UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Éléments de correction pour l'examen partiel du lundi 25 mars 2013

Exercice 3

1 Si $c \in \mathfrak{S}_n$ est un cycle, son support est $\{d \in \{1,\dots,n\},\ c(d) \neq d\}$

2 C'est faux, par exemple $(1,2,3,4)^2 = (1,3)(2,4)$ n'est pas un cycle.

3 Notons S_1 (respectivement S_2) le support de c_1 (respectivement c_2) et $\sigma = c_1c_2$.

Pour $d \in S_1$, on a $d \notin S_2$, soit $\sigma(d) = c_1(c_2(d)) = c_1(d)$ On en déduit par une récurrence facile qu'on a, pour tout entier k, $c_1^k(d) = \sigma^k(d)$.

Comme c_1 et c_2 sont à supports disjoints, c_1 et c_2 commutent. On en déduit, en échangeant les indices 1 et 2, qu'on a également, pour tout entier $d \in S_2$ et tout entier k, $c_2^k(d) = \sigma^k(d)$.

Soit N l'ordre de σ. On a en particulier $\sigma^N = \mathrm{Id}$. Ainsi pour tout $d \in S_1$, on a $c_1^N(d) = \sigma^N(d) = d$. Mais par ailleurs pour tout $d \notin S_1$, on a $c_1(d) = d$, donc $c_1^N(d) = d$. Finalement $c_1^N = \mathrm{Id}$, donc r_1, qui est l'ordre de c_1, divise N. En échangeant les indices 1 et 2, on en déduit que r_2 divise également N. Donc au final $\mathrm{ppcm}(r_1,r_2)$ divise N.

Montrons à présent que $\sigma^{\mathrm{ppcm}(r_1,r_2)} = \mathrm{Id}$, ce qui permettra de conclure que N divise $\mathrm{ppcm}(r_1,r_2)$, donc au final que $N = \mathrm{ppcm}(r_1,r_2)$.

Comme c_1 et c_2 commutent, on a $\sigma^{\mathrm{ppcm}(r_1,r_2)} = c_1^{\mathrm{ppcm}(r_1,r_2)}c_2^{\mathrm{ppcm}(r_1,r_2)}$. Comme r_1, l'ordre de c_1, divise $\mathrm{ppcm}(r_1,r_2)$, on a $c_1^{\mathrm{ppcm}(r_1,r_2)} = \mathrm{Id}$. De même $c_2^{\mathrm{ppcm}(r_1,r_2)} = \mathrm{Id}$, et finalement on a bien $\sigma^{\mathrm{ppcm}(r_1,r_2)} = \mathrm{Id}$.

Exercice 4

Si $\sigma = \mathrm{Id}$, on a bien $\sigma(n) = n$.

Si σ_1 et σ_2 sont deux éléments de G, on a

$$(\sigma_1\sigma_2)(n) = \sigma_1(\sigma_2(n)) = \sigma_1(n) = n$$

donc $\sigma_1\sigma_2 \in G$.

Par ailleurs, comme $\sigma_1(n) = n$, on a $(\sigma_1^{-1}\sigma_1)(n) = \sigma_1^{-1}(n)$ soit $\sigma_1^{-1}(n) = n$ donc $\sigma_1^{-1} \in G$.

Ainsi G est bien un sous-groupe de $\mathfrak{S}_n$.

Montrons que G est isomorphe à $\mathfrak{S}_{n-1}$. On considère l'application $\varphi : \mathfrak{S}_{n-1} \to \mathfrak{S}_n$ qui à $\sigma \in \mathfrak{S}_{n-1}$ associe $\varphi(\sigma) \in \mathfrak{S}_n$ défini comme suit : pour $d \in \{1,\dots,n-1\}$, on pose $\varphi(\sigma)(d) = \sigma(d)$; par ailleurs on pose $\varphi(\sigma)(n) = n$.

Il faut alors montrer que $\varphi(\sigma)$ est bien un élément de $\mathfrak{S}_n$ (c'est-à-dire $\varphi(\sigma)$) est bien bijectif), puis que φ est un morphisme injectif de groupes d'image G. Ceci met en jeu des vérifications un peu fastidieuses mais dont aucune n'est réllement difficile.

À titre d'exemple, voici comment on peut démontrer que φ est injectif : si on a déjà montré que φ est un morphisme, il suffit de montrer que le noyau de φ est égal à $\{\mathrm{Id}_{\{1,\dots,n\}}\}$, et comme ce noyau contient nécessairement $\{\mathrm{Id}_{\{1,\dots,n\}}\}$, il suffit de montrer que si $\varphi(\sigma) = \mathrm{Id}_{\{1,\dots,n\}}$ alors $\sigma = \mathrm{Id}_{\{1,\dots,n\}}$. Mais si $\varphi(\sigma) = \mathrm{Id}_{\{1,\dots,n\}}$, on a, pour tout $d \in \{1,\dots,n-1\}$, $\sigma(d) = \varphi(\sigma)(d) = d$, donc $\sigma = \mathrm{Id}_{\{1,\dots,n\}}$.

Exercice 6

1 Par unicité des coefficients d'un polynôme, l'application

$$\begin{array}{rcl} k^n & \longrightarrow & k[X] \\ (a_0,\dots,a_{n-1}) & \longmapsto & X^n + \sum_{i=0}^{n-1} a_iX^i \end{array}$$

est une bijection de k^n sur l'ensemble des éléments de $k[X]$ de degré n et unitaires. Le cardinal de ce dernier ensemble est donc $\#k^n = q^n$.

2 Le polynôme $P = X(X^2+X+1) \in \mathbf{F}_2[X]$ est sans facteur carré. On peut donner un argument basé sur la décomposition en produit d'irréductibles (*cf.* ci-dessous) mais on peut aussi raisonner

directement : si Q est un polynôme non constant tel que Q^2 divise P, on a $0 < 2\deg(Q) \leqslant \deg(P)$ donc nécessairement $\deg(Q) = 1$, donc $Q \in \{X, X+1\}$, et on vérifie dans chacun des deux cas que Q^2 ne divise pas P.

L'existence et l'unicité du couple (Q, R) est claire si P est sans facteur carré (en particulier si P est constant non nul), car Q est nécessairement constant donc égal à 1. On a dans ce cas $(Q, R) = (1, P)$.

Soit à présent P unitaire qui possède un diviseur de la forme Q^2, avec Q unitaire non constant. Nécessairement $\deg(Q) \leqslant \frac{\deg(P)}{2}$. Considérons un diviseur unitaire de P de la forme Q_0^2 et de degré maximal. Soit $R_0 = P/Q_0^2$. Alors R_0 est sans facteur carré, car si R_0 est divisible par Q_1^2 où Q_1 est non constant, alors P est divisible par $Q_0^2 Q_1^2$ et comme Q_1 est non constant on a $\deg(Q_0^2 Q_1^2) > \deg(Q_0)^2$, contradiction.

Supposons à présent avoir deux écriture $P = Q_0^2 R_0 = Q_1^2 R_1$. Soit Π un facteur irréductible unitaire de Q_0. Alors Π^2 divise $Q_1^2 R_1$. En particulier, comme Π est irréductible, Π divise Q_1 ou R_1. Dans ce dernier cas, comme Π divise $Q_1^2 \frac{R_1}{\Pi}$, que Π est irréductible et que R_1 est sans facteur carré, Π divise Q_1^2 donc Q_1. Ainsi dans tous les cas Π divise Q_1 et donc Π^2 divise Q_1^2. On a donc l'égalité

$$\widetilde{P} \overset{\text{déf}}{=} \left(\frac{Q_0}{\Pi}\right)^2 R_0 = \left(\frac{Q_1}{\Pi}\right)^2 R_1$$

et $\deg(\widetilde{P}) = \deg(P) - 2\deg(\Pi) < \deg(P)$ ce qui permet de démontrer l'unicité par récurrence sur $\deg(P)$.

L'existence et l'unicité du couple (Q, R) peut aussi se voir grâce à l'existence et l'unicité de la décomposition en facteurs irréductibles. Si on note $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $k[X]$, pour tout polynôme P unitaire il existe une unique famille $(\nu_\Pi) \in \mathbf{N}^{\mathscr{P}}$ telle que :

- seul un nombre fini de coefficients ν_Q est non nul ;
- $P = \prod_{\Pi \in \mathscr{P}} \Pi^{\nu_\Pi}$.

On montre alors que P est sans facteur carré si et seulement si pour tout Π on a $\nu_\Pi \leqslant 1$.

Un polynôme P de degré n unitaire a un facteur carré si et seulement s'il existe Q unitaire tel que $0 < 2\deg(Q) \leqslant n$ et R unitaire de degré $n - 2\deg(Q)$ sans facteur carré tel que $P = Q^2.R$. Par unicité de cette écriture, et en considérant tous les $\deg(Q)$ possibles, on aboutit à la formule suivante pour le nombre v_n de polynômes unitaires de degré n *avec* un facteur carré :

$$v_n = \sum_{2 \leqslant 2k \leqslant n} q^k . u_{n-2k}$$

Ceci permet d'établir le résultat demandé par récurrence (notez que $u_n = q^n - v_n$ et que $u_0 = 1$ et $u_1 = q$). On peut prendre pour hypothèse de récurrence $\mathscr{H}_n$, avec $n \geqslant 2$, l'énoncé : « pour tout entier m supérieur à 2 et inférieur à n, $u_n = q^m - q^{m-1}$ ».