   — $W_\lambda \simeq W_{\lambda'}$ si et seulement si $\lambda = \lambda'$;
   — Si $\lambda_1 \neq \lambda_2$, $\lambda_1' \neq \lambda_2'$ alors $V_{\underline{\lambda}} \simeq V_{\underline{\lambda}'}$ si et seulement si $\underline{\lambda} = \underline{\lambda}'$.

Cela nous donne $q - 1$ représentations irréductibles de $\mathbb{C}$-dimension q et $\frac{(q-1)(q-2)}{2}$ représentations irréductibles de $\mathbb{C}$-dimension $q + 1$.

3.3.4.4 Série complémentaire

Soit $\epsilon \in \mathbb{F}_q \setminus \mathbb{F}_q^2$. On a alors $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{\epsilon})$ que l'on regarde comme un $\mathbb{F}_q$-espace vectoriel de base $1, \sqrt{\epsilon}$. On identifie $\mathrm{GL}_2(\mathbb{F}_q)$ au groupe des automorphismes $\mathbb{F}_q$-linéaires de $\mathbb{F}_{q^2}$. Notons

$$C := \left\{ \begin{pmatrix} \mathrm{x} & \mathrm{y}\epsilon \\ \mathrm{y} & \mathrm{x} \end{pmatrix},\ x, y \in \mathbb{F}_q^2 \setminus \{(0,0)\} \right\}$$

le sous-groupe cyclique $\simeq \mathbb{F}_{q^2}^{\times}$. Pour $\mu \in \widehat{\mathbb{C}[C]}$, notons

$$Y_\mu := \mathrm{Ind}_C^{\mathrm{GL}_2(\mathbb{F}_q)}(\mu).$$

1. Montrer que $Y_\mu \simeq Y_{\mu'}$ si et seulement si $\mu' = \mu^q$.
2. Avec les notations du paragraphe 3.3.4.3, calculer le caractère $\phi_{\lambda,\mu}$ de la représentation 'virtuelle'

$$W_1 \otimes V_{(\lambda,1)} - V_{(\lambda,1)} - Y_\mu.$$

3. Montrer que si $\mu \neq \mu^q$ et λ est la restriction de μ à $\mathbb{F}_q^{\times}$ calculer $(\phi_{\lambda,\mu}, \phi_{\lambda,\mu})_{\mathrm{GL}_2(\mathbb{F}_q)}$ et $\phi_{\lambda,\mu}(1)$. En déduire que $\phi_\mu := \phi_{\lambda,\mu}$ est le caractère d'une représentation irréductible U_μ de dimension $q-1$.
4. Montrer que si $\mu \neq \mu^q$, $\mu' \neq \mu^{'q}$ alors $U_\mu \simeq U_{\mu'}$ si et seulement si $\mu' = \mu$ (ou $\mu' = \mu^q$).

Cela nous donne $\frac{q(q-1)}{2}$ représentations irréductibles de $\mathbb{C}$-dimension $q-1$.

Au total, on a donc construit

$$2(q-1) + \frac{q(q-1)}{2} + \frac{(q-1)(q-2)}{2} = |Cl(\mathrm{GL}_2(\mathbb{F}_q))|.$$

Chapitre 4

Indications / Corrections de (la plupart des) exercices

4.1 Chapitre 1

Exercice 1.2.4 : On peut par exemple montrer (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2) : Si $s : M'' \to M$ est un morphisme de A-modules tel que $vs = Id_{M''}$ on vérifie que le morphisme de A-modules $Id - sv : M \to M$ a son image contenue dans $\ker(v) = u(M')$ et que $t := (u|^{u(M')})^{-1} \circ (Id - sv) : M \to M'$ vérifie bien $tu = Id_{M'}$.

(2) $\Rightarrow$ (3) : Si $s : M \to M'$ est un morphisme de A-modules tel que $su = Id_{M'}$, on peut considérer $f := s \oplus v : M \to M' \oplus M''$. Par construction, $p_{M''} \circ f = v$ et $f \circ u(s(m)) = s(m) = \iota_{M'}(s(m))$ donc, comme $s : M \to M'$ est surjective, $f \circ u = \iota_{M'}$. Enfin, $f : M \to M' \oplus M''$ est un isomorphisme. Il est injectif car si $f(m) = 0$ alors $v(m) = 0$ *i.e.* $m \in \ker(v) = u(M')$ donc $m = u(m')$ et $m' = su(m') = 0$. Donc, en fait $m = 0$. Il est surjectif car pour tout $m' \in M'$, $m'' \in M''$, on peut écrire $m'' = v(m) = v(m - us(m) + u(m'))$ et $m' = su(m') = s(m - us(m) + u(m'))$.

(3) $\Rightarrow$ (1) : Si $f : M \tilde{\to} M' \oplus M''$ est un isomorphisme de A-modules tel que $p_{M''} \circ f = v$ et $f \circ u = \iota_{M'}$, on peut considérer $s := f^{-1} \circ \iota_{M''} : M'' \to M$. Par construction $vs(m) = vf^{-1}\iota_{M''} = p_{M''}\iota_{M''} = Id_{M''}$.

Exercice 1.2.5 :

1. Si la sec ´tait scindée, on aurait $\mathbb{Z} \simeq \mathbb{Z} \oplus \mathbb{Z}/n$ comme $\mathbb{Z}$-module (exercice 1.2.4), ce qui est absurde puisque $\mathbb{Z}$ est sans torsion.
2. (a) Comme la sec est une suite de $\mathbb{Z}[X]$-modules, l'action de X sur $\mathbb{Z}^2$, détermine l'action de X sur $\mathbb{Z}$ à gauche : $Xz = z$ et à droite : $Xz = -z$ et la flèche $\mathbb{Z} \to \mathbb{Z}^2$ détermine la flèche $v : \mathbb{Z}^2 \to \mathbb{Z} : (a, b) \to b - a$. Supposons que la sec est scindée par un morphisme $s : \mathbb{Z} \to \mathbb{Z}^2$ de $\mathbb{Z}[X]$-modules. Notons $s(1) = (a, b)$. On a $1 = v \circ s(1) = b - a$ donc $b = a + 1$. Donc, d'une part $Xs(1) = X(a, a + 1) = (a + 1, a)$ et d'autre part, $Xs(1) = s(X1) = s(-1) = -s(1) = (-a, -a - 1)$: contradiction.

   (b) Comme la sec est une suite de $\mathbb{Z}[X]$-modules, l'action de X sur $\mathbb{Z}^2$, détermine l'action de X sur $\mathbb{Z}$ à gauche : $Xz = z$ et à droite : $Xz = z$ (et la flèche $\mathbb{Z} \to \mathbb{Z}^2$ détermine la flèche $v : \mathbb{Z}^2 \to \mathbb{Z} : (a, b) \to b$). Si la sec était scindée comme sec de $\mathbb{Z}[X]$-module, X agirait comme l'identité sur $\mathbb{Z}^2$: contradiction.

Exercice 1.2.6 (Indications) :

1. Facile.

2. (a) Tout d'abord, on peut 'deviner' qui est $\delta : \ker(\alpha'') \to \text{coker}(\alpha')$ car il n'y a pas vraiment de choix pour construire cette flèche de façon naturelle : en partant de $m'' \in \ker(\alpha'')$, la surjectivité de u assure qu'il existe $m \in M$ tel que $u(m) = m''$. Comme $0 = \alpha''u(m) = v\alpha(m)$ on a $\alpha(m) \in \ker(v) = v'(N')$. Comme la restriction $v' : N' \tilde{\to} v'(N')$ est un isomorphisme, on peut poser $\delta(m'') = p_{\alpha'(M')}(v'|^{v'(N')-1}(\alpha(m)))$. Bien sûr, il faut ensuite vérifier que cette construction est indépendante du choix de m et définit bien un morphisme de A-modules (pas juste une application ensembliste). Il faut donc réécrire ce qui précède 'proprement'.

Pour cela, on part de la restriction $u : u^{-1}(\ker(\alpha')) \to \ker(\alpha'')$ qui est surjective et induit un isomorphisme de A-modules $\overline{u} : u^{-1}(\ker(\alpha''))/u(M') \xrightarrow{\sim} \ker(\alpha'')$. Comme $v \circ \alpha u^{-1}(\ker(\alpha'') = \alpha'' \circ u(u^{-1}(\ker(\alpha'')) = \alpha''(\ker(\alpha'')) = 0$, la restriction $\alpha : u^{-1}(\ker(\alpha'')) \to N$ est à valeur dans $\ker(v) = v'(N')$. On peut donc définir un morphisme de A-modules :

$$\delta^\circ : u^{-1}(\ker(\alpha'')) \xrightarrow{\alpha} v'(N') \overset{v'|^{v'(N')-1}}{\to} N' \overset{p_{\alpha'(M')}}{\to} \operatorname{coker}(\alpha')$$

Par construction, $\delta^\circ(u'(m')) = p_{\alpha'(M')}v'|^{v'(N')-1}\alpha u'(m') = p_{\alpha'(M')}v'|^{v'(N')-1}v'\alpha'(m') = p_{\alpha'(M')}\alpha'(m') = 0$ donc $\delta^\circ : u^{-1}(\ker(\alpha'') \to \operatorname{coker}(\alpha')$ se factorise *via* $\overline{\delta}^\circ : u^{-1}(\ker(\alpha'')/u'(M') \to \operatorname{coker}(\alpha')$ et on obtient notre δ comme suit :

$$\delta : \ker(\alpha'') \overset{\overline{u}^{-1}}{\to} u^{-1}(\ker(\alpha'')/u'(M') \overset{\overline{\delta}^\circ}{\to} \operatorname{coker}(\alpha').$$

(b) L'existence des morphismes autres que δ résulte de 1. Pour l'exactitude, la seule difficulté est en δ. Pour cela, on peut utiliser la description 'intuitive' de δ (puisqu'on a montré qu'elle était bien définie).

— $\ker(\delta) = u(\ker(\alpha))$. L'inclusion $\ker(\delta) \supset u(\ker(\alpha))$ est facile car si $m'' = u(m)$ avec $\alpha(m) = 0$ alors $\delta(m'') = p_{\alpha'(M')}(v'|^{v'(N')-1}(\alpha(m))) = 0$. Inversement, soit $m'' \in \ker(\alpha'')$ tel que $\delta(m'') = p_{\alpha'(M')}(v'|^{v'(N')-1}(\alpha(m)))$ *i.e.* $v'|^{v'(N')-1}(\alpha(m)) = \alpha'(m')$ ou, encore, $\alpha(m) = v'\alpha'(m') = \alpha u'(m)$. Donc $m - u'(m) \in \ker(\alpha)$ et $m'' = u(m) = u(m - u'(m)) \in u(\ker(\alpha))$.

— $\delta(\ker(\alpha'')) = v'^{-1}(\alpha(M))/\alpha'(M')$. Là encore l'inclusion $\delta(\ker(\alpha'')) \subset v'^{-1}(\alpha(M))/\alpha'(M')$ est facile car avec $m'' = u(m)$ on a

$$\overline{v}'\delta(m'') = \overline{v}'p_{\alpha'(M')}(v'|^{v'(N')-1}(\alpha(m))) = p_{\alpha(M)}v'(v'|^{v'(N')-1}(\alpha(m))) = p_{\alpha(M)}(\alpha(m))) = 0.$$

Inversement, soit $m \in M$ tel que $\alpha(m) \in v'(N')$ *i.e.* $\alpha(m) = v'(n')$. Alors $\alpha''u(m) = v\alpha(m) = vv'(m') = 0$ donc $m'' := u(m) \in \ker(\alpha'')$. Mais alors, on a

$$\delta(m'') = p_{\alpha'(M')}(v'|^{v'(N')-1}(\alpha(m))) = p_{\alpha'(M')}(v'|^{v'(N')-1}(v'(n')) = p_{\alpha'(M')}(n').$$

(c) Facile.

(d) Facile.

3. Dans les deux cas, il s'agit de reconnaitre un serpent déguisé.

(a) Ici, le serpent déguisé est

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{u_1} & M_2 & \xrightarrow{u_2} & u_2(M_2) \longrightarrow 0 \\ & & \downarrow{\scriptstyle v_1\alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} \\ 0 & \longrightarrow & v_1(N_1) & \xrightarrow{incl.} & N_2 & \xrightarrow{v_2} & N_3 \end{array}$$

Il faut juste vérifier que l'on a bien le droit de remplacer M_3 par $u_2(M_2)$ sans affecter $\ker(\alpha_3)$ *i.e.* que $\ker(\alpha_3) \subset u_2(M_2)$. Mais cela résulte de ce que si $m_3 \in \ker(\alpha_3)$ alors $\alpha_4 u_3(m_3) = v_3\alpha_3(m_3) = 0$ donc $u_3(m_3) \in \ker(\alpha_4)$. Mais, par hypothèse $\ker(\alpha_4) = 0$. Donc en fait $m_3 \in \ker(u_3) = u_2(M_2)$.

(b) Ici, le serpent déguisé est

$$\begin{array}{ccccccc} & & M_3 & \xrightarrow{u_3} & M_4 & \xrightarrow{u_4} & u_4(M_4) \longrightarrow 0 \\ & & \downarrow{\scriptstyle p_{v_2(N_2)}\alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ 0 & \longrightarrow & N_3/v_2(N_2) & \xrightarrow{\overline{v}_3} & N_4 & \xrightarrow{v_4} & N_5 \end{array}$$

Le serpent nous donne que $p_{v_2(N_2)}\alpha_3 : M_3 \twoheadrightarrow N_3/v_2(N_2)$ est surjective *i.e.* $\alpha_3(M_3) + v_2(N_2) = N_3$. Pour en déduire que $\alpha_3 : M_3 \to N_3$ est surjective, il reste donc à montrer que $V_2(N_2) \subset \alpha_3(M_3)$. Mais comme $\alpha_2 : M_2 \twoheadrightarrow N_2$ est surjective, $v_2(N_2) = v_2\alpha_2(N_2) = \alpha_3 u_2(N_2) \subset \alpha_3(M_3)$.

Exercice 1.2.11 (Indications) :

1. Facile.
2. Soit $N' \overset{u}{\to} N \overset{v}{\to} N'' \to 0$ une suite exacte courte de A-modules. La surjectivité de $N \otimes_A M \overset{v\otimes_A Id_M}{\to} N'' \otimes_A M$ se montre en utilisant que $N'' \otimes_A M$ est engendré par les éléments de la forme $n'' \otimes m$. En effet, comme $v : N \to N''$ est surjective, on peut écrire $n'' = v(n)$ donc $n'' \otimes m = v(n) \otimes m = (v \otimes Id_M)(n \otimes m)$. Pour l'exactitude au milieu, l'inclusion $(u \otimes Id_M)(N' \otimes_A M) \subset \ker(v \otimes Id_M)$ est immédiate (fonctorialité). Pour l'inclusion réciproque, il y a deux méthodes.
   — Méthode 'directe' : Notons $I := (u \otimes Id_M)(N' \otimes_A M)$. Le morphisme $v \otimes Id_M : N \otimes_A M \twoheadrightarrow N'' \otimes_A M$ se factorise *via*
   $$\overline{v \otimes Id_M} : N \otimes_A M/I \twoheadrightarrow N'' \otimes_A M$$
   dont on veut montrer que c'est un isomorphisme de A-modules. Pour cela, il suffit de construire un morphisme de A-modules $s : N'' \otimes_A M \to N \otimes_A M/I$ tel que $\overline{sv \otimes Id_M} = Id_{N''\otimes_A M}$. Considérons donc l'application $s : N'' \times M \to N \otimes_A M/I$ définie par $s(n'', m) = (\sigma(n'') \otimes m) mod I$, où $\sigma : N'' \to N$ est une section ensembliste de $v : N \twoheadrightarrow N''$. Tout d'abord, s ne dépend pas de σ car si $\sigma' : N'' \to N$ est une autre section ensembliste de $v : N \twoheadrightarrow N''$, pour tout $n'' \in N''$ on a $\sigma(n'') - \sigma'(n'') \in \ker(v) = u(N')$ donc $\sigma(n'') \otimes m - \sigma'(n'') \otimes m = (\sigma(n'') - \sigma'(n'')) \otimes m \in I$. Cela permet de vérifier que s est A-bilinéaire. Qu'elle le soit en m est immédiat. Pour vérifier qu'elle l'est en n'', calculons $s(a_1 n_1'' + a_2 n_2'', m) = (\sigma(a_1 n_1'' + a_2 n_2'') \otimes m) mod I$. Mais on a montré qu'on pouvait remplacer $\sigma(a_1 n_1'' + a_2 n_2'')$ par n'importe quel autre élément dans $v^{-1}(a_1 n_1'' + a_2 n_2'')$ donc, en particulier, $a_1\sigma(n_1'') + a_2\sigma(n_2'')$. Par propriété universelle du produit tensoriel, $s : N'' \times M \to N \otimes_A M/I$ se factorise *via* $\overline{s} : N'' \otimes_A M \to N \otimes_A M/I$ et, par construction, $\overline{\overline{s}v \otimes Id_M} = Id_{N''\otimes_A M}$.
   — Méthode utilisant (1). Plus précisément, il faut observer (laisser en exercice - facile) qu'en fait, si on a une suite de A-modules
   $$(*) \quad N' \overset{u}{\to} N \overset{v}{\to} N'' \to 0$$
   alors $(*)$ est exacte *si et* seulement si pour tout A-module M, la suite Hom
   $$0 \to \mathrm{Hom}(N'', M) \overset{-\circ v}{\to} \mathrm{Hom}(N, M) \overset{-\circ u}{\to} \mathrm{Hom}(N', M).$$
   Ensuite, on raisonne comme suit : $(**)$ $N' \otimes_A M \overset{u\otimes Id}{\to} N \otimes_A M \overset{v\otimes Id}{\to} N'' \otimes_A M \to 0$ est exacte si et seulement si pour tout A-module L la suite
   $$(\#\#, L) \quad 0 \to \mathrm{Hom}(N'' \otimes_A M, L) \overset{-\circ v\otimes Id_M}{\to} \mathrm{Hom}(N \otimes_A M, L) \overset{-\circ u\otimes Id_M}{\to} \mathrm{Hom}(N' \otimes_A M, L)$$
   est exacte. Mais en utilisant la propriété d'adjonction - 1, cette suite est canoniquement isomorphe à la suite
   $$(\#, L) \quad 0 \to \mathrm{Hom}(N'', \mathrm{Hom}(M, L)) \overset{-\circ v}{\to} \mathrm{Hom}(N, \mathrm{Hom}(M, L)) \overset{-\circ u}{\to} \mathrm{Hom}(N', \mathrm{Hom}(M, L)).$$
   Mais on a vu que si on suppose que $(*)$ est exacte alors pour tout A-module L $(\#, L)$ l'est aussi.
3. Facile : il faut construire deux morphismes de A-modules $M/\mathfrak{i}M \to M \otimes_A A/\mathfrak{i}$ et $M \otimes_A A/\mathfrak{i} \to M/\mathfrak{i}M$ inverses l'un de l'autre en utilisant les propriétés universelles.
4. C'est le lemme du serpent appliqué à
   $$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow p & & \downarrow p & & \downarrow p & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0. \end{array}$$
   On voit en particulier que le foncteur $- \otimes \mathbb{Z}/p$ ne préserve en général pas l'injectivité à gauche dans une suite exacte courte. Une condition suffisante pour qu'il la préserve est que $M''[p] = 0$.

Exercice 1.2.14 (Indications) :

1. Facile mais fastidieux ; il faut utiliser systématiquement les propriétés universelles.

2. Comme dans l'exercice 1.2.9 3., c'est facile : il faut construire deux morphismes de A-modules inverses l'un de l'autre en utilisant les propriétés universelles. On a en particulier
$$\mathbb{Z}/m \otimes \mathbb{Z}/n \simeq \mathbb{Z}/pgcd(m,n),$$
par exemple $\mathbb{Z}/p \otimes \mathbb{Z}/q = 0$ si $p \neq q$ sont deux premiers distincts.

3. Là encore, c'est facile : il faut construire deux morphismes de A-modules inverses l'un de l'autre en utilisant les propriétés universelles. Faisons-le : On part de $f : B \times A[X] \to B[X]/\varphi(P)$ définie par $f(b,Q) = (b\varphi(Q))mod\varphi(P)$. Cette application est clairement A-bilinéaire et contient $0 \times PA[X]$ dans son noyaux donc se factorise en une application - toujours A-bilinéaire
$$f_1 : B \times A[X]/P \to B[X]/\varphi(P)$$
qui, à son tour, par propriété universelle du produit tensoriel, se factorise en un morphisme de A-module $f_2 : B \otimes_A A[X]/P \to B[X]/\varphi(P)$. Explicitement $f_2(b \otimes (QmodP)) = (b\varphi(Q))mod\varphi(P)$. Inversement, on part du morphisme de B-algèbres (pour la structure de B-algèbre décrite dans (1) sur $B \otimes_A A[X]/P$) $g : B[X] \to B \otimes_A A[X]/P$ défini par $g(X) = 1 \otimes (XmodP)$; l'existence de g est assuré par la propriété universelle de $B[X]$. On a clairement $\phi(P)B[X] \subset \ker(g)$ donc $g : B[X] \to B \otimes_A A[X]/P$ se factorise en un morphisme de B-algèbres $g_1 : B[X]/\varphi(P) \to B \otimes_A A[X]/P$. Explicitement $g_1(Qmod\varphi(P)) = g(Q)$. On vérifie immédiatement que f_2 et g_1 sont des applications inverses l'une de l'autre. Cela implique au passage que f_2 est automatiquement un morphisme de B-algèbres (pas juste de A-modules) ; bien sûr, on pouvait aussi le vérifier immédiatement à la main.
On applique cela à
$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}[X]/(X^2+1) \simeq \mathbb{C}[X]/(X+i) \times \mathbb{C}[X]/(X-i) \simeq \mathbb{C} \times \mathbb{C}.$$
(L'avant dernière égalité est le lemme Chinois). Donc $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ n'est pas un corps. Par contre,
$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}[X]/(X^2-2) \simeq \mathbb{Q}(i)[X]/(X^2-2)$$
est un corps, extension quadratique de $\mathbb{Q}(i)$, car X^2-2 reste irréductible dans $\mathbb{Q}(i)[X]$.

Exercice 1.3.4 :

1. Supposons M noetherien (resp. artinien). Toute suite croissante (resp. décroissante) de sous-A modules de M' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. De même, l'image inverse dans M de toute suite croissante (resp. décroissante) de sous-A modules de M'' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. Supposons M' et M'' noetheriens (resp. artiniens). Soit $M_1 \subset \ldots \subset M_n \subset M_{n+1} \subset \ldots M$ une suite croissante de sous-A modules de M. Il existe un entier N tel que $M_N \cap M' = M_n \cap M'$ et $(M_N + M')/M' = (M_n + M')/M'$n $n \geq N$. La conclusion résulte du lemme du serpent appliqué à
$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_N \cap M' & \longrightarrow & M_N & \longrightarrow & (M_N+M')/M' & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_n \cap M' & \longrightarrow & M_n & \longrightarrow & (M_n+M')/M' & \longrightarrow & 0 \end{array}$$
L'assertion pour 'artinien' se montre de la même façon.
2. On procède par induction sur n en utilisant 1.3.4 (1) et la suite exacte courte de A-modules
$$0 \to \oplus_{1 \leq i \leq n} M_i \to \oplus_{1 \leq i \leq n+1} M_i \to M_{n+1} \to 0.$$
3. D'après 1.3.4 (2) $A^{\oplus n}$ est noetherien (resp. artinien) et, par définition, tout A-module de type fini est quotient d'un A-module de la forme $A^{\oplus n}$. Donc la conclusion résulte de 1.3.4 (1).

Exercice 1.3.5 :

1. Il existe un entier $N \geq 1$ tel que $\ker(f^N) = \ker(f^n)$, $n \geq N$ et on applique le lemme du serpent à
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f^N) & \longrightarrow & M & \xrightarrow{f^N} & M & \longrightarrow & 0 \\ & & \downarrow \simeq & & \simeq \downarrow Id & & \downarrow f & & \\ 0 & \longrightarrow & \ker(f^{N+1}) & \longrightarrow & M & \xrightarrow[f^{N+1}]{} & M & \longrightarrow & 0 \end{array}$$

2. Il existe un entier $N \geq 1$ tel que $\mathrm{im}(f^N) = \mathrm{im}(f^n)$, $n \geq N$ et on applique le lemme du serpent à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f^{N+1}} & M & \longrightarrow & M/\mathrm{im}(f^{N+1}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle \simeq} & & \\ 0 & \longrightarrow & M & \xrightarrow[f^N]{} & M & \longrightarrow & M/\mathrm{im}(f^N) & \longrightarrow & 0 \end{array}$$

3. (3) Comme Mest artinien et noetherien, il existe un entier $N \geq 1$ tel que

$$f^\infty(M) := \bigcap_{n\geq 0} \mathrm{im}(f^n) = \mathrm{im}(f^N), \quad f^{-\infty}(M) := \bigcup_{n\geq 0} \ker(f^n) = \ker(f^N).$$

On vérifie que $f^\infty(M)$, $f^{-\infty}(M)$ ainsi définis conviennent. Le seul point un peu astucieux est $M = f^\infty(M) + f^{-\infty}(M)$. On a envie d'écrire $m = f^N(m) + m - f^N(m)$ mais ça ne marche pas. Il faut ajuster en utilisant que $\mathrm{im}(f^N) = \mathrm{im}(f^{2N})$ et donc qu'il existe $\mu \in M$ tel que $f^N(m) = f^{2N}(\mu)$. La décomposition $m = f^N(\mu) + m - f^N(\mu)$ elle, convient.

Exercice 1.4.10

1. Commençons par observer que si M est un A-module de type fini, pour tout $\phi \in \mathrm{End}_A(M)$ il existe un polynôme unitaire (donc en particulier non nul) $P(T) = T^n + \sum_{i=0}^{n-1} a_i T^i \in A[T]$ tel que $P(\phi) = 0$. En effet, soit $m_1, \ldots, m_r$ un système de générateurs de M comme A-module. Pour chaque $j = 1, \ldots, r$ on a $\phi(m_i) = \sum_{1\leq j\leq r} a_{i,j} m_j$, ce qui se réecrit en $\sum_{1\leq i\leq r}(\delta_{i,j}\phi - a_{i,j}Id)m_i = 0$ Notons $\Delta = (\delta_{i,j}\phi - a_{i,j})_{1\leq i,j\leq r} \in M_r(E)$, où $E = A[\phi] \subset \mathrm{End}_A(M)$. Pour tout $\underline{m} \in M^{\oplus m}$ on a $\Delta\underline{m} = 0$ donc *a fortiori*, ${}^tCom(\Delta)\Delta\underline{m} = 0$. Mais ${}^tCom(\Delta)\Delta = det(\Delta)Id_E$ et en developpant $det(\Delta) \in A[\phi]$ on obtient le P cherché.
Supposons maintenant qu'il existe un morphisme de A-modules injectifs $\phi : A^{\oplus r} \hookrightarrow A^{\oplus s}$ avec $r > s$. On peut le composer avec l'injection canonique $\iota : A^{\oplus s} \hookrightarrow A^{\oplus s} \oplus A^{\oplus(r-s)} \simeq A^{\oplus r}$. D'après l'observation précédente, il existe un polynôme unitaire $P(T) = T^n + \sum_{i=0}^{n-1} a_i T^i \in A[T]$ tel que $P(\iota \circ \phi) = 0$. Prenons P de degré minimal. L'injectivité de ϕ assure alors que $a_0 \neq 0$ car sinon on aurait $\phi\circ(\phi^{n-1} + \sum_{i=1}^{n-1} a_i(\iota\circ\phi)^{i-1}) = 0$ avec, par minimalité de r, $\phi^{n-1} + \sum_{i=1}^{n-1} a_i(\iota \circ \phi)^{i-1} \neq 0$: contradiction. Mais alors, en évaluant $P(\phi)$ en $e_m := (0, \ldots, 0, 1) \in A^{\oplus m}$ on obtient $0 = P(\phi)(e_m) = (\iota \circ \phi)^n + \sum_{i=1}^{n-1} a_i(\iota \circ \phi)^i(e_m) + a_0 e_m = (*, \ldots, *, a_0)$: contradiction.
2. Si A est un anneau quelconque, A est toujours un A-module libre sur lui-même. Par contre, un sous-A-module (=idéal) $I \subsetneq A$ est libre si et seulement si il est de la forme $I = Aa$ avec $A \in A \setminus T_A$. La condition suffisante est évidente et la condition nécessaire est la question précédente (ou, de façon plus élémentaire, si $I = \oplus_{j\in J} Aa_j \simeq A^{(J)}$ et J n'est pas un singleton alors pour tout $i \in J$, $a_i I = \oplus_{j\in J} Aa_i a_j \subset Aa_i$ donc pour $i \neq i$, $a_i a_j = 0$, ce qui contredit $Aa_j \simeq A$). Par exemple, $Xk[X,Y] + Yk[X,Y] \subset k[X,Y]$ n'est pas un sous $k[X,Y]$-module libre du $k[X,Y]$-module libre $k[X,Y]$.

Exercice 1.4.20 : L'unicité de s et de la suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ résulte du Corollaire 1.4.10
car $r - s$ est le rang de la partie libre de M/N et $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ est la suite des invariants de la partie de torsion de M/N. L'existence est un peu plus délicate. On procède par reccurence sur r. Si $r = 1$, c'est la traduction du fait que A est principal. Si $r \geq 1$, l'idée est de construire d_1, e_1 à partir de l'inclusion $N \hookrightarrow M$. Pour cela, on introduit l'ensemble $\mathcal{E}$ des idéaux de la forme $f(N) \subset A$, où $f : M \to A$ est un morphisme de A-module. Comme A est noetherien, $\mathcal{E}$ contient au moins un élément maximal $f(N) = Ad = Af(n)$.

1. En fait, pour tout $g : M \to A$ on a $g(N) \subset f(N)$. En effet, si δ est le pgcd de d et $g(n)$ il existe $u, v \in A$ tels que $ud + vg(n) = \delta$. Donc
$$f(N) = Ad \subset A\delta = A(uf + vg)(n) \subset (uf + vg)(N)$$
Par maximalité de $f(N)$, cela implique $f(N) = Ad = A\delta = (uf + vg)(N)$. En particulier, pour tout $n' \in N$, d divise $(uf + vg)(n')$. Mais $f(N) = Ad$, donc d divise aussi $f(n')$. On en déduit que d divise $vg(n')$ et comme d est premier avec v, que d divise $g(n')$. *In fine*, on a $g(N) \subset Ad = f(N)$ comme annoncé.

2. Il existe $\mu \in M$ tel que $dm = n$. Choisissons une A-base quelconque $e_1, \ldots, e_r$ de M et notons $p_i : M \twoheadrightarrow Am_i \simeq A$ la projection correspondante sur la i-ème coordonnée. On a, dans cette base, $n = \sum_{a\leq i\leq r} a_i e_i$ et en appliquant (1) aux p_i, on obtient que d divise a_i, $i = 1, \ldots, r$. Donc en écrivant $a_i = db_i$ pour un certain $b_i \in A$, $i = a, \ldots, r$, on peut prendre $\mu = \sum_{1\leq i\leq r} b_i e_i$.

3. De $de = m$, on déduit $f(d\mu) = df(\mu) = f(n) = d$ donc comme A est intègre, $f(\mu) = 1$. Cela donne une décomposition $M \simeq \ker(f) \oplus A\mu$ ($m = (m - f(m)\mu) + f(m)\mu$ telle que $N = \ker(f) \cap N \oplus Ad\mu$. On peut donc appliquer l'hypothèse de recurrence à $\ker(f) \cap N \subset \ker(f)$ puisqu'on sait que $\ker(f)$ est un A-module libre de rang r (Lemme 1.4.5)
pour obtenir une suite $A \supsetneq Ad_2 \supset \cdots \supset Ad_s \supsetneq 0$ d'idéaux de A et $m_2, \ldots, m_r \in \ker(f)$ tels que

$$\ker(f) \cap N = \bigoplus_{2 \leq i \leq s} Ad_i m_i \subset \bigoplus_{2 \leq i \leq r} Am_i = \ker(f).$$

Enfin, en appliquant à nouveau (1) à la projection $M = A\mu \oplus \bigoplus_{2 \leq i \leq r} Am_i \twoheadrightarrow Am_2 \simeq A$, on voit que d divise d_2.

Exercice 1.4.21 : On suppose $m \geq n$. Notons $M := A^m$, $N := A^n$ et soit $f : M \to N \in \mathrm{Hom}_A(M, N)$. Par le théorème de la base adaptée pour $f(M) \subset N$ il existe un unique $0 \leq r \leq n$, une unique suite d'idéaux $A \supsetneq Ad_1 \supset Ad_2 \supset \ldots \supset Ad_s$ et des éléments $\nu_1, \ldots, \nu_n \in N$ tels que

$$f(M) = \oplus_{1 \leq i \leq r} Ad_i \nu_i \subset \oplus_{1 \leq i \leq n} A\nu_i = N.$$

Comme $f(M)$ est un A-module libre, la suite exacte courte

$$0 \to \ker(f) \to M \xrightarrow{f} f(M) \to 0$$

est scindée. Notons $s : f(M) \to M$ un scindage. On a alors $M \simeq \ker(f) \oplus s(f(N))$. Comme A est principal et M est un A-module libre, $\ker(f) \subset M$ est encore un A-module libre. En concaténant une A-base de $\ker(f)$ et la A-base $s(\nu_1), \ldots, s(\nu_n)$ de $f(N)$, on obtient une A-base $\mu_1, \ldots, \mu_n$ de M. La matrice de f dans les bases $\mu_1, \ldots, \mu_m$ et $\nu_1, \ldots, \nu_n$ est de la forme

$$D(d_1, \ldots, d_n) := \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 \\ 0 & d_2 & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & d_n & 0 \end{pmatrix}.$$

On a donc montré que si $f, g : M \to N$ sont des morphismes de A-modules tels que $N/f(M) \simeq N/g(M)$ alors f, g sont équivalents. La réciproque est presque immédiate car s'il existe des automorphismes $\phi \in Aut_A(M)$, $\psi \in Aut_A(N)$ tels que $f \circ \phi = \psi \circ g$ alors $\psi : N \tilde{\to} N$ se restreint en un isomorphisme de A-modules $\psi : g(M) \tilde{\to} f(\phi(M)) = f(M)$ donc induit un isomorphisme de A-modules $\overline{\psi} : N/g(M) \tilde{\to} N/f(M)$.

Exercice 1.4.22 : L'hypothèse $\phi \otimes \mathbb{Q}$ inversible assure que $\det(\phi) \neq 0$. D'après l'exercice 1.4.22, il existe une base de M dans laquelle la matrice Φ de ϕ vérifie

$$U\Phi V = D(d_1, \ldots, d_n),$$

avec $\mathbb{Z} \supsetneq \mathbb{Z}d_1 \supset \mathbb{Z}d_2 \supset \cdots \supset \mathbb{Z}d_n$ les facteurs invariants de $\mathbb{Z}^n/f(Z^n)$ et $U, V \in GL_n(\mathbb{Z})$. En particulier, en prenant le déterminant, on obtient

$$\pm \det(f) = d_1 \cdots d_n = [M : f(M)].$$

Exercice 1.5.6 :

1. Supposons M semisimple. Soit $N' \subset M'$ un sous-A-module. On a par la caractérisation (3) appliquée à M, $M = N' \oplus N$ comme A-modules. En particulier, pour tout $m' \in M'$, on peut écrire $m' = n' + n$ avec $n' \in N'$, $n \in N$. Mais alors $n = m' - n' \in N \cap M'$. Cela montre que $M' \subset N' \oplus (N \cap M')$; l'inclusion réciproque est immédiate. La caractérisation (3) montre donc que M' est semisimple. Pour M'', il suffit d'observer qu'un quotient d'un module simple est soit trivial, soit simple. On a par la caractérisation (1) appliquée à M, $M = \sum_{i \in I} M_i$ avec $M_i \subset M$ un sous-A-module simple, $i \in I$. On en déduit $M'' = \sum_{i \in I} M_i''$, où M_i'' est l'image de M_i dans M'' et est en particulier soit trivial, soit simple. La caractérisation (1) montre donc que M'' est semisimple. La réciproque est fausse, comme le montre l'extension de $\mathbb{Z}$-modules

$$0 \to \mathbb{Z}/2 \to \mathbb{Z}/4 \to \mathbb{Z}/4 \to 0.$$

2. L'implication (b) $\Rightarrow$ (a) est tautologique. L'implication (b) $\Rightarrow$ (a) résulte de (1) en utilisant que tout A-module M est quotient de $A^{(M)}$ et qu'une somme directe de A-module semisimples est semisimple par la caractérisation (2).

3. Un anneau à division A est un anneau tel que $A^\times = A \setminus \{0\}$; en particulier, les seuls idéaux à gauche de A sont $\{0\}$ et A, ce qui montre que A est simple. Mais les modules simples de A sont tous de la forme $A/\mathfrak{m}$ avec $\mathfrak{m} \subset A$ un idéal à gauche maximal. Donc le seul A-module simple est $A \simeq A/\{0\}$. Par la question (3), tout A-module M est semisimple et, par la caractérisation (2) est somme directe de A-modules simples *i.e.* de la forme $A^{(I)}$.

4. Par le lemme des restes Chinois, $A/\langle a_1^{n_1} \cdots a_r^{n_r}\rangle \simeq A/\langle a_1^{n_1}\rangle \times \cdots \times A/\langle a_r^{n_r}\rangle \simeq A/\langle a_1^{n_1}\rangle \oplus \cdots \oplus A/\langle a_r^{n_r}\rangle$. On peut donc supposer $r = 1$. La conclusion résulte alors du fait que dans un anneau principal, les éléments irréductibles sont premiers.

5. Soit M un $k[G]$-module de dimension finie et $N \subset M$ un sous-$k[G]$-module. Notons $V \subset M$ un supplémentaire de N comme k-espace vectoriel et $p : M \twoheadrightarrow N$ la projection de M sur N parallèlement à V. L'idée est de transformer $p : M \twoheadrightarrow N$ est un morphisme de $k[G]$-module tout en préservant le fait que c'est une projection d'image N ; le noyau du morphisme obtenu fournira alors le supplémentaire de N dans M comme $k[G]$-module. Pour ce faire, on introduit le morphisme moyenné

$$\begin{array}{rccc} p_G : & M & \to & N \\ & m & \to & \frac{1}{|G|}\sum_{g\in G} g^{-1}p(gm) \end{array}$$

On laisse en exercice les vérifications suivantes, qui découlent de la construction : $p_G(M) \subset N$ (car $N \subset M$ est un sous-$k[G]$-module), $p_G \circ p_G = p_G$ (utilise qu'on a introduit le facteur $\frac{1}{|G|}$), $p_G|_N : N \to N$ est l'identité sur N, $p_G(g \cdot m) = g \cdot p_G(m)$, $g \in G$, $m \in M$. On a donc comme annoncé $M = N \oplus \ker(p_G)$ avec $\ker(p_G) \subset M$ un sous-$k[G]$-module. On a utiilisé l'hypothèse que $|G|$ était premier à la caractéristique de k pour pouvoir diviser par $|G|$. Cette condition est en fait nécessaire. En effet, si $p||G|$, $k[G]$ n'est jamais semisimple. Pour cela, on peut considérer la droite $D = k\sigma \subset k[G]$, où $\sigma = \sum_{g\in G} g$. On a $\sigma^2 = |G|\sigma = 0$. Supposons que $k[G] = D \oplus M$ comme $k[G]$-module. En particulier, $1 = a\sigma + m$ avec $0 \neq a \in k$, $0 \neq m \in M$ (D et M sont des idéaux stricts de $k[G]$). Mais on a alors $1 = 1^2 = a^2\sigma^2 + 2a\sigma m + m^2 = m^2 \in M$: contradiction.

4.2 Chapitre 2

Exercice 2.1.1 :

1. Soit $1 \neq \sigma \in \mathcal{S}_n$ donc il existe $a \in \{1, \ldots, n\}$ tel que $\sigma(a) \neq a$. Si $n \geq 3$, on peut trouver $b \in \{1, \ldots, n\}$, $b \neq a, \sigma(a)$. Vérifier alors que $(\sigma(a), b) \circ \sigma \circ (\sigma(a), b) \neq \sigma$.
2. Comme $\mathcal{A}_n = \ker(\epsilon)$, on voit que tout élément de $\mathcal{A}_n$ s'écrit comme le produit d'un nombre *pair* de transpositions. Il suffit donc de montrer que le produit de deux transpositions s'écrit comme produit de 3-cycles. On distingue deux cas :
   — Support non-disjoint : $(a, b)(b, c) = (a, b, c)$.
   — Support disjoint : $(a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d)$.

   On sait déjá que si c, c' sont deux 3-cycles, ils sont conjugués dans $\mathcal{S}_n$. Soit donc $\sigma \in \mathcal{S}_n$ tel que $c' = \sigma^{-1}c\sigma$. Supposons maintenant que $n \geq 5$. Dans ce cas, on peut toujours trouver une permutation τ dont le support est disjoint de celui de c'. On a alors $c' = \tau^{-1}c'\tau = (\sigma\tau)^{-1}c\sigma\tau$. La conclusion résulte alors du fait que σ ou $\sigma\tau$ est dans $\mathcal{A}_n$.
3. (a) On peut utiliser l'equation aux classes. Notons X le support de c. Les supports des cycles qui interviennent dans la décomposition de c^m sont les orbites de c^m agissant sur X. On a donc

$$l = |X| = \sum_{x \in X/\langle c^m\rangle} |\langle c^m\rangle \cdot x|$$

   Mais

$$|\langle c^m\rangle \cdot x| = \frac{|\langle c^m\rangle|}{|Stab_{\langle c^m\rangle}(x)|}$$

   Or d'une part

$$\langle c^m\rangle \simeq m\mathbb{Z}/l \simeq (m\mathbb{Z} + l\mathbb{Z})/l\mathbb{Z} \simeq d\mathbb{Z}/l \simeq \mathbb{Z}/(l/d)$$

   et d'autre part $Stab_{\langle c^m\rangle}(x) \subset Stab_{\langle c\rangle}(x) = 1$ (par définition d'un cycle). On en déduit que chaque orbite est de cardinal l/d et donc qu'il y a d

(b) Si $x = \sum_{1\leq i\leq n} x_i e_i \in k^n$ et $\sigma \in \mathcal{S}_n$ alors

$$\sigma \cdot x = x \Longleftrightarrow x_{\sigma(i)} = x_i,\ i = 1, \ldots, n \Longleftrightarrow x \in \bigoplus_{1\leq i\leq r} ke(c_i),$$

où $\sigma = c_1 \circ \cdots \circ c_r$ est la décomposition de σ en produit de cycles à supports disjoints et $e(c_i) := \sum_{i\in supp(c_i)} e_i$.

(c) Comme l'application $\sigma \to P_\sigma$ est un morphisme de groupes, on voit déjà que si $\sigma, \tau \in \mathcal{S}_n$ sont conjugués dans $\mathcal{S}_n$ alors $P_\sigma, P_\tau \in \mathrm{GL}_n(k)$ sont conjugués dans $\mathrm{GL}_n(k)$. La réciproque est plus délicate. Si P_σ et P_τ sont conjuguées, $P_{\sigma^m} = P_\sigma^m$ et $P_{\tau^m} = P_\tau^m$ le sont également pour tout $m \geq 1$. (b) montre alors que σ^m et τ^m ont même nombre de cycles à supports disjoints *i.e.* $\sum_k l_{\sigma^m}(k) = \sum_k l_{\tau^m}(k)$ pour tout $m \geq 1$. Mais, par (a), on a

$$\sum_k m \wedge k l_\sigma(k) = \sum_k l_{\sigma^m}(k) = \sum_k l_{\tau^m}(k) = \sum_k m \wedge k l_\tau(k),\ m \geq 1.$$

Pour conclure, il suffit donc de montrer que la matrice $D := (i \wedge j)_{1\leq i,j\leq n} \in \mathrm{M}_n(k)$ est inversible. Pour cela, on introduit la matrice 'de divisibilité' $A = (a_{i,j})_{1\leq i\leq n} \in \mathrm{M}_n(k)$ définie par $a_{i,j} = 1$ si $i|j$ et $a_{i,j} = 0$ sinon. Comme A est triangulaire supérieure avec des 1 sur la diagonale, elle est inversible. Par ailleurs, la relation $\sum_{d|N} \varphi(d) = N$ (où $\varphi(d) = |(\mathbb{Z}/d)^\times|$ est l'indicatrice d'Euler) montre que si on note $\Phi = diag(\varphi(1), \ldots, \varphi(n))$ alors $A\Phi {}^t A = D$, donc

$$det(D) = \varphi(1) \cdots \varphi(n) \neq 0.$$

4. Notons $\mathbb{P}^2(\mathbb{F}_p) := \mathbb{F}_p^2 \setminus \{0\}/\mathbb{F}_p^\times$ l'ensemble des droites vectorielles de $\mathbb{F}_p^2$. Comme $|\mathbb{P}^2(\mathbb{F}_p)| = \frac{p^2-1}{p-1} = p+1$, l'action tautologique de $\mathrm{PGL}_2(\mathbb{F}_p)$ sur $\mathbb{P}^2(\mathbb{F}_p)$ définit un morphisme de groupes injectif $\mathrm{PGL}_2(\mathbb{F}_p) \hookrightarrow \mathcal{S}_{p+1}$. On conclut par l'argument usuel de cardinalité.

Exercice 2.2.5 :

1. En utilisant le Théorème 2.2.2 (4) et l'hypothèse $|\mathcal{S}_p(G)| > 1$, $p = 2, 3$ on obtient $|\mathcal{S}_2(G)| = 3$ donc $|\mathrm{Nor}_G(S_2)| = \frac{24}{3} = 8$ et $|\mathcal{S}_3(G)| = 4$ donc $|\mathrm{Nor}_G(S_3)| = \frac{24}{4} = 6$.
2. Comme $|\mathcal{S}_3(G)| = 4$, l'action de G par conjugaison sur $\mathcal{S}_3(G)$ définit bien un morphisme $\phi : G \to \mathcal{S}_4$. Comme $\ker(\phi) = \cap_{S\in\mathcal{S}_3(G)} \mathrm{Nor}_G(S)$, on a $|\ker(\phi)||6$. Mais si $3||\ker(\phi)|$ alors $\ker(\phi)$ contient un 3-Sylow de G donc tous les 3-Sylow de G (puisque ceux-ci sont conjugués dans G et que $\ker(\phi)$ est normal dans G). Mais alors $\ker(\phi)$ contiendrait déjà $3 \times 2 = 6$ éléments d'ordre exactement 3 : une contradiction.
3. Il reste à montrer que $\ker(\phi) = 1$ (on conclut ensuite par cardinalité). Sinon, $\ker(\phi) \in \mathcal{S}_2(G)$ et $\phi(G)/\ker(\phi) \subset \mathcal{S}_4$ est un sous-groupe d'indice 2 de $\mathcal{S}_4$; c'est donc $\mathcal{A}_4$. Mais $\mathcal{A}_4$ possède un unique 2-Sylow : Le sous-groupe $V_4 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ engendré par les doubles transpositions. Or pour tout $S \in \mathcal{S}_2(G)$ on a $\phi(S) \subset V_4$ donc $\phi(S) = V_4$ donc $S = \phi^{-1}(V_4)$. Cela contredit le fait que $|\mathcal{S}_2(G)| = 3$.

Exercice 2.2.9 :

1. Comme l'action de N par conjugaison sur $\mathcal{S}_p(N)$ est transitive (Théorème 2.2.2 (2)), pour tout $g \in G$ il existe $n(g) \in N$ tel que $g^{-1}Pg = n(g)^{-1}Pn(g)$ donc $gn(g)^{-1} \in \mathrm{Nor}_G(P)$.
2. $(a) \Rightarrow (b)$ est immédiat. (b) implique que $|\mathcal{S}_p(G)| = 1$, $p||G|$. Notons donc S_p l'unique p-Sylow de G pour $p||G|$. La multiplication dans G induit une application $\phi : \prod_{p||G|} S_p \to G$. Pour $x_p \in S_p, x_q \in S_q$, on a $[x_p, x_q] = (x_p x_q x_p^{-1})x_p \in S_p \cap S_q = 1$ donc $x_p x_q = x_q x_p$. Cela montre que ϕ est un morphisme de groupes. Si $\prod_{p||G|} x_p = 1$ alors, pour $p||G|$ quelconque on a $x_p = \prod_{p\neq q||G|} x_q$ est d'ordre à la fois une puissance de p et le ppcm de puissances de q pour $p \neq q||G|$. Donc $p = 1$. Cela montre que ϕ est injectif et on conclut par cardinalité que ϕ est un isomorphisme. Cela montre $(b) \Rightarrow (a)$.
Soit $p||G|$ et $P \in \mathcal{S}_p(G)$ tel que $\mathrm{Nor}_G(P) \subsetneq G$. Alors $\mathrm{Nor}_G(P)$ est contenu dans un sous-groupe maximal N de G. Par (c), N est normal dans G. Comme P est un p-Sylow de N, la question (1) montre que $G = N$: une contradiction. Cela montre $(c) \Rightarrow (b)$.

Supposons (a) et notons S_p l'unique p-Sylow de G pour $p||G|$. On a le diagramme commutatif suivant

$$\begin{array}{ccc} \prod_{p||G|} S_p \cap N & \xrightarrow{\phi} & N \\ \downarrow & & \downarrow \\ \prod_{p||G|} S_p & \xrightarrow{\simeq} & G \end{array}$$

Par commutativité du diagramme, ϕ est injectif. Comme pour tout $p||N|$ il existe $g \in G$ tel que $g^{-1}S_pg \cap N(= S_p \cap N) \in \mathcal{S}_p(N)$, on voit que

$$|N| = \prod_{p||N|} |S_p \cap N| = \prod_{p||G|} |S_p \cap N|$$

donc, ϕ est un isomorphisme. Mais, par maximalité de N il existe un unique $p||G|$ tel que $S_p \cap N \subsetneq S_p$ et $S_q \cap N = S_q$, $p \neq q|G|$. $(a) \Rightarrow (c)$ résulte donc du fait que tout sous-groupe maximal d'un p-groupe est normal.

Exemple 2.3.1 : $Grad(\mathcal{S}_4) = \mathbb{Z}/3 \times (\mathbb{Z}/2)^2$. $Gr(\mathbb{H}_8) = Gr(D_8) = (\mathbb{Z}/2)^3$. On notera que $\mathbb{H}_8$ et D_8 ne sont pas isomorphes puisque le premier contient 6 éléments d'ordre 4 et le second un seul.

Exercice 2.3.2 : On fait agir G sur lui-même par translation à gauche, ce qui définit un morphisme injectif $t : G \hookrightarrow \mathcal{S}(G)$ qui envoie $g \in G$ sur un produit de $\frac{|G|}{|\langle g \rangle|}$-cycles de longeur $|\langle g \rangle|$ à supports disjoints. En particulier, si $|G| = 2^r m$ avec $2 \not| m$ et si g un générateur d'un 2-Sylow, alors $t(g)$ est un produit de m cycles de longueur 2^r ; sa signature est donc $(-1)^{(2^r-1)m} = -1$. Cela montre que le morphisme $\epsilon \circ t : G \to \{\pm 1\}$ est surjectif. Comme $|G > 2|$, ce morphisme n'est pas injectif ; son noyau est donc un sous-groupe normal distinct de 1 et G. Comme $\mathbb{Z}/2$est cyclique, on en déduit qu'un groupe simple d'ordre pair est d'ordre divisible par 4 (en fait, un groupe simple non abélien est toujours d'ordre pair).

Exercice 2.3.5 :

1. De façon générale, si un groupe fini G contient un sous-group $H \subsetneq G$, l'action de G sur G/H induit un morphisme non trivial de groupes $G \hookrightarrow \mathcal{S}(G/H)$. Mais si G est simple, ce morphisme est nécessairement injectif. Dans notre cas, on aurait alors $60 = |G| \leq |\mathcal{S}_4| = 24$: une contradiction.
2. Par contre G contient un sous-groupe $H \subset G$ d'indice exactement 5. Sinon, par le Théorème 2.2.2 (4), comme $[G : \mathrm{Nor}_G(S_2)] \in \{1, 3, 5, 15\}$, on aurait forcément $|\mathcal{S}_2(G)| = 15$. En outre, si $S_2 \neq S_2' \in \mathcal{S}_2(G)$ on a nécessairement $S_2 \cap S_2' = 1$. Sinon, si $g \neq 1 \in S_2 \cap S_2'$, on aurait

$$S_2, S_2' \subsetneq \langle S_2, S_2' \rangle \subset \mathrm{Cen}_G(g)$$

donc $4||\mathrm{Cen}_G(g)||60$ et $|\mathrm{Cen}_G(g)| > 4$. Cela impose $[G : \mathrm{Cen}_G(g)] = 5$: une contradiction. Mais alors, G contient déjà $15 \times 3 = 45$ éléments d'ordre une puissance de 2. Et en considérant par exemple les 5-Sylow, on a $|\mathcal{S}_5(G)||12$ et $|\mathcal{S}_5(G)|| \equiv 1[5]$ donc $|\mathcal{S}_5(G)| \geq 6$, ce qui nous donne encore au moins $6 \times 4 = 24$ éléments d'ordre 5 : une contradiction.
3. Donc G contient un sous-groupe $H \subset G$ d'indice exactement 5, ce qui nous donne un morphisme injectif $\phi : G \hookrightarrow \mathcal{S}_5$ dont l'image est d'indice 2 dans $\mathcal{S}_5$ donc est nécessairement $\mathcal{A}_5$.

Exercice 2.3.8 : On distingue deux cas

1. $p = q$. Dans ce cas, $|G| = p^2$. En particulier, G est abélien (sinon $\{1\} \subsetneq Z(G) \subsetneq G$ et $G/Z(G)$ serait d'ordre p donc cyclique : une contradiction. Donc, par le théorème de classification des groupes finis, les seules possibilités sont $G = \mathbb{Z}/p^2$ ou $G = (\mathbb{Z}/p)^{\oplus 2}$.
2. Supposons $p < q$. On a alors un unique q-Sylow - S_q (nécessairement normal dans G). En effet, $|\mathcal{S}_q(G)||p$ et $|\mathcal{S}_q(G)| \equiv 1[q]$ implique $|\mathcal{S}_q(G)| = 1, p$ et $|\mathcal{S}_q(G)| = 1$ ou $> q$. Comme $p < q$, on a $|\mathcal{S}_q(G)| = 1$. Soit S_p un p-Sylow de G. Comme S_q est normal dans G, $S_p \cap S_q = \{1\}$ et $G = S_pS_q$, on en déduit que $G = S_q \rtimes S_p \simeq \mathbb{Z}/q \rtimes \mathbb{Z}/p$. Il reste à étudier les structure de produit semi-direct possibles. Celles-ci correspondent à des morphismes de groupes

$$\phi : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/q) \simeq (\mathbb{Z}/q)^\times \simeq \mathbb{Z}/(q-1)$$

(a) Si $p \not| q-1$, le seul morphisme est le morphisme trivial donc $G = \mathbb{Z}/q \times \mathbb{Z}/p$

(b) Sinon, l'évaluation en 1 fournit un isomorphisme entre $\mathrm{Hom}_{Grp}(\mathbb{Z}/p, \mathbb{Z}/(q-1))$ et le ($\mathbb{Z}/(q-1)$ est cyclique) sous-groupe d'ordre p de $\mathbb{Z}/(q-1)$. Donc soit $\phi(1) = 0$ et $G = \mathbb{Z}/q \times \mathbb{Z}/p$ soit $\neq \phi(1) =: u_\phi \in \mathbb{Z}/p \subset \mathbb{Z}/(q-1)$. Si $u_\phi \neq u_{\phi'}$, il existe $1 \leq k \leq p-1$ tel que $u_{\phi'} = k u_\phi$ donc $\phi' = k\phi$ et on vérifie que la bijection

$$\begin{array}{ccc} \mathbb{Z}/q \rtimes_{k\phi} \mathbb{Z}/p & \to & \mathbb{Z}/q \rtimes_{\phi} \mathbb{Z}/p \\ (\bar{n}, \bar{m}) & \to & (\bar{n}, k\bar{m}) \end{array}$$

est un morphisme de groupes. Donc, à isomorphisme près, il n'y a que deux structures possibles : $G = \mathbb{Z}/q \times \mathbb{Z}/p$ et $G = \mathbb{Z}/q \rtimes \mathbb{Z}/p$ (du coup, on ne précise pas ϕ). Par exemple si $p = 2$ et q est impair, $D_{2q} = \mathbb{Z}/q \rtimes \mathbb{Z}/2$ est le groupe diédral.

Exercice 2.3.9 : On a $255 = 3 \cdot 5 \cdot 17$. On a $|\mathcal{S}_{17}(G)| \equiv 1[17]$ et $|\mathcal{S}_{17}(G)||15$ donc, nécessairement $|\mathcal{S}_{17}(G)| = 1$. Notons S l'unique 17-Sylow de G ; il est cyclique et normal dans G et on donc une suite exacte courte

$$1 \to S \to G \to G/S \to 1$$

avec $|G/S| = 3 \cdot 5$. Comme $5 \not\equiv 1[3]$, l'exercice 2.3.8 montre que G/S est cyclique. Soit $g \in G$ un élément relevant un générateur de G/S. L'ordre de g est donc divisible par 15 et divise 255 : c'est soit 15, soit 255. Dans le second cas, on a gagné. Dans le premier cas, $\langle g \rangle \subset G$ est un complément de G/S dans G donc $G \simeq S \rtimes G/S$. Mais comme 15 est premier à $|\mathrm{Aut}_{Grp}(S)| = 16$ il n'y a pas de morphisme de groupe non-trivial $G/S \to \mathrm{Aut}_{Grp}(S)$ donc le produit semi-direct $G \simeq S \rtimes G/S$ est en fait un produit direct. On conclut par le lemme des restes chinois.

Exercice 2.3.16 :

1. L'implication $\Rightarrow$ est immédiate. Pour l'implication $\Leftarrow$, raisonnons par la contraposée. Si $H \subsetneq G$ il existe un sous-groupe maximal $M \subsetneq G$ tel que $H \subset M$. Mais alors, par définition de $\Phi(G)$, on a $H\Phi(G) \subset M \subsetneq G$.
2. Utilisons la caractérisation du Lemme 2.3.12 (4) (c). Soit S un p-Sylow de $\Phi(G)$. Comme $\Phi(G)$ est normal dans G, on a (Exercice 2.2.9 (1)) $G = \Phi(G)\mathrm{Nor}_G(S)$ et, par la question (1), $G = \mathrm{Nor}_G(S)$. Donc S est normal dans G donc *a fortiori* dans $\Phi(G)$.
3. Notons $\mathcal{M}(G)$ l'ensemble des sous-groupes maximaux de G. Comme G est un p-groupe fini, tout $M \in \mathcal{M}(G)$ est normal et d'indice p dans G donc $\Phi(G)$ se décrit comme le noyau du morphisme de groupes $G \to \prod_{M \in \mathcal{M}(G)} G/M \simeq (\mathbb{Z}/p)^{\mathcal{M}(G)}$. Cela montre déjà que $\Phi(G)$ contient $D(G)$ et les puissances p-ièmes des éléments de G. Inversement, notons $\tilde{D} := \langle D(G)G^p \rangle$, $V := G/\tilde{D}$ et $\pi : G \twoheadrightarrow V$ la projection canonique. Comme tout $M \in \mathcal{M}(G)$ contient $\Phi(G)$ donc $\tilde{D}$, $\pi : G \twoheadrightarrow V$ induit une bijection

$$\mathcal{M}(G) \tilde{\to} \mathcal{M}(V).$$

Mais comme les sous-groupes maximaux de V sont les hyperplans de V (vu comme $\mathbb{F}_p$-espace vectoriel) et que

$$\{0\} = \bigcap_{f \in V^*} \ker(f),$$

on en déduit :

$$\tilde{D} = \ker(\pi) = \bigcap_{f \in V^*} \ker(f \circ \pi) = \bigcap_{\overline{M} \in \mathcal{M}(V)} \pi^{-1}(\overline{M}) = \bigcap_{M \in \mathcal{M}(G)} M = \Phi(G).$$

Exercice 2.3.25 : Le cas où G est d'ordre une puissance d'un nombre premier est trivial. On procède par récurrence sur $|G|$.

1. Comme G est résoluble il contient un p-sous-groupe abélien élémentaire A caractéristique. Par hypothèse de récurrence, il existe un sous groupe $H \subset G$ contenant A tel que H/A soit un π-sous-groupe de Hall de G/A. Si $p \in \Pi$, H est un π-sous-groupe de Hall de G (observer que $[G/A : H/A] = [G : H]$ puisque $A \subset H$). Si $p \notin \pi$, par Schur-Zassenhaus (cas abélien) l'extension

$$1 \to A \to H \to H/A \to 1$$

se scinde et l'image du scindage est un π-sous-groupe de Hall de G.

2. Soit H, H' deux π-sous-groupes maximaux de G. Soit encore A un p-sous-groupe abélien élémentaire caractéristique de G. Si $p \in \pi$, HA est un π-sous-groupe de G contenant H donc, par maximalité, $HA = H$ *i.e.* $A \subset H$. De même, $A \subset K$. De plus $H/A, H'/A \subset G/A$ sont des π-sous-groupes maximaux donc, par hypothèse de récurrence, il existe $g \in G$ tel que $H' = H'A = gHg^{-1}A = gHAg^{-1} = gHg^{-1}$. Si $p \notin \pi$, fixons $H_1/A, H_1'/A \subset G/A$ des π-sous-groupes de Hall contenant $HA/A, H'A/A$ respectivement. Par hypothèse de récurrence, il existe $g \in G$ tel que $H_1'/A = gH_1g^{-1}/A$ donc, quitte à remplacer H par gHg^{-1}, on peut supposer que $H_1 = H_1'$. Mais par Schur-Zassenhaus (cas abélien) l'extension

$$1 \to A \to H_1 \to H_1/A \to 1$$

se scinde et H, H' fournissent deux compléments de A dans H_1. Toujours par Schur-Zassenhaus (cas abélien) on sait qu'il existe $g \in H_1$ tel que $H' = gHg^{-1}$.

Exercice 1.5.14 : On utilise la caractérisation (5) de la Proposition 1.5.13 *i.e.* en écrivant $\mathfrak{i} = Aa$, on doit montrer que pour tout $b \in A$ divisant a et pour tout morphisme de A-modules $u : Ab/Aa \to A/Aa$, on a

$$\begin{array}{ccccc} 0 & \longrightarrow & Ab/Aa & \longrightarrow & A/Aa \\ & & \forall u \downarrow & \swarrow_{\exists \bar{u}} & \\ & & A/Aa & & \end{array}$$

Pour cela, notons $\bar{t} := u(\bar{b})$. Comme $cb = a$ pour un certain $c \in A$, on a $0 = u(\bar{a}) = u(\bar{c}\bar{b}) = \bar{c}u(\bar{b}) = \bar{c}\bar{t}$ donc $ct \in Aa$ *i.e.* $ct = sa = scb$ pour un certain $s \in A$. Comme A est commutatif intègre, on en déduit $t = sb$ donc u est la restriction à Ab/Aa de l'homothétie de rapport $\bar{s}$.

4.3 Chapitre 3

Exercice 3.1.2 :

1. Il suffit d'écrire.
2. Comme M est semi-simple, il existe un sous-A-module $N \subset M$ tel que $M = Am \oplus N$. Notons $\pi : M \twoheadrightarrow Am$ la projection sur Am parallèlement à N ; c'est un morphisme de A-modules. Et

$$M \overset{\pi}{\twoheadrightarrow} Am \hookrightarrow M \in A'$$

donc $\phi \circ \pi = \pi \circ \phi$. En particulier, $\phi(m) = \phi(\pi(m)) = \pi(\phi(m)) \in Am$.

3. On applique la question (1) à $M := M^{\oplus r}$ et $\phi := \phi^{\oplus r} : M^{\oplus r} \to M^{\oplus r}$, $(m_1, \ldots, m_r) \to (\phi(m_1), \ldots, \phi(m_r))$. La seule chose à vérifier est que si $\phi \in \mathrm{End}_{\mathrm{End}_{A(M)}}(M)$ alors $\phi^{\oplus r} \in \mathrm{End}_{\mathrm{End}_{A(M^{\oplus r})}}(M^{\oplus r})$. Pour cela, décomposer M en somme directe de composantes isotypiques afin de se ramener au cas où M est simple. Pour la deuxième partie de la question (3), prendre pour $m_1, \ldots, m_r$ un système de générateurs de M comme A'-module.

Exercice 3.1.7 :

1. $Z(A)$ est un anneau commutatif donc il faut seulement montrer que tout élément non nul est inversible. Soit $0 \neq z \in Z(A)$. Alors $AzA = Az = zA$ est un idéal bilatère non nul de A donc c'est A tout entier. En particulier, $z \in A^\times$. Enfin, pour tout $a \in A$ $az = za$, équivaut à $z^{-1}a = az^{-1}$ donc $z^{-1} \in Z(A)$.
2. Soit $0 \neq \mathcal{I} \subset M_n(A)$ un idéal bilatère et $0 \neq M \in \mathcal{I}$. Il existe donc $1 \leq i, j \leq n$ tel que $M_{i,j} \neq 0$. En multipliant à gauche et à droite par des matrices de permutations, on se ramène à $aE_{1,1} \in \mathcal{I}$. Puis, en utilisant que $AaA = A$, on peut écrire $1_A = \sum_{1 \leq i \leq r} a_i a b_i$. D'où $E_{1,1} = \sum_{1 \leq i \leq r} (a_i E_{1,1})(aE_{1,1})(b_i E_{1,1}) \in \mathcal{I}$. En multipliant à nouveau gauche et à droite par des matrices de permutations, on obtient que $E_{i,j} \in \mathcal{I}$, $1 \leq i, j \leq n$.
3. Si A est de dimension finie sur $Z(A)$, pour tout A-module simple M (par exemple un idéal à gauche de dimension minimal sur $Z(A)$), on a $Z(A) \simeq Z(A)Id_M \subset A' := \mathrm{End}_A(M)$. On peut donc appliquer le lemme de densité (Exercice 3.1.2.3) pour obtenir un morphisme surjectif $L_- : A \twoheadrightarrow A''$. Comme le noyau de ce morphisme est un idéal bilatère, c'est un isomorphisme. Comme M est simple, par le lemme de Schur, A' est un anneau à division. On est donc ramené au cas où A est un anneau à division. Dans ce cas, on peut appliquer le lemme 3.1.5 au

$M_n(A)$-module tautologique $A^{\oplus n}$; il est fidèle et simple donc semislmple. Pour voir qu'il est simple, on procède comme en 2- : soit $0 \neq m \in M$, l existe $A \leq i \leq n$ tel que $m_i \neq 0$. Donc $E_{1,i}m = m_i e_1 \in M$ et comme A est à division, $e_1 \in M$. Donc $E_{i,1}e_1 = e_i \in M$, $1 \leq i \leq n$ *i.e.* $M = A^{\oplus n}$.

Exercice 3.1.8 :

1. Si $\mathcal{M}$ est un idéal à gauche maximal, $A/\mathcal{M}$ est un A-module simple d'idéal annulateur contenu dans $\mathcal{M}$ donc $\mathcal{M} \supset \cap_M Ann_A(M)$ et en prenant l'intersection sur tous les $\mathcal{M}$, $\mathcal{J}_A \supset \cap_M Ann_A(M)$. Inversement, si M est un A-module simple et $0 \neq m \in M$, le noyau $\mathcal{M}_m$ de $R_m : A \twoheadrightarrow Am = M$ est un idéal à gauche maximal de A et $Ann_A(M) = \cap_{m \in M} \mathcal{M}_m$ donc $\mathcal{J}_A \subset \cap_M Ann_A(M)$. Avec cette description de $\mathcal{J}_A$, on voit tout de suite que $\mathcal{J}_A$ est bilatère puisque les idéaux de la forme $Ann_A(M)$ sont bilatères.
2. Considérons la suite décroissante d'idéaux $\mathcal{J}_A \supset \mathcal{J}_A^2 \supset \cdots \supset \mathcal{J}_A^n \supset \cdots$. Comme A est artinien, cette suite stationne à partir d'un certain rang $n \geq 1$: $\mathcal{J}_A^n = \mathcal{J}_A^{n+1}$. Cela implique forcmment que $\mathcal{J}_A^n = 0$. En fait, c'est un cas particulier du lemme de Nakayama, qui dit que si M est un A-module de type fini tel que $\mathcal{J}_A M = M$ implique $M = 0$. En effet, sinon, soit $m_1, \ldots, m_r$ un système de générateurs *de longueur minimale* de M comme A-module. On peut écrire $m_1 = \sum_{1 \leq i \leq r} x_{i,1} m_i$ avec $x_{i,1} \in \mathcal{J}_A$, ou encore $(1 - x_{1,1})m_1 = \sum_{2 \leq i \leq r} x_{i,1} m_i$. Mais par définition de $\mathcal{J}_A$, $1 - x_{1,1}$ est inversible à gauche dans A (sinon, $A(1 - x_{1,1}) \subsetneq A$ serait contenu dans un idéal à gauche maximal $\mathcal{M}$ de A donc $1_A = (1_A - x_{1,1}) + x_{1,1} \in \mathcal{M}$: une contradiction), ce qui contredit la minimalité de r.
3. (a) $\Rightarrow$ (b) est immédiat. Soit $\mathcal{I} \subset A$ un nilidéal et M un A-module simple. Supposons qu'il existe $0 \neq a \in \mathcal{I}$ tel que $aM \neq 0$ *i.e.* il existe $m \in M$ tel que $am \neq 0$. Comme M est un A-module simple on a alors $Aam = M$ donc, en particulier, il existe $\alpha \in A$ tel que $\alpha am = m$. Mais $\alpha a \in \mathcal{I}$ donc il existe $n \geq 1$ tel que $(\alpha a)^n = 0$. Mais alors $m = (\alpha a)m = (\alpha a)^n m = 0$: une contradiction. Cela montre (b) $\Rightarrow$ (c). Enfin (c) $\Rightarrow$ (a) résulte de la question précédente.
4. Notons $\mathcal{E}$ l'ensemble des idéaux à gauche $I \subset A$ tel que A/I est semi-simple. Comme A est artinien, $\mathcal{E}$ possède un élément minimal I_0 pour $\subset$. De plus, pour tout $I \in \mathcal{E}$, on a un morphisme injectif de A-modules $A/(I_0 \cap I) \hookrightarrow A/I_0 \times A/I$, ce qui montre que $I \cap I_0 \in \mathcal{E}$ (tout sous-A-module d'un A-module semi-simple et toute somme directe de A-modules semi-simples est semisimple) donc $I \cap I_0 = I_0 \subset I$ par minimalité de I_0. Comme $\mathcal{E}$ contient les idéaux à gauche maximaux de A, on a $I_0 \subset \mathcal{J}_A$. Par ailleurs, A/I_0 est somme directe de A-modules simples donc, d'après la question (1), $\mathcal{J}_A A/I_0 = 0$ *i.e.* $\mathcal{J}_A \subset I_0$. Mais alors A semisimple $\Leftrightarrow I_0 = 0 \Leftrightarrow \mathcal{J}_A = 0$. Si A est commutatif, l'idéal $\sqrt{0}$ engendré par les éléments nilpotents de A est un nilidéal, qui est forcément égal à $\mathcal{J}_A$ d'après les questions (2) et (3). Donc A semisimple $\Leftrightarrow \mathcal{J}_A = 0 \Leftrightarrow \sqrt{0} = 0$. Soit $\mathcal{M}_1, \ldots, \mathcal{M}_r$ une suite finie d'idéaux à gauche maximaux tels que $0 = \mathcal{J}_A = \cap_{1 \leq i \leq r} \mathcal{M}_i$ (la finitude utilise que A est de dimension finie ; plus généralement, un anneau artinien n'a toujours qu'un nombre fini d'idéaux à gauche maximaux). Par le lemme Chinois, on a alors un isomorphisme d'anneaux

$$A(= A/\cap_{1 \leq i \leq r} \mathcal{M}_i) \tilde{\to} \prod_{1 \leq i \leq r} A/\mathcal{M}_i$$

Mais pour $i = 1, \cdots, r$, $A/\mathcal{M}_i$ est un corps commutatif, de dimension finie sur k *i.e.* une extension algébrique finie de k.
5. Cette question fait appel à un minimum de théorie de Galois. Tout d'abord, observons qu'on peut toujours remplacer K par une extension finie (utiliser les questions (2), (3)) donc supposer que K/k est galoisienne finie de groupe de Galois $G := \mathrm{Gal}(K|k)$. Supposons qu'il existe $0 \neq x \in \mathcal{J}_{A \otimes_k K}$. Soit $a_1, \ldots a_r$ une k-base de A. Alors $1 \otimes a_1, \cdots, 1 \otimes a_r$ est une K-base de $A \otimes_k K$ et on peut écrire

$$x = \sum_{1 \leq i \leq r} \lambda_i \otimes a_i$$

avec $\lambda_i \in K$. Pour tout $\lambda \in K$, $g \in G$ on a alors $g(\lambda x) \in\in \mathcal{J}_{A \otimes_k K}$ (puisque $g(\lambda x)$ est nilpotent) donc

$$\sum_{g \in G} g(\lambda x) = \sum_{g \in G, 1 \leq i \leq r} g(\lambda \lambda_i) \otimes a_i = \sum_{1 \leq i \leq r} \sum_{g \in G} g(\lambda \lambda_i) \otimes a_i = \sum_{1 \leq i \leq r} 1 \otimes \sum_{g \in G} g(\lambda \lambda_i) a_i \in A \cap \mathcal{J}_{A \otimes_k K}.$$

Mais $A \cap \mathcal{J}_{A \otimes_k K}$ est un idéal bilatère nilpotent de A donc est contenu dans $\mathcal{J}_A$. Or, par hypothèse, A est semi-simple donc $\mathcal{J}_A = 0$. On en déduit que pour tout $\lambda \in K$, $Tr_{K|k}(\lambda \lambda_i) = \sum_{g \in G} g(\lambda \lambda_i) = 0$, $i = 1, \ldots, r$. Mais comme la forme k-bilinéaire $K \times K \to k$, $(x, y) \to Tr_{K|k}(xy)$ est non-dégénérée puisque K/k est séparable,

cela implique $\lambda_i = 0$, $i = 1, \dots, r$. Un contre exemple dans le cas où K/k est non séparable est fourni par la $\mathbb{F}_p(X)$-algèbre $A = \mathbb{F}_p(X^{\frac{1}{p}})$ et l'extension $K = A$. En effet

$$\mathbb{F}_p(X^{\frac{1}{p}}) \otimes_{\mathbb{F}_p(X)} \mathbb{F}_p(X^{\frac{1}{p}}) = \mathbb{F}_p(X^{\frac{1}{p}})[Y]/\langle Y^p - X\rangle = \mathbb{F}_p(X^{\frac{1}{p}})[Y]/\langle (Y - X^{\frac{1}{p}})^p\rangle.$$

Exercice 3.1.9 :

1. Comme $\mathcal{J}_{k[G]}$ est un idéal bilatère nilpotent, Pour tout $x \in \mathcal{J}_{k[G]}$, xg_0 est nilpotent. donc la multiplication à gauche $L_{xg_0} : k[G] \to k[G]$ l'est aussi et est, en particulier, de trace nulle. Or en écrivant $x = \sum_{g\in G} x_g g$ on a $Tr(L_{xg_0}) = |G|x_{g_0^{-1}}$. Comme $|G|$ est inversible dans k, on a forcément $x = 0$.
2. Le point clef est de montrer que le seul $k[G]$-module simple est le $k[G]$-module trivial k. Soit donc M un $k[G]$-module simple et $0 \neq m \in M$. On peut considérer le sous-groupe additif $M^\circ \subset M$ engendré par $Gm \subset M$. C'est un groupe abélien fini stable en bijection avec $G/Stab_G(m)$, donc d'ordre une puissance de p. Autrement dit, M° est un $\mathbb{F}_p[G]$-module de $\mathbb{F}_p$-dimension finie. Mais dans ce cas, il est facile de montrer que fixe un vecteur non nul de M° (faire agir G sur $M^\circ \setminus \{0\}$ et utiliser l'équation aux classes pour montrer que $M^{\circ G} \neq 0$ ou, alternativement, invoquer le théorèmes de Sylow pour montrer que l'image de G agissant sur $M^\circ \simeq \mathbb{F}_p^{\oplus n}$ est conjuguée à un sous-groupe du p-Sylow 'standard' de $\mathrm{GL}_{\mathbb{F}_p}(M^\circ) \simeq \mathrm{GL}_n(\mathbb{F}_p)$). Mais alors, par (1) de l'Exercice 3.1.8
$$\mathcal{J}_{k[G]} = \ker(k[G] \overset{g\to 1}{\to} k) = \langle 1 - g\rangle = \oplus_{1\neq g\in G} k(1 - g) \subset k[G].$$

Exercice 3.2.2 : Il faut juste se placer dans des bases adaptées. On obtient $\chi_{\theta\oplus\theta'} = \chi_\theta + \chi_{\theta'}$, $\chi_{\theta\otimes\theta'} = \chi_\theta\chi_{\theta'}$, $\chi_{\theta^\vee} = \chi_\theta(-^{-1})$, $\chi_{\mathrm{Hom}(\theta,\theta')} = \chi_\theta(-^{-1})\chi_{\theta'}$ (on note parfois $\chi_\theta^\vee := \chi_\theta(-^{-1})$). L'anneau $R(G)$ est le quotient de $\mathrm{Mod}^\circ_{/K[G]} \times \mathrm{Mod}^\circ_{/K[G]}$ par $(\theta, \tau) \sim (\theta', \tau')$ si et seulement si $\theta \oplus \tau' = \theta' \oplus \tau$ (penser à la construction de $\mathbb{Z}$ à partir de $\mathbb{N}$).

Exercice 3.2.3 :

1. (a) Notons $M(x) := \frac{1}{|G|}\sum_{g\in G} \theta(gxg^{-1}) \in \mathrm{End}_K(V)$. On vérifie directement que $\theta(g_0) \circ M(x) = M(x) \circ \theta(g_0)$ pour tout $g_0 \in G$. Comme (V, θ) est simple et K algébriquement clos, le Lemme de Schur montre que $M(x)$ est une homothétie de rapport disons λ_x. On calcule λ_x en considérant la trace :
$$\lambda_x\chi_\theta(1) = Tr(\lambda_x Id) = Tr(M(x)) = \frac{1}{|G|}\sum_{g\in G} \chi_\theta(gxg^{-1}) = \frac{1}{|G|}\sum_{g\in G} \chi_\theta(x) = \chi_\theta(x).$$

   (b) Cela résulte de (a). Plus précisément :
$$\begin{aligned}\tfrac{1}{|G|^n}\textstyle\sum_{g_1,\dots,g_n\in G} \chi_\theta(g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1}y) &= Tr(\tfrac{1}{|G|^n}\textstyle\sum_{g_1,\dots,g_n\in G} \theta(g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1}y))\\ &= Tr(M(x_1)\cdots M(x_n)\theta(y))\\ &= \tfrac{\chi_\theta(x_1)\cdots\chi_\theta(x_n)}{\chi_\theta(1)^n}\chi_\theta(y).\end{aligned}$$

2. Pour chaque $i = 1, \dots, n$, fixons $x_i \in C_i$. De façon équivalente, on cherche le nombre de $(g_1, \dots, g_n) \in G^n/(\mathrm{Cen}_G(x_1) \times \cdots \times \mathrm{Cen}_G(x_n))$ tels que
$$g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1} = 1.$$
Or, on a vu que $\frac{1}{|G|}\chi_{reg} = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi(1)\chi$ était la fonction indicatrice de 1 sur $K[G]$. Donc, le cardinal que l'on cherche est
$$\frac{|G|^n}{|_{\mathrm{Cen}_G}(x_1)|\cdots|_{\mathrm{Cen}_G}(x_n)|}\sum_{g_1,\dots,g_n\in G^n}\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(1)\chi(g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1})$$
donc
$$|C_1|\cdots|C_n||G|^{n-1}\sum_{\chi\in\widehat{G}}\frac{\chi(1)}{|G|^n}\sum_{g_1,\dots,g_n\in G^n}\chi(g_1x_1g_1^{-1}\cdots g_nx_ng_n^{-1}) = |C_1|\cdots|C_n||G|^{n-1}\sum_{\chi\in\widehat{G}}\frac{\chi(C_1)\cdots\chi(C_n)}{\chi(1)^{n-2}}.$$

Exercice 3.2.4 :

1. On a clairement $\ker(\theta) \subset N_\theta$. Inversement, comme G est fini, $\theta(g) \in \mathrm{GL}(V)$ vérifie $\theta(g)^{|G|} = 1$ donc est diagonalisable et ses valeurs propres $\zeta_1(g), \ldots, \zeta_{n_\theta}(g)$ sont des racines $|G|$-ièmes de 1. On a donc

$$\chi_\theta(g) = \sum_{1 \leq i \leq n_\theta} \zeta_i(g) = n_\theta.$$

En prenant les parties réelles et imaginaires, on obtient

$$\sum_{1 \leq i \leq n_\theta} Re(\zeta_i(g)) = n_\theta, \ \sum_{1 \leq i \leq n_\theta} Im(\zeta_i(g)) = 0.$$

Mais comme $|Re(\zeta_i(g))| \leq 1$, $i = 1, \ldots, n_\theta$, cela force $Re(\zeta_i(g) = 1$, $i = 1, \ldots, n_\theta$ et donc, $Im(\zeta_i(g)) = 0$, $i = 1, \ldots, n_\theta$. Aurement dit $\zeta_i(g) = 1$, $i = 1, \ldots, n_\theta$.

2. Les ensembles de la forme

$$\bigcap_{(V,\theta) \in E} N_\theta = \bigcap_{(V,\theta) \in E} \ker(\theta)$$

sont bien des sous-groupes normaux de G d'après la question (1). Inversement, si $N \lhd G$ est un sous-groupe normal, notons E l'ensemble des $\mathbb{C}[G]$-modules simples de la forme $(V_\theta, \theta \circ p_N)$ où (V_θ, θ) décrit $\widehat{\mathbb{C}[G/N]}$ et $p_N : G \twoheadrightarrow G/N$ est la projection canonique. On a $N \subset \bigcap_{(V,\theta) \in E} N_\theta$ par construction. L'inclusion inverse vient du fait général (appliqué à N) suivant :

$$\bigcap_{(V,\theta) \in \widehat{\mathbb{C}[G]}} N_\theta = \ker(\chi_{reg}) = 1.$$

3. Immédiat.

Exercice 3.2.7 :

1. Notons $K := k(x)/k$ et soit $P \in k[X]$ le polynôme minimal de x sur k et $\alpha_1, \cdots, \alpha_n$ ses racines (elles sont deux à deux distinctes puisque K/k est séparable). On a donc

$$K \otimes_k \overline{k} = \overline{k}[T]/P \xrightarrow{\sim} \prod_{1 \leq i \leq n} k[T]/(T - \alpha_i) \xrightarrow{\sim} \overline{k}^n, \ \ \overline{Q} \to (Q(\alpha_1), \ldots, Q(\alpha_n))$$

Or on vérifie immédiatement que $T := Tr_{K/k} \otimes_k Id_{\overline{k}}$ est la trace du $\overline{k}$-endomorphisme $L_{x \otimes 1} : K \otimes_k \overline{k} \to K \otimes_k \overline{k}$, $y \otimes \lambda \to (xy) \otimes \lambda$. Modulo les isomorphismes ci-dessus, $T(a_1, \ldots, a_n) = a_1 + \ldots + a_n$ est non nulle. En particulier $Tr_{K/k} : K \to k$ est non nulle.

2. Puisque $x \to Tr_{\mathbb{F}_p}(L_x)$ est un morphisme de groupes $(\mathbb{F}_q, +) \to (\mathbb{F}_p, +)$, $\tau : (\mathbb{F}_q, +) \to (\mathbb{C}^\times, \times)$ est un morphisme de groupes *i.e.* un caractère irréductible puisque $(\mathbb{F}_q, +)$ est abélien. Il est non-trivial par (1).

3. On vérifie immédiatement que $\tau \circ R_-$ est un morphisme de groupes bien défini. De plus, $|\widehat{\mathbb{F}_q}| = |Cl(\mathbb{F}_q)| = |\mathbb{F}_q|$, la dernière égalité résultant du fait que $(\mathbb{F}_q, +)$ est abélien. Il suffit donc de montrer que $\tau \circ R_-$ est injective. Cela résulte encore de (1).

Exercice 3.2.10 :

1. *Cf.* exercice 3.2.4 (1).
2. On a, explicitement

$$\sum_{n \geq 0} (\chi_\theta, \chi_\tau^n)_G X^n = \frac{1}{|G|} \sum_{g \in G} \chi_\theta(g) \sum_{n \geq 0} (\chi_\tau(g) X)^n = \frac{1}{|G|} \sum_{g \in G} \frac{\chi_\theta(g)}{1 - \chi_\tau(g) X} \in \mathbb{C}(X).$$

Donc, en considérant les degrés, $\sum_{n \geq 0} (\chi_\theta, \chi_\tau^n)_G X^n \in \mathbb{C}[X]$ si et seulement si $\sum_{n \geq 0} (\chi_\theta, \chi_\tau^n)_G X^n = 0$, ce qui s'écrit encore

$$\sum_{1 \neq g \in G} \frac{\chi_\theta(g)}{1 - \chi_\tau(g) X} = -\frac{\chi_\theta(1)}{1 - \chi_\tau(1) X}.$$

Ce qui, d'après la question (1) et le fait que $\chi_\theta(1) \neq 0$ est impossible.

3. D'après la question (2), il y a nécessairement une infinité de n pour lesquels $(\chi_\theta, \chi_{\tau^{\otimes n}})_G = (\chi_\theta, \chi_\tau^n)_G \neq 0$ (pour la première égalité, *cf.* l'exercice 3.2.3 (2)).

1. *Cf.* exercice 3.2.7
2. On a, explicitement

$$\sum_{n\geq 0}(\chi_\theta, \chi_\tau^n)_G X^n = \frac{1}{|G|}\sum_{g\in G}\chi_\theta(g)\sum_{n\geq 0}(\chi_\tau(g)X)^n = \frac{1}{|G|}\sum_{g\in G}\frac{\chi_\theta(g)}{1-\chi_\tau(g)X} \in \mathbb{C}(X).$$

   Donc, en considérant les degrés, $\sum_{n\geq 0}(\chi_\theta, \chi_\tau^n)_G X^n \in \mathbb{C}[X]$ si et seulement si $\sum_{n\geq 0}(\chi_\theta, \chi_\tau^n)_G X^n = 0$, ce qui s'écrit encore

$$\sum_{1\neq g\in G}\frac{\chi_\theta(g)}{1-\chi_\tau(g)X} = -\frac{\chi_\theta(1)}{1-\chi_\tau(1)X}.$$

   Ce qui, d'après la question (1) et le fait que $\chi_\theta(1) \neq 0$ est impossible.
3. D'après la question (2), il y a nécessairement une infinité de n pour lesquels $(\chi_\theta, \chi_{\tau^{\otimes n}})_G = (\chi_\theta, \chi_\tau^n)_G \neq 0$.

Exercice 3.2.11 :

1. On vérifie immédiatement que $\chi_{\theta\otimes\theta'}(g, g') = \chi_\theta(g)\chi_{\theta'}(g')$.
2.

$$(\chi_{\theta\otimes\theta'}, \chi_{\theta\otimes\theta'})_{G\times G'} = \frac{1}{|G||G'|}\sum_{g\in G, g'\in G'}\chi_{\theta\otimes\theta'}(g, g')\chi_{\theta\otimes\theta'}(g^{-1}, g'^{-1}) = (\chi_\theta, \chi_\theta)_G(\chi_{\theta'}, \chi_{\theta'})_{G'}.$$

   En outre, comme le produit scalaire de deux caractères (quelconques) est toujours un entiers ≥ 0, on en déduit que $(\chi_{\theta\otimes\theta'}, \chi_{\theta\otimes\theta'})_G = 1$ si et seulement si $(\chi_\theta, \chi_\theta)_G = (\chi_{\theta'}, \chi_{\theta'})_{G'} = 1$.
3. On a $Cl(G\times G') = Cl(G)\times Cl(G')$ donc $|\widehat{G\times G'}| = |\widehat{G}||\widehat{G'}|$. Il suffit donc d'observer que si $(V_i, \theta_i) \in \mathrm{Mod}_{/K[G]}$, $(V_i', \theta_i') \in \mathrm{Mod}_{/K[G']}$, $i = 1, 2$ on a

$$(\chi_{\theta_1\otimes\theta_1'}, \chi_{\theta_2\otimes\theta_2'})_{G\times G'} = (\chi_{\theta_1}, \chi_{\theta_2})_G(\chi_{\theta_1'}, \chi_{\theta_2'})_{G'}$$

   (On peut aussi utiliser que $K[G\times G'] \simeq K[G]\otimes_K K[G']$ comme $K[G\times G']$-module).

Exercice 3.2.13 : La relation $|G|I_{r_G} = \Delta\mathcal{X}^t\mathcal{X}^\vee$ donne $|G|^{r_G} = |C_1|\cdots|C_{r_G}|\det(\mathcal{X})\det(\mathcal{X}^\vee)$. Mais $\det(\mathcal{X}^\vee) = \overline{\det(\mathcal{X})} = \epsilon\det(\mathcal{X})$, où ϵ est la signature de la permutation $C \to C^{-1}$ sur les colonnes de $\mathcal{X}$. D'où :

$$|G|^{r_G} = |C_1|\cdots|C_{r_G}|\epsilon(\det(\mathcal{X}))^2 = |C_1|\cdots|C_{r_G}||\det(\mathcal{X})|^2.$$

La deuxième égalité montre que $\epsilon = 1$ et la première que $\det(\mathcal{X})^2 = \frac{|G|^{r_G}}{|C_1|\cdots|C_{r_G}|}$.

Exercice 3.2.14 :

1. Notons $\mathcal{X}$ l'ensemble des couples $(g, x) \in G\times X$ tels que $gx = x$. Alors

$$\mathcal{X} = \bigsqcup_{g\in G}\{g\}\times X^g = \bigsqcup_{x\in X}\mathrm{Stab}_G(x)\times\{x\}.$$

   En prenant les cardinaux on obtient :

$$\sum_{g\in G}|X^g| = \sum_{C\in X/G}\sum_{x\in C}\frac{|G|}{|C|} = |X/G|.$$

2. Par définition, pour tout $g \in G$, $\chi_X(g) = |X^g|$ donc $(\chi_X, \mathbb{I}) = \frac{1}{|G|}\sum_{g\in G}\chi(g) = |X/G|$ d'après la question (1).
3. Considérons la représentation

$$V_{X\times X} = \bigoplus_{(x,y)\in X\times X} K(x, y)$$

de G. On a $V_{X\times X} = V_X \otimes V_X$ mais aussi $V_{X\times X} = V_{\Delta_X} \oplus V_{X\times X\setminus\Delta_X} = V_X \oplus V_{X\times X\setminus\Delta_X}$ donc

$$|X \times X/G| = (\chi_{X\times X}, \mathbb{I}) = |X \times X \setminus \Delta_X/G| + |X/G|.$$

Cela montre déjà (b) $\Leftrightarrow$ (c).
Par ailleurs, comme V_X est semisimple, on a également $V_X = V_{X,0} \oplus \mathbb{I}$ donc $\chi_{X,0} = \chi_X - 1$ et

$$(*)\ \ (\chi_{X,0}, \chi_{X,0}) = (\chi_X, \chi_X) - 2|X/G| + 1.$$

En outre, en simplifiant $V_X \otimes V_X = V_{X\times X}$ on obtient $V_{X,0} \otimes V_{X,0} \oplus V_{X,0} = V_{X\times X\setminus\Delta_X}$ donc

$$(**)\ \ (\chi_{X,0}, \chi_{X,0}^\vee) + (\chi_{X,0}, \mathbb{I}) = (\chi_{X,0}^2, \mathbb{I}) + (\chi_{X,0}, \mathbb{I}) = |X \times X \setminus \Delta_X/G|.$$

Enfin, remarquons que $(\chi_X^2, \mathbb{I}) = (\chi_X, \chi_X^\vee)$.

(a) $\Rightarrow$ (c) : Comme G agit non trivialement sur X, $V_{X,0} \in \widehat{K[G]}$ implique $(\chi_{X,0}, \mathbb{I}) = 0$ et $V_{X,0}^\vee \in \widehat{K[G]}$ donc $(\chi_{X,0}, \chi_{X,0}^\vee) = 0$ ou 1. En particulier, (*) donne

$$2|X/G| = (\chi_X, \chi_X) = (\chi_{X,0}, \chi_{X,0}) + 2(\chi_{X,0}, \mathbb{I}) + 1 = 2$$

donc $|X/G| = 1$et (**) donne $1 \geq (\chi_{X,0}, \chi_{X,0}^\vee) = |X \times X \setminus \Delta_X/G| \geq 1$ donc, nécessairement $(\chi_{X,0}, \chi_{X,0}^\vee) = |X \times X \setminus \Delta_X/G| = 1$.

(c) $\Rightarrow$ (a) : Si $|X \times X \setminus \Delta_X/G| = |X/G| = 1$ (*) donne $(\chi_{X,0}, \chi_{X,0}) + 1 = (\chi_X, \chi_X) = (\chi_{X,0}, \chi_{X,0}) + 2(\chi_{X,0}, \mathbb{I}) + 1$ donc nécessairement $(\chi_{X,0}, \mathbb{I}) = 0$ et (**) donne alors $(\chi_{X,0}, \chi_{X,0}^\vee) = 1$ *i.e.* $V_{X,0} \simeq V_{X,0}^\vee$ est irréductible.

4. Il suffit d'observer que $\mathcal{S}_n$ agit transitivement et doublement transitivement sur $\{1, \ldots, n\}$ puis utiliser (c) $\Rightarrow$ (a).

Exercice 3.2.15 : Un groupe fini G est abélien si et seulement si $K[G]$ est commutatif mais comme

$$K[G] \simeq \prod_{I \in \widehat{K[G]}} \mathrm{End}_K(I)$$

cela équivaut aussi à $n_I = 1$, $I \in \widehat{K[G]}$.

1. Comme un groupe cyclique est abélien, toutes ses représentations sont de K-dimension 1 *i.e.* ce sont des morphismes de groupes $\phi : \mathbb{Z}/n \to K^\times$. Mais il y a exactement n tels morphismes (rappelons que K est algébriquement clos de caractéristique 0 ou première à n), qui sont définis par $\phi_k(1) = \zeta_n^k$, où $\zeta_n \in K^\times$ est une racine primitive n-ième de 1. Donc il y a au plus n $K[\mathbb{Z}/n]$-modules simples : $\phi_1, \ldots, \phi_n$. Or on sait aussi que $|\widehat{\mathbb{Z}/n}| = |Cl(\mathbb{Z}/n)| = 1$ donc en fait les $\phi_1, \ldots, \phi_n$ sont exactement les $K[\mathbb{Z}/n]$-modules simples.
2. On peut utiliser la suite exacte $1 \to V_4 \to \mathcal{A}_4 \to \mathbb{Z}/3 \to 1$. Les éléments de $\widehat{\mathbb{Z}/3}$ fournissent déjà 3 caractères irréductibles de K-dimension 1. Par ailleurs $|\widehat{\mathcal{A}_4}| = |Cl(\mathcal{A}_4)| = 4$ (1, doubles transpositions W, deux classes de 3-cycles inverses l'une de l'autre C, C^{-1}). Il reste donc un dernier caractère irréductible à déterminer. La représentation correspondante est de dimension $\sqrt{|\mathcal{A}_4| - 3} = 3$. Pour déterminer ses valeurs, on peut utiliser la relation d'orthogonalité avec la première colonne.

	1	W	C	C^{-1}
$\mathbb{I}$	1	1	1	1
χ_2	1	1	j	j^2
χ_3	1	1	j^2	j
χ_4	3	-1	0	0

3. On peut utiliser la suite exacte $1 \to V_4 \to \mathcal{S}_4 \to \mathcal{S}_3 \to 1$. Les éléments de $\widehat{S}_3 = \mathbb{Z}/3 \rtimes \mathbb{Z}/2$ fournissent déjà 2 caractères irréductibles de K-dimension 1 : $\mathbb{I}$, ϵ et un caractères irréductible de K-dimension $\sqrt{4-2} = 2$:

χ. Par ailleurs $|\widehat{\mathcal{S}_4}| = |Cl(\mathcal{S}_4)| = 5$ (1, doubles transpositions W, les k-cycles C_k, $k = 2, 3, 4$). Mais on dispose aussi du caractère irréductible α de dimension 3 attaché à la représentation de permutation (exercice 3.2.14). Celui ci vaut $\alpha(g) = |\{1, 2, 3, 4\}^g| - 1$. Pour déterminer le dernier caractère, β, qui est aussi de dimension $\sqrt{|\mathcal{S}_4| - (2 + 4 + 9)} = 3$, on peut soit utiliser l'orthogonalité avec la première colonne, soit observer que c'est forcément $\epsilon\alpha$ en vérifiant que $||\epsilon\alpha||^2 = 1$, $(\epsilon\alpha, \alpha) = 0$.

	1	W	C_2	C_3	C_4
$\mathbb{I}$	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	2	2	0	-1	0
χ_4	3	-1	1	0	-1
χ_5	3	-1	-1	0	1

Exercice 3.2.16 :

1. Comme G est non abélien $Z(G) \neq G$ et comme G est un 2-groupe, $Z(G) \neq 1$. Donc $|Z(G)| = 2, 4$ mais si $|Z(G)| = 4$, $G/Z(G) \simeq \mathbb{Z}/2$ serait cyclique or on a vu que ce n'´tait pas possible. Donc $|Z(G)| = 2$ et $G/z(G)$ est d'ordre 4. Mais comme $G/Z(G)$ n'est pas cyclique, la seule possibilité est $G/Z(G) = \mathbb{Z}/2 \times \mathbb{Z}/2$.
2. Le quotient $G \twoheadrightarrow G/Z(G)$ donne déjà 4 représentations irréductibles non isomorphes de dimension 1 (celles de $G/Z(G)$). Donc
$$|G| = 8 = 4 + \Sigma,$$
où Σ est une somme de carrés d'entiers. Il n'y a que deux possibilités : $4 = \Sigma = 1 + 1 + 1 + 1$ mais alors G serait abélien ou $4 = \Sigma = 2^2$ donc G aurait une 5ème représentation irréductible de dimension 2.
3. Notons $Z(G) = \{1, z\}$ et a, b, c un syst`eme de représentants dans G des éléments $\neq 1$ de $G/Z(G)$. Les 5 classes de conjugaison de G sont alors : 1, z, a, az, b, bz et c, cz. On connait les caractères irréductibles de $G/Z(G)$, il reste juste χ_5 à d´terminer, ce qui se fait par exemple en utilisant l'orthogonalité avec la première colonne.

	1	z	a, az	b, bz	c, cz
$\mathbb{I}$	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Exercice 3.2.23 : Si G est non abélien et $p < q$, on a vu que $p|q - 1$ et G est le produit semi-direct non direct $\mathbb{Z}/q \rtimes \mathbb{Z}/p$. L'abélianisé de G est $\mathbb{Z}/p$, ce qui nous donne déjà p $K[G]$-modules simples de K-dimension 1. Les autres $K[G]$-modules simples sontde K-dimension p, q ou pq. Mais la relation

$$q^2 > p(q - 1) = n_1^2 + n_2^2 + \cdots$$

montre qu'il ne peut y avoir que les autres $K[G]$-modules simples sont de K-dimension p et qu'il y en a $\frac{q-1}{p}$.

Exercice 3.3.1 : Soit $(V, \theta) \in \widehat{K[G]}$ et soit $A \subset G$ un sous-groupe abélien. Alors $(V, \theta|_A)$ se décompose en somme directe de $n_\theta := \dim_K(V)$ $K[A]$-modules simples

$$V|_A = \oplus_{1 \leq k \leq n_\theta} L_k$$

Le morphisme de $K[G]$-modules $\mathrm{Ind}_A^G(L_k) \to V$ adjoint de l'injection canonique de $K[A]$-modules $L_k \hookrightarrow V|_A$ est non nul par construction et son image est un sous-$K[G]$-module de V. Donc, par simplicité de V, on a

$$\mathrm{Ind}_A^G(L_k) \twoheadrightarrow V$$

donc, en particulier $\dim_K(V) \leq \dim_K(\mathrm{Ind}_A^G(L_k)) = [G : A]$.

Exercice 3.3.2 :

1. On vérifie immédiatement que les matrices de la forme

$$\begin{pmatrix} 1 & \mathrm{b} \\ 0 & 1 \end{pmatrix},\ b \in \mathbb{F}_q$$

forment un sous-groupe normal N isomorphe à $\mathbb{F}_q$ de G. Le groupe G est d'ordre $(q-1)q$ et le quotient G/N est un groupe d'ordre $q-1$. Un scindage de la suite exacte courte

$$1 \to N \to G \xrightarrow{\pi} G/N \to 1$$

est donné par la restriction de π au sous-groupe des matrices de la forme

$$\begin{pmatrix} \mathrm{a} & 0 \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_q^\times.$$

Ce dernier est isomorphe à $\mathbb{F}_q^\times$ (donc cyclique). Comme G est non-abélien, on en déduit que G est le produit semi-direct

$$\mathbb{F}_q \rtimes \mathbb{F}_q^\times.$$

(Explicitement $(b,a)(b',a') = (b+ab', aa')$).

2. Observons d'abord que les classes de conjugaison de G sont $C_0 = \{(0,1)\}$, $C_a := \{(b,a) \mid b \in \mathbb{F}_q\}$, $0, 1 \neq a \in F_q$ et $C := \{(b,1) \mid b \in \mathbb{F}_q^\times\}$.
Soit $(Kw \simeq W, \chi) \in \widehat{K[N]}$, $\chi \neq \mathbb{I}$. On a $\mathrm{Ind}_N^G(\chi) = \oplus_{\alpha \in \mathbb{F}_q^\times} K\alpha \otimes w$. Pour calculer le caractère ψ de $\mathrm{Ind}_N^G(\chi)$, il suffit de considérer les éléments de la forme $(0,1)$, $(0,a)$, $0, 1 \neq a$ et $(1,b)$, $0 \neq b$. On a $\psi(0,1) = q-1$, $\psi(0,a) = 0$ et, comme $(b,1)(1,\alpha) = (0,\alpha)(\alpha^{-1}b, 1)$,

$$\psi(b,1) = \sum_{\alpha \in \mathbb{F}_q^\times} \chi(\alpha^{-1}b) + 1 - 1 = \sum_{b \in \mathbb{F}_q} \chi(b) - 1 = q(\chi, \mathbb{I})_N - 1 = -1.$$

On en déduit que ψ (donc $\mathrm{Ind}_N^G(\chi)$) ne dépend pas de χ et que

$$(\psi, \psi)_G = \frac{1}{q(q-1)}((q-1)^2 + (q-1)) = 1.$$

3. D'après ce qui précède, on a déjà $q-1$ $K[G]$-modules simples de dimension 1 (provenant de l'abélianisé $\mathbb{F}_q^\times$) et le $K[G]$-module simple $\mathrm{Ind}_N^G(\chi)$ de dimension $q-1$; on les a tous puisque G contient q classes de conjugaison.

Exercice 3.3.9 :

1. Notons $I_X \subset R(G)$ l'image de $\oplus_{H \in X} \mathrm{Ind}_H^G : \oplus_{H \in X} R(H) \to R(G)$ est un idéal de $R(G)$. Il suffit de vérifier que pour tout $H \in X$, $\chi \in \widehat{H}$, $\phi \in \widehat{G}$, $\mathrm{Ind}_H^G(\chi)\phi \in I_X$. Or, pour tout $g \in G$,

$$\mathrm{Ind}_H^G(\chi)(g)\phi(g) = \frac{1}{|H|} \sum_{g' \in G | g'^{-1} g g' \in H} \chi(g'^{-1} g g')\phi(g) = \frac{1}{|H|} \sum_{g' \in G | g'^{-1} g g' \in H} \chi(g'^{-1} g g')\phi(g'^{-1} g g') = \mathrm{Ind}_H^G(\chi \mathrm{Res}_G^H \phi) \in I_X$$

2. Notons $R_{\mathbb{Z}}(G) = \oplus_{\chi \in \widehat{G}} \mathbb{Z}\chi \subset R(G)$. Comme pour tout $\chi = \chi_V, \chi' = \chi_{V'} \in \widehat{G}$, $\chi\chi' = \chi_{V \otimes V'}$ est encore une combinaison linéaire à coefficients dans $\mathbb{Z}$ d'éléments de $\widehat{G}$, $R_{\mathbb{Z}}(G) \subset R(G)$ est encore un sous-anneau et comme pour tout $\chi = \chi_W \in \widehat{H}$, $\mathrm{Ind}_H^G(\chi) = \chi_{\mathrm{Ind}_H^G(W)}$ est encore une combinaison linéaire à coefficients dans $\mathbb{Z}$ d'éléments de $\widehat{H}$, $\mathrm{Ind}_H^G : \oplus_{H \in X} R(H) \to R(G)$ se restreint en un morphisme de $\mathbb{Z}$-modules Ind_H^G :

$\oplus_{H\in X}R_{\mathbb{Z}}(H)\to R_{\mathbb{Z}}(G)$. On note $I_{\mathbb{Z},X}\subset R_{\mathbb{Z}}(G)$ son image. Les mêmes considérations s'appliquent avec $\mathbb{Q}$ à la place de $\mathbb{Z}$. Comme X est stable par conjugaison, $G\setminus\cup_{H\in X}H$ est aussi stable par conjugaison. En particulier, tout $\phi\in I_{\mathbb{Q},X}$ s'annule sur $G\setminus\cup_{H\in X}H$. Mais si $I_{\mathbb{Q},X}=R_{\mathbb{Q}}(G)$, $\widetilde{1}\in I_{\mathbb{Q},X}$ ne s'annule sur aucun élément de G, ce qui montre que $G\setminus\cup_{H\in X}H=\emptyset$, d'où (ii) $\Rightarrow$ (i). Inversement, $\oplus_{H\in X}R(H)\to R(G)$ est surjective si et seulement si sa transposée $R(G)^\vee\to(\oplus_{H\in X}R(H))^\vee\simeq\oplus_{H\in X}(R(H)^\vee)$ est injective. Mais sur $R(G)$ et les $R(H)$, $H\in X$ on dispose des formes $\mathbb{Q}$-bilinéaires symétriques $(-,-)_G$, $(-,-)_H$, $H\in X$ qui donnent des identifications canoniques $R(G)\tilde{\to}R(G)^\vee$, $g\to(-,g)_G$ et $R(H)\tilde{\to}R(H)^\vee$, $h\to(-,h)_H$, $H\in X$. Pour $\chi\in\widehat{G}$, $(\mathrm{Ind}_H^G-,\chi)_G=(-,\mathrm{Res}_G^H(\chi))_H$, modulo ces isomorphismes $R(G)^\vee\to(\oplus_{H\in X}R(H))^\vee\simeq\oplus_{H\in X}(R(H)^\vee)$ s'identifie à $R(G)\to\oplus_{H\in X}R(H)$, $\chi\to\oplus_{H\in X}\mathrm{Res}_G^H(\chi)$, qui est clairement injective sous (i).

3. L'ensemble $X=\{\langle g\rangle\mid g\in G\}$ des sous-groupes cycliques de G vérifie les hypothèses de (2).

Exercice 3.3.10 :

1. C'est l'équation aux classes pour l'action de G sur lui-même par conjugaison. Si G est non commutatif, $G/Z(G)$ n'est pas cyclique et son centre est non trivial donc contient un sous groupe cyclique Z non trivial. On peut prendre pour A l'image inverse de Z dans G. En effet, A est bien normal dans G car si $z\in G$ relève dans G un générateur de Z on a pour tout $g\in G$, $p(gzg^{-1})=p(g)p(z)p(g)^{-1})=p(z)$ (puisque $z\in Z(G/Z(G))$ donc $gzg^{-1}\in A$.

2. Supposons d'abord V fidèle. Si $r=1$, l'image de A par $G\hookrightarrow\mathrm{GL}(V)$ est contenue dans le centre de $\mathrm{GL}(V)$ donc, *a fortiori*, A est contenu dans le centre de G, ce qui contredit la définition de A. Donc $r\geq 2$. Par ailleurs, comme A est abélien, on peut décrire explicitement $W_i^{\oplus m_i}$ comme le sous-K espace vectoriel

$$N_{\theta_i}:=\cap_{a\in A}\ker(\theta(a)-\theta_i(a)Id),$$

où $\theta:G\hookrightarrow\mathrm{GL}(V)$, $\theta_i:A\hookrightarrow\mathrm{GL}(W_i)=K^\times$, $i=1,\dots,r$. Comme en outre A est normal dans G, pour tout $g\in G$, $gN_{\theta_i}=N_{\theta_i(g^{-1}-g)}$ donc est isomorphe à l'un des N_{θ_j}, $j=1,\dots,r$. Cela définit un morphisme de groupes $G\to\mathcal{S}_r$, qui est transitif car V est un $K[G]$-module simple. En particulier, $m_1=\cdots=m_r=:m$ et $V|_A=\oplus_{1\leq i\leq r}g_iW_1^{\oplus m}$. Notons H le stabilsateur de 1 dans $G\to\mathcal{S}_r$. Clairement $Z(G)\subsetneq A\subset H\subsetneq G$ (le fait que la dernière inclusion est stricte vient du fait que G agit transtivement sur $\{1,\dots,r\}$ et $r\geq 2$). Alors $G/H\simeq\{1,\dots,r$ donc on peut supposer que $g_1,\dots,g_r$ est un système de représentants de G/H. En outre, $W:=W_1^{\oplus m}\in\widehat{K[H]}$ sinon, $W|_H=U_1\oplus U_2$ impliquerait $V=\oplus_{1\leq i\leq r}g_iW=\oplus_{1\leq i\leq r}g_iU_1\oplus\oplus_{1\leq i\leq r}g_iU_2$. Or, par construction, s$\oplus_{1\leq i\leq r}g_iU_1$ et $\oplus_{1\leq i\leq r}g_iU_2$ sont des sous-$K[G]$-modules, donc comme V est simple, on a forcément $U_1=0$ ou $U_2=0$. Enfin, le morphisme $\mathrm{Ind}_H^G(W)\to V$ adjoint de l'inclusion canonique $W\hookrightarrow V|_H$ est surjectif par construction et donc bijectif puisque $\dim(\mathrm{Ind}_H^G(W))=m[G:H]=mr=\dim(W)$.
Si on ne suppose plus V fidèle, on applique ce qui précède à $G/\ker(\theta)$ et on prend pour H l'image inverse dans G du groupe associé à $G/\ker(\theta)$, V ci-dessus (observer que $G/\ker(\theta)$ est encore non abélien puisque V est un $K[G/\ker(\theta)]$-module simple de K-dimension ≥ 2).

3. On procède par récurrence sur $|G|$. Si $|G|=p^s$ avec $s\geq 2$, G est abélien et on peut prendre $H=1$. Si $s\geq 3$. Si G est abélien, on peut encore prendre $H=1$. Sinon, soit $V\in\widehat{K[G]}$ de K-dimension ≥ 2 on peut appliquer la construction de (1), (2), pour obtenir H, W. Si W est de K-dimension 1, on a gagné. Sinon, on réitère l'argument avec H, W et on utilise la transitivité de l'induction :

$$K[G]\otimes_{K[H]}K[H]\otimes_{K[H']}W'=K[G]\otimes_{K[H']}W'.$$

Exercice 3.3.11 :

1. On applique le critère de Mackey. Tout d'abord $W_{\chi,\theta}:=\widetilde{\chi}\otimes\theta\circ p_\chi\in\widehat{G}_\chi$ car

$$(\widetilde{\chi}\otimes\theta\circ p_\chi\in\widehat{G}_\chi,\widetilde{\chi}\otimes\theta\circ p_\chi\in\widehat{G}_\chi)_{G_\chi}=\frac{1}{|G_\chi|}\sum_{a\in A,h\in H_\chi}\chi(a)\chi_\theta(h)\chi(h^{-1}a^{-1}h)\chi_\theta(h^{-1})=\frac{1}{|A||H_\chi|}\sum_{a\in A,h\in H_\chi}\chi(a)\chi_\theta(h)\chi(a^{-1})\chi_\theta($$

Il faut ensuite vérifier que pour tout $g\in G\setminus G_\chi$ les $K[G_\chi\cap gG_\chi g^{-1}]$-modules $\mathrm{Res}_{G_\chi}^{G_\chi\cap gG_\chi g^{-1}}W_{\chi,\theta}$ et $W_{\chi,\theta}^g$ sont disjoints. Pour cela, il suffit de vérifier que leurs restrictions au sous-groupe $A\subset G_\chi$ le sont. Or

$$(\chi_{W_{\chi,\theta}}|_A,W_{\chi,\theta}^g|_A)_A=\frac{1}{|A|}\sum_{a\in A}\chi(a)\chi_\theta(1)\chi(g^{-1}a^{-1}g)\chi_\theta(1)=\frac{\chi_\theta(1)^2}{|A|}(\chi,g\cdot\chi)_1=0$$

puisque $g\in G\setminus G_\chi$.

2. La condition suffisante est claire. Pour la condition nécessaire, le caractère de $V_{\chi,\theta}|_A$ est donné par

$$a \to \frac{\chi_\theta(1)}{|G_\chi|} \sum_{g\in G|g^{-1}ag\in G_\chi} \chi(g^{-1}ag)$$

donc est dans $\oplus_{g\in G} Kg\cdot\chi = \sum_{\psi\in H\cdot\chi} K\psi$. En particulier, $V_{\chi,\theta}|_A$ détermine $H\cdot\chi$. Mais on peut alors reconstruire $H_\chi := \mathrm{Stab}_G(\chi)$ puis θ comme le sous K-espace vectoriel H_χ-stable $\cap_{a\in A}\ker(\rho_{\chi,\theta}(a) - \chi(a)Id)$.

3. Soit $(V,\rho) \in \widehat{K[G]}$; on a $V|_A = \oplus_{\chi\in\widehat{A}} W_\chi$, où $W_\chi := \cap_{a\in A}\ker(\rho(a) - \chi(a)Id)$. Fixons $\chi \in \widehat{K[A]}$ tel que $W_\chi \neq 0$. Par construction, pour tout $g \in G$, $gW_\chi = W_{g\cdot\chi}$. En particulier, W_χ est un $K[H_\chi]$-module. Soit $(W,\theta) \subset W_\chi$ un sous-$K[H_\chi]$-module simple. Toujours par construction $G_\chi = AH_\chi$ stabilise (W,θ) (puisque $a \in A$ agit sur W_χ *via* $\chi(a)Id$) et (W,θ) est isomorphe à $W_{\chi,\theta}$. PAr adjonction, l'inclusion $W_{\chi,\theta} \subset V|_{G_\chi}$ induit donc un morphisme de $K[G]$-modules non nul $V_{\chi,\theta} \to V$; c'est donc un isomorphisme puisque $V_{\chi,\theta} \in \widehat{K[G]}$.

Chapitre 5

Annales 2014/2019

5.1 Examen 2014/2015

5.1.1 Enoncé

Avertissement.

Sont autorisés : le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*.

Les deux exercices et le problème sont indépendants. Le problème porte sur la théorie des représentations des groupes finis et utilise les techniques standard vues au chapite 3. Ll'exercice 1 discute le problème de la semisimplicité des $k[G]$-modules lorsque la caractéristique de k divise l'ordre de G et est donc plutôt à rattacher au chapitre 1. L'exercice 2 donne deux applications élémentaires de la théorie des Sylow à l'étude de la (non-)simplicité des groupes finis. Chacun des deux exercices est divisé en deux parties indépendantes.

Le sujet est peut-être long. Le barême sera adapté en conséquence.

Exercice 1 ('transfert' de semisimplicité) Soit A un anneau associatif unitaire. On a vu en cours que tout sous-A-module et tout A-module quotient d'un A-module semisimple était encore un A-module semisimple. Donc la semisimplicité se transfère aux sous-A-modules et aux A-modules quotients. Pour d'autres types de construction, en général, les choses sont assez compliquées même si on peut quand-même parfois faire des observations intéressantes. Voici deux exemples dans le cas où $A = k[G]$ avec G un groupe fini et k un corps de caractéristique $p > 0$ *divisant* l'ordre de G.

1. Transferts aux sous-groupes normaux : Soit $N \subset G$ un sous-groupe normal et V un $k[G]$-module de k-dimension finie.
   (a) Expliquer pourquoi V contient toujours un sous-$k[G]$-module simple.
   (b) Montrer que si V est semisimple comme $k[G]$-module alors il est semisimple comme $k[N]$-module. On observera qu'il suffit de traiter le cas où V est un $k[G]$-module simple et on pourra essayer de montrer que dans ce cas, V est somme de sous-$k[N]$-modules simples.
   (c) Montrer que la réciproque est vraie si p ne divise pas $[G : N]$. (Indication : penser à la preuve de la semi-simplicité de $k[G]$ lorsque la caractéristique de k est 0 ou ne divise pas $|G|$).

2. Transfert au produit tensoriel : Supposons $p = 2$, k fini et $G = SL_2(k) \subset GL_2(k)$ le groupe des matrices 2×2 inversibles sur k de déterminant 1. On note $V(d)$ le k-espace vectoriel des polynomes homogènes de degré d en

X, Y sur k. C'est donc un k-espace vectoriel de k-base X^iY^{d-i}, $i = 0, \ldots, d$ et de k-dimension $d+1$. On munit $V(d)$ de la structure de $k[G]$-module induite par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} X = aX + bY, \begin{pmatrix} a & b \\ c & d \end{pmatrix} Y = cX + dY.$$

(a) Montrer que $V(1)$ est un $k[G]$-module simple.

(b) Montrer que $V'(2) = kX^2 \oplus kY^2$ est un sous-$k[G]$-module de $V(2)$.

(c) Montrer que $V(2)/V'(2) \simeq k$ est le $k[G]$-module trivial. En déduire que si $|k| \geq 4$ la suite exacte courte de $k[G]$-modules

$$0 \to V'(2) \to V(2) \to V(2)/V'(2) \to 0$$

n'est pas scindée. En particulier, $V(2)$ n'est pas un $k[G]$-module semisimple.

(d) Construire un morphisme surjectif (naturel) de $k[G]$-modules

$$V(1) \otimes_k V(1) \twoheadrightarrow V(2).$$

(e) Déduire de ce qui précède que $V(1) \otimes_k V(1)$ n'est pas un $k[G]$-module semisimple.

Remarque : La construction ci-dessus s'étend à un corps k fini de caractéristique $p > 0$ comme suit : $V(d)$ est un $k[G]$-module simple si $d < p$, $V'(p) = kX^p \oplus kY^p \subset V(p)$ est un sous-$k[G]$-module, $V(p)/V'(p) \simeq V(p-2)$ mais sauf si $k = \mathbb{F}_2$, la suite exacte courte de $k[G]$-modules

$$0 \to V'(p) \to V(p) \to V(p)/V'(p) \to 0$$

n'est jamais scindée. Par contre, on a toujours des morphismes surjectifs de $k[G]$-modules

$$V(d_1) \otimes_k \cdots \otimes_k V(d_m) \twoheadrightarrow V(p)$$

pour $1 \leq d_i \leq p-1$ tels que $d_1 + \cdots + d_m = p$. En fait, Serre a montré (Inventiones Math. 116, p. 513-530, 1994) que si $V_1, \ldots V_m$ sont des $k[G]$-modules semisimples tels que $\sum_{1 \leq i \leq m} dim_k(V_i) < p$ alors $V_1 \otimes_k \cdots \otimes_k V_m$ est encore un $k[G]$-module semisimple.

Exercice 2 (simplicité et Sylow) Soit G un groupe fini. Si X est un ensemble fini, on note $\mathcal{S}(X)$ le groupe des permutations de X et $\mathcal{A}(X) \subset \mathcal{S}(X)$ le sous-groupe alterné (*i.e.* le groupe des permutations paires).

1. (Simplicité et 2-Sylow)

   (a) En utilisant le morphisme injectif de G induit par l'action à gauche de G sur lui-même par translation

   $$\begin{array}{rccc} L: & G & \hookrightarrow & \mathcal{S}(G) \\ & g & \to & h \to gh \end{array}$$

   montrer que, si G est simple distinct de $\mathbb{Z}/2$ alors $L(G) \subset \mathcal{A}(G)$.

   (b) En déduire que, si G est simple distinct de $\mathbb{Z}/2$ alors les 2-Sylow de G ne peuvent être cycliques.

   (c) Vérifier que pour $n \geq 5$, les 2-Sylow du groupe alterné $\mathcal{A}_n$ ne sont pas cycliques. Sont-ils abéliens ?

   (d) Montrer qu'un groupe G d'ordre pair tel que $\frac{|G|}{2}$ est impair n'est jamais simple.

2. (Simplicité et nombre de p-Sylow)

   (a) Supposons G simple non abélien. Soit p un nombre premier divisant l'ordre de G et s_p le nombre de p-Sylow de G. Montrer que $|G|$ divise $s_p!$.

   (b) Montrer qu'un groupe d'ordre 10000000 ne peut pas être simple.

Problème (caractères irréductibles des groupes non abéliens d'ordre pq)

Soit $p \neq q$ deux nombres premiers distincts avec $p < q$. Soit G un groupe non abélien d'ordre pq.

1. Rappeler rapidement pourquoi, à isomorphisme près, il y a au plus un groupe non abélien G d'ordre pq - que l'on notera donc $G_{p,q}$ dans la suite - et rappeler quelle est sa structure.

Dans la suite, pour fixer les notations, on se donnera $z_p \in G_{p,q}$ un élément d'ordre p, $z_q \in G_{p,q}$ un élément d'ordre q et on posera $C_p := \langle z_p \rangle$, $C_q := \langle z_q \rangle$.

2. Déterminer le groupe dérivé et l'abélianisé de $G_{p,q}$; en déduire les représentations de dimensions 1 de $G_{p,q}$.
3. Calculer le nombre et la dimension des représentations irréductibles de $G_{p,q}$.
4. L'objectif de cette question est de déterminer les classes de conjugaison de $G_{p,q}$.
   (a) Déterminer le nombre de classes de conjugaison de $G_{p,q}$.
   (b) Expliquer pourquoi les éléments z_p^k, $k = 0, \ldots, p-1$ sont deux à deux non conjugués. Déterminer le cardinal de leurs classes de conjugaison.
   (c) Montrer que C_q est réunion disjointe de classes de conjugaison de $G_{p,q}$. Montrer que l'action par conjugaison de $G_{p,q}$ sur C_q se factorise *via* $G_{p,q} \twoheadrightarrow G_{p,q}/C_q \simeq C_p$. En déduire que C_q est réunion disjointe de $1 + \frac{q-1}{p}$ classes de conjugaison dont on déterminera le cardinal.
   (d) Conclure.
5. On considère l'action de C_p sur $\widehat{C}_q$ définie par

$$\begin{array}{lll} C_p \times \widehat{C}_q & \to & \widehat{C}_q \\ (z, \chi) & \to & z \cdot \chi = \chi(z^{-1} - z). \end{array}$$

   Déterminer le nombre d'orbites.
6. Soit $\chi \in \widehat{C}_q$ et $\tilde{\chi} := \mathrm{Ind}_{C_q}^{G_{p,q}}$ son induite.
   (a) Montrer que le caractère de $\tilde{\chi}$ ne dépend que de la C_p-orbite de χ (pour l'action définie à la question précédente).
   (b) Montrer que si χ n'est pas le caractère trivial alors $\tilde{\chi}$ est irréductible et que $\tilde{\chi} \simeq \tilde{\chi}'$ si et seulement si χ et χ' sont dans la même C_q-orbite.
7. Conclure en dressant la liste des représentations irréductibles de $G_{p,q}$.
8. Tracer la table des caractères du groupe non-abélien d'ordre 14.
9. Tracer la table des caractères du groupe non-abélien d'ordre 21.

5.1.2 Corrigé

Exercice 1 ('transfert' de semisimplicité) Soit A un anneau associatif unitaire. On a vu en cours que tout sous-A-module et tout A-module quotient d'un A-module semisimple était encore un A-module semisimple. Donc la semisimplicité se transfère aux sous-A-modules et aux A-modules quotients. Pour d'autres types de construction, en général, les choses sont assez compliquées même si on peut quand-même parfois faire des observations intéressantes. Voici deux exemples dans le cas où $A = k[G]$ avec G un groupe fini et k un corps de caractéristique $p > 0$ *divisant* l'ordre de G.

1. (a) Tout sous $k[G]$-module de V de k-dimension minimale et > 0 est nécessairement simple.
   (b) Il suffit de traiter le cas où V est un $k[G]$-module simple. En particulier, V contient un sous-$k[N]$ -module simple non trivial. Soit $W \subset V$ la somme de tous les $k[N]$-sous-modules simple de V ; c'est un sous-$k[N]$-module semisimple non trivial de V. De plus, comme N est normal dans G, pour tout $V' \subset V$ sous-$k[N]$-module et pout tout $g \in G$ l'application $g\cdot : V' \tilde{\to} gV'$, $v' \to g \cdot v'$ est un isomorphimse de $k[N]$-modules. Cela montre que W est un sous-$k[G]$-module de V donc, comme V est un $k[G]$-module simple, on a $W = V$ donc V est un $k[N]$-module semisimple.

(c) Soit $W \subset V$ un sous-$k[G]$-module. C'est *a fortiori* un sous-$k[N]$-module. Mais comme V est un $k[N]$-module semisimple, il existe un sous-$k[N]$-module $U \subset V$ tel que

$$V = W \oplus U.$$

Notons $p : V \to W$ la projection sur W parallèlement à U ; c'est un morphisme de $k[N]$-modules. Posons

$$\tilde{p} := \frac{1}{[G:N]} \sum_{\overline{g} \in G/N} g^{-1} p(g \cdot -).$$

Notons que c'est bien défini car pour tout $g \in G$, $n \in N$ on a $(ng)^{-1}p(ngv) = g^{-1}n^{-1}np(gv) = g^{-1}p(gv)$, la première égalité résultant du fait que p est un morphisme de $k[N]$-modules. On vérifie alors que $\tilde{p}$ est un projecteur d'image W et un morphisme de $k[G]$-module ; $\ker(\tilde{p})$ est donc un sous-$k[G]$-module de V et $V = W \oplus \ker(\tilde{p})$.

2. (a) $V(1) = kX \oplus kY$ et la matrice dans la base (X, Y) d'un élément

$$M = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in G$$

opérant sur $V(1)$ est M elle-même. En particulier, $V(1)$ est simple (sinon G serait conjugué à un sous-groupe de $SL_2(k)$ de la forme

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

ce qui est impossible, par exemple ici pour des raisons de cardinalité.

(b) Il suffit d'observer que pour

$$M = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in G$$

on a $MX^2 = (aX + bY)^2 = a^2X^2 + b^2Y^2 \in V'(2)$ et $MY^2 = (cX + dY)^2 = c^2X^2 + d^2Y^2 \in V'(2)$.

(c) Avec les notations de la question précédente, on a

$$MXY = (aX + bY)(cX + dY) = acX^2 + (ad + bc)XY + bdY^2 \equiv XY \ [V'(2)]$$

(noter que $ad + bc = ad - bc = 1$). Supposons que $|k| \geq 4$. Si la suite exacte courte de $k[G]$-modules

$$0 \to V'(2) \to V(2) \to V(2)/V'(2) \to 0$$

était scindée, $V(2)$ contiendrait un vecteur fixé par G, que l'on peut toujours supposer de la forme $w = \alpha X^2 + \beta Y^2 + XY$. Donc, pour tout

$$M = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in G$$

on devrait avoir

$$\begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + \begin{pmatrix} ac \\ bd \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

En particulier, si $b = c = 0$ et $d = a^{-1}$ avec $a^2 \neq 1$ (c'est ici qu'on utilise $|k| \geq 4$:)), on doit avoir $(a^2 - 1)\alpha = 0$, $(a^{-2} - 1)\beta = 0$ donc $\alpha = \beta = 0$. Mais XY n'est clairement pas fixé par G non plus (voir calcul dans la question précédente).

(d) Il suffit de considérer l'application k-biliéaire surjective $f : V(1) \times V(1) \to V(2)$ définie par $f(X_1X_2) = X^2$, $f(X_1, Y_2) = f(Y_1, X_2) = XY$, $f(Y_1, Y_2) = Y^2$. Elle se factorise en une application k-linéaire surjective $V(1) \otimes_k V(1) \twoheadrightarrow V(2)$, dont on vérifie immédiatement que c'est un morphisme de $k[G]$-modules.

(e) Si $V(1) \otimes_k V(1)$ était un $k[G]$-module semisimple alors tous ses $k[G]$-modules quotients le seraient aussi. Or ce n'est pas le cas de $V(2)$ comme on l'a vu dans la question (2) (c).

Exercice 2 (simplicité et Sylow)

1. (a) Comme $\mathcal{A}(G)$ est normal dans $\mathcal{S}(G)$, $L(G) \cap \mathcal{A}(G)$ est normal dans $L(G)$. Comme G donc $L(G)$ est simple, on a donc $L(G) \cap \mathcal{A}(G) = 1$ ou $L(G) \cap \mathcal{A}(G) = L(G)$. Dans le premier cas, on aurait alors $G \xrightarrow{\sim} L(G) \subset \mathcal{S}(G) \xrightarrow{\epsilon} \mathbb{Z}/2$ injectif (ici, $\epsilon : \mathcal{S}(G) \to \mathbb{Z}/2$ dsigne la signature), ce qui contredit l'hypothèse sur G. Donc $L(G) \cap \mathcal{A}(G) = L(G)$ ou encore $L(G) \subset \mathcal{A}(G)$.

   (b) Ecrivons $|G| = 2^r m$ avec m impair. Soit S un 2-Sylow de G. Supposons S cyclique de générateur s. Alors $L(s)$ est un produit de m cycles de longueur 2^r à support deux à deux disjoints. En particulier, $\epsilon(L(s)) = (-1)^m = -1$, ce qui contredit le fait que $L(s) \in \mathcal{A}(G)$.

   (c) Supposons $n \geq 4$. Un 2-Sylow S de $\mathcal{A}_n$ est d'ordre 2^r avec $r \geq \frac{n}{2}$ (si n pair) ou $\frac{n-1}{2}$ (si n impair). Si S était cyclique, $\mathcal{A}_n$ contiendrait donc un élément d'ordre $2^{\frac{n}{2}}$ ou $2^{\frac{n-1}{2}}$ selon le cas. Mais en considérant la décomposition en produit de cycles à supports deux à deux disjoints d'un élément d'ordre une puissance de 2 dans $\mathcal{S}_n$, on voit que celui-ci est d'ordre $\leq n$ (le cas dégalité n'étant possible que si n est lui-même une puissance de 2). Pour $n \geq 4$, on a toujours $2^{\frac{n-1}{2}} > n$. En fait, les 2-Sylow de $\mathcal{A}_n$ ne sont pas non plus abéliens dès que $n \geq 6$ (pour $n = 5$, on a $s_5 = 4$ donc les 2-Sylow sont de la forme $(\mathbb{Z}/2)^2$). Il suffit de le montrer pour $n = 6$ (puisque pour $n \geq 6$, $\mathcal{A}_n$ contient des copies de $\mathcal{A}_6$ donc les 2-Sylow de $\mathcal{A}_n$ contiennent des copies des 2-Sylow de $\mathcal{A}_6$ comme on l'a vu en cours). Dans ce cas $s_2 = 8$. Soit S un 2-Sylow de $\mathcal{A}_6$. Comme S est un 2-groupe, les orbites de S opérant sur $\{1, \ldots, 6\}$ sont de longueur 2 ou 4. De plus S opère sans point fixe sinon S serait contenu dans une copie de $\mathcal{A}_5$. Or les 2-Sylow de $\mathcal{A}_5$ sont d'ordre 4. Les orbites ne peuvent pas non plus toutes être de longueur 2 sinon les éléments de S seraient tous d'ordre 2. Mais $\mathcal{A}_6$ contient des éléments d'ordre 4 (les produits d'une transposition et d'un 4-cycle à supports disjoints). Donc S a une orbite de longueur 2 - que l'on peut toujours supposer être $\{1, 2\}$ quitte à renuméroter et une orbite de longueur 4 - $\{3, 4, 5, 6\}$. Comme S contient des éléments d'ordre 4, S contient forcément $(12)(3456)$ et son inverse $(12)(3654)$ et ce sont les seuls éléments d'ordre 4 que S peut contenir. De plus, le centralisateur de $(12)(3456)$ dans $\mathcal{A}_6$ est $\langle (12)(3456) \rangle \subsetneq S$ (en effet, si $\sigma \in \mathcal{A}_6$ centralise $(12)(3456)$, il stabilise forcément $\{1, 2\}$ et $\{3, 4, 5, 6\}$ donc σ s'écrit $\sigma = (12)^a(3456)^b$ car le stabilisateur d'un n-cycle c_n dans $\mathcal{S}_n$ est $\langle c_n \rangle$), ce qui montre que S n'est pas abélien (en fait $S = D_8$ puisque des deux groupes non-abéliens d'ordre 8, c'est celui qui n'a que 2 éléments d'ordre 4).

   (d) Si G est un groupe fini d'ordre pair tel que $\frac{|G|}{2}$ est impair alors ses 2-Sylow sont d'ordre 2 donc cycliques. D'après la question (1) (b) G ne peut être simple.

2. (a) Soit p un nombre premier divisant l'ordre de G, $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G et $s_p := |\mathcal{S}_p(G)|$. On sait que G agit transitivement par conjugaison sur $\mathcal{S}_p(G)$ d'où un morphisme de groupes non trivial

$$G \to \mathcal{S}(\mathcal{S}_p(G)) \simeq \mathcal{S}_{s_p}.$$

   Si on suppose G simple non abélien, ce morphisme est nécessairement injectif donc G s'identifie à un sous-groupe de $\mathcal{S}_{s_p}$ et on a bien $|G| | s_p!$.

   (b) $|G| = 10^7 = 2^7 5^7$. Si G était simple, on aurait $10^7 | s_5!$. Mais $s_5 \equiv 1[5]$ et $s_5 | 2^7$. Cela impose $s_5 = 16 = 2^4$. Mais 10^7 ne divise pas 16! car la puissance de 5 dans la décomposition de 16! en produit de nombres premiers est 3 (seuls 5, 10 et 15 contribuent).

Problème (caractères irréductibles des groupes non abéliens d'ordre pq)

Soit $p \neq q$ deux nombres premiers distincts avec $p < q$. Soit G un groupe non abélien d'ordre pq.

1. *Cf.* Cours.

2. Comme $G_{p,q} = C_q \rtimes C_p \twoheadrightarrow C_p$, on a déjà $DG_{p,q} \subset C_q$. Mais comme C_q est simple, on a soit $DG_{p,q} = C_q$ soit $DG_{p,q} = 1$ mais comme $G_{p,q}$ n'est pas abélien, on a forcément $1 \subsetneq DG_{p,q}$. Donc $DG_{p,q} = C_q$ et $G_{p,q}^{ab} \simeq C_p$. Les représentations irréductibles de dimension 1 de $G_{p,q}$ sont donc les morphismes

$$\phi_k \circ \pi : G_{p,q} \to \mathbb{C}^\times,\ k = 0, \ldots, p-1,$$

   où $\pi : G_{p,q} \twoheadrightarrow G_{p,q}/C_q \simeq C_p$ est la projection canonique et, si on se fixe un générateur z_p de C_p, $\phi_k : C_p \to \mathbb{C}^\times$ est la représentation définie par $\phi_k(z_p) = e^{\frac{k2i\pi}{p}}$, $k = 0, \ldots, p-1$.

3. On a déjà p représentations irréductibles de dimension 1. Notons pour l'instant r le nombre de représentations irréductibles de G de dimension > 1 et $n_1, \dots, n_r$ la dimension de ces représentations. On a

$$pq = p + n_1^2 + \cdots + n_r^2$$

ou encore $p(q-1) = n_1^2 + \cdots + n_r^2$. On sait aussi que les n_i divisent $|G_{p,q}| = pq$; les seules possibilités sont donc $n_i = p, q$ ou pq. Mais comme $p < q$, on a $p(q-1) < q(q-1) < q^2 < (pq)^2$. Donc, finalement, la seule possibilité est $n_i = p$, $r = \frac{q-1}{p}$ (où l'on retrouve que p divise $q-1$ ...).

4. (a) On a $|\widehat{G_{p,q}}| = |Cl(G_{p,q})| = p + \frac{q-1}{p}$. On peut isoler comme d'habitude la classe de conjugaison de 1. Il reste donc $p - 1 + \frac{q-1}{p}$ autres classes de conjugaison à déterminer.

   (b) Si z_p^k et z_p^l étaient conjugués dans $G_{p,q}$ alors leurs images $\bar{z}_p^k$, $\bar{z}_p^l$ seraient conjuguées dans $G_{p,q}/C_q$. Mais comme $G_{p,q}/C_q \simeq C_p$ est abélien, cela signifierait que $\bar{z}_p^k = \bar{z}_p^l$ donc $z_p^k = z_p^l$ (puisque $C_p \subset G_{p,q} \twoheadrightarrow G_{p,q}/C_q$ est un isomorphisme). Notons B_k la classe de conjugaison de z_p^k, $k = 1, \dots, p-1$. On peut la calculer explicitement. On sait que $z_p^{-1} z_q z_p = z_q^u$ pour un certain $1 \neq u \in (\mathbb{Z}/q)^\times$ donc

$$(z_q^i z_p^j) z_p^k (z_q^i z_p^j)^{-1} = z_q^i z_p^k z_q^{-i} = z_p^k z_p^{-k} z_q^i z_p^k z_q^{-i} = z_p^k z_q^{u^k i - i}.$$

   Or comme $1 \neq u$, on a encore $u^k - 1 \in (\mathbb{Z}/q)^\times$ donc l'application $i \to u^k i - i$ est un automorphisme de $\mathbb{Z}/q$. D'où :

$$B_k = \{z_p^k z_q^l \mid l = 0, \dots, q-1\}$$

   et B_k est de cardinal q.

   (c) Comme C_p est normal dans $G_{p,q}$, C_p est réunion (disjointe) de classes de conjugaison. Fixons un générateur z_q de C_q et un générateur z_p de C_p. Tout élément de $G_{p,q}$ s'écrit alors de façon unique sous la forme $z_q^l z_p^k$, $k = 0, \dots, p-1$, $l = 0, \dots, q-1$. En particulier, on voit que les classes de conjugaison des éléments de C_q dans $G_{p,q}$ sont en fait les orbites de C_p agissant par conjugaison sur C_q. De telles orbites sont de longueur 1 ou p. Mais un élément $1 \neq z \in C_q$ est un générateur de C_q donc ne peut commuter avec z_p (sinon $G_{p,q}$ serait abélien) ; son orbite sous l'action par conjugaison de C_p est donc de longueur p. En conclusion, C_q est réunion de (disjointe) la classe $I := \{1\}$ et de $\frac{q-1}{p}$ classes de conjugaison $A_1, \dots, A_{\frac{q-1}{p}}$ de cardinal p.

   (d) On a donc la classe de 1, $p-1$ classes $B_1, \dots, B_{p-1}$ de cardinal q et $\frac{q-1}{p}$ classes $A_1, \dots, A_{\frac{q-1}{p}}$ de cardinal p. Le compte y est puisque

$$1 + (p-1)q + \frac{q-1}{p} p = pq.$$

5. Rappelons que comme C_q est abélien, $|\widehat{C}_q| = |C_q| = q$. La encore, comme p est premier, une orbite de C_p agissant sur $\widehat{C}_q$ est de longueur 1 ou p. Soit $\chi \in \widehat{C}_q$ tel que $C_p \cdot \chi = \{\chi\}$. Comme C_q est abélien, χ est de la forme $\chi(z_q^k) = \omega_q^k$ pour une certaine racine q-ième de l'unité ω_q. Donc $C_p \cdot \chi = \{\chi\}$ signifie que $\omega_q^u \chi(z_q^u) = \chi(z_p^{-1} z_q z_p) = \chi(z_q) = \omega_q$ *i.e.* $\omega_q^{u-1} = 1$ mais comme $1 \neq u$, cela impose $\omega_q = 1$ donc χ est le caractère trivial. En conclusion, on a une seule orbite de longueur 1, celle du caractère trivial et $\frac{q-1}{p}$ orbite de longueur p.

6. Soit $\chi \in \widehat{C}_q$ et

$$\tilde{\chi} := \mathrm{Ind}_{C_q}^{G_{p,q}} = \bigoplus_{0 \leq i \leq p-1} z_p^i \otimes_{\mathbb{C}[C_q]} \chi$$

   son induite. Par abus de notation, on note encore $\tilde{\chi}$ le caractère de $\tilde{\chi}$.

   (a) On a

$$z_q^k z_p^l z_p^i = z_p^{l+i} z_p^{-(l+i)} z_q^k z_p^{l+i} = z_p^{l+i} z_q^{u^{l+i} k}$$

   donc

$$\begin{array}{lll} \tilde{\chi}(z_q^k z_p^l) & = p & \text{si } k = l = 0\,; \\ & = 0 & \text{si } l \neq 0\,; \\ & = \sum_{0 \leq i \leq p-1} z_p^i \cdot \chi(z_q^k) = \sum_{\phi \in C_p \cdot \chi} \phi(z_q^k) & \text{si } l = 0,\ k \neq 0. \end{array}$$

   En particulier, $\tilde{\chi}$ ne dépend que de $C_p \cdot \chi$.

(b) Supposons χ et χ' distincts du caractère trivial. Calculons

$$\begin{aligned}(\tilde{\chi},\tilde{\chi}')_{G_{p,q}} &= \frac{1}{pq}(p^2+\sum_{1\leq k\leq q-1}\tilde{\chi}(z_q^k)\tilde{\chi}'(z_q^{-k}))\\ &= \frac{1}{pq}(p^2+\sum_{1\leq k\leq q-1}\sum_{\phi\in C_p\cdot\chi,\phi'\in\mathbb{C}_p\cdot\chi'}\phi(z_q^k)\phi'(z_q^{-k}))\\ &= \frac{1}{pq}(p^2+\sum_{\phi\in C_p\cdot\chi,\phi'\in\mathbb{C}_p\cdot\chi'}\sum_{1\leq k\leq q-1}\phi(z_q^k)\phi'(z_q^{-k}))\\ &= \frac{1}{pq}(p^2+\sum_{\phi\in C_p\cdot\chi,\phi'\in\mathbb{C}_p\cdot\chi'}(q(\phi,\phi')_{C_q}-1)\end{aligned}$$

Or $(\phi,\phi')_{C_q}=\delta_{\phi,\phi'}$ donc si χ et χ' ne sont pas dans la même C_p-orbite, on a $(\tilde{\chi},\tilde{\chi}')_{G_{p,q}}=\frac{1}{pq}(p^2-p^2)=0$, si χ et χ' sont dans la même C_p-orbite, on a $(\tilde{\chi},\tilde{\chi}')_{G_{p,q}}=\frac{1}{pq}(p^2+p(q-1)-(p^2-p))=1$.

7. On a trouvé p représentations irréductibles de dimension 1 (question (2)) et $\frac{q-1}{p}$ représentations irréductibles de dimension p (question (6)). On les a donc toutes d'après la question (3).

8.

	1	B_1	A_1	A_2	A_3
$\mathbb{I}$	1	1	1	1	1
χ_2	1	-1	1	1	1
χ_3	2	0	$2cos(\frac{2\pi}{7})$	$2cos(\frac{4\pi}{7})$	$2cos(\frac{8\pi}{7})$
χ_4	2	0	$2cos(\frac{8\pi}{7})$	$2cos(\frac{2\pi}{7})$	$2cos(\frac{4\pi}{7})$
χ_5	2	0	$2cos(\frac{4\pi}{7})$	$2cos(\frac{8\pi}{7})$	$2cos(\frac{2\pi}{7})$

9.

	1	B_1	B_2	A_1	A_2
$\mathbb{I}$	1	1	1	1	1
χ_2	j	j^2	1	1	1
χ_3	1	j^2	j	1	1
χ_4	3	0	0	ω	$1-\omega$
χ_5	3	0	0	$1-\omega$	ω

où $\omega=\zeta_7+\zeta_7^2+\zeta_7^4$ et $1-\omega=\zeta_7^3+\zeta_7^5+\zeta_7^6$ avec $\zeta_7=e^{\frac{2i\pi}{7}}$.

5.2 Examen 2015/2016

5.2.1 Enoncé

Avertissement.

Sont autorisés : le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*. L'examen est long ; le barême sera adapté en conséquence.

Exercice 1 (Quelques remarques sur les groupes d'ordre 8)

On rappelle que si G est un groupe fini et p un nombre premier, on note $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G.

1. Déterminer - à isomorphisme près - tous les groupes abéliens d'ordre 8.

2. L'objectif de cette question est de déterminer tous les groupes non-abéliens d'ordre 8. Soit G un groupe non-abélien d'ordre 8.

   (a) Montrer que $|Z(G)| = 2$ et que $G/Z(G) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. On notera $z \in Z(G)$ le générateur de $Z(G)$.

   (b) Montrer que G contient un élément d'ordre 4 - disons a. Notons $C := \langle a \rangle \subset G$ le sous-groupe engendré par a. Montrez que C est normal dans G et que $a^2 = z$.

   (c) D'après (2.b), G est donc une extension de la forme

   $$(*) \quad 1 \to C \to G \to \mathbb{Z}/2 \to 1$$

   i. Si $(*)$ se scinde, montrer qu'il n'y a qu'un seule classe d'isomorphisme pour G. Fixons $b \in G \setminus C$ d'ordre 2. On peut écrire

   $$G = \{b^i a^j,\ i = 0, 1,\ j = 0, 1, 2, 3\}.$$

   En particulier, on doit avoir $b^i a^j b^k a^l = b^{f(i,j,k,l)} a^{g(i,j,k,l)}$. Déterminer les fonctions f, g et lister les éléments de G en fonction de leur ordre.

   ii. Supposons maintenant que $(*)$ ne se scinde pas. Fixons $b \in G \setminus C$. Quel est l'ordre de b ? Montrer que $bab^{-1} = za$. En notant $c := ab$, montrer que G est exactement l'ensemble

   $$\{1, z, a, b, c, az, bz, cz\}.$$

   Construire la table de multiplication de G et lister les éléments de G en fonction de leur ordre.

3. (Plongement des groupes non-abéliens d'ordre 8 dans un groupe symétrique). On note D_8 et $\mathbb{H}_8$ les groupe construits dans les questions (2.c.i) et (2.c.ii) respectivement.

   (a) Montrer que $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ et donner la structure du 2-Sylow V de $\mathcal{A}_4$.

   (b) Soit $S \in \mathcal{S}_2(\mathcal{S}_4)$. Expliquer pourquoi $V \subset S$. En déduire la structure des 2-Sylow de $\mathcal{S}_4$.

   (c) Peut-on plonger $\mathbb{H}_8$ dans $\mathcal{S}_4$? Déterminer le plus petit entier $n \geq 1$ tel que l'on peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_n$.

Exercice 2 (Table des caractères de $\mathcal{A}_5$)

1. (Classes de conjugaison)

   (a) Montrer que les doubles transpositions (resp. les 3-cycles) sont conjuguées dans $\mathcal{A}_5$.

(b) Montrer qu'il y a deux classes de conjugaison de 5-cycles dans $\mathcal{A}_5$.

(c) Montrer que si $c \in \mathcal{A}_5$ est un 5-cycle alors c et c^2 ne sont pas conjugués mais que c et c^{-1} le sont.

(d) Lister les classes de conjugaison de $\mathcal{A}_5$ et pour chaque classe, donner son cardinal et un représentant.

(e) Déterminer le nombre de représentations irréductibles de $\mathcal{A}_5$.

2. On considère la représentation de $\mathcal{A}_5$ sur $V = \mathbb{C}^{\oplus 5}$ par permutation des coordonnées. Montrer que

$$V = \mathbb{I} \oplus V_{std},$$

où $\mathbb{I}$ désigne la représentation triviale. Vérifer, en calculant le caractère χ_{std} de V_{std}, que V_{std} est irréductible.

3. Notons X l'ensemble des parties à deux éléments de $\{1, 2, 3, 4, 5\}$. On considère la représentation de $\mathcal{A}_5$ sur

$$V = \bigoplus_{x \in X} \mathbb{C}x \simeq \mathbb{C}^{\oplus 10}$$

définie par $\sigma \cdot \{x, y\} = \{\sigma(x), \sigma(y)\}$. Vérifer, en calculant le caractère χ_5 de V, que $V = \mathbb{I} \oplus V_{std} \oplus V_5$ et que V_5 est irréductible.

4. Déterminer les dimensions des représentations irréductibles de $\mathcal{A}_5$.

5. Compléter la table des caractères de $\mathcal{A}_5$ en exploitant les relations d'orthogonalité (lignes et colonnes).

6. Notons V l'une des deux représentations irréductibles autre que $\mathbb{I}$, V_{std} et V_5. Déterminer la dimension de la représentation produit tensoriel $V_5 \otimes V$ et sa décomposition en somme directe de sous-représentations irréductibles.

Exercice 3 (Lemme de Brauer-Nesbitt)

Soit k un corps et A une k-algèbre (associative unitaire). Pour tout $a \in A$ et A-module M, on note $a_M \in \mathrm{End}_k(M)$ l'endomorphisme de k-espace vectoriel défini par $a_M(m) = a \cdot m$, $m \in M$. On note également $A'_M := \mathrm{End}_A(M)$, $A''_M := \mathrm{End}_{A'_M}(M)$.
Soit M, N deux A-modules *semisimples* de k-dimension finie. L'objectif de cet exercice est de montrer que les conditions suivantes sont équivalentes :

(i) pour tout $a \in A$, a_M et a_N ont même polynôme caractéristique
(ii) M et N sont isomorphes comme A-modules.

Ecrivons

$$M = \bigoplus_{P \in \widehat{A}} P^{\oplus \mu_P}, \quad N = \bigoplus_{P \in \widehat{A}} P^{\oplus \nu_P}$$

pour les décompositions en somme directe de sous-Amodules simples de M et N (ici, $\widehat{A}$ désigne un système de représentants des classes d'isomorphismes de A-modules simples). Notons également $V := M \oplus N$.

1. Rappeler pourquoi le morphisme canonique de k-algèbres

$$\begin{array}{ccc} A & \to & A''_V \\ a & \to & a_V \end{array}$$

est bien défini et surjectif.

2. En déduire que pour tout $P \in \widehat{A}$ il existe $e_P \in A$ tel que $(e_P)_V \in \mathrm{End}_k(V)$ est la projection sur $P^{\oplus \mu_P + \nu_P}$ parallèlement à
$$\bigoplus_{P \neq Q \in \widehat{A}} Q^{\oplus \mu_Q + \nu_Q}.$$

3. Calculer les polynômes caractéristiques de $(e_P)_M$ et $(e_P)_N$.

4. Conclure.

5. On considère l'action du groupe symétrique $\mathcal{S}_n$ sur la k-algèbre des polynômes à n indéterminées $k[X_1, \ldots, X_n]$ définie par $\sigma \cdot P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ et on note $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \subset k[X_1, \ldots, X_n]$ la sous-k-algèbre des polynômes symétriques *i.e.* tels que $\sigma \cdot P = P$, $\sigma \in \mathcal{S}_n$. Supposons que k est de *caractéristique* 0. On admettra que les polynômes de Newton :
$$\Sigma_k := \sum_{1 \leq i \leq n} X_i^k,\ k = 1 \ldots, n$$
forment une base de transcendance de la k-algèbre $k[X_1, \ldots, X_n]^{\mathcal{S}_n}$. Cela signifie que pour tout $P \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ il existe un unique polynôme $Q_P \in k[T_1, \ldots, T_n]$ vérifiant
$$P = Q_P(\Sigma_1, \ldots, \Sigma_n).$$
En utilisant cela, montrer que les conditions suivantes sont équivalentes :

(i) pour tout $a \in A$, a_M et a_N ont même trace
(ii) M et N sont isomorphes comme A-modules.

ENGLISH VERSION

Exercise 1 (A few remarks about groups of order 8)

We recall that for a finite group G and a prime p we let $\mathcal{S}_p(G)$ denote the set of p-Sylow of G.

1. List - up to isomorphism - all the abelian groups of order 8.

2. Let G be a non-abelian group of order 8.

   (a) Show that $|Z(G)| = 2$ and that $G/Z(G) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. Let $z \in Z(G)$ denote the generator of $Z(G)$.

   (b) Show that G contains an element of orderc4 - say a. Let $C := \langle a \rangle \subset G$ denote the subgroup generated by a. Show that C is normal in G and that $a^2 = z$.

   (c) According to (2.b), G is an extension of the form

   $$(*)\ \ 1 \to C \to G \to \mathbb{Z}/2 \to 1$$

   i. If $(*)$ splits, show that G is unique up to isomorphism. Fix $b \in G \setminus C$ of order 2. One can write

   $$G = \{b^i a^j,\ i = 0, 1,\ j = 0, 1, 2, 3\}.$$

   In particular, one should have $b^i a^j b^k a^l = b^{f(i,j,k,l)} a^{g(i,j,k,l)}$. Determine the maps f, g and list the elements of G according to their order.

   ii. Suppose now that $(*)$ does not split. Fix $b \in G \setminus C$. What is the order of b? Show that $bab^{-1} = za$. Writing $c := ab$, show that G is the set

   $$\{1, z, a, b, c, az, bz, cz\}.$$

   Construct the multiplication table of G and list the elements of G according to their order.

3. (Embedding non-abelian groups of order 8 into a symmetric group). Let D_8 and $\mathbb{H}_8$ denote the groups constructed in questions (2.c.i) et (2.c.ii) respectively.

   (a) Show that $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ and give the structure of the 2-Sylow V of $\mathcal{A}_4$.

   (b) Let $S \in \mathcal{S}_2(\mathcal{S}_4)$. Explain why $V \subset S$. Deduce from this the isomorphism class of the 2-Sylow of $\mathcal{S}_4$.

   (c) Can we embed $\mathbb{H}_8$ in $\mathcal{S}_4$? Determine the smallest integer $n \geq 1$ such that $\mathbb{H}_8$ can be embedded into $\mathcal{S}_n$.

Exercise 2 (Character table of $\mathcal{A}_5$)

1. (Conjugacy classes)

   (a) Show that the double transpositions (resp. the 3-cycles) are conjuguated in $\mathcal{A}_5$.

   (b) Show that there exists two conjugacy classes of 5-cycles in $\mathcal{A}_5$.

(c) Show that if $c \in \mathcal{A}_5$ is a 5-cycle then c and c^2 are not conjugated but c and c^{-1} are.

(d) Give the list of conjugacy classes in $\mathcal{A}_5$ and for each class, give its cardinality and a representative.

(e) Give the number of irreducible representations of $\mathcal{A}_5$.

2. Consider the representation $V = \mathbb{C}^{\oplus 5}$ of $\mathcal{A}_5$ by permutation of the coordinates. Show that

$$V = \mathbb{I} \oplus V_{std},$$

where $\mathbb{I}$ denotes the trivial representation. Compute the character χ_{std} of V_{std} and check that V_{std} is irreducible.

3. Let X denote the set of (unordered) pairs in $\{1, 2, 3, 4, 5\}$ and consider the representation of $\mathcal{A}_5$ on

$$V = \bigoplus_{x \in X} \mathbb{C}x \simeq \mathbb{C}^{\oplus 10}$$

defined by $\sigma \cdot \{x, y\} = \{\sigma(x), \sigma(y)\}$. Compute the character χ_5 of V and check that $V = \mathbb{I} \oplus V_{std} \oplus V_5$ with V_5 irreducible.

4. Give the dimensions of the irreducible representations of $\mathcal{A}_5$.

5. Using the orthogonality relations (lines and columns), complete the character table of $\mathcal{A}_5$.

6. Let V denote one of the two irreducible representations other than $\mathbb{I}$, V_{std} and V_5. Give the dimension of the tensor product representation $V_5 \otimes V$ as well as its decomposition into direct sum of irreducible subrepresentations.

Exercise 3 (Brauer-Nesbitt Lemma)

Let k be a field and A a k-algebra (associative, with unit). For every $a \in A$ and A-module M, let $a_M \in \mathrm{End}_k(M)$ denote the endomorphism of k-vector space defined by $a_M(m) = a \cdot m$, $m \in M$. Set also $A'_M := \mathrm{End}_A(M)$, $A''_M := \mathrm{End}_{A'_M}(M)$. Let M, N be two A-modules *semisimples* of finie k-dimension. The aim of this exercise is two show that the following two conditions are equivalent.

(i) for every $a \in A$, a_M and a_N have the same characteristic polynomial
(ii) M and N are isomorphic as A-modules.

Write

$$M = \bigoplus_{P \in \widehat{A}} P^{\oplus \mu_P}, \quad N = \bigoplus_{P \in \widehat{A}} P^{\oplus \nu_P}$$

for the decompositions into direct sum of simple A-submodules of M and N (here, $\widehat{A}$ denotes as usual a system of representatives of the isomorphism classes of simple A-modules). Set also $V := M \oplus N$.

1. Recall why the canonical morphism of k-algebras

$$\begin{array}{ccc} A & \to & A''_V \\ a & \to & a_V \end{array}$$

is well-defined and surjective.

2. Deduce from (1) that for every $P \in \widehat{A}$ there exists $e_P \in A$ such that $(e_P)_V \in \mathrm{End}_k(V)$ is the projection onto $P^{\oplus \mu_P + \nu_P}$ with respect to the direct sum decomposition

$$V = (P^{\oplus \mu_P + \nu_P}) \bigoplus \Big(\bigoplus_{P \neq Q \in \widehat{A}} Q^{\oplus \mu_Q + \nu_Q} \Big).$$

3. Compute the characteristic polynomials of $(e_P)_M$ and $(e_P)_N$.

4. Conclude.

5. Consider the action of the symmetric group $\mathcal{S}_n$ on the k-algebra $k[X_1, \ldots, X_n]$ of polynomial with n indeterminates defined by $\sigma \cdot P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ and write $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \subset k[X_1, \ldots, X_n]$ for the k-subalgebra of symmetric polynomials *i.e.* those satisfying $\sigma \cdot P = P$, $\sigma \in \mathcal{S}_n$. Assume k has *caracteristic* 0. We will admit that the Newton polynomials :

$$\Sigma_k := \sum_{1 \leq i \leq n} X_i^k,\ k = 1 \ldots, n$$

are a transcdence basis for the k-algebra $k[X_1, \ldots, X_n]^{\mathcal{S}_n}$. This means that for every $P \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ there exists a unique polynomial $Q_P \in k[T_1, \ldots, T_n]$ such that

$$P = Q_P(\Sigma_1, \ldots, \Sigma_n).$$

Using this result, show that the following two conditions are equivalent.

(i) for every $a \in A$, a_M and a_N have the same trace
(ii) M and N are isomorphic as A-modules.

5.2.2 Corrigé

Exercice 1 (Quelques remarques sur les groupes d'ordre 8)

1. Par le théorème de structure, il n'y a à isomorphisme près que 3 groupes abéliens d'ordre 8 :

$$\mathbb{Z}/8,\ \mathbb{Z}/2 \times \mathbb{Z}/4,\ \ \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

2. (a) On sait que $|Z(G)||8$, $|Z(G)| < 8$ (G n'est pas commutatif), $|Z(G)| \geq 2$ (G 2-groupe) et $|Z(G)| \neq 4$ ($G/Z(G)$ ne peut être cyclique)... Il ne reste donc que $|Z(G)| = 2$. Comme $G/Z(G)$ est d'ordre 4 non cyclique, c'est forcément $\mathbb{Z}/2 \times \mathbb{Z}/2$.
   (b) G contient au moins un élément d'ordre 4 sinon tous ses éléments seraient d'ordre 1 ou 2 donc G serait abélien ($ab = (ab^{-1} = b^{-1}a^{-1} = ba)$). Notons a un élément d'ordre 4 et $C := \langle a \rangle \subset G$ le sous-groupe engendré par a. Comme C est d'indice 2, il est normal dans G. Si $a^2 \neq z$ on aurait $Z(G) \cap C = 1$ donc $G = Z(G) \times C$ serait un produit direct (car $Z(G)$ et C sont tous deux normaux dans G) de deux groupes abéliens donc abélien.
   (c) D'après (2.b), G est donc une extension de la forme

$$(*)\ \ 1 \to C \to G \to \mathbb{Z}/2 \to 1$$

   i. Si $(*)$ se scinde, la structure de produit semi-direct est déterminée par un morphisme de groupes

$$\phi : \mathbb{Z}/2 \to \mathrm{Aut}_{Grp}(C) \simeq (\mathbb{Z}/4)^\times = \{Id, -Id\}.$$

   il n'y a donc que deux possibilités : $\phi = Id$, correspondant au produit direct, qui serait abélien donc exclu et $\phi : 1 \to -Id$, qui correspond à un produit semidirect non-abélien. Fixons $b \in G \setminus C$ d'ordre 2. On a la règle

$$bab = bab^{-1}b = \phi(b)(a) = a^{-1}.$$

   D'où $b^i a^j b^k a^l = b^i a^{j+l}$ si $k = 0$ et $b^i a^j b^k a^l = b^{i+1} a^{l-j}$ si $k = 1$. Enfin, on peut classer les éléments de G en fonction de leur ordre :
   — Ordre 1 : 1 ;
   — Ordre 2 : ba^i, $i = 0, \ldots, 3$, a^2 (5 éléments) ;
   — Ordre 4 : a, a^3 (2 éléments).

ii. Supposons maintenant que $(*)$ ne se scinde pas. Fixons $b \in G \setminus C$. Si b ´tait d'ordre 2, $1 \to b$ fournirait un scindage de $(*)$ donc b est forcḿent d'ordre 4. Comme bab^{-1} et a ont la même image par $p_{Z(G)} : G \twoheadrightarrow G/Z(G)$, on a $bab^{-1} \in \{a, za\}$. Mais on ne peut pas avoir $bab^{-1} = a$. Sinon a et b cpmmuteraient or, comme ils enegendrent G, cela imposerait à G d'être abélien. On a

$$G = p^{-1}(0) \sqcup p^{-1}(1) = C \sqcup Cb$$

et, en notant $c := ab$, on a

$$p^{-1}(0) = C = \{1, z, a, az\}$$

et

$$p^{-1}(1) = Cb = \{b, zb, c, zc\}.$$

Avec ces notations, on peut construire la table de multiplication de G.

	1	z	a	za	b	zb	c	zc
1	1	z	a	za	b	zb	c	zc
z	z	1	za	a	zb	b	zc	c
a	a	za	z	1	c	zc	zb	b
za	za	a	1	z	zc	c	b	zb
b	b	zb	zc	c	z	1	a	za
zb	zb	b	c	zc	1	z	za	a
c	c	zc	b	zb	za	a	z	1
zc	zc	c	zb	b	a	za	1	z

Enfin, on peut classer les éléments de G en fonction de leur ordre :
— Ordre 1 : 1 ;
— Ordre 2 : z (1 éléments) ;
— Ordre 4 : a, za, b, zb, c, zc (6 éléments).

3. (2-Sylow de $\mathcal{S}_4$)
   (a) Soit V un 2-Sylow de $\mathcal{A}_4$. On a $|V| = 4$. Par ailleurs, $\mathcal{A}_4$ ne contient que 4 éléments d'ordre une puissance de 2 : Id et l'ensemble $C_{2,2}$ des doubles transpositions. Donc, nécessairement $V = \{Id, C_{2,2}\}$. En particulier, l'ensemble $\{Id, C_{2,2}\}$ est un groupe et $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ et S est normal dans $\mathcal{A}_4$. Comme tous les éléments de V sont d'ordre 1, 2 on a forcément $V = \mathbb{Z}/2 \times \mathbb{Z}/2$.
   (b) On notera que V est normal dans $\mathcal{S}_4$. Par ailleurs, V est un 2-groupe donc il existe $S \in \mathcal{S}_2(\mathcal{S}_4)$ tel que $V \subset S$. Mais alors, pour tout $\sigma \in \mathcal{S}_4$ on a
   $$V = \sigma V \sigma^{-1} \subset \sigma S \sigma^{-1}.$$
   Comme les 2-Sylow de $\mathcal{S}_4$ sont tous conjugués, cela montre bien que V est contenu dans tous les 2-Sylow de $\mathcal{S}_4$. Donc les 2-Sylow de $\mathcal{S}_4$ - étant d'ordre 8 et contenant V sont engendrés par un 4-cycle et V. En particulier, ils sont non abéliens et contiennent 3 éléments d'ordre exactement 2 ; il s'agit donc de groupes isomorphes à D_8.
   (c) On ne peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_4$ sinon on aurait $\mathbb{H}_8$ isomorphe à D_8. Par contre, en faisant agir $\mathbb{H}_8$ par translation à gauche sur lui-même, on peut toujours le plonger dans $\mathcal{S}(\mathbb{H}_8) \simeq \mathcal{S}_8$. Reste à savoir si l'on peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_n$ pour $n = 5, 6, 7$. Cela revient à déterminer si pour $n = 5, 6, 7$ les 2-Sylow de $\mathcal{S}_n$ contiennent un sous-groupe isomorphe à $\mathbb{H}_8$. En observant que
   $$\mathcal{S}_n \simeq \mathrm{Stab}_{\mathcal{S}_{n+1}}(n+1) \subset \mathcal{S}_{n+1},$$
   on voit que les 2-Sylow de $\mathcal{S}_n$ s'injectent dans ceux de $\mathcal{S}_{n+1}$. En particulier, les 2-Sylow de $\mathcal{S}_5$ sont encore isomorphes à D_8 et ceux de $\mathcal{S}_7$ sont isomorphes à ceux de $\mathcal{S}_6$. Enfin, les 2-Sylow de $\mathcal{S}_6$ sont d'ordre 16. Or on peut facilement exhiber un sous-groupe de $\mathcal{S}_6$ d'ordre 16 sous la forme
   $$D_8 \times \mathbb{Z}/2$$
   En prenant pour copie de D_8 le 2-Sylow de $\mathrm{Stab}_{\mathcal{S}_6}(\{1, 2, 3, 4\}) \simeq \mathcal{S}_4$ et pour copie de $\mathbb{Z}/2$ le sous-groupe engendré par la permutation $(5, 6)$. Donc les 2-Sylow de $\mathcal{S}_6$ ne contient que 4 éléments d'ordre 4 : $(c, 1)$, (c, τ), $(c^3, 1)$, (c^3, τ) où c est un élément d'ordre 4 dans D_8 et τ un élément d'ordre 2 dans $\mathbb{Z}/2$. Ils ne peuvent donc contenir $\mathbb{H}_8$ qui, lui, contient 6 éléments d'ordre 4.

Exercice 2 (table des caractères de $\mathcal{A}_5$)

1. (Classes de conjugaison)
   (a) On sait que les doubles transpositions (resp. les 3-cycles) sont conjuguées dans $\mathcal{S}_5$ donc si σ, σ' sont deux doubles transpositions (resp. les 3-cycles) on peut toujours trouver $\tau \in \mathcal{S}_5$ tel que $\sigma' = \tau\sigma\tau^{-1}$. Si $\tau \in \mathcal{A}_5$, il n'y a rien à faire. Sinon, on peut essayer de modifier τ en le composant avec une permutation $c \in \mathcal{S}_5 \setminus \mathcal{A}_5$ qui centralise σ.
   — Si $\sigma = c_1 \circ c_2$ avec c_1, c_2 deux transpositions à supports disjoints, on peut prendre $c = c_1$ par exemple ;
   — Si σ est un 3-cycle, on peut prendre pour c la transposition dont le support est disjoint de celui de σ.
   (b) L'argument de la question précédente ne marche plus pour les 5-cycles dans $\mathcal{A}_5$. Il dit cependant qu'il y a au plus deux classes de conjugaison de 5-cycles. On sait qu'il y a $4! = 24$ 5-cycles dans $\mathcal{A}_5$. Comme les 5-cycles sont conjugués dans $\mathcal{S}_5$, on voit que le cardinal du centralisateur $C_{\mathcal{S}_5}(c)$ d'un 5-cycle c dans $\mathcal{S}_5$ est $\frac{120}{24} = 5$ donc est réduit à $\langle c \rangle$. Comme $C_{\mathcal{A}_5}(c) = C_{\mathcal{S}_5}(c) \cap \mathcal{A}_5 = \langle c \rangle$, on en déduit que la classe de conjugaison de c dans $\mathcal{A}_5$ est de cardinal $\frac{60}{5} = 12$. Il y a donc exactement deux classes de conjugaison de 5-cycles dans $\mathcal{A}_5$: celle des éléments de la forme $\sigma c \sigma^{-1}$ avec $\sigma \in \mathcal{A}_5$ et celle des éléments de la forme $\sigma c \sigma^{-1}$ avec $\sigma \in \mathcal{S}_5 \setminus \mathcal{A}_5$. En effet, si c est un 5-cycle et $\sigma \in \mathcal{S}_5 \setminus \mathcal{A}_5$, c et $\sigma c \sigma^{-1}$ ne peuvent être conjugués dans $\mathcal{A}_5$ sinon il existerait $\tau \in \mathcal{A}_5$ tel que $\tau^{-1}\sigma \in C_{\mathcal{A}_5}(c) = \langle c \rangle$: une contradiction.
   (c) Prenons par exemple $c = (1, 2, 3, 4, 5)$. On a donc $c^2 = (1, 3, 5, 2, 4)$ et en utilisant la formule $\sigma(1, 2, 3, 4, 5)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3), \sigma(4), \sigma(5))$, on en déduit que c et c^2 sont conjugués par $(2, 4, 5, 3) \in \mathcal{S}_5 \setminus \mathcal{A}_5$. Ils ne sont donc pas dans la même classe de conjugaison de $\mathcal{A}_5$. De même $c^{-1} = (1, 5, 4, 3, 2)$ est conjugué à c par $(2, 5)(3, 4) \in \mathcal{A}_5$.
   (d) — C_1, 1, $|C_1| = 1$;
   — $C_{2,2}$, $(1, 2)(3, 4)$, $|C_{2,2}| = 15$;
   — C_3, $(1, 2, 3)$, $|C_3| = 20$;
   — C_5^1, $(1, 2, 3, 4, 5)$, $|C_5^1| = 12$;
   — C_5^2, $(1, 3, 5, 2, 4)$, $|C_5^2| = 12$.
   (e) $|\widehat{\mathcal{A}_5}| = |Cl(\mathcal{A}_5)| = 5$.
   (f) On fait agir $\mathcal{A}_5$ sur $V := \oplus_{1 \leq i \leq 5} \mathbb{C} e_i$ par $\sigma \cdot e_i = e_{\sigma(i)}$. L'application $\mathbb{C}$-linéaire

$$\epsilon : V \to \mathbb{I}, \ \sum_{1 \leq i \leq 5} x_i e_i \to \sum_{1 \leq i \leq 5} x_i$$

   est un morphisme de $\mathbb{C}[\mathcal{A}_5]$-modules, donc $V_{std} := \ker(\epsilon) \subset V$ est un sous-$\mathbb{C}[\mathcal{A}_5]$-module et comme $\mathbb{C}[\mathcal{A}_5]$ est semisimple, on a

$$V = \mathbb{I} \oplus V_{std}.$$

   En particulier, pour $\sigma \in \mathcal{A}_5$ on a

$$\chi_{std}(\sigma) = \chi_V(\sigma) - \chi_{\mathbb{I}}(\sigma) = |\{1, \ldots, 5\}^\sigma| - 1,$$

   où $\{1, \ldots, 5\}^\sigma$ est l'ensemble des points fixes de σ. On a donc :

$$\chi_{std}(C_1) = 4, \ \chi_{std}(C_{2,2}) = 0, \ \chi_{std}(C_3) = 1, \ \chi_{std}(C_5^1) = \chi_{std}(C_5^2) = -1.$$

   Et

$$(\chi_{std}, \chi_{std})_{\mathcal{A}_5} = \frac{1}{60}(4^2 + 15 \times 0 + 20 \times 1 + 12 \times 1 + 12 \times 1) = 1,$$

   ce qui montre que V_{std} est irréductible.
   (g) Notons X l'ensemble des parties à deux éléments de $\{1, 2, 3, 4, 5\}$. On considère la représentation de $\mathcal{A}_5$ sur

$$V = \bigoplus_{x \in X} \mathbb{C} x \simeq \mathbb{C}^{\oplus 10}$$

   définie par $\sigma \cdot \{x, y\} = \{\sigma(x), \sigma(y)\}$. Par construction, on a

$$\chi_V(\sigma) = |X^\sigma|$$

   soit

$$\chi(C_1) = 10, \ \chi(C_{2,2}) = 2, \ \chi(C_3) = 1, \ \chi(C_5^1) = \chi_{std}(C_5^2) = 0.$$

On a également

$$(\chi_V, \chi_{\mathbb{I}})_{\mathcal{A}_5} = \frac{1}{60}(10 + 15 \times 2 + 20 \times 1) = 1,\ (\chi_V, \chi_{std})_{\mathcal{A}_5} = \frac{1}{60}(10 \times 4 + 20 \times 1) = 1.$$

Comme $\mathbb{C}[\mathcal{A}_5]$ est semisimple, on en déduit que V se décompose comme $\mathbb{C}[\mathcal{A}_5]$-module sous la forme

$$V = \mathbb{I} \oplus V_{std} \oplus V_5,$$

où V_5 est de dimension 5 et $\chi_{V_5} = \chi_V - \chi_{\mathbb{I}} - \chi_{std}$ soit

$$\chi(C_1) = 5,\ \chi(C_{2,2}) = 1,\ \chi(C_3) = -1,\ \chi(C_5^1) = \chi_{std}(C_5^2) = 0.$$

On a donc

$$(\chi_5, \chi_5)_{\mathcal{A}_5} = \frac{1}{60}(5^2 + 15 \times 1 + 20 \times 1 + 12 \times 0 + 12 \times 0) = 1,$$

ce qui montre que V_5 est irréductible.

(h) On a $60 = |\mathcal{A}_5| = n_1^2 + n_{std}^2 + n_5^2 + a^2 + b^2 = 1 + 4^2 + 5^2 + a^2 + b^2$ donc $18 = a^2 + b^2$. La seule possibilité est $a = b = 3$. Il reste donc 2 représentations irréductibles de dimension 3.

(i) On a déjà

	C_1	$C_{2,2}$	C_3	C_5^1	C_5^2
$\chi_{\mathbb{I}}$	1	1	1	1	1
χ_{std}	4	0	1	-1	-1
χ_5	5	1	-1	0	0
χ_3^1	3	$a = -1$	$b = 0$	$c = \frac{1-\sqrt{5}}{2}$	$d = \frac{1+\sqrt{5}}{2}$
χ_3^2	3	$e = -1$	$f = 0$	$g = \frac{1+\sqrt{5}}{2}$	$h = \frac{1-\sqrt{5}}{2}$

Et on peut compléter en utilisant l'orthogonalité selon les lignes et les colonnes.

— L'orthogonalité de la 1ère et 2ème colonne donne : $a + e = -2$. Par ailleurs, on sait que a et e sont somme de 3 racines carrée de 1, donc ne peuvent valoir que $-3, -1, 1, 3$. D'un autre coté, orthogonalité de la 2ème colonne avec elle-même donne $a^2 + e^2 = 2$. Donc on a forcément $a = b = -1$.

— L'orthogonalité de la 3ème colonne avec elle-même donne $b^2 + f^2 = 0$. Donc on a forcément $b = f = 0$.

— L'orthogonalité de la 1ère et 4ème (resp. 5ème) ligne donne $c + d = 1$ (resp. $g + h = 1$) et l'orthogonalité de la 4ème (resp. 5ème) ligne avec elle-même donne $c^2 + d^2 = 3$ (resp. $g^2 + h^2 = 3$). Donc $c^2 - c - 1 = 0$ (resp. $g^2 - g - 1 = 0$). On en déduit $c = \frac{1-\sqrt{5}}{2}$, $d = \frac{1+\sqrt{5}}{2}$ puis $g = \frac{+\sqrt{5}}{2}$, $h = \frac{1-\sqrt{5}}{2}$.

(j) En utilisant que $\chi_{V_5 \otimes V_3^2} = \chi_5 \chi_3^2$ et en calculant $(\chi_5 \chi_3^2, \chi)_{\mathcal{A}_5}$ pour $\chi \in \widehat{\mathcal{A}_5}$, on obtient

$$V_5 \otimes V_3^2 = V_{std} \oplus V_5 \oplus V_3^1 \oplus V_3^2.$$

Exercice 3 (Lemme de Brauer-Nesbitt)

1. C'est l'exercice 3.1.4 du cours. On rappelle l'argument. Soit $f \in A_V''$. Montrons d'abord que pour tout $v \in V$ il existe $a \in A$ tel que $f(v) = av$. Comme V est semi-simple, il existe un sous-A-module $W \subset V$ tel que $V = Av \oplus W$. Notons $\pi : V \twoheadrightarrow Av$ la projection sur Av parallèlement à W ; c'est un morphisme de A-modules. Et

$$V \overset{\pi}{\twoheadrightarrow} Av \hookrightarrow V \in A_V'$$

donc $f \circ \pi = \pi \circ f$. En particulier, $f(v) = f(\pi(v)) = \pi(f(v)) \in Av$. On applique ensuite ce qui précèdeà $V^{\oplus r}$ et $f^{\oplus r} : V^{\oplus r} \to V^{\oplus r}$, $(v_1, \ldots, v_r) \to (f(v_1), \ldots, f(v_r))$ pour en déduire qu'il existe $a \in A$ tel que $f(v_i) = av_i$, $i = 1, \ldots, r$. On conclut en invoquant que V est un A-module de type fini.

2. D'après la question (1), il suffit de montrer que la projection $p : V \to P^{\oplus \mu_P + \nu_P}$ parallèlement à

$$\bigoplus_{P \neq Q \in \widehat{A}} Q^{\oplus \mu_Q + \nu_Q}$$

est dans A''_V, *i.e.* que pour tout $f \in A'_V$ on a $pf = fp$. Mais si $f \in A'_V$, par le lemme de Schur, on a $f(Q^{\oplus\mu_Q+\nu_Q}) \subset Q^{\oplus\mu_Q+\nu_Q}$. Notons $f_Q : Q^{\oplus\mu_Q+\nu_Q} \to Q^{\oplus\mu_Q+\nu_Q}$ la restriction de f à $Q^{\oplus\mu_Q+\nu_Q}$. Alors pour tout $v = \sum_{Q\in\widehat{A}} v_Q \in V = \oplus_{Q\in\widehat{A}} Q^{\oplus\mu_Q+\nu_Q}$ on a

$$f(v) = \sum_{Q\in\widehat{A}} f_Q(v_Q)$$

donc $pf(v) = f_P(v_P)$ et $fp(v) = f(v_P) = f_P(v_P)$.

3. Par définition, $(e_P)_M$ (resp. $(e_P)_N$) est la projection sur $P^{\oplus\mu_P}$ parallèlement à $\oplus_{P\neq Q\in\widehat{A}} Q^{\oplus\mu_Q}$ (resp. $P^{\oplus\nu_P}$ parallèlement à $\bigoplus_{P\neq Q\in\widehat{A}} Q^{\oplus\nu_Q}$). Son polynôme caractéristique est donc $\chi_{P,M} = (T-1)^{p\mu_P} T^{m-p\mu_P}$ (resp. $\chi_{P,N} = (T-1)^{p\nu_P} T^{n-d_P\nu_P}$), où p, m, n sont les k-dimensions de P, M et N respectivement.
4. $\chi_{P,M} = \chi_{P,N}$ pour tout $P \in \widehat{A}$ si et seulement si $\mu_P = \nu_P$ pour tout $P \in \widehat{A}$, ce qui équivaut à $M \simeq N$.
5. D'après ce qui précède, la question revient à montrer que les conditions suivantes sont équivalentes :

   (i) pour tout $a \in A$, a_M et a_N ont même trace
   (i') pour tout $a \in A$, a_M et a_N ont même polynôme caractéristique.

   Déjà (i') $\Rightarrow$ (i). Pour l'implication inverse, notons $\chi_{a_M} := \prod_{1\leq i\leq n}(T-\mu_i)$ et $\chi_{a_N} := \prod_{1\leq i\leq n}(T-\nu_i)$ les polynômes caractéristiques de a_M et a_N vus dans $\overline{k}[T]$. En les développant, on obtient

$$\chi_{a_M} = T^n + \sum_{1\leq i\leq n} \sigma_n^i(\mu_1,\ldots,\mu_n)T^{n-i},\ \chi_{a_N} = T^n + \sum_{1\leq i\leq n} \sigma_n^i(\nu_1,\ldots,\nu_n)T^{n-i},$$

   avec $\sigma_n^i(X_1,\ldots,X_n) \in k[X_1,\ldots,X_n]^{\mathcal{S}_n}$, $i = 1,\ldots,n$. Par le théorème de structure de $k[X_1,\ldots,X_n]^{\mathcal{S}_n}$ donné dans l'énoncé on peut donc écrire

$$\sigma_n^i(X_1,\ldots,X_n) = Q_i(\Sigma_1(X_1,\ldots,X_n),\ldots,\Sigma_n(X_1,\ldots,X_n))$$

   pour des polynômes $Q_1,\ldots,Q_n \in k[U_1,\ldots,U_n]$ Mais comme

$$\Sigma_r(\mu_1,\ldots,\mu_n) = \sum_{1\leq i\leq n} \mu_i^r = Tr(a_M^r) = Tr(a_N^r) = \sum_{1\leq i\leq d} \nu_i^r = \Sigma_r(\nu_1,\ldots,\nu_n),\ r \geq 0,$$

   on en déduit

$$\sigma_n^i(\mu_1,\ldots,\mu_n) = \sigma_n^i(\nu_1,\ldots,\nu_n),\ i = 1,\ldots,n$$

   soit $\chi_{a_M} = \chi_{a_N}$.

5.3 Examen 2016/2017

5.3.1 Enoncé

MAT556 'Modules et groupes finis'
Anna Cadoret

Avertissement.

Sont autorisés : le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*. L'examen est long (faire les deux exercices ou le problème suffirait amplement pour obtenir la note maximale) ; le barême sera adapté en conséquence.

On rappelle que si G est un groupe fini et p un nombre premier, on note $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G.

Exercice 1 :

Soit A un anneau intègre et M un A-module libre de rang r.

1. Soit N un A-module. Une application A-s-multilinéaire $f : M^s \to N$ est dite alternée si pour tout $\mu_1, \dots, \mu_s \in M^s$ $f(\mu_1, \dots, \mu_s) = 0$ dès qu'il existe $1 \leq i \neq j \leq s$ tels que $\mu_i = \mu_j$. Notons $M_0 \subset M^{\otimes s}$ le sous-A module engendré par les éléments $\lambda_1 \otimes \cdots \otimes \lambda_s$ pour lesquel il existe $1 \leq i \neq j \leq s$ tel que $\lambda_i = \lambda_j$ et posons

$$\Lambda^s M := M^{\otimes s}/M_0.$$

On note $p_0 : M^{\otimes s} \to \Lambda^s M$ la projection canonique et, pour $\mu_1, \dots, \mu_s \in M^s$

$$\mu_1 \wedge \cdots \wedge \mu_s := p_0(\mu_1 \otimes \cdots \otimes \mu_s).$$

   (a) Expliquer pourquoi le A-module $\Lambda^s M$ est engendré par les éléments de la forme $\mu_1 \wedge \cdots \wedge \mu_s$, $\mu_1, \dots, \mu_s \in M^s$.

   (b) Montrer que l'application $p : M^s \to \Lambda^s M$ définie par $p(\mu_1, \dots, \mu_s) = \mu_1 \wedge \cdots \wedge \mu_s$ est A-s-multilinéaire alternée et que pour toute application A-s-multilinéaire alternée $f : M^s \to N$ il existe un unique morphisme de A-modules $\overline{f} : \Lambda^s M \to N$ tel que $\overline{f} \circ p = f$.

   (c) Montrer que si $\tau = (i, j) \in \mathcal{S}_s$ est une transposition, on a $\mu_{\tau(1)} \wedge \cdots \wedge \mu_{\tau(s)} = -\mu_1 \wedge \cdots \wedge \mu_s$. En déduire que pour tout $\sigma \in \mathcal{S}_s$, $\mu_{\sigma(1)} \wedge \cdots \wedge \mu_{\sigma(s)} = \epsilon(\sigma)\mu_1 \wedge \cdots \wedge \mu_s$, où $\epsilon : \mathcal{S}_s \to \pm 1$ est la signature.

   (d) Supposons $s = r$. Soit $\underline{e} = e_1, \dots, e_r$ une A-base de M. Montrer que $\Lambda^r M$ est un A-module libre de rang 1 et de A-base $e_1 \wedge \ldots \wedge e_r$. Calculer $\mu_1 \wedge \cdots \wedge \mu_r$ en fonction de $e_1 \wedge \ldots \wedge e_r$ et du déterminant de la matrice de la famille $\mu_1, \dots, \mu_r$ dans la A-base $\underline{e}$.

   (e) En déduire que pour tout endomorphisme de A-module $\phi : M \to M$, $\Lambda^r \phi(M) = \det(\phi)\Lambda^r M$.

2. Soit $\psi : M \to M$ un endomorphisme de A-module.

   (a) On note $M_\psi := M/(\psi - Id)(M)$ et $p_\psi : M \to M_\psi$ la projection canonique. Montrer que pour tout morphisme de A-modules $f : M \to N$ tel que $f \circ \psi = f$ il existe un unique morphisme de A-modules $\overline{f} : M_\psi \to N$ tel que $\overline{f} \circ p_\psi = f$.

   (b) Supposons $A = \mathbb{Z}$. On note $P_\psi := \det(\psi - TId) \in \mathbb{Z}[T]$ et on suppose $P_\psi(1) \neq 0$. En appliquant le théorème de la base adaptée au sous-A-module $(\psi - Id)(M) \subset M$, montrer que $|M_\psi| = |P_\psi(1)|$. (Indication : on pourra appliquer la question (1) (d) à $\phi = \psi - Id$).

Exercice 2 (Transfert de Burnside)

Soit G un groupe fini.

1. Transfert. Soit $H \subset G$ un sous-groupe d'indice $r := [G : H]$. Fixons un système de représentants $g_1, \dots, g_r$ de G/H. En particulier, pour tout $g \in G$, $i = 1, \dots, r$ il existe un unique $1 \leq i(g, i) \leq r$ tel que

$$gg_iH = g_{i(g,i)}H.$$

Notons $h(g,i) := g_{i(g,i)}^{-1} g g_i \in H$. On pose

$$T_{G/H}(g) := \prod_{1\leq i\leq r} \overline{h(g,i)} \in H^{ab},$$

où pour $h \in H$ on note $\overline{h}$ l'image de h dans l'abélianisé $H^{ab} = H/[H,H]$.

(a) Montrer que $T_{G/H}(g)$ ne dépend pas du choix du système de représentants $g_1, \ldots, g_r$ de G/H et que $T_{G/H} : G \to H^{ab}$ est un morphisme de groupes (appelé 'transfert de Burnside').

(b) Pour $g \in G$, $i(g,-)$ définit une permutation de $\{1,\ldots,s\}$. Notons $i(g,-) = c_1 \circ \cdots \circ c_s$ sa décomposition en produit de cycles à supports disjoints. Pour $i = 1,\ldots,s$ notons $\ell_i := |c_i|$ et choisissons a_i dans le support de c_i. Noter que $[G:H] = \sum_{1\leq i\leq s} \ell_i$. Montrer que

$$T_{G/H}(g) = \prod_{1\leq i\leq s} \overline{g_{a_i}^{-1} g^{\ell_i} g_{a_i}}.$$

2. Soit maintenant p un premier divisant $|G|$ et $P \in \mathcal{S}_p(G)$. On suppose que P est abélien. Soit $x, y \in P$ tels qu'il existe $g \in G$ vérifiant $y = gxg^{-1}$. Montrer que P et gPg^{-1} sont tous deux des p-Sylow du centralisateur $C_G(y)$ de y dans G. En déduire que x, y sont conjugués dans le normalisateur $N_G(P)$ de P dans G.

3. On suppose de plus que P est contenu dans le centre de son normalisateur $N_G(P)$.

(a) En utilisant (1)(b) et de (2), montrer que pour tout $g \in P$ on a

$$T_{G/P}(g) = g^{[G:P]}.$$

(b) En déduire que $T_{G/P} : G \to P^{ab} = P$ induit un isomorphisme $T_{G/P}|_P : P \xrightarrow{\sim} P$ puis qu'il existe un sous-groupe normal $N \lhd G$ tel que

$$G \simeq N \rtimes P.$$

Problème (Caractères des groupes non-abélien d'ordre 12)

On rappelle qu'un groupe est dit indécomposable s'il ne peut pas s'écrire comme produit direct de deux sous-groupes stricts.

1. Soit G un groupe fini et $Z \lhd G$ un sous-groupe normal. Montrer que si $|Z| = 2$ alors Z est contenu dans le centre de G.

2. En déduire qu'un groupe non abélien d'ordre 12 ne peut avoir un quotient cyclique d'ordre 6.

3. Déterminer le groupe des automorphismes de groupes

(a) $\mathbb{Z}/3$;

(b) $\mathbb{Z}/4$;

(c) $\mathbb{Z}/2 \times \mathbb{Z}/2$ (on observera que tout automorphisme du groupe $\mathbb{Z}/2 \times \mathbb{Z}/2$ est automatiquement $\mathbb{F}_2$-linéaire).

4. Soit G un groupe non-abélien d'ordre 12. Montrer que seuls les cas suivants peuvent se produire :

(a) G possède un unique 2-Sylow S_2 et G est un produit semi-direct $S_2 \rtimes G/S_2$. Montrer que dans ce cas, nécessairement $S_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$ donc $G = (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$.

(b) G possède un unique 3-Sylow S_3 et G est un produit semi-direct $S_3 \rtimes G/S_3$. Montrer que dans ce cas, les deux cas suivants peuvent se produire

i. $G/S_3 = \mathbb{Z}/4$ donc $G = \mathbb{Z}/3 \rtimes \mathbb{Z}/4$;

ii. $G/S_3 = \mathbb{Z}/2 \times \mathbb{Z}/2$ donc $G = \mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$.

5. Dans chacun des cas (4)(a), (4)(b)(i), (4)(b)(ii), déterminer l'abélianisé G^{ab} de G. En déduire

(a) le nombre de $K[G]$-modules simples de dimension 1 ;

(b) le nombre de $K[G]$-modules simples et leur dimension ;

(c) le nombre de classes de conjugaison de G.

6. Décrire les classes de conjugaison de G en fonction des fibres de l'abélianisé $p : G \twoheadrightarrow G^{ab}$.

7. Constuire la table de caractères de G.

5.3.2 Corrigé

Exercice 1 :

Soit A un anneau intègre et M un A-module libre de rang r.

1. (a) Comme $M^{\otimes s}$ est engendré par les éléments de la forme $\mu_1 \otimes \cdots \otimes \mu_s$, le A-module $\Lambda^s M = M^{\otimes s}/M_0$ est engendré par les images des $\mu_1 \otimes \cdots \otimes \mu_s$ *i.e.* précisément les $\mu_1 \wedge \cdots \mu_s$.

(b) Le fait que $p : M^s \to \Lambda^s M$ est A-s-multilinéaire alternée résulte immédiatement de la définition de $\Lambda^s M$. L'unicité (sous réserve d'existence) de $\overline{f} : \Lambda^s M \to N$ tel que $\overline{f} \circ p = f$ résulte de (1) (a) puisque, nécessairement $\overline{f}(\mu_1 \wedge \cdots \mu_s) = f(\mu_1, dots, \mu_s)$. Enfin l'existence de $\overline{f} : \Lambda^s M \to N$ vient du fait que si $f : M^s \to N$ est A-s-multilinéaire alternée alors $f : M^s \to N$ est en particulier A-s-multilinéaire donc, par propriété universelle du produit tensoriel, il existe un unique morphisme de A-modules $\overline{f}_1 : M^{\otimes s} \to N$ tel que $f = \overline{f}_1 \circ p_1$, où $p_1 : M^s \to M^{\otimes s}$ est la projection canonique. Mais, par construction $M_0 \subset \ker(\overline{f}_1)$ donc il existe un unique morphisme de A-modules $\overline{f} : \Lambda^s M \to N$ tel que $\overline{f}_1 = \overline{f} \circ p$ donc $f = \overline{f} \circ p \circ p_1$.

(c) Développer $\mu_1 \wedge \cdots \wedge (\mu_i + \mu_j) \wedge \cdots \wedge (\mu_i + \mu_j) \wedge \cdots \wedge \mu_s = 0$ puis utiliser que la signature est un morphisme de groupes

(d) Supposons $s = r$. Soit $\underline{e} = e_1, \ldots, e_r$ une A-base de M. Déjà, d'après (1)(b), $\Lambda^r M = Ae_1 \wedge \cdots \wedge e_r$. Il faut juste vérifier que
Montrer que $\Lambda^r M$ est un A-module libre de rang 1 et de A-base $e_1 \wedge \ldots \wedge e_r$. Calculer $\mu_1 \wedge \cdots \wedge \mu_r$ en fonction de $e_1 \wedge \ldots \wedge e_r$ et du déterminant de la matrice de la famille $\mu_1, \ldots, \mu_r$ dans la A-base $\underline{e}$.

(e) Pour tout endomorphisme de A-module $\phi : M \to M$, $\Lambda^r \phi(M) = A\phi(e_1) \wedge \cdots \wedge \phi(e_r)$ donc la conclusion résulte de $\phi(e_1) \wedge \cdots \wedge \phi(e_r) = \det_{\underline{e}}(\phi(e_1), \ldots, \phi(e_r)) = \det(\phi) e_1 \wedge \cdots \wedge e_r$.

2. Soit $\psi : M \to M$ un endomorphisme de A-module.

(a) Pour tout morphisme de A-modules $f : M \to N$ tel que $f \circ \psi = f$, $(\phi - Id)(M) \subset \ker(f)$ et on factorise.

(b) Supposons $A = \mathbb{Z}$. Par le théorème de la base adaptée, on sait qu'il existe une $\mathbb{Z}$-base $\underline{e} = e_1, \dots, e_r$ de M et une suite d'entiers > 0 $a_1|a_2|\cdots|a_r$ tels que

$$(\psi - Id)(M) = \bigoplus_{1\le i\le r} \mathbb{Z}a_i e_i \subset \bigoplus_{1\le i\le r} \mathbb{Z}e_i = M.$$

Mais alors $\mathbb{Z}\det(\psi - Id)e_1 \wedge \cdots \wedge e_s = \Lambda^r(\psi - Id)(M)\mathbb{Z}a_1 \cdots a_r e_1 \wedge \cdots \wedge e_s$ donc $|P_\psi(1)| = |\det(\psi - Id)| = a_1 \cdots a_r = |M/(\psi - Id)(M)|$.

Exercice 2 (Transfert de Burnside et applications)

1. (a) Si on remplace g_i par $g'_i = g_i u_i$ avec $u_i \in H$, on a toujours $gg'_i H = gg_i H = g_{i(g,h)}H = g'_{i(g,h)}H$ donc

$$h'(g,i) := g'^{-1}_{i(g,i)} g g'_i = u^{-1}_{i(g,i)} g^{-1}_{i(g,h)} g g_i u_i = u^{-1}_{i(g,i)} h(g,i) u_i$$

d'où

$$T'_{G/H}(g) := \prod_{1\le i\le r} \overline{u^{-1}_{i(g,i)} h(g,i) u_i} = \prod_{1\le i\le r} \overline{h(g,i)} \prod_{1\le i\le r} \overline{u_{i(g,i)}}^{-1} \prod_{1\le i\le r} \overline{u_i}.$$

Et comme l'application $i \to i(g,i)$ est une permutation de $\{1,\dots,r\}$, on a

$$\prod_{1\le i\le r} \overline{u_{i(g,i)}}^{-1} \prod_{1\le i\le r} \overline{u_i} = 1$$

donc $T'_{G/H}(g) = T_{G/H}(g)$. Cela montre que $T_{G/H}(g)$ ne dépend pas du choix du système de représentants $g_1, \dots, g_r$ de G/H.
Par ailleurs, pour tout $g, g' \in G$, on a $gg'g_i = g_{i(gg',i)}h(gg',i)$ mais aussi

$$gg'g_i = gg_{i(g',i)}h(g',i) = g_{i(g,i(g',i))}h(g,i(g',i))h(g',i).$$

Donc $h(gg',i) = h(g,i(g',i))h(g',i)$ et

$$T_{G/H}(gg') = \prod_{1\le i\le r} \overline{h(g,i(g',i))} \prod_{1\le i\le r} \overline{h(g',i)} = T_{G/H}(g)T_{G/H}(g')$$

(on a à nouveau utilisé que l'application $i \to i(g,i)$ est une permutation de $\{1,\dots,r\}$).

(b) Notons $c_i = (a_{i,1}, \dots, a_{i,\ell_i})$ avec $a_{i,1} := a_i$. Alors on a

$$\begin{aligned} gg_{a_{i,1}} &= g_{a_{i,2}} h_{i,1} \\ gg_{a_{i,2}} &= g_{a_{i,3}} h_{i,2} \\ &\dots \\ gg_{a_{i,\ell_i}} &= g_{a_{i,1}} h_{i,\ell_i} \end{aligned}$$

d'où, en utilisant que H^{ab} est abélien

$$T_{G/H}(g) = \prod_{1\le i\le s} \overline{(g^{-1}_{a_{i,1}} g g_{a_{i,\ell_i}})(g^{-1}_{a_{i,\ell_i}} g g_{a_{i,\ell_i-1}}) \cdots (g^{-1}_{a_{i,2}} g g_{a_{i,1}})} = \prod_{1\le i\le s} \overline{g^{-1}_{a_i} g^{\ell_i} g_{a_i}}.$$

2. Comme P est abélien on a $P \subset C_G(x)$, $P \subset C_G(y)$ donc aussi $gPg^{-1} \subset gC_G(x)g^{-1} = C_g(y)$. Comme $[C_G(P) : P] | [G : P]$, P et gPg^{-1} sont tous deux des p-Sylow de $C_G(y)$. En particulier, il existe $z \in C_G(y)$ tel que $P = zgP(zg)^{-1}$. Donc $zg \in N_G(P)$ et $zgx(zg)^{-1} = zyz^{-1} = y$.

3. On suppose de plus que P est contenu dans le centre de son normalisateur $N_G(P)$ ou, de façon équivalente, $C_G(P) = N_G(P)$.

(a) Soit $g \in P$. Avec les notations de (1)(b), comme $g^{\ell_i}, g^{-1}_{a_i} g^{\ell_i} g_{a_i} \in P$ sont conjugués dans G, ils sont conjugués dans $N_G(P) = C_G(P)$ donc, en fait, $g^{\ell_i} = g^{-1}_{a_i} g^{\ell_i} g_{a_i}$. Par (1) (b), cela montre que

$$T_{G/P}(g) = g^{[G:P]}.$$

(b) Par cardinalité, il suffit de montrer que $T_{G/P} : G \to P^{ab} = P$ est surjectif. Comme tout $g \in P$ est d'ordre une puissance de p et que $[G : H]$ est premier à p, (3) (a) montre que l'image du transfert contient $\langle g \rangle$ donc g et, ceci, pour tout $g \in P$. On peut prendre pour N le noyau du transfert.

Problème (Caractères des groupes non abéliens d'ordre 12)

1. Notons $Z = \{1, z\}$. Pour tout $g \in G$, la conjugaison par g induit un automorphisme de groupes de Z ; en particulier $1 \neq gzg^{-1} \in Z$ donc $gzg^{-1} = z$.
2. Si $|G| = 12$ et $G \twoheadrightarrow Q$ est un quotient avec Q cyclique d'ordre 6 alors $Z := \ker(G \twoheadrightarrow Q) \lhd G$ est normal d'ordre 2 donc contenu dans le centre de G. Mais alors, $\mathbb{Z}/6 = Q \simeq G/Z \twoheadrightarrow G/Z(G)$ montre que $G/Z(G)$ est cyclique (comme quotient d'un groupe cyclique) non trivial (car G est supposé non-abélien) : une contradiction.
3. On rappelle que le groupe des automorphismes d'un groupe cyclique $\mathbb{Z}/n$ est le groupe $(\mathbb{Z}/n)^\times$ des inversibles de l'anneau $\mathbb{Z}/n$ (explicitement $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/n) \simeq (\mathbb{Z}/n)^\times$, $\varphi \to \varphi(1)$).
   (a) $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/3) = (\mathbb{Z}/3)^\times = \mathbb{Z}/2$;
   (b) $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/4) = (\mathbb{Z}/4)^\times = \mathbb{Z}/2$;
   (c) $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/2 \times \mathbb{Z}/2) = \mathrm{GL}_2(\mathbb{F}_2)$.
4. $|G| = 12 = 2^2 \cdot 3$. D'après les théorèmes de Sylow, on a $|\mathcal{S}_2(G)| = 1, 3$ et $|\mathcal{S}_3(G)| = 1, 4$. En outre le cas $|\mathcal{S}_2(G)| = 3$ et $|\mathcal{S}_3(G)| = 4$ est impossible. En effet, si $|\mathcal{S}_3(G)| = 4$, G contiendrait $4 \times 2 = 8$ éléments d'ordre 2 (observer que les 3-Sylow de G sont $\simeq \mathbb{Z}/3$ donc d'intersection 2 à 2 triviale) et au moins 5 éléments d'ordre divisible par 2 (observer que $S_2 \cap S_2' = 1, \mathbb{Z}/2$; dans le premier cas on a au moins 6 éléments d'ordre divisible par 2 et dans le second cas, au moins 5). Le cas $|\mathcal{S}_2(G)| = |\mathcal{S}_3(G)| = 1$ est également impossible car G serait alors produit direct de son 2-Sylow et de son 3-Sylow donc serait abélien. Considérons les deux cas restants.
   (a) G possède un unique 2-Sylow S_2. Comme tout 3-Sylow S_3 de G fournit un complément de S_2 dans G, on en déduit que G est un produit semi-direct $S_2 \rtimes G/S_2 \simeq S_3$. Pour S_2, on a *a priori* deux options : $S_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$ et $S_2 \simeq \mathbb{Z}/4$. Mais si $S_2 \simeq \mathbb{Z}/4$, G serait forcément produit direct de S_2 et S_3 car il n'y a pas de morphisme de groupe non-trivial de $\mathbb{Z}/3$ dans $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/4)$ (*cf.* (1)(b)). Le cas $S_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$ par contre peut se produire car on a un morphisme de groupe non-trivial $\mathbb{Z}/3 \to \mathrm{GL}_2(\mathbb{F}_2)$ (observer que $\mathrm{GL}_2(\mathbb{F}_2)$ contient 2 éléments d'ordre 3). Donc $G = (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$.
   (b) G possède un unique 3-Sylow S_3. Comme tout 2-Sylow S_2 de G fournit un complément de S_3 dans G, on en déduit que G est un produit semi-direct $S_3 \rtimes G/S_3 \simeq S_2$. Là encore on a *a priori* deux options : $S_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$ et $S_2 \simeq \mathbb{Z}/4$ pour S_2. Comme le groupe des automorphismes de $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}/3) = \mathbb{Z}/2$ et qu'on a des morphismes de groupes non triviaux $\mathbb{Z}/2 \times \mathbb{Z}/2 \to \mathbb{Z}/2$, $\mathbb{Z}/4 \to \mathbb{Z}/2$, les cas
      i. $G/S_3 = \mathbb{Z}/4$ donc $G = \mathbb{Z}/3 \rtimes \mathbb{Z}/4$;
      ii. $G/S_3 = \mathbb{Z}/2 \times \mathbb{Z}/2$ donc $G = \mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$.

      peuvent tous deux se produire.
5. Comme G est supposé non abélien, il résulte directement de la propriété universelle de G^{ab} que dans le cas (4)(a), $G^{ab} = \mathbb{Z}/3$ (sinon, G^{ab} serait cyclique d'ordre 6, ce qui contredirait (2)), dans le cas (4)(b)(i), $G^{ab} = \mathbb{Z}/2 \times \mathbb{Z}/2$ et dans le cas (4)(b)(ii) $G^{ab} = \mathbb{Z}/4$. En particulier
   (a) dans le cas (4)(a), G a 3 $K[G]$-modules simples de dimension 1, dans les cas (4)(b)(i) et (4)(b)(ii) $G^{ab} = \mathbb{Z}/4$, G a 4 $K[G]$-modules simples de dimension 1 ;
   (b) On doit avoir $12 = \sum_{1 \leq i \leq r} n_i^2$, où $n_1, \ldots, n_r$ sont les dimensions des $K[G]$-modules simples. Dans le cas (4)(a), $12 - 3 = 9 = 3^2$ est la seule possibilité donc on a 3 $K[G]$-modules simples de dimension 1 et un $K[G]$-module simple de dimension 3. Dans les cas (4)(b)(i) et (4)(b)(ii), $12 - 4 = 8 = 2^2 + 2^2$ est la seule possibilité donc on a 4 $K[G]$-modules simples de dimension 1 et 2 $K[G]$-module simple de dimension 2.
   (c) dans le cas (4)(a), on a 4 classes de conjugaison, dans les cas (4)(b)(i) et (4)(b)(ii), on en a 6.
6. Comme G^{ab} est abélien, tout classe de conjugaison C de G est contenue dans une et une seule fibre de $p : G \twoheadrightarrow G^{ab}$. On analyse ensuite cas par cas.
   — (4)(a) : Comme $\ker(p)$ contient au moins deux classes de conjugaison, $\ker(p)$ est formé de deux classes : celle du neutre, $C_{\overline{0},1}$ et $C_{\overline{0},2}$ et $C_{\overline{1}} := p^{-1}(\overline{1})$, $C_{\overline{2}} := p^{-1}(\overline{2})$ forment, elles, chacune une seule classe de conjugaison.

— (4)(b)(i) : Notons $g \in S_2$ un élément d'ordre 4 et $u \in S_3$ un élément d'ordre 3. Comme S_3 est normal dans G et g agit non-trivialement par conjugaison sur S_3, on a forcément $gug^{-1} = u^{-1}$ donc $ugu = g$. On en déduit que $\ker(p)$ est formé de deux classes : celle du neutre, $C_{0,1}$ et $C_{0,2} = \{u, u^{-1}\}$ et que $p^{-1}(\overline{2})$ est également formée de deux classes : celle de g^2, $C_{2,1}$ et $C_{2,2} = \{g^2u, g^2u^{-1}\}$. $C_1 := p^{-1}(\overline{1})$ et $C_3 := p^{-1}(\overline{3})$ forment, elles, chacune une seule classe de conjugaison.

— (4)(b)(ii) : Soit encore $u \in S_3$ un élément d'ordre 3. Notons $a \in S_2$ l'élement qui agit non trivialement par conjugaison sur S_3 et $b \in S_2$ un autre élément d'ordre 2 commutant avec S_3. Alors $S_2 = \{1, a, b, ab\}$ et $aua = u^{-1}$, $bub = u$. On en déduit que $\ker(p)$ est formé de deux classes : celle du neutre, $C_{1,1}$ et $C_{1,2} = \{u, u^{-1}\}$ et que $p^{-1}(b)$ est également formée de deux classes : celle de b, $C_{b,1}$ et $C_{b,2} = \{bu, bu^{-1}\}$. $C_a := p^{-1}(a)$ et $C_{ab} := p^{-1}(ab)$ forment, elles, chacune une seule classe de conjugaison.

7. On peut tout mettre ensemble.

(4)(a) : On remplit la dernière ligne en utilisant l'orthogonalité avec la première colonne. Ici, j est une racine primitive 3-ème de 1.

	$C_{\overline{0},1}$	$C_{\overline{0},2}$	$C_{\overline{1}}$	$C_{\overline{2}}$
$\mathbb{I}$	1	1	1	1
χ_2	1	1	j	j^2
χ_3	1	1	j^2	j
χ_4	3	-1	0	0

(4)(b)(i) : Ici, i est une racine primitive 4-ème de 1. Si $\chi_5 = \chi_2\chi_5$, $\chi_6 = \chi_2\chi_6$, on aurait forcément $b = b' = c = c' = d = d' = e = e' = 0$. L'orthogonalité pour les lignes χ_4, χ_5 et χ_4, χ_6 imposerait alors $a = a' = -1$ donc $\chi_5 = \chi_6$: contradiction. Donc on peut supposer que $\chi_6 = \chi_2\chi_5$ et conclure en utilisant l'orthogonalité avec la première colonne pour a, d, e que $a = -1$, $d = 0$, $e = 0$. Comme $C_{0,2}$ est un singleton z d'ordre 2, b est la somme de ± 1, ± 1 ; il y a 3 possibilité : $-2, 0, 2$. Si $b = 0$, l'orthogonalité des lignes 1 et 5 montre que $c = 0$ donc $\chi_5 = \chi_6$: contradiction. On peut donc supposer $b = 2$ (donc $b' = -2$). On a alors, par orthogonalité entre les lignes 1 et 5 $c = -1$.

	$C_{0,1}$	$C_{0,2}$	$C_{2,1}$	$C_{2,2}$	C_1	C_3
$\mathbb{I}$	1	1	1	1	1	1
χ_2	1	1	-1	-1	i	$-i$
χ_3	1	1	-1	-1	$-i$	i
χ_4	1	1	1	1	-1	-1
χ_5	2	a	b	c	d	e
χ_6	2	a'	b'	c'	d'	e'

(4)(b)(ii) : L'orthogonalité entre la ligne 5 et les lignes $1, 2, 3, 4$ montrent que $a = -1$, $d = e = 0$ et $b + 2c = 0$. De même l'orthogonalité entre la ligne 6 et les lignes $1, 2, 3, 4$ montrent que $a' = -1$, $d' = e' = 0$ et $b' + 2c' = 0$. Comme $\chi_5 \neq \chi_6$, on a forcément $\chi_6 = \chi_3\chi_5$. Enfin, comme $C_{b,1}$ est un singleton z d'ordre 2, b est la somme de ± 1, ± 1 ; il y a 3 possibilité : $-2, 0, 2$. Si $b = 0$, $c = 0$ donc $\chi_5 = \chi_6$: contradiction. On peut donc supposer que $b = 2$ donc $c = -1$.

	$C_{1,1}$	$C_{1,2}$	$C_{b,1}$	$C_{b,2}$	C_a	$C_{ab}s$
$\mathbb{I}$	1	1	1	1	1	1
χ_2	1	1	1	1	-1	-1
χ_3	1	1	-1	-1	1	-1
χ_4	1	1	-1	-1	-1	1
χ_5	2	a	b	c	d	e
χ_6	2	a'	b'	c'	d'	e'

Remarque : Comme les 3 tables de caractères ci-dessus sont distinctes, il y a au moins 3 classes d'isomorphismes de groupes non-abéliens d'ordre 12. En fait, en regardant d'un peu plus près les structures de produit semi-direct, on montre facilement qu'il y en a exactement 3. (4)(a) est $\mathcal{A}_4$ et (4)(b)(ii) est le groupe diédral D_{12}... Je ne sais pas si (4)(b)(i) a un nom.

5.4 Examen 2017/2018

5.4.1 Enoncé

Avertissement.

Sont autorisés : le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*. L'examen est long (faire les deux exercices ou le problème suffirait amplement pour obtenir la note maximale) ; le barême sera adapté en conséquence.

Si G est un groupe fini et p un nombre premier, on note $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G et $N_p(G) := |\mathcal{S}_p(G)|$.

On rappelle également que si n est un entier, le groupe des automorphismes de groupes de $\mathbb{Z}/n$ est le groupe multiplicatif $\mathbb{Z}/n^\times$ de l'anneau $\mathbb{Z}/n$. En utilisant le lemme Chinois, on se ramène au cas $n = p^r$, qui sera le seul dont on a besoin dans l'examen. Dans ce cas $(\mathbb{Z}/p^r)^\times \simeq \mathbb{Z}/p^{r-1}\times\mathbb{Z}/p-1$ (*via* la suite exacte courte $1 \to 1+p\mathbb{Z}/p^r \to (\mathbb{Z}/p^r)^\times \to (\mathbb{Z}/p)^\times \to 1$) sauf si $p = 2$, auquel cas, $(\mathbb{Z}/2^r)^\times \simeq \mathbb{Z}/2^{r-2} \times \mathbb{Z}/2$.

Exercice 1 (Application de la théorie des $k[X]$-module au commutant d'un endomorphisme) :

Soit k un corps quelconque, V un k-espace vectoriel de dimension finie et $u : V \to V$ un endomorphisme du k-espace vectoriel V. On dit que u est simple si V n'admet pas de sous-k-espace vectoriel u-stable non trivial, que u est semisimple si pour tout sous-k-espace vectoriel $W \subset V$ u-stable il existe un sous-k-espace vectoriel $W' \subset V$ u-stable tel que $V = W \oplus W'$ et que u est indécomposable si V ne peut s'écrire comme somme directe de deux sous-espaces vectoriels u-stables non triviaux.

1. Caractériser en termes du polynôme minimal Π_u et du polynôme caractéristique Ξ_u de u les propriétés d'être respectivement simple, semisimple, indécomposable.

2. Est-il vrai que u est semisimple si et seulement si u est diagonalisable sur une extension finie de k ?

3. Pour toute partie $\emptyset \neq A \subset \mathrm{End}_k(V)$, on note $C(A) \subset \mathrm{End}_k(V)$ la sous-k-algèbre des endomorphismes qui commutent avec a, $a \in A$.

   (a) Montrer que $k[u] \subset C(u)$.

   (b) Soit $P, Q \in K[X]$. On note $\mathrm{Hom}_{k[X]}(k[X]/P, k[X]/Q)$ l'ensemble des morphismes de $k[X]$-modules de $k[X]/P$ dans $k[X]/Q$; on notera que c'est un $k[X]$-module donc, en particulier, un k-espace vectoriel. Montrer qu'on a un isomorphisme canonique de k-espaces vectoriels
   $$\mathrm{Hom}_{k[X]}(k[X]/P, k[X]/Q) \tilde{\to} k[X]/gcd(P, Q).$$

   (c) En déduire la dimension de $C(u)$ en fonction du degré des invariants de similitudes de u.

   (d) Donner une condition nécessaire et suffisante sur u pour que $C(u) = k[u]$.

Exercice 2 (Groupes d'ordre 105)

1. Soit G un groupe fini et p un nombre premier divisant l'ordre de G. Montrer que si G possède N sous-groupes d'ordre p alors G contient $N(p-1)$ éléments d'ordre p.

2. Soit G un groupe fini et p le plus petit diviseur premier de $|G|$. Montrer que tout sous-groupe $N \subset G$ d'indice p est normal dans G.

3. Soit G un groupe fini et $N \subset G$ un sous-groupe normal. Soit p un diviseur premier de $|G|$. Montrer que si N contient un p-Sylow de G et que $N_p(N) = 1$ alors $N_p(G) = 1$.

4. Montrer que le seul groupe d'ordre 35 est $\mathbb{Z}/35$.

5. Donner la liste de tous les groupes abéliens d'ordre 105.

6. Soit maintenant G un groupe non-abélien d'ordre 105.

   (a) Montrer que $N_5(G) = 1$ ou $N_7(G) = 1$.

   (b) Montrer que G contient un sous-groupe N d'ordre 35.

   (c) En déduire que $N_5(G) = N_7(G) = 1$.

   (d) Montrer que $G \simeq \mathbb{Z}/5 \times H$ avec $|H| = 21$.

   (e) En déduire qu'à isomorphisme près, il n'existe qu'un seul groupe non-abélien d'ordre 105.

Exercice 3 (Caractères des groupes non-abélien d'ordre p^3)

On a vu en cours qu'il y avait deux groupes non-abéliens d'ordre 8, H_8 (quaternions) et D_8 (groupe dihédral) mais que leur table des caractères étaient identiques. On va étendre ce résultat à p quelconque.

1. Soit G un groupe fini. On note
   $$d := \min\{[G : A] \mid A \lhd G,\ A : \text{ abélien}\}$$
   Montrer que toute représentation irréductible de G est de dimension $\leq d$.

2. Soit p un nombre premier et G un groupe d'ordre p^r.

   (a) Si $r = 2$, montrer que G est abélien. On suppose désormais que G est *non-abélien*.

   (b) Montrer que $Z(G) \simeq \mathbb{Z}/p$ et que $G/Z(G) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$.

   (c) Calculer $D(G)$ et G^{ab}. Donner la liste des représentations irréducibles de dimension 1 de G.

   (d) Montrer qu'il existe un sous-groupe $G_1 \subset G$ d'ordre p^2, normal dans G et contenant $Z(G)$.

   (e) On note $p_Z : G \twoheadrightarrow G/Z(G)$ la projection canonique. Montrer que l'action de G sur lui-même par conjugaison stabilise chacune des fibres $p^{-1}(\overline{g})$, $\overline{g} \in G/Z(G)$. En déduire que G a exactement $p^2 + p - 1$ classes de conjugaison et donner leur cardinal.

   (f) Montrer que les représentations irréductibles de G qui ne sont pas de dimension 1 sont de dimension p et déterminer leur nombre.

   (g) On note z un générateur de $Z(G)$ et $a \in G$ un relèvement dans G d'un générateur de $G/G_1 \simeq \mathbb{Z}/p$. Soit ω une racine p-ième de 1. Montrer que pour $k = 1, \ldots, p-1$ il existe une représentation irréductible χ_k de G_1 telle que $\chi_k(z) = \omega^k$. On note ϕ_k le caractère de la représentation induite à G. Montrer que
   — $\phi_k(z^\ell) = p\omega^{k\ell}$, $\ell = 0, \ldots, p-1$;
   — $\phi_k(g) = 0$, $g \in G \setminus Z(G)$ (on distinguera les cas $g \in G_1$ et $g \in G \setminus G_1$).

   (h) Vérifier que les ϕ_k sont des caractères de représentations irréductibles, deux à deux non isomorphes. Conclure.

3. Montrer qu'il y a au moins deux groupes non-abéliens d'ordre p^3.

5.4.2 Corrigé

Exercice 1 (Application de la théorie des $k[X]$-module au commutant d'un endomorphisme) :

Soit k un corps quelconque, V un k-espace vectoriel de dimension finie et $u : V \to V$ un endomorphisme du k-espace vectoriel V. On dit que u est simple si V n'admet pas de sous-k-espace vectoriel u-stable non trivial, que u est semisimple si pour tout sous-k-espace vectoriel $W \subset V$ u-stable il existe un sous-k-espace vectoriel $W' \subset V$ u-stable tel que $V = W \oplus W'$ et que u est indécomposable si V ne peut s'écrire comme somme directe de deux sous-espaces vectoriels u-stables non triviaux.

1. Notons V_u le k-espace vectoriel V muni de la structure de $k[X]$-module définie par $X \cdot v = u(v)$. Par définition, les invariants de similitude de u sont l'unique suite de polynômes unitaires $P_1|P_2|\cdots|P_r$ tels que le $k[X]$-module V_u est isomorphe à
$$k[X]/P_1 \oplus \cdots \oplus k[X]/P_r.$$
Par définition également u est simple (resp. semisimple, resp. indŕecomposable) si et seulement si le $k[X]$-module V_u l'est. Or on sait que si A est un anneau principal, les A-modules indécoposables sont les A-modules de la forme A/a, $a \in A$ et les A-modules simples sont les A-modules de la forme A/p, $p \in A$ premier. Donc déjà u est indŕecomposable si et seulement si $r = 1$ (ou encore $\Pi_u = \Xi_u$) et u est simple si et seulement si $r = 1$ et P_1 est irréductible (ou encore $\Pi_u = \Xi_u$ est irreéductible dans $k[X]$). u est semisimple si et seulement si V_u est somme directe de $k[X]$-module simples. Si $\Pi_u = P_r$ est sans facteur carré, par le lemme Chinois chacun des facteurs direct $k[X]/P_i$ se décompose comme somme directe de $k[X]$-modules simples et donc u est bien semisimple. Inversement, si u est semisimple, on peut écrire $V_u = \oplus_{1 \le i \le s}(k[X]/Q_i)^{\oplus n_i}$ avec Q_i irréductible dans $k[X]$, $i = 1, \ldots, s$. Si on suppose $n_1 = n_2 = \ldots = n_{s_1} < n_{s_1+1} = \ldots = n_{s_2} < \ldots < n_{s_r} = \ldots = n_s$, on obtient explicitement la suite des invariants de similitude de u en posant $P_r = Q_1 \cdots Q_s = P_{r-1} = \ldots = P_{r-n_{s_1}}$, $P_{r-n_{s_1}-1} = \ldots = P_{r-n_{s_2}} = Q_{s_1+1} \cdots Q_s$ *etc.*. En particulier, $\Pi_u = P_r$ est bien sans facteur carré.

2. Si u est diagonalisable sur une extension finie de k, u est évidemment semisimple. La réciproque n'est vrai que si k est parfait. Par exemple si $k = \mathbb{F}_p(T)$ et u a pour polynôme minimal $X^p - T$, u est semisimple (et même simple) mais il n'est pas diagonalisable car $X^p - T$ n'est pas simplement scindé sur son corps de décomposition, qui est $\mathbb{F}_p(T^{\frac{1}{p}})$: $X^p - T = (X - T^{\frac{1}{p}})^p$.

3. (a) Immédiat.

   (b) Observons qu'un élément $f \in \mathrm{Hom}_{k[X]}(k[X]/P, k[X]/Q)$ est entièrement déterminé par $f(\overline{1})$. Donc on a un morphisme injectif $\Phi : \mathrm{Hom}_{k[X]}(k[X]/P, k[X]/Q) \hookrightarrow [X]/Q$, $f \to \Phi(f) := f(\overline{1})$. Notons $D := gcd(P, Q)$ et $P = R_P D$ $Q = R_Q D$. Il existe $A, B \in k[X]$ tels que $AR_P + BR_Q = 1$. On vérifie immédiatement que l'image de Φ est le sous $k[X]$-module des $R \in k[X]/Q$ tels que $\overline{RP} = 0$ ou encore $RR_P = R_Q C$ *i.e.* $R \in R_Q k[X]$. On a donc
   $$(\Phi) = R_Q k[X]/Q \simeq R_Q k[X]/R_Q D \simeq k[X]/D.$$

   (c) Par définition
   $$C(u) = \mathrm{Hom}_{k[X]}(\bigoplus_{1\leq i\leq r} k[X]/P_i, \bigoplus_{1\leq i\leq r} k[X]/P_i) \simeq \bigoplus_{1\leq i,j\leq r} \mathrm{Hom}_{k[X]}(k[X]/P_i, k[X]/P_j).$$
   Donc si on note d_i le degré de P_i, en utilisant que $P_1|P_2|\cdots|P_r$, on obtient
   $$\dim(C(u)) = \sum_{1\leq i\leq r} d_i + 2\sum_{1\leq i\leq r}(r-i)d_i = (2r-1)d_1 + (2r-3)d_2 + \cdots + 3d_{r-1} + d_r$$
   .

   (d) Comme $k[u] \subset C(u)$, $k[u] = C(u)$ si et seulement si $\dim(k[u]) = \dim(C(u))$ *i.e.* si et seulement si $d_1 + \cdots + d_r = (2r-1)d_1 + (2r-3)d_2 + \cdots + 3d_{r-1} + d_r$. Donc $k[u] = C(u)$ si et seulement si $r = 1$ *i.e.* u est indécomposable.

Exercice 2 (Groupes d'ordre 105)

1. Le seul groupe d'ordre p est $\mathbb{Z}/p$; tous ses éléments sont d'ordre p sauf 0. Si P_1, P_2 sont deux sous-groupes distincts d'ordre p, $P_1 \cap P_2 = 1$ donc chaque sous-groupe d'ordre p contient $p-1$ éléments d'ordre p contenus dans aucun autre sous-groupe d'ordre p. D'où la conclusion.

2. On veut montrer que $N = \cap_{g\in G} gNg^{-1} =: K_G(N)$. On a clairement $K_G(N) \subset N$ et $K_G(N)$ est le noyau du morphisme canonique $t : G \to \mathcal{S}(G/N) \simeq \mathcal{S}_p$ induit par l'action par translation à gauche de G sur G/N. Il suffit donc de montrer que N est dans le noyau de ce morphisme. Or pour $1 \neq n \in N$ d'ordre premier disons q, notons $t(n) = c_1 \circ \cdots \circ c_r$ sa décomposition en produit de cycles à supports disjoints. Comme $t(n)N = N$, le support de $t(n)$ est de cardinal $\leq p-1$. Son ordre est donc de la forme $ppcm(\ell(c_1), \ldots, \ell(c_r))$ avec $\ell(c_i) < p$. En particulier, les diviseurs premiers de l'ordre de $t(n)$ sont tous $< p$ alors que si $t(n) \neq Id$, les diviseurs premiers de l'ordre de $t(n)$ sont des diviseurs premiers de l'ordre de n donc de $|G|$ donc $\geq p$: impossible. Cela montre que $t(n) = Id$.

3. Soit $S \in \mathcal{S}_p(G)$. Par hypothèse $S \subset N$ et $S \lhd N$ donc S est l'*unique* p-sous-groupe de N tel que $p \not| [N : S]$. En particulier pour tout automorphisme de groupe $\phi : N \tilde{\to} N$, on a $\phi(N) = N$. C'est vrai notamment pour les automorphismes de la forme $\phi = g(-)g^{-1}$, $g \in G$. On a donc aussi $N \lhd G$ donc $N_P(G) = 1$.

4. Soit H un groupe d'ordre $35 = 7 \times 5$. Par Sylow, $N_5(H) = N_7(H) = 1$ donc si S_5 et S_7 sont respectivement les uniques 5- et 7-Sylow de H, on a $H \simeq S_5 \times S_7 \simeq \mathbb{Z}/5 \times \mathbb{Z}/7 \simeq \mathbb{Z}/35$ par le lemme Chinois.

5. $105 = 3 \times 5 \times 7$. Donc par le théorème de structure des groupes abéliens de type fini, le seul groupe abélien d'ordre 105 est $\mathbb{Z}/105$.

6. Soit maintenant G un groupe non-abélien d'ordre 105.

(a) Par Sylow $N_5(G) = 1, 21$ et $N_7(G) = 1, 15$. Si $N_5(G) = 21$ et $N_7(G) = 15$ on aurait $21 \times 4 = 84$ éléments d'ordre 5 et $15 \times 6 = 90$ éléments d'ordre 7, ce qui serait trop.

(b) Soit $S_p \in \mathcal{S}_p(G)$, $p = 5, 7$. Notons $\{p, q\} = \{5, 7\}$. On peut supposer, quitte à échanger p, q que S_p est normal dans G. Donc $N := S_pS_q \subset G$ est un sous-groupe d'ordre $pq = 35$ puisque $S_p \cap S_q = 1$.

(c) On a $[G : N] = 3$ donc, d'après (2), N est normal dans G. D'après (4), N est abélien donc $N_5(N) = N_7(N) = 1$ et la conclusion résulte de (3).

(d) Soit $S_3 \in \mathcal{S}_3(G)$ Comme $S_7 \lhd G$, $H = S_7S_3 \subset G$ est un sous-groupe d'ordre 21 (puisque $S_3 \cap S_7 = 1$) qui fournit un complément dans G au sous-groupe normal S_5 dans G. Autrement dit, la suite exacte courte

$$1 \to S_5 \to G \to G/S_5 \to 1$$

est scindée et on a $G \simeq H \rtimes G/S_5$. De plus, comme $\mathrm{Aut}(S_5) \simeq \mathbb{Z}/4$ et qu'il n'y a pas de morphisme de groupes non-trivial d'un groupe d'ordre 21 dans $\mathbb{Z}/4$, ce produit semi-direct est direct.

(e) Pour que G soit non abélien, il faut que H soit non-abélien. Or on sait déjà que $H = S_7 \rtimes S_3$. La conclusion résulte du fait qu'il n'y a qu'un seul morphisme de groupes non-trivial $\mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/7) \simeq \mathbb{Z}/6$ (celui qui envoie 1 sur l'unique élément d'ordre 3 de $\mathbb{Z}/6$).

Exercice 3 (Caractères des groupes non-abélien d'ordre p^3)

1. Soit V une représentation irréductible de G et r sa dimension et $A \subset G$ un sous-groupe abélien d'indice minimal. La restriction $V|_A$ se décompose comme somme directe $V|_A \simeq \oplus_{1 \leq i \leq r} L_i$ de représentations de dimension 1 (puisque A est abélien). L'inclusion $L_1 \hookrightarrow V|_A$ induit un morphisme de G-modules $k[G] \otimes_{k[A]} L_1 \to V$, qui est non trivial donc surjectif puisque V est irréductible. En particulier, $\dim(V) \leq \dim k[G] \otimes_{k[A]} L_1) = [G : A]$.

2. Soit p un nombre premier et G un groupe *non abélien* d'ordre p^3.

   (a) On rappelle que si G est un groupe non abélien, $G/Z(G)$ n'est jamais cyclique. En particulier, si G est un p-groupe non abélien, $p^2|[G : Z(G)]$. Mais si G est d'ordre p^2, on a toujours $p||Z(G)|$ donc nécessairement, $Z(G) = G$.

   (b) Comme dans la question précédente, on a $p||Z(G)|$ et, comme G est non abélien, $p^2|[G : Z(G)]$. La seule possibilité est donc $|Z(G)| = p$ *i.e.* $Z(G) \simeq \mathbb{Z}/p$ et $G/Z(G)$ non cyclique d'ordre p^2 donc, d'après le théorème de structure des groupes abéliens de type fini ; $G/Z(G) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$.

   (c) Comme G est non abélien $p||D(G)|$ et comme $G/Z(G)$ est abélien, $D(G) \subset Z(G)$. Donc $D(G) = Z(G)$ et $G^{ab} = G/Z(G) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. Soit $z \in Z(G)$ un générateur de $Z(G)$ et $a, b \in G$ relevant respectivement $(1, 0), (0, 1) \in G/Z(G) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. Tout élement $g \in G$ s'écrit donc de façon unique sous la forme $g = z^i a^j b^k$, $0 \leq i, j, k \leq p-1$. Si $w \in \mathbb{C}$ est une racine primitive p-ième de 1, les représentations irréducibles de dimension 1 de G, qui sont celles obtenues en relevant les représentations irréducibles de G^{ab} sont les morphismes de groupes $\chi_{u,v} : G \twoheadrightarrow G^{ab} \to \mathbb{C}^\times$ définis par $\chi_{u,v}(z^i a^j b^k) = \omega^{uj}\omega^{vk} = \omega^{ui+vk}$, $0 \leq u, v \leq p-1$. Il y en a p^2.

   (d) Notons $p_Z : G \twoheadrightarrow G/Z(G)$ la projection canonique. Le groupe $G_1 := p^{-1}(\langle p(a) \rangle) \subset G$ par exemple contient $Z(G)$ par construction et est normal comme image inverse d'un sous-groupe normal.

   (e) Comme $G/Z(G)$ est abélien, l'action de G sur lui-même par conjugaison stabilise chacune des fibres $p^{-1}(\overline{g})$, $\overline{g} \in G/Z(G)$. G agit trivialement par conjugaison sur la fibre $\ker(p_Z) = Z(G)$, qui se casse donc en p orbites réduites à des singleton. Pour $\overline{g} \neq 0$, G agit non trivialement sur la fibre $p^{-1}(\overline{g}) = \{g, gz, \ldots, gz^{p-1}\}$, qui est de cardinal p. De pus, comme G est un p-groupe, ses orbites sont de longueur 1 ou une puissance de p. Donc la seule possibilité est que G agisse transitivement sur $p^{-1}(\overline{g})$. Autrement dit, $p^{-1}(\overline{g})$ est

exactement une classe de conjugaison de G. En conclusion, on a p classes de conjugaison de cardinal 1 : $C_k = \{z^k\}$, $0 \leq k \leq p-1$ et p^2-1 classes de conjugaison de cardinal p : $C_{\overline{g}} = p^{-1}(\overline{g}) = \{g, gz, \ldots, gz^{p-1}\}$, $0 \neq \overline{g} \in G/Z(G)$.

(f) Notons $n_1, \ldots, n_{p-1}$ la dimension des $p-1 = (p+p^2-1)-p^2$ représentations irréducibles de dimension > 1 de G. On doit avoir $p^2 + n_1^2 + \cdots + n_{p-1}^2 = p^3$. D'après (1) et (2) (a), on a également $n_i \leq p$. Si $n_i < p$ pour un $i = 1, \ldots, p-1$, on aurait $p^3 = p^2 + n_1^2 + \cdots + n_{p-1}^2 < p^2 + (p-1)\cdot p^2 = p^3$: impossible.

(g) On conserve les notations de (2) (c). Pour G_1, on a *a priori* deux possibilités : $G_1 \simeq \mathbb{Z}/p^2$ et $G_1 \simeq \mathbb{Z}/p \times \mathbb{Z}/p$ selon que la suite exacte courte

$$1 \to Z(G) \to G_1 \to G_1/Z(G) \simeq \langle \overline{a} \rangle \to 1$$

se scinde ou non. Dans le premier cas, on peut supposer que $a \in G_1$ est un générateur et que $z = a^p$. Les caractères irréductibles de G_1 sont alors les $\psi_k : G_1 \to \mathbb{C}^\times$ définis par $\psi_k(a) = \omega'^k$, $k = 0, \ldots, p^2-1$, où ω' est une racine p^2-ième de 1. Dans le second cas, les caractères irréductibles de G_1 sont les $\psi_{u,v} : G_1 \to \mathbb{C}^\times$ définis par $\psi_{u,v}(z,a) = \omega^u \omega^v$, $0 \leq u, v \leq p-1$. Dans tous les cas, il existe bien une représentation irréductible L_k de G_1 de caractère χ_k et telle que $\chi_k(z) = \omega^k$. On note ϕ_k le caractère de la représentation induite à G. On peut écrire

$$k[G] \otimes_{k[G_1]} L_k = \oplus_{0 \leq i \leq p-1} b^i \otimes L_k.$$

Il suffit de calculer ϕ_k sur un système de représentants des classes de conjugaison de G.

— On a $z^\ell b^i \otimes 1 = b^i \otimes \chi_k(z)^\ell 1$ donc $\phi_k(z^\ell) = \sum_{1 \leq i \leq p-1} \chi_k(z)^\ell = p\omega^{k\ell}$, $\ell = 0, \ldots, p-1$;

— Si $g = a^j \in G_1$, on a $ab = baz'$ pour un certain $1 \neq z' \in Z(G)$ (puisque $G/Z(G)$ est abélien mais G ne l'est pas) donc $a^j b^i \otimes 1 = b^i a^j z^\ell z'^{ij} \otimes 1 = b^i \otimes \chi_k(a_j)\chi_k(z')^{ij}$ et $\phi_k(a^j) = \chi_k(a_j) \sum_{0 \leq i \leq p-1} \chi_k(z'^j)^i = 0$ car $\chi_k(z')$ est encore une racine p-ième de 1. Si $g = a^j b^\ell \in G \setminus G_1$ avec $1 \leq \ell \leq p-1$, on a $a^j b^\ell b^i \otimes 1 = a^j b^{\ell+i} \otimes 1 = b^{\ell+i} \otimes \chi_k(a^j z'^{\ell+i})$ donc $\phi_k(a^j b^\ell) = 0$.

(h) On calcule $\langle \phi_k, \phi_\ell \rangle_G = \frac{1}{p^3}(p^2 + p^2 \sum_{1 \leq i \leq p-1} \omega^{i(k-\ell)}) = \frac{1}{p^3}(p^2 + p^2 \sum_{1 \leq i \leq p-1} (\omega^{k-\ell})^i) = \delta_{k,\ell}$. En combinant ce résultat à la question (2) (f), on voit qu'on a obtenu toutes les représentations irréductibles de G. Et ceci sans calculer explicitement G.

3. On peut considérer les p-Sylow de $\mathrm{GL}_3(\mathbb{F}_p)$, dont tous les éléments sont d'ordre 1 ou p et le produit semi-direct $\mathbb{Z}/p^2 \rtimes \mathbb{Z}/p$ donné par un morphisme non trivial $\phi : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/p^2) \simeq (\mathbb{Z}/p^2)^\times \simeq \mathbb{Z}/p \times \mathbb{Z}/(p-1)$. (En fait, il n'est pas très difficile de montrer qu'à isomorphisme près, il n'y a pas d'autres groupes d'ordre p^3).

Chapitre 6

Appendice : Un peu de vocabulaire catégoriel

Nous introduisons ici le strict minimum du langage catégoriel. Ce langage permet d'unifier formellement les mathématiques et de formuler de façon très synthétique certains résultats. Sa puissance vient du fait que tout résultat prouvé au niveau catégoriel s'applique automatiquement à toute catégorie qui en vérifie les hypothèses. Même si nous n'utiliserons ce langage que pour formuler des énoncés, nous encourageons vivement le lecteur à poursuivre plus avant ; il pourra par exemple consulter les notes de cours [S10].
Une *catégorie* $\mathcal{C}$ est la donnée de

- Un ensemble d'*objets*, noté $Ob(\mathcal{C})$;
- Pour tout $X, Y \in Ob(\mathcal{C})$, un ensemble de *morphismes*, noté $\mathrm{Hom}_{\mathcal{C}}(X, Y)$;
- Pour tout $X, Y, Z \in Ob(\mathcal{C})$, une *loi de composition*

$$\circ : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

devant satisfaire aux deux axiomes suivants

- $\circ$ est associative ;
- Pour tout $X \in Ob(\mathcal{C})$ il existe $Id_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ tel que
  - $Id_X \circ f = f$, pour tout $Y \in Ob(\mathcal{C})$ et $f \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$;
  - $f \circ Id_X = f$, pour tout $Y \in Ob(\mathcal{C})$ et $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

En général, on écrira $X \in \mathcal{C}$ plutôt que $X \in Ob(\mathcal{C})$ et $f : X \to Y$ (un morphisme dans $\mathcal{C}$) plutôt que $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Etant donnée une catégorie $\mathcal{C}$, on note $\mathcal{C}^{op}$ la catégorie définie par

- $Ob(\mathcal{C}^{op}) = Ob(\mathcal{C})$;
- Pour tout $X, Y \in \mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

Exemple 6.0.1 Voici quelques catégories classiques.

- Ens : catégorie des ensembles ;
- Grp : catégorie des groupes finis ;
- Si A est un anneau commutatif, $\mathrm{Alg}_{/A}$: catégorie des A-algèbres associatives unitaires ;
- Si A est un anneau (pas forcément commutatif)
  - $\mathrm{Mod}_{/A}$: catégorie des A-modules à gauche ;
  - $\mathrm{Mod}_{/A^{op}}$: catégorie des A-modules à droite (vus comme A^{op}-modules à gauche) ;

On dit qu'un morphisme $f : X \to Y$ dans $\mathcal{C}$ est un *isomorphisme* s'il existe un morphisme $g : Y \to X$ dans $\mathcal{C}$ tel que $f \circ g = Id_Y$ et $g \circ f = Id_X$.

Un *foncteur* $F : \mathcal{C} \to \mathcal{C}'$ entre deux catégories est la donnée de

— Une application $F : Ob(\mathcal{C}) \to Ob(\mathcal{C}')$;
— Pour tout $X, Y \in \mathcal{C}$, une application $F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X),F(Y))$ compatible avec $\circ$ et les identités *i.e.* telle que
  — $F(I_X) = Id_{F(X)}$, pour tout $X \in \mathcal{C}$;
  — $F(g \circ f) = F(g) \circ F(f)$, pour tout $X \xrightarrow{f} Y \xrightarrow{g} Z$ dans $\mathcal{C}$.

Exemple 6.0.2 On a par exemple construit des foncteurs $A[-] : Grp \to Alg_{/A}$, $(-)^\times : Alg_{/A} \to Grp$, $\mathrm{Hom}_A(M,-) : Mod_{/A} \to Mod_{/A}$, $\mathrm{Hom}_A(-,M) : Mod^{op}_{/A} \to Mod_{/A}$, $f^* : Mod_{/A} \to Mod_{/B}$, $f_* : Mod_{/B} \to Mod_{/A}$ *etc.*. On dispose aussi toujours des foncteurs d'oubli, par exemple $\mathrm{Mod}_{/A} \to Grp \to Ens$ (on oubli la structure de A-module puis celle de groupe).

Etant donnés deux foncteurs $F, G : \mathcal{C} \to \mathcal{C}'$, un *morphisme de foncteurs* $\Theta : F \to G$ est la donnée d'un ensemble de morphismes dans $\mathcal{C}'$

$$\Theta(X) : F(X) \to G(X),\ X \in \mathcal{C}$$

tels que, pour tout $X, Y \in \mathcal{C}$ et $f : X \to Y$ dans $\mathcal{C}$, le diagramme suivant commute

$$\begin{array}{ccc} F(X) & \xrightarrow{\Theta(X)} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[\Theta(Y)]{} & G(Y). \end{array}$$

On vérifie facilement que l'ensemble des foncteurs de $\mathcal{C} \to \mathcal{C}'$ muni des morphismes de foncteurs forme une catégorie $F(\mathcal{C},\mathcal{C}')$ (avec les lois de composition et les identités évidentes).

On dit qu'un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est une *équivalence de catégories* s'il existe un morphismes de foncteurs $G : \mathcal{C}' \to \mathcal{C}$ tel que $F \circ G$ soit isomorphe à $Id_{\mathcal{C}'}$ dans $F(\mathcal{C}',\mathcal{C}')$ et $G \circ F$ soit isomorphe à $Id_{\mathcal{C}}$ dans $F(\mathcal{C},\mathcal{C})$. Cela revient à dire que $F : \mathcal{C} \to \mathcal{C}'$ est *essentiellement surjectif* (*i.e.* pour tout $X' \in \mathcal{C}'$ il existe $X \in \mathcal{C}$ tel que $F(X)$ soit isomorphe à X' dans $\mathcal{C}'$) et *pleinement fidèle* (*i.e.* pour tout $X, Y \in \mathcal{C}$ l'application $F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X),F(Y))$ est bijective [1]).

Montrer que deux catégories sont équivalentes est souvent utile car cela permet de considérer un problème sous deux angles distincts. Parmi les exemples classiques, on peut citer l'équivalence entre la catégorie des revêtements topologiques d'un espace topologique et la catégorie des représentations discrètes de son groupe fondamental topologique ou l'équivalence entre la catégorie des schémas et la catégorie opposée des anneaux.

Une autre notion essentielle, est celle de foncteur représentable, derrière laquelle se cache la notion d'objet universel, dont (vous avez déjà rencontré et dont) nous rencontrerons de nombreux exemples. On dit qu'un foncteur $F : \mathcal{C} \to Ens$ est représentable (dans $\mathcal{C}$) s'il existe $X \in \mathcal{C}$ et un isomorphisme de foncteurs

$$\Theta : \mathrm{Hom}_{\mathcal{C}}(X,-) \tilde{\to} F.$$

On dit alors que $(X, \theta(X)(Id_X))$ *représente* F ou est *universel pour* F.

Remarque 6.0.3 De la même façon, on dit qu'un foncteur $F : \mathcal{C}^{op} \to Ens$ est représentable (dans $\mathcal{C}$) s'il existe $X \in \mathcal{C}$ et un isomorphisme de foncteurs

$$\Theta : \mathrm{Hom}_{\mathcal{C}}(-,X) \tilde{\to} F.$$

Etant donnée une catégorie $\mathcal{C}$, introduisons le foncteur

$$\begin{array}{rccl} h_{\mathcal{C}} : & \mathcal{C}^{op} & \to & F(\mathcal{C}, Ens) \\ & X & \to & \mathrm{Hom}_{\mathcal{C}}(X,-) \\ & u : Y \to X & \to & - \circ u. \end{array}$$

Le lemme suivant, bien qu'élémentaire, est essentiel.

1. Plus précisément, si ces applications sont injectives, on parle de foncteur *fidèle* et si elles sont surjectives, de foncteur *plein*.

Lemme 6.0.4 (Yoneda) *Pour tout $X \in \mathcal{C}$ et pour tout foncteur $F : \mathcal{C} \to Ens$, on a un isomorphisme*

$$\begin{array}{rccc} \Phi(X,F) : & \mathrm{Hom}_{F(\mathcal{C},Ens)}(h_{\mathcal{C}}(X),F) & \tilde{\to} & F(X) \\ & \Theta = (\Theta(Y))_{Y\in\mathcal{C}} & \to & \Theta(X)(Id_X) \end{array}$$

fonctoriel en X et F. Son inverse est donné par

$$\begin{array}{rccc} \Psi(X,F) : & F(X) & \tilde{\to} & \mathrm{Hom}_{F(\mathcal{C},Ens)}(h_{\mathcal{C}}(X),F) \\ & e & \to & (f : X \to Y \mapsto F(f)(e))_{Y\in\mathcal{C}}. \end{array}$$

En appliquant le lemme 6.0.4 au cas $F = h_{\mathcal{C}}(Y)$, on obtient que le foncteur $h_{\mathcal{C}} : \mathcal{C}^{op} \to F(\mathcal{C}, Ens)$ est pleinement fidèle. Il est alors facile d'en déduire

— qu'un morphisme $u : X \to Y$ est un isomorphisme dans $\mathcal{C}$ si et seulement si pour tout $Z \in \mathcal{C}$ l'application

$$- \circ u : \mathrm{Hom}_{\mathcal{C}}(Y,Z) \to \mathrm{Hom}_{\mathcal{C}}(X,Z)$$

est bijective.

— que si (X,e) et (X',e') représentent dans $\mathcal{C}$ un même foncteur $F : \mathcal{C} \to Ens$, alors il existe un unique isomorphisme $f : X \to X'$ dans $\mathcal{C}$ tel que $F(f)(e) = e'$. On dit que l'objet universel (X,e) pour $F : \mathcal{C} \to Ens$ est *unique à un unique isomorphisme près.*

Exemple 6.0.5 (Produits et coproduits) Etant donnée une catégorie $\mathcal{C}$ et une famille d'objets $\underline{X} = X_i$, $i \in I$, on peut définir les foncteurs

$$\Pi^{\underline{X}} = \prod_{i\in I} \mathrm{Hom}_{\mathcal{C}}(-, X_i) : \mathcal{C}^{op} \to Ens$$

et

$$\Pi_{\underline{X}} = \prod_{i\in I} \mathrm{Hom}_{\mathcal{C}}(X_i, X) : \mathcal{C} \to Ens$$

Si $\Pi^{\underline{X}}$ (resp. $\Pi_{\underline{X}}$) est représentable, on dit que le couple $(Z, \underline{p} = (p_i : Z \to X_i)_{i\in I})$ (resp. $(Z, \underline{\iota} = (\iota_i : X_i \to Z)_{i\in I})$) qui le représente est le produit (resp. coproduit) des X_i, $i \in I$ et on le note $(\prod_{i\in I} X_i, \underline{p})$ (resp. $(\bigsqcup_{i\in I} X_i, \underline{\iota})$).

On peut citer bien d'autres exemples élémentaires d'objets universels : les noyaux conoyaux, les produits tensoriels, les limites inductives et projectives, les objets 'libres' (groupes libres, anneaux de polynômes *etc.*).

Deux foncteurs $F : \mathcal{C} \to \mathcal{C}'$ et $G : \mathcal{C}' \to \mathcal{C}$ sont dits *adjoints*[2] si on a un isomorphisme de foncteurs $\mathcal{C} \times \mathcal{C}' \to Ens$

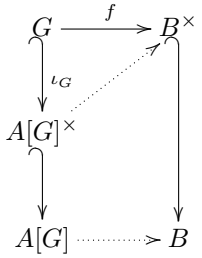
$$\mathrm{Hom}_{\mathcal{C}'}(F(-),+) \tilde{\to} \mathrm{Hom}_{\mathcal{C}}(-, G(+)).$$

Supposons $F : \mathcal{C} \to \mathcal{C}'$ donné alors, d'après le lemme de Yoneda, si $G : \mathcal{C}' \to \mathcal{C}$ existe, il est unique (Pour tout $X' \in \mathcal{C}'$, l'objet $G(X') \in \mathcal{C}$ représente le foncteur $\mathrm{Hom}_{\mathcal{C}'}(F(-), X') : \mathcal{C} \to Ens$.

Exemple 6.0.6 La A-algèbre $A[G]$ a la propriété universelle suivante : pour toute A-algèbre B et morphisme de groupe

$$f : G \to B^{\times}$$

il existe un unique morphisme de A-algèbres $A[f] : A[G] \to B$ tel que $A[f] \circ \iota_G = f$:



Inversement, tout morphisme de A-algèbre $F : A[G] \to B$ induit un morphisme de groupes $F \circ \iota_G : G \to B^{\times}$. On a en fait un isomorphisme de foncteurs $Grp \times Alg_{/A} \to Grp$

$$\mathrm{Hom}_{Grp}(-, (+)^{\times}) \tilde{\to} \mathrm{Hom}_{Alg_{/A}}(A[-], +).$$

2. Plus précisément, F est adjoint à gauche de G et G est adjoint à droite de F.

Autrement dit, les foncteurs $A[-] : Grp \to Alg_{/A}$ et $(-)^\times : Alg_{/A} \to Grp$ sont adjoints.
On a également vu que les produits tensoriels, selon le point de vue, étaient adjoints des foncteurs Hom ou des foncteurs de restriction.

Bibliographie

[ABe95] J.L. Alperin and R.B. Bell, *Groups and Representations*, G.T.M. **162**, Springer, 1995.

[AtM69] M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[B09] P. Baumann, *Introduction à la théorie des représentations*, disponible sur http ://www-irma.u-strasbg.fr/ baumann/

[L02] S. Lang, *Algebra (3rd ed.)*, G.T.M. **211**, Springer, 2002.

[S10] P. Schapira, *Categories and homological algebra*, disponible sur http ://people.math.jussieu.fr/~schapira/lectnotes/

[Se79] J.-P. Serre, *Groupes finis*, cours donnés à l'ENSJF, 1978-1979.

[Se92] J.-P. Serre, *Topics in Galois Theory*, Notes written by Henri Darmon, Jones and Bartlett Publishers, Boston, 1992.

[Se98] J.-P. Serre, *Représentations linéaires des groupes finis (5ème ed.)*, Hermann, 1998.

[W95] C.A. Weibel, *An introduction to homological algebra*, Cambridge University Press, 1995.

Index

A division (anneau), 26
Abelianisé (groupe), 41
ACC (groupe), 39
Adjonction, 71
Adjonction-1 (commutatif), 14
Adjonction-1 (non commutatif), 16
Adjonction-2 (commutatif), 15
Adjonction-2 (non commutatif), 17
Artinien (module), 18

Burnside (théorème), 59

Caractère (groupe), 54
Catégorie, 69
Cohomologie (groupe), 43
Conoyau (module), 11
Coproduit, 71

DCC (groupe), 39
Dérivé (groupe), 41

Equivalence de catégories, 70
Extension (groupe), 40
Extension (module), 30

Foncteur, 69
Frattini (groupe), 42

Gradué (groupe), 39

Indécomposable (groupe), 39
Indécomposable (module), 18
Induit (module), 61
Irréductible (module), 26

Jordan-Holder (théorème, groupe), 39
Jordan-Holder (théorème, module), 29

Krull-Schmidt (théorème, groupe), 39
Krull-Schmidt (théorème, module), 19

Libre (module), 10
Local (anneau), 18

Mackey (Critère), 64
Maschke (théorème), 28
Module, 7
Morphisme de foncteurs, 70

Nilpotent (groupe), 38, 42
Noetherien (module), 17
Noyau (module), 11

Principal (anneau), 20
Produit, 9, 71
Produit semi-direct (groupe), 40
Produit tensoriel, 13

Quotient (module), 11

Radical de Jacobson (anneau), 50
Résoluble (groupe), 42

Schur (Lemme), 26
Schur-Zassenhauss (théorème), 41
Semisimple (anneau), 47
Semisimple (module), 27
Semisimplification (module), 30
Serpent (lemme du), 12
Simple (anneau), 49
Simple (groupe), 39
Simple (module), 26
Somme directe, 9
Suite de composition (module), 28
Suite exacte (module), 12
Suite exacte courte (module), 12
Suite exacte courte scindée (module), 12
Sylow (groupe), 36

Torsion (module), 21
Type fini (module), 17

Yoneda (lemme), 71

anna.cadoret@polytechnique.edu
anna.cadoret@imj-prg.fr
IMJ-PRG - Sorbonne Université,
Paris, FRANCE.