Algèbre avancée

Bas Edixhoven

1994-1995

Table des matières

1 Groupes, sous-groupes et morphismes.

1.1 Définition. *Un groupe est un triplet $(G, \cdot, e)$, où G est un ensemble, $\cdot : G \times G \to G$ est une application qu'on note $(x, y) \mapsto x \cdot y$ et e un élément de G, tel que:*

1: $\cdot$ est associative: $\forall x, y, z \in G$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

2: e est un élément neutre: $\forall x \in G$: $e \cdot x = x = x \cdot e$

3: il existe des inverses: $\forall x \in G\ \exists y \in G$: $x \cdot y = e = y \cdot x$.

L'application $\cdot$ est appelée la multiplication ou encore la loi de composition. Pour x et y dans G, $x \cdot y$ est appelé le produit de x et y; pour simplifier on le notera souvent par xy. L'associativité de la multiplication entraîne qu'un produit de n éléments ($n \geq 3$) est indépendant de la position des parenthèses, et que l'on peut écrire sans risque de confusion des expressions telles que $x_1 x_2 \cdots x_n$. L'élément $e \in G$ est le seul élément neutre de G: si on a $e' \in G$ tel que $e'x = x = xe'$ pour tout $x \in G$ alors $e' = e'e = e$. L'élément y dans 1.1 (3) est le seul élément de G tel que $xy = e = yx$: si on a $y' \in G$ tel que $xy' = e = y'x$ alors $y' = y'e = y'(xy) = (y'x)y = ey = y$; on appelle y l'inverse de x et on le note x^{-1}. Pour l'inverse d'un produit on a: $(xy)^{-1} = y^{-1}x^{-1}$. Dans un groupe, l'égalité $xy = xz$ entraîne $y = z$, et $xy = zy$ entraîne $x = z$. Souvent, s'il est clair quelle est la multiplication $\cdot$, on notera le groupe $(G, \cdot, e)$ simplement par G. On dira que le groupe $(G, \cdot, e)$ est commutatif (ou abélien) si pour tout x et y dans G on a $xy = yx$. La multiplication d'un groupe commutatif se note parfois $+$; si tel est le cas, on note e par 0 et x^{-1} par $-x$.

1.2 Exemples. 1. (style Bourbaki) Le groupe dit trivial: $G = \{e\}$.
2. (plus sérieux) Le groupe additif des entiers: $(\mathbf{Z}, +, 0)$.
3. (plus général) Le groupe additif d'un anneau A: $(A, +, 0)$.
4. (fini la nonsense) Le groupe multiplicatif d'un corps k: $(k - \{0\}, \cdot, 1)$; on le note k^*.
5. Soit k un corps et $n \geq 0$. Le groupe des matrices $n \times n$ inversibles à coefficients dans k: $(\{g \in \mathrm{M}_n(k) \mid \det(g) \neq 0\}, \cdot, I)$; on le note $\mathrm{GL}_n(k)$.
6. Soit X un ensemble. Le groupe des permutations de X: $(\{f : X \to X \mid f \text{ bijective}\}, \circ, \mathrm{id})$; on le note $\mathrm{Sym}(X)$.
7. Soit $n \geq 0$. Le groupe $\mathrm{S}_n := \mathrm{Sym}(\{1, 2, \ldots, n\})$.
8. (vague) Groupes d'automorphismes.

1.3 Définition. *Soit G un groupe. Un sous-groupe de G est un sous-ensemble $H \subset G$ tel que la multiplication de G induit une structure de groupe sur H, c'est à dire: 1: $e \in H$, 2: $\forall x, y \in H$: $xy \in H$ et 3: $\forall x \in H$: $x^{-1} \in H$. Un sous-groupe H de G est distingué si $\forall g \in G\ \forall h \in H$: $ghg^{-1} \in H$.*

Si I est un ensemble et pour tout $i \in I$ on a un sous-groupe $H_i \subset G$ alors l'intersection $\cap_{i \in I} H_i$ est un sous-groupe de G; si pour tout i le sous-groupe H_i est distingué alors $\cap_{i \in I} H_i$ est distingué. Si G est un groupe et $X \subset G$ un sous-ensemble on note $\langle X \rangle$ l'intersection de tous les sous-groupes H de G qui contiennent X, c'est le plus petit sous-groupe de G qui contient X et on l'appelle le sous-groupe de G engendré par X. On montre que $\langle X \rangle$ est l'ensemble des produits finis $x_1 x_2 \cdots x_n$, où $n \geq 0$ et où pour tout i on a $x_i \in X$ ou $x_i^{-1} \in X$.

Soit H un sous-groupe de $\mathbf{Z}$. Si $H \neq \{0\}$ l'ensemble $\{n \in H \mid n > 0\}$ est non-vide donc contient un plus petit élément m. On montre (en utilisant la division Euclidienne) qu'alors $H = m\mathbf{Z} = \langle m \rangle = \{mn \mid n \in \mathbf{Z}\}$. On voit donc que tout sous-groupe H de $\mathbf{Z}$ s'écrit de façon unique comme $m\mathbf{Z}$ avec $m \geq 0$; on dit que m est le générateur non-négatif de H.

1.4 Définition. *Soient G_1 et G_2 des groupes. Un morphisme (de groupes) f de G_1 vers G_2 est une application $f: G_1 \to G_2$ telle que $f(xy) = f(x)f(y)$ pour tout x et y dans G_1. Un antimorphisme f de G_1 vers G_2 est une application telle que $f(xy) = f(y)f(x)$ pour tout $x, y \in G_1$.*

Soit $f: G_1 \to G_2$ un morphisme ou un antimorphisme, alors $f(e_1) = f(e_1e_1) = f(e_1)f(e_1)$, donc $f(e_1) = e_2$; on trouve aussi que $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G_1$. Un exemple d'un antimorphisme est l'application $\iota_G: G \to G$: $x \mapsto x^{-1}$; en plus ι_G est bijectif et $\iota_G \circ \iota_G = \mathrm{id}_G$. Comme $f: G_1 \to G_2$ est un antimorphisme si et seulement si $f \circ \iota_{G_1}$ est un morphisme, on peut se restreindre à étudier seulement les morphismes.

Soit $f: G_1 \to G_2$ un morphisme. On définit le noyau $\ker(f)$ et l'image $\mathrm{im}(f)$ par: $\ker(f) = \{x \in G_1 \mid f(x) = e_2\}$ et $\mathrm{im}(f) = \{f(x) \mid x \in G_1\} = \{y \in G_2 \mid \exists x \in G_1 : y = f(x)\}$; $\ker(f)$ est un sous-groupe distingué de G_1 et $\mathrm{im}(f)$ est un sous-groupe de G_2. Le morphisme f est injectif (resp. surjectif) si et seulement si $\ker(f) = \{e_1\}$ (resp. $\mathrm{im}(f) = G_2$). Le morphisme $f: G_1 \to G_2$ est appelé un isomorphisme s'il existe un morphisme $g: G_2 \to G_1$ tel que $g \circ f = \mathrm{id}_{G_1}$ et $f \circ g = \mathrm{id}_{G_2}$; il revient au même de dire que f est bijectif. Un isomorphisme $f: G \to G$ s'appelle aussi automorphisme de G.

Soit G un groupe et $x \in G$. Pour $n \in \mathbf{Z}$ on définit x^n par: si $n \geq 0$ on pose $x^n = xx \cdots x$ (n facteurs), si $n \leq 0$ on pose $x^n := x^{-1}x^{-1} \cdots x^{-1}$ ($-n$ facteurs). (Si G est commutatif et la multiplication est notée $+$, on note x^n par nx.) L'application $f_x: \mathbf{Z} \to G$: $n \mapsto x^n$ est un morphisme. En plus, chaque morphisme $f: \mathbf{Z} \to G$ est de cette forme: $f = f_x$, où $x = f(1)$. L'image $\mathrm{im}(f_x)$ est le sous-groupe de G engendré par x et $\ker(f_x)$ est l'ensemble $\{n \in \mathbf{Z} \mid x^n = e\}$.

1.5 Définition. *Soit G un groupe et $x \in G$. Si l'ensemble $\{n \geq 1 \mid x^n = e\}$ est non-vide on note* $\mathrm{ordre}(x)$ *et on appelle ordre de x le plus petit élément de cet ensemble, dans l'autre cas on dit que x est d'ordre infini et on note* $\mathrm{ordre}(x) = \infty$.

On montre que $\mathrm{ordre}(x) = \infty$ si et seulement si f_x est injectif et que pour x d'ordre fini $\mathrm{ordre}(x)$ est le générateur non-négatif de $\ker(f_x)$.

2 Quelques propriétés de S_n.

Soit $n \geq 0$. Le groupe S_n est fini et son cardinal est $\#\mathrm{S}_n = n(n-1)\cdots 1 = n!$, il est commutatif si et seulement si $n \leq 2$. Soit $\sigma \in \mathrm{S}_n$, donc par définition $\sigma\colon \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ est une bijection et on peut noter σ par $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{smallmatrix}\right)$. Dans cette notation, le produit de $\sigma, \tau \in \mathrm{S}_n$ se calcule par:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n)\end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma\tau(1) & \sigma\tau(2) & \cdots & \sigma\tau(n)\end{pmatrix}$$

Par exemple on a $\left(\begin{smallmatrix} 1&2&3 \\ 2&3&1\end{smallmatrix}\right)\left(\begin{smallmatrix} 1&2&3 \\ 2&1&3\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3 \\ 3&2&1\end{smallmatrix}\right)$ (et non $\left(\begin{smallmatrix} 1&2&3 \\ 1&3&2\end{smallmatrix}\right)$).

Soient $l \geq 1$ et $i_1, \ldots, i_l \in \{1, 2, \ldots n\}$ distincts. On note $(i_1, \ldots, i_l)$ l'élément σ de S_n tel que $\sigma(i_r) = i_{r+1}$ pour $1 \leq r < l$, $\sigma(i_l) = i_1$ et $\sigma(i) = i$ pour $i \notin \{i_1, \ldots, i_l\}$; on appelle $(i_1, \ldots, i_l)$ un cycle de longueur l. L'ordre d'un cycle de longueur l est l. Noter que $(i_2, \ldots, i_l, i_1) = (i_1, \ldots, i_l)$ etc., et que $(1) = (2) = \cdots = (n) = \mathrm{id}$. Plus précisement on a: $(i_1, \ldots, i_l) = (j_1, \ldots, j_m)$ si et seulement si 1: $l = m$ et 2: si $l > 1$: $\exists a$ tel que $\forall k$: $i_k = j_{(k+a) \bmod l}$. Deux cycles $(i_1, \ldots, i_l)$ et $(j_1, \ldots, j_m)$ sont disjoints si $\{i_1, \ldots, i_l\} \cap \{j_1, \ldots, j_m\} = \emptyset$. Deux cycles disjoints commutent entre eux.

2.1 Proposition. *Tout élément σ de S_n peut s'écrire comme $\sigma = \sigma_1 \cdots \sigma_r$ où les σ_i sont des cycles disjoints; cette écriture est unique à l'ordre des σ_i et aux cycles de longueur 1 près. Pour tout $k \in \mathbf{Z}$ on a $\sigma^k = \sigma_1^k \cdots \sigma_r^k$. Si l_i est la longueur de σ_i, on a $\mathrm{ordre}(\sigma) = \mathrm{ppcm}\{l_1, \ldots, l_r\}$.*

Soit $\sigma \in \mathrm{S}_n$. On définit alors le signe $\varepsilon(\sigma)$ dans le sous-groupe $\{\pm 1\}$ de $\mathbf{Q}^*$ par:

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \tag{2.2}$$

Montrons qu'en fait $\varepsilon(\sigma)$ appartient à $\{\pm 1\}$. Soit X l'ensemble $\{(i,j) \mid 1 \leq i < j \leq n\}$. Soit $f_\sigma\colon X \to X$ l'application donnée par: $f_\sigma(i,j) = (\sigma(i), \sigma(j))$ si $\sigma(i) < \sigma(j)$, et $f_\sigma(i,j) = (\sigma(j), \sigma(i))$ si $\sigma(j) < \sigma(i)$. On vérifie sans peine que f_σ est une bijection. Soit finalement $g\colon X \to \mathbf{Z}$ donnée par $g(i,j) = i - j$. Avec ces définitions on a:

$$|\varepsilon(\sigma)| = \prod_{(i,j) \in X} \frac{|g(f_\sigma(i,j))|}{|g(i,j)|} = \left(\prod_{(i,j) \in X} |g(f_\sigma(i,j))| \right) \left(\prod_{(i,j) \in X} |g(i,j)| \right)^{-1}$$

et comme f_σ est une permutation de X, on trouve $|\varepsilon(\sigma)| = 1$.

La formule (2.2) que nous avons donnée plus haut pour $\varepsilon(\sigma)$ n'est pas très utile en pratique; nous verrons plus loin une méthode plus efficace pour calculer $\varepsilon(\sigma)$. En regardant les signes des facteurs dans la formule pour $\varepsilon(\sigma)$ on voit toutefois que $\varepsilon(\sigma) = (-1)^{m(\sigma)}$, où $m(\sigma) = \#\{(i,j) \mid 1 \leq i < j \leq n \text{ et } \sigma(i) > \sigma(j)\}$. On appelle $m(\sigma)$ le nombre d'inversions de σ. Une permutation σ est dite paire (resp. impaire) si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

2.3 Proposition. *L'application $\varepsilon\colon \mathrm{S}_n \to \{\pm 1\}$ est un morphisme.*

Démonstration. Soit $\sigma, \tau \in \mathrm{S}_n$. Il faut montrer que $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. On a:

$$\varepsilon(\sigma\tau) = \prod_{1\leq i<j\leq n} \frac{(\sigma\tau)(i) - (\sigma\tau)(j)}{i-j} = \left(\prod_{1\leq i<j\leq n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)} \right) \cdot \left(\prod_{1\leq i<j\leq n} \frac{\tau(i)-\tau(j)}{i-j} \right)$$

Le deuxième facteur de la dernière expression est visiblement $\varepsilon(\tau)$, il suffira donc de montrer que le premier facteur égale $\varepsilon(\sigma)$. Notons d'abord que pour $1 \leq i < j \leq n$ on a

$$\frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\sigma(j)-\sigma(i)}{j-i}$$

Soit $f_\tau\colon X \to X$ la bijection définie comme plus haut. Définissons, pour tout σ dans S_n la fonction $h_\sigma\colon X \to \mathbf{Q}$ par:

$$h_\sigma\colon X \longrightarrow \mathbf{Q}: \quad (i,j) \mapsto \frac{\sigma(i)-\sigma(j)}{i-j}$$

Avec ces définitions, on a:

$$\prod_{1\leq i<j\leq n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)} = \prod_{(i,j)\in X} h_\sigma(f_\tau(i,j)) = \prod_{(i,j)\in X} h_\sigma(i,j) = \varepsilon(\sigma)$$

La démonstration est donc finie. $\square$

Autre démonstration de Prop. 2.3. Nous allons maintenant donner une autre démonstration, qui utilise les polynômes. Soit $A := \mathbf{Z}[x_1, x_2, \ldots, x_n]$ l'anneau de polynômes en les variables $x_1, \ldots, x_n$ et à coefficients dans $\mathbf{Z}$. Pour chaque σ dans S_n, soit $\phi_\sigma\colon A \to A$ le morphisme d'anneaux unique tel que $\phi_\sigma(x_i) = x_{\sigma(i)}$ pour tout i. On vérifie facilement que pour tout σ et τ dans S_n et tout i dans $\{1, 2, \ldots, n\}$, $\phi_{\sigma\tau}(x_i) = x_{(\sigma\tau)(i)} = (\phi_\sigma \circ \phi_\tau)(x_i)$, d'où on tire $\phi_{\sigma\tau} = \phi_\sigma \circ \phi_\tau$. Soit f l'élément de A défini comme suit:

$$f := \prod_{1\leq i<j\leq n} (x_i - x_j)$$

Alors pour tout σ dans S_n on a

$$\phi_\sigma(f) = \prod_{1\leq i<j\leq n} \phi_\sigma(x_i - x_j) = \prod_{1\leq i<j\leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Comme le dernier produit est, à un signe près, le produit des $x_i - x_j$ avec $1 \leq i < j \leq n$, il est soit f, soit $-f$. En regardant les signes des facteurs, on voit que le signe correct est $(-1)^{m(\sigma)}$. On a donc $\phi_\sigma(f) = \varepsilon(\sigma) \cdot f$ pour tout σ dans S_n. Soient maintenant σ et τ dans S_n. On a

$$\varepsilon(\sigma\tau)f = \phi_{\sigma\tau}(f) = (\phi_\sigma \circ \phi_\tau)(f) = \phi_\sigma(\phi_\tau(f)) = \phi_\sigma(\varepsilon(\tau)f) = \varepsilon(\tau)\phi_\sigma(f) = \varepsilon(\tau)\varepsilon(\sigma)f$$

On en conclut que $(\varepsilon(\sigma\tau) - \varepsilon(\sigma)\varepsilon(\tau))f = 0$, ce qui implique que $\varepsilon(\sigma\tau) - \varepsilon(\sigma)\varepsilon(\tau) = 0$ car $f \neq 0$ et A est un anneau intègre. $\square$

Comme $\varepsilon\colon \mathrm{S}_n \to \{\pm 1\}$ est un morphisme, son noyau $\mathrm{A}_n := \ker(\varepsilon)$ est un sous-groupe distingué de S_n; c'est le sous-groupe des permutations paires. On montre que $\#\mathrm{A}_n = n!/2$ si $n \geq 2$.

2.4 Proposition. *1. Soient τ et $(i_1, \ldots, i_l)$ dans S_n. Alors:*

$$\tau(i_1, \ldots, i_l)\tau^{-1} = (\tau(i_1), \ldots, \tau(i_l))$$

2. Si $\sigma \in \mathrm{S}_n$ est un cycle de longueur l, alors $\varepsilon(\sigma) = (-1)^{l-1}$.
3. Soit $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ une décomposition de $\sigma \in \mathrm{S}_n$ en cycles disjoints de longueurs $l_1, \ldots, l_r$. Alors:

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{r}(l_i-1)}$$

Démonstration. Démontrons la partie 1. Pour $1 \leq k < l$ on a: $(\tau(i_1, \ldots, i_l)\tau^{-1})(\tau(i_k)) = \tau((i_1, \ldots, i_l)(i_k)) = \tau(i_{k+1})$. On a $(\tau(i_1, \ldots, i_l)\tau^{-1})(\tau(i_l)) = \tau((i_1, \ldots, i_l)(i_l)) = \tau(i_1)$. Pour $i \notin \{\tau(i_1), \ldots, \tau(i_l)\}$ on a $\tau^{-1}(i) \notin \{i_1, \ldots, i_l\}$ d'où $(i_1, \ldots, i_l)(\tau^{-1}(i)) = \tau^{-1}(i)$ etc.

Démontrons maintenant la partie 2. Ecrivons $\sigma = (i_1, \ldots, i_l)$. Soit $\tau \in \mathrm{S}_n$ tel que $\tau(k) = i_k$ pour $1 \leq k \leq l$. Alors $\sigma = \tau(1, 2, \ldots, l)\tau^{-1}$ par la partie 1, donc $\varepsilon(\sigma) = \varepsilon(\tau)\varepsilon((1, 2, \ldots, l))\varepsilon(\tau^{-1})$, ce qui est égal à $\varepsilon((1, 2, \ldots, l))$ car ε est un morphisme et $\{\pm 1\}$ est commutatif. On est donc ramené a montrer que $\varepsilon((1, 2, \ldots, l)) = (-1)^{l-1}$. On voit que le nombre d'inversions de $(1, 2, \ldots, l)$ est $l-1$, d'où ce qu'il faut.

La partie 3 résulte de la partie 2 en utilisant que ε est un morphisme. □

2.5 Application. On considère le jeu bien connu suivant. Il y a un tableau à 16 cases, dont une case est vide et dont les autres sont numérotées de 1 à 15:

(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Dans ce tableau, on peut faire glisser les cases, ou autrement dit: la case vide peut être échangée avec une de ses voisines. Par exemple, en faisant glisser la case 12 dans le tableau ci-dessus, on arrive à la position

(b)

1	2	3	4
5	6	7	8
9	10	11	
13	14	15	12

Ce qu'on se demande alors est si en partant de la position (a) en haut on peut arriver à la position

(c)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Nous allons montrer que cela est impossible. On dira que la case vide est la case 16. En faisant glisser les cases, on fait des permutations de $\{1, 2, \ldots, 16\}$. On appellera un coup un échangement de la case 16 avec une de ses voisines. Chaque fois qu'on fait un coup, la permutation qu'on a est multipliée par un cycle de longueur deux. Donc chaque coup, la permutation qu'on a change de signe. Comme la permutation correspondant à la position (c) est le cycle $(14, 15)$, donc une permutation impaire, on ne pourra pas y arriver en un nombre pair de coups. Maintenant suivons le trajet que fait la case 16 quand on fait des coups. En prétendant que la case 16 fait son trajet sur un échiquier où les cases sont noir et blanc

n	b	n	b
b	n	b	n
n	b	n	b
b	n	b	n

on constate qu'à chaque coup, la case où se trouve le 16 change de couleur. On voit donc qu'après un nombre impair de coups, la case 16 ne peut pas se trouver à sa position initiale. Nous avons vu maintenant que la transition de la position (a) en la position (c) ne peut se faire ni en un nombre pair de coups, ni en un nombre impair de coups.

3 Relations d'équivalence et constructions quotients.

Commençons par quelques rappels sur les relations et les relations d'équivalence. Soient X et Y des ensembles. Une relation R sur $X \times Y$ est alors un sous-ensemble $R \subset X \times Y$; au lieu de noter $(x, y) \in R$ on note souvent xRy. Par exemple la relation $\leq$ sur $\mathbf{Z} \times \mathbf{Z}$ est l'ensemble $\{(x, y) {\in} \mathbf{Z} \times \mathbf{Z} \mid x \leq y\}$.

3.1 Définition. *Une relation d'équivalence $\sim$ sur un ensemble X est une relation $\sim$ sur $X \times X$ telle que: 1: $\sim$ est réflexive: $\forall x{\in}X\colon x{\sim}x$, 2: $\sim$ est symétrique: $x{\sim}y \Rightarrow y{\sim}x$ et 3: $\sim$ est transitive: $(x{\sim}y$ et $y{\sim}z) \Rightarrow x{\sim}z$.*

Un exemple utile et standard d'une relation d'équivalence est le suivant. Pour $n \in \mathbf{Z}$ on a la relation $\equiv_n$ sur $\mathbf{Z}$, où $x \equiv_n y \Leftrightarrow n|(x{-}y)$.

Soient maintenant X un ensemble et $\sim$ une relation d'équivalence sur X. Pour $x \in X$, on appelle classe d'équivalence de x l'ensemble $\overline{x} = \{y{\in}X \mid y{\sim}x\}$. Pour $x, y \in X$ on a $\overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \emptyset$, selon $x{\sim}y$ ou $x{\not\sim}y$. L'ensemble X est donc partitionné par les classes d'équivalence. L'ensemble $X/{\sim} := \{\overline{x} \mid x{\in}X\}$ des classes d'équivalence est appelé l'ensemble quotient de X par $\sim$. L'application $p\colon X \to X/{\sim}\colon x \mapsto \overline{x}$ s'appelle la projection canonique. Elle est surjective et a la propriété suivante:

3.2 Proposition. *Soient $\sim$ une relation d'équivalence sur un ensemble X et $p\colon X \to X/{\sim}$ la projection canonique. Alors pour toute application $f\colon X \to Y$ telle que $x{\sim}y \Rightarrow f(x){=}f(y)$ il existe une application unique $\overline{f}\colon X/{\sim} \to Y$ telle que $f = \overline{f}{\circ}p$.*

Démonstration. Nous disons qu'une application $f\colon X \to Y$ telle que $x{\sim}y \Rightarrow f(x){=}f(y)$ est compatible à $\sim$. Montrons d'abord qu'il existe une application $\overline{f}$ qui satisfait à $f = \overline{f}{\circ}p$. Pour donner une application $\overline{f}\colon X/{\sim} \to Y$, il suffit de dire pour tout $C \in X/{\sim}$ quel est $\overline{f}(C)$. Soit $C \in X/{\sim}$, donc C est une classe d'équivalence dans X. Pour x et y dans C on a $x{\sim}y$, d'où $f(x){=}f(y)$ comme f est compatible à $\sim$. On voit que les images sous f des éléments de C sont tous les mêmes. En plus, une classe d'équivalence a au moins un élément. Nous pouvons donc définir $\overline{f}(C) := f(x)$, quel que soit $x \in C$. Pour tout $x \in X$ on a alors: $(\overline{f}{\circ}p)(x) = \overline{f}(p(x)) = \overline{f}(\overline{x}) = f(x)$, car $x \in \overline{x}$. On a donc montré que $f = \overline{f}{\circ}p$.

Montrons maintenant que $\overline{f}$ est unique. Ceci revient à montrer que si on a $g\colon X/{\sim} \to Y$ avec $f = g{\circ}p$, alors $g = \overline{f}$. Supposons donc que $g\colon X/{\sim} \to Y$ avec $f = g{\circ}p$. Alors $g{\circ}p = \overline{f}{\circ}p$, d'où $g = \overline{f}$ car p est surjective. □

Soit G un groupe et $\sim$ une relation d'équivalence sur G. On se demande si on peut munir l'ensemble $G/{\sim}$ d'une structure de groupe telle que la projection canonique est un morphisme. Autrement dit, est-ce qu'il existe une application $\cdot\colon G/{\sim} \times G/{\sim} \to G/{\sim}$ telle que 1: $G/{\sim}$ avec la multiplication $\cdot$ est un groupe, et 2: $\overline{x}{\cdot}\overline{y} = \overline{xy}$ pour tout x et y dans G? Noter que la condition 2 implique qu'il existe au plus une telle structure de groupe.

3.3 Définition. *Soit $\sim$ une relation d'équivalence sur un groupe G. On dit que $\sim$ est compatible avec la structure de groupe (ou avec la multiplication) de G si pour tous x_1, x_2, y_1 et y_2 dans G tels que $x_1 \sim x_2$ et $y_1 \sim y_2$ on a $x_1 y_1 \sim x_2 y_2$.*

3.4 Proposition. *Soit $\sim$ une relation d'équivalence sur un groupe G. Alors il existe sur $G/\sim$ une structure de groupe telle que la projection canonique est un morphisme si et seulement si $\sim$ est compatible avec la multiplication de G. Si une telle structure de groupe existe, elle est unique et on a: $\overline{x} \cdot \overline{y} = \overline{xy}$ pour tout x et y dans G.*

Démonstration. Supposons d'abord que $\sim$ est une relation d'équivalence sur G qui est compatible avec la structure de groupe. Soit $p\colon G \to G/\sim$ la projection canonique. Nous voulons définir une multiplication $\cdot$ sur $G/\sim$ telle que $(G/\sim, \cdot)$ est un groupe et $p\colon G \to G/\sim$, $x \mapsto \overline{x}$ est un morphisme. Soient a et b deux éléments de $G/\sim$. Soient $x \in a$ et $y \in b$; ceci veit dire que $a = p(x)$ et $b = p(y)$. Dire que p doit être un morphisme signifie qu'on a $a \cdot b = p(x) \cdot p(y) = p(xy)$. L'unicité de la loi de groupe $\cdot$ cherchée est donc claire. Pour montrer l'existence, il faut et il suffit de montrer que pour tous $x' \in a$ et $y' \in b$ on a $p(x'y') = p(xy)$. Pour de tels x' et y' on a $x' \sim x$ et $y' \sim y$, donc $x'y' \sim xy$ car $\sim$ est compatible avec la structure de groupe de G. Il s'ensuit que $p(x'y') = p(xy)$. Dans les exercices on trouvera une autre démonstration (essentiellement la même que celle que nous venons de voire) qui utilise la Proposition 3.2.

Supposons maintenant que nous avons une structure de groupe $\cdot$ sur $G/\sim$ qui fait de p un morphisme. Montrons que $\sim$ est compatible avec la structure de groupe de G. Soient donc x_1, x_2, y_1 et y_2 dans G tels que $x_1 \sim x_2$ et $y_1 \sim y_2$. On a alors $p(x_1) = p(x_2)$ et $p(y_1) = p(y_2)$, donc aussi $p(x_1 y_1) = p(x_1) \cdot p(y_1) = p(x_2) \cdot p(y_2) = p(x_2 y_2)$. Il en résulte que $x_1 y_1 \sim x_2 y_2$. $\square$

4 Opération d'un groupe sur un ensemble.

4.1 Définition. *Soient G un groupe et X un ensemble. Une opération à gauche de G sur X est une application $\cdot\colon G \times X \to X$ telle que:*
1: $\forall a, b \in G\ \forall x \in X$: $a\cdot(b\cdot x) = (ab)\cdot x$
2: $\forall x \in X$: $e\cdot x = x$.
Une opération à droite de G sur X est une application $\cdot\colon X \times G \to X$ telle que:
1: $\forall a, b \in G\ \forall x \in X$: $(x\cdot a)\cdot b = x\cdot(ab)$
2: $\forall x \in X$: $x\cdot e = x$.

Comme pour les groupes on notera souvent $a\cdot x$ par ax etc. S'il est claire quelle est $\cdot$ on dit simplement que G opère sur X.

Supposons que G opère à gauche sur X. Alors pour tout $g \in G$ on a une application $\gamma(g)\colon X \to X\colon x \mapsto gx$. Comme $g^{-1}(gx) = ex = x$ on voit que $\gamma(g^{-1})\circ\gamma(g) = \mathrm{id}_G = \gamma(g)\circ\gamma(g^{-1})$, donc $\gamma(g)$ est une bijection, ou encore, $\gamma(g) \in \mathrm{Sym}(X)$. Comme $g_1(g_2x) = (g_1g_2)x$, on a $\gamma(g_1)\circ\gamma(g_2) = \gamma(g_1g_2)$, donc $\gamma\colon G \to \mathrm{Sym}(X)$ est un morphisme. Si d'autre part on a un morphisme $\gamma\colon G \to \mathrm{Sym}(X)$ on obtient une opération à gauche de G sur X en posant $g\cdot x = (\gamma(g))(x)$. Il y a donc une équivalence entre les opérations à gauche de G sur X et les morphismes $\gamma\colon G \to \mathrm{Sym}(X)$. Même histoire pour les opérations à droite de G sur X et les antimorphismes $\delta\colon G \to \mathrm{Sym}(X)$. Comme on a déjà vu qu'il y a une équivalence entre les antimorphismes et les morphismes, il y a aussi une équivalence entre les opérations à gauche et les opérations à droite.

4.2 Exemples. 1. $\mathrm{Sym}(X)$ opère à gauche sur X si on pose $f\cdot x = f(x)$.
2. Soient G un groupe et $H \subset G$ un sous-groupe. On peut alors définir trois opérations différentes de H sur G.
2.1. Opération à gauche par translation: $h\cdot g = hg$.
2.2. Opération à droite par translation: $g\cdot h = gh$.
2.3. Opération à gauche par conjugaison: $h\cdot g = hgh^{-1}$. Cette opération correspond même à un morphisme $\gamma\colon H \to \mathrm{Aut}(G) \subset \mathrm{Sym}(G)$.
3. S_4 opère à gauche sur l'ensemble $\{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$ des partitions de $\{1,2,3,4\}$ en deux ensembles à deux éléments chacun. Ceci donne un morphisme surjectif $\mathrm{S}_4 \to \mathrm{S}_3$.

4.3 Définition. *Soit G un groupe opérant à gauche sur un ensemble X. Soit $x \in X$. On appelle le sous-ensemble $Gx := \{gx \mid g \in G\} \subset X$ l'orbite de x sous G. On appelle le sous-groupe $G_x := \{g{\in}G \mid gx = x\} \subset G$ le stabilisateur dans G de x. On dit que G opère librement sur X (ou que l'opération est libre) si tous les stabilisateurs sont triviaux, c'est à dire, si $G_x = \{e\}$ pour tout $x{\in}X$. On dit que G opère transitivement sur X s'il y a exactement une orbite. On dit que G opère trivialement sur X si pour tout g dans G et pour tout x dans X on a $gx = x$. Définitions analogues pour une opération à droite.*

4.4 Proposition. *Soit G un groupe opérant à gauche sur un ensemble X. Alors X est partitionné par les orbites. Autrement dit, la relation $\sim$ sur X donnée par $x{\sim}y \Leftrightarrow x \in Gy$ est une relation d'équivalence et on a: $x \in Gy \Leftrightarrow Gx = Gy$. On notera l'ensemble quotient $X/{\sim}$ par $G\backslash X$. Chose analogue pour les opérations à droite.*

Soient G un groupe et $H \subset G$ un sous-groupe. L'orbite $Hg = \{hg \mid h \in H\}$ de g pour l'opération de H sur G à gauche par translation s'appelle la classe à droite de g par rapport à H. Dans ce cas, l'ensemble quotient $G/{\sim}$ pour la relation $\sim$ donnée par $g_1{\sim}g_2 \Leftrightarrow Hg_1{=}Hg_2$ se note $H\backslash G$. Noter que cette opération de H sur G par translation est libre car $hg{=}g$ entraine $h{=}e$.

L'orbite $gH = \{gh \mid h \in H\}$ de g pour l'opération de H sur G à droite par translation s'appelle la classe à gauche de g par rapport à H. L'ensemble quotient $G/{\sim}$ pour la relation $\sim$ donnée par $g_1{\sim}g_2 \Leftrightarrow g_1H{=}g_2H$ se note G/H. L'opération de H sur G par translation à droite est libre.

L'orbite $\{gxg^{-1} \mid g{\in}G\}$ de $x \in G$ sous l'opération de conjugaison par G sur lui-même s'appelle la classe de conjugaison de x. Le stabilisateur $\{g{\in}\, G \mid gxg^{-1}{=}x\}$ de x s'appelle le centralisateur de x dans G et se note $C(x)$. Noter que cette opération n'est libre que pour le groupe trivial car $C(e) = G$.

4.5 Théorème. *Soit G un groupe opérant à gauche sur un ensemble X. Soit x dans X. Alors:*
1. Il y a une bijection $G/G_x \to Gx$: $\overline{a} \mapsto ax$.
2. Pour tout a dans G on a $G_{ax} = aG_xa^{-1} = \{aba^{-1} \mid b{\in}G_x\}$.

Démonstration. Commençons par 1. Nous avons une application $f\colon G \to X$: $a \mapsto ax$. Soit $\sim$ la relation d'équivalence sur G donnée par l'opération de G_x sur G par translation à droite: $a{\sim}b \Leftrightarrow aG_x{=}bG_x$. Alors f est compatible à $\sim$, car $a{\sim}b$ entraine qu'il existe $c{\in}G_x$ tel que $b = ac$, donc $f(b) = bx = (ac)x = a(cx) = ax = f(a)$. Par la Proposition 3.1 il existe alors une application unique $\overline{f}\colon G/G_x \to Gx$ telle que $\overline{f}(\overline{a}) = ax$. Cette application $\overline{f}$ est clairement surjective. Supposons que $\overline{f}(\overline{a}){=}\overline{f}(\overline{b})$. Alors $ax{=}bx$, donc $x{=}a^{-1}bx$, donc $a^{-1}b{\in}G_x$, donc $b{\in}aG_x$ d'où finalement $\overline{a}{=}aG_x{=}bG_x{=}\overline{b}$. On voit donc que $\overline{f}$ est bijective.

Pour démontrer la partie 2 on remarque: $b{\in}G_{ax} \Leftrightarrow bax{=}ax \Leftrightarrow a^{-1}bax{=}x \Leftrightarrow a^{-1}ba{\in}G_x \Leftrightarrow b{\in}aG_xa^{-1}$. □

4.6 Corollaire. *Soit G un groupe opérant librement sur un ensemble fini X. Alors G est fini et on a $|X| = |G|\,|G\backslash X|$.*

4.7 Corollaire. *Soit H un sous-groupe d'un groupe fini G. Alors on a $|G| = |H|\,|G/H| = |H|\,|H\backslash G|$.*

4.8 Définition. *Soient G un groupe et $H \subset G$ un sous-groupe tels que $|G/H|$ est fini (ce qui est certainement le cas si G est fini). On appelle $|G/H|$ l'indice de H dans G et on le note aussi par $[G : H]$. Si G est fini, $[G : H]$ divise $|G|$.*

4.9 Corollaire. *Soit G un groupe fini et x dans G. Alors* ordre(x) *est un diviseur de $|G|$.*

4.10 Corollaire. *Soit G un groupe fini opérant sur un ensemble fini X. Soient $X_1, X_2, \ldots, X_r$ les orbites distinctes, et soit, pour tout i, donné un élément x_i dans X_i. Alors on a:*

$$|X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} |G/G_{x_i}| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

Donnons quelques applications de la théorie étudiée plus haut. Supposons qu'un groupe G d'ordre 1001 opère sur un ensemble X à 6 éléments. Nous allons montrer que cette opération est triviale. Notons d'abord que $1001 = 7{\cdot}11{\cdot}13$. Soit x dans X. Alors $|Gx|$ divise $|G| = 1001$. Comme $|Gx| \leq |X| = 6$ on conclut que $|Gx| = 1$. Ceci veut dire que pour tout g dans G on a $gx = x$, ce qui signifie bien que G opère trivialement sur X.

Pour G un groupe opérant sur un ensemble X, on notera X^G le sous-ensemble de X formé par les points fixes: $X^G = \{x \in X \mid \forall g \in G\colon gx = x\}$. Pour p un nombre premier, on dira qu'un groupe fini G est un p-groupe si $|G|$ est une puissance de p. On a alors le résultat suivant.

4.11 Proposition. *Soient p un nombre premier et G un p-groupe opérant sur un ensemble fini X. Alors*

$$\left|X^G\right| \equiv |X| \pmod{p}$$

Démonstration. Considérons le complément $X - X^G = \{x \in X \mid x \notin X^G\}$ de X^G dans X. Ce complément est partitionné par des orbites à cardinaux plus grand que 1. Soit x un élément de $X - X^G$. Alors $|G{\cdot}x|$, étant un diviseur de $|G|$, est une puissance de p supérieur à 1, donc un multiple de p. Comme $X - X^G$ est partitionné par des orbites à cardinaux des multiples de p, son cardinal est un multiple de p. □

4.12 Corollaire. *Soient p un nombre premier, G un p-groupe et C le centre de G. Supposons que $G \neq \{e\}$. Alors $C \neq \{e\}$.*

Démonstration. Considérons l'opération de G sur G par conjugaison. Alors on a $G^G = C$. D'après la Proposition 4.11, $|C|$ est congru à $|G|$ modulo p, donc $|C|$ est un multiple de p, donc $|C|$ n'est pas égal à 1. □

5 Quotient d'un groupe par un sous-groupe distingué.

Rappelons qu'un sous-groupe $H \subset G$ est distingué si pour tout g dans G et tout h dans H on a $ghg^{-1} \in H$, c'est à dire, si pour tout $g \in G$ on a $gHg^{-1} \subset H$.

5.1 Proposition. *Soit H un sous-groupe d'un groupe G. Alors les conditions suivantes sont equivalentes:*
1: H est distingué,
2: pour tout g dans G on a $gHg^{-1} = H$,
3: pour tout g dans G on a $gH = Hg$.

5.2 Exemples. 1. Pour $f: G_1 \to G_2$ un morphisme, $\ker(f)$ est un sous-groupe distingué de G_1.
2. Soit $\sim$ une relation d'équivalence sur G compatible à la structure de groupe de G. Alors on peut munir $G/\sim$ d'une structure de groupe telle que la projection canonique $p: G \to G/\sim$ est un morphisme. Comme $\ker(p) = \overline{e}$, on voit que $\overline{e}$ est un sous-groupe distingué de G.

On verra dans quelques instants que tout sous-groupe distingué H de G est de la forme $\ker(f)$.

5.3 Proposition. *Soit H un sous-groupe distingué d'un groupe G. Alors les relations d'équivalence sur G données par les opérations de H sur G par translations à gauche ou à droite coïncident: $Hx{=}Hy \Leftrightarrow xH{=}yH$. Cette relation d'équivalence est compatible à la structure de groupe sur G et on peut donc munir $G/H = H\backslash G$ d'une unique structure de groupe telle que la projection canonique $p: G \to G/H$ est un morphisme. On a $\ker(p) = H$. Pour la multiplication sur G/H on a la formule: $\overline{x}{\cdot}\overline{y} = \overline{xy}$. On appelle G/H le groupe quotient de G par H.*

Démonstration. Que les deux relations d'équivalence sont égales résulte de la Proposition 5.1, partie 3. Notons par $\sim$ cette relation d'équivalence. Supposons que $x_1{\sim}x_2$ et $y_1{\sim}y_2$. Ceci signifie que $x_1H{=}x_2H$ et $y_1H{=}y_2H$. Alors on a: $x_1y_1H = x_1y_2H = x_1Hy_2 = x_2Hy_2 = x_2y_2H$, d'où $x_1y_1{\sim}x_2y_2$. On a donc montré que $\sim$ est compatible à la multiplication de G. Les autres assertions du théorème ont déjà été démontrés. □

5.4 Exemples. 1. Soit n un entier. Alors $n\mathbf{Z}$ est un sous-groupe du groupe (additif) $\mathbf{Z}$. Le groupe quotient $\mathbf{Z}/n\mathbf{Z}$ se décrit comme suite. Pour $n = 0$ c'est l'ensemble $\{\{x\} \mid x \in \mathbf{Z}\}$, muni de l'addition $\{x\}{+}\{y\} = \{x{+}y\}$; on constate que $f: \mathbf{Z} \to \mathbf{Z}/0\mathbf{Z}$, $x \to \{x\}$, est un isomorphisme. Pour $n \neq 0$ c'est l'ensemble $\{\overline{x} \mid 0 \leq x < |n|\}$, où $\overline{x} = \{x + nm \mid m \in \mathbf{Z}\}$, muni de l'addition $\overline{x} + \overline{y} = \overline{z}$ avec z l'unique entier tel que $0 \leq z < |n|$ et $n|(x + y - z)$.
2. Soient G un groupe commutatif et H un sous-groupe de G. Dans ce cas H est automatiquement distingué, donc on peut parler du groupe quotient G/H. Il est clair, d'après la construction de G/H, que G/H est commutatif lui aussi.
3. Soient G un groupe quelconque, et $C \subset G$ son centre: $C = \{x \in G \mid \forall y \in G\colon xy = yx\}$. Le centre C est un sous-groupe distingué de G, donc on peut parler du groupe quotient G/C.
4. Soit G un groupe. Soit $G' \subset G$ le sous-groupe dérivé de de G: G' est le sous-groupe engendré par $\{xyx^{-1}y^{-1} \mid x, y \in G\}$. On montre que G' est un sous-groupe distingué de G et que G/G' est commutatif. Encore mieux: on verra plus loin que, dans un certain sens, G/G' est "le plus grand" groupe quotient commutatif de G.

Une des raisons pour lesquelles les groupes quotients sont utiles est que le calcul dans les groupes quotients simplifie souvent énormément les problèmes qu'on peut se poser sur les groupes et leurs sous-groupes distingués. Par exemple, on sait que le calcul dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ rend facile de voir si certains entiers sont divibles par n ou non. Un autre exemple se trouve dans l'exercice 1 de l'examen du 13 septembre 1993 vers la fin de ce polycopié.

6 Propriétés des groupes quotients.

Les résultats qui suivent permettent souvent de mieux comprendre un groupe quotient.

6.1 Proposition. *Soient G un groupe, $N \subset G$ un sous-groupe distingué, G/N le groupe quotient et $p\colon G \to G/N$ le morphisme canonique. Soient H un groupe et $f\colon G \to H$ un morphisme. Si $N \subset \ker(f)$, il existe un morphisme unique $\overline{f}\colon G/N \to H$ tel que $f = \overline{f}\circ p$, et on a $\ker(\overline{f}) = \{p(x) \mid x\in \ker(f)\} = \{xN \mid x\in \ker(f)\} = \ker(f)/N$. Si par contre $N \not\subset \ker(f)$, il n'y a pas d'application $\overline{f}\colon G/N \to H$ telle que $f = \overline{f}\circ p$.*

Démonstration. Soit $\sim$ la relation d'équivalence sur G donnée par le sous-groupe N. Supposons que $N \subset \ker(f)$. Montrons d'abord que $f\colon G \to H$ est une application qui est compatible avec $\sim$. Soient donc a et b dans G tels que $a \sim b$. Cela signifie qu'il existe c dans N tel que $b = ac$. Notons que $f(c) = e$ car $c \in N \subset \ker(f)$. Alors on a $f(b) = f(ac) = f(a)f(c) = f(a)$. Nous savons donc que f est compatible avec $\sim$. Par définition on a $G/N = G/{\sim}$. La Proposition 3.2 nous dit qu'il existe une application unique $\overline{f}\colon G/N \to H$ telle que $f = \overline{f}\circ p$. Vérifions que $\overline{f}$ est un morphisme. Pour a et b dans G on a: $\overline{f}(\overline{a}\cdot\overline{b}) = \overline{f}(\overline{ab}) = \overline{f}(p(ab)) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b})$. Comme tous les éléments de G/N s'écrivent sous la forme $\overline{x}$, avec $x \in G$, on a montré que $\overline{f}$ est un morphisme.

Supposons maintenant que $N \not\subset \ker(f)$. Cela signifie qu'on peut prendre un élément $x \in N$ tel que $f(x) \neq e_H$. L'existence d'une application $\overline{f}\colon G/N \to H$ telle que $f = \overline{f}\circ p$ entraîne la contradiction suivante: $e_H = f(e_G) = \overline{f}(p(e_G)) = \overline{f}(p(x)) = f(x)$. □

6.2 Proposition. *Soit $f\colon G \to H$ un morphisme. Soit $p\colon G \to G/\ker(f)$ le morphisme canonique. Alors le morphisme $\overline{f}\colon G/\ker(f) \to H$ tel que $\overline{f}\circ p = f$, dont l'existence et l'unicité sont garantis par la Proposition 6.1, est injectif et induit un isomorphisme $\tilde{f}\colon G/\ker(f) \to \mathrm{im}(f)$. Si on note $i\colon \mathrm{im}(f) \to H$ l'inclusion, on peut écrire $f = i\circ\tilde{f}\circ p$, où p est un morphisme surjectif, $\tilde{f}$ est un isomorphisme et i est un morphisme injectif.*

Démonstration. Il suffit de montrer que $\overline{f}$ est injectif et que $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. D'après la Proposition 6.1, le noyau de $\overline{f}$ est trivial, donc $\overline{f}$ est injectif. Comme p est surjectif on a $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$. □

6.3 Définition. *Si G est un groupe, $A \subset G$ et $B \subset G$ des sous-ensembles, on note $AB = \{ab \mid a\in A,\, b\in B\}$.*

6.4 Lemme. *Soient $f\colon G_1 \to G_2$ un morphisme et $H \subset G_1$ un sous-groupe. Alors $f^{-1}fH = \ker(f)H = H\ker(f)$.*

Démonstration. Montrons d'abord la première égalité. Pour $x \in \ker(f)$ et $y \in H$ on a $f(xy) = f(x)f(y) = f(y) \in fH$, d'où $\ker(f)H \subset f^{-1}fH$. Montrons maintenant que $f^{-1}fH \subset \ker(f)H$. Pour $x \in f^{-1}fH$ on a $f(x) \in fH$, donc on peut prendre $y \in H$ tel que $f(x) = f(y)$. Pour un tel y, on a $f(xy^{-1}) = e_2$, d'où $xy^{-1} \in \ker(f)$. Ceci montre que $x = (xy^{-1})y \in \ker(f)H$. La deuxième égalité se démontre de la même façon, ou en utilisant que $\ker(f)$ est distingué. □

6.5 Proposition. *Soit $f: G_1 \to G_2$ un morphisme surjectif. Soit X_1 l'ensemble des sous-groupes H_1 de G_1 tels que $H_1 \supset \ker(f)$. Soit X_2 l'ensemble des sous-groupes de G_2. Alors les applications $\alpha: X_1 \to X_2$ et $\beta: X_2 \to X_1$ données par $\alpha: H_1 \mapsto fH_1$ et $\beta: H_2 \mapsto f^{-1}H_2$ sont des applications inverses. En plus, ces bijections entre X_1 et X_2 préservent les sous-groupes distingués.*

Démonstration. Montrons que $\beta \circ \alpha = \mathrm{id}_{X_1}$. Pour $H_1 \in X_1$ on a $\beta(\alpha(H_1)) = f^{-1}fH_1 = \ker(f)H_1$ (d'après le lemme 6.4), et comme $\ker(f) \subset H_1$, $\ker(f)H_1 = H_1$.

Montrons que $\alpha \circ \beta = \mathrm{id}_{X_2}$. Soit $H_2 \in X_2$. Alors $\alpha(\beta(H_2)) = ff^{-1}H_2$. Comme f est une application surjective on a $ff^{-1}H_2 = H_2$.

Soient $H_1 \in X_1$ et $H_2 \in X_2$ tels que $H_2 = \alpha(H_1)$ et donc $H_1 = \beta(H_2)$. Supposons que H_1 est distingué et montrons que H_2 l'est aussi. Soient donc $x \in G_2$ et $h_2 \in H_2$. Comme f est surjectif on peut prendre $y \in G_1$ et $h_1 \in H_1$ tels que $x = f(y)$ et $h_2 = f(h_1)$. Alors on a $xh_2x^{-1} = f(y)f(h_1)f(y)^{-1} = f(yh_1y^{-1}) \in f(H_1) = H_2$. Supposons maintenant que H_2 est distingué. Alors $H_1 = f^{-1}H_2 = \ker(p_2 \circ f)$, où $p_2: G_2 \to G_2/H_2$ est le morphisme canonique. □

6.6 Remarque. *Soient G un groupe et $N \subset G$ un sous-groupe distingué. La Proposition 6.5, appliqué au morphisme canonique $p: G \to G/N$, fournit une bijection entre l'ensemble des sous-groupes de G/N et l'ensemble des sous-groupes de G contenant N.*

6.7 Proposition. *Soient G un groupe, $N \subset G$ un sous-groupe distingué et $H \subset G$ un sous-groupe. Alors $NH = \{ab \mid a \in N,\, b \in H\} = \{ba \mid a \in N,\, b \in H\} = HN$ est un sous-groupe de G, N est un sous-groupe distingué de NH et $N \cap H$ est un sous-groupe distingué de H. Il existe un isomorphisme $f: NH/N \to H/N \cap H$ tel que $f(abN) = b(N \cap H)$ pour tout $a \in N$, $b \in H$.*

Démonstration. Notons $p: G \to G/N$ le morphisme canonique et $i: H \to G$ l'inclusion. Alors $p \circ i: H \to G/N$ est un morphisme, $\ker(p \circ i) = N \cap H$ et $\mathrm{im}(p \circ i) = pH$. La Proposition 6.2 nous fournit un isomorphisme $g: H/N \cap H \to pH$ tel que $g(b(N \cap H)) = p(b)$ pour tout $b \in H$.

Le Lemme 6.4 montre que $p^{-1}pH = NH = HN$. Notons $j: NH \to G$ l'inclusion. Alors $p \circ j: NH \to G/N$ est un morphisme, $\ker(p \circ j) = N$ et $\mathrm{im}(p \circ j) = pH$. La Proposition 6.2 nous fournit un isomorphisme $h: NH/N \to pH$ tel que $h(abN) = p(b)$ pour tout $b \in H$ et $a \in N$. L'isomorphisme f cherché est $g^{-1} \circ h$. □

6.8 Proposition. *Soient G un groupe, H et K des sous-groupes distingués de G tels que $K \subset H$. Alors H/K est un sous-groupe distingué de G/K et il existe un isomorphisme $f: (G/K)/(H/K) \to G/H$ tel que $f \circ p_{H/K} \circ p_K = p_H$, où $p_{H/K}: G/K \to (G/K)/(H/K)$, $p_K: G \to G/K$ et $p_H: G \to G/H$ sont les morphismes canoniques.*

Démonstration. La Proposition 6.1 affirme qu'il existe un morphisme $g: G/K \to G/H$ tel que $g \circ p_K = p_H$, et que $\ker(g) = H/K$. Alors H/K est un sous-groupe distingué de G/K. La Proposition 6.2, appliquée à g, dit qu'il existe un isomorphisme $\tilde{g}: (G/K)/(H/K) \to G/H$; c'est l'isomorphisme cherché. □

7 Groupes cycliques.

On appelle un groupe G cyclique s'il peut être engendré par un seul élément, c'est à dire, s'il existe $a \in G$ tel que $G = \langle a \rangle$. Dans cette section nous allons classifier les groupes cycliques, les morphismes entre eux et leurs sous-groupes.

Supposons que G est un groupe cyclique et que a est un générateur: $G = \langle a \rangle$. Nous avons alors un morphisme surjectif $f_a\colon \mathbf{Z} \to G\colon n \mapsto a^n$. Le sous-groupe $\ker(f_a)$ de $\mathbf{Z}$ est de la forme $n\mathbf{Z}$ pour un unique $n \geq 0$; si a est d'ordre fini on a $n = \mathrm{ordre}(a)$, et si a est d'ordre infini on a $n = 0$. La Proposition 6.2 fournit un isomorphisme $\tilde{f}_a\colon \mathbf{Z}/n\mathbf{Z} \to G$. On voit donc qu'un groupe cyclique infini est isomorphe à $\mathbf{Z}$, et qu'un groupe cyclique fini d'ordre n est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

Passons maintenant à la classification des morphismes entre deux groupes cycliques. Comme tout groupe cyclique est isomorphe à un unique groupe de la forme $\mathbf{Z}/n\mathbf{Z}$ avec $n \geq 0$, il suffit de trouver les morphismes $f\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$, pour $n \geq 0$ et $m \geq 0$. Comme nous avons affaire à différentes sortes de classes d'équivalence, nous notons, pour $a \in \mathbf{Z}$, $\overline{a}_n$ sa classe dans $\mathbf{Z}/n\mathbf{Z}$. Supposons que $f\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ soit un morphisme. Alors $f(\overline{1}_n) \in \mathbf{Z}/m\mathbf{Z}$ satisfait à $n{\cdot}f(\overline{1}_n) = f(\overline{n}_n) = f(\overline{0}_n) = \overline{0}_m$. Cette construction nous donne une application:

$$(7.1) \qquad \mathrm{Hom}(\mathbf{Z}/n\mathbf{Z},\, \mathbf{Z}/m\mathbf{Z}) \longrightarrow \{x \in \mathbf{Z}/m\mathbf{Z} \mid n{\cdot}x = \overline{0}_m\}, \qquad f \mapsto f(\overline{1}_n)$$

Comme $\mathbf{Z}$ est engendré par l'élément 1, l'application (7.1) est injective. Nous allons vérifier qu'elle est aussi surjective. Supposons donc que $x \in \mathbf{Z}/m\mathbf{Z}$ et que $n{\cdot}x = \overline{0}_m$. Alors on a un unique morphisme $f\colon \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ tel que $f(1) = x$. Comme $n{\cdot}x = \overline{0}_m$ on a $n\mathbf{Z} \subset \ker(f)$. D'après la Proposition 6.1 il existe alors un morphisme $\overline{f}\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ tel que $\overline{f}(\overline{a}_n) = f(a) = a{\cdot}x$ pour tout $a \in \mathbf{Z}$. En prenant $a = 1$ on voit que x est l'image de $\overline{f}$ sous l'application (7.1). Nous avons donc montré que (7.1) est une bijection.

L'application inverse de (7.1) peut s'expliciter comme suite:

$$(7.2) \qquad \{x \in \mathbf{Z}/m\mathbf{Z} \mid n{\cdot}x = \overline{0}_m\} \longrightarrow \mathrm{Hom}(\mathbf{Z}/n\mathbf{Z},\, \mathbf{Z}/m\mathbf{Z}), \qquad \overline{x}_m \mapsto (\overline{a}_n \mapsto \overline{xa}_m)$$

On vérifie que sous (7.1) la composition de morphismes correspond à la multiplication. En prenant $m = n$ on constate alors que sous (7.1) les automorphismes de $\mathbf{Z}/n\mathbf{Z}$ correspondent à des $x \in \mathbf{Z}/n\mathbf{Z}$ tel qu'il existe $y \in \mathbf{Z}/n\mathbf{Z}$ avec $xy = \overline{1}_n$. Autrement dit, on trouve que:

$$(7.3) \qquad \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*, \qquad f \mapsto f(\overline{1}_n)$$

est un isomorphisme.

Finalement, classifions les sous-groupes des groupes cycliques. D'après la Proposition 6.5, les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ correspondent a des sous-groupes de $\mathbf{Z}$ qui contiennent $n\mathbf{Z}$. On a déjà vu que les sous-groupes de $\mathbf{Z}$ sont de la forme $d\mathbf{Z}$ avec $d \geq 0$. On vérifie que $d\mathbf{Z} \supset n\mathbf{Z}$ si et seulement si $d|n$. Nous voyons donc que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont les groupes $\langle \overline{d}_n \rangle$, pour $0 \leq d|n$. Noter que ces sous-groupes sont tous cycliques. On a trouvé que si G est cyclique d'ordre n, alors pour tout $d|n$ avec $d \geq 1$, G a exactement un sous-groupe d'ordre d et que ce sous-groupe est cyclique.

8 Isométries.

8.1 Définition. *Soit X un ensemble. Une métrique, aussi appelée une (fonction) distance, sur X est une fonction $d: X \times X \to \mathbf{R}$ telle que:*

1: pour tout x et y dans X on a $d(x, y) \geq 0$,

2: pour tout x et y dans X on a $d(x, y) = d(y, x)$,

3: pour x et y dans X on a $d(x, y) = 0$ si et seulement si $x = y$,

4: pour tout x, y et z dans X on a $d(x, z) \leq d(x, y) + d(y, z)$. (inégalité du triangle.)

Un espace métrique est un couple (X, d), où X est un ensemble et d une distance sur X.

8.2 Exemples. 1. Soit $X := \mathbf{R}^n$. Pour $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, \cdots, y_n)$ dans $\mathbf{R}^n$ notons par $\langle x, y \rangle := x_1 y_1 + \cdots + x_n y_n$ le produit scalaire usuelle de x et y. Soit $\|\cdot\|: \mathbf{R}^n \to \mathbf{R}$ la norme associée à $\langle \cdot, \cdot \rangle$: pour x dans $\mathbf{R}^n$ on a $\|x\| = \langle x, x \rangle^{1/2}$. Alors la distance usuelle d sur $\mathbf{R}^n$ donnée par $d(x, y) = \|x - y\|$ est une métrique sur $\mathbf{R}^n$.

2. Soit S un ensemble. Soit

$$B(S, \mathbf{R}) := \{f: S \to \mathbf{R} \mid \exists b \in \mathbf{R} \text{ tel que } \forall x \in S \text{ on a } |f(x)| \leq b\}$$

l'ensemble des fonctions bornées sur S à valeurs dans $\mathbf{R}$. Soit $\|\cdot\|_{\sup}: B(S, \mathbf{R}) \to \mathbf{R}$ la norme sup: $\|f\|_{\sup} = \sup\{|f(x)| \mid x \in S\}$. Alors la fonction $d: B(S, \mathbf{R}) \to \mathbf{R}$ donnée par $d(f, g) = \|f - g\|_{\sup}$ est une métrique.

8.3 Définition. *Soient (X, d) et (X', d') deux espaces métriques. Un morphisme d'espaces métriques de X vers X' est alors une application $f: X \to X'$ telle que pour tout x et y dans X on a $d'(f(x), f(y)) = d(x, y)$, ou autrement dit, une application qui préserve les distances. Une isométrie de X vers X' est une bijection $f: X \to X'$ qui préserve les distances.*

On vérifie tout de suite que l'application inverse d'une isométrie est encore une isométrie. Ceci entraîne la proposition suivante, dont la démonstration est laissée au lecteur.

8.4 Proposition. *Soit (X, d) un espace métrique. Alors le sous-ensemble des isométries de* $\mathrm{Sym}(X)$ *est un sous-groupe. On l'appelle groupe d'isométries de X et on le note* $\mathrm{Iso}(X, d)$. □

8.5 Exemple. Considérons $\mathbf{R}^n$ avec sa distance usuelle d. Pour v dans $\mathbf{R}^n$ notons $t_v: \mathbf{R}^n \to \mathbf{R}^n$: $x \mapsto v + x$ la translation par v. Comme pour tout v, x et y dans $\mathbf{R}^n$ on a

$$d(t_v(x), t_v(y)) = \|t_v(x) - t_v(y)\| = \|(v + x) - (v + y)\| = \|x - y\| = d(x, y),$$

ces translations sont toutes des isométries de $\mathbf{R}^n$. Notons que $t_0 = \mathrm{id}_{\mathbf{R}^n}$, que $t_v \circ t_w = t_{v+w}$ et que $t_v^{-1} = t_{-v}$. Ceci signifie que l'ensemble des translations $\{t_v \mid v \in \mathbf{R}^n\}$ est un sous-groupe de $\mathrm{Iso}(\mathbf{R}^n)$, isomorphe au groupe $(\mathbf{R}^n, +, 0)$.

Notons par $\mathrm{O}_n(\mathbf{R})$ l'ensemble des applications linéaires orthogonales $g: \mathbf{R}^n \to \mathbf{R}^n$. Rappelons qu'une application linéaire $g: \mathbf{R}^n \to \mathbf{R}^n$ est orthogonale si pour tout x et y dans $\mathbf{R}^n$ on a $\langle g(x), g(y) \rangle = \langle x, y \rangle$ et que la matrice par rapport à une base orthonormale d'une application linéaire orthogonale est une matrice orthogonale, c'est à dire, une matrice A de type (n, n) telle que la transposée de A est l'inverse de A. On vérifie tout de suite que $\mathrm{O}_n(\mathbf{R})$ est un sous-groupe de $\mathrm{Iso}(\mathbf{R}^n)$. Nous verrons plus loin, dans la section 14, que le théorème suivant dit que $\mathrm{Iso}(\mathbf{R}^n)$ est ce qu'on appelle un produit semi-direct de $\mathrm{O}_n(\mathbf{R})$ par $\mathbf{R}^n$.

8.6 Théorème. *Considérons $\mathbf{R}^n$ avec sa distance usuelle. Alors pour tout f dans $\mathrm{Iso}(\mathbf{R}^n)$ il existe un unique v dans $\mathbf{R}^n$ et un unique g dans $\mathrm{O}_n(\mathbf{R})$ tels que $f = t_v \circ g$.*

Démonstration. Soit f dans $\mathrm{Iso}(\mathbf{R}^n)$. Nous cherchons maintenant v et g comme dans l'énoncé du théorème. Alors on doit avoir $f(0) = (t_v \circ g)(0) = t_v(g(0)) = t_v(0) = v$. Ceci veut dire que nous sommes bien contraints de prendre $v := f(0)$. Soit donc $g := t_v^{-1} \circ f$. Alors g est un élément de $\mathrm{Iso}(\mathbf{R}^n)$ tel que $g(0) = 0$. Nous allons montrer qu'en fait g est dans $\mathrm{O}_n(\mathbf{R})$, ce qui achèvera la démonstration.

Notons d'abord que pour tout x dans $\mathbf{R}^n$ nous avons $\|g(x)\| = d(g(x), 0) = d(g(x), g(0)) = d(x, 0) = \|x\|$. Pour tout x et y dans $\mathbf{R}^n$ on a:

$$\begin{aligned} d(g(x), g(y))^2 &= \|g(x) - g(y)\|^2 = \langle g(x) - g(y), g(x) - g(y)\rangle = \\ &= \|g(x)\|^2 + \|g(y)\|^2 - 2\langle g(x), g(y)\rangle = \|x\|^2 + \|y\|^2 - 2\langle g(x), g(y)\rangle, \end{aligned}$$

mais aussi:

$$d(g(x), g(y))^2 = d(x, y)^2 = \|x - y\|^2 = \langle x - y, x - y\rangle = \|x\|^2 + \|y\|^2 - 2\langle x, y\rangle.$$

La conclusion est que $\langle g(x), g(y)\rangle = \langle x, y\rangle$ pour tout x et y.

Soit $e = (e_1, e_2, \ldots, e_n)$ la base orthonormale usuelle de $\mathbf{R}^n$. D'après ce qu'on vient de montrer, $(g(e_1), \ldots, g(e_n))$ est une base orthonormale de $\mathbf{R}^n$. Il existe un unique élément h dans $\mathrm{O}_n(\mathbf{R})$ tel que $h(e_i) = g(e_i)$ pour tout i. Posons $k := h^{-1}g$. Alors k est un élément de $\mathrm{Iso}(\mathbf{R}^n)$ avec la propriété que $k(0) = 0$ et $k(e_i) = e_i$ pour tout i. Le Corollaire 8.8 montre que $k = \mathrm{id}$, d'où $g \in \mathrm{O}_n(\mathbf{R})$. Une façon plus simple de finir la démonstration, sans utiliser ce corollaire, est la suivante: pour tout $x = (x_1, \ldots, x_n)$ dans $\mathbf{R}^n$ et tout i tel que $1 \leq i \leq n$ on a $\langle k(x), e_i\rangle = \langle k(x), k(e_i)\rangle = \langle x, e_i\rangle = x_i$, ce qui montre que $k(x) = (x_1, \ldots, x_n)$. □

8.7 Lemme. *Soient $x_0, x_1, \ldots, x_n$ dans $\mathbf{R}^n$ $n+1$ points qui ne sont pas contenus dans un hyperplan, ou autrement dit, tels que les différences $x_i - x_j$ engendrent $\mathbf{R}^n$ comme $\mathbf{R}$-espace vectoriel. Si y et z dans $\mathbf{R}^n$ sont tels que $d(y, x_i) = d(z, x_i)$ pour tout i, alors $y = z$.*

Démonstration. Supposons que $y \neq z$. Soit H le sous-ensemble de $\mathbf{R}^n$ formé des points x tels que $d(y, x) = d(z, x)$. Alors H est l'hyperplan médian de y et z, ce qui veut dire:

$$H = \frac{1}{2}(y + z) \ + \ (z - y)^{\perp}.$$

Comme H contient tous les x_i $(0 \leq i \leq n)$, on a une contradiction avec l'hypothèse que les x_i ne sont pas contenus dans un hyperplan. On a donc $y = z$. □

8.8 Corollaire. *Soient $x_0, x_1, \ldots, x_n$ dans $\mathbf{R}^n$ $n+1$ points qui ne sont pas contenus dans un hyperplan. Soit g dans $\mathrm{Iso}(\mathbf{R}^n)$ tel que $g(x_i) = x_i$ pour tout i. Alors $g = \mathrm{id}_{\mathbf{R}^n}$.*

Démonstration. Soit $y \in \mathbf{R}^n$. Pour tout i on a $d(g(y), x_i) = d(g(y), g(x_i)) = d(y, x_i)$, donc le Lemme 8.7 affirme que $g(y) = y$. □

Soit maintenant X un sous-ensemble de $\mathbf{R}^n$. On notera par d la distance usuelle sur $\mathbf{R}^n$, ainsi que sa restriction à X. Nous allons étudier la relation entre les groupes d'isométries des deux espaces métriques $(\mathbf{R}^n, d)$ et (X, d). Le groupe $\mathrm{Iso}(\mathbf{R}^n)$ agit sur l'ensemble $\{Y \subset \mathbf{R}^n\}$ des sous-ensembles de $\mathbf{R}^n$ par la formule $g{\cdot}Y = \{g(x) \mid x \in Y\}$. Comme d'habitude, on note par $\mathrm{Iso}(\mathbf{R}^n)_X$ le stabilisateur de X. Si g appartient à $\mathrm{Iso}(\mathbf{R}^n)_X$, alors sa restriction $g|_X\colon X \to X$ à X est une isométrie. Cette construction nous donne un morphisme de groupes

$$\phi\colon \mathrm{Iso}(\mathbf{R}^n)_X \longrightarrow \mathrm{Iso}(X), \quad g \mapsto g|_X \tag{8.9}$$

8.10 Théorème. *Le morphisme ϕ de (8.9) est surjectif. Autrement dit: pour X un sous-ensemble de $\mathbf{R}^n$, muni de la distance de $\mathbf{R}^n$, tout élément de* $\mathrm{Iso}(X)$ *est restriction d'un élément de* $\mathrm{Iso}(\mathbf{R}^n)$.

Démonstration. Si $X = \emptyset$ c'est clair, donc supposons que X est non-vide. Soit x_0 dans X. Soit F le sous-epace vectoriel de $\mathbf{R}^n$ engendré par l'ensemble $\{x - x_0 \mid x \in X\}$. Soit $r := \dim(F)$. Prenons $x_1, \ldots, x_r$ dans X tel que $(x_1 - x_0, \ldots, x_r - x_0)$ est une base de F. Soit g dans $\mathrm{Iso}(X)$ et posons $y_i := g(x_i)$ pour $0 \leq i \leq r$. Nous allons d'abord montrer qu'il existe un élément h de $\mathrm{Iso}(\mathbf{R}^n)$ tel que $h(x_i) = y_i$ pour tout i, ensuite nous montrerons que $g = \phi(h)$.

La construction de h est faite en étapes. Soit $h_0 := t_{y_0 - x_0}$ la translation par $y_0 - x_0$. On a bien $h_0(x_0) = y_0$. Supposons maintenant que pour un j avec $0 \leq j < r$ nous avons h_j dans $\mathrm{Iso}(\mathbf{R}^n)$ tel que $h_j(x_i) = y_i$ pour $0 \leq i \leq j$. Si par hasard $h_j(x_{j+1}) = y_{j+1}$ on pose $h_{j+1} := h_j$. Supposons donc que $h_j(x_{j+1}) \neq y_{j+1}$. Soit s dans $\mathrm{Iso}(\mathbf{R}^n)$ la symétrie par rapport au hyperplan médian de $h_j(x_{j+1})$ et y_{j+1} . Notons que pour $0 \leq i \leq j$ on a

$$d(y_i, y_{j+1}) = d(g(x_i), g(x_{j+1})) = d(x_i, x_{j+1}) = d(h_j(x_i), h_j(x_{j+1})) = d(y_i, h_j(x_{j+1}))$$

d'où on conclut que $s(y_i) = y_i$. Posons $h_{j+1} := s {\circ} h_j$. On a alors $h_{j+1}(x_{j+1}) = y_{j+1}$ et $h_{j+1}(x_i) = s(y_i) = y_i$ pour $i \leq j$. L'élément h_r de $\mathrm{Iso}(\mathbf{R}^n)$ construit ainsi par récurrence a donc la propriété que $h_r(x_i) = y_i$ pour tout i, donc on pose $h := h_r$.

Pour montrer que $g = \phi(h)$, il suffit de montrer que $g(x) = h(x)$ pour tout x dans X. Soit alors x dans X. Comme $g(x)$ appartient à X, on a $g(x) - x \in F$. De la construction de h, on voit que h est le composé d'une translation par une application linéaire orthogonale (cela résulte aussi du Thm. 8.6). Comme $x - x_0$ est une combinaison linéraire de $x_1 - x_0, \ldots, x_r - x_0$, il en résulte que $h(x) - x$ est une combinaison linéaire de $h(x_1) - h(x_0), \ldots, h(x_r) - h(x_0)$, ce qui montre que $h(x) - x$ appartient à F. Le fait que pour $0 \leq i \leq r$, $h(x)$ et $g(x)$ ont même distance à x_i entraîne que $g(x) - h(x)$, qui est dans F, est orthogonale aux $x_1 - x_0, \ldots, x_r - x_0$. Comme ces derniers forment une base de F, on doit avoir $g(x) = h(x)$. □

9 Groupes diédraux et polyèdres réguliers.

Dans cette section nous étudions les groupes d'isométries des polygones réguliers dans $\mathbf{R}^2$ et des cinq polyèdres reguliers dans $\mathbf{R}^3$. Pour l'instant nous ne tentons pas de donner une définition rigoureuse de ce que c'est un polyèdre régulier dans $\mathbf{R}^3$, mais nous présentons plutôt les cinq seuls cas qui existent (le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre). Après cela nous donnerons des définitions rigoureuses, et quelques arguments pourquoi il n'existe pas d'autres polyèdres réguliers dans $\mathbf{R}^3$. Pour un traitement plus rigoureux des polyèdres réguliers nous conseillons les intéressés de voir les chapitres 1 et 12 de la série de livres "Géométrie" de M. Berger, parue chez l'éditeur Cedic/Fernand Nathan.

9.1 Groupes diédraux.

Soit $n \geq 3$. Pour $k \in \mathbf{Z}/n\mathbf{Z}$ notons $x_k = (\cos(2\tilde{k}\pi/n), \sin(2\tilde{k}\pi/n)) \in \mathbf{R}^2$, où $\tilde{k} \in \mathbf{Z}$ et $k = \tilde{k} \bmod n$. Le sous-ensemble $X = \{x_k \mid k \in \mathbf{Z}/n\mathbf{Z}\}$ de $\mathbf{R}^2$ est alors l'ensemble des sommets d'un n-gone régulier. Notons par d la distance de $\mathbf{R}^2$, ainsi que sa restriction à X. On définit alors le groupe dihédral D_n comme étant le groupe $\mathrm{Iso}(X)$ d'isométries de X, où X est muni de la distance d. La rotation de $\mathbf{R}^2$ de $2\pi/n$ est dans $\mathrm{Iso}(\mathbf{R}^2)$ et envoie x_k sur x_{k+1}, donc induit une isométrie de X; notons par ρ cet élément de D_n. D'autre part la symétrie par rapport à la droite $\{(x, 0) \mid x \in \mathbf{R}\}$ et dans $\mathrm{Iso}(\mathbf{R}^2)$ et envoie x_k sur x_{-k}, donc induit une isométrie de X; notons par σ cet élément de D_n. Le sous-groupe $\langle\rho\rangle$ de D_n opère transitivement sur X, donc D_n aussi.

Déterminons le stabilisateur D_{n,x_0} de x_0. Supposons que $f \in D_n$ et $f(x_0) = x_0$. Alors $f(x_1) = x_1$ ou $f(x_1) = x_{-1}$, comme x_{-1} et x_1 sont les seuls des x_k tel que $d(x_k, x_0) = d(x_1, x_0)$. Dans le premier cas on pose $g = f$, dans le deuxième cas on pose $g = \sigma f$. Dans les deux cas on a $g(x_0) = x_0$, $g(x_1) = x_1$ et $g(x_{-1}) = x_{-1}$. Comme $g \in D_n$ on doit avoir, pour tout $x \in X$, et pour $k \in \{\overline{0}, \overline{-1}, \overline{1}\}$: $d(g(x), x_k) = d(g(x), g(x_k)) = d(x, x_k)$. On sait que pour trois points non collinéaires de $\mathbf{R}^2$, un point de $\mathbf{R}^2$ est déterminé par ses distances à ces trois points (voir le Lemme 8.7). Cela entraîne qu'on doit avoir $g(x) = x$ pour tout $x \in X$, ou encore, que $g = \mathrm{id}_X$.

On a donc démontré que $D_{n,x_0} = \{\mathrm{id}_X, \sigma\}$. Ceci nous permet aussi de calculer l'ordre de D_n: le Théorème 4.5 dit que $|X| = |D_n/D_{n,x_0}| = |D_n|/|D_{n,x_0}|$, d'où on tire: $|D_n| = 2n$. En plus le Théorème 4.5, partie 2 dit que $D_{n,x_k} = D_{n,\rho^k(x_0)} = \rho^k D_{n,x_0}\rho^{-k} = \{\mathrm{id}_X, \rho^k\sigma\rho^{-k}\}$.

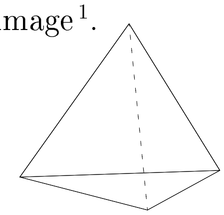
Le sous-groupe $\langle\rho\rangle$ de D_n est d'ordre n. Comme $[D_n : \langle\rho\rangle] = 2$ et $\sigma \notin \langle\rho\rangle$, on a $D_n = \langle\rho, \sigma\rangle$. Les éléments de D_n s'écrivent de façon unique sous la forme $\rho^a\sigma^b$ avec $0 \leq a < n$, $0 \leq b < 2$. Le calcul $(\sigma\rho\sigma)(x_k) = (\sigma\rho)(x_{-k}) = \sigma(x_{1-k}) = x_{k-1}$ montre que $\sigma\rho\sigma = \rho^{-1}$, d'où $\sigma\rho = \rho^{-1}\sigma$. En général on a:

$$(\rho^a\sigma^b)(\rho^c\sigma^d) = \rho^a\sigma^b\rho^c\sigma^b\sigma^{b+d} = \rho^a(\sigma^b\rho\sigma^{-b})^c\sigma^{b+d} = \rho^a\rho^{(-1)^b c}\sigma^{b+d} = \rho^{a+(-1)^b c}\sigma^{b+d}$$

On verra dans le section 14 que D_n est ce qu'on appelle un produit semi-direct de $\langle\rho\rangle$ et $\langle\sigma\rangle$.

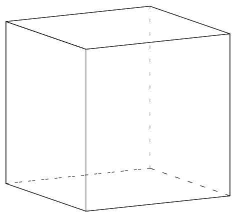
9.2 Le groupe du tétraèdre.

Considérons le sous-ensemble $X := \{(-1,-1,-1),\ (-1,1,1),\ (1,-1,1),\ (1,1,-1)\}$ de $\mathbf{R}^3$. Notons que la distance entre deux éléments distincts de X est toujours $\sqrt{8}$, ce qui montre que X est l'ensemble des sommets d'un tétraèdre régulier, dont voici à côté une image[1]. Nous définissons le groupe G "du tétraèdre" comme étant le groupe $\mathrm{Iso}(X)$ d'isométries de X. Il est facile de voir, en notant que toutes les permutations de X sont induites par des isométries, que G est égal à $\mathrm{Sym}(X)$. Le groupe G est donc isomorphe au groupe symétrique S_4.



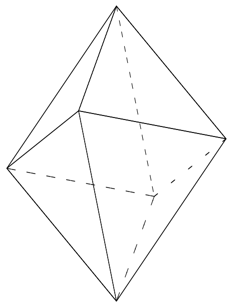
9.3 Le groupe du cube.

Considérons le sous-ensemble $X := (\pm 1, \pm 1, \pm 1)$ de $\mathbf{R}^3$. Notons que X est l'ensemble des huit sommets d'un cube, dont on trouve une image à côté. Soit G le groupe d'isométries de X ; on l'appelle le "groupe du cube". Dans les exercices on montrera que $|G| = 48$ et que G est isomorphe à $\mathrm{S}_4 \times \mathbf{Z}/2\mathbf{Z}$, et aussi à un produit semi-direct (voir section 14 pour cette notion) de $(\mathbf{Z}/2\mathbf{Z})^3$ par S_3.



9.4 Le groupe de l'octaèdre.

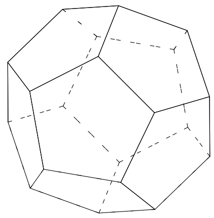
Considérons le sous-ensemble $X := \{(\pm 1, 0, 0),\ (0, \pm 1, 0),\ (0, 0, \pm 1)\}$ de $\mathbf{R}^3$. C'est l'ensemble des six sommets d'un octaèdre régulier, dont on trouve une image à côté. Soit G le groupe d'isométries de X ; on l'appelle groupe de l'octaèdre. Comme l'octaèdre est le "dual" du cube (ses sommets sont les barycentres des faces du cube et les sommets du cube sont les barycentres des faces de l'octaèdre), les groupes du cube et de l'octaèdre sont isomorphes.



En fait, avec les plongements dans $\mathbf{R}^3$ que nous avons choisis, les isométries du cube et du octaèdre sont induites par exactement les mêmes isométries de $\mathbf{R}^3$.

9.5 Le groupe du dodécaèdre.

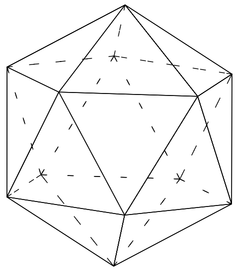
A côté on a une image d'un dodécaèdre. On démontrera un peu plus loin qu'il existe vraiment un polyèdre régulier dans $\mathbf{R}^3$ dont les douze faces sont des 5-gones réguliers. En fait, nous démontrerons de deux façons l'existence de l'icosaèdre et ensuite par "dualité" nous en déduirons l'existence du dodécaèdre. Pour l'instant nous demandons au lecteur de bien vouloir admetttre l'existence du dodécaèdre.



1. Les fichiers PostScript qui décrivent les cinq images du §9 ont été construits par R. Noot à l'aide du logiciel Maple.

Le dodécaèdre a donc douze faces, vingt sommets et trente arêtes. Soit X l'ensemble de ses sommets, et G le groupe d'isométries de X. On montre assez facilement que $|G| = 120$ et moins facilement que G est isomorphe à $\mathrm{A}_5 \times \mathbf{Z}/2\mathbf{Z}$ (voir les exercices).

9.6 Le groupe de l'icosaèdre.



A côté on a une image d'un icosaèdre: c'est un polyèdre régulier dont les vingt faces sont des triangles réguliers dont, en chacun des douze sommets, cinq se rencontrent. Le nombre d'arêtes est trente. Comme l'icosaèdre est le dual du dodécaèdre, son groupe d'isométries est le même que celui du dodécaèdre, donc isomorphe à $\mathrm{A}_5 \times \mathbf{Z}/2\mathbf{Z}$.

Nous démontrons l'existence de l'icosaèdre de deux façons. La première démonstration est assez brutale. Soit $\tau := (1+\sqrt{5})/2$ le nombre de Fibonacci; on a donc $\tau^2-\tau-1 = 0$. Considérons le sous-ensemble X de $\mathbf{R}^3$ consistant des douze points $(0, \pm1, \pm\tau)$, $(\pm\tau, 0, \pm1)$ et $(\pm1, \pm\tau, 0)$. On vérifie en calculant que la distance la plus courte qui sépare deux éléments distincts de X est 2 et que pour chaque élément de X il y a exactement 5 éléments de X qui sont à distance 2. Pour arêtes on prend les segments qui joignent deux éléments de X qui ont distance 2. Encore en faisant des calculs on vérifie que pour chaque élément de X, ces 5 voisins et les arêtes qui les joignent forment un 5-gone régulier. Il est alors clair que les faces de l'enveloppe convexe (voir la Section 9.7 pour la définition) de X sont des triangles réguliers, que X est l'ensemble des sommets de cette enveloppe convexe et qu'en chaque sommet 5 de ces triangles se rencontrent.

La deuxième démonstration de l'existence de l'icosaèdre est plus géométrique et moins calculatoire. On considère d'abord le 10-gone régulier dans le plan d'équation $z = 0$ de $\mathbf{R}^3$, dont les sommets sont les points $(\cos(2k\pi/10), \sin(2k\pi/10), 0)$ avec k dans $\mathbf{Z}$. Noter que les points $(\cos(2k\pi/10), \sin(2k\pi/10), 0)$ avec k pair forment un 5-gone régulier dont les côtés ont longueur $r := 2\sin(\pi/5)$, ainsi que les points $(\cos(2k\pi/10), \sin(2k\pi/10), 0)$ avec k impair. Il est clair qu'il existe un $s > 0$ unique dans $\mathbf{R}$ tel que pour tout k pair, les distances de $P_k := (\cos(2k\pi/10), \sin(2k\pi/10), s)$ à $P_{k+1} := (\cos(2(k+1)\pi/10), \sin(2(k+1)\pi/10), 0)$ et à $P_{k-1} := (\cos(2(k-1)\pi/10), \sin(2(k-1)\pi/10), 0)$ sont toutes les deux égales à r. On peut bien sûr calculer la valeur de s, mais nous n'en aurons pas besoin. L'enveloppe convexe de l'ensemble des dix P_k est un "tambour" dont les faces sont les dix triangles réguliers (P_k, P_{k+1}, P_{k+2}) et les deux 5-gones réguliers $(P_1, P_3, P_5, P_7, P_9)$ et $(P_2, P_4, P_6, P_8, P_{10})$. Pour obtenir un icosaèdre, il suffit d'ajouter un point $P_{11} := (0, 0, t)$ avec $t > 0$ bien choisi, et un point $P_{12} := (0, 0, u)$ avec $u < 0$ bien choisi. Alors les vingt faces sont toutes des triangles réguliers avec des côtés de longueur r, dont en chacun des douze sommets 5 se rencontrent. Ce serait un bon exercice de géométrie de calculer s, t et u.

Pour obtenir un dodécaèdre on procède comme suit. On prend un icosaèdre. L'enveloppe convexe de l'ensemble des barycentres des faces de l'icosaèdre est alors un dodécaèdre. Les sommets de ce dodécaèdre sont donc les douze barycentres des faces de l'icosaèdre. Les arêtes sont les segment qui joignent les barycentres des couples de faces distinctes de l'icosaèdre qui ont un côté en commun.

9.7 Définitions rigoureuses.

Rappelons qu'un sous-ensemble convexe d'un $\mathbf{R}$-espace vectoriel E est un sous-ensemble X de E tel que pour tout x et y dans E, le segment qui joint x et y est contenu dans X. Autrement dit, si X contient x et y, X contient tous les points $\lambda x+\mu y$ avec $\lambda+\mu=1$, $\lambda\geq 0$ et $\mu\geq 0$. Pour X un sous-ensemble d'un $\mathbf{R}$-espace vectoriel, l'enveloppe convexe $\langle X\rangle$ de X est le plus petit ensemble convexe de E qui contient X; c'est l'intersection de tous les sous-ensembles convexes qui contiennent X et plus concrètement, c'est l'ensemble des sommes finies

$$\sum_i \lambda_i x_i, \quad x_i\in X, \ \ \lambda_i\geq 0, \ \ \sum_i \lambda_i = 1.$$

Un polyèdre convexe dans un $\mathbf{R}$-espace vectoriel E est un sous-ensemble de E de la forme $\langle X\rangle$ avec X un sous-ensemble fini de E. La dimension d'un polyèdre convexe $P=\langle X\rangle$ dans E est par définition la dimension du sous-espace vectoriel de E engendré par les différences $x-y$ avec x et y dans P; ce sous-espace est d'ailleurs le sous-espace engendré par les $x-y$ avec x et y dans X, donc il est bien de dimension finie.

Soit P un polyèdre convexe. Un sommet de P est un élément x de P tel qu'il existe un hyperplan H de E, disons d'équation $l=a$ avec l un élément de l'espace dual E^* de E et a dans $\mathbf{R}$, avec $x\in H$ et $P-\{x\}$ contenu dans l'un des deux demi-espaces ouverts déterminés par H (autrement dit, on a $l(x)=a$ et soit $l(y)>a$ pour tout $y\neq x$ dans P, soit $l(y)<a$ pour tout $y\neq x$ dans P). De façon équivalente, les sommets de P sont les $x\in P$ qui ne sont pas de la forme $\lambda_1x_1+\lambda_2x_2$ avec x_1 et x_2 dans P distincts, $\lambda_1+\lambda_2=1$, $\lambda_1>0$ et $\lambda_2>0$. De cette propriété il résulte que pour $P=\langle X\rangle$ avec X fini, l'ensemble des sommets de P, qu'on notera dans la suite par $s(P)$, est contenu dans X; on montre aussi que $\langle s(P)\rangle=P$. Les faces de P sont les polyèdres convexes $\langle Y\rangle$ avec $Y\subset s(P)$ tel qu'il existe un hyperplan H de E avec $Y\subset H$ et P contenu dans l'un des deux demi-espaces fermés déterminés par H. Par exemple, les sommets de P sont les faces de dimension 0 de P. Pour tout $i\geq 0$ nous noterons par $f_i(P)$ le nombre de faces de dimension i de P. Si E est de dimension N et P de dimension n, on voit que P est l'ensemble de solutions dans E d'un système de $N-n$ équations linéaires (non homogènes), $l_i=a_i$, $1\leq i\leq N-n$, et $f_{n-1}(P)$ inégalités $l_i\leq a_i$, $N-n+1\leq i\leq N-n+f_{n-1}(P)$, avec les a_i dans $\mathbf{R}$ et les l_i dans E^*.

Fixons un entier $n\geq 1$ et considérons des polyèdres convexes dans l'espace métrique $\mathbf{R}^n$ (qui est muni de sa distance usuelle). La définition de ce que c'est un polyèdre convexe régulier dans $\mathbf{R}^n$ sera par récurrence sur la dimension du polyèdre. Notons d'abord que pour P un polyèdre convexe dans $\mathbf{R}^n$, son groupe d'isométries $\mathrm{Iso}(P)$ agit, pour chaque $i\geq 0$, sur l'ensemble des faces de dimension i: cela résulte par exemple du fait que les isométries de P sont induits par des isométries de $\mathbf{R}^n$ qui sont des applications affines (c'est à dire, application linéaire suivie d'une translation), donc envoient des faces vers des faces; voir l'exercice 66.

9.7.1 Définition. *Un polyèdre convexe régulier de dimension* 0 *dans* $\mathbf{R}^n$ *est un point. Pour* $k>0$*, un polyèdre convexe régulier de dimension* k *dans* $\mathbf{R}^n$ *est un polyèdre convexe* P *de dimension* k *dans* $\mathbf{R}^n$ *tel que:*

1. *les faces de dimension* $<k$ *sont des polyèdres convexes réguliers,*

2. *son groupe d'isométries* $\mathrm{Iso}(P)$ *opère transitivement sur l'ensemble des faces de dimension* i *pour tout* $i \geq 0$,
3. *pour chaque face* F *de dimension* $< k$, *l'opération sur* F *du stabilisateur* $\mathrm{Iso}(P)_F$ *donne toutes les isométries de* F.

Tout polyèdre convexe de dimension 1 est un segment $\langle\{x, y\}\rangle$, avec $x \neq y$. La symétrie par rapport à l'hyperplan médian de x et y échange x et y. Il en résulte que les polyèdres convexes réguliers de dimension 1 sont exactement ces segments $\langle\{x, y\}\rangle$. C'est un exercice assez facile de montrer que les seuls polyèdres convexes réguliers de dimension 2 sont des n-gones réguliers. On vérifie sans problème que les 5 polyèdres des sections 9.2–9.6 sont des polyèdres convexes réguliers de dimension 3; dans la section suivante nous rendrons plausible le fait que ce sont les seuls.

9.8 Pourquoi il n'y a pas d'autres polyèdres réguliers dans $\mathbf{R}^3$.

Nous allons esquisser deux démonstrations du théorème suivant. Nous appelons polyèdres réguliers dans $\mathbf{R}^3$ les polyèdres convexes réguliers de dimension 3 dans $\mathbf{R}^3$. On appelle face d'un polyèdre régulier les faces de dimension 2; on appelle arête les faces de dimension 1.

9.8.1 Théorème. *Les seuls polyèdres réguliers dans* $\mathbf{R}^3$ *sont les tétraèdres, les cubes, les octaèdres, les dodécaèdres et les icosaèdres.*

Esquisse de la première démonstration. Cette démonstration repose sur le fait suivant. Soit P un polyèdre convexe de dimension 3 dans $\mathbf{R}^3$, et soit x un sommet de P. Alors pour chaque face F de P qui contient x, il y a exactement deux de ses arêtes qui contiennent x; nous notons par α_P l'écart angulaire de ces deux arêtes. Avec ces notations, la somme des α_P, avec P parcourant les faces contenant x, est strictement inférieur à 2π. En considérant quelques cas, on peut se convaincre que cela est vrai, mais une démonstration rigoureuse ne semble pas vraiment facile. Une manière serait de démontrer que 2π moins la somme des α_P est égal à l'angle polyédrique du cône convexe dual du cône de P en X.

Soit maintenant P un polyèdre régulier dans $\mathbf{R}^3$. On sait alors que les faces sont des n-gones réguliers, tous avec le même n, car elles sont permutées transitivement par des isométries. Bien sûr on a $n \geq 3$. Comme les sommets sont permutés transitivement par $\mathrm{Iso}(P)$, il existe un entier $e \geq 3$ tel que chaque sommet de P appartient à exactement e faces. Pour chaque arête il y a exactement 2 faces qui le contiennent. On vérifie facilement que dans un n-gone régulier, les angles sont $\pi(1 - 2/n)$. Le fait nommé au début de cette démonstration a alors comme conséquence que $e\pi(1 - 2/n) < 2\pi$. En utilisant que $e \geq 3$ on trouve tout de suite que $n < 6$. Les seules valeurs possibles pour n sont donc 3, 4 et 5. Pour $n = 3$ on trouve, encore en utilisant cette relation, que $e < 6$. Ceci conduit aux tétraèdre, octaèdre et icosaèdre (il n'est pas difficile de voir qu'une fois n et e fixés, il existe au plus un type de polyèdre convexe régulier avec ces valeurs de n et e). Avec $n = 4$ la seule valeur possible de e est 3 et on tombe sur le cube. Pour $n = 5$ la seule valeur possible pour e est encore 3 et cela correspond au dodécaèdre. $\square$

Esquisse de la deuxième démonstration. Cette démonstration repose sur la formule de Euler qui dit que pour un polyèdre convexe P de dimension 3 on a $f_0 - f_1 + f_2 = 2$, où pour chaque i, f_i est le nombre de faces de dimension i de P. Plus généralement, pour tout polyèdre convexe P de dimension n quelconque, on a $\sum_{i=0}^{n-1}(-1)^i f_i = 1 + (-1)^{n-1}$. Ce résultat est démontré de façon naturelle dans un cours de topologie algébrique; pour une démonstration élémentaire et combinatoire on peut voir ...

Soit maintenant P un polyèdre régulier de dimension 3 dans $\mathbf{R}^3$. Soient e et n comme dans la première démonstration. Comme chaque face a n arêtes, et chaque arête est partagée par deux faces, on a $2f_1 = nf_2$. Un même raisonnement donne: $ef_0 = nf_2$. En divisant l'égalité $f_0 - f_1 + f_2 = 2$ par nf_2 on obtient alors:

$$\frac{1}{e} + \frac{1}{n} = \frac{1}{2} + \frac{1}{f_1}$$

On laisse au lecteurs l'exercice que les seules solutions de cette équation avec $e \geq 3$, $n \geq 3$ et $f_1 \geq 3$ correspondent bien aux valeurs de e, n et f_1 des 5 polyèdres que nous connaissons. □

9.9 Polyèdres réguliers en dimension au moins 4.

La classification des polyèdres réguliers de dimension quelconque est connu depuis 1850; elle a été trouvée par Schläfli. Avant de donner le résultat, donnons quelques exemples.

Le cube de dimension n est le polyèdre convexe

$$\{(x_1, \ldots, x_n) \in \mathbf{R}^n \mid \forall i : |x_i| \leq 1\}$$

On vérifie sans peine que le cube est un polyèdre convexe régulier. Le cocube de dimension n est le sous-ensemble de $\mathbf{R}^n$ suivant:

$$\{(x_1, \ldots, x_n) \in \mathbf{R}^n \mid \sum_i |x_i| \leq 1\}$$

On vérifie que c'est un polyèdre convexe régulier. On l'appelle cocube par ce que c'est le dual du cube. Le simplexe de dimension n est le sous-ensemble de $\mathbf{R}^{n+1}$ donné par:

$$\{(x_0, \ldots, x_n) \in \mathbf{R}^{n+1} \mid \sum_i x_i = 1, \ \ \forall i : x_i \geq 0\}$$

On vérifie que c'est un polyèdre convexe régulier.

9.9.1 Théorème. (Schläfli) *Les seuls polyèdres réguliers en dimension $n > 4$ sont le cube, le cocube et le simplexe de dimension n. En dimension 4, il y a encore 3 autres polyèdres réguliers, appelés le (3,4,3), le (3,3,5) et le (5,3,3).*

Pour les détails le lecteur intéressé est invité de consulter les livres “Géométrie” de Berger, cités au début de ce chapître.

10 Simplicité des groupes A_n, $n \geq 5$.

10.1 Définition. *Un groupe G est dit simple si $G \neq \{e\}$ et les seuls sous-groupes distingués de G sont $\{e\}$ et G.*

Autrement dit, un groupe G est simple si pour tout morphisme $f\colon G \to G_1$, on a $\mathrm{im}(f) = \{e_1\}$ (c'est le cas si $\ker(f) = G$) ou $\overline{f}\colon G \to \mathrm{im}(f)$ est un isomorphisme (c'est le cas si $\ker(f) = \{e\}$).

La classification des groupes simples commutatifs est très facile. Supposons que G est simple et commutatif. Prenons x dans G différent de e (c'est possible car $G \neq \{e\}$). Alors G contient le sous-groupe $\langle x \rangle \neq \{e\}$ engendré par x. Comme G est commutatif, ce sous-groupe est distingué. Par conséquent, on a $\langle x \rangle = G$. On voit donc que G est cyclique, donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un unique $n \geq 0$. Par la classification des sous-groupes des groupes cycliques (voir §7), on sait que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont les $d\mathbf{Z}/n\mathbf{Z}$, où $d|n$. Il en résulte que $\mathbf{Z}/n\mathbf{Z}$ est simple si et seulement si n est un nombre premier. Les seules groupes simples commutatifs sont donc les groupes cycliques finis d'ordre un nombre premier, ou autrement dit, les groupes finis d'ordre un nombre premier.

Le but principal de cette section est de démontrer que les groupes A_n des permutations paires de $\{1, 2, \ldots, n\}$ sont simples pour $n \geq 5$. Avant de commencer la démonstration de ce résultat il nous faut quelques résultats préliminaires.

10.2 Lemme. *Pour $n \geq 1$, le groupe A_n est engendré par son sous-ensemble des cycles de longueur 3.*

Démonstration. La démonstration se fera par récurrence sur n. Pour $n \in \{1, 2\}$ il n'y a rien à montrer, car dans ces cas A_n est le groupe trivial. Supposons donc que $n \geq 3$. Soit $\sigma \in \mathrm{A}_n$. Si $\sigma(n) = n$, on peut considérer σ comme un élément de A_{n-1} et par récurrence on sait alors que σ s'écrit comme produit de cycles de longeur 3. Supposons donc que $\sigma(n) \neq n$. Prenons $m \in \{1, \ldots, n\}$ tel que $m \notin \{n, \sigma(n)\}$ (c'est possible car $n \geq 3$). Considérons alors $\tau := (\sigma(n), n, m)\sigma$. Alors τ est paire et on a $\tau(n) = n$ par construction, donc τ peut être considéré comme un élément de A_{n-1} et par conséquent τ est un produit de cycles de longueur 3. Comme $\sigma = (m, n, \sigma(n))\tau$, σ lui aussi est un produit de cycles de longueur 3. $\square$

10.3 Lemme. *Soit $n \geq 5$. Alors les cycles de longueur 3 dans A_n sont tous conjugués entre eux.*

Démonstration. Soit (a, b, c) un cycle de longueur 3 dans A_n. Nous allons montrer que (a, b, c) est conjugué à $(1, 2, 3)$. Soit σ un élément de S_n tel que $\sigma(1) = a$, $\sigma(2) = b$ et $\sigma(3) = c$ (en effet, le nombre de tels σ est $n!/(n(n-1)(n-2)) \geq 2$). Si σ est pair, alors $\sigma \in \mathrm{A}_n$ et $\sigma(1, 2, 3)\sigma^{-1} = (a, b, c)$, ce qui résoud le problème. Supposons donc que σ est impair. Posons alors $\tau := \sigma \circ (4, 5)$. Alors τ est dans A_n et, comme $\tau(1) = a$, $\tau(2) = b$ et $\tau(3) = c$, on a $\tau(1, 2, 3)\tau^{-1} = (a, b, c)$. $\square$

10.4 Lemme. *On appelle doubles transpositions les élément de A_n dont la décomposition en cycles disjoints consiste en deux cycles de longueur 2. Soit $n \geq 5$. Alors les doubles transpositions dans A_n sont tous conjugués entre eux.*

Démonstration. Soit $(a, b)(c, d)$ une double transposition. Montrons que $(a, b)(c, d)$ est conjugué à $(1, 2)(3, 4)$. Soit σ un élément de S_n tel que $\sigma(1) = a$, $\sigma(2) = b$, $\sigma(3) = c$ et $\sigma(4) = d$ (en effet, le nombre de tels σ est $n!/(n(n-1)(n-2)(n-3)) \geq 1$). Notons que $\sigma(1, 2)(3, 4)\sigma^{-1} = (a, b)(c, d)$, donc si $\sigma \in \mathrm{A}_n$ le problème est résolu. Supposons donc que σ est impair. Posons $\tau := \sigma\circ(1, 2)$. Alors τ est pair et on a $\tau(1) = b$, $\tau(2) = a$, $\tau(3) = c$ et $\tau(4) = d$, donc $\tau(1, 2)(3, 4)\tau^{-1} = (b, a)(c, d) = (a, b)(c, d)$. □

10.5 Lemme. *Soient $n \geq 5$ et H un sous-groupe distingué de A_n contenant un cycle de longueur 3 ou une double transposition. Alors $H = \mathrm{A}_n$.*

Démonstration. Si H contient un cycle de longueur 3, H contient tous les cycles de longueur 3 (car ces cycles sont conjugués d'après le Lemme 10.3 et H est distingué), donc H contient le sous-groupe engendré par les cycles de longueur 3, donc (d'après le Lemme 10.2) $H = \mathrm{A}_n$. Si H contient une double transposition, alors H contient toutes les doubles transpositions d'après le Lemme 10.4, donc H contient $(1, 2)(4, 5) \cdot (4, 5)(2, 3) = (1, 2, 3)$ et comme on vient de montrer, $H = \mathrm{A}_n$. □

10.6 Théorème. *Soit $n \geq 5$. Alors A_n est simple.*

Démonstration. Soient $n \geq 5$ et $H \neq \{e\}$ un sous-groupe distingué de A_n. Prenons un élément $\sigma \neq e$ de H, et soit $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ une décomposition de σ en cycles disjoints telle que les longueurs des σ_i forment une suite décroissante.

L'idée de la démonstration est la suivante. Nous voulons montrer que H contient un cycle de longueur 3 ou une double transposition, car alors le Lemme 10.5 nous dit que $H = \mathrm{A}_n$. Pour $\sigma \in \mathrm{S}_n$ le sous-ensemble $\{x \mid \sigma(x) \neq x\}$ de $\{1, 2, \ldots, n\}$ sera appelé le support de σ. Pour montrer que H contient un cycle de longueur 3 ou une double transposition, il suffit de montrer que H contient un élément dont le support est de cardinal 3 ou 4 (noter qu'en effet les seules permutations paires dont le support est de cardinal 3 ou 4 sont les cycles de longueur 3 et les doubles transpositions). Pour fabriquer un élément de H dont le support est petit, nous allons considérer $\sigma' := \tau\sigma\tau^{-1} \in H$ avec $\tau \in \mathrm{A}_n$ de support petit. Alors σ' est une petite perturbation de σ et on verra que $\sigma^{-1}\sigma' \in H$ est de support petit.

Si $\sigma_1 = (a_1, a_2, \ldots, a_l)$ avec $l \geq 4$, soit $\sigma' := \tau\sigma\tau^{-1}$, avec $\tau = (a_1, a_2, a_3)$. Comme $\tau\sigma_i\tau^{-1} = \sigma_i$ pour $i > 1$, on a $\sigma' = \tau\sigma_1\tau^{-1}\sigma_2 \cdots \sigma_r = (a_2, a_3, a_1, a_4, \ldots, a_l)\sigma_2 \cdots \sigma_r$ et donc $\sigma^{-1}\sigma' = (a_1, a_3, a_l)$. Le Lemme 10.5 nous dit que $H = \mathrm{A}_n$.

Si $\sigma = (a, b, c)(d, e, f)\sigma_3 \cdots \sigma_r$, le choix $\tau = (a, b, d)$, donne $\sigma' = (b, d, c)(a, e, f)\sigma_3 \cdots \sigma_r$ et $\sigma^{-1}\sigma' = (a, d, b, f, c) \in H$. Le raisonnement qu'on vient de faire pour le cas où σ_1 est de longueur au moins 4 nous dit que $H = \mathrm{A}_n$.

Si $\sigma_1 = (a, b, c)$ et les σ_i pour $i > 1$ sont de longueur au plus 2, alors $\sigma^2 = (a, c, b) \in H$, donc $H = \mathrm{A}_n$.

Il reste le cas où tous les σ_i sont de longueur 2. Dans ce cas on doit avoir $r \geq 2$ car autrement σ serait impaire. Donc $\sigma = (a, b)(c, d)\sigma_3 \cdots \sigma_r$. Prenons $\tau = (a, b, c)$. Cela donne $\sigma' = (b, c)(a, d)\sigma_3 \cdots \sigma_r$ et $\sigma^{-1}\sigma' = (a, c)(b, d) \in H$. Le Lemme 10.5 nous dit que $H = \mathrm{A}_n$.

Comme on a traité tous les cas possibles, on a montré que $H = \mathrm{A}_n$, ce qui montre que les seuls sous-groupes distingués de A_n sont $\{e\}$ et A_n, $\square$

Depuis une dizaine d'années la classification des groupes finis simples est connue, mais comme cette matière est très difficile, on ne peut pas en dire grand-chose dans ce cours. La liste complète des groupes finis simples (à isomorphisme près) se trouve dans le livre "Atlas of finite simple groups", écrit par Conway et al., et édité par Clarendon Press, Oxford, 1985. Dans cette liste on trouve d'abord les groupes $\mathbf{Z}/p\mathbf{Z}$ avec p premier. Ensuite il y a les groupes A_n pour $n \geq 5$, les groupes de Chevalley et les tordus des groupes de Chevalley, et les 26 groupes sporadiques. Un exemple d'un groupe de Chevalley est le groupe $\mathrm{PSL}_n(\mathbf{Z}/p\mathbf{Z})$ qui est le quotient du groupe $\mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$ des matrices de type (n,n) à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ et de déterminant 1, par son sous-groupe de matrices scalaires. Le groupe $\mathrm{PSL}_n(\mathbf{Z}/p\mathbf{Z})$ est simple si (n,p) n'appartient pas à $\{(2,2),\, (2,3)\}$. Le plus petit des 26 groupes sporadiques se note M_{11} (M pour Mathieu) et est d'ordre $2^4{\cdot}3^2{\cdot}5{\cdot}11$. Le plus grand des 26 groupes sporadiques s'appelle le Monstre. L'ordre du Monstre est:

$$2^{46}{\cdot}3^{20}{\cdot}5^9{\cdot}7^6{\cdot}11^2{\cdot}13^3{\cdot}17{\cdot}19{\cdot}23{\cdot}29{\cdot}31{\cdot}41{\cdot}47{\cdot}59{\cdot}71$$

Dans la famille des 26 groupes sporadiques il y a en un qui s'appelle Baby Monster.

Nous donnons maintenant une autre démonstration du fait que les A_n sont simples pour $n \geq 5$. Cette démonstration est par récurrence sur n. On montre, en calculant les cardinaux des classes de conjugaison de A_5, que A_5 est simple. Ensuite on procède par récurrence.

10.7 Lemme. *Soient G un groupe et $H \subset G$ un sous-groupe. Alors l'application $\iota\colon G \to G$, $x \mapsto x^{-1}$, induit une bijection entre G/H et $H\backslash G$.*

Démonstration. Notons $p_d\colon G \to G/H$ et $p_g\colon G \to H\backslash G$ les applications canoniques. De l'identité $\iota(xh) = (xh)^{-1} = h^{-1}x^{-1} \in H{\cdot}\iota(x)$ montre que l'application $p_g{\circ}\iota$ est compatible à la relation d'équivalence sur G donnée par les translations à droite par H. D'après la Proposition 3.2 il existe alors une application unique $\overline{p_g{\circ}\iota}\colon G/H \to H\backslash G$ telle que $\overline{p_g{\circ}\iota}{\circ}p_d = p_g{\circ}\iota$. De même, on trouve une application unique $\overline{p_d{\circ}\iota}\colon H\backslash G \to G/H$ telle que $\overline{p_d{\circ}\iota}{\circ}p_g = p_d{\circ}\iota$. De l'unicité il résulte que ces deux applications sont des inverses l'un de l'autre. $\square$

10.8 Lemme. *Soit G un groupe opérant sur un ensemble X, et soit H un sous-groupe de G tel que G/H est fini. Alors pour tout $x \in X$, H opère sur l'orbite Gx de x sous G, et le nombre d'orbites dans Gx pour l'opération de H est au plus $|G/H|$. En plus, si H est distingué dans G, ces orbites ont toutes le même cardinal et leur nombre est $|G/(HG_x)|$.*

Démonstration. Posons $r := |G/H|$. Nous venons de voir qu'alors $|H\backslash G| = r$. Il existe donc $g_1, \ldots, g_r$ dans G tels que $H\backslash G = \{Hg_1, \ldots, Hg_r\}$, ou autrement dit, tels que G est la réunion disjointe des classes $Hg_1, \ldots, Hg_r$. Soit $x \in X$; alors on peut écrire

$$Gx = \{gx \mid g \in G\} = \bigcup_{i=1}^{r} \{hg_ix \mid h \in H\} = \bigcup_{i=1}^{r} Hg_ix$$

On voit donc qu'il y a au plus r orbites.

Supposons maintenant que H est distingué. Soient $x \in X$ et $g \in G$. Alors la multiplication à gauche par g sur X: $y \mapsto gy$ induit une bijection entre Hx et $gHx = Hgx$. Ceci montre que toutes les Hg_ix ont même cardinal. Construisons maintenant une bijection entre l'ensemble $H\backslash(Gx)$ des orbites dans Gx pour l'opération de H et l'ensemble G/HG_x (noter que d'après la Proposition 6.7 HG_x est un sous-groupe de G). Soit $f\colon G \to H\backslash(Gx)$ l'application donnée par $f(g) = Hgx = gHx$. Montrons que f est compatible avec la relation d'équivalence sur G donnée par le sous-groupe HG_x opérant par translations à droite: pour $g_1 \in G$, $g_2 \in G_x$ et $h \in H$ on a $f(g_1hg_2) = Hg_1hg_2x = g_1Hx = f(g_1)$. D'après la Proposition 3.2 il existe alors une unique application $\overline{f}\colon G/HG_x \to H\backslash(Gx)$ telle que $\overline{f}(gHG_x) = f(g)$ pour tout $g \in G$. Par construction $\overline{f}$ est surjective. Montrons que $\overline{f}$ est injective. Soient $g_1, g_2 \in G$ tels que $\overline{f}(g_1) = \overline{f}(g_2)$. Alors on a $Hg_1x = Hg_2x$, d'où $g_2x \in Hg_1x$, donc $x \in g_2^{-1}Hg_1x$, ce qui entraîne l'existence d'un $g_3 \in G_x$ et d'un $h \in H$ tels que $g_3 = g_2^{-1}hg_1$, d'où finalement $g_2 = hg_1g_3^{-1} \in Hg_1G_x = g_1HG_x$. □

10.9 Lemme. *Le groupe* A_5 *a exactement* 5 *classes de conjugaison. Les cardinaux de ces classes de conjugaison sont* 1, 12, 12, 15 *et* 20.

Démonstration. On fait opérer S_5 sur A_5 par conjugaison. Soit $\sigma \in \mathrm{A}_5$ et soit $\sigma = \sigma_1 \cdots \sigma_r$ une décomposition en cycles disjoints de longueurs $l_1, \ldots, l_r$ avec $l_1 + \cdots + l_r = 5$ (ceci revient à ne pas négliger les 1-cycles). Alors d'après la Proposition 2.3 on sait que $\sum_{i=1}^r (l_i - 1)$ est pair et que l'orbite de σ sous l'opération de S_n est l'ensemble des permutations avec une décomposition en cycles disjoints de longueurs $l_1, \ldots, l_r$. On voit facilement qu'il y a exactement 4 orbites correspondant au partitions $5 = 5$, $5 = 3+1+1$, $5 = 2+2+1$ et $5 = 1+1+1+1+1$ de 5. Les cardinaux de ces orbites sont respectivement 24, 20, 15 et 1. Appliquons maintenant le Lemme 10.8 avec $G = \mathrm{S}_5$, $X = G$ avec opération de conjugaison et $H = \mathrm{A}_5$, qui est donc distingué dans S_5. La première orbite est l'orbite de $x := (1,2,3,4,5)$; on a $G_x = \langle x \rangle \subset H$ donc le nombre d'orbites dans Gx pour l'opération de H est $|G/H| = 2$. On peut conclure que la première orbite est composée de deux classes de conjugaison de A_5 qui ont 12 éléments chacun. La deuxième orbite est l'orbite de $x := (1,2,3)(4)(5)$; on a $(4,5) \in G_x$, d'où $HG_x = G$. Conclusion: cette orbite est une classe de conjugaison de A_5 de cardinal 20. La troisième orbite a un nombre impair d'éléments donc ne peut pas "casser" en deux morceaux de mêmes cardinaux. Conclusion: cette orbite aussi est une classe de conjugaison de A_5 et elle a cardinal 15. La quatrième orbite est $\{(1)\}$ et est donc une classe de conjugaison de A_5. □

10.10 Proposition. *Le groupe* A_5 *est simple.*

Démonstration. Soit $H \subset \mathrm{A}_5$ un sous-groupe distingué. Alors H est réunion de certaines classes de conjugaison de A_5, parmi lesquels on a certainement $\{(1)\}$. On trouve donc que $|H| = 1 + 12a + 15b + 20c$ avec $a \in \{0,1,2\}$, $b, c \in \{0,1\}$. En plus on sait que $|H|$ divise $|\mathrm{A}_5| = 60$. On vérifie facilement que $|H| = 1$ ou $|H| = 60$. □

Autre démonstration du Théorème 10.6. Pour $n = 5$ c'est la Proposition 10.10; pour $n \geq 6$ on va faire une démonstration par récurrence sur n. Supposons donc que $n \geq 6$, que A_{n-1} est simple et que N est un sous-groupe distingué de A_n, différent de $\{e\}$ et de A_n. Alors pour tout i dans $\{1, 2, \ldots, n\}$ $\mathrm{A}_{n,i} \cap N$ est distingué dans $\mathrm{A}_{n,i}$ (ici on note par $\mathrm{A}_{n,i}$ le stabilisateur de i pour l'opération naturelle de A_n sur $\{1, 2, \ldots, n\}$). Comme les $\mathrm{A}_{n,i}$ sont isomorphes à A_{n-1} (utiliser l'opération de $\mathrm{A}_{n,i}$ sur $\{1, 2, \ldots, n\} - \{i\}$) il n'y a que deux possibilités pour chaque i: soit $\mathrm{A}_{n,i} \cap N = \{e\}$ ou $\mathrm{A}_{n,i} \cap N = \mathrm{A}_{n,i}$.

Supposons que, pour un certain i, on a $\mathrm{A}_{n,i} \cap N = \mathrm{A}_{n,i}$, alors on a $\mathrm{A}_{n,i} \subset N$ pour le même i. Mais comme N est distingué et les $\mathrm{A}_{n,i}$ sont conjugués (A_n agit transitivement sur $\{1, 2, \ldots, n\}$, utiliser le Théorème 4.5) ceci entraîne que $\mathrm{A}_{n,i} \subset N$ pour tout i. Comme les $\mathrm{A}_{n,i}$, $1 \leq i \leq n$, engendrent A_n (ceci se vérifie sans peine, par exemple on sait que les 3-cycles engendrent A_n) on voit que $N = \mathrm{A}_n$, ce qui est en contradiction avec l'hypothèse que $N \neq \mathrm{A}_n$.

Nous pouvons donc conclure que pour tout i on a $\mathrm{A}_{n,i} \cap N = \{e\}$. Dans ce cas, N opère librement sur $\{1, 2, \ldots, n\}$. Il en résulte que $|N|$ divise n. Comme N est distingué dans A_n, l'opération de A_n sur $\{1, 2, \ldots, n\}$ induit une opération de A_n sur $N\backslash\{1, 2, \ldots, n\}$ (vérifiez ce fait), qui est un ensemble de $d := n/|N| \leq n/2$ éléments. Ceci nous donne un morphisme $\mathrm{A}_n \to \mathrm{S}_d$. Le noyau de ce morphisme est un sous-groupe distingué de A_n qui a au moins $n!/(2 \cdot d!) > n$ éléments. Or, nous avons déjà vu qu'un tel sous-groupe est forcément égal à A_n. Mais cela signifie que l'opération de A_n sur $N\backslash\{1, 2, \ldots, n\}$ est triviale, tandis que par construction cette opération est transitive. On en conclut que $N\backslash\{1, 2, \ldots, n\}$ n'a qu'un seul élément, donc que $|N| = n$.

Nous savons maintenant que N opère librement et transitivement sur $\{1, 2, \ldots, n\}$. Cela veut dire que l'application $\phi\colon N \to \{1, 2, \ldots, n\}$, $\sigma \mapsto \sigma(1)$, est bijective. En identifiant les deux ensembles N et $\{1, 2, \ldots, n\}$ à l'aide de ϕ, nous trouvons que le sous-groupe N_g de $\mathrm{Sym}(N)$, qui a pour éléments les translations à gauche par N, est un sous-groupe distingué du groupe $\mathrm{Alt}(N)$ qui a pour éléments les permutations paires de N. Ceci est très remarquable, et par exemple le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ a cette propriété. Nous montrons qu'un groupe d'ordre au moins 6 ne peut pas avoir cette propriété.

Soit σ un élément de $\mathrm{Alt}(N)$ tel que $\sigma(e) = e$. Soient $x \in N$ et $t_x \in \mathrm{Alt}(N)$ la translation à gauche par x. Comme $\mathrm{Alt}(N)$ normalise N_g, on doit avoir $\sigma t_x \sigma^{-1} = t_y$ pour un certain $y \in N$. En prenant la valeur en e des deux cotés on voit que $y = \sigma(x)$. En évaluant l'identité $\sigma t_x \sigma^{-1} = t_{\sigma(x)}$ en $\sigma(y)$ on voit que $\sigma(xy) = \sigma(x)\sigma(y)$, ce qui signifie que $\sigma \in \mathrm{Aut}(N)$.

Il existe un sous-ensemble X de N tel que $N = \langle X \rangle$ et $|X| \leq \mathrm{entier}(\log_2(n))$ (ceci se voit en prenant $x_1 \neq e$ dans N, $x_2 \notin \langle x_1 \rangle$ etc.). Comme $n \geq 6$, on a

$$|N - \{e\} - X| \geq n - 1 - \mathrm{entier}(\log_2(n)) \geq 3$$

Cela montre qu'il existe un $\sigma \neq \mathrm{Id}_N$ dans $\mathrm{Alt}(N)$ tel que $\sigma(e) = e$ et $\sigma(x) = x$ pour tout $x \in X$. On a vu que σ est un automorphisme de N, mais alors on trouve $\sigma = \mathrm{Id}_N$. $\square$

11 Théorèmes de Sylow.

11.1 Définition. *Soit p un nombre premier. Un groupe fini G est appelé un p-groupe si $|G|$ est une puissance de p.*

11.2 Proposition. *Soient p premier, G un p-groupe opérant sur un ensemble fini X et $X^G := \{x \in X \mid \forall g \in G\colon gx = x\}$ l'ensemble des points fixes. Alors on a*

$$|X^G| \equiv |X| \pmod p$$

Démonstration. Soit Y le complémentaire de X^G dans X. Pour $y \in Y$ on a $G_y \neq G$, donc $|Gy| = |G|/|G_y|$ est de la forme p^a avec $a \geq 1$. On voit donc que Y est partitionné par des orbites dont les cardinaux sont divisibles par p. Il en résulte que $|Y|$ est divisible par p. Comme $|X| = |X^G| + |Y|$, on a montré que $|X|$ et $|X^G|$ sont congrus modulo p. □

11.3 Corollaire. *Soient p premier et $G \neq \{e\}$ un p-groupe. Alors le centre C de G est non-trivial.*

Démonstration. Considérons l'opération de G sur lui-même par conjugaison. L'ensemble des points fixes est alors C, donc $|C| \equiv |G| \equiv 0 \pmod p$. Ceci montre que $|C| > 1$. □

11.4 Définition. *Soit p premier. Si G est un groupe fini, $|G| = p^n m$ avec m premier à p, on appelle p-groupe de Sylow dans G un sous-groupe H de G tel que $|H| = p^n$.*

11.5 Théorème. (Sylow) *Soient G un groupe fini, p un nombre premier, $|G| = p^n m$ avec m premier à p. Alors:*
1: il existe des p-groupes de Sylow dans G,
2: soit $P \subset G$ un sous-groupe qui est un p-groupe, alors il existe un p-groupe de Sylow S dans G tel que $P \subset S$,
3: les p-groupes de Sylow sont conjugués entre eux: pour S et S' des p-groupes de Sylow dans G il existe $g \in G$ tel que $S' = gSg^{-1}$,
4: le nombre de p-groupes de Sylow dans G divise m et est congru à 1 modulo p.

Démonstration (Miller-Wielandt). Soit $X := \{Y \subset G \mid |Y| = p^n\}$ l'ensemble des parties de G à p^n éléments; donc $|X| = \mathrm{C}_{p^n m}^{p^n}$. Considérons l'opération suivante de G sur X: $a \bullet Y := aY = \{ay \mid y \in Y\}$.

Soit $Y \in X$. Alors le stabilisateur G_Y de Y agit sur Y par translations à gauche: $a \cdot y := ay$. Cette opération est libre, donc $p^n = |Y| = |G_Y| \cdot |G_Y \backslash Y|$. Ceci montre que $|G_Y|$ est de la forme p^k, avec $k \leq n$.

Si $k = n$, G_Y est un p-groupe de Sylow dans G et Y est de la forme $G_Y x$, avec $x \in G$. D'autre part, si $S \subset G$ est un p-groupe de Sylow, les Sx, $x \in G$, sont des éléments de X dont le stabilisateur est d'ordre p^n (ce stabilisateur contient S, donc est égal à S).

Posons $X' := \{Y \in X \mid |G_Y| = p^n\}$, $X'' := \{Y \in X \mid |G_Y| < p^n\}$ et N le nombre des p-groupes de Sylow dans G. L'application $Y \mapsto (G_Y, Y)$ est une bijection entre X' et l'ensemble des couples (S, c), où $S \subset G$ est un p-groupe de Sylow et $c \in S \backslash G$. On voit donc que $|X'| = Nm$.

D'autre part, pour $Y \in X''$ on a $|G_Y| = p^k$ avec $k < n$, d'où $|G{\bullet}Y| = p^{n-k}m \equiv 0 \pmod p$. Comme X'' est partitionné par des orbites dont les cardinaux sont divisibles par p, on voit que p divise $|X''|$. Nous avons donc trouvé:

$$\mathrm{C}_{p^n m}^{p^n} = |X| = |X'| + |X''| \equiv Nm \pmod p,$$

ou encore:

$$\overline{N} = \overline{m}^{-1}\overline{\mathrm{C}_{p^n m}^{p^n}}$$

dans $\mathbf{Z}/p\mathbf{Z}$.

Nous pouvons conclure que $\overline{N}$ dépend seulement de p, n et m, et pas de la structure de groupe de G. Pour trouver la valeur de $\overline{N}$ on peut donc supposer que $G = \mathbf{Z}/p^n m\mathbf{Z}$. Dans ce cas on sait (§7.1) que G possède un unique sous-groupe d'ordre p^n, d'où $\overline{N} = \overline{1}$. (Noter que nous avons aussi démontré la congruence $\mathrm{C}_{p^n m}^{p^n} \equiv m \pmod p$.)

Il reste à démontrer les parties 2, 3 et la première moitié de 4. Soient $S \subset G$ un p-groupe de Sylow et $P \subset G$ un sous-groupe qui est un p-groupe. Nous allons montrer qu'il existe $a \in G$ tel que $P \subset aSa^{-1}$ (noter que ceci entraîne les parties 2 et 3). Pour ce faire, nous utilisons le principe général que si l'on doit étudier les conjugués d'un sous-groupe H d'un groupe G, il est utile de considérer l'opération de G sur G/H donnée par: $a{\cdot}gH = agH$. En effet, le stabilisateur de $H \in G/H$ est H, donc le stabilisateur de aH est aHa^{-1} (voir le Théorème 4.5, 2). Maintenant allons-y.

Considérons l'opération de G sur G/S donnée par $a{\cdot}gS = agS$. En prenant seulement des a dans P on obtient une opération de P sur G/S. D'après la Proposition 11.2 nous avons $|(G/S)^P| \equiv |G/S| \equiv m \not\equiv 0 \pmod p$. Il existe donc $a \in G$ tel que $aS \in (G/S)^P$, ou autrement dit, tel que $P \subset G_{aS} = aSa^{-1}$.

Maintenant il nous reste à montrer la première moitié de 4. Pour cela, soit Z l'ensemble des p-groupes de Sylow dans G, et considérons l'opération de G sur Z donnée par conjugaison. Par la partie 1, on sait déjà que $Z \neq \emptyset$; soit donc $S \in Z$. De la partie 3 il résulte que $Z = G{\cdot}S$, donc que $|Z| = |G|/|G_S|$. Le stabilisateur de S pour l'opération de conjugaison de G s'appelle le normalisateur de S dans G et se note $\mathrm{N}_G(S)$. On a évidemment $S \subset \mathrm{N}_G(S)$, d'où $|Z|{\cdot}|\mathrm{N}_G(S)/S| = |G|/|S| = m$. □

Nous donnons maintenant une autre démonstration de l'existence des p-groupes de Sylow. Cette démonstration a été trouvée dans les notes d'un cours sur les groupes finis simples par J-P. Serre à l'ENSJF; elle consiste des trois lemmes suivants. Les détails dans les démonstrations de ces lemmes sont laissés au lecteur.

11.6 Lemme. *Soient p premier et G le groupe $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$. Soit H le sous-groupe de G qui a pour éléments les matrices de la forme*

$$\begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix}$$

(c'est à dire les matrices $(a_{i,j})$ telles que $a_{i,j} = 0$ si $i > j$ et $a_{i,i} = 1$). Alors H est un p-groupe de Sylow de G.

Démonstration. On sait (voir les exercices) que $|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$. On calcule: $|G| = p^{n(n-1)/2}m$, avec m premier à p. Evidemment H est un sous-groupe de G, et $|H| = p^{n(n-1)/2}$. □

11.7 Lemme. *Soient p premier, G un groupe fini, $H \subset G$ un sous-groupe et $S \subset G$ un p-groupe de Sylow. Alors il existe $a \in G$ tel que $H \cap aSa^{-1}$ est un p-groupe de Sylow dans H.*

Démonstration. Comme il faut considérer les conjugués de S, on fait agir G sur G/S par translation à gauche. Notons d'abord que $|G/S|$ est premier à p car $S \subset G$ est de Sylow. Il existe donc des orbites dans G/S, pour l'opération de H, dont le cardinal est premier à p. Soit $H{\cdot}aS$ une telle orbite. Considérons le stabilisateur H_{aS} de aS dans H. Comme $H_{aS} = H \cap G_{aS} = H \cap aG_Sa^{-1} = H \cap aSa^{-1}$, c'est un p-groupe. Comme $|H|/|H_{aS}| = |H{\cdot}aS|$ est premier à p, c'est un p-groupe de Sylow. □

11.8 Lemme. *Soient p premier et G un groupe fini d'ordre n. Alors G est ismorphe à un sous-groupe de* $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$.

Démonstration. En utilisant l'opération de G sur lui-même par translation à gauche, on voit que G est isomorphe à un sous-groupe de $\mathrm{Sym}(G)$. En numérotant les éléments de G, on trouve un isomorphisme entre $\mathrm{Sym}(G)$ et S_n. Finalement, si pour $\sigma \in \mathrm{S}_n$ on définit la matrice $\mathrm{mat}(\sigma)$ telle que $\mathrm{mat}(\sigma)_{i,j} = 1$ si $j = \sigma(i)$ et $\mathrm{mat}(\sigma)_{i,j} = 0$ sinon, on voit que S_n est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z})$. □

Donnons enfin encore une autre démonstration de l'existence des p-groupes de Sylow. Cette fois la démonstration est par récurrence sur $|G|$. D'abord un lemme.

11.9 Lemme. *Soient p premier et G un groupe fini commutatif tel que p divise $|G|$. Alors il existe $a \in G$ tel que* $\mathrm{ordre}(a) = p$.

Démonstration. Par récurrence sur $|G|$. Comme $|G| > 1$ on peut prendre $b \in G$ tel que $b \neq e$. Si $r := \mathrm{ordre}(b)$ est divisible par p, disons $r = ps$, on peut prendre $a = b^s$. Si p ne divise pas r, on considère le morphisme canonique $f\colon G \to G/\langle b\rangle$. Alors on a $p \mid |G|/r = |G/\langle b\rangle| < |G|$, donc par récurrence il existe $c \in G$ tel que $\mathrm{ordre}(f(c)) = p$. Par conséquent, $p|\mathrm{ordre}(c)$ et on procède comme dans le premier cas. □

Démonstration (de 1). On fait opérer G sur G par conjugaison. Le centre C de G est alors l'ensemble des points fixes. Soit X le complémentaire, dans G, de C. On distingue deux cas.

Premier cas: $p \mid |C|$. D'après le lemme précédent il existe $c \in C$ tel que $\mathrm{ordre}(c) = p$. Soit $f\colon G \to G/\langle c\rangle$ le morphisme canonique (noter que $\langle c\rangle$ est distingué dans G). Par récurrence, il existe un p-groupe de Sylow $\overline{S}$ dans $G/\langle c\rangle$. Le groupe $S := f^{-1}\overline{S}$ est alors un p-groupe de Sylow dans G (noter que $|S| = p|\overline{S}| = p^n$).

Deuxième cas: p ne divise pas $|C|$. Comme p divise $|G|$ et $|G| = |C| + |X|$, on peut prendre $x \in X$ tel que p ne divise pas le cardinal de l'orbite $G{\cdot}x$ de x. De $|G{\cdot}x| = |G|/|G_x|$ il résulte que $|G_x| = p^n m'$ avec m' premier à p. Comme $x \notin C$, $G_x \neq G$ donc par récurrence il existe un p groupe de Sylow S dans G_x; ce S est aussi un p-groupe de Sylow dans G (car $|S| = p^n$). □

Comme première application des théorèmes de Sylow nous donnons le résultat suivant.

11.10 Corollaire. (Cauchy) *Soient p premier et G un groupe fini. Alors p divise $|G|$ si et seulement s'il existe $a \in G$ tel que* $\mathrm{ordre}(a) = p$.

Démonstration. Une des deux implications est déjà connue: pour $a \in G$ on sait que $\mathrm{ordre}(a)$ divise $|G|$, donc si p divise $\mathrm{ordre}(a)$, p divise $|G|$. Supposons maintenant que p divise $|G|$. Soit $S \subset G$ un p-groupe de Sylow, et $b \in S$, $b \neq e$. Alors $\mathrm{ordre}(b) = p^k$, avec $k > 0$, donc $a := b^{p^{k-1}}$ est d'ordre p. □

Pour illustrer à quoi peuvent servir les théorèmes de Sylow, considérons les deux résultats suivants.

11.11 Proposition. *Soit G un groupe tel que $|G| = 15$. Alors G est isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$.*

Démonstration. Soit N le nombre de 3-groupes de Sylow dans G. D'après le Thm. 9.5 on a $N \equiv 1 \pmod 3$ et aussi $N|5$; il en résulte que $N = 1$, donc il y a un unique 3-groupe de Sylow S dans G et ce S est distingué. Soit N' le nombre de 5-groupes de Sylow dans G. De $N' \equiv 1 \pmod 5$ et $N'|3$ il résulte que $N' = 1$. Soit alors S' l'unique 5-groupe de Sylow dans G; S' lui aussi est distingué. Soit $f\colon G \to G/S \times G/S'$ donné par $f(g) = (gS, gS')$. Alors f est un morphisme, $\ker(f) = S \cap S' = \{e\}$ (noter que $|S \cap S'|$ divise 3 et 5) donc f est injectif. Comme $|G/S| = 5$, G/S est isomorphe à $\mathbf{Z}/5\mathbf{Z}$. De la même façon, G/S' est isomorphe à $\mathbf{Z}/3\mathbf{Z}$. La source et le but de f ont même nombre d'éléments, donc f est un isomorphisme. □

11.12 Proposition. *Soit G un groupe d'ordre 200. Alors G n'est pas simple.*

Démonstration. Notons que $200 = 2^3 5^2$. Soit N le nombre de 5-groupes de Sylow dans G. D'après le Thm. 11.5, on a $N \equiv 1 \pmod 5$ et aussi $N|8$. Par conséquent, $N = 1$ et l'unique 5-groupe de Sylow dans G est un sous-groupe distingué différent de $\{e\}$ et de G. □

12 Groupes commutatifs de type fini.

12.1 Définition. *Un groupe G est de type fini s'il existe un sous-ensemble fini de G qui engendre G.*

Noter qu'un groupe fini est de type fini. Dans cette section nous allons classifier les groupes commutatifs de type fini, mais nous commençons par la classification des groupes commutatifs finis. Cette classification est donnée par le théorème suivant.

12.2 Théorème. *Soit G un groupe commutatif fini. Il existe alors un entier unique $s \geq 0$ et des entiers uniques $n_i > 1$, $1 \leq i \leq s$, tels que*

$$G \cong \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z} \qquad \text{et} \qquad n_s | \cdots | n_2 | n_1$$

12.3 Corollaire. *Deux groupes commutatifs finis G et G' sont isomorphes si et seulement si $s = s'$ et $n_i = n_i'$ pour $1 \leq i \leq s$.*

Il nous faudra quelques résultats préliminaires pour la démonstration du Théorème 12.2. Le premier est le "Théorème Chinois".

12.4 Théorème. *Soient $n \neq 0$ un entier et $n = n_1 n_2 \cdots n_s$ une factorisation de n en facteurs qui sont deux par deux premiers entre eux: $1 \leq i < j \leq s \Rightarrow \operatorname{pgcd}(n_i, n_j) = 1$. Alors il existe un isomorphisme d'anneaux*

$$f\colon \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}, \qquad \overline{a}_n \mapsto (\overline{a}_{n_1}, \ldots, \overline{a}_{n_s})$$

Démonstration. Considérons l'application $g\colon \mathbf{Z} \to \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$ donnée par $g(a) = (\overline{a}_{n_1}, \ldots, \overline{a}_{n_s})$. Cette application est un morphisme. On a $a \in \ker(f)$ si et seulement si $n_i | a$ pour tout i. On voit donc que $\ker(f) = \operatorname{ppcm}(n_1, \ldots, n_s)\mathbf{Z}$. Comme les n_i sont deux par deux premiers entre eux on a $\operatorname{ppcm}(n_1, \ldots, n_s) = n_1 \cdots n_s = n$. L'existence et l'injectivité de f sont garanties par la Proposition 6.2. Comme la source de f et le but de f ont le même nombre d'éléments, f est un isomorphisme. Comme f est compatible avec la multiplication, f est même un isomorphisme d'anneaux. □

12.5 Lemme. *Soient G un groupe commutatif, $x \in G$ d'ordre $n > 0$ et $y \in G$ d'ordre $m > 0$. Si n et m sont premiers entre eux on a $\operatorname{ordre}(xy) = nm$.*

Démonstration. Posons $z := xy$ et $l := \operatorname{ordre}(z)$. Comme $z^{nm} = (xy)^{nm} = x^{nm}y^{nm} = e$ on a $l | nm$. D'autre part, on a $e = z^l$, donc $e = e^n = z^{ln} = x^{ln}y^{ln} = y^{ln}$, d'où $m | ln$. Comme n et m sont premiers entre eux on doit avoir $m | l$. De la même façon on voit que $n | l$. Utilisant encore que n et m sont premiers entre eux on trouve $nm | l$. □

12.6 Lemme. *Soient G un groupe commutatif, $x \in G$ d'ordre $n > 0$ et $y \in G$ d'ordre $m > 0$. Alors il existe $z \in G$ d'ordre $\operatorname{ppcm}(n, m)$.*

Démonstration. Soient $p_1, \ldots, p_r$ les nombres premiers distincts divisant nm. On a alors, de façon unique, $n = p_1^{n_1} \cdots p_r^{n_r}$ et $m = p_1^{m_1} \cdots p_r^{m_r}$ avec $n_i, m_i \geq 0$. Posant

$$n' := \prod_{\{i \mid n_i \geq m_i\}} p_i^{n_i} \qquad \text{et} \qquad m' := \prod_{\{i \mid n_i < m_i\}} p_i^{m_i}$$

on a $n'|n$, $m'|m$, $\mathrm{pgcd}(n', m') = 1$ et $\mathrm{ppcm}(n', m') = \mathrm{ppcm}(n, m)$. On applique le lemme précédent à $x^{n/n'}$ et $y^{m/m'}$, qui sont d'ordre n' et m'. $\square$

12.7 Lemme. *Soit G un groupe commutatif fini. Il existe $x \in G$ tel que pour tout $y \in G$:* $\mathrm{ordre}(y)|\mathrm{ordre}(x)$.

Démonstration. Soit $x \in G$ un élément tel que $n := \mathrm{ordre}(x)$ est maximal parmi les ordres des éléments de G. Soit $y \in G$. Posons $m := \mathrm{ordre}(y)$. On a bien sûr $m > 0$. D'après le lemme précédent il existe un élément $z \in G$ tel que $\mathrm{ordre}(z) = \mathrm{ppcm}(n, m) \geq n$. Comme l'ordre de x est maximal on doit avoir $\mathrm{ppcm}(n, m) = n$, d'où $m|n$. $\square$

On voit facilement que l'ordre de x dans le Lemme 12.7 est le plus petit entier positif n tel que $y^n = e$ pour tout y dans G. Cet entier n est appelé l'exposant de G.

12.8 Lemme. *Soient G un groupe commutatif fini et $x \in G$ tel que pour tout $y \in G$:* $\mathrm{ordre}(y)|\mathrm{ordre}(x)$. *Soit $f: G \to G/\langle x \rangle$ le morphisme canonique. Pour tout $z \in G/\langle x \rangle$ il existe $y \in G$ tel que $f(y) = z$ et* $\mathrm{ordre}(y) = \mathrm{ordre}(z)$.

Démonstration. Soit $z \in G/\langle x \rangle$, $n = \mathrm{ordre}(z)$. Prenons $t \in G$ tel que $f(t) = z$. Comme $z^{\mathrm{ordre}(t)} = f(t)^{\mathrm{ordre}(t)} = f(t^{\mathrm{ordre}(t)}) = \overline{e}$, on a $n|\mathrm{ordre}(t)$; nous pouvons donc écrire $\mathrm{ordre}(t) = nm$ avec $m \geq 1$. Comme $\ker(f) = \langle x \rangle$ et $f(t^n) = z^n = \overline{e}$ on a $t^n = x^l$ pour un $l \in \mathbf{Z}$. De $nm = \mathrm{ordre}(t)|\mathrm{ordre}(x)$ il résulte qu'on peut écrire $\mathrm{ordre}(x) = nmk$ avec $k \geq 1$. Comme $e = t^{nm} = x^{lm}$ on a $nmk|lm$, d'où $nk|l$. Posons $a := -l/n$ et $y := tx^a$. Alors $f(y) = f(t)f(x^a) = z$. Comme on a vu, $f(y) = z$ entraîne $n|\mathrm{ordre}(y)$. D'autre part, $y^n = t^n x^{na} = x^l x^{-l} = e$, donc $\mathrm{ordre}(y) = n$. $\square$

12.9 Lemme. *Soient $s \geq 0$ et $n_1, \ldots, n_s \in \mathbf{Z}$. Alors $\mathbf{Z}^s/(n_1\mathbf{Z} \times \cdots \times n_s\mathbf{Z})$ est isomorphe à $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$.*

Démonstration. On applique la Proposition 6.2 au morphisme $f: \mathbf{Z}^s \to \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$ donné par $f(a_1, \ldots, a_s) = (\overline{a_1}, \ldots, \overline{a_s})$. $\square$

Démonstration du Théorème 12.2. Nous allons d'abord démontrer l'existence de s et des n_i, et cela par récurrence sur $|G|$. Si $|G| = 1$ on prend $s = 0$. Supposons donc que $|G| > 1$. D'après le Lemme 12.7 nous pouvons prendre $x \in G$ tel que $\forall y \in G$: $\mathrm{ordre}(y)|\mathrm{ordre}(x)$. Soit $f: G \to G/\langle x \rangle$ le morphisme canonique. Comme $|G/\langle x \rangle| < |G|$ nous savons par récurrence qu'il existe $t \geq 0$ et des $m_i > 1$ tels que $G/\langle x \rangle \cong \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_t\mathbf{Z}$ et $m_t| \cdots |m_2|m_1$. Soit $g: \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_t\mathbf{Z} \to G/\langle x \rangle$ un isomorphisme. Pour $1 \leq i \leq t$, notons par e_i l'élément de $\mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_t\mathbf{Z}$ dont toutes les coordonnées sont zéro sauf la $i$ème qui est $\overline{1}$. D'après le Lemme 12.8 il existe des $x_i \in G$ tels que $f(x_i) = g(e_i)$ et $\mathrm{ordre}(x_i) = m_i$. Notons $n =$

ordre(x) et considérons le morphisme $h\colon \mathbf{Z}^{t+1} \to G$ donné par $h(a_1, \ldots, a_{t+1}) = x_1^{a_1} \cdots x_t^{a_t} x^{a_{t+1}}$. Montrons que h est surjectif. Soit $y \in G$. Alors on peut écrire $g^{-1}(f(y)) = (\overline{a_1}, \ldots, \overline{a_t})$ avec $a_i \in \mathbf{Z}$. On calcule: $f(yx_1^{-a_1} \cdots x_t^{-a_t}) = f(y)g(e_1)^{-a_1} \cdots g(e_t)^{-a_t} = g(g^{-1}(f(y)) - (\overline{a_1}, \ldots, \overline{a_t})) = \overline{e}$, d'où $yx_1^{-a_1} \cdots x_t^{-a_t} \in \ker(f) = \langle x \rangle$. Il en résulte qu'on peut écrire $y = x_1^{a_1} \cdots x_t^{a_t} x^{a_{t+1}} = h(a_1, \ldots, a_{t+1})$. Considérons maintenant $\ker(h)$. Il est clair que pour tout $(b_1, \ldots, b_{t+1}) \in \mathbf{Z}^{t+1}$ on a $(m_1 b_1, \ldots, m_t b_t, n b_{t+1}) \in \ker(h)$, ou autrement dit, que $\ker(h) \supset m_1\mathbf{Z} \times \cdots \times m_t\mathbf{Z} \times n\mathbf{Z}$. Par la Prop. 6.1 il existe un morphisme $\overline{h}\colon \mathbf{Z}/(m_1\mathbf{Z} \times \cdots \times m_t\mathbf{Z} \times n\mathbf{Z}) \to G$ tel que $\overline{h}(\overline{(a_1, \ldots, a_{t+1})}) = h(a_1, \ldots, a_{t+1})$. Comme h est surjectif, $\overline{h}$ l'est aussi. Du Lemme 10.9 on déduit un morphisme surjectif $\tilde{h}\colon \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_t\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \to G$. Le calcul $|G| = |\langle x \rangle| \cdot |G/\langle x \rangle| = nm_1 \cdots m_t$ montre que $\tilde{h}$ est bijectif, donc un isomorphisme. Par le choix de x et des m_i on a bien $m_1 = $ ordre$(x_1)|$ordre$(x) = n$ et $m_t | \cdots | m_2 | m_1$. Tout ceci montre qu'on peut prendre $s = t+1$, $n_i = m_{i-1}$ pour $2 \leq i \leq s$ et $n_1 = n$.

Montrons maintenant l'unicité de s et des n_i. Il suffit de montrer que s et les n_i sont déterminés par G. Comme on doit avoir $n_1 n_2 \cdots n_s = |G|$, les nombres premiers p qui figurent dans les décompositions en facteurs premiers des n_i sont les p qui divisent $|G|$. Il suffit de montrer que pour chaque p divisant $|G|$ l'exposant de p en chaque n_i est déterminé par G.

Soit p un nombre premier divisant $|G|$. Pour $j \geq 0$ soit $H_j^p := \{x \in G \mid x^{p^j} = e\}$ le sous-groupe de G ayant pour éléments les $x \in G$ d'ordre divisant p^j. Ecrivons $n_i = p^{m_i} n_i'$ avec $p \not| n_i'$. On a $m_1 \geq m_2 \geq \cdots \geq m_s \geq 0$. Par le Théorème Chinois on a $\mathbf{Z}/n_i\mathbf{Z} \cong \mathbf{Z}/p^{m_i}\mathbf{Z} \times \mathbf{Z}/n_i'\mathbf{Z}$, d'où

$$G \cong \mathbf{Z}/p^{m_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{m_s}\mathbf{Z} \times G'$$

avec $p \not| |G'|$. Utilisant cet isomorphisme on voit que

$$|H_j^p| = \prod_{i=1}^{s} p^{\min(j, m_i)}$$

On calcule que pour $j \geq 1$:

$$|H_j^p|/|H_{j-1}^p| \;=\; \prod_{i=1}^{s} p^{\min(j,m_i) - \min(j-1,m_i)} \;=\; \prod_{1 \leq i \leq s \text{ et } j \leq m_i} p \;=\; p^{|\{i \mid m_i \geq j\}|}$$

Nous pouvons donc conclure que pour $j \geq 1$ le nombre des m_i qui sont plus grand ou égal à j est $\log_p(|H_j^p|/|H_{j-1}^p|)$. Ceci détermine la suite $m_1 \geq m_2 \geq \cdots \geq m_s$. L'entier s est donné par la formule

$$s = \max_{p \mid |G|} \log_p |H_1^p|$$

car pour chaque $p \mid |G|$ on a $\log_p |H_1^p| \leq s$, avec égalité si et seulement si $p | n_s$. $\square$

Nous commençons maintenant l'étude des groupes commutatifs de type fini. Pour G un groupe quelconque nous posons $G_{\text{tors}} := \{x \in G \mid \exists n > 0 \colon x^n = e\}$; donc G_{tors} est le sous-ensemble de G formé des éléments d'ordre fini. On dit que G est “sans torsion” si $G_{\text{tors}} = \{e\}$. Si G_{tors} est un sous-groupe de G on l'appellera le sous-groupe de torsion de G.

12.10 Proposition. *Soit G un groupe commutatif. Alors G_{tors} est un sous-groupe de G et G/G_{tors} est un groupe sans torsion.*

Démonstration. On a $e \in G_{\text{tors}}$. Si $x, y \in G_{\text{tors}}$ il existe n et m positifs tels que $x^n = e = y^m$; alors $(xy)^{nm} = x^{nm}y^{nm} = e$, donc $xy \in G_{\text{tors}}$. Si $x \in G_{\text{tors}}$, $n > 0$ et $x^n = e$, on a $(x^{-1})^n = e$, donc $x^{-1} \in G_{\text{tors}}$. Nous avons montré que G_{tors} est un sous-groupe de G. Soit $x \in (G/G_{\text{tors}})_{\text{tors}}$. On prend $n > 0$ tel que $x^n = \overline{e}$. On prend $y \in G$ tel que $x = \overline{y}$. Alors on a $\overline{y^n} = \overline{y}^n = x^n = \overline{e}$, d'où $y^n \in G_{\text{tors}}$. Il existe alors $m > 0$ tel que $e = (y^n)^m = y^{nm}$, ce qui signifie que $y \in G_{\text{tors}}$ et par conséquent que $x = \overline{e}$. □

12.11 Définition. *Un groupe commutatif de type fini est libre s'il existe $r \geq 0$ tel que $G \cong \mathbf{Z}^r$. Une suite $x_1, \ldots, x_r$ dans un groupe commutatif G est une base si pour tout $x \in G$ il y a un élément unique $(a_1, \ldots, a_r) \in \mathbf{Z}^r$ tel que $x = x_1^{a_1} \cdots x_r^{a_r}$.*

Pour $1 \leq i \leq r$ notons par e_i l'élément de $\mathbf{Z}^r$ dont toutes les coordonnées sont 0 sauf la $i$ème qui est 1. La suite $e_1, \ldots, e_r$ est une base de $\mathbf{Z}^r$.

Soit G un groupe commutatif. Si $f\colon \mathbf{Z}^r \to G$ est un isomorphisme, la suite $f(e_1), \ldots, f(e_r)$ est une base de G. Réciproquement, si $x_1, \ldots, x_r \in G$ on leur associe le morphisme $f\colon \mathbf{Z}^r \to G$ donné par $f(a_1, \ldots, a_r) = x_1^{a_1} \cdots x_r^{a_r}$. Ce morphisme f est surjectif si et seulement si $x_1, \ldots, x_r$ engendrent G; f est un isomorphisme si et seulement si $x_1, \ldots, x_r$ est une base de G. Un groupe commutatif de type fini est donc libre si et seulement s'il existe $r \geq 0$ et une suite $x_1, \ldots, x_r$ dans G qui est une base.

12.12 Théorème. *Soit G un groupe commutatif, de type fini et sans torsion. Il existe un entier $r \geq 0$ unique tel que $G \cong \mathbf{Z}^r$. Cet entier r est appelé le rang de G.*

Nous avons besoin d'un lemme avant de démontrer le théorème.

12.13 Lemme. *Soit $e_1, \ldots, e_r$ une base d'un groupe commutatif G, noté additivement. Soient $i, j \in \{1, \ldots, r\}$ distincts et $a \in \mathbf{Z}$. Soient $e'_k = e_k$ pour $k \neq j$ et $e'_j = e_j + ae_i$. Alors $e'_1, \ldots, e'_r$ est une base de G.*

Démonstration. On a $e_j = e'_j - ae'_i$ et $e_k = e'_k$ pour $k \neq j$. Cela montre que $e'_1, \ldots, e'_r$ engendrent G. Soient $a_1, \ldots, a_r \in \mathbf{Z}$ tels que $a_1e'_1 + \cdots + a_re'_r = 0$. Cela donne

$$0 = \sum_{k \neq j} a_k e_k + a_j(e_j + ae_i) = \sum_{k \neq i} a_k e_k + (a_i + aa_j)e_i,$$

ce qui entraîne $a_k = 0$ pour $k \neq i$ et $a_i + aa_j = 0$. On en déduit que $a_k = 0$ pour tout k. □

Démonstration du Théorème 12.12. Montrons d'abord l'unicité de r. Soit $f\colon \mathbf{Z}^r \to G$ un isomorphisme. L'image du sous-groupe $2\mathbf{Z}^r = \{(2a_1, \ldots, 2a_r) \mid a_1, \ldots, a_r \in \mathbf{Z}\}$ de $\mathbf{Z}^r$ est le sous-groupe $H := \{x^2 \mid x \in G\}$ de G. Soient $p\colon \mathbf{Z}^r \to \mathbf{Z}^r/2\mathbf{Z}^r$ et $p'\colon G \to G/H$ les morphismes canoniques. La Prop. 6.2 nous donne un isomorphisme $\overline{f}\colon \mathbf{Z}^r/2\mathbf{Z}^r \to G/H$. D'après le Lemme 10.9 le groupe $\mathbf{Z}^r/2\mathbf{Z}^r$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^r$. On en déduit que $|G/H| = 2^r$, ce qui montre que G détermine r.

Nous allons maintenant démontrer l'existence de r. Considérons les cardinaux $|X|$ des sous-ensembles $X \subset G$ qui engendrent G; nous appellerons le nombre minimal de générateurs de G le minimum de ces $|X|$. Nous montrerons l'énoncé suivant:

> Soit G un groupe commutatif, de type fini et sans torsion. Soit r le nombre minimal de générateurs de G. Alors tout système générateur $x_1, \dots, x_r$ de r éléments de G est une base.

Noter que cet énoncé démontre l'existence d'un r comme dans l'énoncé du théorème. Soit donc $x_1, \dots, x_r$ un système générateur de G, et $f\colon \mathbf{Z}^r \to G$ le morphisme surjectif associé. Il nous faut montrer que f est injectif. Supposons que f n'est pas injectif. Prenons $0 \neq x = (a_1, \dots, a_r) \in \ker(f)$. Soit $d := \operatorname{pgcd}(a_1, \dots, a_r)$. Dans $\mathbf{Z}^r$ on a alors $x = dx'$ avec $x' = (a_1/d, \dots, a_r/d)$. Comme G est sans torsion, l'égalité $e = f(x) = f(dx') = f(x')^d$ entraîne $f(x') = e$, ou autrement dit, $x' \in \ker(f)$. En remplaçant x par x' nous pouvons donc supposer que $x = (a_1, \dots, a_r)$ avec $\operatorname{pgcd}(a_1, \dots, a_r) = 1$.

Nous allons montrer qu'il existe une base $f_1, \dots, f_r$ de $\mathbf{Z}^r$ telle que $f_r = x$. Notons que cela finit la démonstration du Théorème 12.12 car cela signifie que $f(f_1), \dots, f(f_{r-1})$ engendrent G, ce qui est en contradiction avec la minimalité de r.

Prenons $i \in \{1, \dots, r\}$ tel que $|a_i|$ soit maximal parmi les $|a_k|$, $1 \leq k \leq r$. S'il existe $j \neq i$ tel que $a_j \neq 0$, on peut écrire $a_i = aa_j + b$ avec $0 \leq b < |a_j|$ (c'est la division Euclidienne). D'après le Lemme 12.13 on a une base $e'_1, \dots, e'_r$ de $\mathbf{Z}^r$ donnée par $e'_k = e_k$ pour $k \neq j$ et $e'_j = e_j + ae_i$. Utilisant les égalités $e'_k = e_k$ pour $k \neq j$, $e_j = e'_j - ae'_i$ et $a_i = aa_j + b$ on trouve:

$$x = a_1 e_1 + \cdots + a_r e_r = \sum_{k \neq i,j} a_k e'_k + a_j(e'_j - ae'_i) + (aa_j + b)e'_i = \sum_{k=1}^{r} a'_k e'_k$$

avec $a'_k = a_k$ pour $k \neq i$ et $a'_i = b$. Il en résulte que

$$\sum_{k=1}^{r} |a'_k| < \sum_{k=1}^{r} |a_k| \qquad \text{et} \qquad \operatorname{pgcd}(a'_1, \dots, a'_k) = 1$$

(noter que $a_i = aa'_j + a'_i$ et $a_k = a'_k$ pour $k \neq i$). En itérant ce procédé on tombera donc en au plus $|a_1| + \cdots + |a_r|$ étapes sur une base $f_1, \dots, f_r$ telle que $x = b_1 f_1 + \cdots + b_r f_r$, $\operatorname{pgcd}(b_1, \dots, b_r) = 1$ et les b_j sont 0 sauf un, disons b_i. Dans ce cas on a $x = \pm f_i$. La base voulue s'obtient par un changement de signe (si nécessaire) et une permutation. $\square$

Le théorème suivant donne enfin la classification des groupes commutatifs de type fini.

12.14 Théorème. *Soit G un groupe commutatif de type fini. Il existe alors des entiers uniques $r, s \geq 0$ et des entiers uniques $n_i > 1$, $1 \leq i \leq s$, tels que*

$$G \cong \mathbf{Z}^r \times \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z} \qquad \text{et} \qquad n_s | \cdots | n_2 | n_1$$

Ces entiers r, s, $n_1, \dots, n_s$ s'appellent les invariants de G.

Avant de démontrer ce théorème, dont les Théorèmes 12.2 et 12.12 sont des cas spéciaux, démontrons les lemmes suivants.

12.15 Lemme. *Soit $f\colon G \to H$ un morphisme surjectif. Si G est de type fini, H l'est aussi.*

Démonstration. Soit $X \subset G$ un sous-ensemble fini qui engendre G. Alors $\{f(x) \mid x \in X\}$ est un sous-ensemble fini de H qui engendre H. $\square$

12.16 Lemme. *Soit G un groupe commutatif de type fini tel que $G = G_{\text{tors}}$. Alors G est fini.*

Démonstration. Soient $x_1, \ldots, x_r$ un système de générateurs de G. Notons n_i l'ordre de x_i. Soit $f\colon \mathbf{Z}^r \to G$ le morphisme surjectif associé a $x_1, \ldots, x_r$: $f(a_1, \ldots, a_r) = x_1^{a_1} \cdots x_r^{a_r}$. On a $\ker(f) \supset n_1\mathbf{Z} \times \cdots \times n_r\mathbf{Z}$, d'où, d'après la Proposition 6.1, un morphisme surjectif $\mathbf{Z}^r/(n_1\mathbf{Z} \times \cdots \times n_r\mathbf{Z}) \to G$. Il résulte du Lemme 12.9 que G est fini. $\square$

Démonstration de 12.14. Montrons d'abord l'existence de r, s et des n_i. D'après la Proposition 12.10 et le Lemme 12.15, G/G_{tors} est sans torsion et de type fini. D'après le Théorème 12.12 il existe $r \geq 0$ tel que $G/G_{\text{tors}} \cong \mathbf{Z}^r$. Prenons $x_1, \ldots, x_r \in G$ tels que $\overline{x_1}, \ldots, \overline{x_r}$ est une base de G/G_{tors}. Considérons le morphisme:

$$f\colon \mathbf{Z}^r \times G_{\text{tors}} \longrightarrow G, \qquad ((a_1, \ldots, a_r), y) \mapsto x_1^{a_1} \cdots x_r^{a_r} y$$

Si $((a_1, \ldots, a_r), y) \in \ker(f)$ on a $x_1^{a_1} \cdots x_r^{a_r} = y^{-1} \in G_{\text{tors}}$, donc $\overline{x_1}^{a_1} \cdots \overline{x_r}^{a_r} = \overline{e}$ dans G/G_{tors}, d'où $a_1 = \cdots = a_r = 0$. On en déduit que $y = e$ et on voit donc que f est injectif. Montrons que f est surjectif. Soit $x \in G$. Il existe $(a_1, \ldots, a_r)$ unique tel que $\overline{x} = \overline{x_1}^{a_1} \cdots \overline{x_r}^{a_r}$. Posons $y := x x_1^{-a_1} \cdots x_r^{-a_r}$. Alors on a $\overline{y} = \overline{e}$, d'où $y \in G_{\text{tors}}$ et $x = f((a_1, \ldots, a_r), y)$. Nous savons maintenant que f est un isomorphisme.

Notons $\text{pr}_2\colon \mathbf{Z}^r \times G_{\text{tors}} \to G_{\text{tors}}$ le morphisme donné par $\text{pr}_2(x, y) = y$. L'application $\text{pr}_2 \circ f^{-1}$ de G vers G_{tors} est alors un morphisme surjectif. D'après le Lemme 12.15 G_{tors} est de type fini. D'après le Lemme 12.16 nous dit alors que G_{tors} est fini. L'existence de s et des n_i résulte du Théorème 12.2.

Montrons maintenant l'unicité de r, s et des n_i. Il suffit de montrer que ces nombres sont déterminés par G. Comme $G/G_{\text{tors}} \cong \mathbf{Z}^r$, l'entier r est le rang de G/G_{tors}. Comme $G_{\text{tors}} \cong \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$, les entiers $s, n_1, \ldots, n_s$ sont déterminés par G d'après le Théorème 12.2. $\square$

Nous allons donner maintenant une autre démonstration du Théorème 12.14 qui est basée sur l'idée suivante. Si G est un groupe commutatif de type fini, engendré par $x_1, \ldots, x_n$ on a le morphisme surjectif $f\colon \mathbf{Z}^r \to G$ donné par $f(a_1, \ldots, a_n) = x_1^{a_1} \cdots x_n^{a_n}$. D'après la Proposition 6.2, G est alors isomorphe à $\mathbf{Z}^n/\ker(f)$. On pourrait donc étudier tous les groupes quotients de $\mathbf{Z}^n$.

12.17 Théorème. *Soient $n \geq 0$ et H un sous-groupe de $\mathbf{Z}^n$. Alors H est libre de rang au plus n.*

Démonstration. Par récurrence sur n. Pour $n = 0$ on a $H \cong \mathbf{Z}^0$. Pour $n = 1$, H est un sous-groupe de $\mathbf{Z}$, donc $H = k\mathbf{Z}$ pour un unique $k \geq 0$; on a $H \cong \mathbf{Z}^0$ si $k = 0$ et $H \cong \mathbf{Z}^1$ si $k \neq 0$. Supposons donc que $n \geq 2$. Soit $p\colon H \to \mathbf{Z}$ le morphisme donné par $p(a_1, \ldots, a_n) = a_n$. Soit $H' := \text{im}(p)$; comme H' est un sous-groupe de $\mathbf{Z}$, $H' \cong \mathbf{Z}^{k'}$ avec $k' \in \{0, 1\}$. Soit $H'' := \ker(p)$, donc H'' est le sous-groupe d'éléments de H de la forme $(a_1, \ldots, a_{n-1}, 0)$. On peut considérer

H'' comme un sous-groupe de $\mathbf{Z}^{n-1}$, donc par récurrence $H'' \cong \mathbf{Z}^{k''}$ pour un $k'' \leq n-1$. Si $k' = 0$ on a $H = H'' \cong \mathbf{Z}^{k''}$. Supposons donc que $k' = 1$. Soient alors $k := k'' + 1$, $x_1, \ldots, x_{k''}$ une base de H'' et $x_k \in H$ tel que $p(x_k)$ est une base de H'. Soit $f\colon \mathbf{Z}^k \to H$ le morphisme donné par $f(a_1, \ldots, a_k) = a_1x_1 + \cdots + a_kx_k$. On montre que f est un isomorphisme de la même façon qu'on a utilisée pour le morphisme f dans la démonstration du Théorème 12.14. □

12.18 Théorème. *Soient $n \geq 0$ et $H \subset \mathbf{Z}^n$ un sous-groupe. Il existe alors des bases $e_1, \ldots, e_n$ de $\mathbf{Z}^n$ et $f_1, \ldots, f_m$ de H, telles que pour $1 \leq i \leq m$ on a $f_i = n_ie_i$, avec $n_i \geq 0$ et $n_m | \cdots | n_2 | n_1$.*

Démonstration. La construction de telles bases est faite en étapes. On commence avec des bases arbitraires $e = (e_j)_{1\leq j\leq n}$ de $\mathbf{Z}^n$ et $f = (f_i)_{1\leq i\leq m}$ de H. Deux telles bases donnent une matrice $(x_{i,j})$ avec coefficients dans $\mathbf{Z}$, de m lignes et n colonnes déterminée par: $f_i = \sum_j x_{i,j}e_j$. Pour construire des nouvelles bases, on se permet de faire les opérations suivantes sur les deux bases:

1. permutations des éléments d'une base,
2. multiplier n'importe quel élément d'une base par -1,
3. ajouter un multiple de l'$i$ème élément d'une base au $j$ème élément de cette base, avec j différent de i.

On a vu en effet que ces opérations transforment une base en une base (voir le Lemme 12.13). Si la base $e' = (e'_j)_{1\leq j\leq n}$ est obtenue par une telle opération appliquée à la base $e = (e_j)_{1\leq j\leq n}$, on obtient la matrice $(x'_{i,j})$ de la matrice $(x_{i,j})$ par l'opération correspondente suivante:

1. la même permutation, mais appliquée aux colonnes de $(x_{i,j})$,
2. multiplier la colonne correspondente par -1,
3. ajouter le même multiple de la $i$ème colonne au $j$ème colonne.

Si la base $f' = (f'_i)_{1\leq i\leq m}$ est obtenue par une telle opération appliquée à la base $f = (f_i)_{1\leq i\leq m}$, on obtient la matrice $(x'_{i,j})$ de la matrice $(x_{i,j})$ par les mêmes opérations, mais appliquées cette fois aux lignes. On voit donc que si on arrive, par ces opérations, de transformer la matrice $(x_{i,j})$ en une matrice $(x'_{i,j})$ telle que $x'_{i,j} = 0$ si $i \neq j$ et $x'_{1,1} | \cdots | x'_{m,m}$, les bases cherchées sont trouvées: si f' et e' sont les bases qui donnent la matrice $(x'_{i,j})$, on prend $f'_m, \ldots, f'_1$ et $e'_n, \ldots, e'_1$.

L'algorithme suivant fait la transformation cherchée sur les matrices:

12.19 Algorithme. 1. Si $x_{i,j} = 0$ pour tout i, j on arrète; sinon, faire une permutation sur les colonnes et une permutation sur les lignes telles que $|x_{1,1}|$ est non-nul et minimal parmi les $|x_{i,j}|$ qui sont non-nuls.

2. S'il existe $i > 1$ tel que $x_{1,1} \nmid x_{i,1}$, écrire $x_{i,1} = qx_{1,1} + r$ avec $0 \leq r < |x_{1,1}|$, soustraire q fois la ligne 1 de la ligne i, échanger les lignes 1 et i. Répéter ceci jusqu'à $x_{1,1} | x_{i,1}$ pour tout i.
3. Pour $2 \leq i \leq n$, soustraire la ligne 1 $x_{i,1}/x_{1,1}$ fois de la ligne i. Maintenant $x_{i,1} = 0$ pour tout $i \geq 2$.
4. Répéter l'étape (1) et les étapes (2) et (3) et leurs analogues avec la première ligne (en faisant des opérations sur les colonnes) pour avoir $x_{i,1} = 0$ si $i > 1$ et $x_{1,j} = 0$ si $j > 1$.

5. S'il existe i, j avec $x_{1,1} \nmid x_{i,j}$, écrire $x_{i,j} = qx_{1,1} + r$ avec $0 \le r < |x_{1,1}|$, ajouter la ligne 1 à la ligne i, soustraire la colonne 1 q fois de la colonne j, recommencer avec (1). Sinon, multiplier la colonne 1 par ± 1 pour avoir $x_{1,1} > 0$ et recommencer l'algorithme avec la matrice $(x_{i,j})_{2 \le i \le m, 2 \le j \le n}$.

La vérification que cet algorithme fait ce qu'il faut est laissée au lecteur. □

Remarque. On peut montrer que les entiers $n_1, \ldots, n_m$ ne dépendent pas des bases e et f. Par exemple, le nombre n_1 est le plus grand commun diviseur des $x_{i,j}$.

Deuxième démonstration de 12.14. L'unicité de r, s et de n_i se démontrent comme dans la première démonstration. Montrons leur existence. Soient $x_1, \ldots, x_n$ un système générateur de G et $f \colon \mathbf{Z}^n \to G$ le morphisme surjectif associé. D'après le Théorème 12.17 $\ker(f)$ est libre de rang $m \le n$. D'après le Théorème 12.18 il existe des bases $e_1, \ldots, e_n$ de $\mathbf{Z}^n$ et $f_1, \ldots, f_m$ de $\ker(f)$ et des entiers non-négatifs n_i, $1 \le i \le m$, tels que $f_i = n_i e_i$ pour $1 \le i \le m$ et $n_m | \cdots | n_2 | n_1$. Comme $f_1, \ldots, f_m$ est une base, on a $n_i \ne 0$ pour tout i. Soit $g \colon \mathbf{Z}^n \to \mathbf{Z}^n$ le morphisme donné par $g(a_1, \ldots, a_n) = a_1 e_1 + \cdots + a_n e_n$. Comme les e_i forment une base de $\mathbf{Z}^n$, g est un isomorphisme. On a un morphisme surjectif $f \circ g \colon \mathbf{Z}^n \to G$ dont le noyau est $g^{-1} \ker(f)$. La Proposition 6.2 dit alors que G est isomorphe à $\mathbf{Z}^n / g^{-1} \ker(f)$. En remarquant que la suite $g^{-1}(f_1), \ldots, g^{-1}(f_m)$ est une base de $g^{-1} \ker(f)$ on voit que

$$g^{-1} \ker(f) = n_1 \mathbf{Z} \times \cdots \times n_m \mathbf{Z} \times \{0\}^{n-m}$$

Utilisant le Lemme 12.9 on trouve:

$$G \cong \mathbf{Z}^n / (n_1 \mathbf{Z} \times \cdots \times n_m \mathbf{Z} \times \{0\}^{n-m}) \cong \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_m\mathbf{Z} \times \mathbf{Z}^{n-m}$$

Comme $n_m | \cdots | n_2 | n_1$, il existe $j \ge 0$ tels que la suite $n_1, \ldots, n_m$ termine par exactement j fois 1. Noter que $\mathbf{Z}/1\mathbf{Z} = \{\overline{0}\}$. On a donc

$$G \cong \mathbf{Z}^{n-m} \times \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_{m-j}\mathbf{Z}$$

avec $n_k > 1$ pour $1 \le k \le m-j$, et $n_{m-j} | \cdots | n_1$. □

12.20 Application de l'Algorithme 12.19. Soient $n \ge 0$, $f_1, \ldots, f_m \in \mathbf{Z}^n$. Soit $H := \langle \{f_1, \ldots, f_m\} \rangle$ le sous-groupe de $\mathbf{Z}^n$ engendré par $f_1, \ldots, f_m$. On aimerait calculer les invariants r, s, $n_1, \ldots, n_s$ du groupe $\mathbf{Z}^n/H$. Nous allons expliquer comment cela peut être fait avec l'Algorithme 12.19. Notons $e_1, \ldots, e_n$ la base canonique de $\mathbf{Z}^n$. On obtient une matrice $(x_{i,j})$ avec m lignes, n colonnes en posant: $f_i = \sum_j x_{i,j} e_j$. On se permet maintenant de faire les 3 opérations données sur la page 42 sur la base $e_1, \ldots, e_n$ de $\mathbf{Z}^n$ et sur le système générateur $f_1, \ldots, f_m$ de H (noter que ces opérations tranforment en effet un système générateur en un système générateur). L'effet de ces opérations sur la matrice $x_{i,j}$ est la même que sur la page 42. L'Algorithme 12.19 démontre donc l'existence d'une base $e'_1, \ldots, e'_n$ de $\mathbf{Z}^n$, d'un entier $m' \ge 0$ et d'une base $f'_1, \ldots, f'_{m'}$ de H tel qu'il existe des entiers strictement positifs $d_1, \ldots, d_{m'}$ tels que $f_i' = d_i e_i'$ pour $1 \leq i \leq m'$ et $d_1 | d_2 | \cdots | d_{m'}$. Disons que la suite $d_1, \ldots, d_{m'}$ commence par exactement j fois 1. Alors de la formule

$$\mathbf{Z}^n / H \cong \mathbf{Z}^{n-m'} \times \mathbf{Z}/d_{m'}\mathbf{Z} \times \cdots \times \mathbf{Z}/d_{j+1}\mathbf{Z}$$

on déduit facilement les invariants de $\mathbf{Z}^n/H$: $r = n - m'$, $s = m' - j$ et $n_1 = d_{m'}, \ldots, n_s = d_{j+1}$.

13 Le théorème de Jordan-Hölder.

Soit G un groupe fini. Nous allons associer à G des listes de groupes finis simples, à isomorphisme près, avec multiplicités. La construction d'une telle liste dépend de certains choix, mais le théorème de Jordan-Hölder affirme qu'en fait on ne trouve, à permutation près, qu'une seule liste. Tout le procédé est d'ailleurs un analogue assez exact de la décomposition en atomes d'une molécule en chimie.

Voici le procédé, qui est par récurrence sur $|G|$. Si $G = \{e\}$, on lui associe la liste vide. Si G est simple, on lui associe G. Finalement, si G est non-trivial et non-simple, on prend un sous-groupe distingué N de G, différent de $\{e\}$ et de G, et la liste associée à G est alors la réunion des listes associées à N et à G/N.

13.1 Théorème. (Jordan-Hölder) *La liste associée à G comme ci-dessus ne dépend pas, à permutation près, des choix des sous-groupes distingués.*

Nous allons démontrer ce théorème un peu plus loin, après quelques exemples et préliminaires. Notons tout de suite que si G_1 et G_2 sont des groupes finis isomorphes, les listes associées à G_1 et à G_2 sont les mêmes. Regardons quelques exemples.

13.2 Exemples. (1) $G := \mathbf{Z}/30\mathbf{Z}$. Pour N on peut prendre $2\mathbf{Z}/30\mathbf{Z}$. La liste de $\mathbf{Z}/30\mathbf{Z}$ est la réunion des listes de $2\mathbf{Z}/30\mathbf{Z}$ et de $(\mathbf{Z}/30\mathbf{Z})/(2\mathbf{Z}/30\mathbf{Z})$. Le deuxième de ces groupes est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ par la Proposition 6.8; comme $\mathbf{Z}/2\mathbf{Z}$ est simple, sa liste est $\mathbf{Z}/2\mathbf{Z}$. Le premier des deux groupes est isomorphe à $\mathbf{Z}/15\mathbf{Z}$ (il est engendré par $\overline{2}$ qui est d'ordre 15). Dans $\mathbf{Z}/15\mathbf{Z}$ on peut prendre le sous-groupe $3\mathbf{Z}/15\mathbf{Z}$, qui est isomorphe au groupe simple $\mathbf{Z}/5\mathbf{Z}$. Le quotient $(\mathbf{Z}/15\mathbf{Z})/(3\mathbf{Z}/15\mathbf{Z})$ est isomorphe au groupe simple $\mathbf{Z}/3\mathbf{Z}$ (encore la Proposition 6.8). On voit finalement que la liste associée à $\mathbf{Z}/30\mathbf{Z}$ est $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$.

(2) $G := \mathrm{S}_3$. Dans ce cas il n'y a qu'un seul sous-groupe distingué différent de $\{e\}$ et de G: c'est A_3. Comme $\mathrm{A}_3 \cong \mathbf{Z}/3\mathbf{Z}$ et $\mathrm{S}_3/\mathrm{A}_3 \cong \mathbf{Z}/2\mathbf{Z}$, la liste associée à S_3 est $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$.

(3) $G := \mathrm{S}_4$. On sait (Exemple 4.2 (3)) qu'il existe un morphisme surjectif $f\colon \mathrm{S}_4 \to \mathrm{S}_3$, tel que $\ker(f) = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. On a déjà vu que la liste de S_3 est $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$. Pour tout $x \in \ker(f)$ on a $x^2 = e$, donc $\ker(f)$ est commutatif (ce qui se vérifie aussi directement, si on veut). Comme $\ker(f)$ n'a pas d'élément d'ordre 4, il est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. La liste associée à S_4 est donc $\mathbf{Z}/2\mathbf{Z}$ (3 fois), $\mathbf{Z}/3\mathbf{Z}$.

(4) $G := \mathrm{S}_n$ avec $n \geq 5$. Prenons $N := \mathrm{A}_n$. Comme $n \geq 5$, A_n est simple, donc la liste associée à S_n est $\mathbf{Z}/2\mathbf{Z}$, A_n.

Notons enfin que deux groupes non-isomorphes peuvent bien donner la même liste. Par exemple les listes associées à $\mathbf{Z}/4\mathbf{Z}$ et à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ sont les mêmes.

Pour la démonstration suivante du Théorème 13.1, qui est tirée de notes d'un cours sur les groupes finis simples par J-P. Serre à l'ENSJF, nous aurons besoin des notions de suite exacte et de filtration.

13.3 Définition. *Une suite de morphismes de groupes*

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow \cdots \xrightarrow{f_{n-1}} G_n \tag{13.3.1}$$

est exacte en degré i (avec $1 < i < n$) si on a $\ker(f_i) = \mathrm{im}(f_{i-1})$. Une telle suite est appelée exacte si elle est exacte en degré i pour tout i avec $1 < i < n$.

Notons par exemple qu'une suite $\{e\} \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to \{e\}$ est exacte si et seulement si f est injectif, g est surjectif et $\ker(g) = \mathrm{im}(f)$. Pour simplifier la notation dans ce qui suit nous noterons le groupe trivial $\{e\}$ par 1. Pour des raisons de notation, nous noterons aussi l'élément neutre d'un groupe par 1 dans la suite.

13.4 Lemme. *Soit*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & A & \to & B & \to & C & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & D & \to & E & \to & F & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & G & & H & & I & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

un diagramme commutatif de morphismes de groupes tel que les lignes et les colonnes sont exactes. Alors il existe des morphismes uniques $\alpha: G \to H$ et $\beta: H \to I$ qui font commuter le diagramme complété. En plus, la suite $1 \to G \to H \to I \to 1$ est exacte.

Démonstration. Montrons d'abord qu'il existe un morphisme $\alpha: G \to H$ comme dans le lemme. Pour définir α, nous allons dire pour tout g dans G quel est son image dans H. Soit donc g dans G. Comme le morphisme $D \to G$ dans le diagramme est surjectif, on peut prendre un d dans D qui a image g dans G. Notons e l'image de d dans E par le morphisme $D \to E$ du diagramme (attention: e n'est pas forcément l'élément neutre 1 de E). Soit h dans H l'image de e par le morphisme $E \to H$ du diagramme. Montrons que cet élément h ne dépend pas du choix de d. Soit d' dans D un élément qui a g pour image dans G. Alors $d'd^{-1}$ est dans le noyau de $D \to G$, donc il existe un élément a dans A qui a image $d'd^{-1}$ par $A \to D$. Notons b l'image de a par $A \to B$, e' l'image de d' par $D \to E$ et h' l'image de e' par $E \to H$. Alors l'image de b par $B \to E$ est $e'e^{-1}$, ce qui implique que $e'e^{-1}$ est dans le noyau de $E \to H$. On en conclut que $h' = h$. La construction que nous venons de faire définit une application $\alpha: G \to H$. La surjectivité de $D \to G$ implique que c'est la seule application de G vers H qui peut faire commuter le diagramme. Montrons que α est un morphisme. Soient g_1 et g_2 dans G. Soient d_1 et d_2 dans D tels que leurs images dans H sont g_1 et g_2. Soient h_1 et h_2 les images de d_1 et d_2 dans H par la composée de $D \to E$ et $E \to H$. Alors on a $h_1 = \alpha(g_1)$ et $h_2 = \alpha(g_2)$. Comme les images de $d_1 d_2$ par $D \to G$ et $D \to E \to H$ sont $g_1 g_2$ et $h_1 h_2$, on a aussi $\alpha(g_1 g_2) = h_1 h_2$. L'existence et unicité de α sont maintenant démontrées.

L'existence et unicité de β se démontrent de la même façon, donc nous indiquons seulement quel est l'image d'un h dans H par β. Comme $E \to H$ est surjectif, nous pouvons prendre un e dans E qui a h comme image dans H. Soit f l'image de e par $E \to F$. Soit i l'image de f par $F \to I$. Alors ce i ne dépend pas du choix de e, et on a $\beta(h) = i$.

Abordons maintenant la question d'exactitude du lemme. On voit facilement que β est surjectif, car la composée de $E \to F$ et $F \to I$ est surjective. Montrons que $\ker(\beta) = \mathrm{im}(\alpha)$ en montrant les deux inclusions. Soit g dans G. Prenons d dans D qui a image g par $D \to G$. Soit e l'image de d par $D \to E$. Alors $\alpha(g)$ est l'image de e par $E \to H$. L'image de e dans F est 1, ce qui implique que $\beta(\alpha(g)) = 1$. On a donc montré que $\mathrm{im}(\alpha) \subset \ker(\beta)$. Soit h dans $\ker(\beta)$. Prenons un e dans E qui a image h par $E \to H$. Soit f l'image de e par $E \to F$. Alors f est dans le noyau de $F \to I$, donc on peut prendre c dans C qui a image f par $C \to F$. Prenons un b dans B qui a image c par $B \to C$; notons e_1 l'image de b par $B \to E$. Posons $e_2 := ee_1^{-1}$. Alors e_2 a image 1 par $E \to F$ et image h par $E \to H$. Prenons un d qui a image e_2 par $D \to E$. Soit g l'image de d par $D \to G$. Alors on a $\alpha(g) = h$. On a donc montré que $\ker(\beta) \subset \mathrm{im}(\alpha)$.

Il reste à montrer que α est injectif. Soit g dans $\ker(\alpha)$. Prenons d dans D qui a image g par $D \to G$. Soit e l'image de d dans E. Comme e est dans le noyau de $E \to H$, on peut prendre un b dans B qui a image e dans E. Notons c l'image de b dans C. Alors l'image de c dans F est 1, donc $c = 1$. On peut donc prendre un a dans A qui a image b dans B. Soit d_1 l'image de a dans D. Alors d_1 a image e dans E, ce qui montre que $d_1 = d$. Par conséquent, $g = 1$. $\square$

13.5 Remarque. La technique de démonstration que nous venons de voir s'appelle la chasse de diagrammes. Le Lemme 13.4 est un cas spécial du “lemme du serpent”, qu'on peut trouver dans chaque livre sur l'algèbre homologique.

13.6 Définition. *Soit G un groupe. Une filtration (décroissante) sur G est une suite de sous-groupes $(G_i)_{i\geq 0}$, de G telle que pour tout $i \geq 0$ on a $G_i \supset G_{i+1}$. Une filtration*

$$G \supset G_0 \supset G_1 \supset G_2 \supset \cdots$$

de G est appelée une filtration de Jordan-Hölder si

1: $G_0 = G$,

2: G_{i+1} est distingué dans G_i pour tout $i \geq 0$,

3: pour tout $i \geq 0$ le quotient G_i/G_{i+1} est trivial ou simple,

4: il existe un i tel que G_i est trivial.

13.7 Lemme. *Pour tout groupe fini G il existe des filtrations de Jordan-Hölder.*

Démonstration. Récurrence sur $|G|$. Pour G trivial ou simple c'est clair. Supposons donc que G n'est pas trivial ou simple. Prenons un sous-groupe distingué non-trivial N de G, différent de G. Par récurrence, il existe des filtrations de Jordan-Hölder pour N et G/N, disons $(N_i)_{i\geq 0}$ et $((G/N)_i)_{i\geq 0}$. Soit $j \geq 0$ tel que $(G/N)_j$ est trivial. Notons $p\colon G \to G/N$ la projection canonique et posons $G_i := p^{-1}(G/N)_i$ pour $i \leq j$. Pour $i > j$ nous posons $G_i := N_{i-j}$. On peut vérifier que $(G_i)_{i\geq 0}$ est une filtration de Jordan-Hölder pour G. $\square$

13.8 Lemme. *Soit $(G_i)_{i\geq 0}$ une filtration de Jordan-Hölder d'un groupe G. Soit N un sous-groupe distingué de G. Pour tout $i \geq 0$ posons $N_i := N \cap G_i$ et $(G/N)_i := p(G_i)$, où $p\colon G \to G/N$ est la projection canonique. Alors $(N_i)_{i\geq 0}$ et $((G/N)_i)_{i\geq 0}$ sont des filtrations de Jordan-Hölder, et pour tout $i \geq 0$ on a une suite exacte*

$$1 \to N_i/N_{i+1} \to G_i/G_{i+1} \to (G/N)_i/(G/N)_{i+1} \to 1$$

Démonstration. Vérifions que $(N_i)_{i\geq 0}$ est une filtration de Jordan-Hölder. Comme $N_0 = N \cap G_0 = N \cap G = N$ la première condition est satisfaite. Le noyau de la composée $f_i \colon N_i \to G_i/G_{i+1}$ de l'inclusion $N_i \to G_i$ par la projection canonique $G_i \to G_i/G_{i+1}$ est N_{i+1}, donc N_{i+1} est distingué dans N_i. En plus, notons que que f_i induit un morphisme injectif de N_i/N_{i+1} dans G_i/G_{i+1} et que l'image de cette injection est un sous-groupe distingué car la projection $G_i \to G_i/G_{i+1}$ est surjective. Il en résulte que N_i/N_{i+1} est trivial ou simple. Finalement, si G_i est trivial, N_i l'est aussi.

Vérifions maintenant que $((G/N)_i)_{i\geq 0}$ est une filtration de Jordan-Hölder. On a $(G/N)_0 = p(G_0) = G/N$. Soit $g_i \colon G_i \to (G/N)_i$ la surjection induite par la restriction de $p \colon G \to G/N$ à G_i. Comme g_i est surjectif, l'image du sous-groupe distingué G_{i+1} de G_i par g_i est distingué dans $(G/N)_i$; cet image est $(G/N)_{i+1}$. Soit $h_i \colon G_i \to (G/N)_i/(G/N)_{i+1}$ le composé de g_i par la projection canonique $(G/N)_i \to (G/N)_i/(G/N)_{i+1}$. Alors h_i est surjectif et son noyau contient G_{i+1}, donc h_i induit un morphisme surjectif de G_i/G_{i+1} vers $(G/N)_i/(G/N)_{i+1}$, ce qui montre que $(G/N)_i/(G/N)_{i+1}$ est trivial ou simple. Finalement, si G_i est trivial, $(G/N)_i$ l'est aussi.

Pour construire la suite exacte, notons que pour tout i nous avons $p|_{G_i} \colon G_i \to (G/N)_i$, qui est surjectif et qui a noyau N_i. On laisse (comme toujours) la vérification que le diagramme suivant, où tous les morphismes sont induits par inclusions et projections canoniques, est commutatif au lecteur:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & N_{i+1} & \to & G_{i+1} & \to & (G/N)_{i+1} & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & N_i & \to & G_i & \to & (G/N)_i & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N_i/N_{i+1} & & G_i/G_{i+1} & & (G/N)_i/(G/N)_{i+1} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Une application du Lemme 13.4 finit la démonstration. □

13.9 Définition. *Pour G un groupe, $(G_i)_{i\geq 0}$ une filtration de Jordan-Hölder de G et S un groupe simple, soit $n(G, (G_i)_{i\geq 0}, S)$ le nombre d'indices $i \geq 0$ tel que G_i/G_{i+1} est isomorphe à S.*

Maintenant nous pouvons énoncer une version plus précise du Théorème de Jordan-Hölder, et le démontrer.

13.10 Théorème. (Jordan-Hölder) *Soit G un groupe fini. Soient $(G_i)_{i\geq 0}$ et $(G'_i)_{i\geq 0}$ deux filtrations de Jordan-Hölder de G. Soit S un groupe simple. Alors on a $n(G, (G_i)_{i\geq 0}, S) = n(G, (G'_i)_{i\geq 0}, S)$.*

Démonstration. Récurrence sur $|G|$. Si G est trivial c'est clair. Si G est simple, on a pour chaque filtration de Jordan-Hölder un $i \geq 0$ unique tel que $G_i = G$ et $G_{i+1} = \{e\}$, ce qui montre le résultat. Supposons donc que G n'est pas simple, et prenons un sous-groupe distingué N de

G différent de $\{e\}$ et de G. Soient $(N_i)_{i\geq 0}$ et $(G/N)_{i\geq 0}$ les filtrations de Jordan-Hölder induites par $(G_i)_{i\geq 0}$ comme dans le Lemme 13.8. Soient $(N'_i)_{i\geq 0}$ et $((G/N)'_i)_{i\geq 0}$ les filtrations analogues induites par $(G'_i)_{i\geq 0}$. Par récurrence nous avons

$$n(N,(N_i)_{i\geq 0},S) = n(N,(N'_i)_{i\geq 0},S) \qquad \text{et} \qquad n(G/N,((G/N)_i)_{i\geq 0},S) = n(G,((G/N)'_i)_{i\geq 0},S)$$

D'après les suites exactes du Lemme 13.8, on a

$$n(G,(G_i)_{i\geq 0},S) = n(N,(N_i)_{i\geq 0},S) + n(G/N,((G/N)_i)_{i\geq 0},S)$$

et

$$n(G,(G'_i)_{i\geq 0},S) = n(N,(N'_i)_{i\geq 0},S) + n(G/N,((G/N)'_i)_{i\geq 0},S)$$

En combinant ces formules, la démonstration est terminée. □

13.11 Remarque. En généralisant un peu le principe de récurrence dans la démonstration du Théorème 13.10, on peut démontrer le même résultat pour G quelconque. En général, bien sûr, un groupe G n'admet pas forcément des filtrations de Jordan-Hölder.

14 Produits semi-directs.

Soit G un groupe et $N \subset G$ un sous-groupe distingué. Notons $\overline{G} := G/N$, $p: G \to \overline{G}$ le morphisme canonique et $i: N \to G$ l'inclusion. Nous avons alors ce qu'on appelle une suite exacte courte:

$$N \overset{i}{\hookrightarrow} G \overset{p}{\twoheadrightarrow} \overline{G} \tag{14.1}$$

c'est à dire: i et p sont des morphismes, i est injectif, p est surjectif et $\ker(p) = \mathrm{im}(i)$. Si on part d'une suite exacte courte quelconque:

$$G_1 \overset{f_1}{\hookrightarrow} G_2 \overset{f_2}{\twoheadrightarrow} G_3 \tag{14.2}$$

alors $\mathrm{im}(f_1)$ est un sous-groupe distingué de G_2 (car c'est $\ker(f_2)$) et d'après la Proposition 6.2 il existe un isomorphisme $\overline{f_2}: G_2/\mathrm{im}(f_1) \to G_3$ tel que $f_2 = \overline{f_2}\circ p_2$, où $p_2: G_2 \to G_2/\mathrm{im}(f_1)$ est le morphisme canonique. De façon un peu vague, on peut dire que la donnée d'un sous-groupe distingué N d'un groupe G équivaut à la donnée d'une suite exacte courte (14.2) avec $G_2 = G$ et $\mathrm{im}(f_1) = N$.

14.3 Définition. *Soit $G_1 \overset{f_1}{\hookrightarrow} G_2 \overset{f_2}{\twoheadrightarrow} G_3$ une suite exacte courte. On dira que G_2 est une extension de G_3 par G_1. Un morphisme $s: G_3 \to G_2$ est appelé une section de f_2 si $f_2\circ s = \mathrm{id}_{G_3}$. On dira que la suite exacte courte est scindée, ou encore que G_2 est une extension scindée de G_3 par G_1, s'il existe une section de f_2.*

14.4 Proposition. (1) *La suite exacte courte (14.2) est scindée si et seulement s'il existe un sous-groupe H de G_2 tel que $H \cap \mathrm{im}(f_1) = \{e_2\}$ et $\mathrm{im}(f_1)H = G_2$.*

(2) *Si $s: G_3 \to G_2$ est une section de f_2, $H := \mathrm{im}(s)$ est un tel sous-groupe de G_2 et la restriction de f_2 à H est un isomorphisme de H vers G_3.*

(3) *Si H est un tel sous-groupe de G_2, alors la restriction de f_2 à H est un isomorphisme $f: H \to G_3$ et $s := j\circ f^{-1}$, où $j: H \to G_2$ est l'inclusion, est une section de f_2.*

(4) *Si $s: G_3 \to G_2$ est une section de f_2, tout élément $x \in G_2$ s'écrit de façon unique sous la forme $x = f_1(y)s(z)$, avec $y \in G_1$ et $z \in G_3$.*

Démonstration. Supposons que $s: G_3 \to G_2$ est une section de f_2. Posons $H := \mathrm{im}(s)$. Soit $x \in H \cap \mathrm{im}(f_1)$. Par définition de H, nous pouvons écrire $x = s(y)$, avec $y \in G_3$. Comme $\mathrm{im}(f_1) = \ker(f_2)$ on a $e_3 = f_2(x) = f_2(s(y)) = y$, d'où $x = s(e_3) = e_2$. Montrons que $\mathrm{im}(f_1)H = G_2$. Soit $x \in G_2$; posons $y := f_2(x)$. Le calcul $f_2(xs(y)^{-1}) = f_2(x)f_2(s(y)^{-1}) = yy^{-1} = e_3$ montre que $xs(y)^{-1} \in \ker(f_2) = \mathrm{im}(f_1)$. Nous pouvons donc écrire $xs(y)^{-1} = f_1(z)$, pour un certain $z \in G_1$. On a alors $x = xs(y)^{-1}s(y) = f_1(z)s(y)$.

Supposons maintenant que $H \subset G_2$ satisfait $H \cap \mathrm{im}(f_1) = \{e_2\}$ et $\mathrm{im}(f_1)H = G_2$. Soit $f: H \to G_3$ la réstriction de f_2 à H: pour $h \in H$ on a $f(h) = f_2(h)$. Montrons que f est un isomorphisme. Pour $h \in \ker(f)$ on a $f_2(h) = e_3$, donc $h \in \ker(f_2) \cap H = \{e_2\}$. Ceci montre que f est injectif. Soit $x \in G_3$. Comme f_2 est surjectif, on peut prendre $y \in G_2$ tel que $f_2(y) = x$. Comme $\mathrm{im}(f_1)H = G_2$, il existe $z \in G_1$ et $h \in H$ tels que $y = f_1(z)h$. On a alors

$f(h) = f_2(h) = f_2(f_1(z))f_2(h) = f_2(y) = x$. Ceci montre que f est surjectif. On a donc montré que f est un isomorphisme. Si on note $j: H \to G_2$ l'inclusion, on peut alors prendre $s = j \circ f^{-1}$.

Il reste à montrer la partie (4). Nous avons déjà vu que $H := \mathrm{im}(s)$ satisfait $\mathrm{im}(f_1)H = G_2$ et $H \cap \mathrm{im}(f_1) = \{e_2\}$. Comme s et f_1 sont injectifs, il suffit de montrer que chaque $x \in G_2$ s'écrit de façon unique sous la forme $x = yz$, avec $y \in \mathrm{im}(f_1)$ et $z \in H$. De l'identité $G_2 = \mathrm{im}(f_1)H$ il résulte que chaque x s'écrit sous cette forme. Supposons que $x = y_1z_1 = y_2z_2$ avec $y_1, y_2 \in \mathrm{im}(f_1)$ et $z_1, z_2 \in H$. Alors on a $y_2^{-1}y_1 = z_2z_1^{-1} \in H \cap \mathrm{im}(f_1) = \{e_2\}$, d'où $y_1 = y_2$ et $z_1 = z_2$. □

Supposons maintenant que $N \subset G$ est un sous-groupe distingué tel que la suite exacte courte (14.1) est scindée. Soit $H \subset G$ un sous-groupe tel que $NH = G$ et $N \cap H = \{e\}$. Nous avons vu (Proposition 14.4, (4)) que chaque $x \in G$ s'écrit de façon unique comme $x = nh$ avec $n \in N$ et $h \in H$. Il est alors intéressant d'écrire le produit $n_1h_1n_2h_2$ de deux éléments arbitraires de G sous cette forme. Pour le faire, introduisons le morphisme $\alpha: H \to \mathrm{Aut}(N)$ donné par l'opération de conjugaison de H sur N: pour $h \in H$ et $n \in N$ on a $(\alpha(h))(n) = hnh^{-1}$ (noter que $hnh^{-1} \in N$ car N est distingué dans G). On peut alors écrire:

$$n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1(\alpha(h_1))(n_2)\cdot h_1h_2$$

Ceci est la motivation pour la proposition suivante.

14.5 Proposition. *Soient N et H des groupes et $\alpha: H \to \mathrm{Aut}(N)$ un morphisme. Le triple $(N \times H, *, (e_N, e_H))$, avec*

$$(n_1, h_1) * (n_2, h_2) = (n_1(\alpha(h_1))(n_2), h_1h_2)$$

est alors un groupe. On l'appelle le produit semi-direct de N par H par rapport à α et on le note $N \times_\alpha H$. Les applications $f_1: N \to N \times_\alpha H: n \mapsto (n, e_H)$ et $f_2: N \times_\alpha H \to H: (n, h) \mapsto h$ sont des morphismes qui font de $N \times_\alpha H$ une extension de H par N. L'application $s: H \to N \times_\alpha H: h \mapsto (e_N, h)$ est une section de f_2. Finalement, si G est un groupe et $i: N \hookrightarrow G$, $j: H \hookrightarrow G$ des morphismes injectifs tels que $i(N)j(H) = G$, $i(N) \cap j(H) = \{e\}$ et pour tout $n \in N$, $h \in H$: $j(h)i(n)j(h)^{-1} = i((\alpha(h))(n))$, alors l'application $f: N \times_\alpha H \to G: (n, h) \mapsto i(n)j(h)$ est un isomorphisme.

Démonstration. Tout se vérifie sans problème. □

14.6 Exemples. (1) Soit $n \geq 3$. On a vu (§9.1) que dans le groupe diédral D_n tout élément s'écrit de façon unique sous la forme $\rho^a\sigma^b$, avec $0 \leq a < n$ et $0 \leq b < 2$, et que $\rho^a\sigma^b\rho^c\sigma^d = \rho^{a+(-1)^bc}\sigma^{b+d}$. On voit que $\langle\rho\rangle \subset D_n$ est un sous-groupe distingué, isomorphe à $\mathbf{Z}/n\mathbf{Z}$, et que $\langle\sigma\rangle \subset D_n$ est un sous-groupe isomorphe à $\mathbf{Z}/2\mathbf{Z}$ tel que $\langle\rho\rangle\langle\sigma\rangle = D_n$ et $\langle\rho\rangle \cap \langle\sigma\rangle = \{e\}$. L'opération de conjugaison de $\langle\sigma\rangle$ sur $\langle\rho\rangle$ est donnée par le morphisme

$$\alpha: \langle\sigma\rangle \to \mathrm{Aut}(\langle\rho\rangle) : \qquad (\alpha(\sigma^b))(\rho^a) = \sigma^b\rho^a\sigma^{-b} = \rho^{(-1)^b a}$$

La Proposition 14.5 nous dit alors que D_n est isomorphe à $\mathbf{Z}/n\mathbf{Z} \times_\beta \mathbf{Z}/2\mathbf{Z}$, où $\beta: \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ est donné par $(\beta(\overline{b}))(\overline{a}) = (-1)^b\overline{a}$.

(2) Soient $n \geq 0$ et G le groupe des isométries de $\mathbf{R}^n$. On sait que chaque élément de G s'écrit comme $t \circ \sigma$, avec t une translation et σ une application linéaire orthogonale. Considérons le groupe N des translations de $\mathbf{R}^n$ et le groupe H des applications linéaires orthogonales de $\mathbf{R}^n$. Alors N est isomorphe à $\mathbf{R}^n$ (groupe additif) via $\mathbf{R}^n \ni x \mapsto (a \mapsto a+x) = t_x \in N$, et H est isomorphe au groupe $\mathrm{O}_n(\mathbf{R})$ des matrices orthogonales. Soient $h \in H$ et $x \in \mathbf{R}^n$. Calculons, pour tout $a \in \mathbf{R}^n$:

$$(ht_xh^{-1})(a) = (ht_x)(h^{-1}(a)) = h(x + h^{-1}(a)) = h(x) + a = t_{h(x)}(a)$$

ce qui montre que $ht_xh^{-1} = t_{h(x)}$. Le sous-groupe $N \subset G$ est donc distingué. L'intersection $N \cap H = \{e\}$ car une translation qui fixe l'origine est l'identité. La Proposition 14.5 montre que G est isomorphe à $\mathbf{R}^n \times_\alpha \mathrm{O}_n(\mathbf{R})$, où $(\alpha(A))(x) = Ax$.

(3) Soit B le sous-groupe de $\mathrm{GL}_2(\mathbf{R})$ qui a pour éléments les matrices triangulaires supérieur: $B = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbf{R},\ ac \neq 0\}$. Soit $U \subset B$ le sous-groupe des matrices $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbf{R}\}$. Soit $T \subset B$ le sous-groupe des matrices diagonales: $T = \{\left(\begin{smallmatrix} a & 0 \\ 0 & c \end{smallmatrix}\right) \mid a, c \in \mathbf{R},\ ac \neq 0\}$. On voit tout de suite que $UT = B$ et que $U \cap T = \{e\}$. Le calcul

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & ac^{-1}b \\ 0 & 1 \end{pmatrix}$$

montre que U est distingué (comme $B = UT$, il suffit de vérifier que $gUg^{-1} \subset U$ pour $g \in T$). La Proposition 14.5 dit alors que $B \cong U \times_\alpha T$, où l'opération α de T sur U est donnée par la formule ci-dessus. En utilisant les isomorphismes $\mathbf{R} \to U$: $b \mapsto \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ et $\mathbf{R}^* \times \mathbf{R}^* \to T$: $(a, c) \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & c \end{smallmatrix}\right)$ on voit que B est isomorphe au produit semi-direct $\mathbf{R} \times_\beta (\mathbf{R}^* \times \mathbf{R}^*)$, avec $(\beta(a, c))(b) = ac^{-1}b$.

(4) Le groupe S_n, $n \geq 2$, est isomorphe à un produit semi-direct $\mathrm{A}_n \times_\alpha \mathbf{Z}/2\mathbf{Z}$.

(5) On a $GL_n(\mathbf{R}) \cong \mathrm{SL}_n(\mathbf{R}) \times_\alpha \mathbf{R}^*$ pour un certain α.

15 Exercices.

1. Quels des triples suivants sont des groupes?
   1: $(\mathbf{N}, +, 0)$, 2: $(\{x \in \mathbf{Q}^* \mid x > 0\}, \cdot, 1)$, 3: $(\mathbf{R}, \circ, 1)$ où $x \circ y = x + y - 1$,
   4: $(]-\pi/2, \pi/2[\,, x \circ y, 0)$ où $x \circ y = \arctan(\tan(x) + \tan(y))$, 5: $(\mathrm{M}_n(\mathbf{R}), +, 0)$,
   6: $(\mathrm{M}_n(\mathbf{R}), \cdot, I)$.
2. Soit G un groupe tel que $\forall x \in G$: $x^2 = e$. Montrer que G est commutatif.
3. Soit G un groupe. Montrer que l'antimorphisme $\iota\colon G \to G\colon x \mapsto x^{-1}$ est un morphisme si et seulement si G est commutatif.
4. Soit G un groupe tel que l'application $f\colon G \to G\colon x \mapsto x^2$ est un morphisme. Montrer que G est commutatif.
5. Soit G un groupe fini tel que $\#G$ est pair. Montrer que G contient un élément d'ordre 2. (Indication: considérer l'application $\iota\colon G \to G\colon x \mapsto x^{-1}$.)
6. Soit G un groupe fini et $x \in G$ d'ordre 2. Montrer que $\#G$ est pair. (Indication: considérer l'application $t_x\colon G \to G\colon y \mapsto xy$.)
7. Soit p premier et $n \geq 1$. Montrer que $\#\mathrm{GL}_n(\mathbf{Z}/p\mathbf{Z}) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$. (Indication: c'est aussi le nombre de bases de l'espace vectoriel $(\mathbf{Z}/p\mathbf{Z})^n$ sur $\mathbf{Z}/p\mathbf{Z}$. Pour le premier vecteur d'une base il y a $p^n - 1$ choix, pour le deuxième $p^n - p$ etc.)
8. Donner un exemple de: un groupe G et des sous-groupes H_1 et H_2, tels que $H_1 \cup H_2$ n'est pas un sous-groupe.
9. Soit G un groupe, H_1 et H_2 des sous-groupes. Montrer que $H_1 \cup H_2$ est un sous-groupe si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.
10. On définit le centre $C = C(G)$ d'un groupe G par: $C = \{x \in G \mid \forall y \in G\colon xy = yx\}$.
    (a) Montrer que $C \subset G$ est un sous-groupe distingué.
    (b) Montrer que G est commutatif si et seulement si $C = G$.
    (c) Montrer que pour $f\colon G_1 \to G_2$ un morphisme surjectif on a $f(C(G_1)) \subset C(G_2)$.
    (d) Montrer que $C(\mathrm{GL}_2(\mathbf{R})) = \{\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \mid x \in \mathbf{R}^*\}$.
11. Soient G_1 et G_2 des groupes. Montrer que $(G_1 \times G_2, \cdot, (e_1, e_2))$, où $(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$, est un groupe. Ce groupe est appelé le produit (direct, ou cartésien) de G_1 et G_2.
12. (a) Montrer que $\mathbf{Z}/6\mathbf{Z}$ et S_3 ne sont pas isomorphes.
    (b) Montrer que $\mathbf{Z}/6\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ sont isomorphes.
    (c) Montrer que $(\mathbf{R}, +, 0)$ et $(\{x \in \mathbf{R} \mid x > 0\}, \cdot, 1)$ sont isomorphes.
    (d) Donner un morphisme surjectif de $(\mathbf{C}, +, 0)$ sur $\mathbf{C}^*$.
13. Soit G un groupe. Un élément de G de la forme $xyx^{-1}y^{-1}$ est appelé un commutateur. Soit G' le sous-groupe de G engendré par tous les commutateurs: $G' = \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$.
    (a) Montrer que G' est un sous-groupe distingué de G.
    (b) Soit $f\colon G_1 \to G_2$ un morphisme avec G_2 commutatif. Montrer que $G_1' \subset \ker(f)$.
14. Soit $f\colon G_1 \to G_2$ un morphisme et $x \in G_1$ d'ordre fini. Montrer que $\mathrm{ordre}(f(x)) | \mathrm{ordre}(x)$.

15. Soit $G := \{\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{R}) \mid b \neq 0\}$.
   (a) Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbf{R})$.
   (b) Montrer que $H_1 := \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) \mid b \neq 0\}$ est un sous-groupe non-distingué de G.
   (c) Montrer que $H_2 := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbf{R}\}$ est un sous-groupe distingué de G.
   (d) Montrer que $f_1 \colon G \to \mathbf{R}^* \colon \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \mapsto b$ est un morphisme et que $H_2 = \ker(f_1)$.
   (e) Montrer que $f_2 \colon G \to \mathbf{R} \colon \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \mapsto a$ n'est pas un morphisme.
   (f) Montrer que $g_1 \colon \mathbf{R}^* \to H_1 \colon b \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$ est un isomorphisme.
   (g) Montrer que $g_2 \colon \mathbf{R} \to H_2 \colon a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ est un isomorphisme.
16. Soit $x \in G$ d'ordre fini. Montrer que $x^n = e$ si et seulement si $\mathrm{ordre}(x) | n$.
17. Soit $f \colon G_1 \to G_2$ un morphisme de groupes.
   (a) Montrer que pour tout sous-groupe $H_1 \subset G_1$, l'image fH_1 de H_1 par f est un sous-groupe de G_2.
   (b) Montrer que pour tout sous-groupe $H_2 \subset G_2$, l'image réciproque $f^{-1}H_2$ de H_2 par f est un sous-groupe de G_1 contenant $\ker(f)$.
   (c) Soit maintenant f surjectif, $X_1 := \{H_1 \subset G_1 \mid H_1 \text{ sous-groupe contenant } \ker(f)\}$ et $X_2 = \{H_2 \subset G_2 \mid H_2 \text{ sous-groupe}\}$. On a alors des applications $f_* \colon X_1 \to X_2 \colon H_1 \mapsto fH_1$ et $f^* \colon X_2 \to X_1 \colon H_2 \mapsto f^{-1}H_2$. Montrer que f_* et f^* sont des applications inverses.
18. Soit $n \in \mathbf{Z}$. Déterminer tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.
19. Soit G un groupe. Soit $\mathrm{Aut}(G)$ l'ensemble d'automorphismes de G.
   (a) Montrer que $(\mathrm{Aut}(G), \circ, \mathrm{id})$, où $\circ$ est la composition, est un groupe. Montrer que pour tout $x \in G$ l'application $\phi_x \colon G \to G \colon y \mapsto xyx^{-1}$ est un automorphisme de G.
   (b) Montrer que $\phi \colon G \to \mathrm{Aut}(G) \colon x \mapsto \phi_x$ est un morphisme. Son image s'appelle le groupe des automorphismes intérieurs de G et se note $\mathrm{Inn}(G)$.
   (c) Montrer que $\mathrm{Inn}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
20. Ecrire comme produit de cycles disjoints:
   1: $\sigma = (3,1,4)(1,5,9,2,6)(5,3) \in \mathrm{S}_9$ 2: σ^{-1}, où $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{smallmatrix}\right) \in \mathrm{S}_5$
   3: σ^{-1}, où $\sigma = (5,6,2)(1,3) \in \mathrm{S}_6$.
21. Soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{smallmatrix}\right) \in \mathrm{S}_{12}$. Calculer σ^{2000}.
22. Déterminer les 7 ensembles $X_n := \{\mathrm{ordre}(\sigma) \mid \sigma \in \mathrm{S}_n\}$, où $1 \leq n \leq 7$.
23. Montrer que $\sigma \in \mathrm{S}_n$ entraîne que $\mathrm{ordre}(\sigma) \leq e^{n/e}$.
24. Soit $n \geq 3$. Montrer que le centre $C(\mathrm{S}_n)$ de S_n est trivial; c'est à dire, montrer que tout τ dans S_n qui commute avec tous les σ de S_n est égal à (1).
25. Soit $2 \leq k \leq n$. Calculer le nombre de cycles de longueur k dans S_n. (On devrait trouver $n(n-1)\cdots(n-k+1)/k$.)
26. Montrer que $\sigma \in \mathrm{S}_{10}$ entraîne $\mathrm{ordre}(\sigma) \leq 30$.
27. Soit G un groupe. Montrer que pour tout $x \in G$ l'application $t_x \colon G \to G \colon y \mapsto xy$ est une bijection. Montrer que l'application $t \colon G \to \mathrm{Sym}(G) \colon x \mapsto t_x$ est un morphisme injectif. Conclure que G est isomorphe à un sous-groupe de $\mathrm{Sym}(G)$.

28. Soit G un groupe fini à n éléments. Montrer que G est isomorphe à un sous-groupe de S_n. Expliciter ceci pour $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

29. (a) Trouver les $\sigma \in \mathrm{S}_4$ tels que $\sigma^2 = (1,2)(3,4)$.

    (b) Soit $n \geq 2$. Est-ce qu'il existe $\sigma \in \mathrm{S}_n$ tel que $\sigma^2 = (1,2)$? Même question pour $n \geq 6$ et $(1,2)(3,4,5,6)$.

    (c) Décrire l'ensemble $\{\sigma^2 \,|\, \sigma{\in}\mathrm{S}_n\}$. (Plus précisément: quelles sont les longueurs des cycles dans les décompositions en cycles disjoints des σ^2?)

30. Montrer que S_n est engendré par $\{(1,2),(2,3),\ldots,(n{-}1,n)\}$.

31. Montrer que pour $n \geq 3$ le groupe A_n est engendré par ses cycles de longueur 3.

32. Montrer que S_n est engendré par $\{(1,2),(2,3,\ldots,n)\}$.

33. Pour quels n est-ce que $\{(1,2,3),(3,4,\ldots,n)\}$ engendre S_n?

34. Montrer que A_n est engendré par les commutateurs de S_n; c'est à dire, que $\mathrm{A}_n = \langle\{\sigma\tau\sigma^{-1}\tau^{-1} \,|\, \sigma,\tau{\in}\mathrm{S}_n\}\rangle$. (Indication: calculer $(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}$.) Conclure que si $f\colon \mathrm{S}_n \to G$ est un morphisme avec G commutatif, $\mathrm{A}_n \subset \ker(f)$.

35. Soit $f\colon \mathrm{S}_n \to \mathrm{S}_m$ un morphisme. Montrer que $f\mathrm{A}_n \subset \mathrm{A}_m$. (Indication: faire d'abord l'exercice précédent.)

36. Montrer que si σ et τ sont des cycles de longueur n dans S_n tels que $\sigma\tau = \tau\sigma$, on a $\tau \in \langle\sigma\rangle$.

37. Soient n impair et $\sigma \in \mathrm{S}_n$ tel que $\sigma^2 = (1)$. Montrer que σ a un point fixe; c'est à dire, montrer qu'il existe i tel que $\sigma(i) = i$.

38. Pour chacune des trois conditions dans la Définition 3.1, donner un exemple d'une relation $\sim$ sur un ensemble X qui ne satisfait pas à cette condition tandis qu'elle satisfait bien aux deux autres.

39. Soit $E(n)$ le nombre de relations d'équivalence sur l'ensemble $\{1,2,\ldots,n\}$. Calculer $E(n)$ pour $n \leq 5$.

40. (a) Soient X_1 et X_2 deux ensembles, $\sim_1$ une relation d'équivalence sur X_1 et $\sim_2$ une relation d'équivalence sur X_2. Soit $\sim$ la relation sur $X := X_1 \times X_2$ telle que $(x_1,x_2){\sim}(y_1,y_2)$ si et seulement si $x_1{\sim_1}y_1$ et $x_2{\sim_2}y_2$. Montrer que pour (x_1x_2) dans X la classe d'équivalence de (x_1,x_2) pour $\sim$ est le produit de la classe d'équivalence de x_1 pour $\sim_1$ par la classe d'équivalence de x_2 pour $\sim_2$.

    Notons par p, p_1 et p_2 les projections canoniques. Montrer qu'il existe une bijection unique $f\colon X/{\sim} \to X_1/{\sim_1} \times X_2/{\sim_2}$ tel que $f(p(x_1,x_2)) = (p_1(x_1),p_2(x_2))$ pour tout (x_1,x_2) dans X.

    (b) Soient G un groupe et $\sim$ une relation d'équivalence sur G qui est compatible avec la structure de groupe de G. Montrer qu'il existe une application unique $\cdot\colon G/{\sim} \times G/{\sim} \to G/{\sim}$ qui fait de $G/{\sim}$ un groupe et de la projection $p\colon G \to G/{\sim}$ un morphisme, en utilisant la partie (a) et la Proposition 3.2.

41. Soit G un groupe opérant sur un ensemble X. Montrer que les trois conditions suivantes sont équivalentes:

    (1) G opère transitivement sur X.

(2) Il existe un x dans X tel que pour tout y dans X il existe un g dans G avec $y = gx$.
(3) X n'est pas vide et pour tout x et y dans X il existe g dans G tel que $y = gx$.

42. (a) Soit $\sigma = (i_1, \ldots, i_k)$ un cycle de longueur k dans S_n. On considère l'opération de $\langle\sigma\rangle \subset \mathrm{S}_n$ sur $\{1, 2, \ldots, n\}$. Déterminer les orbites pour cette opération.
    (b) Soit $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ une décomposition en cycles disjoints d'un élément σ de S_n. Donner la relation entre les longueurs l_i des σ_i et les orbites dans $\{1, 2, \ldots, n\}$ pour l'opération de $\langle\sigma\rangle$.
43. Soit G un groupe. On considère l'opération à gauche de G sur lui-même par conjugaison. L'orbite $\{aba^{-1} \mid a \in G\}$ de b s'appelle la classe de conjugaison de b. Le stabilisateur $G_b = \{a{\in}G \mid aba^{-1}{=}b\}$ s'appelle le centralisateur de b et se note $C(b)$.
    (a) Déterminer les classes de conjugaison et les centralisateurs dans S_3.
    (b) Soit $n \geq 1$. On appelle partition de n une suite finie $(x_1, x_2, \ldots, x_r)$ d'entiers telle que $n = x_1{+}x_2{+} \cdots {+}x_r$ et $x_1{\geq}x_2{\geq} \cdots {\geq}x_r{>}0$. Donner une bijection entre l'ensemble des classes de conjugaison dans S_n et l'ensemble des partitions de n.
    (c) Pour tout $\sigma \in \mathrm{S}_4$, déterminer son centralisateur $C(\sigma)$ et sa classe de conjugaison $\mathrm{conj}(\sigma)$. Vérifier dans chaque cas que $|\mathrm{conj}(\sigma)|\,|C(\sigma)| = |\mathrm{S}_4|$.
44. Soit G un groupe opérant à gauche sur un ensemble X. Soit $F := \{f\colon X \to \mathbf{R}\}$ l'ensemble des fonctions sur X à valeurs dans $\mathbf{R}$. Montrer que l'application $F \times G \to F$: $(f, a) \mapsto (x{\mapsto}f(ax))$ définit une opération à droite de G sur F.
45. Soient k un corps et $n \geq 1$ un entier. Montrer que l'application $\mathrm{GL}_n(k) \times k^n \to k^n$: $(A, x) \mapsto Ax$ définit une opération à gauche. Déterminer les orbites. Déterminer le stabilisateur de $(1, 0, \ldots, 0)$.
46. Soient k un corps et $n \geq 1$ un entier. Nous allons étudier les relations d'équivalence induites par quelques opérations de $\mathrm{GL}_n(k)$ sur $\mathrm{M}_n(k)$.
    (a) Considérons l'opération de $\mathrm{GL}_n(k)$ sur $\mathrm{M}_n(k)$ par conjugaison. Montrer que pour x et y dans $\mathrm{M}_n(k)$ on a $x \sim y$ si et seulement si x et y sont des matrices semblables.
    (b) Faisons opérer $\mathrm{GL}_n(k)$ sur $\mathrm{M}_n(k)$ par multiplication à gauche. Montrer que pour x et y dans $\mathrm{M}_n(k)$ on a $x \sim y$ si et seulement si $\ker(x) = \ker(y)$.
    (c) Faisons opérer $\mathrm{GL}_n(k)$ sur $\mathrm{M}_n(k)$ à droite par multiplication à droite. Montrer que pour x et y dans $\mathrm{M}_n(k)$ on a $x \sim y$ si et seulement si $\mathrm{im}(x) = \mathrm{im}(y)$.
47. Soient k un corps et $n \geq 1$, $m \geq 1$ des entiers. Considérons l'opération suivante de $\mathrm{GL}_n(k) \times \mathrm{GL}_m(k)$ sur $\mathrm{M}_{n,m}(k)$ donnée par: $(g, h){\cdot}x = gxh^{-1}$. Soit $\sim$ la relation d'équivalence sur $\mathrm{M}_{n,m}(k)$ induite par cette opération. Montrer que pour x et y dans $\mathrm{M}_{n,m}(k)$ on a $x \sim y$ si et seulement si x et y ont même rang.
48. Donner un exemple d'un groupe G et une relation d'équivalence sur G qui n'est pas compatible avec la multiplication de G.
49. Soit G un groupe opérant à gauche sur un ensemble X. Soit $n \geq 1$. On dit que l'opération de G sur X est n-transitive si pour tous $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ dans X^n avec les x_i tous distincts et les y_i tous distincts il existe $g \in G$ tel que $g(x_i) = y_i$ pour tout i.
    (a) Montrer que l'opération de S_n sur $\{1, 2, \ldots, n\}$ est n-transitive.

(b) Montrer que pour $n \geq 3$ l'opération de A_n sur $\{1, 2, \dots, n\}$ est $(n-2)$-transitive mais pas $(n-1)$-transitive.

50. On dit qu'un groupe G est cyclique s'il existe un élément x dans G tel que $G = \langle x \rangle$. Montrer qu'un groupe fini d'ordre un nombre premier p est cyclique.

51. Soient G un groupe et H un sous-groupe. Donner une bijection entre G/H et $H\backslash G$. On appelle $|G/H| = |H\backslash G|$ l'indice de H dans G, et on le note $[G : H]$.

52. Soient G un groupe fini et $H \subset G$ un sous-groupe. Supposons que $H \neq G$. Nous allons montrer que H ne coupe pas toutes les classes de conjugaison de G, ou autrement dit, qu'il existe une classe de conjugaison C de G telle que $H \cap C = \emptyset$.

 (a) Montrer que H coupe toutes les classes de conjugaison de G si et seulement si

$$\bigcup_{a \in G} aHa^{-1} = G.$$

 (b) Montrer que pour a et b dans G: $aH = bH$ entraîne $aHa^{-1} = bHb^{-1}$.

 (c) Soit $n = |G|$ et $d = |H|$. Montrer que

$$\left| \bigcup_{a \in G} aHa^{-1} \right| \leq 1 + (n/d)(d-1)$$

 (Indication: $|aHa^{-1}| = d$ et $e \in aHa^{-1}$.)

53. Un groupe de 35 éléments opère sur un ensemble de 19 éléments sans fixer aucun d'entre eux. Combien y a-t'il d'orbites pour cette opération?

54. Soient G un groupe et $G' \subset G$ le sous-groupe engendré par les commutateurs: $G' = \langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$. Montrer que G' est distingué. Montrer que G/G' est commutatif.

55. Soit G un groupe et soit $C \subset G$ son centre: $C = \{a{\in}G \mid \forall b{\in}G : \ \ ba = ab\}$. On sait que C est un sous-groupe distingué. Supposons qu'il existe $x \in G/C$ tel que $G/C = \langle x \rangle$ (autrement dit, on suppose que G/C est cyclique). Montrer que G est commutatif.

56. Soient p un nombre premier et $0 < i < p$. Dans cet exercice on va montrer que $p | C_p^i$, à l'aide d'une opération du groupe $\mathbf{Z}/p\mathbf{Z}$ sur un ensemble X.

 (a) Soit $X = \{A \subset \mathbf{Z}/p\mathbf{Z} \mid |A| = i\}$. Montrer que l'opération à gauche par translations de $\mathbf{Z}/p\mathbf{Z}$ sur lui-même induit une opération à gauche de $\mathbf{Z}/p\mathbf{Z}$ sur X.

 (b) Montrer que cette opération de $\mathbf{Z}/p\mathbf{Z}$ sur X est libre.

 (c) Conclure en utilisant la formule qui relie $|X|$ et les cardinaux des orbites.

 (d) Où est-ce qu'on a utilisé l'hypothèse "$0 < i < p$"?

57. Soient G un groupe et $N \subset G$ un sous-groupe distingué. Montrer que $G/N = \{\overline{e}\}$ si et seulement si $N = G$. (Indication: utiliser les définitions.)

58. (a) Soit C le cercle $\{z \in \mathbf{C} \mid |z|{=}1\}$. Montrer que C est un sous-groupe de $\mathbf{C}^*$.

 (b) Montrer que $\mathbf{R}/\mathbf{Z}$ est isomorphe à C. (Indication: considérer le morphisme de groupes $f \colon \mathbf{R} \to \mathbf{C}^*\colon x \mapsto \exp(2\pi i x)$.)

59. Soient $G := \mathrm{S}_4$ et $N := \{(1), (1{,}2)(3{,}4), (1{,}3)(2{,}4), (1{,}4)(2{,}3)\}$. Montrer que $N \subset G$ est un sous-groupe distingué et que G/N est isomorphe à S_3. (Indication: voir Exemple 4.2 (3).)

60. Soit $G := \{\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{R}) \mid a{\in}\mathbf{R},\ b{\neq}0\}$. Soit $N := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{R}) \mid a{\in}\mathbf{R}\}$.
   (a) Montrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbf{R})$.
   (b) Montrer que N est un sous-groupe distingué de G.
   (c) Montrer que G/N est isomorphe à $\mathbf{R}^*$.
61. Pour n et m des entiers positifs, calculer $|\mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})|$. (Indication: utiliser la bijection (7.1). Si on ne voit pas quel sera le résultat, essayer quelques cas spéciaux.)
62. Soient G un groupe et H un groupe additif (et donc commutatif). Pour des applications $f, g\colon G \to H$ on définit une application $f * g\colon G \to H$: $(f * g)(x) = f(x) + g(x)$.
   (a) Montrer que si f et g sont des morphismes, $f * g$ est un morphisme.
   (b) Montrer que $\mathrm{Hom}(G, H)$ avec la multiplication $*$ est un groupe commutatif.
   (c) Soient n et m des entiers positifs. Montrer que $\mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$, muni de cette multiplication $*$, est isomorphe à $\mathbf{Z}/\mathrm{pgcd}(n, m)\mathbf{Z}$. (Indication: montrer que la bijection (7.1) est un isomorphisme.)
63. (a) Donner quatre points distincts dans $\mathbf{R}^3$ tels que les distances entre eux sont toutes les mêmes. (Indication: pour trouver une belle solution, considérer les sommets d'un cube.)
   (b) Soit $n \geq 1$. Montrer que dans $\mathbf{R}^n$ il existe $n{+}1$ points distincts tels que les distances entre eux sont toutes les mêmes. (Indication: trouver d'abord $n{+}1$ points dans $\mathbf{R}^{n+1}$ avec cette propriété, et remarquer ensuite que ces points sont contenus dans un hyperplan.)
   (c) Montrer que dans $\mathbf{R}^n$ on ne peut pas trouver $n{+}2$ points distincts tels que toutes les distances entre eux sont les mêmes. (Indication: utiliser la partie précédente.)
64. Considérons l'ensemble X des sommets du tétraèdre régulier plongé dans $\mathbf{R}^3$ comme dans la section 9.3. Montrer que chaque élément de $\mathrm{Iso}(X)$ est induit par un élément unique du groupe orthogonal $\mathrm{O}_3(\mathbf{R})$, et donner la liste des 24 matrices orthogonales ainsi obtenues.
65. On considère l'ensemble $X = \{(\pm 1, \pm 1, \pm 1)\}$ de 8 points dans $\mathbf{R}^3$. Noter que X est l'ensemble des sommets d'un cube. Soit G le groupe d'isométries de X (on considère ici la distance usuelle sur $\mathbf{R}^3$).
   (a) Montrer que $|G| = 48$.
   (b) Montrer que pour tout $\sigma \in G$ il existe un élément unique s de $\mathrm{O}_3(\mathbf{R})$ telle que $\sigma(x) = s(x)$ pour tout $x \in X$. Ecrire les 48 matrices qui correspondent aux éléments de G.
   (c) Notons par $i\colon G \to \mathrm{O}_3(\mathbf{R})$ l'injection définie par la partie (b). Montrer que i est un morphisme. Soit $f_1\colon G \to \{\pm 1\}$ le morphisme $g \mapsto \det(i(g))$.
   (d) Soit Y l'ensemble des diagonales du cube qui passent par $(0, 0, 0)$. Choisissez une bijection entre $\{1, 2, 3, 4\}$ et Y. Soit $f_2\colon G \to \mathrm{S}_4$ le morphisme induit par l'opération de G sur Y et la bijection choisie. Montrer que $f\colon G \to \mathrm{S}_4 \times \{\pm 1\}$ donné par $g \mapsto (f_1(g), f_2(g))$ est un isomorphisme.

66. Soit P un polyèdre convexe dans un $\mathbf{R}$-espace vectoriel E. Soit $g\colon E \to E$ un élément du groupe affine de E, c'est à dire, g est de la forme $t \circ h$, avec $t\colon E \to E$ une translation et $h\colon E \to E$ une application linéaire inversible.
    (a) Montrer que $g(P)$ est un polyèdre convexe dans E.
    (b) Montrer que que pour toute face F de P, l'image $g(F)$ de F par g est une face de $g(P)$, de même dimension que F.
67. Soient G un groupe fini et p un nombre premier. Montrer que le cardinal de l'ensemble des éléments d'ordre p est un multiple de $p-1$.
68. Soit G un groupe fini d'ordre n. Montrer que si p est un diviseur de n et x un élément de G d'ordre p alors le cardinal de l'ensemble des conjugués de x divise n/p.
69. Soit G un groupe fini à 15 éléments. On suppose que G n'est pas commutatif.
    (a) Montrer que le centre de G est réduit à l'élément neutre de G. (Indication: utiliser l'exercice 55.)
    (b) On fait opérer G sur G par conjugaison. Montrer qu'il existe exactement une orbite à 5 éléments. Montrer que les éléments de cette orbite sont d'ordre 3.
    (c) Conclure que tout groupe d'ordre 15 est commutatif.
70. Soit k un corps de caractéristique $p > 0$. On fait opérer $G := \mathbf{Z}/p\mathbf{Z}$ sur $k[X]$ par $(i, P) \mapsto P(X+i)$. On fixe un élément a de k et on considère le polynôme $F(X) := X^p - X - a$.
    (a) Montrer que F est invariant par l'action de G; en déduire que G opère sur l'ensemble des facteurs irréductibles (unitaires) de F dans $k[X]$.
    (b) Si $H \in k[X]$ est G-invariant, montrer que le degré de H est multiple de p. (On pourra, par exemple, considérer les racines de H dans une clôture algébrique de k.)
    (c) Déduire de (a) et (b) que F est soit irréductible, soit décomposé dans $k[X]$.
    (d) Montrer que $X^p - X - 1$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$.
71. (a) Soient s et t deux entiers. Montrer qu'on peut écrire $s = uu'$, $t = vv'$ avec u, v, u', v' dans $\mathbf{Z}$, u et v premiers entre eux et $\operatorname{ppcm}(s,t) = uv$.
    (b) Soient a et b deux éléments d'un groupe G, d'ordres respectifs s et t. On suppose que $ab = ba$. Montrer que (avec les notations du (a)) $a^{u'}b^{v'}$ est d'ordre $\operatorname{ppcm}(s,t)$.
    (c) Si G est un groupe commutatif fini, montrer qu'il existe un élément de G dont l'ordre est multiple de tous les ordres des éléments de G. Ce résultat est-il encore valable si G n'est pas commutatif?
72. Soit G un groupe commutatif fini d'ordre n. On suppose que pour tout d divisant n, G admet un unique sous-groupe d'ordre d. Montrer que G est cyclique. (Utiliser l'exercice précédent.)
73. Soit K un corps commutatif, et soit G un sous-groupe fini d'ordre n de K^*.
    (a) Montrer que $G = \{x \in K \mid x^n = 1\}$. (Considérer le polynôme $X^n - 1$.)
    (b) Montrer que G est cyclique. (Utiliser l'exercice précédent.)
74. Montrer que pour $n \geq 8$ le groupe A_n est engendré par ses éléments de la forme $\sigma_1\sigma_2$, avec σ_1 et σ_2 des cycles disjoints de longueur 4.

75. On se propose de montrer que le groupe $\mathrm{SL}_2(\mathbf{C})/\{\pm 1\}$ est simple.

    (a) Soit $G := \mathrm{SL}_2(\mathbf{C})$. Montrer qu'il suffit de démontrer que les seuls sous-groupes distingués de G sont G, $\{1\}$ et $\{\pm 1\}$.

    (b) Montrer, en utilisant que par des opérations élémentaires sur les lignes et les colonnes qui préservent le déterminant on peut transformer tout élément de G en l'élément neutre, que les matrices de la forme $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ engendrent G.

    (c) Supposons, aussi dans les parties qui suivent, que N est un sous-groupe distingué de G qui contient un élément h différent de 1 et de -1. Montrer que si N contient un élément h de la forme $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{smallmatrix}\right)$ avec $\lambda \neq \pm 1$, alors N contient tous les élément de la forme $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$. (Indication: considérer le commutateur de h et $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$.)

    (d) Montrer que si N contient un élément de la forme $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ avec $a \neq 0$, alors N contient tous les éléments de la forme $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$. (Indication: conjuguer avec des éléments bien choisis de G.)

    (e) Montrer, en utilisant la forme canonique de Jordan, que N contient un élément de la forme $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{smallmatrix}\right)$ avec $\lambda \neq \pm 1$ ou $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ avec $a \neq 0$. Conclure.

76. (a) Pour $G \in \{\mathrm{S}_3, \mathrm{S}_4, \mathrm{S}_5\}$ et $p \in \{2, 3, 5\}$ donner des générateurs pour un p-groupe de Sylow dans G et calculer le nombre des p-groupes de Sylow.

    (b) Donner un exemple d'un groupe fini G, d'un nombre premier p et deux p-groupes de Sylow distincts S_1 et S_2 dans G où $S_1 \cap S_2 \neq \{e\}$. (Indication: on peut prendre $G = \mathrm{S}_4$.)

77. Déterminer les p-groupes de Sylow des groupes diédraux D_n pour $n \geq 3$.

78. Déterminer les p-groupes de Sylow du groupe des symétries du cube.

79. Montrer que les 2-groupes de Sylow du groupe des symétries du dodécaèdre sont isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. (Indication: utiliser un des 5 cubes inscrits dans le dodécaèdre.)

80. (a) Soit G un groupe fini. Soit p premier tel que p divise $|G|$ mais p^2 ne divise pas $|G|$. Montrer que deux p-groupes de Sylow distincts dans G ont intersection égale à $\{e\}$. Montrer que le nombre d'éléments d'ordre p dans G est $p-1$ fois le nombre de p-groupes de Sylow dans G.

    (b) Montrer qu'un groupe d'ordre 30 a un sous-groupe distingué d'ordre 2, 3 ou 5.

81. Soient p premier, N un entier tel que $1 < N < p$ et G un groupe d'ordre pN. Montrer que G n'est pas simple.

82. Montrer que tous les groupes finis simples d'ordre < 60 sont commutatifs.

83. Montrer qu'un groupe fini commutatif est isomorphe au produit direct de ses p-groupes de Sylow. (Indication: soient $p_1, p_2, \ldots, p_r$ les nombres premiers qui divisent $|G|$ et S_i l'unique p_i-groupe de Sylow dans G. Montrer que l'application

$$f\colon S_1 \times S_2 \times \cdots \times S_r \longrightarrow G, \qquad (x_1, x_2, \ldots, x_r) \mapsto x_1 x_2 \cdots x_r$$

est un morphisme. Etudier $\ker(f)$.)

84. Soient G un groupe fini, p_1 et p_2 des nombres premiers distincts, $H_1 \subset G$ un sous-groupe qui est un p_1-groupe et $H_2 \subset G$ un sous-groupe qui est un p_2-groupe. Montrer que $H_1 \cap H_2 = \{e\}$.
85. Soit p premier. Montrer qu'un groupe fini G est un p-groupe si et seulement si tout $x \in G$ a pour ordre une puissance de p.
86. Soient G un groupe, $H \subset G$ un sous-groupe distingué et p un nombre premier. Montrer que G est un p-groupe si et seulement si H et G/H sont des p-groupes.
87. Soient p premier et $k \geq 0$. Soit G un groupe fini tel que p^k divise $|G|$. Montrer qu'il existe un sous-groupe H de G tel que $|H| = p^k$. (Indication: on se ramène, par les théorèmes de Sylow, au cas où G est un p-groupe. Pour les p-groupes on procède par récurrence sur k en utilisant que le centre d'un p-groupe est non-trivial.)
88. Soient p premier et G un p-groupe. Montrer que pour tout $k \geq 0$ tel que p^k divise $|G|$ il existe un sous-groupe distingué H de G tel que $|H| = p^k$. (Indication: récurrence sur k en utilisant que le centre d'un p-groupe est non-trivial.)
89. Soit G un groupe fini tel que ses p-groupes de Sylow sont distingués. Montrer que G est isomorphe au produit direct de ses p-groupes de Sylow. (Indication: soient $p_1, p_2, \ldots, p_r$ les nombres premier qui divisent $|G|$ et S_i l'unique p_i-groupe de Sylow dans G. Montrer que pour tout i le sous-groupe $N_i := \langle \cup_{j \neq i} S_j \rangle$ est un sous-groupe distingué de G et que $|N_i| = \prod_{j \neq i} |S_j|$. Montrer que G/N_i est isomorphe à S_i. Montrer que le morphisme
$$f\colon G \longrightarrow \prod_i G/N_i$$
est un isomorphisme.)
90. Soit G un groupe fini d'ordre p^m avec p premier et $m \geq 2$. Montrer que G a au moins $p^2 + (m-2)(p-1)$ classes de conjugaison. (Indication: récurrence sur m.)
91. Quels sont les invariants s, $n_1, \ldots, n_s$ du groupe $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/100\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z}$?
92. Pour $n \in \{1, 2, 3\}$ calculer le nombre de groupes commutatifs à isomorphisme près d'ordre 2^n, 5^n et 10^n.
93. Redémontrer le résultat de l'exercice 73: un sous-groupe fini G du groupe multiplicatif K^* d'un corps K est cyclique. (Indication: on sait qu'il existe $s \geq 0$, $n_1, \ldots, n_s$ avec $n_i > 1$, $n_s | \cdots | n_1$ et $G \cong \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$. Montrer que le nombre de racines dans K du polynôme $X^{n_s} - 1$ est alors au moins n_s^s et conclure que $s \leq 1$.)
94. Trouver une base du sous-groupe $H = \{(a, b, c) \mid a+b+c = 0\} \subset \mathbf{Z}^3$. (Indication: suivre la démonstration du Théorème 12.17.)
95. Trouver une base du sous-groupe $H = \{(a, b, c) \mid a+b+c \equiv 0 \pmod 3\} \subset \mathbf{Z}^3$.
96. Soit $H \subset \mathbf{Z}^2$ le sous-groupe engendré par $\{(2, -2), (6, 10)\}$. Montrer que $\mathbf{Z}^2/H \cong \mathbf{Z}/16\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
97. Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $\{(2, 3, 5), (-3, 1, -2), (5, 2, 0)\}$. Montrer que $\mathbf{Z}^3/H \cong \mathbf{Z}/77\mathbf{Z}$.
98. Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $\{(4, 8, 10), (-6, 6, 0), (6, 6, 12), (-2, 14, 10)\}$. Montrer que $\mathbf{Z}^3/H \cong \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

99. (a) Soient G_1, G_2 et H des groupes commutatifs de type fini. Supposons que $G_1 \times H$ est isomorphe à $G_2 \times H$. Montrer qu'alors G_1 est isomorphe à G_2.

    (b) L'assertion de la partie (a) reste valable si G_1, G_2 et H sont des groupes finis mais non nécessairement commutatifs (ce résultat s'appelle le théorème de Krull-Remak-Schmidt). Montrer par un exemple que l'assertion n'est pas vraie pour les groupes quelconques, même si on les suppose commutatifs.

100. Soit p un nombre premier. Montrer qu'il existe $x \in \mathbf{Z}/p\mathbf{Z}$ tel que $x^2 = -\overline{1}$ si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$. (Indication: traiter d'abord le cas $p = 2$. Pour $p > 2$ considérer l'ordre d'un tel x et utiliser que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.)

101. Calculer:

    (a) $\{x \in \mathbf{Z}/1001\mathbf{Z} \mid x^2 = \overline{1}\}$.

    (b) $\{x \in \mathbf{Z}/1001\mathbf{Z} \mid x^3 = \overline{1}\}$.

    (c) $\{x \in \mathbf{Z}/1001\mathbf{Z} \mid x^2 = -\overline{1}\}$.

    (Indication: factoriser 1001, utiliser le Théorème Chinois.)

102. Soit G un groupe fini commutatif d'ordre $n = p_1^{e_1} \cdots p_r^{e_r}$, avec $p_1, \ldots, p_r$ des nombres premiers distincts. Montrer que la liste associée à G comme dans la Section 13 est: $\mathbf{Z}/p_1\mathbf{Z}$ (e_1 fois),..., $\mathbf{Z}/p_r\mathbf{Z}$ (e_r fois).

103. Pour K un corps et $n \geq 1$ notons par $\mathrm{PSL}_n(K)$ le quotient de $\mathrm{SL}_n(K)$ par son sous-groupe H de matrices scalaires.

    (a) Montrer que H est isomorphe au sous-groupe $\{x \in K^* \mid x^n = 1\}$ de K^*.

    (b) Soit p premier. En sachant que $\mathrm{PSL}_n(\mathbf{Z}/p\mathbf{Z})$ est simple pour $n \geq 2$ et (n, p) différent de $(2, 2)$ et $(2, 3)$, donner la liste associée à $\mathrm{GL}_n(\mathbf{Z}/5\mathbf{Z})$ comme dans la Section 13 pour $n = 1$, 2 et 3.

104. On dit qu'un groupe G est résoluble s'il existe une filtration décroissante $(G_i)_{i\geq 0}$ de G tel que 1: pour tout $i \geq 0$ le sous-groupe G_{i+1} de G_i est distingué et le quotient G_i/G_{i+1} est commutatif, 2: on a $G_0 = G$ et $G_i = \{e\}$ pour i assez grand.

    (a) Soient G un groupe et N un sous-groupe distingué de G. Montrer que G est résoluble si et seulement si N et G/N le sont.

    (b) Soit k un corps et $n \geq 1$. Montrer que le sous groupe B (B pour Borel) de $\mathrm{GL}_n(k)$ dont les éléments g sont tels que $g_{i,j} = 0$ pour $i > j$ est résoluble.

    (c) Pour un groupe G, on définit la filtration par les sous-groupes dérivés comme suit. On pose $G_0 := G$. Pour $i \geq 0$ on définit G_{i+1} comme étant le sous-groupe de G_i qui est engendré par les commutateurs des éléments de G_i. Montrer que G est résoluble si et seulement si cette filtration est finie (autrement dit: si on a $G_i = \{e\}$ pour i suffisamment grand).

    (d) Soit G un groupe fini. Montrer que G est résoluble si et seulement si la liste de groupes finis simples associée à G par le théorème de Jordan-Hölder ne contient que des groupes commutatifs.

(e) Montrer que les seuls $n \geq 1$ tel que S_n est résoluble sont les $n \leq 4$. (La théorie de Galois explique que ceci est la raison profonde pour laquelle il n'y a pas de formule générale pour les racines de l'équation polynomiale de degré ≥ 5 en une variable, qui ne contient que des sommes, différences, produits, divisions et racines d'ordre quelconque.)

105. (a) Donner un exemple d'un groupe qui n'admet pas de filtration de Jordan-Hölder.

  (b) Donner un exemple d'un groupe infini qui admet une filtration de Jordan-Hölder.

106. Soient N et H deux sous-groupes distingués d'un groupe G, tels que $N \cap H = \{e\}$ et $NH = G$. Montrer que l'application $f\colon N \times H \to G\colon (n,h) \mapsto nh$ est un isomorphisme. (Indication: noter que pour $n \in N$ et $h \in H$ on a $nhn^{-1}h^{-1} \in N \cap H$.)

107. Donner un exemple d'un groupe G et deux sous-groupes H et N de G tel que: $H \subset N$, N est distingué dans G, H est distingué dans N mais H n'est pas distingué dans G. (Indication: considérer des produits semi-directs.)

108. Soit $G_1 \overset{f_1}{\hookrightarrow} G_2 \overset{f_2}{\twoheadrightarrow} G_3$ une suite exacte courte. Un morphisme $r\colon G_2 \to G_1$ s'appelle une rétraction de f_1 si $r \circ f_1 = \mathrm{id}_{G_1}$. Supposons que r est une rétraction de f_1. Montrer que le morphisme $f\colon G_2 \to G_1 \times G_3\colon x \mapsto (r(x), f_2(x))$ est un isomorphisme.

109. Soient K un corps et $n \geq 1$.

  (a) Montrer que la suite exacte courte $\mathrm{SL}_n(K) \overset{f_1}{\hookrightarrow} \mathrm{GL}_n(K) \overset{\det}{\twoheadrightarrow} K^*$ est scindée.

  (b) Donner $\alpha\colon K^* \to \mathrm{Aut}(\mathrm{SL}_n(K))$ tel que $\mathrm{GL}_n(K)$ est isomorphe au produit semi-direct $\mathrm{SL}_n(K) \times_\alpha K^*$.

  (c) Montrer que, pour n impair, $\mathrm{GL}_n(\mathbf{R})$ est isomorphe à $\mathrm{SL}_n(\mathbf{R}) \times \mathbf{R}^*$. (Indication: choisir une section $s\colon \mathbf{R}^* \to \mathrm{GL}_n(\mathbf{R})$ de $\det\colon \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^*$ telle que $\mathrm{im}(s)$ est dans le centre de $\mathrm{GL}_n(\mathbf{R})$.)

110. Montrer que le groupe d'isométries du cube est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^3 \times_\alpha \mathrm{S}_3$, où S_3 opère sur $(\mathbf{Z}/2\mathbf{Z})^3$ par permutation des coordonnées. (Indication: considérer l'action du groupe d'isométries sur l'ensemble des trois axes qui joignent les barycentres des faces opposées, ou aussi: considérer les matrices trouvées dans l'exercice 65.)

111. Soient N, H des groupes et $\alpha\colon H \to \mathrm{Aut}(N)$ un morphisme.

  (a) Soit $\sigma \in \mathrm{Aut}(H)$. Posons $\beta := \alpha \circ \sigma$. Montrer que $N \times_\beta H$ est isomorphe à $N \times_\alpha H$.

  (b) Soit $\tau \in \mathrm{Aut}(N)$. Posons $\gamma := \mathrm{Inn}(\tau) \circ \alpha$, où $\mathrm{Inn}(\tau) \in \mathrm{Aut}(\mathrm{Aut}(N))$ est la conjugaison par τ. Montrer que $N \times_\gamma H$ est isomorphe à $N \times_\alpha H$.

112. Donner un exemple de groupes N et H, d'un morphisme non-trivial $\alpha\colon H \to \mathrm{Aut}(N)$, tels que les groupes $N \times_\alpha H$ et $N \times H$ sont isomorphes.

113. Soient p et q des nombres premiers avec $p < q$. Soit G un groupe d'ordre pq.

  (a) Montrer qu'il existe un unique q-groupe de Sylow N dans G et que N est distingué.

  (b) Soit H un p-groupe de Sylow dans G. Montrer que $G = NH$ et que $N \cap H = \{e\}$. Conclure que G est isomorphe à $N \times_\alpha H$, où $\alpha\colon H \to \mathrm{Aut}(N)$ est l'opération par conjugaison.

  (c) Montrer que si $q-1$ n'est pas divisible par p, G est isomorphe à $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

(d) Montrer que si p divise $q-1$, il y a, à isomorphisme près, exactement deux groupes d'ordre pq. (Indication: on a déjà vu qu'un tel G est isomorphe à un produit semi-direct de $\mathbf{Z}/q\mathbf{Z} \times_\alpha \mathbf{Z}/p\mathbf{Z}$, où $\alpha\colon \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/q\mathbf{Z}) \cong \mathbf{Z}/(q-1)\mathbf{Z}$; utiliser l'exercice 111 (a).)

16 Sujets d'examen plus solutions.

Partiel d'algèbre avancée.

le 10 avril 1993, 7:30–9:30

- Vous pouvez consulter tout document.
- Donnez des références pour les résultats que vous utilisez et qui ne se trouvent pas dans les notes du cours.
- Vérifiez vos solutions le mieux possible. Bonne chance.

1. Soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 5 & 3 & 7 & 8 & 9 & 10 & 6 \end{smallmatrix}\right) \in \mathrm{S}_{10}$. Calculer σ^{1999}.
2. Soit $f\colon G_1 \to G_2$ un morphisme de groupes. Supposons que G_1 est engendré par l'ensemble de ses éléments d'ordre 2 et que G_2 est fini et d'ordre impair. Montrer que pour tout $x \in G_1$ on a $f(x) = e_2$ (ici e_2 est l'élément neutre de G_2).
3. Soit G un groupe opérant sur un ensemble X. Supposons que $|G| = 143 = 11{\cdot}13$ et que $|X| = 108$. Montrer qu'il existe $x \in X$ tel que $gx = x$ pour tout $g \in G$. (Indication: supposer qu'il n'en existe pas, considérer les orbites.)
4. Soit $n \geq 5$ un entier impair.
   (a) Soient G un groupe et $X \subset G$ un sous-ensemble qui est stable par conjugaison: $gxg^{-1} \in X$ pour tout $x \in X$ et tout $g \in G$. Montrer que le sous-groupe $\langle X \rangle$ de G engendré par X est distingué.
   (b) Montrer qu'il existe des éléments d'ordre n dans A_n.
   (c) Soit $X = \{\sigma \in \mathrm{A}_n \mid \mathrm{ordre}(\sigma) = n\}$. Montrer que A_n est engendré par X. (Indication: A_n est simple.)

Corrigé du partiel d'algèbre avancée.

le 10 avril 1993, 7:30–9:30

1. $\sigma = (1,2)(3,4,5)(6,7,8,9,10)$ est une décomposition en cycles disjoints. Comme ces cycles sont disjoints, ils commutent, donc: $\sigma^k = (1,2)^k(3,4,5)^k(6,7,8,9,10)^k$ pour tout $k \in \mathbf{Z}$. Les congruences

$$1999 \equiv 1\,(2), \qquad 1999 \equiv 1\,(3) \qquad \text{et} \qquad 1999 \equiv -1\,(5)$$

montrent que

$$\sigma^{1999} = (1,2)(3,4,5)(10,9,8,7,6) = \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 2&1&4&5&3&10&6&7&8&9 \end{smallmatrix}\right)$$

2. Soit $x \in G_1$. On peut écrire $x = x_1x_2\cdots x_r$, avec x_i d'ordre 2 pour tout i. Soit $y \in G_1$ un élément d'ordre 2. Alors $f(y)^2 = f(y^2) = f(e_1) = e_2$, ce qui montre que $f(y)$ est d'ordre 1 ou 2. Comme $|G_2|$ est impair, il n'y a pas d'éléments d'ordre 2 dans G_2, donc $f(y)$ est d'ordre 1, ce qui signifie que $f(y) = e_2$. Comme les x_i sont d'ordre 2, $f(x_i) = e_2$ pour tout i, donc $f(x) = f(x_1)\cdots f(x_r) = e_2$.
3. Supposons qu'il n'y a pas de point fixe. Pour $x \in X$ on a $|G{\cdot}x| \in \{1, 11, 13, 143\}$ (ce sont les diviseurs de 143). Mais 1 est exclu car x n'est pas un point fixe, et 143 est exclu car $143 > 108$. Comme X est partitionné par les orbites, on doit avoir $108 = 11a + 13b$, où $a \geq 0$ (resp. $b \geq 0$) est le nombre d'orbites de cardinal 11 (resp. 13). Modulo 11 on trouve: $\overline{2}{\cdot}\overline{b} = -\overline{2}$, donc $b \equiv -1\,(11)$. On peut écrire $b = 10 + 11c$ avec $c \geq 0$. Ceci est impossible car $13{\cdot}10 > 108$.
4. Soit $n \geq 5$ un entier impair.
   (a) Soient $x \in \langle X \rangle$ et $g \in G$. On peut écrire $x = x_1x_2\cdots x_r$ avec, pour tout i, $x_i \in X$ ou $x_i^{-1} \in X$. On a
   $$gxg^{-1} = (gx_1g^{-1})(gx_2g^{-1})\cdots(gx_rg^{-1})$$
   Posons $y_i = gx_ig^{-1}$. Si $x_i \in X$ on a $y_i \in X$. Si $x_i^{-1} \in X$ on a $y_i^{-1} = gx_i^{-1}g^{-1} \in X$. On peut donc écrire $gxg^{-1} = y_1\cdots y_r$ avec, pour tout i, $y_i \in X$ ou $y_i^{-1} \in X$.
   (b) Comme n est impair, le n-cycle $(1,2,\ldots,n)$ est pair, donc dans A_n.
   (c) X est stable par conjugaison: ordre$(\sigma\tau\sigma^{-1})$ = ordre(τ) dans n'importe quel groupe. D'après (a) le sous-groupe $\langle X \rangle$ de A_n est distingué. D'après (b) on a $\langle X \rangle \neq \{e\}$. Comme $n \geq 5$, A_n est simple, donc on doit avoir $\langle X \rangle = \mathrm{A}_n$.

Examen d'algèbre avancée.

le 26 mai 1993, 7:30–10:30

- Vous pouvez consulter tout document.
- Donnez des références pour les résultats que vous utilisez et qui ne se trouvent pas dans les notes du cours.
- Vérifiez vos solutions le mieux possible. Bonne chance.

1. (a) Soient G_1 et G_2 deux groupes et $f\colon G_1 \to G_2$ un morphisme surjectif. Supposons que G_1 est commutatif. Montrer que G_2 est commutatif.

   (b) Soient G et H deux groupes, $x \in G$ d'ordre n et $y \in H$ d'ordre m. Montrer que l'ordre de l'élément (x, y) de $G \times H$ est le plus petit commun multiple de n et m.

   (c) Montrer que $\mathbf{C}/\mathbf{Z}$ est isomorphe à $\mathbf{C}^*$.

   (d) Soit G un groupe fini. Supposons qu'il existe $x \in G$, $x \neq e$, tel que

   $$G = \{e\} \cup \{gxg^{-1} \mid g \in G\}.$$

   Montrer que G est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

2. (a) Soit G un groupe d'ordre $870 = 2{\cdot}3{\cdot}5{\cdot}29$. Montrer que G n'est pas simple. (On pourra utiliser sans démonstration que, comme $|G|$ est sans facteurs carrés, pour tout nombre premier p le nombre d'éléments d'ordre p dans G est $(p-1)n_p$, où n_p est le nombre de p-groupes de Sylow dans G.)

   (b) Soient G un groupe fini, p un nombre premier, $S \subset G$ un p-groupe de Sylow de G qui est distingué et $f\colon G \to G$ un morphisme. Montrer que $fS \subset S$.

   (c) Donner des générateurs d'un 3-groupe de Sylow dans S_6.

3. (a) Soit $f\colon \mathbf{Z}^3 \to \mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ le morphisme donné par $f(x, y, z) = (x + y - 2z, \overline{x + z})$. Calculer une base de $\ker(f)$.

   (b) Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $\{(3, 3, 15), (-3, 3, 9), (6, 0, 6)\}$. Trouver $r, s \geq 0$ et $n_1, \ldots, n_s > 1$ tels que $\mathbf{Z}^3/H \cong \mathbf{Z}^r \times \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$ et $n_s | \cdots | n_1$.

   (c) Les deux groupes $\mathbf{Z}/250\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/500\mathbf{Z}$ et $\mathbf{Z}/60\mathbf{Z} \times \mathbf{Z}/50\mathbf{Z} \times \mathbf{Z}/125\mathbf{Z}$ sont-ils isomorphes?

Corrigé de l'examen d'algèbre avancée.

le 26 mai 1993, 7:30–10:30

1. (a) Soient $x, y \in G_2$. Comme f est surjectif, il existent $a, b \in G_1$ tels que $x = f(a)$ et $y = f(b)$. Alors on a $xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$.

   (b) Soit $k \in \mathbf{Z}$. On a $(x, y)^k = (x^k, y^k)$, donc $(x, y)^k = (e_G, e_H)$ si et seulement si $x^k = e_G$ et $y^k = e_H$, ce qui équivaut à: $n|k$ et $m|k$. Il en résulte que $\mathrm{ppcm}(m, n) = \min\{k \in \mathbf{Z} \mid k \geq 1 \text{ et } (x, y)^k = (e_G, e_H)\}$.

   (c) Soit $f\colon \mathbf{C} \to \mathbf{C}^*$ le morphisme donné par $f(z) = \exp(2\pi i z)$. Comme f est surjectif et $\ker(f) = \mathbf{Z}$, le théorème d'isomorphisme dit que $\overline{f}\colon \mathbf{C}/\mathbf{Z} \to \mathbf{C}^*$: $\overline{f}(\overline{z}) = f(z)$ est un isomorphisme.

   (d) Soit $n := |G|$. Alors $|\{gxg^{-1} \mid g \in G\}| = n-1$. Comme le cardinal d'une orbite divise le cardinal du groupe, on a $(n-1)|n$. Il en résulte que $n = 2$. Tout groupe d'ordre 2 est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

2. (a) Supposons que G est simple. Alors pour $p \in \{2, 3, 5, 29\}$ on a $n_p \geq p+1$, car $n_p \equiv 1(p)$ et si $n_p = 1$ l'unique p-groupe de Sylow serait distingué. Il y a donc au moins $30{\cdot}28 = 840$ éléments d'ordre 29 dans G, au moins $6{\cdot}4 = 24$ d'ordre 5 et au moins $4{\cdot}2 = 8$ d'ordre 3. Comme $840 + 24 + 8 > 870$ on est arrivé à une contradiction; l'hypothèse que G est simple est donc fausse.

   (b) Comme S est distingué et les p-groupes de Sylow sont conjugués, S est l'unique p-groupe de Sylow dans G. L'image fS de S par f est un p-groupe (utiliser que $|fS|$ divise $|S|$). Tout sous-groupe de G qui est un p-groupe est contenu dans un p-groupe de Sylow, donc dans S.

   (c) On a $|\mathrm{S}_6| = 6! = 3^2{\cdot}2^4{\cdot}5$, donc un 3-groupe de Sylow dans S_6 est d'ordre 9. Soient $x := (1, 2, 3)$, $y := (4, 5, 6)$ et $H := \langle\{x, y\}\rangle$. Alors x et y sont d'ordre 3, $yx = xy$ et $H = \{x^a y^b \mid 0 \leq a, b < 3\}$. Donc $|H| \leq 9$. Comme $|\langle\{x\}\rangle| = 3$ et $y \notin \langle\{x\}\rangle$, on a $|H| = 9$.

3. (a) On va montrer que v_1, v_2 est une base de $\ker(f)$, où $v_1 = (2, 0, 1)$ et $(-3, 3, 0)$. On calcule d'abord que $v_1, v_2 \in \ker(f)$. Si $x = (a, b, c) \in \ker(f)$, on a $y := x - cv_1 = (a', b', 0) \in \ker(f)$, où $a' = a - 2c$ et $b' = b$. On a alors $0 = a' + b'$ et $\overline{a'} = 0$, d'où $y = dv_2$ avec $d = b'/3 \in \mathbf{Z}$. Ceci montre que $x = cv_1 + dv_2$. On a donc montré que v_1 et v_2 engendrent $\ker(f)$. Il est clair que v_1 et v_2 sont indépendants.

   (b) En faisant des opérations élémentaires sur les colonnes et les lignes de la matrice de lignes $(3, 3, 15)$, $(-3, 3, 9)$ et $(6, 0, 6)$ on arrive à la matrice de lignes $(3, 0, 0)$, $(0, 6, 0)$ et $(0, 0, 0)$. Cela montre qu'on peut prendre $r = 1$, $s = 2$, $n_1 = 6$ et $n_2 = 3$.

   (c) Par le théorème chinois on montre que les deux groupes sont respectivement isomorphes à $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$ et à $\mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \times \mathbf{Z}/m_3\mathbf{Z}$, où $n_1 = 2^2{\cdot}3{\cdot}5^3$, $n_2 = 2{\cdot}5^3$, $m_1 = 2^2{\cdot}3{\cdot}5^3$, $m_2 = 2{\cdot}5^2$ et $m_3 = 5$. On a bien $1 < n_2|n_1$ et $1 < m_3|m_2|m_1$ donc les n_i sont les invariants du premier groupe et les m_i sont les invariants du deuxième groupe. Comme ces invariants ne sont pas les mêmes, les deux groupes ne sont pas isomorphes.

Examen d'algèbre avancée.

le 13 septembre 1993, 8:00–11:00

- Vous pouvez consulter tout document.
- Donnez des références pour les résultats que vous utilisez et qui ne se trouvent pas dans les notes du cours.
- Vérifiez vos solutions le mieux possible. Bonne chance.

1. [4 points] Soient G un groupe, $x, y, z \in G$ et $N \subset G$ un sous-groupe distingué tels que $x^5 \in N$, $y^7 \in N$ et $y^{-1}zxz^{-1} \in N$. Montrer que $x \in N$ et que $y \in N$. (Indication: calculer dans G/N; quels peuvent être ordre($\overline{x}$), ordre($\overline{y}$) et que peut-on tirer de $y^{-1}zxz^{-1} \in N$?)
2. On se propose de déterminer tous les groupes finis qui ont exactement trois classes de conjugaison. Soit donc G un groupe fini, disons d'ordre n, et supposons que G a exactement trois classes de conjugaison.
   (a) [2 points] En considérant l'opération de G sur G par conjugaison, montrer qu'on a
   $$(*) \qquad 1 = \frac{1}{n} + \frac{1}{a} + \frac{1}{b}$$
   avec des entiers $a \geq b > 0$ tels que $a|n$ et $b|n$.
   (b) [2 points] Déterminer toutes les solutions de l'équation $(*)$ en entiers $n \geq a \geq b > 0$ tels que $a|n$ et $b|n$. (Indication: on a $b \leq 3$ car $n \geq a \geq b$.)
   (c) [2 points] Donner la liste complète des groupes finis, à isomorphisme près, qui ont exactement trois classes de conjugaison. (On pourra utiliser sans démonstration que tout groupe d'ordre 4 est commutatif et que tout groupe non-commutatif d'ordre 6 est isomorphe à S_3.)
3. (a) [1 point] Calculer le nombre d'éléments d'ordre 3 dans le groupe S_6.
   (b) [1 point] Montrer que $\langle\{(1,2,3),(4,5,6)\}\rangle$ est un 3-groupe de Sylow de S_6.
   (c) [1 point] Montrer que tout 3-groupe de Sylow de S_6 s'écrit $\langle\{(a,b,c),(d,e,f)\}\rangle$, avec $\{a,b,c,d,e,f\} = \{1,2,3,4,5,6\}$.
   (d) [1 point] Soit $S \subset \mathrm{S}_6$ un 3-groupe de Sylow. Montrer que l'opération de S sur $\{1,2,\ldots,6\}$ a exactement deux orbites de trois éléments chacun.
   (e) [1 point] Montrer que le nombre de 3-groupes de Sylow de S_6 est égal au nombre de partitions de $\{1,2,\ldots,6\}$ en deux ensembles de trois éléments.
   (f) [1 point] Calculer le nombre de 3-groupes de Sylow de S_6.
4. (a) [2 points] Soit $f\colon \mathbf{Z}^3 \to \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ le morphisme donné par
   $$f(x,y,z) = (\overline{x+y-2z}, \overline{x+z}).$$
   Calculer une base de $\ker(f)$.
   (b) [2 points] Soit $H \subset \mathbf{Z}^3$ le sous-groupe $\langle\{(-1,-2,6),(3,2,0),(-1,-2,12)\}\rangle$. Trouver $r, s \geq 0$ et $n_1, \ldots, n_s > 1$ tels que $\mathbf{Z}^3/H \cong \mathbf{Z}^r \times \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$ et $n_s|\cdots|n_1$.

Corrigé de l'examen d'algèbre avancée.

le 13 septembre 1993, 8:00–11:00

1. Comme $x^5 \in N$, on a $\overline{x}^5 = \overline{e}$. De même, on a $\overline{y}^7 = \overline{e}$. On voit donc que ordre($\overline{x}$) $\in \{1,5\}$ et que ordre($\overline{y}$) $\in \{1,7\}$, car 5 et 7 sont des nombres premiers. De $y^{-1}zxz^{-1} \in N$ on tire $\overline{y} = \overline{z}{\cdot}\overline{x}{\cdot}\overline{z}^{-1}$, ce qui veut dire que $\overline{x}$ et $\overline{y}$ sont conjugués. Comme deux éléments conjugués dans un groupe ont même ordre, on doit avoir ordre($\overline{x}$) $= 1$ et ordre($\overline{y}$) $= 1$. Ceci veut dire que $\overline{x} = \overline{e} = \overline{y}$, ou encore: $x \in N$ et $y \in N$.
2. (a) Soient $\{e\}$, C_1 et C_2 les trois classes de conjugaison de G. On a alors

$$n = 1 + |C_1| + |C_2|.$$

Comme les classes de conjugaison sont des orbites pour une opération de G, on peut écrire $n = a{\cdot}|C_1|$ et $n = b{\cdot}|C_2|$. En échangeant, si nécessaire, C_1 et C_2, on peut supposer que $a \geq b$. En divisant par n on trouve $1 = n^{-1} + a^{-1} + b^{-1}$ avec $a \geq b > 0$, $a|n$ et $b|n$.

(b) Supposons que (n, a, b) est une solution. Comme $n \geq a \geq b$ on a $1 = n^{-1}+a^{-1}+b^{-1} \leq 3b^{-1}$, d'où $b \leq 3$. On a donc $b = 2$ ou $b = 3$. Essayons $b = 2$. Dans ce cas on a $2^{-1} = n^{-1} + a^{-1} \leq 2a^{-1}$, d'où $a \leq 4$. Les possibilités pour a sont donc 3 et 4. On trouve les deux solutions $(n, a, b) = (6, 3, 2)$ et $(n, a, b) = (4, 2, 2)$. Maintenant essayons $b = 3$. Alors $2/3 = n^{-1} + a^{-1} \leq 2a^{-1}$, d'où $a \leq 3$. Il n'y a qu'une seule possibilité: $a = 3$. On trouve une seule solution $(n, a, b) = (3, 3, 3)$. En total, il y a donc trois solutions.

(c) Soit G un groupe fini qui a exactement trois classes de conjugaison et posons $n := |G|$. De (a) et (b) il résulte que $n \in \{3, 4, 6\}$. Supposons que $n = 3$. Comme 3 est premier, G est alors isomorphe à $\mathbf{Z}/3\mathbf{Z}$ et en fait ce groupe a exactement trois classes de conjugaison. Supposons que $n = 4$. Alors G est commutatif, donc il a exactement quatre classes de conjugaison; $n = 4$ est donc impossible. Supposons $n = 6$. De (b) il résulte que les trois classes de conjugaison de G ont 1, 3 et 2 éléments, donc G n'est pas commutatif. On conclut que G est isomorphe à S_3, qui a en fait exactement trois classes de conjugaison. La liste demandée est donc $\{\mathbf{Z}/3\mathbf{Z}, \mathrm{S}_3\}$.
3. (a) Un élément d'ordre 3 de S_6 est un 3-cycle ou un produit de deux trois-cycles disjoints. Le nombre de 3-cycles est $6{\cdot}5{\cdot}4/3 = 40$. Le nombre de produits de deux 3-cycles disjoints est $\mathrm{C}_6^3{\cdot}2{\cdot}2/2 = 40$. La réponse est donc 80.

(b) Soit $\sigma := (1, 2, 3)$ et $\tau := (4, 5, 6)$. Alors σ et τ sont deux 3-cycles disjoints, donc ils commutent. On a donc

$$S := \langle\{\sigma, \tau\}\rangle = \{\sigma^a\tau^b \mid 0 \leq a < 3 \text{ et } 0 \leq b < 3\}$$

et ces $\sigma^a\tau^b$ sont tous distincts. On conclut que $|S| = 9$. Comme $|\mathrm{S}_6|/9 = 720/9 = 80$ n'est pas divisible par 3, S est un 3-groupe de Sylow.

(c) Tous les 3-groupes de Sylow de S_6 sont conjugués (c'est dans le théorème de Sylow), et on a la formule

$$\sigma\langle\{(1,2,3),(4,5,6)\}\rangle\sigma^{-1} = \langle\{(\sigma(1),\sigma(2),\sigma(3)),(\sigma(4),\sigma(5),\sigma(6))\}\rangle$$

(d) En écrivant S comme en (c), on remarque que les orbites sont $\{a,b,c\}$ et $\{d,e,f\}$.

(e) Soit X l'ensemble des 3-groupes de Sylow de S_6 et Y l'ensemble des partitions de $\{1,2,\dots,6\}$ en deux ensembles de trois éléments. On a une application $f\colon X \to Y$ en associant à $S \in X$ la partition donnée par les orbites de S (en (d) on a vu que c'est une partition en deux ensembles de trois éléments). Soit d'autre part $\{1,2,\dots,6\}$ partitionné en $\{a,b,c\}$ et $\{d,e,f\}$. A cette partition on associe le 3-groupe de Sylow

$$\langle\{(a,b,c),(d,e,f)\}\rangle = \langle\{(a,b,c),(a,c,b),(d,e,f),(d,f,e)\}\rangle,$$

et soit $g\colon Y \to X$ l'application donnée par cette association. On vérifie tout de suite que f et g sont des application inverses.

(f) D'après (e), ce nombre est égal au nombre de partitions de $\{1,2,\dots,6\}$ en deux ensembles de trois éléments. Ce nombre est donc $C_6^3/2 = 10$.

4. (a) On constate que $(-1,3,1) \in \ker(f)$; c'est le premier vecteur de notre base de $\ker(f)$. Supposons maintenant que $(x,y,0) \in \ker(f)$. Alors on a $5|x$ et $5|y$, donc pour le deuxième vecteur de notre base on peut prendre $(0,5,0)$, et pour le troisième $(5,0,0)$.

   (b) On trouve $r = 0$, $s = 2$, $n_1 = 12$ et $n_2 = 2$.

Partiel d'algèbre avancée.

le 12 mars 1994, 8:00–10:00

- Vous pouvez consulter tout document.
- Donnez des références pour les résultats que vous utilisez et qui ne se trouvent pas dans les notes du cours.
- Vérifiez vos solutions le mieux possible. Bonne chance.

1. Pour chacun des énoncés suivants, donner une démonstration ou un contre-exemple.
   (a) [2 points] Soient G un groupe et $N \subset G$ un sous-groupe distingué tels que G/N est fini, disons d'ordre n. Alors pour tout x dans G on a $x^n \in N$.
   (b) [2 points] Soient $f\colon G_1 \to G_2$ un morphisme de groupes et $X \subset G_1$ un sous-ensemble. Alors on a $f\langle X\rangle = \langle fX\rangle$.
   (c) [2 points] Soient $f\colon G_1 \to G_2$ un morphisme de groupes et $H_1 \subset G_1$ un sous-groupe distingué. Alors fH_1 est un sous-groupe distingué de G_2.
   (d) [2 points] Dans un groupe engendré par des éléments d'ordre 2, tout élément est d'ordre 1 ou 2.
   (e) [2 points] Soient G un groupe, $H \subset G$ un sous-groupe et $X \subset G$ un sous-ensemble. Supposons que $\langle X\rangle = G$ et que pour tout $x \in X$ on a $xHx^{-1} = H$. Alors H est distingué.
2. [4 points] Soient G un groupe et $C = \{x \in G \mid \forall y \in G\colon xy = yx\}$ son centre. On sait que C est un sous-groupe distingué de G. Soit $\mathrm{Aut}(G)$ le groupe d'automorphismes de G (l'opération est la composition). Montrer que G/C est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$. (Indication: considérer l'opération de G sur G par conjugaison.)
3. [6 points] Combien déléments d'ordre 20 y-a t'il dans S_{10}?
   Combien déléments d'ordre 20 y-a t'il dans A_{10}?

Corrigé du partiel d'algèbre avancée.

le 12 mars 1994, 8:00–10:00

1. (a) Soit x dans G. Alors dans G/N on a $\overline{x^n} = \overline{x}^n = \overline{e}$, ce qui signifie que $x^n \in \overline{e} = N$.

   (b) Soit $g_2 \in f\langle X\rangle$. Il existe $g_1 \in \langle X\rangle$ tel que $g_2 = f(g_1)$. Par la définition de $\langle X\rangle$, il existe $n \geq 0$ et $x_1, \ldots, x_n$ avec, pour tout i, $x_i \in X$ ou $x_i^{-1} \in X$, tels que $g_1 = x_1x_2\cdots x_n$. Posons $y_i := f(x_i)$. Pour tout i on a $y_i \in fX$ ou $y_i^{-1} \in fX$. Comme $g_2 = y_1y_2\cdots y_n$, on a montré que $f\langle X\rangle \subset \langle fX\rangle$.

   Montrons maintenant l'autre inclusion. Soit $g_2 \in \langle fX\rangle$. Alors on peut écrire $g_2 = y_1y_2\cdots y_n$, avec $n \geq 0$ et $y_i \in fX$ ou $y_i^{-1} \in fX$ pour tout i. Prenons des $x_i \in G_1$ tels que $y_i = f(x_i)$, et $x_i \in X$ ou $x_i^{-1} \in X$. Alors on a $g_2 = f(x_1x_2\cdots x_n)$, ce qui montre que $g_2 \in f\langle X\rangle$.

   (c) Ceci est faux. Pour avoir un contre-exemple, prenons pour G_1 le sous-groupe de S_3 engendré par $(1,2)$, $H_1 = G_1$, $G_2 = \mathrm{S}_3$ et f l'injection.

   (d) Ceci est faux. Contre-exemple: S_3 est engendré par ses 2-cycles, mais contient des éléments d'ordre 3.

   (e) Considérons l'opération de G sur G par conjugaison. Cette opération induit une opération de G sur l'ensemble des sous-groupes de G. Le stabilisateur G_H de H contient X. Comme G_H est un sous-groupe de G, G_H contient $\langle X\rangle$. Donc $G_H = G$ et H est distingué.

2. On considère l'opération de G sur G par conjugaison. Cela donne un morphisme de groupes $\gamma\colon G \to \mathrm{Aut}(G)$. On a $x \in \ker(\gamma)$ si et seulement si $xyx^{-1} = y$ pour tout y, c'est à dire, $\ker(\gamma) = C$. Il en résulte que G/C est isomorphe à $\mathrm{im}(\gamma)$, qui est un sous-groupe de $\mathrm{Aut}(G)$.

3. Supposons que $\sigma \in \mathrm{S}_{10}$ est d'ordre 20. Soit $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ une décomposition en cycles disjoints, de longueurs $l_1 \geq l_2 \geq \ldots \geq l_r$. Alors on a $\mathrm{pgcd}(l_1, \ldots, l_r) = 20$, et $l_1 + \cdots + l_r = 10$ (on suppose qu'on n'a pas négligé les 1-cycles). Au moins un des l_i doit être un multiple de 5; on ne peut pas avoir $l_i = 10$ car alors r serait 1 et σ serait d'ordre 10. Au moins un des l_i est un multiple de 4; comme on a déjà un 5-cycle, on a aussi un 4-cycle. On a donc $r = 3$, $l_1 = 5$, $l_2 = 4$ et $l_3 = 1$. Pour σ_1, il y a $10{\cdot}9{\cdot}8{\cdot}7{\cdot}6/5$ possibilités. Ensuite pour σ_2 il reste $5{\cdot}4{\cdot}3{\cdot}2/4$ possibilités et pour σ_3 il reste exactement une possibilité. En total: il y a $10!/20 = 181440$ éléments d'ordre 20 dans S_{10}. Tout ces éléments sont impairs, donc dans A_{10} il y en a 0.

Examen d'algèbre avancée.

le 30 mai 1994, 8:00–11:00

- Vous pouvez consulter tout document.
- Donnez des références pour les résultats que vous utilisez. Les résultats de tous les exercices du polycopié, y compris ceux des examens et partiels précédents, peuvent être utilisés sans démonstration.
- Ce n'est pas nécessaire de tout faire pour avoir 20 points: le total est 22.
- Vérifiez vos solutions le mieux possible. Bonne chance.

1. Pour chacun des énoncés suivants, donner une démonstration ou montrer que l'énoncé est faux.
   (a) [2 points] Les deux groupes $G_1 = \mathbf{Z}/15\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/36\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ et $G_2 = \mathbf{Z}/24\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z} \times \mathbf{Z}/20\mathbf{Z}$ sont isomorphes.
   (b) [2 points] Les deux groupes $G_1 = \mathbf{Z}^3/\langle\{(0,-12,-12),(0,12,-24),(20,0,22)\}\rangle$ et $G_2 = \mathbf{Z}/45\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ sont isomorphes.
   (c) [2 points] Soit $f\colon G_1 \to G_2$ un morphisme surjectif avec G_2 commutatif. Soit $H \subset G_1$ un sous-groupe contenant $\ker(f)$. Alors H est distingué dans G_1.
   (d) [2 points] Soit $f\colon G_1 \to G_2$ un morphisme avec G_2 commutatif. Soit $H \subset G_1$ un sous-groupe contenant $\ker(f)$. Alors H est distingué dans G_1.
   (e) [2 points] Soient X un ensemble, G un groupe opérant à gauche sur X, H un groupe opérant à droite sur X. Alors pour tout x dans X, g dans G et h dans H on a $(gx)h = g(xh)$.
   (f) [2 points] Soient N et H deux groupes, $\alpha\colon H \to \mathrm{Aut}(N)$ un morphisme tel que $\ker(\alpha)$ est différent de H. Alors $N \times_\alpha H$ n'est pas commutatif.
2. Soit G un groupe fini, disons d'ordre n, non commutatif. Soit C le centre de G et notons $c := |C|$. Soit r le nombre de classes de conjugaison de G.
   (a) [2 points] Montrer que $c \le n/4$. (Indication: que peut-on dire de G/C?)
   (b) [2 points] En considérant l'opération de G sur G par conjugaison, montrer que r est au plus $5n/8$.
3. (a) [4 points] Montrer que tout groupe d'ordre $7{\cdot}11{\cdot}13$ est isomorphe à $\mathbf{Z}/1001\mathbf{Z}$. (Indication: considérer les p-groupes de Sylow.)
   (b) [2 points] Soient G un groupe, $N \subset G$ un sous-groupe distingué, $H \subset N$ un sous-groupe. Supposons que N est cyclique et fini. Montrer que H est un sous-groupe distingué de G.

Corrigé de l'examen d'algèbre avancée.

le 30 mai 1994, 8:00–11:00

1. (a) Vrai. Les groupes G_1 et G_2 sont isomorphes à $\mathbf{Z}/360\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, d'après le théorème chinois.

   (b) Faux. Les invariants de G_1 sont: $r = 0$, $s = 3$, $n_1 = 360$, $n_2 = 12$ et $n_3 = 2$, tandis que ceux de G_2 sont $r = 0$, $s = 2$, $n_1 = 360$ et $n_2 = 24$.

   (c) Vrai. Voir la partie (d).

   (d) Vrai. Soit $G_3 := \mathrm{im}(f)$ et $f_1\colon G_1 \to G_3$ le morphisme surjectif induit. D'après la Proposition 6.5, $H = f_1^{-1}f_1H$. Comme G_3 est commutatif, f_1H est un sous-groupe distingué de G_3. D'après la Proposition 6.5, H est distingué dans G_1.

   (e) Faux. On peut prendre $X = \{1, 2, 3\}$, $G = H = \mathrm{S}_3$ avec l'opération usuelle de G: $g{\cdot}i = g(i)$ et l'opération suivante de H: $i{\cdot}h = h^{-1}(i)$.

   (f) Vrai. Soit h dans H et n dans N tel que $(\alpha(h))(n) \neq n$ (ceci existe car $\ker(\alpha) \neq H$). On a alors: $(e_N, h) * (n, e_H) = ((\alpha(h))(n), h)$ tandis que $(n, e_H) * (e_N, h) = (n, h)$.

2. (a) Supposons que $c > n/4$. Alors $|G/C| \in \{1, 2, 3\}$. Donc G/C est un groupe cyclique. D'après l'exercice 50, G est commutatif, ce qui est une contradiction.

   (b) On considère l'opération de G sur G par conjugaison. Soit r le nombre d'orbites. Dans chaque orbite, on prend un élément x_i. Comme pour $x \in C$ on a $G{\cdot}x = \{x\}$, on peut supposer que $\{x_1, \ldots, x_c\} = C$. Pour $i > c$ on a $|G{\cdot}x_i| \geq 2$. Ceci donne:

   $$n = |G| = \sum_{i=1}^{r} |G{\cdot}x_i| = c + \sum_{i=c+1}^{r} |G{\cdot}x_i| \geq c + (r - c)2$$

   Donc $2r \leq n + c \leq n + n/4 = 5n/4$, ce qui donne le résultat.

3. (a) Soit G un groupe d'ordre 1001. En utilisant le théorème de Sylow, on voit que le nombre de p-groupes de Sylow est égal à 1 pour p dans $\{7, 11, 13\}$. Les p-groupes de Sylow de G sont donc distingués. D'après l'exercice 80, G est isomorphe au produit direct de ses p-groupes de Sylow. Comme ces groupes sont d'ordre p, ils sont cycliques et isomorphes à $\mathbf{Z}/p\mathbf{Z}$, donc G est isomorphe à $\mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/13\mathbf{Z}$, et on finit par le théorème chinois.

   (b) Soit $g \in G$. Alors gHg^{-1} est un sous-groupe de gNg^{-1} donc de N. Notons que $|gHg^{-1}| = |H|$. Comme N est cyclique et fini, N n'a qu'un seul sous-groupe d'ordre $|H|$ (voir le texte du polycopié en haut de la page 18), d'où $gHg^{-1} = H$.

Examen d'algèbre avancée.

le 13 septembre 1994, 8:00–11:00

– Vous pouvez consulter tout document.
– Donnez des références pour les résultats que vous utilisez. Les résultats de tous les exercices du polycopié, y compris ceux des examens et partiels précédents, peuvent être utilisés sans démonstration.
– Ce n'est pas nécessaire de tout faire pour avoir 20 points: le total est 22.
– Vérifiez vos solutions le mieux possible. Bonne chance.

1. Pour chacun des énoncés suivants, donner une démonstration ou montrer que l'énoncé est faux.
   (a) [2 points] Les deux groupes $G_1 = \mathbf{Z}/54\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/72\mathbf{Z}$ et $G_2 = \mathbf{Z}/48\mathbf{Z} \times \mathbf{Z}/27\mathbf{Z} \times \mathbf{Z}/36\mathbf{Z}$ sont isomorphes.
   (b) [2 points] Les deux groupes $G_1 = \mathbf{Z}^3/\langle\{(36,0,180),(36,36,36),(30,36,42)\}\rangle$ et $G_2 = \mathbf{Z}/216\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z}$ sont isomorphes.
   (c) [2 points] Soient p, q et r trois nombres premiers (non nécessairement distincts) et G un groupe d'ordre pqr. Alors G peut être engendré par 3 éléments.
   (d) [2 points] Soient G un groupe, $N \subset G$ un sous-groupe distingué et x, y dans G tels que $xyx^{-1}y^{-1} \in N$. Alors pour tout n, m dans $\mathbf{Z}$, on a $x^n y^m x^{-n} y^{-m} \in N$.
   (e) [2 points] Il existe un élément σ du groupe symétrique S_9 tel que $\sigma^3 = (1,2,3)$.
2. (a) [1 point] Soient G un groupe fini, $N \subset G$ un sous-groupe distingué et $H \subset G$ un sous-groupe. Supposons que $H \cap N = \{e\}$. Montrer que $|H| \leq |G/N|$.
   (b) [3 points] Soit $n \geq 5$ et soit $N \subset \mathrm{S}_n$ un sous-groupe distingué. Montrer que N appartient à $\{\{e\}, \mathrm{A}_n, \mathrm{S}_n\}$. (Indication: considérer $N \cap \mathrm{A}_n$.)
   (c) [3 points] Soit $n \geq 5$ et soit $H \subset \mathrm{S}_n$ un sous-groupe tel que $|\mathrm{S}_n/H| < n$. Montrer que $H = \mathrm{A}_n$ ou que $H = \mathrm{S}_n$. (Indication: considérer l'opération de S_n sur S_n/H donnée par $\sigma \cdot (\tau H) = (\sigma\tau)H$, et le morphisme $\gamma\colon \mathrm{S}_n \to \mathrm{Sym}(\mathrm{S}_n/H)$ induit par cette opération.)
3. (a) [2 points] Soient $m \geq 2$ et $n \geq 2$ des entiers. Soit G le groupe $\mathbf{Z}/m\mathbf{Z} \times \cdots \times \mathbf{Z}/m\mathbf{Z}$ (n facteurs). Montrer que $|\mathrm{Aut}(G)| > 1$.
   (b) [3 points] Montrer que tout groupe fini G avec $|\mathrm{Aut}(G)| = 1$ est isomorphe à $\{e\}$ ou à $\mathbf{Z}/2\mathbf{Z}$. (Indication: considérer d'abord l'opération de conjugaison de G sur G.)

Corrigé de l'examen d'algèbre avancée.

le 13 septembre 1994, 8:00–11:00

1. (a) Faux. Les invariants de G_1 sont: $r = 0$, $s = 3$, $n_1 = 216$, $n_2 = 36$ et $n_3 = 6$, tandis que ceux de G_2 sont: $r = 0$, $s = 3$, $n_1 = 432$, $n_2 = 36$ et $n_3 = 3$.

   (b) Vrai. Les deux groupes ont mêmes invariants: $r = 0$, $s = 3$, $n_1 = 216$, $n_2 = 36$ et $n_3 = 6$.

   (c) Vrai. Soit $x \in G$ tel que $x \neq e$. Si x engendre G on a bien montré ce qu'il fallait, donc supposons que ce n'est pas le cas. Prenons y dans G tel que $y \notin \langle\{x\}\rangle$. Si $\langle\{x,y\}\rangle = G$ on a fini, donc supposons que ce n'est pas le cas. Prenons z dans G tel que $z \notin \langle\{x,y\}\rangle$. La suite d'inclusions strictes

   $$\{e\} \subset \langle\{x\}\rangle \subset \langle\{x,y\}\rangle \subset \langle\{x,y,z\}\rangle$$

   montre que $|\langle\{x,y,z\}\rangle|$ est produit d'au moins trois nombres premiers. On conclut que $|\langle\{x,y,z\}\rangle| = pqr$ donc $\langle\{x,y,z\}\rangle = G$.

   (d) Vrai. Dans le groupe quotient G/N on a $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$, donc aussi $\overline{x}^n\overline{y}^m = \overline{y}^m\overline{x}^n$. Ceci implique bien que $x^n y^m x^{-n} y^{-m}$ est dans N.

   (e) Faux. Supposons que σ dans S_9 est tel que $\sigma^3 = (1,2,3)$. Alors l'ordre de σ est 9. Donc σ est un cycle de longueur 9 (ici on utilise qu'on est dans S_9). Mais la puissance troisième d'un cycle de longueur 9 est produit de trois cycles disjoints de longueur 3. Contradiction.

2. (a) Considérons le morphisme $f\colon G \to G/N$. L'image fH de H est isomorphe à $H/H \cap N \cong H$. Donc H est isomorphe à un sous-groupe de G/N, ce qui entraîne $|H| \leq |G/N|$.

   (b) Soit $N' := N \cap \mathrm{A}_n$. Alors N' est un sous-groupe distingué de A_n. Comme $n \geq 5$, A_n est simple, donc $N' = \{e\}$ ou $N' = \mathrm{A}_n$. Dans le deuxième cas, comme $[\mathrm{S}_n : \mathrm{A}_n] = 2$ est premier, on doit avoir $N = \mathrm{A}_n$ ou $N = \mathrm{S}_n$. Supposons que $N' = \{e\}$. Alors on a vu dans la partie (a) de cet exercice que $|N| \leq 2$. Il suffit de montrer que $|N| = 1$, donc supposons que $|N| = 2$. Alors on peut écrire $N = \{e, \sigma\}$. Comme N est distingué dans S_n, on a $\tau\sigma\tau^{-1} = \sigma$ pour tout τ dans S_n. Mais cela signifie que σ est dans le centre de S_n et comme $n \geq 2$ on sait que ce centre est $\{e\}$. Ceci montre que $|N| = 2$ est impossible.

   (c) Posons $k := |\mathrm{S}_n/H|$. Alors $|\mathrm{im}(\gamma)| \leq k!$, donc $|\ker(\gamma)| \geq n!/k! > 1$. D'après la partie (b), on a $\ker(\gamma) = \mathrm{A}_n$ ou $\ker(\gamma) = \mathrm{S}_n$. Comme le stabilisateur de $H \in \mathrm{S}_n/H$ est H, on a $\ker(\gamma) \subset H$, donc H contient A_n. Il en résulte que $H = \mathrm{A}_n$ ou $H = \mathrm{S}_n$.

3. (a) Soit $f\colon G \to G$ l'application définie par $f(a_1, a_2, a_3, \ldots, a_n) = (a_2, a_1, a_3, \ldots, a_n)$. Il est clair que f est un automorphisme de G qui n'est pas id_G.

   (b) Pour chaque x dans G, la conjugaison $y \mapsto xyx^{-1}$ par x est un automorphisme de G, donc est id_G par hypothèse. Cela signifie que pour tout x et y dans G, on a

$xyx^{-1} = y$. Donc G est commutatif. Donc G est isomorphe à un groupe de la forme $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$, avec $n_i > 1$ pour tout i. L'application $x \mapsto x^{-1}$ de G vers G est un automorphisme. On conclut que pour chaque x dans G on a $x^2 = e$ et que $n_i = 2$ pour tout i. De la partie (a) de cet exercice il résulte que $s = 0$ ou $s = 1$.

Partiel d'algèbre avancée

Le 25 mars 1995, 10:30–12:30

Vous pouvez consulter tout document et tout livre que vous avez emporté(s). Il est autorisé d'utiliser les résultats de tous les exercices du polycopié, même de ceux que vous n'avez pas faits. L'utilisation de calculatrices est autorisée.

Dans chaque partie de chaque exercice, vour pourrez utiliser les énoncés des parties précédentes, même si vous n'avez pas réussi à les prouver.

1. Pour chacun des énoncés suivants, donner une démonstration ou un contre-exemple.
   (a) Soient G_1 et G_2 des groupes finis tels que $\operatorname{pgcd}(|G_1|, |G_2|) = 1$ et soit $f: G_1 \to G_2$ un morphisme. Alors f est trivial. (Un morphisme $f: G_1 \to G_2$ est dit trivial si $\ker(f) = G_1$.)
   (b) Soient G_1 et G_2 des groupes finis tels que $\operatorname{pgcd}(|G_1|, |G_2|) > 1$. Alors il existe un morphisme non-trivial $f: G_1 \to G_2$.
   (c) Soient G_1 et G_2 des groupes et soit $N_i \subset G_i$ un sous-groupe distingué pour $i = 1, 2$. Alors $N_1 \times N_2 \subset G_1 \times G_2$ est un sous-groupe distingué et $(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.
2. (a) Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $(7, -7, -7)$, $(10, 5, -5)$ et $(13, 17, -3)$. Montrer que $H \cong \mathbf{Z}^2$ et que $\mathbf{Z}^3/H \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}$.
   (b) Soit $H = \{ (a, b, c) \in \mathbf{Z}^3 \mid a + 3b + 5c \equiv 0 \pmod{11} \}$. Montrer que $\mathbf{Z}^3/H \cong \mathbf{Z}/11\mathbf{Z}$ et que $H \cong \mathbf{Z}^3$. (On pourra étudier l'application $\phi: \mathbf{Z}^3 \to \mathbf{Z}/11\mathbf{Z}$ donnée par $\phi(a, b, c) = \overline{a + 3b + 5c}$.)
3. Soit G un groupe d'ordre 6. Dans cet exercice on montrera que G est soit isomorphe à $\mathbf{Z}/6\mathbf{Z}$ soit à S_3.
   (a) Montrer que si G est commutatif, alors $G \cong \mathbf{Z}/6\mathbf{Z}$.

   Dans la suite de l'exercice on supposera que G ne soit pas commutatif.

   (b) Montrer que G contient un élément a d'ordre 3. (On pourra utiliser l'exercice 2 du polycopié.)
   (c) Soit $a \in G$ un élément d'ordre 3 dont l'existence est garanti par 3 et soit $H \subset G$ le sous-groupe engendré par a. Montrer que H est un sous-groupe distingué.
   (d) Soit $x \in G$ tel que $x \notin H$. Montrer que pour tout $g \in G$ on a $gxg^{-1} \notin H$.
   (e) La partie 3 montre que G opère à gauche sur l'ensemble $G - H$ par conjugaison. Montrer que ceci définit un isomorphisme $G \cong \mathrm{S}_3$.

Barème approximatif: Ex. 1: $3 \times 2 = 6$ points, Ex. 2: $2 + 2 = 4$ points et Ex. 3: $4 \times 2 + 3 = 11$ points.

Bonne chance.

Corrigé du partiel

le 25 mars 1995

Exercice 1

a) L'énoncé est vrai. Comme $\mathrm{im}(f) \subset G_2$ est un sous-groupe, $|\mathrm{im}(f)|$ divise $|G_2|$. D'autre part, $\mathrm{im}(f) \cong G_1/\ker(f)$, donc $|\mathrm{im}(f)|$ divise $|G_1|$. Or $\mathrm{pgcd}(|G_1|, |G_2|) = 1$, donc $|\mathrm{im}(f)| = 1$ et $\ker(f) = G_1$.

b) L'énoncé est faux. Pour donner un contre-exemple on peut prendre $G_1 = \mathrm{S}_3$ et $G_2 = \mathbf{Z}/3\mathbf{Z}$. Si $f\colon \mathrm{S}_3 \to \mathbf{Z}/3\mathbf{Z}$ est un morphisme non-trivial, alors $\mathrm{im}(f) \subset \mathbf{Z}/3\mathbf{Z}$ est un sous-groupe avec $\mathrm{im}(f) \neq \{\bar{0}\}$, donc f est surjectif. Il s'ensuit que $\ker(f) \subset \mathrm{S}_3$ est un sous-groupe d'ordre 2, donc $\ker(f)$ est engedré par un élément d'ordre 2, c'est-à-dire par $(1,2)$, $(1,3)$ ou $(2,3)$. On verifie facilement que les sous-groupes $\{(1),(1,2)\}$, $\{(1),(1,3)\}$ et $\{(1),(2,3)\}$ ne sont pas distingués.

c) L'énoncé est vrai. Soit $\phi\colon G_1 \times G_2 \to G_1/N_1 \times G_2/N_2$ défini par $\phi(g_1, g_2) = (g_1N_1, g_2N_2)$. On vérifie aisement que ϕ est un morphisme de groupes, que ϕ est surjectif et que $\ker(\phi) = N_1 \times N_2$. On conclut que $N_1 \times N_2 \subset G_1 \times G_2$ est un sous-groupe distingué et que $(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.

Exercice 2

a) En appliquant l'algortithme 12.19, on transforme la matrice

$$\begin{pmatrix} 7 & -7 & -7 \\ 10 & 5 & -5 \\ 13 & 17 & -3 \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 35 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Il existe donc une base (e_1, e_2, e_3) de $\mathbf{Z}^3$ telle que $(e_1, 35e_2)$ est une base de H. Il s'ensuit que $H \cong \mathbf{Z}^2$ et que $\mathbf{Z}^3/H \cong \mathbf{Z}/35\mathbf{Z} \times \mathbf{Z}$ et on conclut à l'aide du théorème Chinois.

b) Il est clair que $\phi\colon \mathbf{Z}^3 \to \mathbf{Z}/11\mathbf{Z}$ est un morphisme surjectif et que $\ker(\phi) = H$. On a donc un isomorphisme $\mathbf{Z}^3/H \cong \mathbf{Z}/11\mathbf{Z}$. En tant que sous-groupe de $\mathbf{Z}^3$, H est libre de rang au plus 3. Si le rang de H est strictement inférieur à 3, alors il existe une base (e_1, e_2, e_3) de $\mathbf{Z}^3$ et des nombres $n_1, n_2 \in \mathbf{N}$ (possiblement nuls) tels que H est engendré par n_1e_1 et n_2e_2. Dans ce cas, le groupe $\mathbf{Z}^3/H$ est infini. C'est une contradiction, donc $H \cong \mathbf{Z}^3$.

Exercice 3

a) Si les invariants de G sont r, s et $n_1, \ldots n_s$, alors $r = 0$ et le produit des n_i est égal à 6. Comme $n_s | n_{s_1} | \cdots | n_1$, cela implique que $s = 1$ et $n_1 = 6$.

b) Si $x^2 = e$ pour tout $x \in G$, alors G est commutatif, donc il existe $a \in G$ tel que ordre(a) ne divise pas 2. On a donc ordre$(a) = 3$ ou 6 mais dans le dernier cas, G est cyclique et comme G n'est pas commutatif, cela est impossible. Il s'ensuit que ordre$(a) = 3$.

c) Comme il y a 2 orbites pour l'action de H sur G par translations à droite, on a $gH = H$ ou $gH = G - H$ pour tout $g \in G$. Si $gH = H$, alors $g \in H$ donc $Hg = H = gH$. Si $gH = G - H$ alors $g \notin H$, donc $Hg = G - H = gH$. Dans chaque cas, on trouve $gH = Hg$, donc H est un sous-groupe distingué.

d) H est distingué, donc $x \in H$ si et seulement si $gxg^{-1} \in H$.

e) L'ensemble $G - H$ est d'ordre 3, donc l'action de G sur $G - H$ donne un morphisme $G \to \mathrm{S}_3$. Soit $x \in G - H$, alors $G - H = xH = \{x, xa, xa^2\}$. Le conjugué xax^{-1} est d'ordre 3 et comme H est distingué, $xax^{-1} \in H$ donc $xax^{-1} = a$ ou a^2. Si $xax^{-1} = a$, alors G est commutatif, donc $xax^{-1} = a^2$. Cela implique que la conjugaison par x fixe x et échange xa et xa^2. L'image de x dans S_3 est donc la transposition qui fixe x. Comme ceci est le cas pour tout élément de $G - H$, toutes les transpositions sont dans l'image de notre application $G \to \mathrm{S}_3$ donc cet application est surjective. Comme $|G| = |\mathrm{S}_3|$, elle est également injective.

Examen d'algèbre avancée

le mardi 6 juin 1995, 8:00–11:00

Vous pouvez consulter tout document et tout livre que vous avez emporté(s). Il est autorisé d'utiliser les résultats de tous les exercices du polycopié, même de ceux que vous n'avez pas faits. L'utilisation de calculatrices et de modèles de polyèdres réguliers est autorisée.

Dans chaque partie de chaque exercice, vour pourrez utiliser les énoncés des parties précédentes, même si vous n'avez pas réussi à les prouver.

1. Pour chacun des énoncés suivants, donner une démonstration ou un contre-exemple.
   (a) Soit $k > 0$ un entier et soit $f : \mathbf{Z}^k \to \mathbf{Z}^k$ un morphisme injectif. Alors f est surjectif.
   (b) Soit $k > 0$ un entier et soit $f : \mathbf{Z}^k \to \mathbf{Z}^k$ un morphisme surjectif. Alors f est injectif.
   (c) Soit G un groupe et soient $x, y \in G$ tels que $\text{ordre}(x) = \text{ordre}(y)$. Alors x et y sont conjugués.
   (d) Soient G_1 et G_2 deux groupes finis tels que la liste de groupes simples associée à G_1 par le théorème de Jordan–Hölder est, à permutation près, égale à celle associée à G_2. Alors $|G_1| = |G_2|$.
   (e) Il existe un morphisme surjectif $f\colon \mathrm{S}_5 \to \mathbf{Z}/5\mathbf{Z}$.
   (f) Il existe un morphisme injectif $f\colon \mathbf{Z}/5\mathbf{Z} \to \mathrm{S}_5$.
   (g) Soient $n \geq 2$ un nombre entier, D_n le groupe diédral d'ordre $2n$ et $N \subset D_n$ le sous-groupe (distingué) des rotations. Si $x \in D_n$ tel que $x \notin N$ alors $\text{ordre}(x) = 2$.
2. (a) Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $(2, 3, 0)$, $(4, 4, -6)$ et $(2, 5, 6)$. Montrer que $\mathbf{Z}^3/H \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$.
   (b) Soit $H' \subset \mathbf{Z}^3$ le sous-groupe

$$\{\, (a, b, c) \in \mathbf{Z}^3 \mid 3a + 5b \equiv 0 \pmod{12} \text{ et } 5a + 7c \equiv 0 \pmod{25} \,\}.$$

   Montrer que $\mathbf{Z}^3/H' \cong \mathbf{Z}/300\mathbf{Z}$. (Indication: Trouver une application convenable $f\colon \mathbf{Z}^3 \to \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$.)
3. Soient G un groupe fini, $A \subset G$ un sous-groupe et $E = \{\, gAg^{-1} \mid g \in G \,\}$ l'ensemble de conjugués de A. Soit p un nombre premier tel que $[G\colon A] < p$.
   (a) Montrer que $|E| < p$. (Indication: Considérer l'action de G sur E par conjugaison.)
   (b) Soit S un p-groupe de Sylow de G. Montrer que les orbites pour l'action de S sur E par conjugaison sont triviales.
   (c) Soient $g \in G$ et $B = gAg^{-1}$. On vient de montrer que $sBs^{-1} = B$ pour tout $s \in S$. Montrer que BS est un sous-groupe de G et que B est un sous-groupe distingué de BS.
   (d) Appliquer la Proposition 6.7 pour montrer que $BS = B$ et que $S \subset B$. En déduire que $S \subset \bigcap_{g \in G} gAg^{-1}$.

Corrigé de l'examen d'algèbre avancée

le 6 juin 1995

Exercice 1

a) L'énoncé est faux, un contre-exemple est fourni par l'application $f\colon \mathbf{Z} \to \mathbf{Z}$ définie par $f(x) = 2x$.

b) L'énoncé est vrai. Si $f\colon \mathbf{Z}^k \to \mathbf{Z}^k$ est un morphisme, alors on a $\ker(f) \cong \mathbf{Z}^{k'}$ avec $k' \leq k$ et par le théorème 12.18, $\mathbf{Z}^k/\ker(f) \cong \mathbf{Z}^{k-k'} \times$ (un groupe fini). Si f est surjectif, alors $\mathbf{Z}^k/\ker(f) \cong \mathbf{Z}^k$, et il s'ensuit que $k' = 0$ et donc que $\ker(f) = 0$, c'est-à-dire que f est injectif.

c) L'énoncé est faux, les éléments $\bar{1}, \bar{2} \in \mathbf{Z}/3\mathbf{Z}$ donnent un contre-exemple.

d) L'énoncé est vrai. Si on a une suite exacte $1 \to N \to G \to Q \to 1$, alors $|N| \cdot |Q| = |G|$. Ceci permet de montrer par récurrence sur $|G|$ que $|G|$ est le produit des ordres des groupes simples dans la liste qui lui est associée: Si G est simple c'est clair. Si G n'est pas simple il existe une suite comme ci-dessus avec $|N| < |G|$ et $|Q| < |G|$. Par hypothèse de récurrence, $|N|$ (resp. $|Q|$) est le produit des ordres des groupes simples dans la liste qui lui est associée. Comme la liste de G est la réunion des listes de N et de Q, on déduit le résultat pour G de l'égalité $|N| \cdot |Q| = |G|$.

e) L'énoncé est faux. Soit $f\colon \mathrm{S}_5 \to \mathbf{Z}/5\mathbf{Z}$ un morphisme surjectif. Si $\tau \in \mathrm{S}_5$ est une transposition, alors $2 \cdot f(\tau) = f(\tau^2) = \bar{0}$, donc $f(\tau) = 3 \cdot (2 \cdot f(\tau)) = \bar{0}$. Comme S_5 est engendré par les transpositions, il s'ensuit que $f(\sigma) = \bar{0}$ pour tout $\sigma \in \mathrm{S}_5$, contradiction.

f) L'énoncé est vrai. L'application $f\colon \mathbf{Z} \to \mathrm{S}_5$ définie par $f(k) = (1,2,3,4,5)^k$ induit un tel morphisme par passage au quotient.

g) L'énoncé est vrai. Soit ρ un générateur de N (par exemple la rotation d'angle $2\pi/n$) et soit σ la symétrie par rapport à l'axe des x. Si $x \in D_n - N$, alors $\alpha = \sigma\rho^k$ et $\alpha^2 = \sigma\rho^k\sigma\rho^k = \sigma\sigma\rho^{-k}\rho^k = \mathrm{id}$.

Exercice 2

a) On applique l'algorithme 12.19.

b) Le morphisme $f\colon \mathbf{Z}^3 \to \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$ défini par

$$f(a,b,c) = (3a + 5b \pmod{12}, 5a + 7c \pmod{25})$$

est surjectif car $f(0, 5x, 18y) = (\bar{x}, \bar{y})$. Visiblement, $\ker(f) = H'$, donc ce morphisme induit un isomorphisme $\mathbf{Z}/H' \cong \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$. Le théorème chinois permet de conclure.

Exercice 3

a) Par définition, E est l'orbite de A pour l'opération de G sur E par conjugaison, donc $|E| = [G : G_A]$. Si $a \in A$, alors $aAa^{-1} = A$, donc $A \subset G_A$. Il s'ensuit que $|E| = [G : G_A] \leq [G : A] < p$.

b) Comme S est un p-groupe, une orbite non-triviale pour l'action de S sur E contient au moins p éléments. Il ne peut donc y avoir que des orbites triviales.

c) Clairement, $BS \neq \emptyset$. Si $b, b' \in B$ et $s, s' \in S$, alors $bsb's' = b(sb's^{-1})ss' \in BS$ et $(bs)^{-1} = s^{-1}b^{-1} = (s^{-1}b^{-1}s)s^{-1} \in BS$ donc BS est un sous-groupe de G. Si $b, b' \in B$ et $s \in S$, alors $(bs)b'(bs)^{-1} = b(sbs^{-1})b^{-1} \in B$, donc B est un sous-groupe distingué de BS.

d) Appliquant la Propostition 6.7 avec $G = BS$, $N = B$ et $H = S$, on trouve un isomorphisme $BS/B \cong S/(B \cap S)$. Comme S est un p-groupe, on déduit que $|S/(B \cap S)|$ est une puissance de p. Le fait que $[BS : B] \leq [G : B] = [G : A] < p$ implique alors que $BS/B \cong \{e\}$, donc $BS = B$. On a $S \subset BS = B$. Ceci montre que $S \subset gAg^{-1}$ pour tout $g \in G$, donc $S \subset \bigcap_{g \in G} gAg^{-1}$.

Examen d'algèbre avancée

le 8/9/1995, 14:00–17:00 heures

Il est autorisé, mais déconseillé, de consulter les documents et les livres que vous avez emporté(s). Vous pouvez utiliser les résultats de tous les exercices du polycopié, même de ceux que vous n'avez pas faits. L'utilisation de calculatrices est autorisée.

Dans chaque partie de chaque exercice, vour pourrez utiliser les résultats donnés dans les parties et les exercices précédents, même si vous n'avez pas réussi à les prouver.

1. Dans tout l'exercice p désigne un nombre premier. On pourra utiliser le résultat suivant:

   16.1 Théorème. *Soit G un groupe et soit $C = \{\, x \in G \mid xy = yx$ pour tout $y \in G \,\}$ le centre de G. Si G/C est cyclique, alors G est commutatif.*

   (a) Soit G un groupe d'ordre p^2. Montrer que G est isomorphe à $\mathbf{Z}/p^2\mathbf{Z}$ ou à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

   (b) Soit G un groupe d'ordre p^3. Montrer que si G n'est pas commutatif, alors le centre de G est d'ordre p.

2. Pour chacun des énoncés suivants, indiquer si l'énoncé est vrai ou faux et donner une démonstration de votre réponse.

   (a) Pour tout entier $n > 3$, le groupe symétrique S_n est engendré par $(1,3,2)$ et $(1,2,\ldots,n)$.

   (b) Le groupe symétrique S_6 contient exactement 240 éléments d'ordre 6.

   (c) Soit G un groupe engendré par des éléments d'ordre 3. Alors G ne contient pas d'élément d'ordre 2.

   (d) Il existe un isomorphisme $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong \mathrm{S}_3$.

   (e) Soient G un groupe fini et p un nombre premier. Si G admet un p-groupe de Sylow qui est cyclique, alors tous les p-groupes de Sylow de G sont cycliques.

   (f) Soient G_1 et G_2 deux groupes finis tels que $|G_1| = |G_2|$. Alors la liste de groupes simples associée à G_1 par le théorème de Jordan–Hölder est, à permutation près, égale à celle associée à G_2.

   (g) Soient p et q deux nombres premiers (pas necessairement distincts!) et soient G_1 et G_2 deux groupes tels que $|G_1| = |G_2| = pq$. Alors la liste de groupes simples associée à G_1 par le théorème de Jordan–Hölder est, à permutation près, égale à celle associée à G_2.

   (h) Soit G un groupe simple d'ordre 60. Alors le nombre de 3-groupes de Sylow de G est égal à 10.

3. (a) Soit $H \subset \mathbf{Z}^3$ le sous-groupe engendré par $\{\, (1,3,4), (2,2,3), (-1,1,1), (4,3,2) \,\}$. Est-ce que $\mathbf{Z}^3/H \cong \mathbf{Z}$?

   (b) Calculer le rang du groupe $\{\, (a,b,c) \in \mathbf{Z}^3 \mid a + 2b + 3c \equiv 0 \pmod 4 \,\}$.

   (c) Trouver une base du groupe $\{\, (a,b,c) \in \mathbf{Z}^3 \mid 3a + 7b = 0 \,\}$.

Corrigé de l'examen d'algèbre avancée

du 8/9/1995

Exercice 4

a) Soit C le centre de G. Comme G est un p-groupe, C est non-trivial, donc $|C| = p$ ou p^2. Si $|C| = p$, alors G/C est d'ordre p, donc cyclique et G est commutatif. Si $|C| = p^2$, alors $G = C$ donc G est également commutatif. Ceci montre que tout groupe d'ordre p^2 est commutatif. La classification des groupe commutatifs de type fini montre qu'il y a, à isomorphisme près, deux groupes commutatifs d'ordre p^2 : $\mathbf{Z}/p^2\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

b) Soit encore C le centre de G. Dans ce cas, on à $|C| = p$, p^2 ou p^3. Si $|C| = p^2$ alors G/C est d'ordre p, donc cyclique et G est commutatif. Si $|C| = p^3$, alors $G = C$ donc G est également commutatif. Il ne reste que la possibilité que $|C| = p$.

Exercice 5

a) L'énoncé est faux. Si $n = 5$, alors $(1, 3, 2)$ et $(1, 2, \ldots, 5)$ sont des permutations paires, donc le groupe qu'ils engendrent est contenu dans A_5.

b) L'énoncé est vrai. Si $\sigma \in \mathrm{S}_6$ est d'ordre 6, alors σ est un cycle de longueur 6 ou le produit de 2 cycles disjoints : une transposition et un cycle de longueur 3. Il y a $\frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{6} = 120$ cycles de longueur 6 et $\frac{6 \cdot 5}{2} \cdot \frac{4 \cdot 3 \cdot 2}{3} = 120$ produits de l'autre forme, soit au total 240 éléments d'ordre 6.

c) L'énoncé est faux. Le groupe alterné A_5 est engendré par les cycles de longueur 3, donc par des éléments d'ordre 3. Mais $(1, 2)(3, 4) \in \mathrm{A}_5$, qui contient donc un élément d'ordre 2.

d) L'énoncé est vrai. Le groupe $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ opère sur l'espace vectoriel $(\mathbf{Z}/2\mathbf{Z})^2$ par des automorphismes linéaires, donc ce groupe opère sur l'ensemble $E = \{(1, 0), (0, 1), (1, 1)\}$. Ceci induit une application $\alpha: \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \to \mathrm{Sym}(E) = \mathrm{S}_3$. Si un élément $\phi \in \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ fixe les éléments de E, alors $\phi = \mathrm{id}$, donc α est injective. Comme les deux groupes ont 6 éléments, c'est en effet un isomorphisme.

e) L'énoncé est vrai. Soit $S \subset G$ un p-groupe de Sylow cyclique et soit $x \in S$ un générateur. Si $S' \subset G$ est un autre p-groupe de Sylow, alors il existe $y \in G$ tel que $S' = y^{-1}Sy$. Comme $|S| = |S'|$ et comme l'ordre de $y^{-1}xy$ est égal à l'ordre de x, il s'ensuit que S' est engendré par $y^{-1}xy$. S' est donc cyclique.

f) L'énoncé est faux. La liste associée à A_5 est (A_5) et celle associée à $\mathbf{Z}/60\mathbf{Z}$ est

$$(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/5\mathbf{Z}),$$

quoique évidemment $|\mathrm{A}_5| = |\mathbf{Z}/60\mathbf{Z}|$.

g) L'énoncé est vrai. Si $p \neq q$, alors c'est un résultat du cours que G_1 admet un sous-groupe distingué N d'ordre $\max(p, q)$. On a $G/N \cong \mathbf{Z}/\min(p, q)\mathbf{Z}$ donc la liste associée à G_1 est $(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/q\mathbf{Z})$. Il en est de même pour G_2.

Si $p = q$ alors il s'ensuit de l'ecercice 1.a) que les listes de G_1 et de G_2 sont tous les deux égales à $(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z})$.

h) L'énoncé est vrai. Il s'ensuit du théorème de Sylow que le nombre de 3-groupes de Sylow de G est égal à 1, 4 ou 10.

   Si ce nombre vaut 1, alors l'unique 3-groupe de Sylow est distingué, ce qui contredit l'hypothèse que G est simple.

   Si ce nombre vaut 4, alors G opère de façon transtitive, donc non-triviale, sur l'ensemble de ses 4 3-groupes de Sylow. Ceci donne un morphisme non-trivial $G \to \mathrm{S}_4$, qui ne peut pas être injectif car $|G| > |\mathrm{S}_4|$. Son noyau est donc un sous-groupe distingué non-trivial de G, contredisant encore l'hypothèse.

Exercice 6

a) Non, application de l'algorithme du cours montre que $\mathbf{Z}^3/H \cong \mathbf{Z}/11\mathbf{Z}$.

b) Le morphisme $\mathbf{Z}^3 \to \mathbf{Z}/4\mathbf{Z}$ donné par $(a,b,c) \mapsto \overline{a+2b+3c}$ induit un isomorphisme

$$\mathbf{Z}^3/\{\,(a,b,c) \in \mathbf{Z}^3 \mid a+2b+3c \equiv 0 \pmod 4\,\} \cong \mathbf{Z}/4\mathbf{Z}.$$

   Le rang du groupe donné est donc égal à 3.

c) En applicant l'algorithme donné dans la démonstration du théorème 12.17, on trouve par exemple $((-7,3,0),(0,0,1))$.