9. Complément I : Anneaux quotients

Dans ce complément on explique la construction des anneaux quotients. On se donne un anneau $(A, +, \cdot)$, que l'on ne supposera pas nécessairement commutatif par souci de généralité. Un *idéal bilatère* de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on a $ax \in I$ et $xa \in I$. Quand A est commutatif, on retrouve la notion d'idéal (tout court). Commençons par metttre en évidence l'énoncé élémentaire suivant déjà mentionné dans le chapitre.

LEMME 9.1. *Soit $f : A \to B$ un morphisme d'anneaux.*

(i) Alors $\ker f := \{a \in A \,|\, f(a) = 0\}$ *est un idéal bilatère de A.*

(ii) Plus généralement, si I est un idéal (à droite, à gauche, bilatère) de B alors $f^{-1}(I)$ est un idéal du même type A.

(iii) Si f est surjective, et si I est un idéal (à droite, à gauche, bilatère) de A, alors $f(I)$ est un idéal de B.

Pour I un sous-groupe additif de A, et pour $a, b \in A$ on rappelle que la notation $a \equiv b \bmod I$ signifie $a - b \in I$, ou encore $a + I = b + I$. Le lemme suivant dit que l'on peut *additionner, soustraire ou multiplier les congruences modulo un idéal bilatère.*

LEMME 9.2. *Soient A un anneau, I un idéal de A et $a, a', b, b' \in A$ avec $a \equiv a' \bmod I$ et $b \equiv b' \bmod I$. Alors on a $a + b \equiv a' + b' \bmod I$, $a - a' \equiv b - b' \bmod I$ et*

$$ab \equiv a'b' \bmod I. \tag{61}$$

DÉMONSTRATION — Pour l'addition et la soustraction, cela découle simplement du fait que I est un sous-groupe additif de A. Pour la multiplication, on écrit $a = a' + i$ et $b = b' + j$ avec $i, j \in I$ et on constate que l'on a $ab = a'b' + a'j + ib' + ij$ avec $a'j + ib' + ij \in I$ car I est un idéal. □

Cette observation élémentaire constitue l'essentiel du (ii) du résultat suivant. Le (i) est une variante de l'argument d'unicité de la loi de groupe quotient vu au §6 Chap. 2.

THÉORÈME 9.3. *Soit A un anneau et I un sous-groupe additif de A.*

(i) Il existe au plus une structure d'anneau sur le groupe quotient A/I telle que la projection canonique $A \to A/I$ est un morphisme d'anneaux.

(ii) Une telle structure existe si, et seulement si, I est un idéal bilatère de A.

DÉMONSTRATION — Montrons d'abord la condition suffisante du (ii). On définit deux lois $+$ et $\star$ sur A/I en posant, pour $a, b \in A$,

$$(a + I) + (b + I) := (a + b) + I \text{ et } (a + I) \star (b + I) := ab + I. \tag{62}$$

Le Lemme 9.2 montre que ces deux lois sont bien définies, au sens où les éléments $(a+b)+I$ et $ab+I$ ne dépendent que des classes $a+I$ et $b+I$ et non des représentants a et b choisis dans ces classes. Par construction, $\pi : A \to A/I$ vérifie $\pi(a + b) = \pi(a) + \pi(b)$ et $\pi(ab) = \pi(a) \star \pi(b)$ pour tout $a, b \in A$. Par surjectivité de π, le fait que $(A, +, \cdot)$ est un anneau implique immédiatement que $(A, +, \star)$ est un anneau, et que π est un morphisme d'anneaux. Par exemple,

$$(a + I) \star ((b + I) + (c + I)) = \pi(a) \star \pi(b + c) = \pi(a(b + c))$$

$$= \pi(ab+ac) = \pi(a)\pi(b) + \pi(a)\pi(c) = (a+I)\star(b+I) + (a+I)\star(c+I),$$

démontrent la distributivité d'un côté. On vérifie de même la distributivité de l'autre côté, l'associativité de $+$ et $\star$, et que les neutres additifs et multiplicatifs de $(A/I, +, \star)$ sont $\pi(0) = I$ et $\pi(1) = 1 + I$.

Vérifions maintenant le (i). Supposons qu'il existe une structure d'anneau sur A/I, disons $(A/I, +, \star)$, telle que la projection canonique $\pi : A \to A/I, a \mapsto a+I$, est un morphisme d'anneaux. Les formules $\pi(a+b) = \pi(a)+\pi(b)$ et $\pi(ab) = \pi(a)\star\pi(b)$ montrent bien que que $+$ et $\star$ sont uniquement déterminés par l'addition et la multiplication de A, et vérifient nécessairement (62). Ce conclut la démonstration du (i). Un condition nécessaire supplémentaire est que I est un idéal bilatère de A. En effet, on sait $I = \ker\pi$, et pour $a, b \in A$ et $x \in I$, on a $\pi(axb) = \pi(a)\star\pi(x)\star\pi(b) = 0$ car $\pi(x) = 0$. □

Remarque 9.4. Tout comme pour les groupes quotients, nous aurions aussi pu observer que la loi multiplicative de l'anneau A/I, vu comme sous-ensemble de $\mathrm{P}(A)$, est induite par $(X, Y) \mapsto XY + I$ (produit et somme des parties, l'ajout de I est cette fois-ci nécessaire).

Définition 9.5. *Si A est un anneau et I un idéal bilatère de A, l'anneau quotient A/I est l'ensemble A/I muni de son unique structure d'anneaux telle que la projection canonique $\pi : A \to A/I$ est un morphisme d'anneaux.*

Exemple 9.6. (Retour sur $\mathbb{Z}/N\mathbb{Z}$) Pour $N \in \mathbb{Z}$, $N\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$. La structure d'anneau quotient sur $\mathbb{Z}/N\mathbb{Z}$ est celle rendant la projection $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}, k \mapsto \overline{k}$ un morphisme d'anneaux, *i.e.* $\overline{k+k'} = \overline{k} + \overline{k'}$, $\overline{kk'} = \overline{k}\cdot\overline{k'}$. C'est bien celle considérée au chapitre 2.

Exemple 9.7. (L'anneau $k[X]/(P)$) Soient k un anneau commutatif et $P \in k[X]$. La structure d'anneau quotient sur le groupe additif quotient $k[X]/(P)$ est l'unique telle que pour tout $A, B \in k[X]$, on a $\overline{A}\cdot\overline{B} = \overline{AB}$, où $\overline{A}$ désigne la classe de A modulo (P). Faisons deux observations supplémentaires :

(i) Supposons P de degré de $n \geqslant 1$ et de coefficient dominant dans $k^\times$. Tout élément de $k[X]/(P)$ possède alors un unique représentant dans $k[X]$ de degré $< n$. En effet, pour tout $Q \in k[X]$ il existe des uniques $A, B \in k[X]$ avec $Q = AP + B$ et $\deg B < n$ si B est non nul (*division euclidienne par un polynôme de coefficient dominant inversible*).

(ii) Si k est un corps, l'hypothèse sur le coefficient dominant de P est automatiquement satisfaite. De plus, l'anneau $k[X]/(P)$ est un k-espace vectoriel de manière naturelle (laquelle ?), et on vient de voir qu'il a pour base les classes des n monômes $1, X, \ldots, X^{n-1}$.

Proposition 9.8. *(Propriété universelle des anneaux quotients) Soient A un anneau, I un idéal bilatère de A et $f : A \to B$ un morphisme d'anneaux vérifiant $I \subset \ker f$. Alors il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ envoyant $a + I$ sur $f(a)$ pour tout $a \in A$.*

Bien sûr, la propriété $\overline{f}(a+I) = f(a)$ s'écrit aussi $f = \overline{f} \circ \pi$ avec $\pi : A \to A/I$ la projection canonique.

Démonstration — L'existence et unicité d'un morphisme de groupes additifs $\overline{f} : A/I \to B$ vérifiant $\overline{f}(a+I) = f(a)$ pour tout $a \in A$ découle par exemple de la Proposition 6.16 Chap. 2. Cette propriété entraîne automatiquement que $\overline{f}$ est un morphisme d'anneaux. En effet, on a $\overline{f}(1+I) = f(1) = 1$, et pour $a, a' \in A$ on a

$$\overline{f}((a+I)(a'+I)) = \overline{f}(aa'+I) = f(aa') = f(a)f(a') = \overline{f}(a+I)\overline{f}(a'+I).$$

(On n'a finalement utilisé l'hypothèse I bilatère que pour assurer l'existence de l'anneau quotient A/I). □

Corollaire 9.9. *(même hypothèses) Si en outre f est surjective et vérifie* $\ker f = I$*, alors $\overline{f}$ est un isomorphisme d'anneaux $A/I \xrightarrow{\sim} B$.*

Démonstration — En effet, le noyau de $\overline{f}$ est $\{a+I \mid f(a) = 0\}$, c'est donc $\{I\}$ (élément neutre de $(A/I, +)$). Ainsi, $\overline{f}$ est injective. Comme elle est clairement surjective car f l'est, elle est bijective : c'est un isomorphisme. □

La proposition suivante est l'analogue pour les anneaux de la Proposition 6.19 Chap. 2.

Proposition 9.10. *Soit I un idéal bilatère de l'anneau A.*

(i) L'application $J \mapsto J/I$ induit une bijection croissante entre idéaux bilatères J de A (resp. à gauche, resp. à droite) contenant I et idéaux bilatères (resp. à gauche, resp. à droite) de A/I.

(ii) Si J est un idéal bilatère de A contenant I, le morphisme d'anneaux naturel $A/I \to A/J$ est surjectif de noyau J/I, et induit un isomorphisme d'anneaux $(A/I)/(J/I) \simeq A/J$.

Démonstration — On sait déjà que $J \mapsto J/I$ induit une bijection entre sous-groupes J de A contenant I et sous-groupes du groupe additif quotient A/I, de bijection réciproque $K \mapsto \pi^{-1}(K)$, par la Proposition 6.19 Chap. 2. Le (i) se déduit du fait que pour un morphisme surjectif d'anneaux quelconque $A \to B$, l'image d'un idéal bilatère (resp. à gauche, resp. à droite) de A est un idéal bilatère (resp. à gauche, resp. à droite) de B, et l'image inverse d'un idéal bilatère de B (resp. à gauche, resp. à droite) est un idéal bilatère (resp. à gauche, resp. à droite) de A (Lemme 9.1).

Pour le (ii), la Proposition 9.8 montre qu'il existe un unique morphisme d'anneaux $A/I \to A/J, a+I \mapsto a+J$. Il est clairement surjectif de noyau $\{a+I \in A/I \mid a+J = J\} = J/I$. On conclut par le Corollaire 9.9. □

En guise d'application des anneaux quotients, discutons quelques constructions d'anneaux simples et de corps.

Définition 9.11. *Un anneau A est dit* simple *s'il est non nul, et si ses seuls idéaux bilatères sont $\{0\}$ et A.*

EXEMPLE 9.12. *(i) Si k un anneau à division, alors k est simple.* En effet, soit I un idéal bilatère de k contenant un élément x non nul. Alors x est inversible dans k, donc il existe $y \in k$ avec $yx = 1$. On a alors $1 = yx \in I$, puis $a = a.1 \in I$ pour tout $a \in k$, et enfin $I = k$.

(ii) Un anneau commutatif est simple si, et seulement si, c'est un corps. En effet, on a vu au (i) qu'un corps est simple. Réciproquement, soit A un anneau simple et commutatif, et soit $x \in A$ non nul. Alors $Ax \subset A$ est un idéal bilatère de A car A est commutatif. Comme on a $Ax \neq \{0\}$, on a donc $Ax = A$ car A est simple, puis $x \sim 1$ et $x \in A^\times$.

(iii) Si k est un anneau à division, l'anneau $\mathrm{M}_n(k)$ est simple (non commutatif pour $n > 1$). En effet, soient I idéal bilatère $\mathrm{M}_n(k)$ et $X \in I$ non nul. Il existe $1 \leqslant i, j \leqslant n$ avec $X_{i,j} \in k^\times$. Notant $\mathrm{E}_{i,j}$ les matrices élémentaires usuelles, pour tout $1 \leqslant p, q \leqslant n$ on a donc $X_{i,j}^{-1}\mathrm{E}_{p,i}X\mathrm{E}_{j,q} = \mathrm{E}_{p,q} \in I$ car I est bilatère, puis $I = \mathrm{M}_n(k)$. Plus généralement, pour un anneau A quelconque cet argument montre que les idéaux bilatères de $\mathrm{M}_n(A)$ sont les $\mathrm{M}_n(I)$ avec I idéal bilatère de A.

DÉFINITION 9.13. *Un idéal bilatère I d'un anneau A est dit* maximal *si on a $I \neq A$, et si pour tout idéal bilatère J de A contenant I on a $J = I$ ou $J = A$.*

LEMME 9.14. *Soient A un anneau et I un idéal bilatère de A. L'anneau quotient A/I est simple si, et seulement si, I est maximal.*

DÉMONSTRATION — L'assertion (i) de la Proposition 9.10 affirme que les idéaux bilatères de A/I sont en bijection naturelle avec les idéaux bilatères de A contenant I. Ainsi, I est maximal si, et seulement si, A/I a pour uniques idéaux les deux idéaux distincts $\{0\}$ et A/I, ce qui équivaut à dire que A/I est simple. □

On suppose désormais A commutatif. Le lemme ci-dessus affirme qu'un idéal $I \subsetneq A$ est maximal si, et seulement si, l'anneau quotient A/I est un corps. Cela fournit une technique importante de construction de corps.

EXEMPLE 9.15. (*Une construction du corps des réels*) Soit A l'ensemble des suites de Cauchy de rationnels.[3] On constate que A est un sous-anneau de l'anneau produit $\mathbb{Q}^{\mathbb{N}}$, et que le sous-ensemble $I \subset A$ constitué des suites (x_n) qui tendent vers 0 est un idéal de A. On a $I \neq A$ car la suite constante $1 = (1)$ est dans $A \smallsetminus I$. L'idéal I est maximal. En effet, si une suite de Cauchy $x = (x_n) \in A$ ne tend pas vers 0, il existe $\epsilon > 0$ et $N \geqslant 1$ avec $|x_n| \geqslant \epsilon$ pour tout $n \geqslant N$ (couper les ϵ en deux). Ainsi, la suite $y = (y_n)$ définie par $y_n = 0$ pour $n < N$, et $y_n = 1/x_n$ pour $n \geqslant N$, est une suite de Cauchy, et on a $yx - 1 \in I$. Ainsi, A/I est un corps : c'est l'une des constructions possibles du corps $\mathbb{R}$ des réels à partir de $\mathbb{Q}$.

.

COROLLAIRE 9.16. *Soient A un anneau principal et $\pi \in A$ un irréductible. Alors l'anneau quotient $A/\pi A$ est un corps.*

3. On rappelle que cela signifie que pour tout $\epsilon \in \mathbb{Q}_{>0}$, il existe $N \geqslant 1$ tel que $|x_n - x_m| < \epsilon$ pour tout $m, n \geqslant N$. Dans le cas particulier $\epsilon = 1$, et posant $M = \mathrm{Max}_{m \leqslant N}|x_m|$, on a alors $|x_n| \leqslant M + 1$ pour tout $n \geqslant 0$, et donc (x_n) est bornée.

Démonstration — Soit I un idéal de A contenant π. On peut écrire $I = \omega A$ car A est principal. On a $\pi \in I$ donc $\omega \mid \pi$. Comme π est irréductible, on a soit $\omega \sim \pi$, soit $\omega \sim 1$, ou ce qui revient au même, soit $I = \pi A$, soit $I = A$. Comme on a $\pi A \neq \{0\}$ (car π est irréductible), on a montré que πA est maximal. □

Par exemple, on retrouve que si $p \in \mathbb{Z}$ est un nombre premier, alors l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps. Pour $A = k[X]$ on en déduit aussi :

Corollaire 9.17. *Soient k un corps et $P \in k[X]$ un polynôme irréductible. Alors l'anneau quotient $k[X]/(P)$ est un corps.*

Ce corollaire est la source de nombreuses constructions d'*extensions de corps*. En effet, l'application $k \mapsto K := k[X]/(P)$, $\lambda \mapsto \overline{\lambda}$, est un morphisme injectif de corps, souvent simplement vu comme une inclusion. Le corps K est alors un k-espace vectoriel de dimension $n := \deg P$, avec pour base naturelle les classes de $1, X, X^2, \ldots, X^{n-1}$ (Exemple 9.7).

Exemple 9.18. (i) Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, et le corps quotient $C := \mathbb{R}[X]/(X^2+1)$ est une définition possible du corps $\mathbb{C}$ des nombres complexes. On pose simplement $i := X \bmod (X^2 + 1)$ dans C.

(ii) Soit p un nombre premier. Il existe p^2 polynômes unitaires de degré 2 dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\frac{p(p+1)}{2}$ d'entre eux sont réductibles, il y en a $\frac{p(p-1)}{2} \geqslant 1$ qui sont irréductibles. Si P est un tel polynôme, le corps $(\mathbb{Z}/p\mathbb{Z})[X]/(P)$ est un surcorps de $\mathbb{Z}/p\mathbb{Z}$ de cardinal p^2. En fait, pour $p \neq 2$ on peut prendre $P = X^2 - a$ où $a \in \mathbb{Z}/p\mathbb{Z}$ n'est pas un carré (il en existe !). Pour $p = 2$, l'unique possibilié pour P est $X^2 + X + 1$.

(iii) Dans le cours d'Algèbre 2 nous verrons qu'il existe des polynômes irréductibles de tout degré à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et en particulier des surcorps de $\mathbb{Z}/p\mathbb{Z}$ de cardinal p^n pour tout $n \geqslant 1$. Mieux, un tel corps est unique à isomorphisme près.

Terminons par une application du Lemme de Zorn importante dans ce contexte.

Proposition 9.19. (Théorème de Krull) *Soient A un anneau et I un idéal bilatère de A avec $I \subsetneq A$. Il existe un idéal maximal M de A contenant I.*

Démonstration — L'ensemble $\mathscr{J}$ des idéaux bilatères J de A avec $I \subset J$ et $J \subsetneq A$ est non vide, car il contient I par hypothèse. Ordonné par l'inclusion, il est inductif. En effet, si $\{J_i\}$ est une famille totalement ordonnée d'idéaux bilatères de A avec $I \subset J_i \subsetneq A$, alors $J = \bigcup_i J_i$ est encore un idéal bilatère de A contenant I. Il est strict car sinon $1 \in J$ et donc $1 \in J_i$ pour un certain i, puis $A = J_i$, une absurdité. D'après le Lemme de Zorn, $\mathscr{J}$ possède un élément maximal M, qui répond à la question. □

10. Complément II : Quaternions entiers, sommes de 4 carrés et sous-groupes libres de SO(3)

On se propose dans ce complément d'aborder l'arithmétique du sous-anneau

$$\mathrm{H}_{\mathbb{Z}} := \mathbb{Z} \oplus \mathbb{Z}\, I \oplus \mathbb{Z}\, J \oplus \mathbb{Z}\, K \subset \mathbb{H}$$

des *quaternions entiers*, aussi appelés *quaternions de Lipschitz*, revisitant notamment des travaux de Hurwitz [4] et Dickson [5]. Cet anneau non commutatif contient par exemple les "copies" $\mathbb{Z}[I]$, $\mathbb{Z}[J]$ et $\mathbb{Z}[K]$ de l'anneau des entiers de Gauss, ainsi que tous les $\mathbb{Z}[\sqrt{-d}]$ quand d est somme de 3 carrés. [6] Comme nous le verrons, il n'est pas très loin d'être principal (des deux côtés !) et des assertions de factorisation unique seront valables dans cet anneau, malgré sa non commutativité. Nous en donnerons dans ce complément deux applications, l'une à l'étude des sommes de 4 carrés, et l'autre à la construction de sous-groupes libres de SO(3).

10.1. Sommes de 4 carrés. Parallèlement aux liens entre $\mathbb{Z}[i]$ et les sommes de deux carrés, l'arithmétique de $\mathrm{H}_{\mathbb{Z}}$ est très reliée à l'étude des sommes de 4 carrés d'entiers. En effet, si l'on pose

$$\mathrm{r}_4(n) = |\{(x_1,x_2,x_3,x_4) \in \mathbb{Z}^4 \mid x_1^2+x_2^2+x_3^2+x_4^2 = n\}|$$

pour $n \in \mathbb{N}$, on a bien sûr $\mathrm{r}_4(n) = |\{q \in \mathrm{H}_{\mathbb{Z}} \mid \mathrm{n}(q) = n\}|$. Nous allons démontrer les deux résultats classiques suivants :

Théorème 10.1. (Lagrange, 1770) *Tout entier $\geqslant 0$ est somme de 4 carrés.*

Notons $v(n)$ la somme des diviseurs *impairs* de l'entier $n \geqslant 1$. En particulier, on a $v(n) = \sum_{d|n} d$ pour n impair, et $v(2n) = v(n)$ pour tout n.

Théorème 10.2. (Jacobi, 1834) *Soit $n \geqslant 1$. On a $\mathrm{r}_4(n) = 8\,v(n)$ pour n impair, $\mathrm{r}_4(n) = 24\,v(n)$ pour n pair. En particulier, pour tout nombre premier p on a*

$$\mathrm{r}_4(p) = 8\,(p+1).$$

Le théorème de Jacobi entraîne évidemment celui de Lagrange, qui s'écrit aussi $\mathrm{r}_4(n) \geqslant 1$ pour tout $n \geqslant 1$. Examinons l'énoncé de Jacobi sur quelques exemples, en considérant les écritures $n = x_1^2+x_2^2+x_3^2+x_4^2$ avec les $x_i \in \mathbb{Z}$:

($n=2$) Deux x_i sont nuls et les autres valent ± 1, on a bien $\mathrm{r}_4(2) = \binom{4}{2}2^2 = 24$.

($n=3$) Un des x_i est nul et les autres valent ± 1, on a bien $\mathrm{r}_4(3) = 4\cdot 2^3 = 8\cdot 4$.

($n=4$) Soit tous les x_i valent ± 1, soit tous les x_i sont nuls sauf 1 qui vaut ± 2, et on a bien $\mathrm{r}_4(4) = 2^4 + 4\cdot 2 = 24\cdot 1$.

($n=13$) De même, il y a $4\cdot 3\cdot 2^2 = 8\cdot 6$ écritures de la forme $13 = 2^2+3^2+0+0$, et $2^4\cdot 4 = 8\cdot 8$ écritures de la forme $13 = 1+4+4+4$, puis $\mathrm{r}_4(13) = 8\cdot 14$.

La démonstration originale de Jacobi, de nature analytique, consiste à montrer et utiliser le fait que la série génératrice $\sum_{n\geqslant 0} \mathrm{r}_4(n)\,q^n$ est le développement de Fourier d'une « forme modulaire ». La preuve exposée ci-dessous, dont les idées remontent à Lipchitz, Hurwitz et Dickson, est basée sur l'arithmétique de l'anneau $\mathrm{H}_{\mathbb{Z}}$. Terminons cette partie par des réductions élémentaires :

Lemme 10.3. *Pour $n \geqslant 1$ on pose $f(n) = \frac{1}{8}\mathrm{r}_4(n)$. On a*

(i) $f(mn) = f(m)f(n)$ pour $m,n \geqslant 1$ avec $m \wedge n = 1$ et n impair,
(ii) $f(p^k) = 1+p+\cdots+p^k$ pour p premier impair et $k \geqslant 0$,

4. A. Hurwitz, *Vorlesungen Über die Zahlentheorie der Quaternionen*, Springer Verlag (1919).
5. L. E. Dickson, *Arithmetic of Quaternions*, Proc. London Math. Soc. (1922), 225–232.
6. En effet, pour $q = aI+bJ+cK$ avec $a,b,c \in \mathbb{Z}$ on a $q^2 = -d$ avec $d = a^2+b^2+c^2$.

(iii) $f(2^k) = 3$ *pour* $k \geqslant 1$.

Les points (i) et (ii) de ce lemme constituent le coeur de la démonstration, et seront démontrés dans les sections suivantes. Montrons immédiatement le point (iii), qui s'écrit aussi $\mathrm{r}_4(2^m) = 24$ pour $m \geqslant 1$. On a déjà vu $\mathrm{r}_4(2) = \mathrm{r}_4(4) = 24$ ci-dessus. Soient $x \in \mathbb{Z}^4$ avec $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2^m$ et $m \geqslant 3$. Comme le carré d'un nombre impair est $\equiv 1 \bmod 8$, on en déduit que tous les x_i sont pairs. On a montré $\mathrm{r}_4(2^m) = \mathrm{r}_4(2^{m-2})$ pour $m \geqslant 3$, ce qui conclut.

Démonstration — (Le Lemme 10.3 entraîne le Théorème 10.2). Soient $m, n \geqslant 1$ premier entre eux. Tout diviseur impair de mn s'écrit de manière unique ab avec $a|m$, $b|m$ et a, b impairs. On a donc $\upsilon(mn) = \upsilon(m)\upsilon(n)$. Pour n impairs on a aussi $f(mn) = f(m)f(n)$ par le (i) du lemme, et pour p premier impair, on a $f(p^k) = \upsilon(p^k)$ par le (ii). On en déduit $f(2^k n) = f(2^k)\upsilon(n)$ pour tout n impair et tout $k \geqslant 0$ en décomposant n en produit de puissances de premiers impairs distincts. Par le (iii) du lemme on a $f(2^k) = 3$ pour $k > 0$, et on a $f(1) = 1$. Pour conclure il suffit d'observer que l'on a $\upsilon(2^k n) = \upsilon(2^k)\upsilon(n) = \upsilon(n)$. □

10.2. La divisibilité dans l'anneau $\mathrm{H}_\mathbb{Z}$. On s'intéresse aux questions de divisibilité dans l'anneau $\mathrm{H}_\mathbb{Z}$. Soient q et q' dans $\mathrm{H}_\mathbb{Z}$. Nous dirons que q divise q', et noterons $q \,|\, q'$ s'il existe $h \in \mathrm{H}_\mathbb{Z}$ avec $q' = hq$. Autrement dit, on a

$$q \,|\, q' \iff q' \in \mathrm{H}_\mathbb{Z}\, q \tag{63}$$

Dans cette situation non commutative, cette notion de divisibilité *par la droite* est bien sûr concurrente à celle de divisibilité *par la gauche*, qui consisterait à demander $q' \in q\,\mathrm{H}_\mathbb{Z}$. Nous n'utiliserons pas cette dernière dans ce qui suit au delà de l'exemple ci-dessous, qui montre que les deux notions ne sont pas équivalentes en général (sauf bien sûr si quand l'élement q est en fait dans $\mathbb{Z}$).

Exemple 10.4. *Considérons les éléments* $q = 1 + 2I$ *et* $q' = 1 + 2J$*, tous deux de norme* 5*, on a donc* $qq' = 1 + 2I + 2J + 4K$*. Mais* q *ne divise pas* qq' *! En effet, si on avait* $qq' = hq$ *avec* $h \in \mathrm{H}_\mathbb{Z}$ *on aurait* $qq'q^{-1} \in \mathrm{H}_\mathbb{Z}$*, mais on constate*

$$qq'q^{-1} = \frac{1}{5}qq'q^\star = \frac{1}{5}(1 + 2I + 2J + 4K)(1 - 2I) = \frac{1}{5}(5 - 6J + 8K) \notin \mathrm{H}_\mathbb{Z}.$$

On a toujours manifestement $q \,|\, q'$ et $q' \,|\, q'' \implies q \,|\, q''$. De plus, comme dans le cas commutatif, on dira que q et q' sont *associés* si on a $q \,|\, q'$ et $q' \,|\, q$, c'est une relation d'équivalence sur $\mathrm{H}_\mathbb{Z}$ que l'on notera $q \sim q'$. On vérifie immédiatement :

$$q \sim q' \iff \mathrm{H}_\mathbb{Z}\, q = \mathrm{H}_\mathbb{Z}\, q' \iff \exists\, u \in \mathrm{H}_\mathbb{Z}^\times \,|\, q' = uq. \tag{64}$$

Il nous faut maintenant déterminer le groupe des inversibles $\mathrm{H}_\mathbb{Z}^\times$ de $\mathrm{H}_\mathbb{Z}$. On rappelle

$$\mathrm{H}_8 = \{\pm 1, \pm I, \pm J, \pm K\} \subset \mathrm{H}_\mathbb{Z}.$$

De plus, $\mathrm{H}_\mathbb{Z}$ est stable par la *conjugaison* $q \mapsto q^\star$.

Proposition 10.5. *On a* $\mathrm{H}_\mathbb{Z}^\times = \{q \in \mathrm{L} \mid \mathrm{n}(q) = 1\} = \mathrm{H}_8$.

Démonstration — La seconde égalité est immédiate, car les seuls éléments $x \in \mathbb{Z}^4$ vérifiant $\sum_{i=1}^4 x_i^2 = 1$ sont les 8 avec 3 coordonnées nulles et la dernière égale à ± 1. Montrons la première. Supposons $qq' = 1$ avec $q, q' \in \mathrm{H}_\mathbb{Z}^\times$. En prenant la norme on a

$\mathrm{n}(q)\mathrm{n}(q') = 1$ puis $\mathrm{n}(q) = 1$ car $\mathrm{n}(\mathrm{H}_\mathbb{Z}) \subset \mathbb{Z}_{\geqslant 0}$. Réciproquement, comme L est stable par conjugaison, pour $q \in \mathrm{L}$ avec $\mathrm{n}(q) = qq^\star = q^\star q = 1$, on a $q \in \mathrm{L}^\times$ et $q^{-1} = q^\star$. □

La multiplicativité de la norme $\mathrm{n} : \mathrm{H}_\mathbb{Z} \to \mathbb{N}$ a joué un rôle ci-dessus. Comme pour les anneaux $\mathbb{Z}[\sqrt{d}]$ c'est un outil important pour comprendre la divisibilité dans $\mathrm{H}_\mathbb{Z}$:

LEMME 10.6. *Soient $q, q' \in \mathrm{H}_\mathbb{Z}$ avec q non nul et $q \,|\, q'$. On a la divisibilité $\mathrm{n}(q) \,|\, \mathrm{n}(q')$ dans $\mathbb{Z}$, et on a $q \sim q'$ si et seulement si, $\mathrm{n}(q) = \mathrm{n}(q')$.*

DÉMONSTRATION — Écrivons $q' = hq$ avec $h \in \mathrm{H}_\mathbb{Z}$. En prenant la norme on a $\mathrm{n}(q') = \mathrm{n}(h)\mathrm{n}(q)$ puis $\mathrm{n}(q) \,|\, \mathrm{n}(q')$. Supposant $\mathrm{n}(q) = \mathrm{n}(q')$, on a $\mathrm{n}(h) = 1$ puis $h \in L^\times$ par la Proposition 10.5, et donc $q \sim q'$. Si réciproquement on a $q = \xi q'$ avec $\xi' \in \mathrm{H}_\mathbb{Z}^\times$, on a $\mathrm{n}(q) = \mathrm{n}(q')$ car $\mathrm{n}(\xi) = 1$. □

Comme on s'intéresse à la divisibilité par la droite nous allons étudier les idéaux à gauche de $\mathrm{H}_\mathbb{Z}$ (Définition (63)). Pour faire court, *nous utiliserons désormais la terminologie « idéal » pour « idéal à gauche »*.[7] Un idéal de $\mathrm{H}_\mathbb{Z}$ sera dit *impair* s'il contient un élément de norme impaire. Un idéal de $\mathrm{H}_\mathbb{Z}$ sera dit principal s'il est de la forme $\mathrm{H}_\mathbb{Z}\, q$ avec $q \in \mathrm{H}_\mathbb{Z}$. Nous allons montrer la :

PROPOSITION 10.7. (Dickson) *Tout idéal impair de $\mathrm{H}_\mathbb{Z}$ est principal.*

On commence par établir une forme de division euclidienne. L'élément *de Hurwitz*

$$\omega = \frac{1}{2}(1 + I + J + K) \;\in\; \mathbb{H}$$

jouera un rôle important. On a $2\,\omega \in \mathrm{H}_\mathbb{Z}$, mais ω n'est pas dans $\mathrm{H}_\mathbb{Z}$.

LEMME 10.8. *Soit $h \in \mathbb{H}$, il existe $q \in \mathrm{H}_\mathbb{Z}$ avec soit $\mathrm{n}(h - q) < 1$, soit $h - q = \omega$.*

DÉMONSTRATION — Écrivons $h = x_1 + x_2 I + x_3 J + x_4 K$ avec $x_1, x_2, x_3, x_4 \in \mathbb{R}$, on peut toujours trouver $x_1', x_2', x_3', x_4' \in \mathbb{Z}$ avec $|x_i - x_i'| \leqslant 1/2$ pour tout i. Posant $q = x_1' + x_2' I + x_3' J + x_4' K \in \mathrm{H}_\mathbb{Z}$ on a alors $\mathrm{n}(h - q) = \sum_{i=1}^4 (x_i - x_i')^2 \leqslant 1/4 + 1/4 + 1/4 + 1/4 = 1$, avec égalité si, et seulement si, on a $h - q = \frac{1}{2}(\pm 1 \pm I \pm J \pm K)$. Dans ce cas d'égalité, on a en particulier $h \in \mathrm{H}_\mathbb{Z} + \omega$. □

Pour gérer l'alternative donnée par le Lemme 10.8, nous aurons besoin de deux observations simples sur l'élément ω, connues de Hurwitz.

LEMME 10.9. *(i) Pour tout $q \in \mathrm{H}_\mathbb{Z}$ on a $\mathrm{n}(q + \omega) \in \mathbb{Z}$.*
(ii) Pour $q \in \mathrm{H}_\mathbb{Z}$ de norme impaire, on a $\omega q \notin \mathrm{H}_\mathbb{Z}$.

DÉMONSTRATION — Pour le (i), on constate que l'on a $q + \omega = \frac{1}{2}(x_1 + x_2 I + x_3 J + x_4 K)$ avec $x_i \in 2\mathbb{Z} + 1$ pour tout i. En particulier, on a $x_i^2 \equiv 1 \bmod 4$, et donc $\mathrm{n}(q + \omega) \in \frac{1}{4}(4 + 4\mathbb{Z}) = \mathbb{Z}$. Pour le (ii), supposons $\mathrm{n}(q) = 2k + 1$ impair. En multipliant à gauche par ω on trouve $\omega = (\omega q)\overline{q} - (2\omega)k$, puis $\omega \in \mathrm{H}_\mathbb{Z}$ si $\omega q \in \mathrm{H}_\mathbb{Z}$, une contradiction. □

7. En fait, l'involution $q \mapsto q^\star$ de $\mathrm{H}_\mathbb{Z}$ vérifie $(xy)^\star = y^\star x^\star$ et donc échange idéaux à gauche et idéaux à droite, de sorte que tout ce que nous prouverons sur les idéaux (à gauche) aura un analogue sur ceux à droite, que nous n'expliciterons pas car cela ne nous servira pas.

Démonstration — (de la Proposition 10.7) Soit $I \subset \mathrm{H}_\mathbb{Z}$ un idéal non nul. On a alors $\mathrm{n}(I \setminus \{0\}) \subset \mathbb{Z}_{>0}$. Considérons $m \in I \setminus \{0\}$ de norme minimale. Il est inversible dans le corps gauche $\mathbb{H}$. Pour $h \in I$, on peut trouver par le Lemme 10.8 un $q \in \mathrm{H}_\mathbb{Z}$ avec soit $\mathrm{n}(hm^{-1}-q) < 1$, soit $hm^{-1} = q+\omega$. Dans le premier cas, on a $\mathrm{n}(h-qm) < \mathrm{n}(m)$ par multiplicativité de la norme, et aussi $h-qm \in I$, et donc $h = qm$ par minimalité de m. Dans le second cas, on a $h = qm + \omega m$. En particulier, on a montré

$$\mathrm{H}_\mathbb{Z}\, m \;\subset\; I \;\subset\; \mathrm{H}_\mathbb{Z}\, m \;\cup\; (\mathrm{H}_\mathbb{Z} + \omega)\, m.$$

Par hypothèse sur I, la réunion $\mathrm{H}_\mathbb{Z}\, m \;\cup\; (\mathrm{H}_\mathbb{Z} + \omega)\, m$ contient donc un élément de norme impaire. Par le (i) du lemme précédent, on en déduit que $\mathrm{n}(m)$ est impair. Mais alors par le (ii) du même lemme, le second cas ci-dessus ne peut se produire pour aucun $h \in I$, car on aurait alors $q \in \mathrm{H}_\mathbb{Z}$ avec $h - qm = \omega m \in \mathrm{H}_\mathbb{Z}$. Ainsi, on est toujours dans le premier cas et on a $I = \mathrm{H}_\mathbb{Z}\, m$. □

Pour utilisation future, mentionnons la proposition suivante, conséquence immédiate de la relation (64), du Lemme 10.6 et de la Proposition 10.5. Bien sûr, un *générateur* d'un idéal I est un élément $q \in I$ avec $I = \mathrm{H}_\mathbb{Z}\, q$.

Proposition 10.10. *Chaque idéal principal non nul de* $\mathrm{H}_\mathbb{Z}$ *possède exactement* 8 *générateurs, associés, et qui sont ses éléments non nuls de plus petite norme.*

Nous sommes maintenant en mesure de démontrer le (i) du Lemme 10.3.

Lemme 10.11. *Soit* $q \in \mathrm{H}_\mathbb{Z}$ *de norme* mn *avec* $m \wedge n = 1$ *et* n *impair. Il existe* $h, h' \in \mathrm{H}_\mathbb{Z}$ *avec* $q = h'h$ *et* $\mathrm{n}(h) = n$. *De plus, si on a* $h'h = z'z$ *avec* $\mathrm{n}(z) = \mathrm{n}(h)$, *il existe un unique* $\xi \in \mathrm{H}_\mathbb{Z}^\times$ *tel que* $z = \xi h$ *et* $z' = h'\xi^{-1}$.

Démonstration — Soit $I = \mathrm{H}_\mathbb{Z}\, q + \mathrm{H}_\mathbb{Z}\, n$. C'est un idéal impair de $\mathrm{H}_\mathbb{Z}$ car il contient n. Il est donc principal, puis de la forme $I = \mathrm{H}_\mathbb{Z}\, h$ avec h standard. Tout élément de I est de norme $\equiv 0 \bmod n$. En effet, pour tout $u, v \in \mathrm{H}_\mathbb{Z}$ on a

$$\mathrm{n}(uq + vn) = \mathrm{n}(u)\mathrm{n}(q) + n\mathrm{tr}(uq\overline{v}) + n^2\mathrm{n}(v) \equiv 0 \bmod n.$$

En particulier, on a $\mathrm{n}(h) \equiv 0 \bmod n$. On a $q \in I = \mathrm{H}_\mathbb{Z}\, h$, donc il existe $h' \in \mathrm{H}_\mathbb{Z}$ avec $q = h'h$. L'égalité $nm = \mathrm{n}(h')\mathrm{n}(h)$ implique alors $\mathrm{n}(h) = n$ car $m \wedge n = 1$.

Montrons enfin l'assertion d'unicité. Pour h comme ci-dessus on peut écrire $h = uq + vn$ avec $u, v \in \mathrm{H}_\mathbb{Z}$. Supposons $q = z'z$ avec $z \in \mathrm{H}_\mathbb{Z}$ de norme n. On a alors $h = uz'z + vz^\star z \in \mathrm{H}_\mathbb{Z} z$ et $\mathrm{n}(h) = \mathrm{n}(z)$, donc $z = \xi h$ pour un unique $\xi \in \mathrm{H}_\mathbb{Z}^\times$ par le Lemme 10.6. On a donc $h'h = z'\xi h$, puis $z' = h'\xi^{-1}$. □

Démonstration — (de Lemme 10.3 (i)) Posons $\mathrm{Q}(n) = \{q \in \mathrm{H}_\mathbb{Z} \,|\, \mathrm{n}(q) = n\}$. On a $|\mathrm{Q}(n)| = \mathrm{r}_4(n) = 8f(n)$. Pour $m, n \geqslant 1$, la multiplication dans $\mathrm{H}_\mathbb{Z}$, $(h', h) \mapsto h$, définit par multiplicativité de la norme une application $\mathrm{Q}(m) \times \mathrm{Q}(n) \to \mathrm{Q}(mn)$. Pour $m \wedge n = 1$, le Lemme 10.11 montre que cette application est surjective, et que ses fibres ont chacune $|\mathrm{H}_\mathbb{Z}^\times| = 8$ éléments. On a montré $|\mathrm{Q}(m)||\mathrm{Q}(n)| = 8|\mathrm{Q}(mn)|$. □

Remarque 10.12. *La Proposition 10.7 ne vaut pas pour les idéaux non impairs. Considérons en effet le sous-ensemble* $B \subset \mathrm{H}_\mathbb{Z}$ *des quaternions de norme paire. On a*

$$B = \{t + xI + yJ + zK \in \mathrm{H}_\mathbb{Z} \;\mid\; t + x + y + z \equiv 0 \bmod 2\},$$

car on a $n^2 \equiv n \bmod 2$ *pour tout* $n \in \mathbb{Z}$. *En particulier,* B *est un sous-groupe d'indice* 2 *de* $\mathrm{H}_{\mathbb{Z}}$. *C'est alors clairement un idéal bilatère. Mais il n'est pas principal. En effet,* B *contient les* 24 *éléments de* $\mathrm{H}_{\mathbb{Z}}$ *de norme* 2, *à savoir*

$$\pm 1 \pm I, \pm 1 \pm J, \pm 1 \pm K, \pm I \pm J, \pm I \pm K \text{ et } \pm J \pm K.$$

Mais si l'idéal B *était principal, il n'aurait que* 8 *éléments de norme minimale, par la Proposition 10.10. Et en effet, on constate que l'on a*

$$(1+I)(1-J)^{-1} = \frac{1}{2}(1+I)(1+J) = \omega \notin \mathrm{H}_{\mathbb{Z}}^{\times}.$$

Hurwitz a observé que l'on peut remédier à ces problèmes en considérant

$$\mathrm{Hur} := \mathrm{H}_{\mathbb{Z}} + \mathbb{Z}\,\omega$$

(quaternions à coordonnées soit toutes dans $\mathbb{Z}$, *soit toutes dans* $\frac{1}{2}+\mathbb{Z}$*). Il observe que* Hur *est un sous-anneau de* $\mathbb{H}$. *Les arguments de cette section montrent immédiatement que tout idéal de* Hur *est principal (Hurwitz). Nous aurions pu étudier plutôt cet anneau dans cette partie, mais il est un peu moins naturel, et surtout moins commode pour l'étude des sommes de* 4 *carrés. Ajoutons que l'on a* $|\mathrm{Hur}^{\times}| = 24$.

10.3. Quaternions entiers de norme première. Notre but dans cette partie est de montrer que pour tout premier p impair on a $\mathrm{r}_4(p) = 8(p+1)$.

Lemme 10.13. *Soient* p *un nombre premier et* $q \in \mathrm{H}_{\mathbb{Z}}$. *On a*

$$\mathrm{n}(q) = p \iff \mathrm{H}_{\mathbb{Z}}\, p \subsetneq \mathrm{H}_{\mathbb{Z}}\, q \subsetneq \mathrm{H}_{\mathbb{Z}}.$$

Démonstration — La relation $\mathrm{n}(q) = p$ entraîne $p = \overline{q}q \in \mathrm{H}_{\mathbb{Z}}\, q$. On peut donc supposer $\mathrm{H}_{\mathbb{Z}}\, p \subset \mathrm{H}_{\mathbb{Z}}\, q \subset \mathrm{H}_{\mathbb{Z}}$. D'après le Lemme 10.6, on a

$$\mathrm{n}(1) \mid \mathrm{n}(q) \mid \mathrm{n}(p), \quad \text{avec } \mathrm{n}(1) = 1 \text{ et } \mathrm{n}(p) = p^2,$$

et les deux inclusions ci-dessus sont strictes si, et seulement si, les deux divisibilités ci-dessus sont strictes. Comme p est premier, c'est équivalent à $\mathrm{n}(q) = p$. □

D'après le Lemme 10.13 et les Propositions 10.10 et 10.7, il faut donc montrer la :

Proposition 10.14. *Pour* p *premier impair, il existe exactement* $p+1$ *idéaux* I *de* $\mathrm{H}_{\mathbb{Z}}$ *vérifiant* $\mathrm{H}_{\mathbb{Z}}\, p \subsetneq I \subsetneq \mathrm{H}_{\mathbb{Z}}$.

Observons que pour $n \in \mathbb{Z}$, l'idéal $\mathrm{H}_{\mathbb{Z}}\, n = n\,\mathrm{H}_{\mathbb{Z}}$ est un idéal *bilatère* de $\mathrm{H}_{\mathbb{Z}}$, car n est central dans $\mathrm{H}_{\mathbb{Z}}$. En particulier, pour p premier on dispose de l'anneau quotient $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$. D'après la générale Proposition 9.10, les idéaux à gauche de $\mathrm{H}_{\mathbb{Z}}$ contenant p sont en bijection naturelle avec les idéaux à gauche de l'anneau quotient $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$. Il s'agit donc de monter que cet anneau a exactement $p+1$ idéaux pour p impair. Il se trouve que cet anneau est familier :

Proposition 10.15. *Pour* p *premier impair on a un isomorphisme d'anneaux*

$$\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}} \simeq \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}).$$

Autrement dit, pour p premier impair, l'anneau $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ peut-être vu comme un anneau de *quaternions modulo* p ! Nous aurons besoin du lemme :

LEMME 10.16. *Soit p premier impair. Il existe $A, B \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ avec*

$$A^2 = -1_2,\ B^2 = -1_2 \text{ et } AB = -BA.$$

De plus, $1_2, A, B, AB$ est une base du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

DÉMONSTRATION — On prend pour $B \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ la matrice compagnon

$$B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

qui vérifie $B^2 = -1_2$. Les matrices $A \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ vérifiant $AB = -BA$ sont les

$$A_{x,y} := \begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \text{ avec } x, y \in \mathbb{Z}/p\mathbb{Z},$$

comme le montre un petit calcul immédiat. On a aussi $A_{x,y}^2 = (x^2 + y^2)1_2$. Or il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ vérifiant $x^2 + y^2 \equiv -1$. En effet, on sait qu'il existe $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$, et donc aussi $\frac{p+1}{2}$ éléments de la forme $-1 - y^2$ avec $y \in \mathbb{Z}/p\mathbb{Z}$, et on conclut car ces $p+1$ éléments au total ne peuvent être tous distincts. On fixe donc de tels x, y, et on pose $A := A_{x,y}$. Il ne reste qu'à vérifier que $1_2, A, B$ et AB forme nécessairement une famille libre. Mais 1_2 et B sont clairement linéairement indépendantes : on a $AB = -BA$ et $-BA \neq BA$ car $p > 2$. Donc A et AB le sont aussi car A est inversible. On conclut car elles ne sont pas dans le même espace propre de la symétrie $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}), X \mapsto BXB^{-1}$ (car $p > 2$). □

La Proposition 10.15 est maintenant à portée de main.

DÉMONSTRATION — (de la Proposition 10.15) Soit $1_2, A, B, AB$ une base de $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ comme dans la Proposition 10.16. Soit $f : \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$ l'application $\mathbb{Z}/p\mathbb{Z}$-linéaire envoyant $1_2, A, B, AB$ sur $1, I, J, K \bmod p\,\mathrm{H}_{\mathbb{Z}}$ respectivement. C'est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.[8] On a $f(1) = 1$ et il ne reste qu'à montrer que l'on a $f(xy) = f(x)f(y)$ pour tout $x, y \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Par bilinéarité, on peut supposer $x, y \in \{1_2, A, B, AB\}$, et même $x, y \neq 1_2$. Mais pour les 9 tels (x, y) restants, cela découle immédiatement des relations correspondantes $I^2 = -1$, $J^2 = -1$ et $IJ = -JI$. □

Il ne reste qu'à rappeler la structure des idéaux de $\mathrm{M}_n(k)$.

PROPOSITION 10.17. *Soient V un espace vectoriel de dimension finie sur un corps k et $A = \mathrm{End}_k(V)$ l'anneau des endomorphismes de V. Pour tout sous-espace $W \subset V$ on note $\mathrm{I}_W \subset A$ l'idéal à gauche des endomorphismes de V s'annulant sur W.*

(i) On a $\mathrm{I}_W = A\,u$ pour tout $u \in A$ de noyau W.

(ii) L'application $W \mapsto \mathrm{I}_W$ est une bijection entre sous-espaces de V et idéaux à gauche de A.

8. Comme $1, I, J, K$ est une $\mathbb{Z}$-base du groupe additif de $\mathrm{H}_{\mathbb{Z}}$, sa réduction modulo $p\mathrm{H}_{\mathbb{Z}}$ est une $\mathbb{Z}/p\mathbb{Z}$-base du groupe abélien p-élémentaire $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$.

Démonstration — Soit I un idéal à gauche de A. Soient $f_1, \cdots, f_n \in I$ avec $I = \sum_{i=1}^n Af_i$. De tels éléments existent toujours (en nombre fini) car I est de dimension finie comme k-espace vectoriel. Posons $W = \cap_{i=1}^n \ker f_i$. On a clairement $I \subset \mathrm{I}_W$, et nous allons montrer $\mathrm{I}_W = I$. Considérons l'application linéaire

$$f : V \to V^n, x \mapsto (f_1(x), \ldots, f_n(x)).$$

On a $\ker f = W$. Soit $h \in I_W$. Par définition, on a $\ker f \subset \ker h$. Par un énoncé classique de factorisation,[9] il existe une application linéaire $g : V^n \to V$ vérifiant $g \circ f = h$. Mais on peut écrire $g(x_1, x_2, \ldots, x_n) = \sum_{i=1}^n g_i(x_i)$ pour des endomorphismes $g_1, \ldots, g_n$ de V (uniquement déterminés par g). La relation $g \circ f = h$ s'écrit alors $\sum_{i=1}^n g_i f_i = h$ dans A. Comme I est un idéal à gauche, on en déduit $h \in I$, puis $\mathrm{I}_W = I$. Cela montre le (i) (cas $n = 1$), ainsi que la surjectivité dans le (ii). L'assertion d'injectivité du (ii) est une conséquence immédiate du (i). □

Démonstration — (de la Proposition 10.14, et donc de $\mathrm{r}_4(p) = 8(p+1)$) D'après la Proposition 10.16, il faut montrer que $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ possède $p+1$ idéaux à gauche *stricts*. Mais d'après la Proposition 10.17, ces idéaux sont en bijection avec les sous-espaces $0 \subsetneq W \subsetneq (\mathbb{Z}/p\mathbb{Z})^2$, c'est à dire avec les droites de $(\mathbb{Z}/p\mathbb{Z})^2$ (*i.e.* avec $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$). Mais on sait qu'il y a exactement $p+1$ telles droites (par exemple, par le Lemme 5 Chap. 4.1). □

10.4. Factorisation des quaternions de norme puissance d'un premier impair. Soit p un nombre premier impair. Pour démontrer le Lemme 10.3 (ii), nous allons étudier les factorisations des quaternions de norme p^k comme produit de quaternions de norme p. Il faudra particulièrement prendre garde au fait que pour chacun des $8(p+1)$ éléments $\pi \in \mathrm{H}_\mathbb{Z}$ de norme p on a la décomposition

$$p = \pi^\star \pi. \tag{65}$$

Un quaternion $q \in \mathrm{H}_\mathbb{Z}$ sera dit *primitif* s'il n'est pas dans $n\,\mathrm{H}_\mathbb{Z}$ pour $n \in \mathbb{Z}_{>1}$. Si $q \in \mathrm{H}_\mathbb{Z}$ est de la forme nq' avec $q' \in \mathrm{H}_\mathbb{Z}$ et $n \in \mathbb{Z}_{\geqslant 1}$, on a bien sur $n^2 \,|\, \mathrm{n}(q)$. En particulier, si p est premier un quaternion de norme p est primitif, et un quaternion de norme p^k est non primitif si, et seulement si, il est dans $p\,\mathrm{H}_\mathbb{Z}$.

On a vu au § 10.3 qu'il existe exactement $p+1$ classes d'association d'éléments de norme p dans $\mathrm{H}_\mathbb{Z}$. Nous noterons en général Π un ensemble de représentants de ces classes. Par exemple pour $p = 5$, on peut prendre $\Pi = \{1 \pm 2I, 1 \pm 2J, 1 \pm 2K\}$.

Théorème 10.18. *Soient p premier impair, Π un ensemble de représentants des éléments de norme p de $\mathrm{H}_\mathbb{Z}$ pour $\sim$, et $k \geqslant 1$ entier. Tout quaternion primitif $q \in \mathrm{H}_\mathbb{Z}$ de norme p^k s'écrit de manière unique sous la forme $q = \xi\pi_1 \cdots \pi_k$ avec*

$$\xi \in \mathrm{H}_\mathbb{Z}^\times,\ \pi_i \in \Pi \text{ pour } 1 < i \leqslant k, \text{ et } \pi_{i-1} \not\sim \pi_i^\star \text{ pour } 1 < i \leqslant k.$$

Réciproquement, tout tel produit définit un quaternion primitif de norme p^k.

Nous aurons besoin de plusieurs lemmes pour démontrer ce résultat.

Lemme 10.19. *Soient p premier impair et $q \in \mathrm{H}_\mathbb{Z}$ primitif de norme $\equiv 0 \bmod p$. Alors il existe $\pi \in \mathrm{H}_\mathbb{Z}$ de norme p, unique modulo association, tel que $q \in \mathrm{H}_\mathbb{Z}\,\pi$.*

9. Il suffit d'introduire un supplémentaire S de $\mathrm{Im}\, f$ dans V^n et de poser $g(x) = 0$ pour $x \in S$, et $g(f(x)) = h(x)$ pour $x \in V$. C'est bien défini car pour $x, x' \in V$, on a $f(x) = f(x') \implies x - x' \in \ker f \implies x - x' \in \ker h \implies h(x) = h(x')$. L'application g est trivialement linéaire.

Autrement dit, sous les hypothèses q a un unique diviseur dans Π ! Bien remarquer que ce lemme est faux pour q non primitif, par exemple on a $p \in \mathrm{H}_{\mathbb{Z}}\,\pi$ pour tout $\pi \in \Pi$ par la Formule (65).

Démonstration — Regardons l'idéal $I = \mathrm{H}_{\mathbb{Z}}\,p + \mathrm{H}_{\mathbb{Z}}\,q$ de $\mathrm{H}_{\mathbb{Z}}$. Il est impair car il contient p, il est donc principal, *i.e.* de la forme $I = \mathrm{H}_{\mathbb{Z}}\,\pi$ avec $\pi \in \mathrm{H}_{\mathbb{Z}}$. Mais tout élément de I est de norme $\equiv 0 \bmod p$. En effet, pour tout $h, h' \in \mathrm{H}_{\mathbb{Z}}$ on a

$$\mathrm{n}(hp + h'q) \;=\; p^2\,\mathrm{n}(h) \;+\; \mathrm{n}(q)\mathrm{n}(h') \;+\; p\,\mathrm{tr}(h^\star h' q) \in p\,\mathbb{Z}.$$

On en déduit $\mathrm{n}(\pi) \equiv 0 \bmod p$. Mais I n'est pas inclus dans $\mathrm{H}_{\mathbb{Z}}\,p$ car q est primitif, on a donc une inclusion stricte $\mathrm{H}_{\mathbb{Z}}\,p \subset \mathrm{H}_{\mathbb{Z}}\,\pi$, et donc $\mathrm{n}(\pi)$ est un diviseur strict de $\mathrm{n}(p) = p^2$, c'est donc p. Enfin, si on a $q \in \mathrm{H}_{\mathbb{Z}}\,\pi'$ avec $\mathrm{n}(\pi') = p$, on a $I \subset \mathrm{H}_{\mathbb{Z}}\,\pi'$ puis $\pi \in \mathrm{H}_{\mathbb{Z}}\,\pi'$ et $\pi \sim \pi'$ par le Lemme 10.6. □

Démonstration — (du Théorème 10.18, première partie) Montrons par récurrence sur $k \geqslant 1$ que tout $q \in \mathrm{H}_{\mathbb{Z}}$ primitif de norme p^k est le la forme $\xi\pi_1 \cdots \pi_k$ avec $\xi \in L^\times$ et les $\pi_i \in \Pi$ uniques. Il n'y rien à montrer pour $k = 0$, on suppose donc $k \geqslant 1$. Le lemme montre qu'il existe un unique $\pi \in \Pi$ avec $q \in \mathrm{H}_{\mathbb{Z}}\,\pi$. On a donc $q = q'\pi$ pour $q' \in \mathrm{H}_{\mathbb{Z}}$, nécessairement primitif car q l'est, de norme p^{k-1}. On conclut par récurrence. □

Il reste à montrer la condition portant sur les π_i dans la décomposirtion de q. Le lemme clé (et un peu surprenant !) est le suivant.

Lemme 10.20. *Soient p premier impair et $h, \pi, h' \in \mathrm{H}_{\mathbb{Z}}$ avec $\mathrm{n}(\pi) = p$. On a*

$$h\pi h' \in p\,\mathrm{H}_{\mathbb{Z}} \iff h\pi \in p\,\mathrm{H}_{\mathbb{Z}} \text{ ou } \pi h' \in p\,\mathrm{H}_{\mathbb{Z}}.$$

Démonstration — Fixons un morphisme surjectif d'anneaux $f : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ de noyau $p\mathrm{Hur}$ comme dans la Proposition. La relation $p = \pi\overline{\pi}$ dans Hur donne $0 = f(\pi)f(\overline{\pi})$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Mais ni $f(\pi)$, ni $f(\overline{\pi})$ n'est nul car $\pi, \overline{\pi} \notin p\mathrm{Hur}$ (sinon la norme de π serait multiple de p^2). Donc $X := f(\pi)$ est une matrice de rang 1. Posons $H = f(h)$ et $H' = f(h')$. On a H, X, H' dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ avec X de rang 1. Supposons $XH' \neq 0$. Comme on est en dimension 2, XH' est aussi de rang 1 avec même image que X. Mais alors $\mathrm{Im}\,HXH' = \mathrm{Im}\,HX$, et donc HXH' est nul si, et seulement si, HX est nul. □

Corollaire 10.21. *Soient p premier impair et $\pi_1, \pi_2, \ldots, \pi_k \in \mathrm{H}_{\mathbb{Z}}$ avec $\mathrm{n}(\pi_i) = p$ pour tout i et $\pi_1\pi_2 \cdots \pi_k \in p\,\mathrm{H}_{\mathbb{Z}}$. Alors il existe $1 \leqslant i < k$ tel que $\pi_i\pi_{i+1} \in p\,\mathrm{H}_{\mathbb{Z}}$.*

Démonstration — Par récurrence sur l'entier $k \geqslant 1$, les cas $k = 1, 2$ étant évidents. Soit $h = \pi_1\pi_2 \cdots \pi_{k-2}$. Si $h\pi_{k-1}$ est dans $p\,\mathrm{H}_{\mathbb{Z}}$ on conclut par récurrence. Sinon, on applique le lemme précédent à h, $\pi = \pi_{k-1}$ et $h' = \pi_k$, et on en déduit $\pi_{k-1}\pi_k \in p\,\mathrm{H}_{\mathbb{Z}}$. □

Démonstration — (fin de la preuve du Théorème 10.18) Les assertions restantes résultent du Corollaire 10.21 et de la remarque suivante. □

REMARQUE 10.22. *Soient $\pi, \pi' \in \mathrm{H}_{\mathbb{Z}}$ de norme p. La condition $\pi'\pi \in p\,\mathrm{H}_{\mathbb{Z}}$ signifie $\pi'\pi = p\,\xi$ pour un certain $\xi \in \mathrm{H}_{\mathbb{Z}}$ de norme 1, i.e. $\xi \in \mathrm{H}_{\mathbb{Z}}^{\times}$, soit encore $\pi' = \xi\pi^{\star}$ en multipliant à droite par $\pi^{\star}$. Autrement dit, on a $\pi'\pi \in p\,\mathrm{H}_{\mathbb{Z}} \iff \pi' \sim \pi^{\star}$.*

En guise d'application, nous obtenons le corollaire suivant, qui entraîne le Lemme 10.3 (ii) et termine donc la démonstration du théorème de Jacobi.

COROLLAIRE 10.23. *Pour p premier impair et si $k \geqslant 1$, il existe exactement $8(1 + p + \cdots + p^k)$ éléments de $\mathrm{H}_{\mathbb{Z}}$ de norme p^k.*

DÉMONSTRATION — Notons $\mathrm{a}_k(p)$ le nombre de quaternions *primitifs* de norme p^m. On a déja vu $\mathrm{a}_0(p) = 8$ et $\mathrm{a}_1(p) = 8(p+1)$. D'après le Théorème 10.18 et la remarque qui le suit, on a $\mathrm{a}_k(p) = 8(p+1)p^{k-1} = 8(p^k + p^{k-1})$. En effet, il y a $p + 1 = |\Pi|$ pour l'élément π_k, p choix pour l'élément π_{k-1} (un élément de Π non associé à $\pi_k^{\star}$), p choix pour π_{k-2} (un élément de Π non associé à $\pi_{k-1}^{\star}$), $\cdots$, et enfin 8 choix pour l'unité. Mais tout quaternion de norme p^k s'écrit de manière unique sous la forme $p^m q$ avec $0 \leqslant n \leqslant k/2$ et q primitif de norme $k - 2n$. Le nombre cherché est donc $\mathrm{a}_k(p) + \mathrm{a}_{k-2}(p) + \ldots$ qui est bien le nombre donné ! □

10.5. Une application à la construction de sous-groupes libres de $\mathrm{SO}(3)$.

.

On se propose d'utiliser l'arithmétique de $\mathrm{H}_{\mathbb{Z}}$ pour démonter le théorème suivant. On rappelle que F_n le groupe libre sur $n \geqslant 1$ générateurs (§ 8 Chap. 2).

THÉORÈME 10.24. *Pour tout entier $n \geqslant 1$, le groupe $\mathrm{SO}(3)$ possède un sous-groupe isomorphe à F_n.*

Cet énoncé, pour $n = 2$, est par exemple l'un des ingrédients clés pour démontrer le fameux *paradoxe de Banach-Tarski*, pour lequel nous renvoyons à ce court exposé de T. Tao. On rappelle que l'on a un morphisme de groupes

$$f : \mathbb{H}^{\times} \longrightarrow \mathrm{SO}(3),$$

associant à $h \in \mathbb{H}^{\times}$ la matrice de l'isométrie int_h de l'espace euclidien des quaternions purs dans la base orthonormée I, J, K (§2 Chap. 5). On a montré *loc. cit.* que f est surjectif de noyau $\mathbb{R}^{\times}$.

LEMME 10.25. *Soient p premier impair et $\pi_1, \pi_2, \ldots, \pi_n \in \mathrm{H}_{\mathbb{Z}}$ de norme p. On suppose que les $2n$ éléments $\pi_1, \pi_1^*, \pi_2, \pi_2^*, \ldots, \pi_n, \pi_n^*$ sont deux à deux non associés. Alors $f(\pi_1), f(\pi_2), \ldots, f(\pi_n)$ engendrent un sous-groupe de $\mathrm{SO}(3)$ isomorphe à F_n.*

DÉMONSTRATION — Posons $S = \{\pi_1, \pi_1^{\star}, \ldots, \pi_n, \pi_n^{\star}\}$. Pour tout $s \in S$ on a $ss^{\star} = p$ dans $\mathbb{H}^{\times}$, et donc $f(s^{\star}) = f(s)^{-1}$. Soient $k \geqslant 1$ et $m_1, m_2, \ldots, m_k \in S$ avec $m_{i-1} \neq m_i^{\star}$ pour tout $1 < i \leqslant k$. Il faut montrer $f(m_1)f(m_2)\cdots f(m_k) \neq 1$ dans $\mathrm{SO}(3)$. Posons $m = m_1 m_2 \cdots m_k \in \mathrm{H}_{\mathbb{Z}}$ et supposons donc par l'absurde $f(m) = 1$, ou ce qui revient au même $m \in \mathbb{R}^{\times} = \ker f$. On a donc $m \in \mathrm{H}_{\mathbb{Z}} \cap \mathbb{R} = \mathbb{Z}$, et aussi $\mathrm{n}(m) = \prod_{i=1}^{k} \mathrm{n}(\pi_i) = p^k$. On en déduit $m = \pm p^{k/2}$, $k \equiv 0 \bmod 2$, et en particulier, $m \in p\,\mathrm{H}_{\mathbb{Z}}$. Le Corollaire 10.21 et la Remarque 10.22 entraînent donc qu'il existe $1 < i \leqslant k$ avec $m_{i-1} \sim m_i^*$. Cela contredit notre hypothèse $m_{i-1} \neq m_i^*$, car on a $s \not\sim s'$ pour s, s' distincts dans S. □

Il existe bien d'autres méthodes pour construire des sous-groupes libres de SO(3). L'un des charmes de celle-ci est qu'elle produit des exemples explicites de matrices à petits coefficients, comme le montrent les deux exemples ci-dessous.

EXEMPLE 10.26. *Pour $p = 3$, on constate aisément*[10] *que les deux éléments $\pi_1 = 1 + I + J$ et $\pi_2 = 1 + I - J$ vérifient l'hypothèse du Lemme 10.25. Un simple calcul montre que l'on a*

$$f(\pi_1) = \frac{1}{3}\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{bmatrix} \text{ et } f(\pi_2) = \frac{1}{3}\begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ 2 & 2 & -1 \end{bmatrix}.$$

Ces deux matrices engendrent donc un sous-groupe de SO(3) *isomorphe à* F_2.

Notons que les éléments π_1 et π_2 ci-dessus ont été bien choisis ! Par exemple, les éléments $\pi_1' = K\pi_1 = -I + J + K$ et $\pi_2' = K\pi_2 = -I - J - K$, bien qu'associés respectivement à π_1 et π_2, ne conviennent pas : pour $\pi = \pi_1'$ ou π_2' on a même $\pi^* = -\pi$ et donc $f(\pi)^2 = 1$. Donnons un second exemple.

EXEMPLE 10.27. *Pour $p = 5$, les éléments $\pi_1 = 1+2I$, $\pi_2 = 1+2J$ et $\pi_3 = 1+2K$ vérifient l'hypothèse du Lemme 10.25. On en déduit que les* 3 *rotations*

$$f(\pi_1) = \frac{1}{5}\begin{bmatrix} 5 & 0 & 0 \\ 0 & -3 & -4 \\ 0 & 4 & -3 \end{bmatrix},\ f(\pi_2) = \frac{1}{5}\begin{bmatrix} -3 & 0 & 4 \\ 0 & 5 & 0 \\ -4 & 0 & -3 \end{bmatrix} \text{ et } f(\pi_3) = \frac{1}{5}\begin{bmatrix} -3 & -4 & 0 \\ 4 & -3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

engendrent un sous-groupe de SO(3) *isomorphe à* F_3. *Autrement dit, on a montré que « trois rotations de $\mathbb{R}^3$ d'axes deux à deux orthogonaux et d'angles* $\arccos(-3/5)$ *engendrent un groupe libre isomorphe à* F_3 *».*

Terminons enfin la démonstration du Théorème 10.24.

DÉMONSTRATION — (du Théorème 10.24). Soit p un nombre premier avec $p \equiv 1 \bmod 4$. Soit Π l'ensemble des éléments de norme p de $\mathrm{H}_\mathbb{Z}$ dont le coefficient en 1 dans la base $1, I, J, K$ est impair et > 0. Observons que Π est un système de représentants des éléments de norme p de $\mathrm{H}_\mathbb{Z}$ pour $\sim$. En effet, si on a $(x_i) \in \mathbb{Z}^4$ avec $p = x_1^2+x_2^2+x_3^2+x_4^2$ on constate par réduction modulo 4 que un, et un seul, des x_i est impair. Ainsi, tout $\pi \in \mathrm{H}_\mathbb{Z}$ de norme p a un unique associé dans Π.

L'involution $\pi \mapsto \pi^\star$ préserve Π. Elle est sans point fixe, car si on a $\pi = \pi^\star$ alors π est dans $\mathbb{Z}$ puis $p = \mathrm{n}(\pi)$ est un carré : absude. Ainsi, si n est un entier $\leqslant \frac{p+1}{2}$, on peut trouver $\pi_1, \dots, \pi_n$ dans Π tels que les $2n$ éléments $\pi_1, \pi_1^*, \dots, \pi_n, \pi_n^*$ sont distincts et dans Π, donc deux à deux non associés. On conclut alors par le Lemme 10.25 et le classique Lemme 10.28 (il existe des premiers $\equiv 1 \bmod 4$ arbitrairement grands !). □

LEMME 10.28. *Il existe une infinité de nombres premiers $\equiv 1 \bmod 4$.*

DÉMONSTRATION — Supposons qu'il n'y en ait qu'un nombre fini $p_1, \dots, p_n$. Considérons l'entier $N = 4(p_1 p_2 \cdots p_n)^2 + 1$. Il est > 1 et donc admet un diviseur premier p. On a $(2p_1 \cdots p_n)^2 \equiv -1 \bmod p$. En particulier, p est impair, distinct des p_i, et -1 est un carré modulo p. Par Euler (Exemple 5.8 Chap. 2), on sait que cette dernière propriété entraîne $p \equiv 1 \bmod 4$: une contradiction. □

10. Soient $X = \{\pi_1, \pi_2, \pi_1^\star, \pi_2^\star\}$ et $Y := X \cup -X$. L'ensemble Y a 8 éléments et coïncide avec $\{\pm 1 \pm I \pm J\}$. Pour $\xi \in \mathrm{H}_\mathbb{Z}^\times$ on constate $\xi Y \cap Y \neq \varnothing \iff \xi = \pm 1$. On conclut car $X \cap -X = \varnothing$.