UVSQ 2009/2010
Licence de sciences et technologie, santé
LSMA211 (algèbre générale)

Cours en bref

Table des matières

1 Premiers éléments sur les groupes

1.1 La structure de groupe

Structures de groupe (abélien surtout pour cette UE), mais aussi d'anneau, de corps, d'espace vectoriel. Lecture du polycopié pour les groupes.
Exemples déjà accessibles sur les groupes : $(\mathbb{Z}, +)$, extension aux sous-groupes additifs de $\mathbb{C}$; $(\mathbb{Q}^*, \times)$, extension aux sous-groupes multiplicatifs de $\mathbb{C}^*$, dont les groupes de racines de l'unité qui sont finis (deux mots sur les racines $n^{\text{ième}}$ de l'unité, ce sont les puissances de $\exp(2i\pi/n)$, il y en a n) ; $(\mathbb{Q}_+^*, \times)$, extension aux sous-groupes multiplicatifs de $\mathbb{R}_+^*$. Les homomorphismes fondamentaux pour ces groupes : $x \mapsto ax$ pour les structures additives, $x \mapsto x^n$ pour les structures multiplicatives ($n \in \mathbb{Z}$), exponentielle $(\mathbb{C}, +) \to (\mathbb{C}^*, \times)$ et sa restriction aux sous-groupes additifs de $\mathbb{C}$; en composant, $(\mathbb{R}, +) \to (\{z \in \mathbb{C},\ |z| = 1\}, \times)$, $x \mapsto \exp(ix)$.
Les bijections d'un ensemble sur lui-même pour la composition des applications (pas du tout commutatif). Les automorphismes d'un groupe ou d'un espace vectoriel pour la composition. Les matrices inversibles pour la multiplication. Un homomorphisme fondamental : le déterminant.

Définition L'*ordre* d'un groupe G est son cardinal. On le note $|G|$. Quand G est fini, $|G|$ est le nombre d'éléments de G.
Exemple : $|\mathbb{U}_4| = 4$. Un autre groupe d'ordre 4 : le sous-groupe $G = \{\pm I_2, \pm A\}$ de $\mathrm{GL}(2, \mathbb{R})$ où A est la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Ces groupes ne sont pas isomorphes car le carré de tout élément de G est trivial alors que $i^2 \neq 1$.

L'image réciproque d'un sous-groupe est un sous-groupe. Définition du noyau, c'est un sous-groupe. Injectivité des homomorphismes. Exemple de $\mathrm{SL}(n, \mathbb{C})$, sous-groupe de $\mathrm{GL}(n, \mathbb{C})$ (on peut remplacer $\mathbb{C}$ par n'importe quel corps, commentaire).
L'image d'un sous-groupe est un sous-groupe. L'image d'un homomorphisme est un sous-groupe.
Si $f : G \to G'$ est un homomorphisme, alors pour tout $x' \in \operatorname{im} f$, si $x \in G$ est tel que $f(x) = x'$, alors $f^{-1}(x') = x.\ker f = \ker f.x$. En particulier, par le théorème des bergers, $|G| = |\operatorname{im} f|.|\ker f|$ (même si les cardinaux sont infinis).

Si H est un sous-groupe d'un groupe G et si $x \in G$, on note $Hx = \{hx,\ h \in H\}$ la *classe à droite de x modulo H*. L'application $H \to Hx$, $h \mapsto hx$ est une bijection dont la réciproque est $y \mapsto yx^{-1}$. Ainsi, toutes les classes à droite ont-elles l'ordre de H pour cardinal commun. De la même manière, les *classes à gauche* $xH = \{xh,\ h \in H\}$ ont toutes le même cardinal : $|H|$.
Les classes à gauches sont les classes pour la relation d'équivalence sur G définie par $x \sim y \iff x^{-1}y \in H$ (exercice : c'est une relation d'équivalence ; rappels s'il faut sur relation d'équivalence, classes, partition). Elles forment donc une partition de G. L'ensemble des classes à gauche est noté $(G/H)_g$. Son cardinal est appelé *l'indice*

de H dans G ; on le note $[G : H]$. Exercice : le cardinal de l'ensemble $(G/H)_d$ des classes à droite est aussi $[G : H]$.
Théorème de Lagrange Si G est un groupe fini et si H un sous-groupe de G, alors $|G| = |H| \times [G : H]$. En particulier, $|H|$ divise $|G|$.
Exemple : si $n \geq 1$, on note $\mathbb{U}_n$ le groupe des racines $n^{\text{ième}}$ de l'unité. Il n'y a pas de sous-groupe de $\mathbb{U}_n$ dont l'ordre ne soit un diviseur de n (il n'y a pas de sous-groupe d'ordre 14 de $\mathbb{U}_{352}$).

1.2 Sous-groupe engendré, groupe monogène

Proposition L'intersection d'une famille de sous-groupes est un sous-groupe.
Exemple des matrices inversibles triangulaires inférieures de déteminant égal à 1.
Définition Si A est une partie d'un groupe G, le *sous-groupe engendré par A* est l'intersection des sous-groupes de G contenant A. On le note $\langle A \rangle$. Dans le cas des ensembles finis, on note en général $\langle \{x_1, \ldots, x_n\} \rangle = \langle x_1, \ldots, x_n \rangle$.
Proposition Le sous-groupe de G engendré par la partie A est le plus petit (pour l'inclusion) sous-groupe de G contenant A, *i.e.* si H est n'importe quel sous-groupe, $A \subseteq H \Longrightarrow \langle A \rangle \subseteq H$.
Exercice : traduction de $\langle A \rangle$ en termes de mots formés d'éléments A ou de leurs inverses, à savoir $\langle A \rangle = \{a_1 a_2 \ldots a_n,\ n \in \mathbb{N}^* \text{ et } \forall k \in \{1, \ldots n\},\ a_k \in A \text{ ou } a_k^{-1} \in A\}$.
Exemple (exercice) : démontrer toutes les assertions suivantes. On prend un carré du plan euclidien. L'ensemble $\mathcal{C}^+$ des rotations du plan qui préservent le carré est un sous-groupe du groupe des permutations du carré. Toute rotation de $\mathcal{C}^+$ a pour centre le centre du carré (l'intersection des diagonales), envoie un sommet sur un sommet et est déterminée par l'image d'un seul de ces sommets. Ainsi, $\mathcal{C}^+$ est-il formé de l'identité, des rotations d'angle $\pm\pi/2$ et de la rotation d'angle π (symétrie centrale). En particulier, $\mathcal{C}^+$ est d'ordre 4 et est engendré par la rotation r d'angle $\pi/2$. On note $\mathcal{C}$ le groupe de toutes les isométries qui préservent le carré, qui est constitué, outre des rotations, des symétries axiales qui préservent le carré. Il contient la symétrie axiale s par rapport à une diagonale donnée. Si t est une autre symétrie axiale, alors st^{-1} est une rotation (la composée de deux symétries axiales est une rotation). Ainsi, $\mathcal{C} = \langle r, s \rangle$. Plus précisément, $\mathcal{C}$ contient les 8 isométries suivantes : les 4 rotations de $\mathcal{C}^+$ et les symétries par rapport aux médianes et par rapport aux diagonales du carré.
Exercice : montrer que le groupe des isométries qui préservent un rectangle non carré est d'ordre 4, engendré par les symétries par rapport aux deux médianes.

Définition Un groupe G est *monogène* lorsqu'il existe $x \in G$ tel que $G = \langle x \rangle$. Un groupe monogène et fini est dit *cyclique*.

Le groupe $\mathbb{U}_n$ est cyclique d'ordre n, engendré par $\exp(2i\pi/n)$ (reformulation d'une propriété connue). Le groupe $\mathbb{Z}$ est monogène infini, engendré par 1.
Exercice : le groupe des isométries qui préservent un rectangle non carré n'est pas cyclique.

Rappels d'arithmétique dans $\mathbb{Z}$ et dans $k[X]$: division euclidienne, Bézout, Gauss ou Euclide, unicité de la décomposition en produit de facteurs premiers.

Définition Si x est un élément d'un groupe G, l'*ordre* de x dans G est l'ordre du sous-groupe $\langle x\rangle$; c'est aussi, lorsque c'est un nombre fini, le nombre $\min\{n \in \mathbb{N}^*,\ x^n = 1\}$.

Proposition Si G est un groupe fini, tout élément de G a un ordre fini qui est un diviseur de $|G|$ (preuve avec Lagrange). En particulier, $x^{|G|} = 1$ pour tout $x \in G$.

Exercices. 1- Si x et y commutent dans un groupe et si leurs ordres sont des entiers premiers entre eux, alors l'ordre du produit xy est le produit des ordres.
2- Soient x et y d'ordres finis dans un groupe G, tels que $\langle x\rangle \cap \langle y\rangle = (1)$. Si x et y commutent, alors xy est d'ordre fini égal au ppcm des ordres de x et de y.

Proposition Soit $n \in \mathbb{N}^*$.
1- Si $k \in \mathbb{Z}$, l'ordre de $\exp(2ik\pi/n)$ dans $\mathbb{U}_n$ est $n/\operatorname{pgcd}(n,k)$.
2- Les générateurs de $\mathbb{U}_n$ sont les $\exp(2ik\pi/n)$ où k est premier avec n.

Le nombre de générateurs de $\mathbb{U}_n$ est noté $\varphi(n)$ (fonction d'Euler). Calcul de $\varphi(p)$ pour p nombre premier et des premières valeurs de φ.

Proposition Si $G = \langle x\rangle$ est d'ordre $n \geq 1$, les générateurs de G sont les x^k où k est premier avec n (notation multiplicative), ou les kx où k est premier avec n (notation additive).
Preuve : exercice, adapter la preuve de la proposition précédente.

Proposition Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

Proposition Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{U}_n$ (preuve rendue plus naturelle plus tard avec $\mathbb{Z}/n\mathbb{Z}$).
Preuve : si $G = \langle x\rangle$ est d'ordre n, l'application $\mathbb{U}_n \to G$, $\exp(2ik\pi/n) \mapsto x^k$ est bien définie, est un homomorphisme injectif de groupes, et les cardinaux finis sont égaux.

Proposition Si d est un diviseur de $n \geq 1$, un groupe cyclique $\langle x\rangle$ d'ordre n a un unique sous-groupe d'ordre d : c'est le sous-groupe cyclique $\langle \frac{n}{d}x\rangle$ (notation additive) ou $\langle x^{n/d}\rangle$ (notation multiplicative)
Preuve avec les racines $n^{\text{ième}}$ de l'unité ; le sous-groupe est le groupe des racines $d^{\text{ième}}$ de l'unité. Par isomorphisme, cela suffit.

1.3 Produit direct de groupes

SI G et G' sont deux groupes, la loi de composition interne définie sur le produit cartésien $G \times G'$ par $(x,x').(y,y') = (xy, x'y')$ lui confère une structure de groupe. Le neutre est $(1_G, 1_{G'})$. L'inverse de (x,y) est $(x^{-1}, y^{-1}$.
Définition Si G et G' sont deux groupes, on appelle *groupe produit* $G \times G'$ la loi de groupe définie ci-dessus sur le produit cartésien $G \times G'$.

Exercice : l'application $G \times G' \to G' \times G$, $(x, x') \mapsto (x', x)$ est un isomorphisme de groupes.

Exercice : si $(G_a)_{a\in A}$ est une famille quelconque de groupes, la loi de composition définie par $(x_a)_a.(y_a)_a = (x_a y_a)_a$ sur le produit cartésien $\prod_{a\in A} G_a$ en fait un groupe : le *produit* des groupes G_a. La même loi définit une loi de groupe sur les familles presque nulles : la *somme* des groupes G_a.

Exercice : si f est une permutation de A, les groupes $\prod_A G_a$ et $\prod_A G_{f(a)}$ sont isomorphes.

Exercice : $A\times(B\times C) \to (A\times B)\times C$, $(a,(b,c)) \mapsto ((a,b),c)$ et $A\times B\times C \to A\times(B\times C)$, $(a,b,c) \mapsto (a,(b,c))$ sont des isomorphismes de groupes.

Notation Si G est un groupe et n un entier naturel non nul, on note G^n le groupe produit $G \times G \times \cdots G$ (définition par récurrence).

Exemple de systèmes générateurs de $\mathbb{Z}^2$.
Exercice : (a, b) et (c, d) engendrent $\mathbb{Z}^2$ si, et seulement si leur déterminant dans la base canonique est ± 1 (à relier avec Bézout).

Proposition $\mathbb{Z}^a$ et $\mathbb{Z}^b$ sont isomorphes si, et seulement si $a = b$.
Preuve en prolongeant un isomorphisme en un isomorphisme $\mathbb{Q}$-linéaire entre $\mathbb{Q}^a$ et $\mathbb{Q}^b$ et en utilisant la notion de dimension d'un espace vectoriel. Le prolongement : si $x \in \mathbb{Q}^a$ et si $n \in \mathbb{Z}\setminus\{0\}$ est tel que $nx \in \mathbb{Z}^a$ (il en existe), on pose $f(x) = \frac{1}{n} f(nx)$. Ce prolongement est bien défini car si $nx \in \mathbb{Z}^a$ et $mx \in \mathbb{Z}^a$, alors $mf(nx) = f(mnx) = nf(mx)$. Il est $\mathbb{Q}$-linéaire : soient $x \in \mathbb{Q}^a$ et n et $d \neq 0$ entiers. Soit m entier non nul tel que $m.(\frac{n}{d}x) \in \mathbb{Z}^a$ En particulier, $mnx \in \mathbb{Z}^a$. Alors, $f(\frac{n}{d}x) = \frac{1}{m} f(m\frac{n}{d}x) = \frac{1}{md} f(mnx) = \frac{n}{d} f(x)$ la dernière égalité venant du fait que $mnx \in \mathbb{Z}^a$.

Exemple (chinois non encore dit sur les quotients de $\mathbb{Z}$) : si n et m sont premiers entre eux, $\mathbb{U}_m \times \mathbb{U}_n$ et $\mathbb{U}_{mn}$ sont isomorphes ($\mathbb{U}_m \times \mathbb{U}_n \to \mathbb{U}_{mn}$, $(x, y) \mapsto xy$ est un homomorphisme de groupes, injectif (Bézout) et égalité des cardinaux).

2 $\mathbb{Z}/n\mathbb{Z}$

2.1 Congruences

Définition Soit $n \in \mathbb{Z}$, $n \neq 0$. Deux entiers x et y sont *congrus modulo* n lorsque $x - y$ est un multiple de n. On note $x \equiv y\ [n]$ ou simplement $x = y\ [n]$.

Exercice : 1- $x \equiv y\ [n]$ si, et seulement si x et y ont le même reste dans la division euclidienne par n.
2- La congruence définit une relation d'équivalence sur $\mathbb{Z}$.

Proposition L'addition et la multiplication sont compatibles avec les congruences, *i.e.*pour tous x, x', y, y' entiers, $x \equiv x'\ [n]$ et $y \equiv y'\ [n]$ implique $x + x' \equiv y + y'\ [n]$

et $xx' \equiv yy'$ $[n]$.
Exemples : 1- critère de divisibilité par 3, 9, 11 (et même calcul du reste de la division euclidienne par celui de la somme des chiffres).

2- Soit p un nombre premier. Si $k \in \{1, \dots, p-1\}$, alors p divise $\binom{p}{k}$ (avec le théorème de Gauß). On en déduit que pour tous x et y entiers, $(x+y)^p \sim x^p + y^p$ $[p]$. Par récurrence sur a, on en déduit que pour tout $a \in \mathbb{N}^*$, pour tous x et y entiers, $(x+y)^{p^a} \sim x^{p^a} + y^{p^a}$ $[p]$. On en déduit que p divise $\binom{p^a}{k}$ pour tout $k \in \{1, \dots, p^a - 1\}$ (essayer de démontrer ce résultat sans utiliser la compatibilité de la congruence...).

2.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de la relation de congruence modulo n sur $\mathbb{Z}$.

Autrement dit un élément de $\mathbb{Z}/n\mathbb{Z}$ est une classe d'équivalence pour la relation de congruence modulo n, c'est-à-dire une partie de $\mathbb{Z}$ de la forme $\overline{a} = a + n\mathbb{Z} = \{a + kn,\ k \in \mathbb{Z}\}$.

L'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto x + n\mathbb{Z}$ est surjective. On l'appelle la *projection canonique* ou *surjection canonique*.

Proposition $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ a pour cardinal n. Preuve : l'application $\mathbb{Z}/n\mathbb{Z} \to \{0, \dots, n-1\}$, $\overline{x} \mapsto R(x)$ (reste de la division euclidienne de x par n) est bien définie car tous les éléments d'une même classe modulo n ont le même reste. Elle est bijective car la restriction à $\{0, \dots, n-1\}$ de la projection canonique en est une réciproque.

La compatibilité de $+$ et $\times$ pour la congruence s'écrit encore : pour tous x, x', y, y' entiers, $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ implique $\overline{x+x'} = \overline{y+y'}$ et $\overline{xx'} = \overline{yy'}$. Cela permet de donner du sens aux lois suivantes sur $\mathbb{Z}/n\mathbb{Z}$.
Définition Soit $n \in \mathbb{N}^*$. Pour tous $\overline{x}$ et $\overline{y}$ dans $\mathbb{Z}/n\mathbb{Z}$, on note $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x}\,\overline{y} = \overline{xy}$.

Proposition Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif. Le neutre pour l'addition est $\overline{0}$, l'opposé de $\overline{x}$ est $\overline{-x}$. Le neutre pour la multiplication est $\overline{1}$.
Preuve : exercice (voir le polycopié *Structures abstraites*).

Proposition La projection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un homomorphisme d'anneaux.
Preuve : paraphrase de la définition de $+$ et $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ (compatibilité).

Exemple : dans $\mathbb{Z}/6\mathbb{Z}$, 2 et 3 ne sont pas nuls mais $2 \times 3 = 0$.

Proposition Soit $n \in \mathbb{N}^*$.
1- Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ où k est premier avec n.
2- $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si n est un nombre premier.

Preuve : exercice (Bézout).

2.3 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$

Proposition Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{Z}$.
Preuve : les $n\mathbb{Z}$ sont des sous-groupes (exercice). Si G est un sous-groupe non trivial, soit $n = \min G \cap \mathbb{N}^*$. Le sous-groupe $n\mathbb{Z} = \langle n \rangle$ est inclus dans G. Si $x \in G$, soient q et r le quotient et le reste de la division euclidienne de x par n. Alors $x - nq = r \in G$ avec $0 \leq r \leq n-1$. Par minimalité de n, nécessairement, $r = 0$. Ainsi, $x \in n\mathbb{Z}$. On a montré que $G = n\mathbb{Z}$.

Proposition (Propriété universelle du quotient $\mathbb{Z}/n\mathbb{Z}$)
Soient $n \in \mathbb{N}^*$ et $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection canonique.
1- Si $f : \mathbb{Z} \to G$ est un homomorphisme de groupes dont le noyau est inclus dans $n\mathbb{Z}$, il existe un unique homomorphisme de groupes $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G$ tel que $f = \overline{f} \circ p$.
2- $\overline{f}$ est injectif si, et seulement si $\ker f = n\mathbb{Z}$.
3- $\overline{f}$ est surjectif si, et seulement f est surjectif.
Dessiner un diagramme et dire qu'il commute.
Preuve. Unicité : si $\overline{f}$ existe, elle vérifie $\overline{f}(\overline{x}) = f(x)$. Existence : la formule ci-dessus a du sens dès que $n\mathbb{Z} \subseteq \ker f$ puisque cela entraîne que f est constante sur les classes modulo n. Injectivité : $\ker \overline{f} = p(\ker f)$. Surjectivité : $\operatorname{im} \overline{f} = \operatorname{im} f$.

Exemple : $k \mapsto \exp(2ik\pi/n)$ est un homomorphisme de groupes $(\mathbb{Z}, +) \to (\mathbb{U}_n, \times)$. Son noyau est $n\mathbb{Z}$. Il se factorise donc en un homomorphisme injectif $(\mathbb{Z}/n\mathbb{Z}, +) \to (\mathbb{U}_n, \times)$, qui est un isomorphisme (cardinaux, ou surjectivité dans la PUQ). Cela montre que les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

Proposition Tout groupe cyclique à n éléments est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
Preuve : déjà vu *via* $\mathbb{U}_n$ avec la proposition précédente. Preuve directe (à retenir) : soit $x \in G$ tel que $G = \langle x \rangle$. L'application $k \in \mathbb{Z} \mapsto x^k$ est un homomorphisme de groupes dont le noyau est $n\mathbb{Z}$ puisque l'ordre de x est n. Par la PUQ, il se factorise en un isomorphisme $\mathbb{Z}/n\mathbb{Z} \to G$ (la surjectivité est obtenue là encore de deux manières : dire que x engendre signifie que $k \mapsto x^k$ est surjectif, ou cardinaux).

Proposition Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ où k est premier avec n.
Preuve : déjà vu sur les racines de l'unité. On transporte par l'isomorphisme (un isomorphisme envoie un générateur sur un générateur).

Proposition Soit $n \in \mathbb{N}^*$.
1- Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont tous cycliques, de la forme $\langle \overline{k} \rangle = \mathbb{Z}\overline{k}$, $k \in \mathbb{Z}$.
2- Si $k \in \mathbb{Z}$, alors $\mathbb{Z}\overline{k} = \mathbb{Z}\overline{n \wedge k}$ est d'ordre $\frac{n}{n \wedge k}$.
3- Si $d|n$, alors $\mathbb{Z}/n\mathbb{Z}$ contient un unique sous-groupe d'ordre d : c'est le sous-groupe engendré par la classe de n/d.
Preuve : déjà vu sur les racines de l'unité. Exercice important : faire une preuve directe. L'ingrédient principal est le théorème de Bézout.

En particulier, slogan : *tout sous-groupe d'un groupe monogène est monogène.*

Exercice : montrer que si m et n sont premiers entre eux, les groupes $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes (théorème des restes chinois, déjà énoncé plus haut sur les racines de l'unité).

3 Quotient d'un groupe abélien, structure des GAF

3.1 Quotient d'un groupe abélien

Si G est un groupe abélien et H un sous-groupe de G, les classes à gauche et à droite modulo H coincident. On note G/H l'ensemble quotient pour cette relation d'équivalence commune sur G : $x \sim y \iff xy^{-1} \in H \iff x^{-1}y \in H$. En notation additive, $x \sim y \iff x - y \in H$. On adopte la notation additive dans tout le chapitre. Ainsi, $G/H = \{x + H,\ x \in G\}$. On notera parfois $x + H = \overline{x}$.

Proposition Soient G un groupe additif et H un sous-groupe de G. La loi + sur G/H définie par $\overline{x} + \overline{y} = \overline{x + y}$ a un sens et confère à G/H une structure de groupe commutatif.
Preuve : exo, comme pour $\mathbb{Z}/n\mathbb{Z}$. L'addition dans G est compatible avec la congruence modulo le sous-groupe H.

Proposition La projection canonique $G \to G/H$, $x \mapsto x + H$ est un homomorphisme de groupes.
Preuve : paraphrase de la définition de l'addition dans G/H.

Proposition (Propriété universelle du quotient)
Soit G un groupe abélien, H un sous-groupe de G et $p : G \to G/H$ la projection canonique.
1- Si $f : G \to G'$ est un homomorphisme de groupes dont le noyau contient H, il existe un unique homomorphisme de groupes $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ p$.
2- $\overline{f}$ est injectif si, et seulement si $\ker f = H$.
3- $\overline{f}$ est surjectif si, et seulement si f est surjectif.
Preuve : comme pour $\mathbb{Z}/n\mathbb{Z}$.

Exemple : $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $H = \{(x, y) \in G,\ y = 0\} = \mathbb{Z}/m\mathbb{Z} \times \{0\}$. L'application $G \to \mathbb{Z}/n\mathbb{Z}$, $(x, y) \mapsto x$ est un homomorphisme de groupes surjectif dont le noyau égale H. Il se factorise en l'isomorphisme de groupes $G/H \to \mathbb{Z}/n\mathbb{Z}$, $\overline{(x, y)} \mapsto x$. Le slogan : $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})/\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$.
Exercice : généraliser cela au quotient $(G \times G')/(H \times H') \simeq G/H \times G'/H'$ si les groupes en question sont abéliens.

3.2 Théorème chinois et produits de groupes cycliques

Théorème chinois Si m et n sont des entiers premiers entre eux, alors les groupes

$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomophes.
Preuve : factoriser le produit des projections $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et PUQ. Conclure par l'égalité des cardinaux finis.
Exemple : soit $G = \mathbb{Z}/540\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$. On décompose par le chinois : $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/27 \times \mathbb{Z}/5\mathbb{Z}\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$. On regroupe selon les puissances de nombres premiers et on obtient $G \simeq (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ (décomposition en *composantes primaires* de G). On regroupe selon les plus grandes puissances des nombres premiers, récursivement et on obtient $G \simeq \mathbb{Z}/3.4\mathbb{Z} \times \mathbb{Z}/16.27.5\mathbb{Z} = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2160\mathbb{Z}$, décomposition en *facteurs invariants* (12 divise 2160).

3.3 Structure des GAF

Définition Soient G un groupe abélien et p un nombre premier. La *composante de p-torsion* de G est son sous-groupe $G(p) := \{x \in G,\ \exists a \geq 0,\ x^{p^a} = 1\}$. Autrement dit, $G(p)$ est l'ensemble des éléments de G dont l'ordre est une puissance de p.
Exercice : $G(p)$ est un sous-groupe de G.

Lemme Si G est un groupe abélien fini, G est isomorphe au produit de ses sous-groupes de torsion.
Preuve : Bézout, récurrence sur le nombre de facteurs premiers distincts de $|G|$.

Lemme Si G est un groupe abélien fini dont l'ordre est la puissance d'un nombre premier p, il existe une unique suite finie décroissante d'entiers naturels non nuls $a_1 \geq a_2 \geq \cdots \geq a_r$ telle que G soit isomorphe au produit $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$.
Preuve : Bézout, récurrence sur l'ordre de G.

Théorème (Décomposition en composantes primaires)
Soit G un groupe abélien fini. Il existe une unique suite finie croissante $p_1 \leq p_2 \leq \cdots \leq p_m$ de nombres premiers et, pour chaque $k \in \{1, \ldots, m\}$ une unique suite décroissante d'entiers naturels non nuls $a_{(p_k,1)} \geq a_{(p_k,2)} \geq \cdots \geq a_{(p_k,r_{p_k})}$ telles que G soit isomorphe au produit

$$\left(\mathbb{Z}/p_1^{a_{(p_1,1)}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{a_{(p_1,r_{p_1})}}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_m^{a_{(p_m,1)}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{a_{(p_m,r_{p_m})}}\mathbb{Z}\right).$$

Théorème (Décomposition en facteurs invariants)
Soit G un groupe abélien fini. Il existe une unique suite finie de nombres entiers naturels $(a_1, \ldots, a_n)$ tels que $a_1 | \ldots | a_n$ et tels que G soit isomorphe au produit $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$.

On passe d'une décomposition à l'autre à l'aide du théorème chinois.

[Quotient d'un espace vectoriel par un sous-espace vectoriel, PUQ. Dimension. Pas en 2010, ou plus tard pour réduire les endomorphismes.]

4 Algèbre bilinéaire en dimension finie

4.1 Dualité en dimension finie

Si V est un espace vectoriel sur un corps k, son *dual* est l'espace vectoriel $V^* = \mathcal{L}(V, k)$ des formes linéaires sur V (rappel des lois sur V^*).
Proposition Soient V un espace vectoriel de dimension finie d et $(e_1, \ldots, e_d)$ est une base de V.
1- Le d-uplet de formes linéaires $(e_1^*, \ldots, e_d^*)$ définies par

$$\forall (j,k) \in \{1, \ldots, d\}^2,\ e_j^*(e_k) = \delta_{j,k}$$

(Kronecker) est une base de V^*.
2- Si $f \in V^*$, on a la formule

$$f = \sum_{k=1}^{d} f(e_k) e_k^*.$$

Preuve : les formules de 1- définissent une famille de formes linéaires puisque toute forme linéaire est déterminée par l'image d'une base. La formule 2- est vraie car les formes linéaires à droite et à gauche de l'égalité coincident sur la base $(e_1, \ldots, e_d)$: la famille est génératrice. Enfin, si $\sum_k a_k e_k^* = 0$, alors pour chaque k, prendre la valeur en e_k montre que $a_k = 0$: la famille est libre.
Définition La base $(e_1^*, \ldots, e_d^*)$ de V^* est appelée *base duale* de la base $(e_1, \ldots, e_d)$. La formule 2- de la proposition donne les coordonnées d'une forme linéaire f dans la base duale.
Corollaire Si V est de dimension finie, alors V et V^* ont la même dimension (et sont donc des espaces vectoriels isomorphes).
Exercice : les coordonnées d'un vecteur $v \in V$ dans la base $(e_1, \ldots, e_d)$ s'écrivent

$$v = \sum_{k=1}^{d} e_k^*(v) e_k.$$

Cette formule et la formule 2- de la proposition sont "duales".
Proposition Si V est un espace vectoriel de dimension finie, l'application linéaire $\delta : V \to V^{**} = (V^*)^*$, définie par $\delta(v)(f) = f(v)$ pour tout $v \in V$ et pour toute $f \in V^*$, est un isomorphisme.
Preuve : elle est linéaire. On prend une base $(e_1, \ldots, e_d)$ de V et sa base duale $(e_1^*, \ldots, e_d^*)$. Dire que $v \in \ker \delta$ signifie que $\delta(v)(e_k^*) = e_k^*(v) = 0$ pour tout k. Comme ces nombres sont les coordonnées de v dans la base $(e_1, \ldots, e_d)$, cela signifie que $v = 0$.

Raisonnement *par orthogonalité* : en dimension d, un vecteur est nul si, et seulement si ses images par une famille de d formes linéaires indépendantes sont toutes nulles (*i.e.* ssi son image par δ est nulle).

Exemple de raisonnement par orthogonalité : on note $\mathbb{R}_d[X]$ l'espace des polynômes à coefficients réels de degré au plus d. Si $f \in \mathbb{R}_d[X]$ est tel que $\int_0^{+\infty} f(x)x^k e^{-x^2}dx = 0$ pour tout $k \in \{0,\dots,d\}$, alors $f = 0$. En effet, pour chaque k, $l_k : g \mapsto \int_0^{+\infty} g(x)x^k e^{-x^2}dx$ est une forme linéaire (bien définie) sur l'espace vectoriel réel $\mathbb{R}_d[X]$ de dimension finie $d+1$. Ces $d+1$ formes linéaires sont indépendantes car $\sum_{k=0}^d a_k l_k = 0$ signifie que $\int_0^{+\infty} f(x)(\sum_{k=0}^d a_k x^k)e^{-x^2}dx = 0$ pour tout $f \in \mathbb{R}_d[X]$; en particulier, $\int_0^{+\infty}(\sum_{k=0}^d a_k x^k)^2 e^{-x^2}dx = 0$ ce qui implique par positivité et continuité que les a_k sont tous nuls. Comme f annule $d+1$ formes linéaires indépendantes, $f = 0$.

Notation, crochet de dualité. Si $v \in V$ et $f \in V^*$, on note $f(v) = \langle v, f\rangle$. Les formules duales s'écrivent alors $v = \sum\langle v, e_k^*\rangle e_k$ et $f = \sum\langle e_k, f\rangle e_k^*$.

4.2 Formes bilinéaires

Définition Une *forme bilinéaire* sur un k-espace vectoriel V est une application $f : V \times V \to k$ telle que pour tout $v \in V$, les applications $f(v,.) : V \to k$, $w \mapsto f(v,w)$ et $f(.,v) : V \to k$, $w \mapsto f(w,v)$ sont des formes linéaires.
En d'autres termes, $f(x+y,z) = f(x,z) + f(y,z)$, $f(ax,y) = af(x,y)$, $f(x,y+z) = f(x,y) + f(x,z)$, $f(x,ay) = af(x,y)$ pour tout $a \in k$ et pour tous x, y, z dans V.
Exemples pour $V = \mathbb{R}^2$: $f((x_1,x_2),(y_1,y_2)) = 2x_1y_1 - \pi x_1y_2 + x_2y_2$ est bilinéaire. $g((x_1,x_2),(y_1,y_2)) = x_1x_2$ ne l'est pas. Sur l'espace des polynômes à coefficents réels, $(f,g) \mapsto \int_{-\infty}^{+\infty} f(t)g(t)e^{-t^2}dt$ est une forme bilinéaire.
Exercice : l'ensemble des formes bilinéaires sur V est un sous-espace vectoriel de l'espace des fonctions $V^2 \to k$ pour les lois usuelles.
On note $\mathcal{L}_2(V)$ l'espace des formes bilinéaires sur V.

Proposition Toute forme bilinéaire est déterminée par l'image des couples de vecteurs d'une base. Plus précisément, en dimension finie d, si $(e_1,\dots,e_d)$ est une base de V et si $f \in \mathcal{L}_2(V)$,

$$f(x,y) = \sum_{(j,k)\in\{1,\dots,d\}^2} x_j y_k f(e_j,e_k)$$

pour tous $x = \sum_{k=1}^d x_k e_k$ et $y = \sum_{k=1}^d y_k e_k$.
Preuve : bilinéarité.

Représentation matricielle.
Si $A \in \mathcal{M}_d(k)$ est une matrice carrée, l'application définie sur le carré de l'espace vectoriel $\mathcal{M}_{d,1}(k)$ des vecteurs-colonne à coefficients dans k par

$$\begin{array}{ccc} \mathcal{M}_{d,1}(k)\times\mathcal{M}_{d,1}(k) & \to & k \\ (X,Y) & \mapsto & {}^tXAY \end{array}$$

est bilinéaire (exercice, "associativité" du produit matriciel). Si E_k désigne le $k^{\text{ième}}$ vecteur de la base canonique de $\mathcal{M}_{d,1}(k)$ et si $A = (a_{i,j})_{1\le i,j\le d}$, alors pour tout

couple (i,j), on a $a_{i,j} = {}^tE_iAE_j$. Preuve : exercice, double application de la formule générale du produit de deux matrices (rectangulaires) : $(PQ)_{i,j} = \sum_k p_{i,k}q_{k,j}$.
Inversement, soit f une forme bilinéaire sur un espace vectoriel V de dimension finie d. On fixe une base $\mathcal{B} = (e_1, \ldots, e_d)$ de V et on note $A = (a_{i,j})_{i,j} \in \mathcal{M}_d(k)$ la matrice carrée définie par

$$\forall (i,j),\ a_{i,j} = f(e_i, e_j).$$

Alors, si X et Y sont les vectuers-colonne des coordonnées de $x \in V$ et $y \in V$ dans le base $\mathcal{B}$, l'image $f(x,y)$ se calcule à l'aide de la formule $f(x,y) = {}^tXAY$. On dit que A est la *matrice de f dans la base $\mathcal{B}$* et on note $A = \mathrm{Mat}_{\mathcal{B}}(f)$.

Proposition Si V est un k-espace vectoriel de dimension finie d et si $\mathcal{B}$ est une base de V, l'application $\mathcal{L}_2(V) \to \mathcal{M}_d(k)$, $f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$ est un isomorphisme d'espaces vectoriels. En particulier, $\dim_k \mathcal{L}_2(V) = d^2$.
Preuve : elle est linéaire (exercice). Elle est surjective (toute forme bilinéaire se représente par une matrice, étude ci-dessus) ; elle est injective (les coefficient de la matrice sont les images des couples des vecteurs de la base, on utilise la première proposition du paragraphe).

Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases d'une même espace vectoriel V, la *matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$* est la matrice dont le $k^{\text{ième}}$ vecteur-colonne est le vecteur-colonne des coordonnées du $k^{\text{ième}}$ vecteur de $\mathcal{B}'$ dans la base $\mathcal{B}$, pour tout k. Autrement dit, c'est $\mathrm{Mat}_{\mathcal{B}',\mathcal{B}}(\mathrm{id}_V)$.
Proposition (matrice et changement de base) Soient f une forme bilinéaire sur un espace vectoriel V de dimension finie, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de V. On note $A = \mathrm{Mat}_{\mathcal{B}}(f)$ et $A' = \mathrm{Mat}_{\mathcal{B}'}(f)$. On note enfin P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Alors, $A' = {}^tPAP$.
Preuve. On note $\mathcal{B} = (e_1, \ldots, e_d)$, $\mathcal{B}' = (e'_1, \ldots, e'_d)$ et $P = (p_{i,j})_{1 \leq i,j \leq d}$. Par définition de P, on a $e'_k = \sum_{j=1}^d p_{j,k}e_j$, pour tout k. Alors, pour tout couple (p,q), $f(e'_p, e'_q) = \sum_{i,j} p_{i,p}p_{j,p}f(e_i, e_j) = \sum_i p_{i,p}(\sum_j f(e_i, e_j)p_{j,p})$ qui est la formule attendue. Autre preuve : soient x et y deux vecteurs de V ; on note X et Y les vecteurs-colonne de leurs coordonnées dans $\mathcal{B}$ et X' et Y' les vecteurs-colonne de leurs coordonnées dans $\mathcal{B}'$. Alors, $X = PX'$ et $Y = PY'$, ce qui entraîne que $f(x,y) = {}^tXAY = {}^tX'({}^tPAP)Y' = {}^tX'A'Y'$. La dernière égalité, vraie pour tous les vecteurs-colonne X' et Y', implique le résultat.
Définition et slogan : on dit que deux matrices A et B sont *congruentes* lorsqu'il existe une matrice inversible P telle que $B = {}^tPAP$. Exercice : cela définit une relation d'équivalence sur les matrices carrées de dimension données. Le slogan : pour les formes bilinéaires, changer de base revient à transformer la matrice en une matrice congruente.

4.3 Formes bilinéaires symétriques et formes quadratiques

Définition Une forme bilinéaire f sur un espace vectoriel V est *symétrique* lorsque $f(x,y) = f(y,x)$ pour tous x et y dans V.

Proposition Soit V un espace vectoriel et f une forme bilinéaire sur V.
1- f est symétrique si, et seulement s'il existe une base de V dans laquelle la matrice de f est symétrique.
2- f est symétrique si, et seulement si la matrice de f est symétrique dans n'importe quelle base de V.
Preuve : exercice.
Autrement dit, les formes bilinéaires symétriques sont les formes bilinéaires représentées par les matrices symétriques.

Les formes bilinéaires symétriques sur V forment un sous-espace vectoriel de $\mathcal{L}_2(V)$ que l'on notera $\mathcal{S}_2(V)$. Si V est de dimension d finie, à partir du choix d'une base de V et de la représentation matricielle des formes bilinéaires, on obtient que $\dim_k \mathcal{S}_2(V) = d(d+1)/2$.
Exemples de formes bilinéaires symétriques sur k^2 : $f((x,y),(x',y')) = xx' + yy'$ (produit scalaire usuel) ; $f((x,y),(x',y')) = 2xx'$; $f((x,y),(x',y')) = 4xx' - yy'$; $f((x,y),(x',y')) = xy' + yx'$.

Définition Un polynôme de $k[X_1, \ldots, X_d]$ est dit *homogène de degré* $p \in \mathbb{N}$ lorsqu'il est la somme de monômes de degré p.
Exercice : si un polynôme P est homogène de degré p alors pour tout $a \in k$, $P(aX_1, \ldots aX_d) = a^p P(X_1, \ldots X_d)$. Sur $\mathbb{C}$ ou sur un de ses sous-corps, la propriété est équivalente. Pourquoi cette restriction sur le corps ?
Proposition On suppose que k est un sous-corps de $\mathbb{C}$ (ou, plus généralement, un corps de caractéristique différente de 2). Soient V un k-espace vectoriel de dimension finie et $q : V \to k$ une application. Il y a équivalence entre :
1- il existe $b \in \mathcal{S}_2(V)$ telle que $q(x) = b(x,x)$ pour tout $x \in V$;
2- il existe une base $\mathcal{B}$ de V telle que pour tout $x \in V$, $q(x)$ est un polynôme homogène de degré 2 en les coordonnées de x dans $\mathcal{B}$;
3- pour toute base $\mathcal{B}$ de V, pour tout $x \in V$, $q(x)$ est un polynôme homogène de degré 2 en les coordonnées de x dans $\mathcal{B}$.
NB : 2- et 3- restent équivalentes et impliquées par 1- si k est un corps de caractéristique 2.
Preuve : (1⇒3) : $q(x) = {}^tXAX = \sum a_{i,j} x_i x_j$ est un polynôme homogène de degré 2 en les x_i. (3⇒2) est trivial. (2⇒1) : par linéarité, il suffit de le montrer si q est un monôme de degé 2. Quitte à permuter les coordonnées, il suffit de le montrer lorsque $q(x) = x_1^2$ et lorsque $q(x) = x_1 x_2$ où x_1 et x_2 désignent les coordonnées de x. Dans le premier cas, prendre $b(x,y) = x_1 y_1$, dans le second prendre $b(x,y) = \frac{1}{2}(x_1 y_2 + x_2 y_1)$.
Définition On suppose que k est un sous-corps de $\mathbb{C}$ (ou, plus généralement, un corps de caractéristique différente de 2). Une *forme quadratique* sur un k-espace vectoriel V est une application qui vérifie les assertions équivalentes de la proposition précédente.
Si q est une forme quadratique, la forme bilinéaire symétrique $b \in \mathcal{S}_2(V)$ telle que $q(x) = b(x,x)$ pour tout vecteur x est appelée *forme polaire* de q.
Proposition La forme polaire d'une forme quadratique q s'exprime par les formules $b(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$.

Preuve : le voir si q est un monôme x_1^2 ou x_1x_2 dans une base suffit.

L'ensemble des formes quadratiques sur V est un sous-espace vectoriel de l'espace des fonctions de V dans k. On le note $\mathcal{Q}(V)$.
Proposition Si V est un espace vectoriel de dimension finie sur un corps de caractéristique différente de 2, l'application $\mathcal{S}_2(V) \to \mathcal{Q}(V)$ qui à une forme bilinéaire symétrique associe sa forme polaire est un isomorphisme d'espaces vectoriels.
En particulier, si $\dim_k V = d$, alors $\dim_k \mathcal{Q}(V) = d(d+1)/2$.

Exemples de formes quadratiques : $f(x_1, \dots x_d) = x_1^2 + \cdots + x_d^2$ sur $\mathbb{R}^d$ (norme euclidienne standard), $f(x, y, z, t) = x^2 + y^2 + z^2 - c^2t^2$ sur $\mathbb{R}^4$ (forme de Lorentz), $f(x, y, z) = x(y + z - x)$ sur k^3, $f(x, y, z) = yz$ sur k^3. Exercice : calculer les formes poliares de ces exemples (loi de dédoublement).

Réduction des formes quadratiques.
Le choix d'une base $(e_1, \dots, e_d)$ de V étant fait, la matrice diagonale $\mathrm{diag}(a_1, \dots, a_d)$ représente la forme quadratique $q(x) = \sum_i a_i x_i^2$ (les x_i sont les coordonnées de x).
En particulier, si b est la forme polaire de q, alors $i \neq j \Longrightarrow b(e_i, e_j) = 0$.
Définition Si $b \in \mathcal{S}_2(V)$, deux vecteurs x et y de V sont dits *orthogonaux* lorsque $b(x, y) = 0$. Une base de V formée de vecteurs deux à deux orthogonaux est dite *orthogonale*. On utilise le même vocabulaire pour une forme quadratique en considérant sa forme polaire (en caractéristique différente de 2).
Réduire une forme quadratique signifie en chercher une base orthogonale ou, de manière équivalente, trouver une base dans laquelle sa matrice soit diagonale.

4.4 Noyau et rang d'une forme quadratique

Définition Le *noyau* d'une forme quadratique $q \in \mathcal{Q}(V)$ ou de sa forme polaire $b \in \mathcal{S}_2(V)$ est le noyau de l'application linéaire $V \to V^*$, $v \mapsto b(v, .) = b(., v)$. On le note $N(q) = N(b)$. Le *rang* d'une forme quadratique (ou de sa forme polaire) est la codimension de son noyau.
Autrement dit, $x \in N(q)$ si, et seulement si x est orthogonal à tous les vecteurs de E.
Exemple : sur $\mathbb{C}^3$, le noyau de $q(x, y, z) = x(x + z)$ est la droite $\mathbb{C}(0, 1, 0)$. Cela se voit en calculant la forme polaire : $b((x, y, z), (x', y', z')) = xx' + \frac{1}{2}(xz' + x'z)$. La forme est donc de rang 2.

[**Définition** Un vecteur est dit *isotrope* lorsqu'il est orthogonal à lui-même, *i.e.* lorsqu'il annule la forme quadratique. Exercice : si x est isotrope, alors tous les ax le sont, $a \in k$ (on parle du *cône isotrope*). Tout vecteur du noyau est isotrope, la réciproque est fausse. Exemple : pour la forme précédente, $(1, 2, -1)$ est un vecteur isotrope qui n'est pas dans le noyau.]

Définition Une forme quadratique est *non dégénérée* lorque son noyau est nul. Sinon, on dit qu'elle est *dégénérée*.

Exemple de forme quadratique non dégénérée : le *produit scalaire standard* sur k^d,

défini par $q(x_1, \dots, x_d) = \sum_{n=1}^{d} x_n^2$. Preuve de la non dégénérescence : la forme polaire est $b(x, y) = \sum_n x_n y_n$. Si x est tel que $b(x, y) = 0$ pour tout y, en prenant successivement pour y les vecteurs de la base canonique, on montre que $x = 0$. De la même manière, si $a_1, \dots a_d$ sont tous non nuls, la forme quadratique $\sum_{n=1}^{d} a_n x_n^2$ est non dégénérée sur k^d.

Proposition (théorème de représentation des formes linéaires) Soient V un k-espace vectoriel de dimension finie d et $\langle \cdot, \cdot \rangle$ une forme bilinéaire symétrique non dégénérée. Alors, l'application $V \to V^*$, $x \mapsto \langle x, \cdot \rangle$ est linéaire et bijective.
Si $f \in V^*$, on dit que l'unique vecteur x tel que $f = \langle x, \cdot \rangle$ *représente* f.
Preuve. La linéarité est évidente. L'injectivité vient de la non dégénérescence. On conclut avec l'égalité des dimensions.
Exemple du gradient (sonder avant pour savoir si les étudiants connaissent la différentielle et le gradient).

Proposition (théorème de représentation des formes bilinéaires) Soient V un k-espace vectoriel de dimension finie d et $\langle \cdot, \cdot \rangle$ une forme bilinéaire symétrique non dégénérée. Alors, l'application $\mathrm{End}_k(V) \to \mathcal{L}_2(V)$, $f \mapsto \langle \cdot, f(\cdot) \rangle$ est linéaire et bijective.
Si $b \in \mathcal{L}_2(V)$, on dit que l'unique $f \in \mathrm{End}(V)$ tel que $b = \langle \cdot, f(\cdot) \rangle$ *représente* b.
Preuve. La linéarité est évidente. L'injectivité vient de la non dégénérescence. On conclut avec l'égalité des dimensions.

4.5 Algorithme de Gauß

Le corps k est dans cette section un sous-corps de $\mathbb{C}$ (ou un corps de caractéristique nulle).
L'algorithme de Gauß est un algorithme de réduction des formes quadratiques. Il est basé sur les deux identités polynomiales $X^2 + 2XY = (X + Y)^2 - Y^2$ (début du développement d'un carré) et $4XY = (X+Y)^2-(X-Y)^2$ (compensation des carrés). Il s'agit d'écrire une forme quadratique donnée sur k^d sous la forme d'une combinaison linéaire de carrés de formes linéaires indépendantes.

Deux exemples sur k^3 ($\mathrm{car}\, k \neq 2$). 1- $f(x, y, z) = 5xy + y^2 - 2xz - yz = (y + \frac{1}{2}(5x - z))^2 - \frac{1}{4}(5x - z)^2 - 2xz = l_1^2 - \frac{25}{4}x^2 + \frac{1}{2}xz - \frac{1}{4}z^2 = l_1^2 - \frac{25}{4}(x^2 - \frac{2}{25}xz) - \frac{1}{4}z^2 = l_1^2 - \frac{25}{4}(x - \frac{1}{25}z)^2 + \frac{13}{50}z^2 = l_1^2 - \frac{25}{4}l_2^2 + \frac{13}{50}l_3^2$ où l_1, l_2 et l_3 sont des formes linéaires indépendantes (les variables sont échelonnées). La morale : quand on peut isoler le carré d'une variable, on fait apparaître le début du développement d'un carré qui épuise la dite variable.
2- $f(x, y, z) = xy+2xz-3yz = (x-3z)(y+2z)+6z^2 = \frac{1}{4}(x+y-z)^2-\frac{1}{4}(x-y-5z)^2+6z^2$ qui est combinaison linéaire de carré de formes linéaires indépendantes (exercice : elles sont indépendantes). La morale : quand n'apparaissent que des termes rectangles, on isole *deux* variables simultanément et on les épuise par la formule $xy + Ax + By = (x + B)(y + A) - AB$.

Ces deux techniques appliquées récursivement consistent en l'algorithme de Gauss qui permet, en isolant successivement les variables une par une ou deux par deux, d'exprimer toute forme quadratique sur k^d comme combinaison linéaire de carrés de formes linéaires indépendantes.

Théorème (Algorithme de gauß) Si k est un sous-corps de $\mathbb{C}$ et $d \in \mathbb{N}^*$, toute forme quadratique sur k^d est une combinaison linéaire de carrés de formes linéaires indépendantes.
Preuve : on procède par récurrence sur d, comme dans les exemples ci-dessus qui ont valeur génériques. Pour l'indépendance des formes linéaires obtenues, on évoque l'échelonnement des variables et le fait que si l et m sont deux formes indépendantes, alors $l+m$ et $l-m$ le sont aussi.

Commentaire sur les choix dans l'algorithme et la non unicité des la décomposition.

Théorème Soit q une forme quadratique. Si q est combinaison linéaire de r carrés de formes linéaires indépendantes, alors $r = \mathrm{rg}(q)$.
Ainsi l'algorithme de Gauß permet-il de calculer le rang d'une forme quadratique. En particulier, même si la décomposition en carré n'est pas (du tout) unique, le nombre de formes qui apparaissent, lui, est toujours le même.
Preuve. On note b la forme polaire de q. On suppose que $q = \sum_{n=1}^{r} a_n l_n^2$ où les l_n sont des formes linéaires indépendantes. On complète en une base $(l_1, \ldots, l_d)$ de V^* et on note $(e_1, \ldots, e_d)$ sa base duale de vecteurs de V. Alors, $b(x,y) = \sum_{n=1}^{r} a_n l_n(x) l_n(y)$ pour tous x et y de V (c'est clair, prendre la diagonale). On en déduit que $b(e_n, \cdot) = l_n$ si $1 \leq n \leq r$ et $b(e_n, \cdot) = 0$ si $r+1 \leq n \leq d$. Cela montre que l'image de $V \to V^*$, $v \mapsto b(v, \cdot)$ contient $l_1, \ldots, l_d$ et que son noyau contient $e_{r+1}, \ldots, e_d$, et donc ainsi que $r = \mathrm{rg}\, q$.

Exercice. Autre interprétation du rang, plus intrinsèque : $\mathrm{rg}\, q$ est le plus grand entier n tel qu'il existe un sous-espace de V de dimension n sur lequel q soit non dégénérée.

Exercice. Matrice de Gram dans une base : $(b(e_i, e_j))_{i,j}$. Le rang de b est le rang de la matrice de Gram.

4.6 Formes quadratiques réelles

Dans ce paragraphe, le corps de base est $\mathbb{R}$.
Définition Une forme quadratique q sur V (ou sa forme polaire b) est dite *positive* lorsque $q(x) \geq 0$ pour tout vecteur x. *Idem* pour *négative*. La forme q est dite *définie positive* lorsqu'elle est positive et lorsque $\forall x \in V$, $(q(x) = 0) \Rightarrow (x = 0)$. *Idem* pour *définie négative*.
Vocabulaire : une forme bilinéaire symétrique définie positive est un *produit scalaire*.

Exercice. Une forme est définie positive si, et seulement si elle est à la fois positive et non dégénérée.

Théorème d'inertie de Sylvester Soit Q une forme quadratique réelle. Si Q se décompose sous la forme

$$Q = \sum_{k=1}^{p} l_k^2 - \sum_{k=p+1}^{p+q} l_k^2$$

où les l_k sont des formes linéaires indépendantes, alors p est la dimension maximale d'un sous-espace sur lequel la restriction de Q est définie positive, q est la dimension maximale d'un sous-espace sur lequel la restriction de Q est définie négative et $\operatorname{rg} Q = p + q$.
En particulier, les nombres p et q de nombres de coefficients positifs (*resp.* négatifs) dans les décompositions de Q en combinaisons linéaires de carrés de formes linéaires indépendantes sont invariants (sont les mêmes pour toutes les décompositions).
Preuve. On complète les l_k en une base $(l_1, \dots, l_d)$ de V^*. On note E_+ le sous-espace d'équations $l_k = 0,\ k \geq p+1$. On note E_- le sous-espace d'équations $l_k = 0,\ k \notin \{p+1, \dots, p+q\}$. On note E_0 le sous-espace d'équations $l_k = 0,\ k \leq p+q$. La restriction de Q à E_+ est définie positive, celle à E_- est définie négative. Si la restriction de Q à un sous-espace W de V est définie positive, alors W et $E_- \oplus E_0$ sont en somme directe (c'est clair) et donc $\dim W \leq p = \dim E_+$. *Idem* pour l'interprétation de q. Assertion sur le rang : déjà vue au théorème précédent.

Définition Le couple (p, q) est appelé la *signature* de la forme quadratique Q (ou de sa forme polaire).

Remarque. Il est faux de dire que V a un sous-espace maximum (pour l'inclusion) sur lequel Q est définie positive. En effet, si $Q(x, y) = x^2 - y^2$, sa signature est $(1, 1)$ et la restriction de Q aux droites respectivement engendrée par $(1, 0)$ et $(2, 1)$ est définie négative. Autre exemple (essentiellement le même) : la forme quadratique xy sur $\mathbb{R}^2$ a pour signature $(1, 1)$ mais sa restriction à toute droite d'équation $y = ax$, $a > 0$ est définie positive.

[Pas en 2010 : orthonormalisation de Gram-Schmidt, classifier les formes quadratiqus par la signature sur $\mathbb{R}$ et par le rang sur $\mathbb{C}$. Application aux coniques affines. Groupes orthogonaux (matrices, endomorphismes).]

5 Quotients d'anneaux de polynômes à une variable

Quotient d'un anneau commutatif par un idéal. PUQ.
Exemple des polynômes d'une variable sur un corps (arithmétique).

6 Réduction des endomorphismes

Les espaces vectoriels considérés sont de dimension finie.

6.1 Polynômes d'endomorphismes

Définition Si a est un endomorphisme d'un k-espace vectoriel V et si $P = \sum_n p_n X^n \in k[X]$, on note $P(a)$ l'endomorphisme $\sum_n p_n a^n$, avec la convention $a^0 = \mathrm{id}_V$. On dit que $P(a)$ est un *polynôme en a*. Même définition pour les polynômes en une matrice carrée.

Exercices. 1- Si A est la matrice d'un endomorphisme a dans une base $\mathcal{B}$ et si P est un polynôme, alors $P(A)$ est la matrice de $P(a)$ dans la base $\mathcal{B}$.
2-Si a est un endomorphisme et si P et Q sont des polynômes, les endomorphismes $P(a)$ et $Q(a)$ commutent. *Idem* pour les matrices.

Théorème de Cayley Hamilton Si a est un endomorphisme d'un espace vectoriel de dimension finie et si χ_a est son polynôme caractéristique, alors $\chi_a(a)$ est l'endomorphisme nul.
[Pas de preuve, c'est un rappel.]

6.2 Sous-espaces caractéristiques d'un endomorphisme

Soient a un endomorphisme d'un espace vectoriel V et $\mathrm{Sp}(a)$ l'ensemble de ses valeurs propres (son *spectre*). *On suppose que le polynôme caractéristique de a est scindé* et on le note $\chi_A = \prod_{\lambda \in \mathrm{Sp}(a)} (X - \lambda)^{m_\lambda}$.
Remarque : sur $\mathbb{C}$, les polynômes sont tous scindés.
Définition Si λ est une valeur propre de a (ou même n'importe quel nombre de k), le *sous-espace caractéristique* de a associé à la valeur propre λ est le sous-espace vectoriel $\ker(a - \lambda \,\mathrm{id}_v)^{m_\lambda}$.

Exemple. Sous-espaces caractéristiques et sous-espaces propres de l'endomorphisme de $\mathbb{R}^3$ représenté dans la base canonique par la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

Exercice. Si $a \in \mathrm{End}(V)$, la suite

$$\ker(a - \lambda \,\mathrm{id}_V) \subseteq \ker(a - \lambda \,\mathrm{id}_V)^2 \subseteq \ker(a - \lambda \,\mathrm{id}_V)^3 \subseteq \dots$$

est croissante est stationnaire, égale au sous-espace caractéristique associé à λ à partir d'un certain rang. En particulier, tout sous-espace caractéristique contient le sous-espace propre associé à la même valeur propre.

Notations. Pour tout $\lambda \in \mathrm{Sp}(a)$, on note P_λ le polynôme défini par

$$P_\lambda = \frac{\chi_a}{(X - \lambda)^{m_\lambda}} = \prod_{\mu \in \mathrm{Sp}(a) \setminus \{\lambda\}} (X - \mu)^{m_\mu}.$$

Ces polynômes sont premiers entre eux dans leur ensemble. On choisit une relation

de Bézout, c'est-à-dire des polynômes Q_λ tels que

$$1 = \sum_{\lambda \in \mathrm{Sp}(a)} P_\lambda Q_\lambda.$$

[Cela est possible grâce à la division euclidienne dans $k[X]$ qui en fait un anneau principal, voir le cours d'arithmétique de première année.] En particulier, en spécialisant ces polynômes en a, on obtient que

$$\mathrm{id}_V = \sum_{\lambda \in \mathrm{Sp}(a)} P_\lambda(a) \circ Q_\lambda(a) = \sum_{\lambda \in \mathrm{Sp}(a)} Q_\lambda(a) \circ P_\lambda(a).$$

Lemme Soit $a \in \mathrm{End}(V)$ dont le polynôme caractéristique est scindé. Pour toute $\lambda \in \mathrm{Sp}(a)$, on note V_λ le sous-espace caractéristique associé à λ.
1- V_λ est stable par a et $V = \bigoplus_{\lambda \in \mathrm{Sp}(a)} V_\lambda$.
2- $p_\lambda = Q_\lambda(a) \circ P_\lambda(a)$ est la projection sur le sous-espace V_λ relativement à la somme directe de 1- (en particulier, ces projections commutent).
3- Pour tous $\lambda, \mu \in \mathrm{Sp}(a)$, $p_\lambda^2 = p_\lambda$ et $(\lambda \neq \mu \Longrightarrow p_\lambda \circ p_\mu = 0)$.

Remarque : ce qu'il faut retenir, notamment, c'est que les sous-espaces caractéristiques sont supplémentaires et que les projections sont des polynômes en a.

Preuve du lemme. Si $x \in V_\lambda$, $(a - \lambda \,\mathrm{id}_v)^{m_\lambda}(ax) = a((a - \lambda \,\mathrm{id}_v)^{m_\lambda}(x)) = 0$, ce qui montre que V_λ est a-stable. Pour tout $y \in V$ et pour tout λ, $P_\lambda(a)(y) \in V_\lambda$ à cause du théorème de Cayley-Hamilton. Cela montre que tout vecteur $x = \sum_\lambda P_\lambda(a)[Q_\lambda(a)(x)]$ se décompose dans la somme des V_λ. Par ailleurs, si $\lambda, \mu \in \mathrm{Sp}(a)$ sont distincts et si $x \in V_\mu$, alors $P_\lambda(a)(x) = 0$. En particulier, si $x \in V_\lambda$, la décomposition ci-dessus, qui s'écrit aussi $x = \sum_\lambda Q_\lambda(a)[P_\lambda(a)(x)]$, fournit $x = Q_\lambda(a) \circ P_\lambda(a)(x)$. Ainsi, si des vecteurs $x_\lambda \in V_\lambda$ vérifient $\sum_\lambda x_\lambda = 0$, alors pour tout λ, $0 = Q_\lambda(a) \circ P_\lambda(a)(0) = Q_\lambda(a) \circ P_\lambda(a)(x_\lambda) = x_\lambda$. On a prouvé le 1-. On a aussi prouvé le 2- en écrivant la décomposition $x = \sum_\lambda (P_\lambda Q_\lambda)(a)(x)$. Le 3- est une propriété générale des projections relatives à une décomposition en sous-espaces supplémentaires.

Exercice. La restriction d'un endomorphisme à un de ses sous-espaces caractéristiques V_λ admet λ pour unique valeur propre.

6.3 Réduction des endomorphismes, décomposition $D + N$

Définition Un endomorphisme a est *nilpotent* lorsqu'il existe une entier naturel m tel que $a^m = 0$. Le plus petit entier ν tel que $a^\nu = 0$ est l'*indice* de a. Même vocabulaire pour une matrice carrée.
Exercice : les matrices triangulaires avec des 0 sur la diagonale sont nilpotentes. Si a est nilpotent, son polynôme caractéristique est $X^{\dim V}$. Comme ce polynôme caractéristique est scindé, cela montre, par trigonalisation, que a admet une matrice

triangulaire à diagonale nulle dans une base *ad hoc*. Inversement, si un endomorphisme a dont le polynôme caractéristique est scindé n'a que 0 comme valeur propre (*i.e.* égale $X^{\dim V}$), alors a est nilpotent.

Si a a une unique valeur propre λ, alors $a - \lambda \,\mathrm{id}_V$ est un endomorphisme nilpotent. Autrement dit, a est la somme $a = \lambda \,\mathrm{id}_V + n$ d'une homothétie et d'un nilpotent (qui commutent puisque les homothéties sont centrales). Cela se généralise au cas général de la façon suivante.

Théorème Soit a un endomorphisme d'un espace vectoriel de dimension finie, dont le polynôme caractéristique est scindé. Alors, il existe deux endomorphismes d et n tels que :
1- d est diagonalisable ;
2- n est nilpotent ;
3- n et d sont des polynômes en a (et donc commutent) ;
4- $a = d + n$.
Preuve. Avec les notations du paragraphe précédent, soit $d = \sum_{\lambda \in \mathrm{Sp}(a)} \lambda p_\lambda$, polynôme en a. Si $x \in V_\lambda$, alors $d(x) = \lambda p_\lambda(x) = \lambda x$, ce qui montre que les V_λ sont des espaces propres pour d. Comme ils sont supplémentaires, cela montre que d est diagonalisable. Soit $n = a - d$, polynôme en a. Si $x \in V_\lambda$, alors $n^{m_\lambda}(x) = (a - \lambda \,\mathrm{id}_V)^{m_\lambda} = 0$ ce qui montre que n est nilpotent, d'indice inférieur ou égal à $\max\{m_\lambda,\ \lambda \in \mathrm{Sp}(a)\}$ puisque les V_λ sont supplémentaires.

Calculs de $a^m = (d + n)^m$ par la fomule du binôme de Newton (d et n commutent).

Interprétation matricielle du raisonnement.
Décomposer V en la somme des V_λ qui sont des sous-espaces stables revient à trouver une base de V dans laquelle la matrice de a est constituée de blocs diagonaux qui n'ont qu'une seule valeur propre (concatener des bases des V_λ). Ensuite, chaque bloc diagonal $B \in \mathcal{M}_t(k)$ est la somme d'une homothétie et d'un nilpotent : l'homothétie est λI_t, la matrice nilpotente est $B - \lambda I_t$ (elle est nilpotente car sa seule valeur propre est 0 et parce que son polynôme caractéristique est scindé, comme celui de a).

[En TD, exemples génériques, principes et réflexes de base en petites dimensions. Pas de polynôme minimal en 2010, sauf peut-être en TD.]

UVSQ 2009/2010
Licence de sciences et technologie, santé
LSMA211 (algèbre générale)

Axiomatique des structures abstraites : groupes, anneaux, corps, espaces vectoriels

1 Groupes

1.1 Définition, axiomes

Un **groupe** est un ensemble G muni d'une *loi de composition interne* notée ici $\times$ (*i.e.* une application $G \times G \to G$, $(x, y) \mapsto x \times y$) vérifiant les trois axiomes suivants :

1- la loi $\times$ est *associative* (*i.e.* $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, et z de G ; on note $x \times y \times z$ ce produit) ;

2- G possède un *élément neutre* e pour $\times$ (*i.e.* $x \times e = e \times x = x$ pour tout $x \in G$; on note souvent 1 l'élément neutre) ;

3- tout élément de G possède un *symétrique* pour $\times$ (*i.e.* pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = e$; on note souvent $y = x^{-1}$).

Si en outre $\times$ est *commutative* (*i.e.* $x \times y = y \times x$ pour tous x et y de G), le groupe est dit *commutatif* ou *abélien*.

On omet souvent le symbole $\times$ de la loi en notant $xy = x \times y$. On note parfois $+$ la loi des groupes commutatifs ; dans ces conditions, l'élément neutre est noté 0 et le symétrique de tout $x \in G$ est noté $-x$.

1.2 Sous-groupe, homomorphisme de groupes

Un **sous-groupe** d'un groupe G est une partie de G qui soit un groupe pour la loi de G.

Proposition *Une partie non vide H d'un groupe G est un sous-groupe de G si, et seulement si :*

1- H est stable pour la loi de G (i.e. $x \times y \in H$ pour tous x et y de H) ;

2- le symétrique (pour la loi de G) de tout élément de H est dans H.

Un **homomorphisme de groupes** est une application f d'un groupe G dans un groupe G' qui préserve les lois de G et de G', c'est-à-dire telle que $f(xy) = f(x)f(y)$ pour tous x et y de G.

1.3 Exemples fondamentaux

L'addition usuelle dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{Z}$, et dans leurs puissances.

La multiplication usuelle dans $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ ou $\mathbb{C}^*$, dans l'ensemble des nombres complexes de module un, dans l'ensemble des racines n-ièmes de l'unité ($n \geq 1$) et dans l'ensemble de toutes les racines de l'unité.

La composition dans l'ensemble des bijections d'un ensemble sur lui-même (groupe symétrique) ; dans $\mathrm{GL}(E)$ (groupe linéaire de l'espace vectoriel E) et dans ses sous-groupes $\mathrm{SL}(E)$, $\mathrm{O}(E)$, $\mathrm{SO}(E)$, $\mathrm{U}(E)$, $\mathrm{SU}(E)$; dans l'ensemble des similitudes (resp. des similitudes directes) vectorielles planes. *etc.*

Le produit matriciel dans $\mathrm{GL}_n(A)$ (matrices carrées $n \times n$ inversibles à coefficients dans l'anneau A), $\mathrm{SL}_n(A)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$, $\mathrm{SU}_n(\mathbb{C})$; dans l'ensemble des matrices triangulaires supérieures (resp. inférieures) inversibles, dans l'ensemble des matrices diagonales inversibles, *etc.*

2 Anneaux

2.1 Définition, axiomes

Un **anneau** (unitaire) est un ensemble A muni de deux lois de composition interne notées ici $+$ (addition) et $\times$ (multiplication) vérifiant les axiomes suivants :

1- $(A, +)$ est un groupe abélien ; on note souvent son élément neutre 0 et $-a$ le symétrique de $a \in A$ pour $+$ (on parle de l'*opposé* de a) ;

2- la loi $\times$ est associative et admet un élément neutre souvent noté 1 ;

3- la multiplication est *distributive* par rapport à l'addition (*i.e.* $a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$ pour tous a, b et c de A).

Si en outre la multiplication est commutative, l'anneau est dit *commutatif*.

Les règles de calcul dans un anneau commutatif sont celles de $\mathbb{Z}$; en particulier, la formule du binôme de Newton est vraie dans un anneau commutatif (ou dans un anneau général entre deux éléments qui commutent). Dans les systèmes de parenthésages, on donne la priorité à la multiplication ; ainsi, $a \times b + c = (a \times b) + c$.

2.2 Sous-anneau, idéal, homomorphisme d'anneaux

Un **sous-anneau** d'un anneau A est une partie de A qui soit un anneau pour les lois de A. Une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A si, et seulement si $(B, +)$ est un sous-groupe de $(A, +)$ contenant 1, et B est stable pour la multiplication de A.

Un **idéal** d'un anneau commutatif A est une partie I de A telle $(I, +)$ soit un sous-groupe de $(A, +)$ et $ia \in I$ pour tous $i \in I$ et $a \in A$.

Une application f d'un anneau A dans un anneau B est un **homomorphisme d'anneaux** si, et seulement si elle préserve les unités et les lois de A et B, c'est-à-dire si, et seulement si $f(1) = 1$, $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous x et y de A.

2.3 Exemples fondamentaux

Pour leurs lois usuelles, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 2$, les corps de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'ensemble des nombres décimaux.

Les anneaux de polynômes à coefficients dans un anneau A.

L'anneau des endomorphismes d'un espace vectoriel (la multiplication est la composition), l'anneau des matrices carrées à coefficients dans un anneau (la multiplication est le produit matriciel).

L'ensemble des applications d'un ensemble E dans un anneau A (pour les lois usuelles $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$).

3 Corps

3.1 Définition, axiomes

Un **corps** est un anneau A dans lequel tout élément non nul x admet un symétrique pour la multiplication (on parle alors de l'*inverse* de x, souvent noté x^{-1}). Cela revient à demander que $A \setminus \{0\}$ soit un groupe pour la multiplication.

3.2 Sous-corps, plongements

Un **sous-corps** d'un corps L est une partie K de L qui soit un corps pour les lois de L. Cela revient à demander que $(K, +)$ soit un sous-groupe de $(L, +)$ et que $(K \setminus \{0\}, \times)$ soit un sous-groupe de $(L \setminus \{0\}, \times)$.

Un homomorphisme d'anneaux $k \to A$ où k est un corps est toujours injectif. On parle de **plongement** de k dans A ou d'**extension** de k.

3.3 Exemples fondamentaux

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ pour leurs lois usuelles. Le corps des nombres algébriques.

$\mathbb{Z}/p\mathbb{Z}$ si p est un nombre premier, les corps finis $\mathbb{F}_{p^a}$.

$k[X]/(P)$ si k est un corps et si P est un polynôme irréductible de $k[X]$; plus généralement, le quotient d'un anneau par un idéal maximal.

L'ensemble des fractions rationnelles sur un corps (une ou plusieurs indéterminées).

Le corps des quaternions (non commutatif).

4 Espaces vectoriels

4.1 Définition, axiomes

Un **espace vectoriel** sur le corps k est un ensemble E muni d'une loi de composition interne (*addition*) notée ici $+$ et d'une loi externe sur k notée $.$ (*i.e.* une application $k \times E \to E$, $(a, x) \mapsto a.x$, *multiplication par les scalaires*) vérifiant :

1- $(E, +)$ est une groupe abélien ;

2- pour tous $(a, b) \in k^2$ et $(x, y) \in E^2$,

- $1.x = x$;
- $(a + b).x = a.x + b.x$;
- $a.(x + y) = a.x + a.y$;
- $a.(b.x) = (ab).x$.

4.2 Sous-espace vectoriel, application linéaire

Un **sous-espace vectoriel** d'un espace vectoriel E est une partie de E qui soit un espace vectoriel pour les lois de E. Une partie F d'un espace vectoriel E est un sous-espace vectoriel de E si, et seulement si F est non vide et stable pour les lois de E, *i.e.* $x + y \in F$ et $a.x \in F$ pour tous $(x, y) \in F^2$ et $a \in k$.

Une application f d'un espace vectoriel E sur k dans un espace vectoriel F sur k est une **application linéaire** (ou homomorphisme d'espaces vectoriels) si, et seulement si elle préserve les lois de E et F, c'est-à-dire si, et seulement si $f(x+y) = f(x)+f(y)$ et $f(a.x) = a.f(x)$ pour tous $(x, y) \in E^2$ et $a \in k$.

4.3 Exemples fondamentaux

k^n où $n \in \mathbb{N}^*$, pour les lois $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $a.(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$; prototype d'espace vectoriel de dimension finie égale à n.

L'ensemble des applications linéaires d'une espace vectoriel dans un autre (pour les lois $(f+g)(x) = f(x)+g(x)$ et $(a.f)(x) = a.f(x)$) ; en particulier, l'espace des formes linéaires (dual).

L'ensemble des suites à coefficient dans k (dimension dénombrable), pour les lois $(x_n)_n + (y_n)_n = (x_n + y_n)_n$ et $a.((x_n)_n) = (ax_n)_n$.

L'ensemble des applications d'un ensemble dans le corps k pour les lois usuelles.

Si A est un anneau, extension d'un corps k, alors A est un espace vectoriel sur k (d'où les cardinaux des corps finis).