Université de Genève
Section de Mathématiques

Algèbre I
Session de printemps 2009
Série 1, corrigé

Ex.1

Soit $k = qn + r$, avec $q \in \mathbb{N}$ et $r \in [\![0, n-1]\!]$, la division euclidienne de k par n. Par minimalité de n, on a alors $1 = g^k = g^{qn+r} = (g^n)^q.g^r = 1^q.g^r = g^r$ si et seulement si $r = 0$.

Autrement dit, $g^k = 1$ si et seulement si n divise k.

Ex.2

a) En listant tous les éléments de Sym_4, on constate rapidement que seuls les transpositions et les produits de transpositions à supports disjoints sont d'ordre 2.

b) Plus généralement, dans Sym_n pour tout $n \in \mathbb{N}^*$, seuls les produits de transpositions à supports disjoints sont d'ordre 2. C'est une conséquence directe de l'exercice 3.b. Ce résultat peut néanmoins être démontré indépendemment en faisant une récurrence sur n[1].

Rappel

Pour tout $n \in \mathbb{N}^*$, le groupe symétrique Sym_n s'injecte naturellement dans Sym_{n+1} en rajoutant $n+1$ comme point fixe. Réciproquement, tout élément de Sym_{n+1} fixant $n+1$ peut être vu comme une permutation des n premiers entiers, donc comme un élément de Sym_n.

Ex.3

a) Montrons l'existence d'une telle décomposition par récurrence sur $n \in \mathbb{N}^*$.
   * C'est trivialement vrai pour n=1.
   * Supposons le résultat vrai au rang n et considérons une permutation $\sigma \in \mathrm{Sym}_{n+1}$. On note c le cycle $\big(n+1, \sigma(n+1), \dots, \sigma^k(n+1)\big)$ avec $\sigma^{k+1}(n+1) = n+1$ et $\sigma^s(n+1) \neq n+1$ pour tout $1 \leq s \leq k$. Si $k = 0$, alors $c = \mathrm{Id}$. La permutation $\sigma' = c^{-1}.\sigma$ fixe alors $n+1$ et tous ses itérés par σ. On peut notamment voir σ' comme un élément de Sym_n. Par hypothèse de récurrence, elle s'écrit de manière unique, à l'ordre des facteurs près, comme produit $c_1.\cdots.c_r$ de cycles à supports disjoints. De plus, aucun de ces supports ne contient l'un des $\sigma^i(n+1)$ car celui-ci ne serait alors pas laissé fixe par σ'. On a donc $\sigma = c.c_1.\cdots.c_r$ produit de cycles à supports disjoints.

   Pour l'unicité, on remarque qu'un entier apparaissant dans l'un des cycles, notons ce cycle c, est laissé invariant par tous les autres cycles puisqu'il n'apparait pas dans leurs supports. L'image de cet entier par c correspond donc à son image par σ. Chacun des cycle est donc entièrement déterminé par σ et par n'importe lequel de ses éléments.

b) Soit $\sigma = c_1.\cdots.c_s$ une permutation d'ordre n, décomposée en cycles disjoints. Pour tout $i \in [\![1, s]\!]$, on note k_i l'ordre de c_i et k le ppcm de tous les k_i. Enfin, on note

[1]voir TD

$n = qk + r$ la division euclidienne de n par q. Puisque tous les c_i sont à supports disjoints, ils commutent entre eux et on a

$$\sigma^n = c_1^{qk+r}.\cdots.c_s^{qk+r} = c_1^{q_1k_1}.c_1^r.\cdots.c_s^{q_sk_s}.c_s^r$$

avec $q_i \in \mathbb{N}$ pour tout $i \in [\![1,s]\!]$ puisque qk est un multiple de k, donc de k_i. On obient donc $\mathrm{Id} = \sigma^n = c_1^r.\cdots.c_s^r$. Par unicité de la décomposition en cycles disjoints, on a $c_i^r = \mathrm{Id}$ *i.e.* r multiple de k_i pour tout $i \in [\![1,s]\!]$. L'entier r est donc un multiple de k. Mais puisque $|r| < k$, on obtient que $r = 0$, autrement dit que n est un multiple non nul de k, ce qui implique que $n \geq k$. Or il est clair que $\sigma^k = c_1^k.\cdots.c_s^k = \mathrm{Id}$. Par minimalité de n dans $\mathbb{N}^*$, on a $n = k$.

Ex.4

Commençons par remarquer que, pour tout élément x de l'anneau, on a $0 = (1-1)x = x + (-1)x$ et $0 = (-1+1)x = (-1)x + x$. On en déduit donc que $(-1)x = -x$, l'inverse de x pour l'addition.

Il s'agit maintenant de montrer $a + b = b + a$ pour tout a et b éléments de l'anneau, ce qui est équivalent à $a + b - a - b = 0$. Or, en factorisant et grâce à l'existence de l'élément unité, on a

$$a + b - a - b = 1.(a+b) + (-1).(a+b) = (1-1).(a+b) = 0.(a+b) = 0.$$

Ex.5

Soit e un élément idempotent d'un anneau intègre. On a alors $e^2 = e$ ou encore $e^2 - e = e(e-1) = 0$. Or, puisque l'anneau est intègre, cela implique que $e = 0$ ou que $e = 1$.

Réciproquement, il est clair que 0 et 1 sont toujours des éléments idempotents.

Ex.6

Soit f un élément inversible de $C[0,1]$. Il existe donc une fonction g continue sur $[0,1]$ telle que $f(x)g(x) = 1$ pour tout $x \in [0,1]$. Cela implique que f ne s'annule jamais.

Réciproquement, si une fonction f ne s'annule jamais sur $[0,1]$, alors on peut définir $g \in C[0,1]$ $g(x) = {}^1\!/_{f(x)}$. Cette fonction est bien définie, elle est continue sur $[0,1]$ et satisait clairement $f.g \equiv 1$.

En conclusion, les éléments inversibles de $C[0,1]$ sont exactement les fonctions qui ne s'annulent jamais.