Notes et résumés, Cours d'algèbre (cursus "Maths-Info", M1)

(Université Denis Diderot Paris 7, septembre 2005 – janvier 2006)

(Marc Hindry)

A. Groupes de actions de groupes

B. Modules

C. Corps et anneaux

D. Théorie de Galois (résumé)

Introduction. Le cours comporte une partie révision et approfondissement des notions de groupes et actions de groupes. On y démontre notamment les théorèmes de Sylow; on introduit la notion de groupe résoluble et on montre que les groupes de permutations $\mathcal{S}_n$ ne sont pas résolubles pour $n \geq 5$. Le chapitre "groupe abélien" rappelle la structure des groupes $(\mathbf{Z}/n\mathbf{Z})^*$ et n'est pas traité en cours. La deuxième partie du cours traite succintement des modules (de type fini sur un anneau principal) avec comme objectif d'étudier les $\mathbf{Z}$-modules (alias les groupes abéliens) et les K-espaces vectoriels munis d'un endomorphisme (devenant ainsi des $K[X]$-modules). Une série de rappels sur les corps est inclus, ce qui permet ensuite de développer le clou du sujet : la théorie de Galois, qui tresse une belle guirlande liant polynômes, extensions de corps et groupes. En particulier on démontre le célèbre énoncé dû à Galois : "Une équation est résoluble par radicaux si et seulement si son groupe de Galois est résoluble; en particulier l'équation générale de degré ≥ 5 n'est par résoluble par radicaux".

Les racines de $X^2 + aX + b = 0$ s'écrivent $(-a \pm \sqrt{a^2 - 4b})/2$. Pour résoudre par radicaux une équation du 3ème degré on peut procéder ainsi

(1) On se ramène, quitte à faire une translation à l'équation : $X^3 + pX + q = 0$.
(2) Si α_1, α_2, α_3 sont les racines et j une racine troisième primitive de l'unité, on introduit $\beta_1 = \alpha_1 + j\alpha_2 + j^2\alpha_3$ et $\beta_2 = \alpha_1 + j^2\alpha_2 + j\alpha_3$. On montre que $\gamma_1 = \beta_1^3$ et $\gamma_2 = \beta_2^3$ sont racines de l'équation $Y^2 + 27qY - 27p^3 = 0$
(3) On résoud le système linéaire $0 = \alpha_1 + \alpha_2 + \alpha_3$, $\beta_2 = \alpha_1 + j^2\alpha_2 + j\alpha_3$, $\beta_1 = \alpha_1 + j\alpha_2 + j^2\alpha_3$ et $\beta_2 = \alpha_1 + j^2\alpha_2 + j\alpha_3$ qui permet d'exprimer les α_i en termes de β_1, β_2.

Pour résoudre par radicaux une équation du 4ème degré on peut procéder ainsi (en suivant Descartes plutôt que Cardan).

(1) On se ramène, quitte à faire une translation à l'équation : $X^4 + pX^2 + qX + r = 0$.
(2) On factorise $X^4 + pX^2 + qX + r = (X^2 + aX + b)(X^2 + cX + d)$ sur $K(a)$ où a^2 est racine de l'équation du troisième degré $Y^3 - 2pY^2 + (p^2 - 4r)Y - q^2 = 0$ et $c = -a$, $b = \frac{1}{2}(p - a^2 - q/a)$ et $d = \frac{1}{2}(p - a^2 + q/a)$.
(3) On résoud enfin $X^2 + aX + b = 0$ et $X^2 + cX + d$.

La recherche de méthode similaire pour les équations de degré supérieur ou égal à 5 a occupé pas mal de mathématiciens avant qu'Abel et Galois ne démontrent son impossibilité. Le cours détaille cette découverte.

Bibliographie partielle et subjective.

Références d'algèbre générale (jusqu' à l'agrégation) :

Cours d'algèbre, D. Perrin (collection Ellipses) (ne traite pas la théorie de Galois)

Algebra, S. Lang (collection Addison-Wesley).

Algebra, M. Artin (collection Prentice-Hall).

Algebra, Birkhoff & MacLane (collection Chelsea) .

Pour la théorie de Galois :

Galois Theory, . I. Stewart, Chez Chapman & Hall.

Théorie de galois, Escofier, Chez Dunod.

Enfin quelques cours accessibles sur la toile.

Field and Galois Theory, Page de J. Milne, http://www.jmilne.org/math/

Algèbre corporelle, Page de A. Chambert-Loir,
http://name.math.univ-rennes1.fr/antoine.chambert-loir/publications/poly.html

A. GROUPES ET ACTIONS ET GROUPES

Une présentation des groupes, de leurs quotients avec des exemples. La notion centrale présentée est celle d'action de groupe.

A.1. Généralités sur les groupes.

Définition. Un *groupe* est la donnée d'un ensemble G et d'une loi interne $G \times G \to G$ vérifiant
(i) (élément neutre) Il existe $e \in G$ tel que, pour tout $g \in G$, on ait $e * g = g * e = g$.
(ii) (associativité) Pour tout $g, g', g'' \in G$, on a $(g * g') * g'' = g * (g' * g'')$.
(iii) (inverse d'un élément) Pour tout $g \in G$, il existe $g' \in G$ tel que, $g' * g = g * g' = e$.

Remarques. L'ensemble G s'appelle l'*ensemble sous-jacent*; par abus de langage, on parlera du groupe G, sous-entendant ainsi la loi que l'on notera le plus souvent comme un produit; l'inverse de g sera alors noté g^{-1}. Lorsque la loi vérifie de plus $g * g' = g' * g$, on dira que le groupe est *commutatif* ou *abélien* et l'on notera alors parfois la loi comme une addition et l'inverse de g s'écrira $-g$.

Exemples. Vous connaissez déjà bien sûr des groupes comme $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ (munis de l'addition), ou $\mathcal{S}_n$ (le groupe des permutations sur n éléments) ou $\mathrm{GL}(n, \mathbf{R})$, le groupe des matrices de taille $n \times n$ inversibles à coefficients réels. Comme exemple initial, ajoutons l'ensemble des transformations linéaires préservant une figure dans le plan, l'espace ou plus généralement $\mathbf{R}^n$; ces transformations sont d'ailleurs des isométries. Concrètement l'ensemble des transformations linéaires du plan préservant un polygone régulier à n côtés est un groupe noté D_n (dont on montre ci-dessous qu'il est de cardinal $2n$); l'ensemble des transformations linéaires du plan préservant un cube est un groupe (dont on peut montrer qu'il est de cardinal 48);

Premiers calculs. Dans un groupe, "on peut toujours simplifier", c'est-à-dire que $xy = xz$ entraîne $y = z$. En effet il suffit de multiplier par x^{-1} :

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z.$$

L'inverse de x^{-1} est x et l'inverse de xy est $y^{-1}x^{-1}$, en effet :

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e.$$

Définition.

$$x^n := \begin{cases} e & \text{si } n = 0 \\ \underbrace{x \dots x}_{(n \text{ fois})} & \text{si } n > 0 \\ \underbrace{x^{-1} \dots x^{-1}}_{(|n| \text{ fois})} & \text{si } n < 0 \end{cases}$$

On a $x^m.x^n = x^{m+n}$ et $(x^m)^n = x^{mn}$. Si $y = gxg^{-1}$ alors $y^n = gx^ng^{-1}$.

Un sous-ensemble H d'un groupe G est un *sous-groupe* si la loi de groupe sur G induit une loi de groupe sur H. C'est-à-dire si H est stable par multiplication, passage à l'inverse et contient

l'élément neutre (l'associativité est alors automatique). On voit facilement que cette condition équivaut à dire que $e \in H$ et que $x, y \in H$ entraîne $xy^{-1} \in H$. De même il est immédiat de montrer que l'intersection de sous-groupes est un sous-groupe.

Si S est un sous-ensemble d'un groupe G on définit le *sous-groupe engendré par* S comme le plus petit sous-groupe de G contenant S, i.e. l'intersection de tous les sous-groupes contenant H. C'est un exercice facile de voir que c'est aussi l'ensemble des produits $x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$ avec $r \geq 0$, $x_i \in S$ et $\epsilon_i = \pm 1$.

Soit G_1 et G_2 deux groupes. On définit le *produit de groupes* qui a comme ensemble sous-jacent $G_1 \times G_2$ par la loi de composition :

$$(g_1, g_2) * (g_1', g_2') := (g_1 g_1', g_2 g_2').$$

Une application $f : G_1 \to G_2$ entre deux groupes est un *homomorphisme de groupes* si elle vérifie

$$\forall x, y \in G_1,\ f(xy) = f(x)f(y);$$

c'est un *isomorphisme* si elle est bijective, un *automorphisme* si de plus $G_1 = G_2$. On appelle *noyau* le sous-groupe $\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e\}$ et *image* le sous-groupe $f(G_1) = \{y \in G_2 \mid \exists x \in G_1,\ f(x) = y\}$. Il est immédiat que le composé d'homomorphismes (resp. d'isomorphismes, resp. d'automorphismes) est encore un homomorphisme (resp. un isomorphisme, resp. un automorphisme). En particulier l'ensemble des automorphismes d'un groupe G est un groupe que l'on notera $\mathrm{Aut}(G)$. Remarquons aussi que la bijection réciproque d'un isomorphisme est automatiquement un homomorphisme.

Exemples. L'application $x \mapsto x^2$ est un homomorphisme de groupes si et seulement si le groupe G est *abélien* (i.e. commutatif). Soit $x \in G$, l'application $\phi_x : G \to G$ définie par $\phi_x(y) := xyx^{-1}$ est un automorphisme appelé *automorphisme intérieur* de G; de plus l'application $x \mapsto \phi_x$ de G dans $\mathrm{Aut}(G)$ est un homomorphisme de groupes. L'ensemble des images par automorphisme intérieur d'un élément $y \in G$ s'appelle la *classe de conjugaison* de y.

Décrivons maintenant l'exemple cité plus haut de groupe d'origine géométrique: le groupe dièdral D_n.

Théorème. *Le groupe des isométries planes d'un polygone régulier à n côtés ($n \geq 3$), de centre O a pour cardinal $2n$; il contient n rotations, les rotations d'angle $2k\pi/n$ et de centre O et n symétries, les symétries orthogonales fixant les droites passant par O et un sommet ou le milieu d'une arête.*

Preuve. On voit facilement que les isométries décrites dans l'énoncé laissent invariant le polygone, il s'agit de démontrer que ce sont les seules. Pour cela on va utiliser le lemme suivant (dont on laisse la preuve en exercice) :

Lemme. *Soit s une isométrie plane laissant invariant un polygone régulier à n côtés, de centre O et sommets $A_1, \ldots, A_n$ alors*

- Si s fixe deux sommets adjacents, alors s est l'identité;

- Si s fixe un sommet A_i, alors s est soit l'identité soit la symétrie par rapport à la droite OA_i.

Soit maintenant σ une isométrie du polygone, il existe une rotation r d'angle $2k\pi/n$ telle que $r \circ \sigma(A_1) = A_1$ (en effet ces rotations permutent circulairement les sommets). Donc, d'après le

lemme, ou bien $r \circ \sigma = id$ et alors σ est une rotation d'angle $-2k\pi/n$ ou bien $r \circ \sigma$ est la symétrie s_1 par rapport à OA_1 et $\sigma = r^{-1} \circ s_1$. Cela suffit pour voir que $\mathrm{card}(D_n) = 2n$ et permet de vérifier (indirectement) que $r^{-1} \circ s_1$ est une des symétries décrites. □

Remarques. Les rotations forment un sous-groupe de D_n isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Si r est une rotation et s une symétrie, alors $srs^{-1} = srs = r^{-1}$ (vérifiez-le). On peut utiliser cela pour montrer que le centre de D_n est trivial si n est impair et d'ordre 2 (engendré par la rotation d'angle π) si n est pair. On peut aussi interpréter D_2 comme le groupe des isométries planes laissant invariant un segment (il est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).

A.2. Quotient d'un groupe par un sous-groupe.

On intoduit les notations suivantes, si A et B sont des parties d'un groupe G. On pose $A.B := \{a.b \mid a \in A, b \in B\}$ et de même $A^{-1} := \{a^{-1} \mid a \in A\}$. On écrira $g.A$ pour $\{g\}.A$

Soit H un sous-groupe de G, on définit deux relations d'équivalence par

$$x\mathcal{R}y \Leftrightarrow xH = yH \Leftrightarrow y^{-1}x \in H$$
$$x\mathcal{R}'y \Leftrightarrow Hx = Hy \Leftrightarrow xy^{-1} \in H$$

On notera G/H l'ensemble quotient $G/\mathcal{R}$ (resp. $H\backslash G$ l'ensemble quotient $G/\mathcal{R}'$). Vérifions, par exemple, que $\mathcal{R}$ est une relation d'équivalence. On a $x^{-1}x = e \in H$ donc $x\mathcal{R}x$. Si $x\mathcal{R}y$ alors $y^{-1}x \in H$ donc $x^{-1}y = (y^{-1}x)^{-1} \in H$ et $y\mathcal{R}x$. Si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $y^{-1}x \in H$ et $z^{-1}y \in H$ donc $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$ et $x\mathcal{R}z$.

Remarque. Hormis ces relations d'équivalence "jumelles", la seule autre relation d'équivalence "intéressante" est la relation de conjugaison : $x\mathcal{R}y$ si il existe $g \in G$ avec $y = gxg^{-1}$. Les classes d'équivalence pour cette relation s'appelle naturellement *classes de conjugaison*.

Il faut faire attention qu'en général $gH \neq Hg$ (on verra plus loin que l'égalité n'est vraie pour tout g que si le sous-groupe H est distingué). Par contre la transformation $A \mapsto A^{-1}$ envoie gH sur Hg^{-1} donc il y a une bijection naturelle entre G/H et $H\backslash G$. Remarquons ensuite que les classes d'équivalence ont toutes le même cardinal que H. En effet l'application de H vers gH (resp. $H.g$) qui, à x associe gx (resp. xg) est visiblement une bijection. On a ainsi démontré le théorème suivant

Théorème. (Lagrange) *Soit G un groupe et H un sous-groupe, alors* $\mathrm{card}(G/H) = \mathrm{card}(H\backslash G)$ *et*

$$\mathrm{card}(G) = \mathrm{card}(H)\,\mathrm{card}(G/H).$$

Exemples. On tire facilement que si $x \in G$ et G fini, alors l'ordre de g divise $\mathrm{card}(G)$. Ainsi, comme $(\mathbf{Z}/p\mathbf{Z})^*$ a pour cardinal $p-1$ on en tire que, pour a entier premier avec p, on a $a^{p-1} \equiv 1 \bmod p$, ou encore que pour tout entier $a^p \equiv a \bmod p$ ("petit théorème" de Fermat). Plus généralement, si on note $\phi(n) = \mathrm{card}(\mathbf{Z}/n\mathbf{Z})^*$ on obtient que, pour a entier premier avec n, on a $a^{\phi(n)} \equiv 1 \bmod p$ (théorème d'Euler).

Définition. Un sous-groupe H de G est *distingué* si, pour tout $g \in G$, on a $H = gHg^{-1}$.

Remarquons qu'il est équivalent de demander que, pour tout $g \in G$, on ait $gH = Hg$ ou encore que, pour tout $g \in G$, on ait $H \subset gHg^{-1}$. Par ailleurs, le noyau d'un homomorphisme $f : G \to G'$ est toujours distingué; en effet si $y \in \mathrm{Ker}(f)$ alors $f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = f(x)e'f(x)^{-1} = e'$ donc $xyx^{-1} \in \mathrm{Ker}(f)$.

Proposition. *L'intersection de sous-groupes distingués est un sous-groupe distingué. Si $f : G \to G'$ est un homomorphisme de groupes et si $H' \triangleleft G'$ alors $f^{-1}(H') \triangleleft G$; si $H \triangleleft G$ alors $f(H) \triangleleft f(G)$.*

Preuve. Immédiat. □

Remarquons que dans la dernière partie de la proposition, on ne peut pas conclure que $f(H)$ est distingué dans G', sauf si f est surjective.

Le principal intérêt des sous-groupes distingués est le suivant.

Proposition. *Soit H un sous-groupe de G. Il existe une structure de groupe sur l'ensemble G/H telle que la surjection canonique $s : G \to G/H$ soit un homomorphisme si et seulement si le sous-groupe H est distingué.*

Preuve. Supposons qu'une telle structure existe sur G/H alors H est le noyau de l'homomorphisme $s : G \to G/H$ donc est distingué dans G. Supposons inversement H distingué dans G, on est amené à définir une loi sur G/H par la formule $(xH) * (yH) = xyH$ (pour que s soit un homomorphisme) et le point est de vérifier que cette formule est bien définie, i.e. que si $x' \in xH$ et $y' \in yH$ alors $x'y'H = xyH$. Or on a bien, puisque H est distingué et $x' = xh$, $y' = yh'$, l'égalité $x'y'H = xhyh'H = xhyH = xhHy = xHy = xyH$. L'application $s : G \to G/H$ est surjective et vérifie donc $s(x) * s(y) = s(xy)$; on en tire immédiatement que G/H muni de la loi $*$ est un groupe. □

Théorème. (Propriété universelle du quotient) *Soit $f : G \to G'$ un homomorphisme de groupes. Soit H un sous-groupe et $s : G \to G/H$ la surjection canonique. Il existe une application $\hat{f} : G/H \to G'$ telle que $f = \hat{f} \circ c$ si et seulement si $H \subset \mathrm{Ker}(f)$. Dans ce cas, si de plus H est un sous-groupe distingué (et donc G/H un groupe), alors $\hat{f}$ est un homomorphisme de groupes, $\hat{f}(G/H) = f(G)$ et $\mathrm{Ker}(\hat{f}) = \mathrm{Ker}(f)/H$.*

Preuve. La condition ensembliste garantissant l'existence de $\hat{f}$ est que $s(x) = s(y)$ entraîne $f(x) = f(y)$. Or $s(x) = s(y)$ équivaut à $xH = yH$ ou encore $x^{-1}y \in H$ alors que $f(x) = f(y)$ équivaut à $f(x^{-1}y) = e'$ ou encore $x^{-1}y \in \mathrm{Ker}(f)$. La deuxième partie est immédiate sauf peut-être la détermination du noyau de $\hat{f}$. Soit xH un élément de G/H qui soit dans le noyau de $\hat{f}$ alors $f(x) = \hat{f}(xH) = e'$ donc $x \in \mathrm{Ker}(f)$ d'où l'égalité $\mathrm{Ker}(\hat{f}) = \mathrm{Ker}(f)/H$. □

Corollaire. *Soit $f : G \to G'$ un homomorphisme de groupe, alors $f(G) \cong G/\mathrm{Ker}(f)$.*

Preuve. On applique la propriété universelle avec $H = \mathrm{Ker}(f)$ alors $\mathrm{Ker}(\hat{f}) = \mathrm{Ker}(f)/\mathrm{Ker}(f)$ est trivial donc $\hat{f}$ injective. □

Applications. a) Le sous-groupe $\langle x \rangle$ engendré par un élément $x \in G$ est isomorphe soit à $\mathbf{Z}$ (on dira que x est d'*ordre infini*) soit à $\mathbf{Z}/n\mathbf{Z}$ avec $n \geq 1$ (on dira que x est d'*ordre* n). En effet

d'après le corollaire appliqué à l'homomorphisme défini par $f(m) := x^m$ de $\mathbf{Z}$ vers $\langle x \rangle \subset G$, on a $\langle x \rangle \cong \mathbf{Z}/\operatorname{Ker}(f)$.

b) Le noyau de l'homorphisme $G \to \operatorname{Aut}(G)$ qui a un élément associe l'automorphisme intérieur associé est le centre de G, noté $Z(G)$; si l'on note $\operatorname{Int}(G)$ le groupe des automorphismes intérieurs, on a donc $\operatorname{Int}(G) \cong G/Z(G)$.

A.3. Action de groupe.

La notion suivante est fondamentale; d'une part les groupes apparaissent naturellement dans la plupart des problèmes à travers leurs actions (ou représentations) et d'autre part, pour étudier les groupes eux-mêmes, on verra qu'il est souvent avantageux de les faire agir.

Définition. Une *action* d'un groupe G sur un ensemble X est une application $\Phi : G \times X \to X$ telle que
(i) $\Phi(e, x) = x$.
(ii) $\Phi(g, \Phi(g', x)) = \Phi(gg', x)$.

Remarque. Il est équivalent de se donner un homomorphisme $\rho : G \to \operatorname{Bij}(X)$. La correspondance est donnée par

$$\rho(g)(x) = \Phi(g, x).$$

On abrègera en général $\Phi(g, x)$ en $g.x$.

Exemple. Si ϕ est une bijection de X sur X, alors $\mathbf{Z}$ agit sur X par l'action $n \cdot x = \phi^n(x)$. Le groupe $\mathrm{GL}(2, \mathbf{R})$ agit naturellement sur $\mathbf{R}^2$; voici une action moins évidente. Choisissons $G = \mathrm{SL}(2, \mathbf{R})$ et $\mathcal{H} := \{z \in \mathbf{C} \mid \operatorname{Im}(z) > 0\}$ le demi-plan de Poincaré, l'application suivante est une action de groupe:

$$\begin{array}{ccc} G \times \mathcal{H} & \to & \mathcal{H} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z & \mapsto & \frac{az+b}{cz+d} \end{array}$$

Une action définit une relation d'équivalence

$$x \mathcal{R} y \Leftrightarrow \exists g \in G,\ y = g.x$$

dont les classes d'équivalence $G.x = \{g.x \mid g \in G\}$ s'appellent les *orbites* de l'action. L'ensemble quotient $X/\mathcal{R}$ sera noté X/G, l'orbite de x sera notée $\mathcal{O}(x)$.

Définitions. Le *stabilisateur* d'un élément $x \in X$ est le sous-groupe de G des éléments qui fixe x, i. e. $G_x = \{g \in G \mid g \cdot x = x\}$. Le *noyau* d'une action est l'intersection des stabilisateurs de tous les points (c'est aussi le noyau de l'homomorphisme associé). Une action est dite *fidèle* si son noyau est trivial, *transitive* s'il n'y a qu'un orbite.

Exemples. Le noyau de l'action de $\mathrm{SL}(2, \mathbf{R})$ sur $\mathcal{H}$ donnée ci-dessus est $\pm I$, l'action de $\mathrm{SL}(2, \mathbf{R})$ est transitive, le stabilisateur de $i \in \mathcal{H}$ est $\mathrm{SO}(2, \mathbf{R}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbf{R},\ a^2 + b^2 = 1 \right\}$.

Remarques. Si on dispose d'une action $G \times X \to X$, on peut lui associer les actions suivantes:
(a) Pour tout sous-groupe H de G, une action de H sur X.
(b) Si $K = \cap_{x \in X} G_x$ est le noyau de l'action, alors on hérite d'une action de G/K sur X qui est fidèle.

(c) Si $\mathcal{P}(X)$ (resp. $\mathcal{P}_n(X)$) désigne l'ensemble des parties de X (resp. l'ensemble des parties de cardinal n) alors onpeut définir une action de G sur $\mathcal{P}(X)$ (resp. $\mathcal{P}_n(X)$) par $g \cdot A = \{g \cdot a \mid a \in A\}$.

Formule des classes (1ère forme).

$$\mathrm{card}(X) = \sum_{C \in X/G} \mathrm{card}(C)$$

Formule des classes (2ème forme).

$$\mathrm{card}(\mathcal{O}(x)) = \mathrm{card}(G/G_x).$$

En effet, considérons l'application $f : G \to \mathcal{O}(x)$ définie par $f(g) = g.x$. On a alors $f(g) = f(g')$ si et seulement si $g.x = g'.x$ ou encore $x = (g^{-1}g').x$ ou encore $g^{-1}g' \in G_x$ ou encore $gG_x = g'G_x$. Ainsi, d'après la propriété universelle du quotient, f passe au quotient pour donner une bijection $\hat{f} : G/G_x \to \mathcal{O}(x)$. On en tire

Théorème. (Formule des classes) *Soit G fini agissant sur X fini et soit R un système d'éléments de X représentant les classes de X/G, alors*

$$\mathrm{card}(X) = \sum_{x \in R} \mathrm{card}(G/G_x) = \sum_{x \in R} \frac{\mathrm{card}(G)}{\mathrm{card}(G_x)}.$$

On note X^G l'ensemble des points fixes, c'est-à-dire

$$X^G = \{x \in X \mid \forall g \in G,\ g \cdot x = x\} = \{x \in X \mid G_x = G\}$$

Un groupe de cardinal une puissance d'un nombre premier p sera appelé un p-groupe.

Corollaire. *Soit G un p-groupe agissant sur un ensemble fini X alors*

$$|X^G| \equiv |X| \bmod p.$$

En particulier, si $|X|$ n'est pas divisible par p, il existe un point fixe.

Preuve. On écrit la formule des classes en observant que l'orbite d'un point fixe est, bien sûr, réduite à un point et que les autres orbites ont pour cardinal $(G : G_x)$ avec $G_x \neq G$ donc ce cardinal est divisible par p et $|X| \equiv \sum_{x \in X^G} 1 \bmod p$. □

Corollaire. *Le centre d'un p-groupe est non trivial.*

Preuve. Soit G un p-groupe. Considérons l'action de G sur lui-même par conjugaison (i.e. $X = G$ et $g \cdot x = gxg^{-1}$). On voit aisément que $X^G = Z(G)$ et donc $|Z(G)|$ est divisible par p d'après le corollaire précédent. □

Exercice. Montrer que si $(G : H) = p$ est le plus petit nombre premier divisant $\mathrm{card}(G)$ alors H est distingué dans G. (Indication : considérer l'action de G sur G/H par translation, introduire l'homomorphisme associé $\rho : G \to \mathcal{S}_p = \mathrm{Bij}(G/H)$ et montrer que $H = \mathrm{Ker}(\rho)$).

A.4. Théorèmes de Sylow.

Le théorème suivant recense essentiellement ce que l'on peut dire d'un groupe fini en ne connaissant que son cardinal.

Théorème. (Sylow) *Soit p un nombre premier et G un groupe de cardinal $p^r m$ avec m non divisible par p.*

(i) Il existe un sous-groupe P de cardinal p^r (un tel sous-groupe s'appelle un p-sous-groupe de Sylow de G).

(ii) Soit H un p-sous-groupe et P un p-sous-groupe de Sylow de G, alors il existe $g \in G$ tel que $H \subset gPg^{-1}$. En particulier deux p-sous-groupes de Sylow de G sont conjugués.

(iii) Soit n_p le nombre de p-sous-groupes de Sylow de G. Alors $n_p \equiv 1 \bmod p$ et n_p divise m.

Preuve. Il s'agit de variations sur le thème des actions de groupes et de la formule des classes.

(i) Considérons l'action de G sur lui-même par translation et l'action induite sur $X = \mathcal{P}_{p^r}(G)$. Si R désigne un ensemble des représentants des classes d'équivalence, on a par la formule des classes

$$C_{mp^r}^{p^r} = |X| = \sum_{A \in R} (G : G_A).$$

Admettons provisoirement (voir lemme ci-dessous) que p ne divise pas $|X|$. Alors il existe une orbite, disons celle de A_0 de cardinal premier avec p. On a donc $(G : G_{A_0})$ non divisible par p donc $|G_{A_0}|$ est divisible par p^r. Mais par ailleurs, si l'on choisit $a_0 \in A_0$, on peut considérer l'application $G_{A_0} \to A$ définie par $g \mapsto ga_0$ qui est clairement injective donc $|G_{A_0}|$ est majoré par p^r et divisible par p^r donc égal à p^r. Ainsi G_{A_0} est un p-sous-groupe de Sylow. La preuve sera complète grâce au lemme

Lemme. *Soit m non divisible par un nombre premier p, alors*

$$C_{mp^r}^{p^r} \equiv m \bmod p.$$

On peut démontrer cela directement, en effet

$$C_{mp^r}^{p^r} = \frac{(mp^r)!}{(p^r)!(mp^r - p^r)!} = m \prod_{k=1}^{p^r-1} \left(\frac{mp^r - k}{p^r - k} \right).$$

Or si $k = p^s \ell$ alors $(mp^r - k)(p^r - k)^{-1} = (mp^{r-s} - \ell)(p^{r-s} - \ell)^{-1} \equiv 1 \bmod p$ d'où le lemme.

Une deuxième preuve du lemme consiste à appliquer la formule des classes précédente avec $G = \mathbf{Z}/p^r\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$, vérifier que $\mathbf{Z}/p^r\mathbf{Z} \times \{0\}$ est le seul sous-groupe à p^r éléments et que les seules parties à p^r éléments qu'il laisse stable sont les $\mathbf{Z}/p^r\mathbf{Z} \times \{x\}$; toutes ces parties forment une orbite unique de cardinal m, les autres parties vérifient $(G : G_A) \equiv 0 \bmod p$ et donc on a bien $C_{mp^r}^{p^r} = |\mathcal{P}_{p^r}(G)| \equiv m \bmod p$.

(ii) Soit P un p-sous-groupe de Sylow (dont l'existence est maintenant garantie) et H un p-sous-groupe de G. Nous faisons agir H sur G/P par la formule $(h, gP) \mapsto hgP$. Comme le cardinal de G/P n'est pas divisible par p et que H est un p-groupe, on en déduit l'existence d'un point fixe. Donc il existe $g_0 \in G$ tel que pour tout $h \in H$ on ait $hg_0P = g_0P$ ou encore $hg_0 \in g_0P$ ou encore $h \in g_0Pg_0^{-1}$. Ainsi $H \subset g_0Pg_0^{-1}$; si de plus H est un p-sous-groupe de Sylow, on a donc égalité.

(iii) Notons $X = Syl_p$ l'ensemble des p-sous-groupes de Sylow de G et n_p son cardinal. Si $P \in X$ alors gPg^{-1} est de nouveau un p-sous-groupe de Sylow de G. On dispose ainsi d'une action

par conjugaison de G sur X qui est transitive d'après le résultat précédent. Si P est un p-sous-groupe de Sylow de G, on a clairement $P \subset G_P$ puisque P est un sous-groupe, par conséquent

$$n_p = (G : G_P) = \frac{|G|}{(G_P : P)|P|} = \frac{m}{(G_P : P)}.$$

Ainsi n_p divise m. Considérons maintenant l'action de P sur $Sy\ell_p$, toujours par conjugaison. L'élément P est visiblement fixe; nous allons montrer qu'il est l'unique point fixe et nous pourrons alors conclure que

$$n_p \equiv |Sy\ell^P| \equiv 1 \bmod p$$

Soit donc $Q \in Sy\ell^P$ et introduisons $G_0 = \langle P, Q\rangle$ le sous-groupe engendré par P et Q (argument dit "de Frattini"). On constate que P et Q sont encore deux p-sous-groupes de Sylow de G_0 et par conséquent sont conjugués dans G_0 : il existe $y \in G_0$ tel que $P = yQy^{-1}$ mais Q est fixé par P (par hypothèse) et, bien sûr, est fixé par Q donc par G_0 et on peut conclure que $P = Q$. □

Corollaire. *Soit G un groupe fini. Il existe un élément d'ordre p dans G si et seulement si p divise* $\mathrm{card}(G)$.

Preuve. La nécessité provient du théorème de Lagrange. Supposons que p divise $\mathrm{card}(G)$, alors il existe un p-sous-groupe non trivial H (par exemple un p-sous-groupe de Sylow) et $y \in H \setminus \{e\}$. L'élément y est d'ordre une puissance de p, disons p^r avec $r \geq 1$. On voit immédiatement que l'élément $x = y^{p^{r-1}}$ est d'ordre p. □

A.5. Théorème de Jordan-Holder et groupes résolubles.

Si un groupe G possède un sous-groupe distingué H non trivial (distinct de G et $\{e\}$), on peut écrire une suite exacte $1 \to H \to G \to G/H \to 1$ et considérer qu'on a ramené l'étude de G à l'étude de deux groupes plus petits : H et G/H. Toutefois il est inexact de penser que l'on sait tout sur G si l'on ne connait que H et G/H : par exemple si $\mathbf{Z}/3\mathbf{Z} \cong H \triangleleft G$ et $G/H \cong \mathbf{Z}/2\mathbf{Z}$ alors $G \cong \mathbf{Z}/6\mathbf{Z}$ ou $\mathcal{S}_3$. Ces considérations nous amènent naturellement aux deux définitions suivantes.

Définition. Un groupe est *simple* s'il n'admet aucun sous-groupe distingué non trivial.

L'exemple de groupe simple le plus facile à décrire est $\mathbf{Z}/p\mathbf{Z}$, ce sont d'ailleurs les seuls groupes simples abéliens; on les exclut parfois par convention (parce qu'ils sont trop simples!). On verra au paragraphe suivant que les groupes $\mathcal{A}_n$ sont simples lorsque $n \geq 5$.

Définition. Une *suite de composition* d'un groupe G est la donnée d'une suite de sous-groupes emboités i.e. $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$ telle que $G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est simple. Une autre suite de composition $G = G'_0 \supset G'_1 \supset \ldots \supset G'_m = \{e\}$ est dite *équivalente* à la première si $m = n$ et il existe une permutation $\sigma : [1, n] \to [1, n]$ telle que $G_{\sigma(i)}/G_{\sigma(i)+1} \cong G'_i/G'_{i+1}$.

Remarquons que demander que G_i/G_{i+1} soit simple équivaut à demander que la suite G_i soit maximale au sens que si $G_i \supset H \supset G_{i+1}$ avec $H \triangleleft G_i$ alors $H = G_i$ ou G_{i+1}.

Théorème. (Jordan-Holder) *Soit G un groupe fini, alors G admet une suite de composition qui est unique à équivalence près.*

Preuve. La première partie est claire, démontrons donc la deuxième. Supposons données deux suites de composition $G = H_0 \supset H_1 \supset \ldots \supset H_m$ et $G = K_0 \supset K_1 \supset \ldots \supset K_n$ et supposons (raisonnement par induction) que le théorème est déjà démontré pour les groupes admettant une suite de composition de longueur $\leq m-1$. Si $H_1 = K_1$ alors on peut appliquer l'hypothèse de récurrence à H_1 et conclure. Dans le cas contraire on introduit une suite de composition de $H_1 \cap K_1$ notée (attention à la numérotation) $H_1 \cap K_1 = L_2 \supset L_3 \supset \ldots \supset L_r$ de sorte que l'on a le diagramme suivant où les flèches indiquent que le groupe en bas de la flèche est un sous-groupe distingué du groupe au-dessus.

$$
\begin{array}{ccccccc}
 & & & G & & & \\
 & & \swarrow & & \searrow & & \\
 & H_1 & & & & K_1 & \\
 & \downarrow & \searrow & & \swarrow & \downarrow & \\
 & H_2 & & H_1 \cap K_1 & & K_2 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & H_3 & & L_3 & & K_3 & \\
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow & & \downarrow & & \downarrow & \\
\{e\} & = & H_m & & L_r & & K_n & = \{e\}
\end{array}
$$

De plus tous les quotients sont simples; c'est clair par construction, sauf pour les inclusions de $H_1 \cap K_1$ dans K_1 et H_1 où cela résulte du lemme suivant

Lemme. *Dans la situation ci-dessus, si $H_1 \neq K_1$ alors $G/H_1 \cong K_1/H_1 \cap K_1$ et $G/K_1 \cong H_1/H_1 \cap K_1$. En particulier $K_1/H_1 \cap K_1$ et $H_1/H_1 \cap K_1$ sont simples.*

Preuve. L'application $K_1 \hookrightarrow K_1H_1 \to K_1H_1/H_1$ a pour noyau $H_1 \cap K_1$ d'où l'isomorphisme classique $K_1/H_1 \cap K_1 \cong K_1H_1/H_1$. Par ailleurs on a $K_1 \lhd K_1H_1 \lhd G$, mais, vues les hypothèses, $K_1 \neq K_1H_1$ donc $H_1K_1 = G$. □

Suite de la preuve. On dispose donc de deux suites de composition de H_1 de longueur $m-1$ et $r-1$; on peut donc appppliquer l'hypothèse de récurrence et conclure que $m = r$ et les quotients $\{H_1/H_2, \ldots, H_{m-1}/H_m\}$ et $\{H_1/H_1 \cap K_1, H_1 \cap K_1/L_3, \ldots, L_{r-1}/L_r\}$ sont isomorphes deux à deux. Le même raisonnement appliqué aux deux suites de composition de K_1 montre que $n = r$ et que les quotients $\{K_1/K_2, \ldots, K_{n-1}/K_n\}$ et $\{K_1/H_1 \cap K_1, H_1 \cap K_1/L_3, \ldots, L_{r-1}/L_r\}$ sont isomorphes deux à deux. On en tire, en se souvenant du lemme précédent, que les quotients $\{G/H_1, H_1/H_2, \ldots, H_{m-1}/H_m\}$ sont isomorphes (à permutation près) aux quotients $\{K_1/H_1 \cap K_1, H_1/H_1 \cap K_1, H_1 \cap K_1/L_3, \ldots, L_{r-1}/L_r\}$ donc également aux quotients $\{K_1/K_2, H_1/H_1 \cap K_1, K_2/K_3, \ldots, K_{n-1}/K_n\}$ et enfin aux quotients $\{K_1/K_2, G/K_1, K_2/K_3, \ldots, K_{n-1}/K_n\}$; ce qui achève la démonstration. □

Il est naturel d'introduire la définition suivante qui a par ailleurs une grande importance historique : d'après Galois, les équations polynomiales $P(x) = 0$ dont on peut exprimer les racines à l'aides des opérations de corps et de radicaux $\sqrt[n]{}$ sont celles qui ont un groupe résoluble (voir la dernière partie du cours).

Définition. Un groupe G est *résoluble* s'il existe une suite $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$ telle que $G_{i+1} \lhd G_i$ et G_i/G_{i+1} est abélien.

Si le groupe G est fini, il revient au même de demander que ses facteurs de Jordan-Holder soient isomorphes à $\mathbf{Z}/p\mathbf{Z}$. Un des théorèmes les plus difficiles de la théorie des groupes finis (Feit-Thomson) dit qu'un groupe de cardinal impair est toujours résoluble.

Proposition. *Un sous-groupe et un quotient d'un groupe résoluble est encore résoluble. Soit H un sous-groupe distingué de G alors*

$$G \text{ résoluble } \Leftrightarrow \quad H \text{ et } G/H \text{ sont résolubles.}$$

Preuve. Si G est résoluble, soit $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ telle que G_{i+1}/G_i est abélien, posons alors $H_i = H \cap G_i$ et, si $H \triangleleft G$ et $s : G \to G/H$, posons $K_i = s(G_i)$. On a alors $\{e\} = H_0 \subset H_1 \subset \ldots \subset H_n = H$ et l'homomorphisme $H_{i+1} = H \cap G_{i+1} \to G_{i+1}/G_i$ a pour noyau H_i qui est donc distingué dans H_{i+1} et de plus H_{i+1}/H_i est isomorphe à un sous-groupe de G_{i+1}/G_i donc est abélien et H est bien résoluble. De même l'homomorphisme $G_{i+1} \to K_{i+1} \to K_{i+1}/K_i$ est surjectif et son noyau contient G_i donc K_{i+1}/K_i est un quotient de G_{i+1}/G_i et est donc abélien et ainsi G/H est résoluble. Inversement si H et G/H sont résolubles, soit $\{e\} = H_0 \subset H_1 \subset \ldots \subset H_n = H$ et $\{e\} = K_0 \subset K_1 \subset \ldots \subset K_m = G/H$ les suites de composition associées. Considérons $s : G \to G/H$ et posons $G_i := H_i$ pour $0 \leq i \leq n$ et $G_{n+j} := s^{-1}(K_j)$ pour $0 \leq j \leq m$; la notation est cohérente car pour $j = 0$ on obtient $G_n = s^{-1}(K_0) = H$. L'homomorphisme $G_{n+j+1} \to K_{j+1} \to K_{j+1}/K_j$ est surjectif de noyau $s^{-1}(K_j) = G_{n+j}$ qui est donc distingué dans G_{n+j+1} et tel que G_{n+j+1}/G_{n+j} est abélien, ce qui achève la preuve. □

Exemples. 1) Un groupe abélien est bien sûr résoluble. 2) Les groupes diédraux D_n sont résolubles puisqu'ils contiennent un sous-groupe H_n (le sous-groupe des rotations) cyclique tel que $D_n/H_n \cong \mathbf{Z}/2\mathbf{Z}$. 3) Un p-groupe est résoluble. On peut montrer cela par récurrence sur le cardinal $|G| = p^n$; en effet on a vu que le centre $Z(G)$ est non trivial donc $G/Z(G)$ est un p-groupe de cardinal p^m avec $m < n$ et est donc résoluble (hypothèse de récurrence) et $Z(G)$ abélien donc G est résoluble.

Exercices. Montrer qu'un groupe de cardinal ≤ 100 et $\neq 60$ est résoluble (Indication : utiliser les théorèmes de Sylow!). Montrer qu'un groupe G de cardinal $2n$ avec n impair contient un sous-groupe distingué d'indice 2 et en particulier n'est pas simple (Indication : l'action par translation induit $\rho : G \to \mathcal{S}_{2n}$, montrer que $\mathrm{Ker}(\epsilon \circ \rho)$ est d'indice 2 dans G). En admettant le théorème de Feit-Thomson, montrer que G est résoluble.

A.6 Le groupe $\mathcal{S}_n$.

Le groupe $\mathcal{S}_n$ est le groupe des bijections de l'ensemble $[1, n] = \{1, 2, \ldots, n\}$, il est isomorphe au groupe des bijections d'un ensemble fini de cardinal n. Il intervient donc chaque fois qu'un groupe agit sur un ensemble fini, en particulier dans les questions de combinatoire. D'un autre côté, le groupe $\mathcal{S}_n$ est "trop" riche pour pouvoir être entièrement décrit; par exemple tout groupe fini est sous-groupe d'un $\mathcal{S}_n$: en effet, l'action de G par translation sur lui-même est fidèle et induit donc une injection de G dans les bijections de G.

Le *support* d'une permutation $\sigma \in \mathcal{S}_n$ est le sous-ensemble $\{i \in [1,n] \mid \sigma(i) \neq i\}$. Le groupe $\mathcal{S}_n$ agit transitivement sur $[1,n]$ et le stabilisateur de n est naturellement isomorphe à $\mathcal{S}_{n-1}$ donc la formule des classes nous dit que $\mathrm{card}(\mathcal{S}_n/\mathcal{S}_{n-1}) = n$ d'où l'on tire aisément par récurrence

$$\mathrm{card}(\mathcal{S}_n) = n!$$

Une première façon de noter les éléments de $\mathcal{S}_n$ est simplement d'écrire la liste exhaustive des images, par exemple la permutation σ de $\mathcal{S}_{10}$ définie par $\sigma(1) = 2$, $\sigma(2) = 6$, $\sigma(3) = 3$, $\sigma(4) = 5$, $\sigma(5) = 8$, $\sigma(6) = 4$, $\sigma(7) = 10$, $\sigma(8) = 9$, $\sigma(9) = 1$ et $\sigma(10) = 7$, peut être notée $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 6 & 3 & 5 & 8 & 4 & 10 & 9 & 1 & 7 \end{pmatrix}$. Cette notation est toutefois lourde et ne reflète pas vraiment les propriétés de σ (par exemple : quel est son ordre?). La situation est un peu similaire à l'écriture d'un nombre entier : l'écriture de la décomposition en facteurs premiers contient beaucoup plus d'information arithmétique que la donnée du nombre en base 10. Il est donc utile d'introduire une telle notion pour les permutations.

Définition. Un *cycle de longueur* m (ou m-cycle) est associé à un sous-ensemble ordonné $I = \{i_1 \ldots, i_m\}$ et est donné par $\sigma(i_1) = i_2, \ldots, \sigma(i_{m-1}) = i_m$, $\sigma(i_m) = i_1$ et, pour tout $j \notin I$, $\sigma(j) = j$. L'ensemble I s'appelle le *support* du cycle. On note une telle permutation $\sigma = (i_1 \ldots, i_m)$. Un cycle de longueur 2 est une *transposition*.

Remarquons que, avec la notation introduite $(i_1 \ldots, i_m) = (i_2 \ldots, i_m, i_1)$, etc. Un cycle de longueur m a clairement pour ordre m. L'intérêt de cette notion provient en bonne partie du résultat suivant.

Théorème. (Décomposition en cycles) *Soit $\sigma \in \mathcal{S}_n \setminus \{id\}$ il existe $\sigma_1, \ldots, \sigma_r$, cycles de longueurs $m_1, \ldots, m_r$ ayant des supports disjoints, tels que*

$$\sigma = \sigma_1 \cdots \sigma_r.$$

De plus, l'union des supports des σ_i est le support de σ, les σ_i commutent entre eux et sont uniques (à l'ordre près).

Preuve. On décompose l'ensemble $X = [1,n]$ sous l'action du groupe engendré par σ en orbites. Sur chaque orbite X_i de cardinal $m \geq 2$, la permutation σ agit comme un cycle σ_i de support X_i. Il est alors immédiat que σ est égale au produit des σ_i et celles-ci sont uniquement déterminées par σ. Deux permutations dont les supports sont disjoints commutent; le reste est clair. □

Si σ s'écrit $\sigma_1 \cdots \sigma_r$ comme dans l'énoncé du théorème, i.e. est produit de cycles à supports disjoints de longueur $m_1, \ldots, m_r$, on dira que σ est de *type* $(m_1, \ldots, m_r)$.

Corollaire. *Soit σ une permutation de type $(m_1, \ldots, m_r)$, alors son ordre est égal au PPCM de $m_1, \ldots, m_r$.*

Preuve. Notons $M := \mathrm{PPCM}(m_1, \ldots, m_r)$. Comme $\sigma = \sigma_1 \ldots \sigma_r$ on a $\sigma^M = \sigma_1^M \ldots \sigma_r^M = id$ et d'autre part si $\sigma^N = \sigma_1^N \ldots \sigma_r^N = id$, alors σ^N agit sur le support de σ_i comme σ_i^N et comme l'identité donc $\sigma_i^N = id$ et m_i divise N donc M divise N. □

Exemple. La décomposition en produit de cycles de la permutation donnée ci-dessus s'écrit $\sigma = (1,2,6,4,5,8,9)(7,10)$. Elle a donc pour ordre 14.

Corollaire. *La classe de conjugaison d'une permutation de type $(m_1, \ldots, m_r)$ est l'ensemble des permutations de même type.*

Preuve. Commençons par vérifier la "formule-clef" suivante où ρ désigne une permutation quelconque :

$$\rho(i_1, \ldots, i_m)\rho^{-1} = (\rho(i_1), \ldots, \rho(i_m)).$$

Notons $\sigma = (i_1, \ldots, i_m)$. Si $j \notin \{\rho(i_1), \ldots, \rho(i_m)\}$ alors $\rho^{-1}(j) \notin \{i_1, \ldots, i_m\}$ donc $\rho\sigma\rho^{-1}(j) = j$. Si $j = \rho(i_k)$ alors $\rho^{-1}(j) = i_k$ donc $\sigma\rho^{-1}(j) = i_{k+1}$ (avec la convention que $m + 1 = 1$) et $\rho\sigma\rho^{-1}(j) = \rho(i_{k+1})$ comme annoncé. Ainsi le conjugué d'un m-cycle est un m-cycle; de plus si $\sigma' = (j_1, \ldots, j_m)$ est un autre m-cycle on peut choisir $\rho \in \mathcal{S}_n$ telle que $\rho(i_k) = j_k$ et donc $\sigma' = \rho\sigma\rho^{-1}$. Ainsi la classe de conjugaison d'un m-cycle est l'ensemble des m-cycles. Dans le cas général, si $\sigma = \sigma_1 \ldots \sigma_r$, alors $\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1}) \ldots (\rho\sigma_r\rho^{-1})$ donc le conjugué d'une permutation de type $m_1, \ldots, m_r$ est encore du même type et réciproquement. □

La *signature* d'une permutation $\sigma \in \mathcal{S}_n$ peut être définie par la formule

$$\epsilon(\sigma) := \prod_{1 \leq i < j \leq n} \frac{(\sigma(i) - \sigma(j))}{(i - j)}.$$

Proposition. *L'application $\epsilon : \mathcal{S}_n \to \{\pm 1\}$ est un homomorphisme de groupes. La signature d'une transposition est égale à -1. Son noyau est noté $\mathcal{A}_n$ et s'appelle le groupe alterné.*

Preuve. Observons que $\eta_\sigma(i, j) = (\sigma(i) - \sigma(j))/(i - j)$ ne dépend que de la paire $\{i, j\}$. On peut écrire

$$\epsilon(\sigma\tau) = \prod_{\{i,j\}} \frac{\sigma\tau(i)) - \sigma\tau(j)}{\tau(i) - \tau(j)} . \frac{\tau(i) - \tau(j)}{i - j} = \left(\prod_{\{i,j\}} \eta_\sigma(\tau(i), \tau(j)) \right) \epsilon(\tau) = \epsilon(\sigma)\epsilon(\tau).$$

Pour la deuxième affirmation, il suffit de vérifier que $\epsilon((1, 2)) = -1$ ce qui est élémentaire. □

Remarques. On sait (Cf plus loin) que toute permutation peut s'écrire comme le produit d'un certain nombre de transpositions, disons $\sigma = \tau_1 \ldots \tau_s$; on en déduit que $\epsilon(\sigma) = (-1)^s$. Un m-cycle est le produit de $m - 1$ transpositions donc la signature d'un m-cycle est $(-1)^{m-1}$, la signature d'une permutation de type $(m_1, \ldots, m_r)$ est $(-1)^{m_1 + \ldots + m_r - r}$.

Corollaire. *Le sous-groupe $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ et* $\mathrm{card}(\mathcal{A}_n) = n!/2$.

Preuve. Immédiat. □

Générateurs de $\mathcal{S}_n$ et $\mathcal{A}_n$.

Tout d'abord l'ensemble des cycles est un ensemble de générateurs de $\mathcal{S}_n$ d'après le théorème de décomposition en cycles. Ensuite tout cycle peut s'écrire comme produit de transpositions car

$$(i_1, \ldots, i_m) = (i_1, i_2)(i_2, i_3) \cdots (i_{m-1}, i_m)$$

donc l'ensemble des transpositions est un ensemble de générateurs de $\mathcal{S}_n$. On peut même se restreindre au sous-ensemble des transpositions de la forme $(i, i+1)$ pour $1 \leq i \leq m-1$. En effet si $i < j$ et $\rho = (i + 1, i + 2) \ldots (j - 1, j)$ alors $\rho(i) = i$ et $\rho(j) = i + 1$ donc $\rho(i, j)\rho^{-1} = (i, i + 1)$.

A titre d'exercice on pourra montrer qu'une transposition et un cycle de longueur n forme un système minimal de générateurs. Montrons que les cycles de longueur 3 engendrent $\mathcal{A}_n$. Un élément $\sigma \in \mathcal{A}_n$ s'écrit comme un produit d'un nombre pair de transpositions (puisque $\epsilon(\sigma) = +1$) donc $\mathcal{A}_n$ est engendré par les éléments de la forme $(i,j)(k,\ell)$, où l'on peut supposer $(i,j) \neq (k,\ell)$. Si $\mathrm{card}\,(\{i,j\}\{k,\ell\}) = 1$ alors $(i,j)(k,\ell)$ est un 3-cyle, sinon on peut écrire $(i,j)(k,\ell) = (i,j)(j,k)(j,k)(k,\ell)$ et chacune des permutations $(i,j)(j,k)$ et $(j,k)(k,\ell)$ est un 3-cycle.

Exemple de sous-groupes de $\mathcal{S}_n$ (resp. de $\mathcal{A}_n$).

(a) Si $n \leq 2$, le groupe $\mathcal{S}_n$ est commutatif, cependant si $n \geq 3$, le centre de $\mathcal{S}_n$ est trivial. En effet si $\rho \in Z(\mathcal{S}_n)$ alors $(i,j) = (\rho(i), \rho(j))$ donc $\{\rho(i), \rho(j)\} = \{i,j\}$; supposons qu'il existe i avec $\rho(i) \neq i$, alors pour tout $j \neq i$ on a $\rho(i) = j$, ce qui est aburde dès que $n \geq 3$.

(b) Soit $m \leq n$, un cycle de longueur m dans $\mathcal{S}_n$ est déterminé par son support (il y a $C_n^m = \binom{n}{m}$ possibilités) et l'ordre donné à ce support (à permutation cyclique près, soit $(m-1)!$ possibilités). Ainsi $\mathcal{S}_n$ contient $(m-1)!C_n^m$ cycles de longueur m et le nombre de sous-groupes cycliques que ceux-ci engendrent est $(m-1)!C_n^m/\phi(m)$. Attention : ce n'est pas, en général, le nombre de sous-groupes cycliques de cardinal m, néanmoins, si p est premier et $p \leq n < 2p$, un sous-groupe de cardinal p est engendré par un p-cycle et il y a donc $(p-2)!C_n^p$ tels sous-groupes. (Exercice : vérifier dans ce cas un des théorèmes de Sylow qui affirme que $(p-2)!C_n^p \equiv 1 \bmod p$ et en déduire le théorème de Wilson $(p-2)! \equiv 1 \bmod p$).

(c) Soit $n = n_1 + n_2 + \ldots + n_r$ une partition de n, alors on dispose d'une injection $\mathcal{S}_{n_1} \times \ldots \times \mathcal{S}_{n_r} \hookrightarrow \mathcal{S}_n$ en associant à $(\sigma_1, \ldots, \sigma_r \in \mathcal{S}_{n_1} \times \ldots \times \mathcal{S}_{n_r}$ la permutation définie, pour $1 \leq i \leq r$ et $1 \leq j \leq n_i$, par $\sigma(n_1 + \ldots + n_{i-1} + j) = n_1 + \ldots + n_{i-1} + \sigma_i(j)$.

(d) Il existe néanmoins d'autres façons de plonger $\mathcal{S}_m$ dans $\mathcal{S}_n$. Ainsi le groupe $\mathcal{S}_5$ possède six 5-sous-groupes de Sylow d'où une injection $\mathcal{S}_5 \hookrightarrow \mathcal{S}_6$. Notons que l'image de $\mathcal{S}_5$ ne stabilise aucun élément puisqu'il agit transitivement.

(e) (centralisateur d'un élément) Soit $\sigma \in \mathcal{S}_n$, on veut déterminer le sous-groupe

$$C(\sigma) := \{\rho \in \mathcal{S}_n \mid \rho\sigma = \sigma\rho\}.$$

Si $\sigma = (i_1, \ldots, i_m)$ un m-cycle, un élément ρ commute avec σ si l'on a l'égalité de cycles $(\rho(i_1), \ldots, \rho(i_m))$ donc si et seulement si le sous-ensemble $\{i_1, \ldots, i_m\}$ est une orbite (sous l'action du sous-groupe engendré par σ) sur lequel σ agit par permutation circulaire. Si l'on identifie le sous-groupe des permutations de support $\{i_1, \ldots, i_m\}$ (resp. fixant le sous-ensemble $\{i_1, \ldots, i_m\}$)avec $\mathcal{S}_m$ (resp. $\mathcal{S}_{n-m}$) alors $\mathcal{S}_{n-m} \hookrightarrow C(\sigma)$; de plus le sous-groupe $\mathcal{S}_{n-m}$ est distingué dans $C(\sigma)$ et le quotient est isomorphe au sous-groupe engendré par σ (i.e. à $\mathbf{Z}/m\mathbf{Z}$); en particulier $\mathrm{card}(C(\sigma)) = (n-m)!m$. Montrer plus généralement que si σ est le produits de r_2 transpositions, r_3 cycles de longueur 3 etc (avec disons $n = r_1 + 2r_2 + 3r_3 + \ldots + sr_s$) alors

$$\mathrm{card}(C(\sigma)) = r_1!r_2! \ldots r_s!2^{r_1} \ldots s^{r_s}.$$

Le groupe $\mathcal{S}_1$ est trivial, le groupe $\mathcal{S}_2$ est commutatif. Le groupe $\mathcal{S}_3$ possède trois sous-groupes de cardinal 2 (autant que de transpositions), un unique sous-groupe de cardinal 3 : le sous-groupe $\mathcal{A}_3$ (puisque $\mathcal{A}_3 \lhd \mathcal{S}_3$) qui est cyclique. En particulier $\mathcal{S}_3$ est résoluble. Le groupe $\mathcal{S}_4$ contient quatre sous-groupes isomorphes à $\mathcal{S}_3$ qui sont tous conjugués (les stabilisateurs de $1, 2, 3, 4$) et donc quatre sous-groupes de cardinal 3 (qui sont tous conjugués). Les 2-sous-groupes de Sylow de $\mathcal{S}_4$ sont au nombre de 3 et sont isomorphes au groupe dièdral D_4. En effet l'action de D_4 sur

les sommets d'un carré induit un isomorphisme de D_4 sur un sous-groupe de $\mathcal{S}_4$; ce sous-groupe ne peut être distingué car sinon il contiendrait tous les éléments d'ordre 2 ou 4 de $\mathcal{S}_4$ donc il y a 3 tels sous-groupes (qui sont tous conjugués). On peut en déduire un sous-groupe particulier

Le *sous-groupe de Klein* de $\mathcal{S}_4$ est l'intersection de ses 2-sous-groupes de Sylow, ou encore le sous-groupe constitué de l'élément neutre et des doubles transpositions

$$K := \{id, (1,2)(34), (1,3)(2,4), (1,4)(2,3)\}.$$

Ce sous-groupe est donc distingué dans $\mathcal{S}_4$ et isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. En particulier la suite $\mathcal{S}_4 \supset \mathcal{A}_4 \supset K \supset \{id, (1,2)(34)\} \supset \{id\}$ est une suite de composition avec quotients successifs $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z}$ donc $\mathcal{S}_4$ est résoluble. Le groupe quotient $\mathcal{S}_4/K$ est isomorphe $\mathcal{S}_3$; en effet, si l'on fait agir $\mathcal{S}_4$ sur ses 2-sous-groupes de Sylow, le stabilisateur (normalisateur) de chacun de ces sous-groupes de Sylow est égal à lui-même, donc leur intersection est K; l'homomorphime $\rho : \mathcal{S}_4 \to \mathcal{S}_3$ associé à cette action a donc pour noyau K et est donc surjectif.

Théorème. *Soit H un sous-groupe distingué non trivial de $\mathcal{S}_n$, alors ou bien $H = \mathcal{A}_n$ ou bien $n = 4$ et H est le sous-groupe de Klein. Le groupe $\mathcal{S}_n$ est résoluble si et seulement si $n \leq 4$, le groupe $\mathcal{A}_n$ est simple si et seulement si $n \geq 5$.*

Preuve. Montrons d'abord que, si $n \geq 5$ tous les 3-cycles sont conjugés dans $\mathcal{A}_n$ et donc un sous-groupe distingué qui contient un 3-cycle les contient tous et est donc égal à $\mathcal{A}_n$. Soit $\sigma = (i,j,k)$, dès que $\rho(1) = i, \rho(2) = j$ et $\rho(3) = k$, on a $\rho(1,2,3)\rho^{-1} = (i,j,k)$. A priori $\rho \in \mathcal{S}_n$ mais, si $n \geq 5$ on peut s'arranger pour que $\rho \in \mathcal{A}_n$, quitte à remplacer éventuellement ρ par $\rho(4,5)$.

Montrons que $\mathcal{A}_5$ est simple. Soit $H \neq \{id\}$ sous-groupe distingué de $\mathcal{A}_5$. Si H contient un 3-cycle alors $H = \mathcal{A}_5$. Si H contient une double transposition $\sigma = (i,j)(k,\ell)$, alors, en posant $\rho = (k,\ell,m)$ avec m le cinquième élément, on a $\sigma\rho\sigma\rho^{-1} = (k,\ell,m) \in H$ donc $H = \mathcal{A}_5$. Si H contient un 5-cycle alors il contient un 5-Sylow de $\mathcal{A}_5$ et donc tous et donc les 24 cycles de longueur 5; mais 25 ne divise pas $\mathrm{card}(\mathcal{A}_5) = 60$ donc H contient d'autres éléments donc un 3-cycle ou une double transposition.

Montrons que $\mathcal{A}_{n-1}$ simple entraîne $\mathcal{A}_n$ simple (pour $n \geq 6$). Soit $H \triangleleft \mathcal{A}_n$ un sous-groupe non trivial. Considérons $G_i = \{\sigma \in \mathcal{A}_n \mid \sigma(i) = i\} \cong \mathcal{A}_{n-1}$, on a $H \cap G_i \triangleleft G_i$ donc $H \cap G_i = G_i$ ou $\{id\}$. Si $G_i \subset H$ alors H contient un 3-cycle et $H = \mathcal{A}_n$. Il nous reste à montrer qu'on ne peut avoir $H \cap G_i = \{id\}$. Soit donc $\sigma \in H \setminus \{id\}$. On a $\sigma(1) = i \neq 1$, choisissons $j \neq 1, i$ alors $\sigma(j) = k$ et on peut choisir $\ell, m \notin \{1,i,j,k\}$. Soit $\rho = (j,\ell,m) \in \mathcal{A}_n$ alors $\tau := \rho^{-1}\sigma^{-1}\rho\sigma$ est dans H et $\tau(1) = 1$ alors que $\tau(j) = m$ onc $\tau \in H \cap G_1 \setminus \{id\}$, ce qui est une contradiction.

Enfin montrons que $H \triangleleft \mathcal{S}_n$ et $H \neq \{id\}, \mathcal{S}_n$ entraîne $H = \mathcal{A}_n$ pour $n \geq 5$ (les cas $n \leq 4$ sont laissés en exercice). On a ou bien $H \cap \mathcal{A}_n = \mathcal{A}_n$ mais alors $H = \mathcal{A}_n$ ou bien $H \cap \mathcal{A}_n = \{id\}$ mais alors $\mathrm{card}(H) = 2$ ce qui est impossible car les conjugués d'un produit de transposition ne lui sont pas tous égaux. L'analyse des cas où $n \leq 4$ est laissée au lecteur. □

Remarques. Le groupe $\mathcal{A}_5$ a pour cardinal 60, c'est le plus petit groupe simple (non commutatif); Le groupe $\mathcal{A}_5$ contient 5 "copies" de $\mathcal{A}_4$ (les stabilisateurs de $1,2,3,4,5$) qui contiennent chacun une copie du groupe de Klein, ce qui fournit les cinq 2-sous-groupes de Sylow. En effet si on écrit $K \subset \mathcal{A}_4 \subset \mathcal{A}_5$ on sait que $\mathcal{A}_4$ normalise K et en fait doit être égal au normalisateur de K dans $\mathcal{A}_5$ car K ne peut pas être distingué; il y a donc bien $5 = (\mathcal{A}_5 : \mathcal{A}_4)$ sous-groupes de Sylow.

Montrons qu'un groupe simple G de cardinal 60 est isomorphe à $\mathcal{A}_5$. Un tel groupe n'admet pas d'homomorphisme non trivial vers $\mathcal{S}_4$ (sinon le noyau contredirait la simplicité de G) donc pas d'action non triviale sur des ensembles de cardinal ≤ 4. D'après les théorèmes de Sylow, le nombre de 2-sous-groupes de Sylow est donc *a priori* 5 ou 15, Le nombre de 5-sous-groupes de Sylow est 6 (donc il y a 24 éléments d'ordre 5) et le nombre de 3-sous-groupes de Sylow est 10 (donc il y a 20 éléments d'ordre 3). Supposons $n_2 = 5$, alors l'action de G sur les 2-sous-groupes de Sylow donne une injection $G \hookrightarrow \mathcal{S}_5$. L'image est d'indice deux donc distinguée donc c'est $\mathcal{A}_5$. Supposons $n_2 = 15$, alors un décompte des éléments montre qu'il existe deux 2-sous-groupes de Sylow tels que $\mathrm{card}(P_1 \cap P_2) > 1$ (sinon l'union des 2-sous-groupes de Sylow aurait pour cardinal $(15 \times 3) + 1 = 46$). Soit $x \in P_1 \cap P_2 \setminus \{e\}$, alors P_1 et P_2, étant commutatifs, sont dans le commutateur $C(\sigma)$ qui est donc de cardinal $4m$ avec $m > 1$. Le groupe G agit transitivement sur $G/C(\sigma)$ qui est de cardinal $15/m$. mais on a vu que $m > 1$ et que $15/m \geq 5$ donc $G/C(\sigma)$ a pour cardinal 5 et on en tire un homorphisme $\rho : G \to \mathcal{S}_5$ qui, comme précédemment doit être un isomorphisme avec $\mathcal{A}_5$. (Bien entendu la possibilité $n_2 = 15$ est impossible *a posteriori*).

Exercices (illustrations géométriques). 1) Soit K un corps commutatif, montrer que l'action naturelle de $\mathrm{SL}(2, K)$ sur K^2 induit une action transitive sur $\mathbf{P}^1(K)$ (l'ensemble des droites de K^2 passant par l'origine) et que son noyau est $\{\pm Id\}$. On note $\mathrm{PSL}(2, K)$ le quotient de $\mathrm{SL}(2, K)$ par $\{\pm Id\}$. En déduire les isomorphismes suivants :
(i) $\mathrm{PSL}(2, \mathbf{Z}/2\mathbf{Z}) \cong \mathcal{S}_3$
(ii) $\mathrm{PSL}(2, \mathbf{Z}/3\mathbf{Z}) \cong \mathcal{A}_4 \subset \mathcal{S}_4$
(iii) $\mathrm{PSL}(2, \mathbf{Z}/5\mathbf{Z}) \cong \mathcal{A}_5 \subset \mathcal{A}_6$

2) Considérons G le groupe du cube (qu'on peut supposer centré en l'origine) et faisons-le agir sur les quatre "grandes" diagonales. Montrer que cette action induit un homomorphisme $\rho : G \to \mathcal{S}_4$ dont le noyau est $\{\pm Id\}$ et en déduire que

$$G \cong \mathcal{S}_4 \times \{\pm Id\}.$$

Décrire les isométries correspondant aux transpositions, cycles, etc.

A.7. Groupes abéliens.

Ce paragraphe inclut, à titre de rappels, une description détaillée la structure des groupes $\mathbf{Z}/n\mathbf{Z}$ *et* $(\mathbf{Z}/n\mathbf{Z})^*$*; on y décrit aussi la structure générale des groupes finis abéliens ou même abéliens de type fini.*

Remarquons tout de suite qu'un groupe abélien est la même chose qu'un $\mathbf{Z}$-module (i.e. un "espace vectoriel" sur l'anneau $\mathbf{Z}$). Comme exemples de groupes abéliens nous citerons au départ $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, $(\mathbf{Z}/n\mathbf{Z})^*$, $\mathbf{Q}$, $\mathbf{Q}/\mathbf{Z}$. Un groupe abélien est *de type fini* s'il possède un nombre fini de générateurs; il est dit *libre* s'il possède une base sur $\mathbf{Z}$, *libre de rang fini* s'il possède une base finie (et est donc isomorphe à $\mathbf{Z}^r$). Les groupes abéliens en général ne sont pas libres, en effet $\mathbf{Z}/n\mathbf{Z}$, par exemple, ne peut pas être libre. Dans le groupe $\mathbf{Q}$ deux éléments sont toujours liés mais le groupe n'est pas isomorphe à $\mathbf{Z}$. Un élément $x \in G$ est dit de *torsion* s'il existe $m \geq 1$ tel que $x^m = e$. Tous les éléments de $\mathbf{Q}/\mathbf{Z}$ sont de torsion sans que le groupe soit fini, donc il ne peut pas être de type fini. L'ensemble des éléments de torsion dans G abélien forme un sous-groupe $G_{\mathrm{torsion}} := \{g \in G \mid \exists m \geq 1,\ g^m = e\}$; en effet si x est d'ordre m et y d'ordre n alors $(xy)^{mn} = (x^m)^n (y^n)^m = e$. Observons d'ailleurs que, si de plus m et n sont premiers entre

eux, alors l'ordre de xy est exactement mn; en effet si $(xy)^k = e$, alors $x^{kn} = e$ (resp. $y^{km} = e$) donc m divise kn (resp. n divise km) donc m divise k (resp. n divise k) et enfin mn divise k.

Notation. Dans ce chapitre nous noterons (sauf mention contraire) additivement les groupes abéliens; l'élément neutre de $(G, +)$ sera noté 0.

Les groupes $\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}$ (rappels).

Le groupe $\mathbf{Z}$ est l'unique groupe (à isomorphisme près) qui est cyclique (engendré par un élément) et infini. Tous ses sous-groupes sont du type $m\mathbf{Z}$ pour $m \geq 0$. L'ensemble $\mathbf{Z}$ est également muni d'une multiplication qui en fait un anneau commutatif. Dans cet anneau on a la notion de divisibilité et l'on suppose connue la notion de PGCD et PPCM (que l'on révisera dans le cadre plus général des anneaux). Dans le cas de $\mathbf{Z}$ on voit que la notion d'*idéal* (voir le chapitre sur les anneaux) coïncide avec celle de sous-groupe. On peut en déduire facilement le théorème suivant

Théorème. (Bézout) *Soit $m, n \in \mathbf{Z}$ et soit d leur PGCD, alors il existe $a, b \in \mathbf{Z}$ tels que*

$$d = am + bn.$$

Preuve. L'ensemble $H := m\mathbf{Z} + n\mathbf{Z} = \{am + bn \mid a, b \in \mathbf{Z}\}$ est clairement un sous-groupe; il est donc de la forme $d'\mathbf{Z}$ et il existe a, b tels que $d' = am + bn$. Comme d divise a et b, on voit que d divise $am + bn = d'$ mais a, b appartiennent à H donc d' divise a et b donc d' divise également d et on conclut que $d = d'$ (si l'on a pris soin de les prendre tous les deux positifs). □

Le groupe $\mathbf{Z}/n\mathbf{Z}$ est l'unique groupe cyclique à n éléments (à isomorphisme près) i.e. engendré par un élément d'ordre n. On peut déjà étudier ses générateurs

Proposition. *Soit $m \in \mathbf{Z}$ et $\bar{m}$ sa classe dans $\mathbf{Z}/n\mathbf{Z}$, les trois propriétés suivantes sont équivalentes*
(i) L'élément $\bar{m}$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$.
(ii) Les éléments m et n sont premiers entre eux.
(iii) L'élément $\bar{m}$ est inversible modulo n, c'est-à-dire qu'il existe $m' \in \mathbf{Z}$ tel que $mm' \equiv 1 \bmod n$ ou encore $\bar{m}\bar{m}' = 1 \in \mathbf{Z}/n\mathbf{Z}$.

Preuve. Supposons que $\bar{m}$ engendre $\mathbf{Z}/n\mathbf{Z}$ alors il existe $m' \in \mathbf{Z}$ tel que $m'\bar{m} = 1 \in \mathbf{Z}/n\mathbf{Z}$; ainsi $mm' \equiv 1 \bmod n$ ce qui signifie que m est inversible modulo n. Si $mm' \equiv 1 \bmod n$ alors $mm' = 1 + an$ et donc m est premier avec n. Si m est premier avec n alors, d'après le théorème de Bézout, il existe a, b tels que $am + bn = 1$ donc $a\bar{m} = 1 \in \mathbf{Z}/n\mathbf{Z}$ et donc $\bar{m}$ engendre $\mathbf{Z}/n\mathbf{Z}$. □

En particulier on voit que l'ensemble des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$, qui forment automatiquement un groupe, est égal à

$$(\mathbf{Z}/n\mathbf{Z})^* = \{\bar{m} \in \mathbf{Z}/n\mathbf{Z} \mid m \text{ est premier avec } n\}.$$

On note $\phi(n) := \operatorname{card}((\mathbf{Z}/n\mathbf{Z})^*)$ l'*indicatrice d'Euler*. On en déduit facilement que, si p est premier, $\phi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1}$. Le calcul en général de $\phi(n)$ se fait grâce au lemme classique suivant.

Proposition. (Lemme chinois) *Soit $m, n \in \mathbf{Z}$, supposons m et n premiers entre eux, alors les groupes $\mathbf{Z}/mn\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ sont naturellement isomorphes. De plus cet isomorphisme est*

aussi un isomorphisme d'anneaux et, par conséquent induit un isomorphisme entre $(\mathbf{Z}/mn\mathbf{Z})^*$ *et* $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$.

Preuve. Considérons l'application $f : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ donnée par $x \mapsto (x \bmod m, x \bmod n)$. C'est un homomorphisme de groupe de noyau $\mathrm{PPCM}(m,n)\mathbf{Z}$, d'où une injection

$$\hat{f} : \mathbf{Z}/\,\mathrm{PPCM}(m,n)\mathbf{Z} \hookrightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

Comme m et n sont supposés premiers entre eux, on a $\mathrm{PPCM}(m,n) = mn$ et, pour des raisons de cardinalité, l'homomorphisme $\hat{f}$ doit être un isomorphisme. De manière générale, si A et B sont des anneaux, on a $(A \times B)^* = A^* \times B^*$ d'où la deuxième assertion. □

La description des sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ est assez simple.

Proposition. *Pour chaque entier* $d \geq 1$ *divisant* n*, il existe un unique sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *d'ordre* d*, c'est le sous-groupe cyclique engendré par la classe de* n/d *dans* $\mathbf{Z}/n\mathbf{Z}$.

Preuve. Supposons $n = dd'$ alors l'élément $x = \bar{d}' \in \mathbf{Z}/n\mathbf{Z}$ est d'ordre d car clairement $dx = 0$ et, si $cx = 0$ alors n divise cd' donc d divise c. Soit maintenant H un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d. Notons $s : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ la surjection canonique. On sait que $s^{-1}(H) = m\mathbf{Z}$ est engendré par m donc H est engendré par $\bar{m} \in \mathbf{Z}/n\mathbf{Z}$. On a $d\bar{m} = 0$ donc n divise dm donc d' divise m donc le sous-groupe H est contenu dans le sous-groupe engendré par $\bar{d}'$ et donc égal à ce sous-groupe. □

Comme application, on peut en tirer la formule (que nous utiliserons plus bas)

$$n = \sum_{d \,|\, n} \phi(d).$$

En effet on écrit $\mathbf{Z}/n\mathbf{Z}$ comme union (disjointe) des ensembles d'éléments d'ordre d pour d divisant n. Le nombre de ces éléments est le nombre de générateurs de l'unique sous-groupe de cardinal d, et comme ce dernier est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, le nombre de générateurs est $\phi(d)$.

Les groupes $(\mathbf{Z}/n\mathbf{Z})^*$ **(rappels).**

On notera (à titre d'exception dans ce chapitre) multiplicativement la loi du groupe $(\mathbf{Z}/n\mathbf{Z})^*$. D'après ce que nous avons vu, si $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ alors

$$(\mathbf{Z}/n\mathbf{Z})^* \cong (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^* \times \dots \times (\mathbf{Z}/p_s^{\alpha_s}\mathbf{Z})^*$$

et en particulier

$$\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_s^{\alpha_s}) = \prod_{i=1}^{s} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Il reste à décrire la structure des groupes $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

Proposition. *Soit* p *premier et* $\alpha \geq 1$ *alors*
(i) Si p *est impair* $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ *est cyclique.*
(ii) Si $p = 2$ *et* $\alpha \geq 3$ *alors* $(\mathbf{Z}/2^{\alpha-2}\mathbf{Z})^* \cong \mathbf{Z}/2^\alpha\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ *n'est pas cylique. Par contre* $(\mathbf{Z}/2\mathbf{Z})^* = \{1\}$ *et* $(\mathbf{Z}/4\mathbf{Z})^* \cong \mathbf{Z}/2\mathbf{Z}$ *sont cycliques.*

Preuve. Commençons par montrer que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique, en fait plus généralement on a le résultat suivant.

Lemme. *Soit k un corps commutatif et G un sous-groupe fini de k^*, alors G est cyclique. En particulier $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.*

Preuve du lemme. Notons $n := \mathrm{card}(G)$ et $\psi(d)$ le nombre d'éléments d'ordre d dans G. On a clairement $n = \sum_{d\,|\,n} \psi(d)$. Soit d divisant n, ou bien il n'y a pas d'élément d'ordre d dans G auquel cas $\psi(d) = 0$, ou bien il en existe un qui engendre alors un sous-groupe cyclique H d'ordre d. Tous les éléments de H sont solutions de l'équation $X^d = 1$, mais, comme k est un corps commutatif, une telle équation possède au plus d racines dans k; tous les éléments d'ordre d sont donc dans H et il en a $\phi(d)$ puisque $H \cong \mathbf{Z}/d\mathbf{Z}$. Ainsi $\psi(d)$ vaut zéro ou $\phi(d)$, mais comme $n = \sum_{d\,|\,n} \psi(d) = \sum_{d\,|\,n} \phi(d)$, on voit que $\psi(d) = \phi(d)$ pour tout d divisant n. En particulier $\psi(n) = \phi(n) \geq 1$, ce qui implique bien que G est cyclique. □

Lemme. *Soit p premier impair, la classe de $p+1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est d'ordre $p^{\alpha-1}$.*

Preuve du lemme. Montrons d'abord par récurrence la congruence

$$(p+1)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}.$$

Pour $k = 0$, la congruence est triviale. Supposons donc $(p+1)^{p^{k-1}} = 1 + p^k + ap^{k+1}$ alors $(p+1)^{p^k} = \left(1 + p^k + ap^{k+1}\right)^p \equiv 1 + p(p^k + ap^{k+1}) \equiv 1 + p^{k+1} \bmod p^{k+2}$. Pour l'avant-dernière congruence, on a besoin de $p \neq 2$; en effet la formule du binôme de Newton fait apparaître des termes multiples de p^{kr} donc nuls modulo p^{k+2} sauf peut-être si $r = 2$ et $k = 1$ mais le terme s'écrit alors $C_p^2 p^2$ qui est bien nul modulo p^3 si p est impair. En particulier, on voit que $(p+1)^{p^{\alpha-1}} \equiv 1 \bmod p^\alpha$ mais $(p+1)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \not\equiv 1 \bmod p^\alpha$, ce qui implique bien que $p+1$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

On peut maintenant terminer la preuve de la proposition pour p impair. Soit $x \in \mathbf{Z}$ tel que x modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^*$ i.e. est d'ordre $p-1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$; alors $\bar{x}$ est d'ordre $m(p-1)$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ et donc $y = \bar{x}^m$ est d'ordre exactement $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. L'élément $y(p+1)$ est donc d'ordre $p^{\alpha-1}(p-1)$ donc est un générateur de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ (car $p^{\alpha-1}$ et $p-1$ sont premiers entre eux).

Lemme. *La classe de 5 dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est d'ordre $2^{\alpha-2}$. De plus la classe de -1 n'appartient pas au sous-groupe engendré par la classe de 5.*

Preuve du lemme. On montre d'abord par récurrence que

$$5^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}.$$

La congruence est triviale pour $k = 0$, supposons donc que $5^{2^{k-1}} = 1 + 2^{k+1} + a2^{k+2}$ alors $5^{2^k} = (1 + 2^{k+1} + a2^{k+2})^2 = 1 + 2(2^{k+1} + a2^{k+2}) + 2^{2(k+1)}(1+2a)^2 \equiv 1 + 2^{k+2} \bmod 2^{k+3}$. En particulier $5^{2^{\alpha-2}} \equiv 1 \bmod 2^\alpha$ mais $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \not\equiv 1 \bmod 2^\alpha$ donc 5 est bien d'ordre $2^{\alpha-2}$. Supposons que $5^\beta \equiv -1 \bmod 2^\alpha$ alors $5^{2\beta} \equiv 1 \bmod 2^\alpha$ donc $2^{\alpha-2}$ divise 2β donc $2^{\alpha-3}$ divise β ou encore $\beta = \gamma 2^{\alpha-3}$. Comme 5 est d'ordre $2^{\alpha-2}$, on peut considérer β comme un entier modulo $2^{\alpha-2}$ et donc γ modulo 2. L'entier γ doit être impair donc on peut le supposer égal à 1, c'est-à-dire $5^{2^{\alpha-3}} \equiv 1 \bmod 2^\alpha$, mais $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \bmod 2^\alpha$ donc $-1 \equiv 1 + 2^{\alpha-1} \bmod 2^\alpha$ ou encore $2 + 2^{\alpha-1} \equiv \bmod 2^\alpha$ soit $1 + 2^{\alpha-2} \equiv \bmod 2^{\alpha-1}$, ce qui n'est pas possible. □

Pour la démonstration de la deuxième partie de la proposition, on peut supposer $\alpha \geq 3$ (en effet le calcul de $(\mathbf{Z}/2\mathbf{Z})^*$ et $(\mathbf{Z}/4\mathbf{Z})^*$ est immédiat). La classe de 5 engendre donc un sous-groupe isomorphe à $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ et -1 engendre un sous-groupe d'ordre 2 non contenu dans le précédent donc $(\mathbf{Z}/2^\alpha\mathbf{Z})^* = \langle 5\rangle \oplus \langle -1\rangle \cong \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. □

Exercice. Montrer que si la classe de $x \in \mathbf{Z}$ engendre $(\mathbf{Z}/p^2\mathbf{Z})^*$ alors elle engendre aussi $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ (pour p impair).

Remarque. Le sous-groupe quaternionique $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ est un sous-groupe fini du groupe multiplicatif du corps $\mathbf{H}$ mais n'est pas cyclique (cela ne contredit pas le lemme vu car $\mathbf{H}$ n'est pas commutatif).

Théorèmes de structure.

Les produits finis de groupes cycliques sont évidemment abéliens de type fini. Nous allons voir réciproquement que tout groupe abélien de type fini est en fait isomorphe à un groupe de la forme $\mathbf{Z}^r \times \mathbf{Z}/m_1\mathbf{Z} \times \ldots \times \mathbf{Z}/m_s\mathbf{Z}$. Toutefois le lemme chinois indique qu'une telle décomposition n'est pas *a priori* unique. On peut néanmoins en extraire des éléments invariants ou canoniques.

Théorème. *Tout groupe abélien G de type fini est produit de groupes cycliques. Plus précisément il existe $r \geq 0$ et $a_1, \ldots a_s$ avec $a_i \geq 2$ et a_i divise a_{i+1} tels que*

$$G \cong \mathbf{Z}^r \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z}.$$

De plus les entiers $r, s, a_1, a_2, \ldots a_s$ sont uniques.

Nous allons utiliser dans la preuve un autre théorème de structure, décrivant les sous-groupes de $\mathbf{Z}^r$, qui est démontré au chapitre sur les modules sur les anneaux principaux.

Théorème. *Soit H un sous-groupe de $\mathbf{Z}^r$ alors*
(i) Le groupe H est libre de rang $s \leq r$.
(ii) Il existe $e_1, \ldots, e_r$ base de $\mathbf{Z}^r$ et $a_1, \ldots a_s \geq 1$ tels que a_i divise a_{i+1} et $a_1e_1, \ldots a_se_s$ forment une base de H.

Preuve (du théorème antérieur). Supposons que G possède n générateurs, alors on en déduit un homomorphisme surjectif $f : \mathbf{Z}^n \to G$ et un isomorphisme $\mathbf{Z}^n/\operatorname{Ker}(f) \cong G$. On applique le théorème précédent à $\operatorname{Ker}(f)$ et on obtient des e_i et a_i tels que $\mathbf{Z}^n = \mathbf{Z}e_1 \oplus \ldots \mathbf{Z}e_n$ et tels que $\operatorname{Ker}(f) = \mathbf{Z}a_1e_1 \oplus \ldots \mathbf{Z}a_me_m$. D'où l'on tire aisément

$$G \cong \mathbf{Z}^n/\operatorname{Ker}(f) \cong \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_m\mathbf{Z} \times (\mathbf{Z})^{n-m}$$

avec a_i divisant a_{i+1} et $a_i \geq 1$. En éliminant les facteurs correspondant à $a_i = 1$, on obtient l'existence de la décomposition annoncée. Montrons maintenant l'unicité. Nous allons utiliser le

Lemme. *Soit $M \geq 1$ alors le sous-groupe $M\mathbf{Z}/n\mathbf{Z}$ est cyclique de cardinal $n/\operatorname{PGCD}(n, M)$; le quotient $(\mathbf{Z}/n\mathbf{Z})/M(\mathbf{Z}/n\mathbf{Z})$ est cyclique de cardinal $\operatorname{PGCD}(n, M)$.* □

Preuve. Notons $d = PGCD(n, M)$ et $n = n'd$, $M = M'd$. Considérons la composée $\mathbf{Z} \xrightarrow{\times M} \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Son noyau est le sous-groupe des $x \in \mathbf{Z}$ tels que n divise Mx ou encore tels que n' divise x d'où un isomorphisme entre $\mathbf{Z}/n'\mathbf{Z}$ et l'image, c'est-à-dire $M\mathbf{Z}/n\mathbf{Z}$. Enfin $(\mathbf{Z}/n\mathbf{Z})/M(\mathbf{Z}/n\mathbf{Z})$ est cyclique de cardinal d donc isomorphe à $\mathbf{Z}/d\mathbf{Z}$. □

Supposons maintenant

$$G \cong \mathbf{Z}^r \times \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z} \cong \mathbf{Z}^{r'} \times \mathbf{Z}/b_1\mathbf{Z} \times \ldots \times \mathbf{Z}/b_t\mathbf{Z}$$

avec $a_i, b_i \geq 2$ et a_i divise a_{i+1}, resp. b_i divise b_{i+1}. On commence par choisir un entier M multiple de a_s et b_t alors $MG \cong \mathbf{Z}^r \cong \mathbf{Z}^{r'}$ donc $r = r'$. En remplaçant G par G_{torsion} on peut maintenant supposer G fini (i.e. $r = r' = 0$). Choisissons p divisant a_1 (noter que $a_1 \geq 2$) alors $PGCD(p, a_i) = p$ et $PGCD(p, b_i) = p$ ou 1 suivant que p divise b_i ou non. Donc d'après le lemme $G/pG \cong (\mathbf{Z}/p\mathbf{Z})^s \cong (\mathbf{Z}/p\mathbf{Z})^{t-\text{card}\{i \mid p \text{ ne divise pas } b_i\}}$. Ainsi $s \leq t$ et, par symétrie $t = s$ et donc p divise b_1. Ecrivons donc $a_i = pa'_i$ et $b_i = pb'_i$, alors $pG \cong \mathbf{Z}/a'_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a'_s\mathbf{Z} \cong \mathbf{Z}/b'_1\mathbf{Z} \times \ldots \times \mathbf{Z}/b'_s\mathbf{Z}$. par récurrence sur $\text{card}(G)$ on en tire que $a'_i = b'_i$ et donc $a_i = b_i$. □

Revenons aux groupes abéliens finis et montrons qu'on peut écrire une autre décomposition canonique.

Théorème. *Un groupe abélien fini G est somme directe de ses p-sous-groupes de Sylow. Un p-groupe abélien est isomorphe à un produit $(\mathbf{Z}/p\mathbf{Z})^{m_1} \times (\mathbf{Z}/p^2\mathbf{Z})^{m_2} \times \ldots \times (\mathbf{Z}/p^r\mathbf{Z})^{m_r}$ avec $m_i \geq 0$. De plus les m_i sont uniques.*

Le groupe G est abélien donc possède un unique p-sous-groupe de Sylow. On voit aisément que celui-ci est égal à $G_p := \{x \in G \mid \exists m \geq 0,\ p^m x = 0\}$. La première partie du théorème est alors une conséquence du lemme ci-dessous; la deuxième partie découle directement du théorème de structure précédent.

Lemme. *Soit G un groupe de cardinal MN avec M et N premiers entre eux. Soit $G_1 = \{x \in G \mid Mx = 0\}$ et $G_2 = \{x \in G \mid Nx = 0\}$, alors $G = G_1 \oplus G_2$.*

Preuve. D'après le théorème de Bézout, il existe $a, b \in \mathbf{Z}$ tels que $aM + bN = 1$. Si $x \in G_1 \cap G_2$ alors $x = (aM + bN)x = 0$. Si maintenant $x \in G$ alors $x = bNx + aMx$ et, comme MN est un exposant pour G, on a $bNx \in G_1$ et $aMx \in G_2$. □

Exercice. Soit une décomposition $G \cong \mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z}$ avec $a_i \geq 2$ et a_i divise a_{i+1}. Montrer que l'exposant de G est égal à a_s et que le nombre minimal de générateurs de G est s.

B. MODULES.

*On donne une brève présentation de la théorie des modules sur un anneau commutatif avec comme objectifs et motivations d'une part, la théorie des groupes abéliens (**Z**-modules) la description de la décomposition d'un endomorphisme d'espace vectoriel et la détermination de sa classe de similitude ($K[X]$-modules).*

B.1. Modules : généralités et exemples.

Soit A un anneau commutatif, un *A-module* est un ensemble M muni d'une addition $M \times M \to M$ et d'une multiplication par les scalaires $A \times M \to M$ vérifiant les mêmes axiomes qu'un espace vectoriel, c'est-à-dire :

(i) $(M, +)$ est un groupe abélien
(ii) $\forall a, b \in A, \forall x \in M$ on a $a \cdot (b \cdot x) = (ab) \cdot x$
(ii) $\forall a \in A, \forall x, y \in M$ on a $a \cdot (x + y) = a \cdot x + a \cdot y$
(iv) $\forall a, b \in A, \forall x \in M$ on a $(a + b) \cdot x = a \cdot x + b \cdot x$
(v) $\forall x \in M$ on a $1 \cdot x = x$

Remarque. Si A n'est pas commutatif on peut néanmoins définir des modules à droite ou à gauche.

Exemples. Si A est un corps, un A-module n'est rien d'autre qu'un A-espace vectoriel. Un groupe abélien est, de manière "évidente", un **Z**-module si l'on pose $n \cdot x = x + \cdots + x$ (n fois) pour $n > 0$ et $n \cdot x = -x - \cdots - x$ ($|n|$ fois) pour $n < 0$. Si A est un anneau commutatif et si I est un idéal, alors A/I est naturellement un A-module en posant $a \cdot (x + I) = ax + I$. En particulier A peut être vu comme un A-module.

Opérations sur les modules.

Un *sous-module* N d'un module M est un sous-ensemble tel que les opérations sur M induisent une structure de A-module sur N. C'est-à-dire :

(i) N est un sous-groupe de M
(ii) N est stable par multiplication par un scalaire
ou encore
(i') $\forall x, y \in N, \forall a, b \in A, ax + by \in N$.

Exemples. Les sous-modules de A sont les idéaux de A. Si $a \in A$, l'ensemble $aM := \{ax \mid x \in M\}$ est un sous-module de M; plus généralement, si I est un idéal de l'anneau A, l'ensemble $I \cdot M := \{x = a_1 x_1 + \ldots a_r x_r \mid r \geq 0,\ a_i \in I \text{ et } x_i \in M\}$ est un sous-module.

Si N_1 et N_2 sont des sous-modules de M, l'intersection $N_1 \cap N_2$ est un sous-module, la *somme* est le sous-module $N_1 + N_2 = \{x_1 + x_2 \,|\, x_1 \in N_1 \text{ et } x_2 \in N_2\}$. Si de plus $N_1 \cap N_2 = \{0\}$ on dit que la somme est *directe* et on la note $N_1 \oplus N_2$. La notion de somme (directe ou non) se généralise à une famille quelconque de sous-modules $\{N_i\}_{i \in I}$.

Une application $f : M \to N$ est un *homomorphisme de modules*, si elle vérifie $f(x + y) = f(x) + f(y)$ et $f(a \cdot x) = a \cdot f(x)$. Si de plus f est bijective, on dit que c'est un *isomorphisme de modules*.

Remarques. La dernière appellation est justifiée car on vérifie immédiatement que la bijection réciproque f^{-1} est encore un homomorphisme de modules. Le composé de deux homomorphismes est encore un homomorphisme. L'image directe ou réciproque par un homomorphisme d'un sous-module est encore un sous-module. En particulier le noyau $\mathrm{Ker}(f)$ est un sous-module de M et l'image $\mathrm{Im}(f)$ est un sous-module de N. L'ensemble des endomorphismes $f : M \to M$ forme un anneau (non commutatif en général) en posant $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(g(x))$. Si $M = A^r$, alors $\mathrm{End}(M)$ est isomorphe à l'anneau des matrices $r \times r$ à coefficients dans A.

Si N_1 et N_2 sont des sous-modules de M, le *produit de modules* est définit comme l'ensemble $N_1 \times N_2$ muni des lois $(x_1, x_2) + (x_1', x_2') = (x_1 + x_1', x_2 + x_2')$ et $a \cdot (x_1, x_2) = (a \cdot x_1, a \cdot x_2)$.

Remarque. La notion de produit se généralise à une famille quelconque de modules $\{N_i\}_{i \in I}$. Lorsque les N_i sont des sous-modules en somme directe, on a $\prod_{i \in I} N_i \cong \oplus_{i \in I} N_i$ seulement lorsque I est fini.

Soit N un sous-module de M, on peut construire le *module quotient* M/N comme le groupe abélien M/N (déjà construit) muni de la multiplication par un scalaire $a \cdot (x + N) = (a \cdot x) + N$. On a alors la propriété universelle du quotient

Théorème *Soit $f : M \to M'$ un homomorphisme de A-modules et soit N un sous-module et $s : M \to M/N$ la surjection canonique.*
(i) Il existe une application $\hat{f} : M/N \to M'$ telle que $f = \hat{f} \circ s$ si et seulement si $N \subset \mathrm{Ker}(f)$.
(ii) Dans ce cas l'application $\hat{f}$ est un homomorphisme de modules, son image est égale à celle de f (i. e. $\hat{f}(M/N) = f(M)$) et son noyau est $\mathrm{Ker}(f)/N$.

Preuve. En terme de groupe quotient "tout" a déjà été prouvé; il reste seulement à vérifier que l'application $\hat{f}$, quand elle existe, est bien un homomorphisme de modules, ce qui est immédiat. □

Par exemple on en déduit que $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. Si N_1 et N_2 sont deux sous modules de M, l'application $x \mapsto (x, -x)$ identifie $N_1 \cap N_2$ à un sous-module de $N_1 \times N_2$ et l'on voit que $N_1 + N_2 \cong (N_1 \times N_2)/(N_1 \cap N_2)$.

Les notions de *combinaison linéaire*, *partie libre*, de *partie génératrice* ou de *base* se définissent comme en algèbre linéaire sur un corps. Néanmoins une différence notable est la non-existence de base d'un module en général. En fait on peut introduire la notion suivante (qui n'a d'intérêt que si M n'est pas un espace vectoriel ou encore si A n'est pas un corps).

Définition. Soit x élément d'un A-module M, on appelle *annulateur* de x l'idéal

$$\mathrm{Ann}(x) = \{a \in A \,|\, a \cdot x = 0\}.$$

Si N est un sous-module, son annulateur est

$$\mathrm{Ann}(N) = \bigcap_{x \in N} \mathrm{Ann}(x) = \{a \in A \,|\, \forall x \in N, a \cdot x = 0\}.$$

Remarquons qu'un A-module M est automatiquement un $A/\mathrm{Ann}(M)$-module en posant $\bar{a} \cdot x = ax$ (ce qui est loisible puisque ax ne dépend que de la classe $\bar{a}$ de a modulo l'idéal $\mathrm{Ann}(M)$).

Exemple. Soit $M = A/I$ vu comme A-module (avec I idéal de A), on a clairement $\mathrm{Ann}(M) = I$. Considérons $M = \mathbf{Q}/\mathbf{Z}$ vu comme $\mathbf{Z}$-module, pour tout élément x égal à la classe de a/b avec a et b premiers entre eux on a $\mathrm{Ann}(x) = b\mathbf{Z}$, néanmoins $\mathrm{Ann}(M) = \{0\}$. Remarquons que l'ensemble

$$M_{\text{torsion}} := \{x \in M \mid \exists a \in A \setminus \{0\},\ a \cdot x = 0\} = \{x \in M \mid \mathrm{Ann}(x) \neq 0\}$$

est un sous-module de M.

Supposons A intègre, lorsque l'annulateur d'un élémént non nul de M n'est pas réduit à $\{0\}$ on voit tout de suite qu'il ne peut pas exister de base sur A. On donne donc un statut spécial aux modules possédant une base. On définit de même l'analogue de la dimension finie dans les espaces vectoriels.

Définition. Un A-module M est *libre* s'il possède une base (i. e. une partie libre et génératrice sur A). Il est de *type fini* s'il possède une partie génératrice finie.

Ainsi un module libre de type fini est isomorphe à A^n. Il n'est pas évident que l'entier n soit unique, même si cela est vrai ; au paragraphe suivant on vérifie que si A est principal et $A^n \cong A^m$ alors $m = n$. Remarquons aussi que A, considéré comme A-module, est libre de rang 1 et que ses sous-modules non nuls (c'est-à-dire ses idéaux non nuls) sont libres de rang 1 si et seulement si A est principal.

B.2. Modules de type fini sur les anneaux principaux.

Rappelons qu'un anneau commutatif unitaire A est *principal* s'il est intègre et tout idéal est de la forme aA. Nous commençons par montrer qu'on a bien une notion de "dimension", qu'on appellera plutôt *rang*, et on donne ensuite la description des sous-modules d'un module libre de type fini sur un tel anneau.

Proposition. *Soit A un anneau principal, M un A-module admettant deux bases $\mathcal{B}$ et $\mathcal{B}'$ alors* $\mathrm{card}(\mathcal{B}) = \mathrm{card}(\mathcal{B}')$. *Si $M = N \oplus N'$ et si $\mathcal{B}$ et $\mathcal{B}'$ sont des bases de N et N' respectivement, alors $\mathcal{B} \cup \mathcal{B}'$ est une base de M.*

Preuve. Si A est un corps, le résultat est la base de l'algèbre linéaire. Sinon, soit a un élément irréductible de A, alors $k = A/aA$ est un corps et le module quotient M/aM est annulé par aA donc peut être vu comme un k-module c'est-à-dire un k-espace vectoriel. Mais si $e_1, \ldots, e_r$ forment une base de M sur A et si l'on désigne par $\bar{e}_i$ la classe de e_i modulo aM, il est immédiat que $\bar{e}_1, \ldots, \bar{e}_r$ forment une base de M/aM sur k. L'entier r est donc la dimension du k-espace vectoriel M/aM et ne dépend donc pas de la base choisie. La deuxième affirmation est immédiate. □

Définition. Si M est un A-module libre de type fini, on appelle *rang* de M le cardinal d'une base.

Théorème *Soit A un anneau principal, M un A-module libre de rang r, et N un sous-module alors*

(i) Le module N est libre de rang $s \leq r$.

(ii) Il existe $e_1, \ldots, e_r$ base de M sur A et $a_1, \ldots, a_s \in A$ tels que a_i divise a_{i+1} et

$$N = Aa_1e_1 \oplus \ldots \oplus Aa_se_s.$$

Preuve. La preuve se fait par récurrence sur l'entier r, le cas $r = 1$ étant vérifié précisément parce que l'anneau A est supposé principal. Commençons par la preuve de (i). Si l'on note $e_1, \ldots, e_r$ une base de M on peut écrire $M = Ae_1 \oplus \ldots \oplus Ae_r$ et considérer l'homomorphisme de A-modules $e_r^* : M \to A$ défini par $e_r^*(a_1e_1 + \ldots + a_re_r) = a_r$. L'ensemble $e_r^*(N)$ est un sous-module, c'est-à-dire un idéal de A. Choisissons $x_0 \in N$ tel que $e_r^*(x_0) = a$ avec $e_r^*(N) = aA$. On va appliquer le lemme suivant

Lemme. *Soit $f : M \to A$ un homomorphisme non nul de modules et x tel que $f(x)A = f(M)$ alors $M = \mathrm{Ker}(f) \oplus Ax$.*

Preuve du lemme. Soit $y \in \mathrm{Ker}(f) \cap Ax$ alors $y = ax$ et $f(y) = af(x) = 0$, mais $f(x) \neq 0$ car sinon l'homomorphisme f serait nul, donc $a = 0$ (l'anneau A est intègre) et $y = 0$. Soit maintenant $y \in M$, on sait qu'il existe $b \in A$ tel que $f(y) = bf(x) = f(bx)$, donc $f(y - bx) = 0$ et $y - bx \in \mathrm{Ker}(f)$. On peut donc écrire $y = (y - bx) + (bx) \in \mathrm{Ker}(f) + Ax$. □

Si $N \subset \mathrm{Ker}(e_r^*)$ alors, comme $\mathrm{Ker}(e_r^*) = Ae_1 \oplus \ldots \oplus Ae_{r-1}$, on peut appliquer l'hypothèse de récurrence et conclure que N est libre de rang $\leq r - 1$. Sinon, en appliquant le lemme à $e_r^* : N \to A$ on obtient que $N = (\mathrm{Ker}(e_r^*) \cap N) \oplus Ax_0$. En appliquant l'hypothèse de récurrence au sous-module $\mathrm{Ker}(e_r^*) \cap N \subset \mathrm{Ker}(e_r^*)$, on obtient que $\mathrm{Ker}(e_r^*) \cap N$ est libre de rang $\leq r - 1$. Donc N est libre de rang $\leq r$.

Montrons maintenant (ii), toujours par récurrence sur r. Pour chaque homomorphisme de modules $f : M \to A$ tel que $f(N) \neq 0$, on choisit $a_f \in A$ tel que $f(N) = a_fA$ et $u_f \in N$ tel que $f(u_f) = a_f$. On choisit ensuite f_1 tel que $a_{f_1}A$ soit maximal parmi les a_fA. Remarque : cela signifie que si $a_{f_1}A \subset a_fA$ alors $a_{f_1}A = a_fA$ mais on ne peut pas, à ce stade de la preuve, affirmer que a_{f_1} divise tous les a_f. Pour alléger les notations on écrira $a_1 = a_{f_1}$; on choisit aussi $u_1 \in N$ tel que $f_1(u_1) = a_1$. Montrons d'abord que pour tout f on a a_1 divise $f(u_1)$. Appelons $d = \mathrm{PGCD}(a_1, f(u_1))$, alors, d'après le théorème de Bézout, il existe $b, c \in A$ tels que $d = ba_1 + cf(u_1)$. Considérons alors l'homomorphisme $f' = bf_1 + cf$, on a $f'(u_1) = d$ donc $a_{f'}$ divise d qui divise a_1 ou encore $a_1A \subset a_{f'}A$ d'où $a_1A = dA = a_{f'}A$. Mais $a_1 = \mathrm{PGCD}(a_1, f(u_1))$ signifie exactement que a_1 divise $f(u_1)$. On en tire l'existence de $e_1 \in M$ tel que $u_1 = a_1e_1$ et donc $f(e_1) = 1$; en effet si $y_1, \ldots, y_r$ est une base de M alors $y_i^*(u_1) = a_1b_i$ et donc $u_1 = \sum_i y_i^*(u_1)y_i = a_1(\sum_i b_iy_i)$. On applique alors le lemme précédent à $f_1 : M \to A$ avec l'élément e_1 puis à $f_1 : N \to A$ avec l'élément u_1, ce qui donne

$$M = Ae_1 \oplus \mathrm{Ker}(f_1) \qquad \text{et} \qquad N = Aa_1e_1 \oplus (N \cap \mathrm{Ker}(f_1)).$$

Comme, d'après (i), $\mathrm{Ker}(f_1)$ est libre de rang $r - 1$, on peut lui appliquer l'hypothèse de récurrence et conclure qu'il existe une base $e_2, \ldots, e_r$ de $\mathrm{Ker}(f_1)$ et des éléments $a_r, \ldots, a_r \in A$ tels que a_i divise a_{i+1} et

$$N \cap \mathrm{Ker}(f_1) = Aa_2e_2 \oplus \ldots \oplus Aa_re_r.$$

Il reste donc seulement à vérifier que a_1 divise a_2. Pour cela considérons $f = e_1^* + e_2^*$; on a $f(a_2e_2) = a_2$ donc a_f divise a_2 et par ailleurs $f(u_1) = f(a_1e_1) = a_1$ donc a_f divise a_1 mais on a vu que cela entraînait $a_1A = a_fA$ donc on a bien a_1 qui divise a_2. □

Théorème *Soit A un anneau principal, M un A-module de type fini, il existe $r, m \in \mathbf{N}$ et $a_1, \ldots, a_m \in A$ éléments non nuls et non inversibles tels que a_i divise a_{i+1} et*

$$M \cong A^r \times A/a_1A \times \ldots \times A/a_mA,$$

De plus, les entiers r, s et la suite d'idéaux $a_m A \subset \ldots \subset a_1 A$ sont uniques.

Preuve. Soient $x_1, \ldots, x_n$ des générateurs de M (comme A-module), on a donc un homomorphisme surjectif $\Phi : A^n \to M$ défini par $\Phi(b_1, \ldots, b_n) = b_1 x_1 + \ldots + b_n x_n$. Soit $N = \mathrm{Ker}(\Phi)$, on a $M \cong A^n/N$ et, d'après le théorème précédent il existe une base $e_1, \ldots, e_n$ de M sur A et $a_1, \ldots, a_n \in A$ que a_i divise a_{i+1} et $N = Aa_1e_1 \oplus \ldots \oplus Aa_ne_n$. On montre aisément que

$$M \cong A^n/N = (Ae_1 \oplus \ldots \oplus Ae_n) \,/\, (Aa_1e_1 \oplus \ldots \oplus Aa_ne_n) \cong A/a_1A \times \ldots \times A/a_nA.$$

On peut omettre dans cette décomposition les facteurs avec a_i inversible et si $a_i = 0$ on peut écrire $A/a_iA \cong A$ d'où le résultat annoncé. L'unicité se démontre aisément à partir de l'observation que, d'une part $M/bM \cong (A/bA)^r \times A/\operatorname{PGCD}(a_1, b)A \times \ldots \times A/\operatorname{PGCD}(a_n, b)A$ et d'autre part $bM \cong A^r \times A/(a_1/\operatorname{PGCD}(a_1, b))A \times \ldots \times A/(a_n/\operatorname{PGCD}(a_n, b))A$. □

Pour accentuer le parallèle avec les groupes abéliens, définissons un *A-module cyclique* comme un A-module isomorphe à A/aA. Le théorème précédent affirme qu'un module de torsion et de type fini est isomorphe à un produit ou somme fini de modules cycliques. Ceci est bien une généralisation du théorème décrivant les groupes finis abéliens comme produit de groupes cycliques.

Terminons ce paragraphe en donnant une version utile du théorème de structure des sous-modules de A^n.

Lemme. *Soit $M \in \mathrm{Mat}(n \times m, A)$ avec A principal, il existe $U \in \mathrm{GL}_n(A)$ et $V \in \mathrm{GL}_m(A)$ et $a_1, \ldots, a_s \in A \setminus \{0\}$ avec $s = \mathrm{rang}(M) \leq \min(m, n)$ et a_i divisant a_{i+1} tels que*

$$M = U \begin{pmatrix} a_1 & & & 0 \\ 0 & a_2 & & \\ & & \ldots & 0 \\ & & a_s & 0 \\ & & & 0 \end{pmatrix} V.$$

Variante. *Soit un homomorphisme $f : A^n \to A^m$, il existe $e_1, \ldots, e_n$ base de A^n et $f_1, \ldots, f_m$ base de A^m et $a_1, \ldots, a_s \in A \setminus \{0\}$ avec $s = \mathrm{rang}(f) \leq \min(m, n)$ et a_i divisant a_{i+1} tels que*

$$f(e_i) = \begin{cases} a_i f_i & \text{si } 1 \leq i \leq s \\ 0 & \text{sinon} \end{cases}$$

Preuve. Prouvons par exemple la variante. Il existe a_i et f_i tels que le sous-module $f(A^n) \subset A^m$ soit égal à $a_1Af_1 \oplus \ldots \oplus a_sAf_s$. Choisissons $e_i \in A^n$ tel que $f(e_i) = a_if_i$ (pour $1 \leq i \leq s$); on a alors $A^n = Ae_1 \oplus \ldots \oplus Ae_s \oplus \mathrm{Ker}(f)$. En choisissant $e_{s+1}, \ldots, e_n$ une base de $\mathrm{Ker}(f)$ on obtient l'énoncé.

B.3. Polynômes invariants associés à un endomorphisme

Définition. Soit E un K-espace vectoriel de dimension finie n et $u \in \mathrm{End}_K(E)$. On définit une structure de $K[X]$-module sur l'ensemble E de la façon suivante : l'addition est l'addition dans l'espace vectoriel et la multiplication par un polynôme $P = a_0 + a_1X + \ldots + a_dX^d$ est définie par

$$P \cdot x = P(u)(x) = (a_0I + a_1u + \ldots + a_du^d)(x) = a_0x + a_1u(x) + \ldots + a_du^d(x).$$

On notera E_u le $K[X]$-module ainsi obtenu. On remarque tout de suite qu'il s'agit d'un module de type fini. De plus, $\mathrm{Ann}(E_u)$ est non trivial puisqu'il contient le polynôme caractéristique (théorème de Cayley-Hamilton) donc le module E_u est de torsion (on peut aussi utiliser le fait que, pour $x \in E$, les vecteurs $x, u(x), u^2(x), \ldots, u^n(x)$ sont liés).

Proposition. *Soit $u, v \in \mathrm{End}_k(E)$, alors les $K[X]$-modules E_u et E_v sont isomorphes si et seulement si les endomorphismes u et v sont semblables, c'est-à-dire qu'il existe une application K-linéaire inversible h telle que $v = h \circ u \circ h^{-1}$.*

Preuve. Pour distinguer les structures de $K[X]$-modules E_u et E_v dans cette preuve nous noterons $P \cdot_u x = P(u)(x)$ et $P \cdot_v x = P(v)(x)$. Supposons qu'il existe h linéaire inversible telle que $v = h \circ u \circ h^{-1}$, alors $v^m = h \circ u^m \circ h^{-1}$ et plus généralement $P(v) = h \circ P(u) \circ h^{-1}$ donc

$$h(P \cdot_u x) = h(P(u)(x)) = (h \circ P(u))(x) = (P(v) \circ h)(x) = P \cdot_v h(x).$$

Ainsi h est en fait un isomorphisme de $K[X]$-modules $h : E_u \to E_v$. Supposons inversement qu'il existe un tel isomorphisme de $K[X]$-modules $h : E_u \to E_v$. L'application h est en particulier K-linéaire et bijective et de plus

$$h(u(x)) = h(X \cdot_u x) = X \cdot_v h(x) = v(h(x))$$

donc on a $h \circ u = v \circ h$ et u et v sont semblables. □

Par ailleurs, avant d'appliquer à notre situation les théorèmes de structure du paragraphe précédent, observons qu'un $K[X]$-sous-module de E_u n'est rien d'autre qu'un sous-espace vectoriel stable par u. Ainsi une décomposition en somme de sous-modules correspond à une décomposition en somme de sous-espaces vectoriels stables par u. De même un sous-module cyclique correspond à un sous-espace vectoriel engendré par un vecteur x et ses images successives $u(x), u^2(x), \ldots$ par l'endomorphisme u.

Le module E_u est isomorphe à $K[X]/P_1K[X] \times \ldots \times K[X]/P_rK[X]$ avec P_i non constants et P_i divise P_{i+1}, de plus les P_i sont uniques (à un scalaire près), ce qui justifie la

Définition. Les polynômes P_i s'appellent les *facteurs invariants* de u.

Remarquons qu'il est assez facile de voir (démontrez-le!) que P_r est le polynôme minimal de u, tandis que le polynôme caractéristique est égal au produit $P_1 \ldots P_r$. Nous allons généraliser cette observation ci-dessous.

D'après ce qui précède, u et v sont semblables si et seulement si ils ont mêmes facteurs invariants. Donnons maintenant une interprétation de ces invariants et une méthode de calcul (théorique). Le module E_u se décompose en $E_1 \oplus \ldots \oplus E_r$ avec E_i module cyclique de la forme $K[X]/PK[X]$. Ces sous-modules correspondent à des sous-espaces vectoriels stables par u sur lequel u agit comme la multiplication par X sur $K[X]/PK[X]$. Soit $P = X^d + p_{d-1}X^{d-1} + \ldots + p_0$, prenons comme K-base de $K[X]/PK[X]$ les éléments $1, X, \ldots, X^{d-1}$ et soit $e_1, \ldots, e_d$ la K-base correspondante de E_i, la matrice de u dans cette base est une matrice dite *compagnon* :

$$\mathrm{Mat}(u; e_1, \ldots, e_d) = \begin{pmatrix} 0 & & & -p_0 \\ 1 & & & \vdots \\ & \ddots & 0 & -p_{d-2} \\ & & 1 & -p_{d-1} \end{pmatrix}$$

On obtient en particulier que toute matrice est semblable à une matrice dont les blocs diagonaux sont les matrices compagnon associées à ses facteurs invariants.

Soit A la matrice de u dans une base. Définissons $D_i = D_i(A)$ comme le PGCD des mineurs d'ordre i de la matrice $A - XId$. En particulier D_n est le polynôme caractéristique de u ou A.

Théorème *Les matrices A et B sont semblables si et seulement si $D_i(A) = D_i(B)$ pour $1 \leq i \leq n$.*

Preuve. Posons $A = \mathrm{Mat}(u; (e_1, \ldots, e_n)$. La matrice $A - Xid$ définit un endomorphisme $\Phi : K[X]^n \to K[X]^n$; définissons également $\mu : K[X]^n \to E_u$ par

$$\mu(P_1, \ldots, P_n) = P_1 \cdot e_1 + \ldots + P_n \cdot e_n = P_1(u)(e_1) + \ldots + P_n(u)(e_n).$$

L'homomorphisme μ est clairement surjectif et $\Phi(K[X]^n) \subset \mathrm{Ker}\,\mu$; en effet

$$\begin{aligned}\mu(\Phi(0, \ldots, P_i, \ldots, 0) &= \mu(a_{1i}P_i, \ldots, a_{ii}P_i - XP_i, \ldots, a_{ni}P_i) \\ &= a_{1i}P_i(e_1) + \ldots + a_{ni}P_i(e_n) - uP_i(u)(e_i) \\ &= P_i(u)\,(a_{1i}e_1 + \ldots + a_{ni}e_n - u(e_i)) = 0\end{aligned}$$

Par ailleurs on a vu que le théorème de structure des sous-modules de modules libres peut s'interpréter comme l'existence de deux matrices de changement de base U et V (à coefficient dans $K[X]$) et de polynômes $Q_1, \ldots, Q_n$ avec Q_i divise Q_{i+1} et $A - Xid = U\,\mathrm{diag}(Q_1, \ldots, Q_n)V$. On voit, d'une part, que le PGCD des mineurs d'ordre i est $D_i = Q_1 \ldots Q_i$ et d'autre part que $K[X]^n/\Phi(K[X]^n) \cong K[X]/Q_1K[X] \times \ldots \times K[X]/Q_nK[X]$ d'où l'on tire que $K[X]^n/\Phi(K[X]^n)$ est un K-espace vectoriel de dimension $\sum \deg(Q_i) = \deg\det(A - Xid) = n$. Comme l'espace $K[X]^n/\,\mathrm{Ker}(\mu)$ est de même dimension, on en tire $\Phi(K[X]^n) \subset \mathrm{Ker}\,\mu$ et $E_u \cong K[X]^n/\Phi(K[X]^n)$. L'unicité des facteurs invariants de u, disons, $P_1, \ldots, P_r$, implique donc l'égalité $(Q_1, \ldots, Q_n) = (1, \ldots, 1, P_1, \ldots, P_r)$. Ainsi la donnée des facteurs invariants P_i équivaut à celle des D_i, ce qui achève la preuve. □

Commentaire. La théorie des $K[X]$-modules nous donne que deux matrices (ou endomorphismes) sont semblables si elles ont les mêmes polynômes "P_i" et le raisonnement précédent montre que la donnée des "P_i" équivaut à celle des "D_i". En fait explicitement $D_{n-i} = P_1 \ldots P_{r-i}$ et $D_{n-r} = \ldots = D_1 = 1$.

Corollaire. *Les matrices A et ${}^tA$ sont semblables.*

Preuve du corollaire. En effet on a clairement $D_i({}^tA) = D_i(A)$. □

Exercice. Fabriquer deux matrices 4×4 non semblables ayant les mêmes polynômes caractéristiques et minimaux (indication : choisir le polynôme minimal $(X - \lambda)^2$ et le polynôme caractéristique $(X - \lambda)^4$). Peut-on fabriquer de tels exemples en dimension 2 ou 3 ?

Exercice. Démontrer de deux façons (en utilisant les résultats précédents et directement) l'énoncé suivant : deux matrices $A, B \in \mathrm{Mat}(n \times n, \mathbf{R})$ sont semblables sur $\mathbf{C}$ (i. e. il existe $U \in \mathrm{GL}(n, \mathbf{C})$ telle que $B = UAU^{-1}$) si et seulement si elles sont semblables sur $\mathbf{R}$ (i. e. il existe $U \in \mathrm{GL}(n, \mathbf{R})$ telle que $B = UAU^{-1}$).

On termine ce chapitre avec la preuve du théorème de décomposition de Jordan, qui décrit complètement les classes de conjugaison de matrices sur un corps algébriquement clos.

On suppose dans la fin de ce paragraphe que le corps K est algébriquement clos et donc tout polynôme est scindé sur K.

Définition. On appelle *bloc de Jordan* de taille d et valeur propre λ la matrice carrée

$$J(d;\lambda) := \begin{pmatrix} \lambda & 0 & & \dots & & \\ 1 & \lambda & & & & \\ 0 & 1 & \ddots & & & \\ & & \ddots & \ddots & & \\ & & & 1 & \lambda & 0 \\ & & & 0 & 1 & \lambda \end{pmatrix}$$

Si $\lambda = 0$ on note simplement $J(d) = J(d,0)$. Remarquons que certains auteurs appellent bloc de Jordan la transposée de $J(d,\lambda)$; le principal intérêt de ces matrices est de fournir des représentants explicites des classes de conjugaison de matrices et d'après le corollaire précédent J et ${}^tJ$ sont semblables donc choisir l'une ou l'autre a peu d'influence sur le résultat fondamental suivant

Théorème (Décomposition de Jordan) *Toute matrice carrée est semblable à une matrice composée de blocs de Jordan sur la diagonale et de zéros ailleurs, i.e. du type*

$$J = \begin{pmatrix} J(d_1,\lambda_1) & & \\ & \ddots & \\ & & J(d_r,\lambda_r) \end{pmatrix}$$

De plus les blocs sont uniques, à l'ordre près.

Nous donnons une preuve en terme de $K[X]$-modules, pour une preuve uniquement en terme de K-espace vectoriel, voir un cours d'algèbre linéaire.

Preuve. Le $K[X]$-module peut être décomposé en produit de modules cycliques $K[X]/PK[X]$ et comme $P = \prod_\lambda (X-\lambda)^{m_\lambda}$, on peut, en utilisant le lemme chinois généralisé le décomposer en produit de modules cycliques de la forme $K[X]/(X-\lambda)^m K[X]$. Pour analyser ce dernier, quitte à faire le changement de variable $Y = X - \lambda$ (ce qui revient aussi à remplacer u par $u - \lambda id$) on peut supposer $\lambda = 0$. Si l'on note x la classe de X dans $K[X]/X^m K[X]$, une K-base de $K[X]/X^m K[X]$ est fournie par $e_1 = 1$, $e_2 = x$, …, $e_m = x^{m-1}$ et dans cette base l'action de u, qui correspond à la multiplication par x est donnée par $u(e_1) = e_2$, $u(e_2) = e_3$, …, $u(e_{m-1}) = e_m$ et enfin $u(e_m) = x^m = 0$. La matrice de $u - \lambda id$ dans cette base est donc bien un bloc de Jordan $J(m)$. L'unicité des blocs (à l'ordre près) est claire si l'on observe que les dimensions des $\mathrm{Ker}(u-\lambda)^j$ sont déterminées par les (d_i,λ_i) et vice versa. □

C. CORPS et ANNEAUX.

C.1. Généralités et exemples de corps.

On supposera ici les corps commutatifs. Pour les corps finis, cette hypothèse n'est pas nécessaire (voir appendice à ce chapitre). Il existe des corps non commutatifs, le plus célèbre est le corps des quaternions, il est étudié dans un chapitre spécial. Nous connaissons déjà un certain nombre de corps commutatif : $\mathbf{Z}/p\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, si K est un de ces corps $K(X_1, \ldots, X_n)$ est encore un corps. Nous allons en construire d'autres.

Commençons par déterminer la caractéristique d'un corps K. L'homomorphisme $i_A : \mathbf{Z} \to K$ a une image qui est un sous-anneau intègre de K donc $\mathrm{Ker}(i_A)$ est un idéal premier. Ainsi soit $\mathrm{Ker}(i_A) = \{0\}$ et i_A est injectif et $\mathrm{car}(K) = 0$, soit il existe un nombre premier p tel que $\mathrm{Ker}(i_A) = p\mathbf{Z}$ et alors $\mathrm{car}(K) = p$. Dans le premier cas K contient un sous-anneau isomorphe à $\mathbf{Z}$ donc contient un sous-corps isomorphe à $\mathbf{Q}$, dans le second cas K contient un sous-corps isomorphe à $\mathbf{Z}/p\mathbf{Z}$. En caractéristique p le phénomène le plus remarquable est le suivant:

Lemme. *Soit K un corps de caractéristique p, alors l'application $\phi : K \to K$ définie par $\phi(x) = x^p$ est un homomorphisme de corps.*

Preuve. On a toujours $(xy)^p = x^p y^p$ (puisque l'on ne considère que les corps commutatifs); il suffit donc de prouver que, lorsque $\mathrm{car}(K) = p$, on a $(x+y)^p = x^p + y^p$. Ceci est en fait immédiat si l'on utilise la formule du binôme de Newton et l'observation que les coefficients binomiaux C_p^r sont divisibles par p pour $1 \leq r \leq p-1$. □

Remarque. Le lemme ne dit pas que ϕ est un isomorphisme, et d'ailleurs il n'est pas en général surjectif (prendre par exemple $K = (\mathbf{Z}/p\mathbf{Z})(X)$); par contre ϕ est toujours injectif, comme le montre un lemme ci-dessous, et définit donc un isomorphisme avec un sous-corps de K que l'on note souvent K^p. Dans le cas $K = (\mathbf{Z}/p\mathbf{Z})(X)$ on voit aisément que $K^p = (\mathbf{Z}/p\mathbf{Z})(X^p) \neq (\mathbf{Z}/p\mathbf{Z})(X)$.

Un autre phénomène spécifique à la caractéristique p est la possibilité pour un polynôme d'avoir une dérivée identiquement nulle sans être constant. En effet si $\mathrm{car}(K) = p$ et si $P \in K[X]$ est non constant, posons $Q(X) := P(X^p)$ alors $Q'(X) \equiv 0$. On définit ici bien sûr formellement la dérivée de $P = a_n X^n + \ldots + a_0$ par $P' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + a_1$. Montrons que la dérivée permet néanmoins de caractériser les racines simples d'un polynôme même en caractéristique p.

Lemme. *Soit K un corps, $\alpha \in K$ et $P \in K[X]$. Alors $(X - \alpha)$ divise P si et seulement si $P(\alpha) = 0$; de plus $(X-\alpha)^2$ divise P si et seulement si $P(\alpha) = P'(\alpha) = 0$.*

Preuve. On écrit d'abord la division euclidienne $P = (X-\alpha)Q + R$ avec $\deg(R) < 1$ donc R est constant et $P(\alpha) = R$ d'où le premier énoncé. On écrit ensuite la division euclidienne $P = (X-\alpha)^2 Q + R$ avec $\deg(R) \leq 1$ donc $R(X) = aX + b$. On a donc $P'(\alpha) = R'(\alpha) = a$ donc $P'(\alpha) = 0$ entraîne $a = 0$ et alors $P(\alpha) = b = 0$. □

Lemme. *Soit $f : K \to L$ un homomorphisme de corps, alors f est injectif.*

Preuve. Par définition $f(1_K) = 1_L$ et par conséquent, si $x \in K \setminus \{0\}$ on en tire $1_L = f(xx^{-1}) = f(x)f(x^{-1})$ donc $f(x) \neq 0$. □

Lorsque $f : K \to L$ est un homomorphisme de corps, on peut identifier K avec un sous-corps de L; on peut aussi considérer L comme un K-espace vectoriel en introduisant l'application:

$$\begin{array}{ccc} K \times L & \to & L \\ (x, y) & \mapsto & f(x)y \end{array}$$

Dans ce contexte on notera $[L : K] = \dim_K L$ la dimension de L vu comme K-espace vectoriel. La notation est en bonne partie motivée par la propriété importante suivante.

Proposition. *Soit $K \subset L \subset F$ une tour de corps, alors $[F : K] = [F : L][L : K]$.*

Preuve. Nous donnons la preuve lorsque ces dimensions sont finies, en fait l'énoncé et même la preuve restent valables avec des cardinaux quelconques. Considérons $e_1, \ldots, e_m$ une base de L sur K et $f_1, \ldots, f_n$ une base de F sur L, nous allons montrer que $\{e_i f_j \mid 0 \leq i \leq m,\ 0 \leq j \leq n\}$ fournit une base de L sur K. Montrons d'abord que c'est une partie génératrice. Soit $x \in F$, alors il existe $\lambda_i \in L$ tels que $x = \sum_{i=1}^{n} \lambda_i f_i$ (car les f_j forment une L-base de F). Par ailleurs il existe $\alpha_{ij} \in K$ tels que $\lambda_i = \sum_{j=1}^{m} \alpha_{ij} e_j$ (car les e_j forment une K-base de L) et donc $x = \sum_{i,j} \alpha_{ij} e_j f_i$. Montrons maintenant l'indépendance linéaire. Si $\alpha_{ij} \in K$ et $\sum_{i,j} \alpha_{ij} e_j f_i = 0$ alors $\sum_i \left(\sum_j \alpha_{ij} e_j \right) f_i = 0$ donc $\sum_j \alpha_{ij} e_j = 0$ (puisque les f_i sont L-linéairement indépendants) et donc les α_{ij} sont nuls (puisque les e_j sont K-linéairement indépendants). □

Un corollaire "évident" est que, si $K \subset L \subset F$ alors $[L : K] \leq [F : K]$; de plus, si ces dimensions sont finies, on a $[L : K] = [F : K]$ si et seulement si $F = L$.

Terminons ce paragraphe en citant sans détail d'autres exemples de corps.

(i) Soit p premier, considérons

$$\mathbf{Z}_p := \left\{ (a_n)_{n \geq 1} \in \prod_{n \geq 1} \mathbf{Z}/p^n\mathbf{Z} \mid a_{n+1} \equiv a_n \bmod p^n \right\}.$$

C'est un anneau intègre, appelé l'anneau des *entiers p-adiques*, son corps des fractions $\mathbf{Q}_p$ appelé le corps des *nombres p-adiques*. On peut montrer que $\mathbf{Q}_p$ est un analogue de $\mathbf{R}$ au sens qu'il est la complétion de $\mathbf{Q}$ pour la valeur absolue $|x|_p := p^{-\mathrm{ord}_p(x)}$.

(ii) Soit U un ouvert connexe du plan complexe, alors l'ensemble $\mathcal{M}(U)$ des fonctions méromorphes sur U est un corps.

(i) Soit K un corps, l'ensemble des *séries formelles* $\sum_{n=0}^{\infty} a_n X^n$ peut être muni d'une structure d'anneau noté $K[\![X]\!]$. En rendant inversible X, on obtient un corps appelé *corps des séries formelles* et noté $K(\!(X)\!)$. On peut aussi le voir comme l'ensemble des séries $\sum_{n \geq -n_0}^{\infty} a_n X^n$.

C.2. Eléments algébriques et transcendants.

Soit $K \subset L$ une extension de corps et $\alpha \in L$. Considérons l'homomorphisme d'anneaux "évaluation en α" définie de la manière suivante:

$$\begin{array}{rccc} ev_\alpha : & K[X] & \to & L \\ & P & \mapsto & P(\alpha) \end{array}$$

Lorsque $\mathrm{Ker}(ev_\alpha) = \{0\}$, on dit que α est *transcendant* sur K. Lorsque $\mathrm{Ker}(ev_\alpha) \neq \{0\}$, on dit que α est *algébrique* sur K. Si $\mathrm{Ker}(ev_\alpha) = PK[X]$, on appellera P le *polynôme minimal* de α sur K (il n'est tout-à-fait unique que si on lui impose d'être unitaire).

Notons $K[\alpha]$ le plus petit sous-anneau de L contenant K et α et $K(\alpha)$ le plus petit sous-corps de L contenant K et α. Par construction $K[\alpha]$ est l'image de ev_α donc est isomorphe à $K[X]/\operatorname{Ker}(ev_\alpha)$. Si α est trancendant, on voit que $K[\alpha] \cong K[X]$ et $K(\alpha) \cong K(X)$; en particulier $K(\alpha)$ est de dimension infinie sur K. Si α est algébrique et P son polynôme minimal sur K, alors P est irréductible dans $K[X]$ donc l'idéal engendré par P est maximal et $K[\alpha] = K(\alpha) \cong K[X]/PK[X]$. De plus dans ce cas on a $[K(\alpha) : K] = \deg(P)$. En effet une base de $K[\alpha] = K(\alpha)$ sur K est donnée par $1, \alpha, \alpha^2, \ldots, \alpha^{\deg(P)-1}$. On a en particulier prouvé:

Proposition. *Soit $\alpha \in L \supset K$ alors α est algébrique sur K si et seulement si $[K(\alpha) : K] < \infty$. Dans ce cas $[K(\alpha) : K]$ est le degré du polynôme minimal de α sur K.*

Remarque. On peut en déduire que si $K \subset F \subset L$ alors $[F(\alpha) : F] \leq [K(\alpha) : K]$. En effet le membre de gauche est le degré du polynôme minimal de α sur F qui divise le polynôme minimal de α sur K dont le degré est le membre de droite.

Corollaire. *Soit $\alpha, \beta \in L \supset K$ et supposons α, β algébriques sur K alors $\alpha + \beta$, $\alpha\beta$ et α/β sont algébriques sur K.*

Preuve. Il suffit de montrer que $[K(\alpha, \beta) : K] < \infty$. En effet on aura alors, pour tout élément $x \in K(\alpha, \beta)$ l'inégalité $[K(x) : K] \leq [K(\alpha, \beta) : K] < \infty$ et donc x algébrique sur K. Mais par ailleurs on a

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] \leq [K(\beta) : K][K(\alpha) : K] < \infty$$

ce qui achève la démonstration. □

Exemple. Soit $\delta = \sqrt[5]{2} + \sqrt[7]{3} + \sqrt[2]{5}$ alors δ est algébrique sur $\mathbf{Q}$. Illustrons les méthodes précédentes en montrant que $[\mathbf{Q}(\delta) : \mathbf{Q}] = 70$ donc son polynôme minimal est de degré 70 et serait fastidieux à écrire. Notons pour abréger $\alpha = \sqrt[5]{2}$, $\beta = \sqrt[7]{3}$ et $\gamma = \sqrt[2]{5}$. Alors le polynôme minimal sur $\mathbf{Q}$ de α (resp. β, resp. γ) est $X^5 - 2$ (resp. $X^7 - 3$, resp. $X^2 - 5$) donc $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 5$ (resp. $[\mathbf{Q}(\beta) : \mathbf{Q}] = 7$, resp. $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 2$). On a

$$[\mathbf{Q}(\delta) : \mathbf{Q}] \leq [\mathbf{Q}(\alpha, \beta, \gamma) : \mathbf{Q}] \leq [\mathbf{Q}(\alpha) : \mathbf{Q}][\mathbf{Q}(\beta) : \mathbf{Q}][\mathbf{Q}(\gamma) : \mathbf{Q}] = 5 \cdot 7 \cdot 2 = 70.$$

Mais $[\mathbf{Q}(\alpha, \beta, \gamma) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \beta, \gamma) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}]$ donc 5 (resp. 7, resp. 2) divise $[\mathbf{Q}(\alpha, \beta, \gamma) : \mathbf{Q}]$, donc 70 également d'où $[\mathbf{Q}(\alpha, \beta, \gamma) : \mathbf{Q}] = 70$. Enfin on laisse en exercice de vérifier que $\mathbf{Q}(\delta) = \mathbf{Q}(\alpha, \beta, \gamma)$ et donc le polynome minimal de δ est de degré 70. On pourra procéder ainsi: a) Vérifier que $\mathbf{Q}(\alpha + \beta) = \mathbf{Q}(\alpha, \beta)$ etc. b) Montrer que $\mathbf{Q}(\delta, \gamma) = \mathbf{Q}(\alpha, \beta, \gamma)$. c) Montrer que γ ne peut être de degré 2 sur $\mathbf{Q}(\delta)$ car sinon α serait aussi de degré 2 et conclure.

Corollaire. *Soit $K \subset L$ une extension de corps. Le sous-ensemble*

$$F := \{\alpha \in L \mid \alpha \text{ est algébrique sur } K\}$$

est un sous-corps de L.

Preuve. L'ensemble F est stable par toutes les opérations de corps donc est un sous-corps de L. □

Exemple. Considérons $\bar{\mathbf{Q}} := \{x \in \mathbf{C} \mid \text{ est algébrique sur } \mathbf{Q}\}$, c'est un sous-corps de $\mathbf{C}$. De plus $\bar{\mathbf{Q}}$ est algébriquement clos. En effet soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \bar{\mathbf{Q}}[X]$, montrons qu'il possède une racine dans $\bar{\mathbf{Q}}$. Introduisons $K = \mathbf{Q}(a_0, \ldots, a_{n-1})$ alors $[K : \mathbf{Q}] < \infty$. En effet

$$[\mathbf{Q}(a_0, \ldots, a_{n-1}) : \mathbf{Q}] = [\mathbf{Q}(a_0, \ldots, a_{n-1}) : \mathbf{Q}(a_0, \ldots, a_{n-2})] \ldots [\mathbf{Q}(a_0) : \mathbf{Q}]$$

et $[\mathbf{Q}(a_0,\ldots,a_i):\mathbf{Q}(a_0,\ldots,a_{i-1})] \leq [\mathbf{Q}(a_i):\mathbf{Q}] < \infty$. Soit maintenant $x \in \mathbf{C}$ une racine de P (il en existe puisque $\mathbf{C}$ est algébriquement clos) alors, comme $P \in K[X]$ on a $[K(x):K] < \infty$ donc $[\mathbf{Q}(x):\mathbf{Q}] \leq [K(x):\mathbf{Q}] = [K(x):K][K:\mathbf{Q}] < \infty$. Donc x est algébrique sur $\mathbf{Q}$ et appartient donc bien à $\bar{\mathbf{Q}}$.

Nous disposons maintenant de tous les outils nécessaires pour construire des extensions de corps. Nous savons déjà construire, à partir de K le corps $K(X) = \mathrm{Frac}(K[X])$. Soit $P = a_0 + a_1X + \ldots + a_nX^n$ un polynôme irréductible de $K[X]$ alors $L := K[X]/PK[X]$ est un corps qui contient de manière naturelle un sous-corps isomorphe à K. En effet considérons

$$i = s \circ j : K \overset{j}{\hookrightarrow} K[X] \overset{s}{\to} K[X]/PK[X]$$

on obtient $K' := i(K) \cong K$. Montrons que l'élément $\alpha \in L$ égal à la classe de X dans $K[X]/PK[X]$ est racine de $P' = i(a_0) + i(a_1)X + \ldots + i(a_n)X^n \in K'$. En effet

$$\begin{aligned} P'(\alpha) &= i(a_0) + i(a_1)\alpha + \ldots + i(a_n)\alpha^n \\ &= s \circ j(a_0) + s \circ j(a_1)s(X) + \ldots + s \circ j(a_n)s(X)^n \\ &= s\left(j(a_0) + j(a_1)X + \ldots + j(a_n)X^n\right)) \\ &= s(P) \\ &= 0 \end{aligned}$$

On voit qu'ainsi on peut fabriquer des extensions L d'un corps K quelconque, telles que des polynômes donnés à coefficients dans K admettent des racines dans L. On peut se demander si de telles constructions sont uniques en un certain sens. Voici la réponse.

Théorème. *Soit K un corps et $P \in K[X]$ non constant.*

(i) Il existe $L \supset K$ telle que L contienne une racine de P. De plus, si P est irréductible dans $K[X]$ et si L est minimale (i.e. si $K \subset L' \subset L$ et P possède une racine dans L' alors $L = L'$) alors L est unique à isomorphisme près et s'appelle un corps de rupture de P (en fait $L \cong K[X]/PK[X]$).

(ii) Il existe une extension $L \supset K$ telle que P soit scindé sur L c'est-à-dire $P = a(X-\alpha_1)\ldots(X-\alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L$ et minimale; une telle extension est unique à isomorphisme près et s'appelle le corps de décomposition de P sur K.

Preuve. (i) Soit L un corps contenant une racine α de P, alors $K(\alpha) \subset L$ donc L est minimal si et seulement si $L = K(\alpha)$; dans ce cas l'évaluation en α induit un isomorphisme $K[X]/PK[X] \cong K(\alpha) = L$. Prouvons maintenant, par récurrence sur $n = \deg(P)$, l'existence d'un corps de décomposition. Soit P_1 un facteur irréductible de P et K_1 un corps de rupture minimal de P_1 dans lequel il acquiert une racine α_1. Alors, dans $K_1[X]$ on peut factoriser $P = (X - \alpha_1)Q$. On dispose, par hypothèse de récurrence, d'une extension $L_1 \supset K_1$ sur laquelle Q, et par conséquent P est scindé, i.e. $P = a(X - \alpha_1)\ldots(X - \alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L_1$. On pose $L := K(\alpha_1, \ldots, \alpha_n)$ et alors P est encore scindé sur L et L est minimal puisque si $K \subset L' \subset L$ et P scindé sur L' alors L' contient K et les racines de P, c'est-à-dire $\alpha_1, \ldots, \alpha_n$ donc contient L. Prouvons maintenant, par récurrence sur $n = \deg(P)$, l'unicité (à isomorphisme près) d'un corps de décomposition. Pour faciliter l'induction, on va démontrer un résultat un tout petit plus général (qui achèvera la preuve du théorème) :

Lemme. *Soit $i : K \to K'$ un isomorphisme de corps. Soit P un polynôme de $K[X]$ et L un corps de décomposition de P sur K et soit L' un corps de décomposition de $i(P)$ sur K' alors il existe un isomorphisme $\phi : L \to L'$ qui prolonge i.*

Preuve. Tout d'abord on étend i en un isomorphisme $K[X] \to K'[X]$ que l'on note encore i. Soit $\alpha_1 \in L$ une racine de P et P_1 son polynôme minimal alors $P = P_1 Q$ et $i(P) = i(P_1)i(Q)$. Soit $\alpha'_1 \in L'$ une racine de $i(P_1)$. Alors $L_1 = K(\alpha_1)$ est un corps de rupture de P_1 et $L'_1 = K(\alpha'_1)$ est un corps de rupture de $i(P_1)$ donc on peut prolonger i en un isomorphisme $\phi_1 : L_1 :\to L'_1$ qui envoie α_1 sur α'_1. La factorisation $P = (X - \alpha_1)R$ dans $L_1[X]$ se traduit par la factorisation $i(P) = (X - \alpha'_1)\phi_1(R)$ dans $L'_1[X]$. Mais L est un corps de décomposition de R sur L_1 et L' est un corps de décomposition de $\phi_1(R)$ sur L'_1 donc, par hypothèse de récurrence, l'isomorphisme ϕ_1 se prolonge en un isomorphisme $\phi : L \to L'$. □

Exemple de corps de décomposition. Soit $K = \mathbf{Q}$ et $P = X^n - 2$, alors un corps de rupture est $\mathbf{Q}(\sqrt[n]{2})$ et un corps de décomposition $L = \mathbf{Q}\left(\exp(2i\pi/n)\sqrt[n]{2}, k = 0, 1, \ldots, n-1\right) = \mathbf{Q}\left(\sqrt[n]{2}, \exp(2i\pi/n)\right)$.

Ces théorèmes généraux montrent l'importance des polynômes irréductibles dans $K[X]$. Il est clair que les polynômes de degré 1 sont toujours irréductibles. De même un polynôme de degré 2 ou 3 est irréductible si et seulement si il ne possède pas de racine dans K. Déterminer les autres polynômes irréductibles est nettement plus délicat en général. Nous rappelons seulement ici que les seuls polynômes irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes du second degré sans racines réelles; nous donnons aussi deux critères d'irréductibilité et l'exemple des polynômes cyclotomiques.

Proposition. *Soit A un anneau factoriel et $K := \mathrm{Frac}(A)$, soit $P = a_n X^n + \ldots + a_0 \in A[X]$ et soit $p \in A$ un élément irréductible.*

(i) (Critère d'Eisenstein) Supposons que p ne divise pas a_n, que p divise $a_{n-1}, \ldots, a_0$, mais que p^2 ne divise pas a_0, alors P est irréductible dans $K[X]$.

(ii) (Critère de réduction) Supposons que p ne divise a_n, et que $\bar{P} \in (A/pA)[X]$ soit irréductible, alors P est irréductible dans $K[X]$.

Preuve. Pour les deux critères, on considère l'homomorphisme de réduction des coefficients d'un polynôme $P \mapsto \bar{P}$ de $A[X]$ dans $(A/pA)[X]$. Supposons donc que $P = QR$ avec $Q, R \in A[X]$, on en déduit $\bar{P} = \bar{Q}\bar{R}$. L'hypothèse de (i) indique que $\bar{P} = uX^n$ avec $u \neq 0$. Ainsi $uX^n = \bar{Q}\bar{R}$ entraîne $\bar{Q} = vX^d$ et $\bar{R} = wX^{n-d}$, si $d \neq 0, n$ on en tirerait que $Q = q_d X^d + \ldots + q_0$ avec p divisant q_0 et $R = r_{n-d}X^{n-d} + \ldots + r_0$ avec p divisant r_0; d'où p^2 divise $q_0 r_0$, ce qui contredirait les hypothèses. On conclut que $\bar{Q}$ ou $\bar{R}$ est constant et donc Q ou R est constant. L'hypothèse de (ii) indique que $\bar{Q}$ ou $\bar{R}$ est inversible donc constant dans $(A/pA)[X]$. Mais l'hypothèse $a_n \notin pA$ entraîne que les coefficients dominants de Q et R ne sont pas non plus divisibles par p et donc que $\deg(Q) = \deg(\bar{Q})$ et $\deg(R) = \deg(\bar{R})$ donc l'un des deux est constant. □

Remarques et exemples. Si l'on sait de plus que $c(P) = 1$ alors, sous les hypothèses de l'un des deux critères, on a P irréductible dans $A[X]$. En utilisant le critère d'Eisenstein pour $A = \mathbf{Z}$ et $p = 2$, on voit que $X^n - 2$ est irréductible dans $\mathbf{Q}[X]$ (ou $\mathbf{Z}[X]$). En utilisant le critère d'Eisenstein pour $A = \mathbf{Z}[Y]$ et $p = Y$, on voit que $P = (Y-1)X^n - Y^2X + Y$ est irréductible dans $A[Y] = \mathbf{Z}[X, Y]$. Le polynôme $\bar{P} = X^4 + X + 1 \in \mathbf{Z}/2\mathbf{Z}[X]$ est irréductible, en effet il n'a pas de racine dans $\mathbf{Z}/2\mathbf{Z}$ et le seul polynôme irréductible sur $\mathbf{Z}/2\mathbf{Z}$ de degré deux est $X^2 + X + 1$ qui ne divise pas $\bar{P}$. Par conséquent le polynôme $P = 11X^4 - 6X^3 + 4X^2 + 7X - 5$ est irréductible dans $\mathbf{Q}[X]$ (ou $\mathbf{Z}[X]$).

Les polynômes cyclotomiques sont les facteurs irréductibles de $X^n - 1$ dans $\mathbf{Q}[X]$ (ou $\mathbf{Z}[X]$); on peut les définir ainsi:

Définition. Soit $n \geq 1$, le n-ème *polynôme cyclotomique* est défini par

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

où μ_n^* est l'ensemble des racines n-èmes primitives de l'unité (dans $\mathbf{C}$).

Avec la définition donnée $\Phi_n \in \mathbf{C}[X]$ et il est clair que $\deg(\Phi_n) = \phi(n)$ et que

$$X^n - 1 = \prod_{d \,|\, n} \Phi_d(X) \qquad (*)$$

Cependant il est moins évident qu'en fait $\Phi_n \in \mathbf{Z}[X]$ et que Φ_n est irréductible dans $\mathbf{Q}[X]$ (ou $\mathbf{Z}[X]$). Commençons par voir que les coefficients de Φ_n sont entiers. Il est clair que $\Phi_1(X) = X - 1 \in \mathbf{Z}[X]$. On peut alors démontrer ce que l'on veut par induction sur n en utilisant la formule $(*)$. En effet le polynôme $B := \prod_{d \,|\, n, d \neq n} \Phi_d(X)$ est unitaire et, par hypothèse de récurrence, à coefficients entiers; on peut donc effectuer dans $\mathbf{Z}[X]$ la division euclidienne $X^n = BQ + R$. La formule $(*)$ garantit alors que $R = 0$ et $Q = \Phi_n$. Nous concluons avec le résultat suivant:

Théorème. *Le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$.*

Preuve. Soit ζ une racine primitive n-ème de l'unité et P son polynôme minimal sur $\mathbf{Q}$, on veut montrer que $P = \Phi_n$. Observons d'abord que $P \in \mathbf{Z}[X]$. Choisissons ensuite p un nombre premier ne divisant pas n alors ζ^p est encore une racine primitive n-ème de l'unité. Soit Q son polynôme minimal qui est également dans $\mathbf{Z}[X]$. Si P et Q étaient distincts, le produit PQ diviserait Φ_n. Mais comme $Q(\zeta^p) = 0$ on voit que ζ est racine de $Q(X^p)$ et donc $Q(X^p) = P(X)R(X)$ pour un certain $R \in \mathbf{Z}[X]$. En réduisant les coefficients modulo p on obtient:

$$\bar{Q}(X^p) = \bar{Q}(X)^p = \bar{P}(X)\bar{R}(X).$$

ou encore $\bar{P}(X)$ divise $\bar{Q}(X)^p$ dans $(\mathbf{Z}/p\mathbf{Z})[X]$ mais les facteurs de $X^n - 1$ et donc de $\bar{P}(X)$ sont simples dans $(\mathbf{Z}/p\mathbf{Z})[X]$ (la dérivée de $X^n - 1$ est nX^{n-1} et on a pris soin de choisir p ne divisant pas n) donc en fait $\bar{P}(X)$ divise $\bar{Q}(X)$. Mais alors $\bar{P}(X)^2$ divise $\bar{\Phi}_n(X)$ dans $(\mathbf{Z}/p\mathbf{Z})[X]$, ce qui contredit le fait que les facteurs de $\bar{\Phi}_n(X)$ sont simples. En résumé on a prouvé que, pour p premier ne divisant pas n, le polynôme minimal de ζ annulait ζ^p. On en tire aisément que, si m est premier avec n alors $P(\zeta^m) = 0$. Ainsi $\deg(P) \geq \phi(n)$ et comme P divise Φ_n, on a donc $P = \Phi_n$ et ce dernier est irréductible. □

Corollaire. *Soit ζ une racine primitive m-ème, alors $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(m)$.*

Preuve. Le polynôme minimal sur $\mathbf{Q}$ de ζ est Φ_m qui est de degré $\phi(m)$. □

Exercices. Montrer les formule suivantes
(a) Si p est premier, $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$.
(b) Si p premier divise n, alors $\Phi_{np}(X) = \Phi_n(X^p)$.
(c) Si p premier ne divise pas n, alors $\Phi_{np}(X)\Phi_n(X) = \Phi_n(X^p)$.

Montrer que, si $n \geq 3$, on a $[\mathbf{Q}(\cos(2\pi/n)) : \mathbf{Q}] = \phi(n)/2$. Pouvez-vous déterminer la dimension $[\mathbf{Q}(\sin(2\pi/n)) : \mathbf{Q}]$?

C.3. Corps finis.

Nous verrons en appendice qu'un corps fini est nécessairement commutatif. Si K est fini, sa caractéristique est un nombre premier p et K est un espace vectoriel de dimension finie (disons n) sur $\mathbf{Z}/p\mathbf{Z}$. On en tire en particulier que $\mathrm{card}(K) = \mathrm{card}\,((\mathbf{Z}/p\mathbf{Z})^n) = p^n$. Nous allons démontrer

Théorème. *Soit p un nombre premier et un entier $n \geq 1$, alors il existe un corps de cardinal p^n, unique à isomorphisme près. On le note $\mathbf{F}_{p^n}$.*

Remarque. Si $n = 1$ on connait déjà ce résultat et en fait $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Cependant, si $n \geq 2$, on a $\mathbf{F}_{p^n} \cong (\mathbf{Z}/p\mathbf{Z})^n$ en tant que $\mathbf{Z}/p\mathbf{Z}$-espaces vectoriels ou en tant que groupes additifs mais pas en tant qu'anneaux. On a ainsi trois anneaux à ne pas confondre : $\mathbf{Z}/p^n\mathbf{Z}$, $(\mathbf{Z}/p\mathbf{Z})^n$ et $\mathbf{F}_{p^n}$.

Exemple. Le polynôme $X^2 + X + 1 \in \mathbf{F}_2[X]$ est irréductible donc $\mathbf{F}_2[X]/(X^2 + X + 1)\mathbf{F}_2[X]$ est un corps de dimension 2 sur $\mathbf{F}_2$ donc de cardinal 4 donc isomorphe à $\mathbf{F}_4$.

Revenons à un corps fini K de cardinal $q = p^n$. On sait donc que $\mathrm{card}(K^*) = q - 1$ et donc que pour tout $x \in K^*$ on a $x^{q-1} = 1$ et donc pour tout $x \in K$ on a $x^q - x = 0$. Remarquons que si $X^q - X$ est considéré comme un polynôme à coefficients dans $\mathbf{F}_p$ on obtient la factorisation $X^q - X = \prod_{\alpha \in K}(X - \alpha) \in K[X]$. Ceci suggère l'énoncé suivant:

Théorème. *Soit $q = p^n$ et K le corps de décomposition de $X^q - X$ sur $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. C'est un corps de cardinal $q = p^n$ et tout corps de cardinal q lui est isomorphe.*

Preuve. Il suffit de prouver que si K est le corps de décomposition de $X^q - X$ sur $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, c'est un corps de cardinal q. Dans $K[X]$ on a $X^q - X = \prod_{i=1}^{q}(X - \alpha_i)$. Posons $S := \{\alpha \in K \mid \alpha^q - \alpha = 0\}$. L'ensemble S des racines de $X^q - X$ dans K a pour cardinal q car $X^q - X$ est scindé sur K et les racines sont simples car la dérivée est le polynôme constant -1. Montrons que S est un sous-corps de K et donc $K = S$. En effet si $\alpha^q - \alpha = 0$ et $\beta^q - \beta = 0$ alors $(\alpha + \beta)^q - (\alpha + \beta) = \alpha^q + \beta^q - \alpha - \beta = 0$ et donc $\alpha + \beta \in S$; par ailleurs si $p \neq 2$, on a $(-\alpha)^q - (-\alpha) = -\alpha^q + \alpha = 0$ donc $-\alpha \in S$; enfin $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$ donc $\alpha\beta \in S$ et (si α est non nul) $(\alpha^{-1})^q = \alpha^{-q} = \alpha^{-1}$ donc $\alpha^{-1} \in S$. □

Remarques. Il est clair que l'homomorphisme $\phi : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ défini par $\phi(x) = x^p$ est un isomorphisme car une application injective entre deux ensembles finis de même cardinal est une bijection. On a clairement $\phi^n = id_{\mathbf{F}_{p^n}}$ puisque $x^{p^n} = x$ pour tout $x \in \mathbf{F}_{p^n}$. Par ailleurs, nous avons vu qu'un sous-groupe fini de K^* (avec K corps commutatif) est cyclique, donc $\mathbf{F}_{p^n}^*$ est isomorphe (comme groupe) à $\mathbf{Z}/(p^n - 1)\mathbf{Z}$. On voit donc que l'application $x \mapsto x^m$ définit une bijection de $\mathbf{F}_{p^n}^*$ (ou $\mathbf{F}_{p^n}$) si et seulement si $\mathrm{PGCD}(m, p^n - 1) = 1$; c'est un homomorphisme de groupe sur $\mathbf{F}_{p^n}^*$ mais bien sûr pas un homomrphisme d'anneaux sur $\mathbf{F}_{p^n}$. Lorsque $d := \mathrm{PGCD}(m, p^n - 1)$ est différent de 1, le noyau est cyclique de cardinal d et on a $(\mathbf{F}_{p^n}^* : \mathbf{F}_{p^n}^{*m}) = d$.

Exercices. Montrer que $\mathbf{F}_q$ est (isomorphe à) un sous-corps de $\mathbf{F}_{q'}$ si et seulement si $q = p^m$ et $q' = p^n$ avec m divisant n.

Appendice : le théorème de Wedderburn.

Il s'agit du résultat suivant:

Théorème. (théorème de Wedderburn) *Soit K un corps fini, alors K est commutatif.*

Preuve. Soit $Z = \{x \in K \mid \forall y \in K,\ xy = yx\}$ alors Z est clairement un sous-corps commutatif de K; notons $q = \mathrm{card}(Z)$ et $n = \dim_Z K$. On va montrer par l'absurde qu'on ne peut avoir

$n \geq 2$. Considérons le groupe K^* et son action sur lui-même par conjugaison. Soit $y \in K^*$, si on pose $C(y) = \{x \in K \mid xy = yx\}$ alors $C(y)$ est un sous-corps de K qui contient Z; notons $n_y = \dim_Z C(y)$. On a $C(y) = K$ si et seulement si $y \in Z$ et le stabilisateur de y sous l'action de K^* est $C(y)^* = C(y) \setminus \{0\}$, ainsi la formule des classes s'écrit:

$$q^n - 1 = \mathrm{card}(K^*) = \mathrm{card}(Z^*) + \sum_{y \in R} \frac{\mathrm{card}(K^*)}{\mathrm{card}(C(y)^*)} = q - 1 + \sum_{y \in R} \frac{q^n - 1}{q^{n_y} - 1}$$

où R désigne un ensemble de représentants des classes de conjugaison non réduites à un élément, ou encore telles que $1 \leq n_y < n$. On fait maintenant l'observation que $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ où $\Phi_d \in \mathbf{Z}[X]$ désigne le polynôme cyclotomique. On voit donc que $q^n - 1 = \prod_{d \mid n} \Phi_d(q)$ et donc que $\Phi_n(q)$ divise $q^n - 1$ et même $(q^n - 1)/(q^{n_y} - 1)$ lorsque $n_y < n$. En revenant à l'équation des classes, on voit donc que $\Phi_n(q)$ divise $q - 1$. En particulier $|\Phi_n(q)| \leq q - 1$. Mais $|\Phi_n(q)| = \prod_\zeta |q - \zeta|$ où ζ parcourt les racines n-èmes primitives et l'on a $|q - \zeta| \geq q - 1$, d'où une contradiction si $n \geq 2$. $\square$

Exercice (Théorème de Chevalley-Waring). Soit $k = \mathbf{F}_q$ un corps fini de caractéristique p. On veut montrer que si $P \in k[x_1, \ldots, x_n]$ avec $\deg(P) < n$ alors

$$\mathrm{card}\{x \in k^n \mid P(x) = 0\} \equiv 0 \bmod p.$$

En particulier, si P est homogène de degré $d < n$ alors P possède un zéro non trivial (i;e. distinct de 0). On pourra procéder ainsi :

(a) Montrer que $\sum_{x \in k} x^m$ est nul si $m = 0$ ou si $q - 1$ ne divise pas m mais vaut -1 dans les autres cas. [Comme le polynôme "X^0" est le polynôme constant, il est naturel de prendre ici la convention $0^0 = 1$].

(b) Soit $P \in k[x_1, \ldots, x_n]$ avec $\deg(P) < (q-1)n$, en déduire que $\sum_{x \in k^n} P(x) = 0$.

(c) Appliquer le résultat précédent à $P(x)^{q-1}$ et conclure.

(d) Démontrer par une méthode analogue la généralisation suivante. Soient $P_1, \ldots, P_s$ des polynômes de degrés $d_1, \ldots, d_s$ avec $d_1 + \ldots + d_s < n$, montrer que

$$\mathrm{card}\{x \in k^n \mid P_1(x) = \ldots = P_s(x) = 0\} \equiv 0 \bmod p.$$

En particulier, si les polynômes sont homogènes, ils ont un zéro commun non trivial.

Exercice. Montrer que $\mathbf{F}_{p^m} \subset \mathbf{F}_{p^n}$ si et seulement si m divise n.

D. Théorie de Galois (Résumé)

Ce chapitre donne les énoncés mais ne détaille pas les démonstrations (qui seront elles données en cours). Dans tout le chapitre, les extensions sont des extensions algébriques finis (sauf mention contraire); on fera un usage modéré de la clôture algébrique d'un corps.

D.1. Automorphismes de corps et propriétés des extensions.

Rappelons les "opérations" sur les extensions. Si F est une extension de K et L une extension de F, alors L est une extension de K; on dira aussi que F est une extension intermédiaire ou sous extension de L/K. Si K_1 et K_2 sont deux extensions de K, toutes deux contenues dans une extension L on peut fabriquer d'autres extensions : d'une part $K_1 \cap K_2$ est une extension de K et, d'autre part la plus petite sous-extension de L contenant K_1 et K_2 est une extension appelée *compositum* de K_1 et K_2 et notée K_1K_2. Remarquez que ces deux dernières ($K_1 \cap K_2$ et K_1K_2) n'ont de sens que si K_1 et K_2 sont contenues toutes deux dans une extension plus grande.

Notations. On notera $\mathrm{Aut}(L)$ le groupe d'automorphismes d'un corps L. Si L est une extension de K on notera $\mathrm{Aut}(L/K)$ le sous-groupe de $\mathrm{Aut}(L)$ composé des automorphismes induisant l'identité sur K:

$$\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \forall x \in K,\ \sigma(x) = x\}.$$

Si G est un sous-groupe de $\mathrm{Aut}(L)$ on note L^G le sous-corps fixé par G, c'est-à-dire :

$$L^G := \{x \in L \mid \forall \sigma \in G,\ \sigma(x) = x\}.$$

Proposition. *Soit G un sous-groupe fini de $\mathrm{Aut}(L)$ de cardinal n, posons $K := L^G$ alors on a $[L : K] = n$ et $\mathrm{Aut}(L/K) = G$.*

Définition. Une extension algébrique L/K est *normale* si pour tout $\alpha \in L$ les racines du polynôme minimal de α sur K sont toutes dans L.

En d'autres termes, si P est un polynôme irréductible de $K[X]$ et possède 1 racine dans L alors il est scindé sur L.

Exemples. 1) L'extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ n'est pas normale car le polynôme minimal de $\alpha = \sqrt[3]{2}$ sur $\mathbf{Q}$ est $X^3 - 2$ et les deux autres racines $j\alpha$ et $j^2\alpha$ ne sont pas dans $\mathbf{Q}(\sqrt[3]{2})$. Ainsi $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{id\}$. Par contre une extension de degré 2 est toujours normale. En effet; si α est racine de $X^2 + aX + b \in K[X]$, alors l'autre racine s'écrit $\beta = -a - \alpha$ et on a bien $\beta \in K(\alpha)$.
2) Si $P \in K[X]$ est scindé dans une certaine extension et a pour racine $\alpha_1, \ldots, \alpha_n$, posons $L = K(\alpha_1, \ldots, \alpha_n)$, alors l'extension L/K est normale.

Proposition. *Si $L = K(\alpha)$ et les racines du polynôme minimal de α sur K sont toutes dans L, alors L/K est normale. Soit K_1 et K_2 normales sur K et contenues dans une même extension, le compositum K_1K_2 est normal sur K.*

Définition. Une extension algébrique L/K est *séparable* si pour tout $\alpha \in L$ les racines du polynôme minimal de de α sur K sont toutes distinctes.

Exemples. 1) Une extension de corps de caractéristique zéro L/K est toujours séparable. En effet si $P \in K[X]$ est irréductible et $\alpha \in L$ est une racine double de P alors α est une racine de

P' et donc P divise P', ce qui, pour des raisons de degrés, impose $P' = 0$, ce qui est impossible en caractéristique zéro (en caractéristique p, cela entraîne seulement qu'il existe $Q \in K[X]$ tel que $P(X) = Q(X^p)$).
2) Une extension de corps finis L/K est toujours séparable. En effet si on note p la caractéristique et on reprend le raisonnement précédent, on voit que $P' = 0$ n'est possible que si $P(X) = a_0 + a_1X^p + \ldots + a_dX^{dp}$. Cependant, l'application $x \mapsto x^p$ est bijective de K sur K donc il existe $b_j \in K$ tel que $b_j^p = a_j$ et donc

$$P(X) = a_0 + a_1X^p + \ldots + a_dX^{dp} = b_0^p + b_1^pX^p + \ldots + b_d^pX^{dp} = \left(b_0 + b_1X + \ldots + b_dX^d\right)^p,$$

ce qui contredirait P irréductible.
3) Un exemple typique d'extension non séparable est $\mathbf{F}_p(T)/\mathbf{F}_p(T^p)$ où T est une indéterminée.

Proposition. *Soit L/K une extension de degré n, alors le groupe* $\mathrm{Aut}(L/K)$ *a un cardinal inférieur ou égal à n (en fait divisant n). De plus on a $|\mathrm{Aut}(L/K)| = [L : K]$ si et seulement si l'extension L/K est normale et séparable.*

Le point clef est de montrer que si $L = K(\alpha)$, le nombre de plongements de L dans $\bar{B}$ une clôture algébrique de K, induisant l'identité sur K est égal au nombre de racines du polynôme minimal de α sur K. Ainsi, si L/K est séparable, il y a $[L : K]$ tels plongements. Enfin ces plongements correspondent à des automorphismes de L si et seulement si les dites racines sont dans L, i.e. si L/K est normale.

D.2. Correspondance de Galois.

Définition. Une extension L/K est *galoisienne* si elle est normale et séparable. Dans ce cas on note on appelle *groupe de Galois* de l'extension L/K et on note $\mathrm{Gal}(L/K)$ le groupe $\mathrm{Aut}(L/K)$.

D'après les proprositions précédentes, si L/K est galoisienne et $G = \mathrm{Gal}(L/K)$ alors on a $K = L^G$ et $|G| = [L : K]$. Le théorème fondamental de la théorie de Galois est le suivant.

Théorème. *Soit L/K une extension galoisienne de groupe $G := \mathrm{Gal}(L/K)$.*
(i) L'application qui a un sous-groupe H de G associe le sous-corps L^H et l'application qui a une sous-extension $K \subset F \subset L$ associe le sous-groupe $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ *sont des bijections réciproques l'une de l'autre.*
(ii) Une sous-extension F est galoisienne sur K si et seulement si le sous-groupe associé $H :=$ $\mathrm{Gal}(L/F)$ *est distingué dans* $\mathrm{Gal}(L/K)$*. Dans ce cas l'application définie par restriction $\rho : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ est un homomorphisme surjectif de noyau* $\mathrm{Gal}(L/F)$ *et induit donc un isomorphisme naturel entre* $\mathrm{Gal}(F/K)$ *et le quotient* $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.

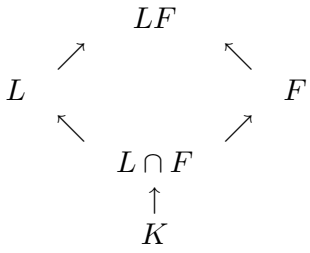
Corollaire. *Soit L/K une extension galoisienne, il existe un nombre fini de sous-extensions $K \subset F \subset L$.*

En effet il existe clairement un nombre fini de sous-groupes de $G := \mathrm{Gal}(L/K)$.

Le corollaire peut paraître évident pour une extension finie, il ne l'est pas. Ainsi si $L = \mathbf{F}_p(X, Y)$ et $K = \mathbf{F}_p(X^p, Y^p)$ on a $[L : K] = p^2$ et il existe une infinité de sous-extensions distinctes! Bien entendu, l'extension L/K dans ce cas n'est pas galoisienne, ni même séparable.

Donnons maintenant d'autres propriétés "fonctorielle" des groupes de Galois. plaçons-nous dans le cas suivant : on dispose de deux extensions L, F de K, toute deux contenues dans un même corps (par exemple une clôture algébrique de K) et on peut donc considérer le compositum LF

des deux extensions. On peut représenter la situation par un diagramme (où une flèche $K \to F$ désigne une injection de corps) :



Corollaire. *Supposons que L/K et F/K soient galoisiennes, alors LF/K est également galoisienne, et* $\mathrm{Gal}(LF/K)$ *est naturellement un sous-groupe de* $\mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$. *On a* $[LF : K] = [L : K][F : K]/[L \cap F : K]$. *En particulier on a une identification naturelle* $\mathrm{Gal}(LF/L \cap F) = \mathrm{Gal}(L/L \cap F) \times \mathrm{Gal}(F/L \cap F)$.

Corollaire. *Soit L/K un extension galoisienne de groupe de Galois G, soit F une extension de K contenue dans une même extension que L (de sorte que LF soit défini) alors l'extension LF/F est galoisienne et son groupe de Galois est (isomorphe à) un sous-groupe de G.*

D.3. Applications et exemples.

Commençons par quelques calculs de groupes de Galois sur $\mathbf{Q}$. On a vu que si $P \in \mathbf{Q}[X]$ est un polynôme (irréductible ou non) de racine $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ alors le corps de décomposition $L = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ est galoisien sur $\mathbf{Q}$; on appellera $G := \mathrm{Gal}(L/\mathbf{Q})$ le *groupe de Galois du polynôme.*

Soit α une racine de $P = X^2 + aX + b$ supposé irréductible sur $\mathbf{Q}$. Soit $\delta \in \mathbf{C}$ tel que $\delta^2 = a^2 - 4b$, on a alors $\mathbf{Q}(\alpha) = \mathbf{Q}(\delta) = \mathbf{Q} \oplus \mathbf{Q}\delta$ et $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q}) = \{id, \sigma\} \cong \mathbf{Z}/2\mathbf{Z}$ avec σ donné par $\sigma(m + n\delta) = m - n\delta$.

Soit $\alpha = \alpha_1, \alpha_2, \alpha_3$ les racines de $P = X^3 + aX + b$ supposé irréductible sur $\mathbf{Q}$, soit $L = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$ et $G = \mathrm{Gal}(L/\mathbf{Q})$. Comme P est irréductible, on a $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$ donc 3 divise $[L : \mathbf{Q}] = |G|$. Par ailleurs G peut être vu comme un sous-groupe de $\mathcal{S}_3$ donc, ou bien $G = \mathcal{A}_3 \cong \mathbf{Z}/3\mathbf{Z}$ (et dans ce cas $L = \mathbf{Q}(\alpha)$) ou bien $G = \mathcal{S}_3$. Il est possible de distinguer les deux cas en introduisant $\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ et $\Delta := \delta^2 = -(4a^3 + 27b^2)$. On a $G = \mathcal{A}_3$ si Δ est un carré dans $\mathbf{Q}$ (i.e. si $\delta \in \mathbf{Q}$) et $G = \mathcal{S}_3$ sinon. Dans ce dernier cas $\mathbf{Q}(\delta) = L^{\mathcal{A}_3}$. Exemples concrets. Si $P = X^3 - X + 1$, on trouve $\Delta = -23$ donc $[L : \mathbf{Q}] = 6$, $G = \mathcal{S}_3$ et $\mathbf{Q}(i\sqrt{23}) = L^{\mathcal{A}_3} \subset L$. Si $P = X^3 - 21X - 7$, on trouve $\Delta = 3^6 \cdot 7^2$ et ainsi $[L : \mathbf{Q}] = 3$.

On a vu en introduction comment écrire les racines d'une équation de degré 2,3,4 avec des extractions de racines carrés, cubiques etc; formalisons cela en terme d'extensions de corps.

Définition Soit $a \in K$, une *racine n-ème* de a est un élément α dans une extension de K tel que $\alpha^n = a$. Une extension L/K est *engendrée par des radicaux* s'il existe une suite d'extensions $K = K_0 \subset K_1 \subset \ldots \subset K_m$ telles que $L \subset K_m$ et $K_{i+1} = K_i(\alpha_i)$ avec $\alpha_i^{n_i} = a_i \in K_i$. Une équation $P(X) = 0$ est *résoluble par radicaux* au dessus d'un corps K si son corps de décomposition est engendré par des radicaux sur K.

Lemme. *Soit $P = X^5 + \ldots + a_0$ un polynôme irréductible dans $\mathbf{Q}[X]$ possédant trois racines réelles et une paire de racines complexes. Le groupe de Galois de P est $\mathcal{S}_5$.*

Soit $L := \mathbf{Q}(\alpha_1, \ldots, \alpha_5)$ et $G := \mathrm{Gal}(L/\mathbf{Q}) \subset \mathcal{S}_5$. Comme P irréductible on a $[\mathbf{Q}(\alpha_1) : \mathbf{Q}] = 5$ donc 5 divise $[L : \mathbf{Q}] = |G|$ et G contient donc un élément d'ordre 5, c'est-à-dire un 5-cycle. La conjugaison complexe est un élément de G, laisse fixe 3 des racines et échange les deux autres, ainsi G contient une transposition. Un lemme de théorie des groupes indique qu'un 5-cycle et une transposition engendrent $\mathcal{S}_5$, donc $G = \mathcal{S}_5$.

Proposition. *Le groupe de Galois du polynôme $P = X^5 - 10X + 2$ est $\mathcal{S}_5$.*

En effet il est irréductible par le critère d'Eisenstein (appliqué avec $p = 2$) et l'étude de ses variations permet de vérifier aisément qu'il possède 3 racines réelles.

Théorème. *Soit $\zeta = \exp(2\pi i/n)$ une racine primitive n-ème de l'unité, l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est galoisienne de groupe $(\mathbf{Z}/n\mathbf{Z})^*$. Plus généralement, si K est un corps de caractéristique première à n et si ζ est une racine primitive n-ème de l'unité, l'extension $K(\zeta)/K$ est galoisienne de groupe de Galois un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$.*

Théorème. *Soit K un corps contenant les racines n-èmes de l'unité, soit $a \in K^*$ et α une racine de $X^n - a = 0$ alors $K(\alpha)/K$ est galoisienne de groupe isomorphe à un sous-groupe de $\mu_n \cong \mathbf{Z}/n\mathbf{Z}$.*

Les deux théorèmes précédents montrent que l'adjonction de racines n-èmes produit des extensions abéliennes par étages et donc engendre des extensions dont le groupe de Galois sera résoluble. Le résultat suivant est une sorte de réciproque du théorème précédent.

Théorème. *Soit K un corps contenant les racines n-èmes de l'unité et L une extension galoisienne avec $\mathrm{Gal}(L/K) \cong \mathbf{Z}/n\mathbf{Z}$ alors il existe $\alpha \in L$ tel que $\alpha^n \in K$ et $L = K(\alpha)$.*

Théorème. *Une équation $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$ est résoluble par radicaux (à partir du corps K) si et seulement si son groupe de Galois est résoluble.*

Corollaire. *Les équations de degré $2, 3$ et 4 sont résolubles par radicaux; une équation de degré $n \geq 5$ n'est pas en général résoluble par radicaux.*

La dernière phrase peut être explicitée de deux façons. Soit $P = X^5 + aX^4 + bX^3 + cX^2 + dX + e$ (ou de degré ≥ 5), alors il n'existe pas de formule exprimant les racines de P à l'aide de a, b, c, d, e et des opérations de corps et d'extraction de racines n-èmes. On peut aussi établir qu'il existe des polynômes de degré n dont le groupe de Galois est $\mathcal{S}_n$ (cette dernière propriété utilise la nature du corps $\mathbf{Q}$ puisqu'elle est visiblement fausse si on remplace $\mathbf{Q}$ par $\mathbf{R}$ ou un corps fini (Cf ci dessous).

Exemple. Soit $P = X^5 - 2 \in \mathbf{Q}[X]$, notons $\zeta := \exp(2\pi i/5)$ et $\alpha = \alpha_1 = \sqrt[5]{2}$ alors les racines de P sont $\alpha_j = \zeta^j\alpha$ (pour $0 \leq j \leq 4$) et ainsi $L := \mathbf{Q}(\alpha_1, \ldots, \alpha_4) = \mathbf{Q}(\alpha, \zeta)$. L'extension $F := \mathbf{Q}(\zeta)$ est galoisienne sur $\mathbf{Q}$ de groupe $(\mathbf{Z}/5\mathbf{Z})^* \cong \mathbf{Z}/4\mathbf{Z}$ et L/F est galoisienne de groupe $\mathbf{Z}/5\mathbf{Z}$. On a donc

$$\{id\} \subset \mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/\mathbf{Q})$$

avec $\mathrm{Gal}(L/F)$ et $\mathrm{Gal}(L/\mathbf{Q})/\mathrm{Gal}(L/F)$ abéliens, ce qui montre bien que $\mathrm{Gal}(L/\mathbf{Q})$ est résoluble. On notera que $\mathrm{Gal}(L/F)$ n'est pas abélien car $\mathrm{Gal}(L/\mathbf{Q}(\alpha))$ n'est pas distingué dans $\mathrm{Gal}(L/F)$ (sinon $\mathbf{Q}(\alpha)/\mathbf{Q}$ serait galoisienne, ce qui n'est pas).

La théorie de Galois sur les corps finis est particulièrement simple:

Théorème. *Soit L/K un extension de corps fini, notons $q = \mathrm{card}(K)$ et $m = [L : K]$ alors*

$$\mathrm{Gal}(L/K) = \mathbf{Z}/m\mathbf{Z}$$

où un générateur canonique (appelé "Frobenius" est donné par $\Phi(x) = x^q$.

Remarque. On retrouve ainsi le critère pour qu'un élément $\alpha \in L$ soit dans K : il faut et il suffit que $\alpha^q = \alpha$.

Terminons par un théorème permettant de se ramener, la plupart du temps, aux extensions par un élément.

Théorème. (théorème de l'élément primitif) *Soit L/K une extension finie, les deux propriétés suivantes sont équivalentes :*

(i) Il existe $\alpha \in L$ tel que $L = K(\alpha)$.

(ii) Il existe un nombre fini de sous-extensions $K \subset F \subset L$.

De plus, si L/K est séparable, ces propriétés sont vérifiées.

Preuve. Supposons $L = K(\alpha)$, pour toute sous-extension F, introduisons P_F le polynôme minimal de α sur F. Comme P_F divise $P := P_K$ (disons dans $L[X]$), il ne peut prendre qu'un nombre finide valeurs. Introduisons F_0 l'extension de K engendrée par les coefficients du polynôme P_F; on a bien sûr $K \subset F_0 \subset F$ et un instant de réflexion montre que $P_{F_0} = P_F$. On en tire que $[L : F] = [F(\alpha) : F] = \deg(P_F)$ est donc égal à $[L : F_0]$, ce qui entraîne $F = F_0$. Ainsi F est caractérisé par P_F et il n'y a qu'un nombre fini de possibilités. Inversement comme $L = K(\alpha_1, \ldots, \alpha_n)$, par récurrence, il suffit de prouver que si $L = K(\alpha, \beta)$ ne contient qu'un nombre fini de sous-extensions, alors il existe $\gamma \in L$ avec $L = K(\gamma)$. Si K est fini c'est évident car L^* est cyclique. Si K est infini alors les extensions $K(\alpha + c\beta)$ étant en nombre fini lorsque c parcourt K, il existe $c_1 \neq c_2 \in K$ tels que $F := K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Mais alors comme on a

$$\beta = \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} \qquad \text{et} \qquad \alpha = \frac{c_1(\alpha + c_2\beta) - c_2(\alpha + c_1\beta)}{c_1 - c_2}$$

on en tire $F = K(\alpha, \beta) = L$. Enfin si L/K est séparable, soit L'/K l'extension normale obtenue en rajoutant les conjugués d'éléments de K, i.e. une clôture galoisienne de L/K; l'extension $L'K$ est donc galoisienne et ne contient qu'un nombre fini de sous-extensions et par conséquent L également. □

Remarques. La démonstration montre que, si $L = K(\alpha_1, \ldots, \alpha_n)$ est séparable sur K alors il existe $c_2, \ldots, c_n \in K$ tel que l'élément $\gamma := \alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$ vérifie $L = K(\gamma)$. Inversement, comme tout élément $\alpha \in L := \mathbf{F}_p(X, Y)$ vérifie $\alpha^p \in K := \mathbf{F}_p(X^p, Y^p)$, on a $K(\alpha) \neq L$ ainsi il y a une infinité de sous-extensions. En fait en reprenant la preuve, on voit que les extensions $K(X + UY)$ pour $U \in K$ sont toutes distinctes.

Terminons en explicitant, en terme de théorie de Galois, la résolution de l'équation de degré 3 ou 4. On prend donc un polynôme de degré 3 (resp. 4) sur K et on note L le corps de décomposition; on suppose que $\mathrm{Gal}(L/K) = \mathcal{S}_3$ (resp. $\mathcal{S}_4$), sinon la solution s'en trouve simplifiée.

(n=3). A la suite $\{id\} \subset \mathcal{A}_3 \subset \mathcal{S}_3 = \mathrm{Gal}(L/K)$ correspond $K = K_0 \subset K_1 \subset K_2 = L$ avec $[K_1 : K] = 2$ et $[L : K_1] = 3$, ainsi $K_1 = K(\sqrt{\Delta})$ pour un certain $\Delta \in K$ et *si l'on rajoute les racines troisièmes de l'unité* en posant $K_1' = K_1(\zeta_3)$, l'extension LK_1'/K_1' est galoisienne de groupe $\mathbf{Z}/3\mathbf{Z}$ donc $LK_1' = K_1'(\alpha)$ avec $\alpha^3 \in K_1'$. Ainsi l'extension $L(\zeta_3)$ est engendrée par des radicaux.

(n=4). A la suite $\{id\} \subset \mathcal{K} \subset \mathcal{A}_4 \subset \mathcal{S}_4 = \mathrm{Gal}(L/K)$ correspond $K = K_0 \subset K_1 = L^{\mathcal{A}_4} \subset K_2 = L^{\mathcal{K}} \subset K_3 = L$; l'extension L/K_2 galoisienne de groupe de galois $\mathcal{K} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ donc $L = K_2(\sqrt{\Delta_1}, \sqrt{\Delta_2})$; l'extension K_2/K_1 galoisienne de groupe de galois $\mathcal{A}_4/\mathcal{K} \cong \mathbf{Z}/3\mathbf{Z}$ donc après avoir rajouté une racine troisième de l'unité $K_2' = K_1'(\sqrt[3]{E})$; enfin K_1/K est quadratique.