Travaux dirigés n° 15

Correction de II.

1. *Il est possible de calquer la réponse sur la démonstration de la structure des sous-groupes de* $\mathbf{Z}$*, résultat qui du reste pourrait s'énoncer, puisque* $\mathbf{Z}$ *est le modèle de groupe monogène infini, ainsi : tout sous-groupe d'un groupe monogène infini, est monogène infini. Nous choisirons toutefois de recourir à un artifice qui déduit le résultat de la structure des sous-groupe de* $\mathbf{Z}$*, nous épargnant ainsi de refère, à peu de chose près, un travail bien connu.*

   L'abélianité de G (il est cyclique) nous permet d'user pour G d'une notation additive. Soit l'application
   $$\phi \ : \ \mathbf{Z} \to G \, ; \ k \mapsto k \cdot a,$$
   où a est un générateur de G. On a vu — et c'est du cours — que ϕ est un morphisme de groupes, surjectif. Prenons un sous-groupe H de G. Son image réciproque par le morphisme ϕ est un sous-groupe de $\mathbf{Z}$, il est donc de la forme $p\mathbf{Z}$, avec $p \in [\![1, n]\!]$. Mais la surjectivité de ϕ donne :
   $$H = \phi\Big(\phi^{-1}\left(H\right)\Big).$$
   Donc $H = \phi(p\mathbf{Z}) = \{(k \times p) \cdot a, k \in \mathbf{Z}\} = \{k \cdot (p \cdot a), k \in \mathbf{Z}\} = \langle p \cdot a \rangle$. Donc H est monogène, de cardinal fini par inclusion dans G, il est même cyclique.

   Complément. Démontrons la propriété utilisée dans cette preuve ; *si* f *est une surjection d'un ensemble* A *dans un ensemble* B*, alors pour toute partie* C *de* B *:*
   $$f(f^{-1}(C)) = C.$$
   Par définition de l'image réciproque $f(f^{-1}(C)) \subset C$. Soit maintenant, c est un élément de C, alors la surjectivité de f permet de choisir d un de ces antécédants par f et alors $c = f(d)$ et $d \in f^{-1}(C)$, donc $c \in f(f^{-1}(C))$. D'où $f(f^{-1}(C)) \supset C$. Conclusion $f(f^{-1}(C)) = C$.

2. Comme G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, il est loisible de prendre $\mathbf{Z}/n\mathbf{Z}$ pour G.

   • D'abord $\bar{q}$ engendre un groupe à d éléments.

   En effet, d'une part $d \cdot \bar{q} = \overline{dq} = \bar{n} = \bar{0}$ et donc $\omega(q)$ divise d. D'autre part par définition de l'ordre de q,
   $$\bar{0} = \omega(q)\bar{q} = \overline{\omega(q)q},$$
   donc n divise $\omega(q)q$ et donc d divise $\omega(q)$. La positivité de $\omega(q)$ et de d ne laisse que $\omega(q) = q$.

   • Soit H un sous groupe de $\mathbf{Z}/n\mathbf{Z}$ à d éléments. Par 1, H est cyclique, désignons par q' un de ses générateurs. Alors $\overline{dq'} = d \cdot \bar{q}' = \bar{0}$, donc n divise dq', et donc q divise q', donc finalement $H = \langle \bar{q}' \rangle \subset \langle \bar{q} \rangle$. Mais par égalité de leurs cardinaux les groupes H et $\langle \bar{q} \rangle$, sont égaux.

   Donc $\mathbf{Z}/n\mathbf{Z}$ admet comme seul groupe à d éléments le groupe engendré par $\bar{q}$.

3. Notons D_n, l'ensemble des diviseurs positifs de n et pour tout d élément de D_n, notons O_d l'ensemble des éléments de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d et H_d LE sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d.
On a :
$$\mathbf{Z}/n\mathbf{Z} = \biguplus_{d\in D_n} O_d \tag{1}$$
En effet tout élément a de $\mathbf{Z}/n\mathbf{Z}$ a comme ordre un diviseur de n et donc est élément d'un des O_d, $d \in D_n$ et, ne pouvant avoir qu'un ordre, n'est élément que d'un de ces ensembles.
Donc
$$n = |\mathbf{Z}/n\mathbf{Z}| = \sum_{d\in D_n} |O_d|. \tag{2}$$
Soit à présent $\delta \in D_n$. Tout élément de O_δ, engendre par définition même de O_δ un sous groupe de $\mathbf{Z}/n\mathbf{Z}$ de cardinal δ, qui, par la question 1, ne peut être que H_δ ; Réciproquement tout générateur de H_δ est d'ordre δ, donc élément de O_δ. Ainsi O_δ est l'ensemble des générateurs de H_d, donc $|O_\delta| = \varphi(\delta)$, puisque H_δ, qui est cyclique d'ordre δ, est isomorphe à $\mathbf{Z}/\delta\mathbf{Z}$.
Donc (16) devient :
$$n = \sum_{d\in D_n} \varphi(d).$$

4. Soit m un entier supérieur ou égal à 2. On appelle racines primitives m^{e} de l'unité les générateurs de $\mathcal{U}_m$, groupe des racines m^{e} de l'unité.
   (a) Le nombre h_m de racines primitives m^{e} de l'unité est $\varphi(m)$, puisque $\mathcal{U}_n$ est isomorphe à $\mathbf{Z}/m\mathbf{Z}$.
   (b) Le cours nous dit que $\varphi(p) = p - 1$, autrement dit tout élément distinct de 1 de $\mathcal{U}_p$ engendre ce groupe. Donc en faisant une courte excursion dans $\mathbf{C}(X)$,
   $$\phi_p = \prod_{\omega\in\mathcal{U}_p\setminus\{1\}} X - \omega = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + ... + X^{p-1}.$$
   (c) L'ordre de tout élément de $\mathcal{U}_n$ est élément de D_n, donc en notant pour tout $d \in d_n$, O_d, l'ensemble des éléments de $\mathcal{U}_n$ d'indice d, comme dans 3,
   $$\mathcal{U}_n = \biguplus_{d\in D_n} O_d$$
   Mais 1. nous apprend que pour tout $d \in D_n$ $\mathcal{U}_n$ admet un et un seul sous-groupe d'ordre d celui-ci est connu, c'est $\mathcal{U}_d$ (qui est bien un groupe d'ordre d inclus dans $\mathcal{U}_n$, et donc les éléments de O_d sont les générateurs de $\mathbf{Z}/d\mathbf{Z}$, autrement dit les racines primirives d^{e} de l'unité. Donc :
   $$X^n - 1 = \prod_{\omega\in\mathcal{U}_n} X - \omega = \prod_{d\in D_n} \left(\prod_{\omega\in O_d} (X - \omega) \right) = \prod_{d\in D_n} \phi_d$$
   (d) Notre réponse se fonde sur le résultat suivant
   Lemme : *Soit A un élément de $\mathbf{Z}[X]$ et B un élément de $\mathbf{Z}[X]$ unitaire. Alors le quotient et le reste dans la division euclidienne de A par B effectuée dans $\mathbf{Q}[X]$ sont éléments de $\mathbf{Z}[X]$* [1].

1. Plus généralement on a le résultat suivant guère plus difficile à montrer. Soit $\mathcal{A}$ un anneau commutatif. Soient A et B des élément de $\mathcal{A}[X]$. On suppose que B est non nul et que son coefficient dominant est un élément inversible de $\mathcal{A}$ Alors il existe un unique couple (Q, R) d'éléments de $\mathcal{A}[X]$ tel que $A = QB + R$ et $\mathrm{d}^{\mathrm{o}}(R) < \mathrm{d}^{\mathrm{o}}(B)$

Preuve du lemme : Soit B un polynôme unitaire, à coefficients entiers

Récurrons sur le degré de A

• Le cas où $\mathrm{d}^\circ(A) < \mathrm{d}^\circ(B)$ ne pose pas de problème : le quotient est nulle et le reste vaut A, les deux sont éléments de $\mathbf{Z}[X]$.

• Soit $d \in [\![\mathrm{d}^\circ(B) - 1, +\infty[\![$. Supposons le résultat acquis pour A de degré inférieur ou égal à d. Prenons alors $A \in \mathbf{Z}[X]$ de degré $d+1$. Notons $a_n X^n$ le monôme dominant de A. Ainsi $A - a_n B$ est un polynôme de degré inférieur ou égal à d et à coefficients entiers. Par division euclidienne et par l'hypothèse de récurrence il s'écrit : $A - a_n B = Q'B + R'$ avec (Q', R') dans $(\mathbf{Z}[X])^2$ et $\mathrm{d}^\circ(R') < \mathrm{d}^\circ(B)$, mais alors puisque

$$A = (Q' + a_n X^n)B + R'$$

le reste dans la division de A par B (dans $\mathbf{Q}[X]$) est R', le quotient $(Q' + a_n X^n)$, ils sont tous deux dans $\mathbf{Z}[X]$.

D'où le résultat pour A de degré $d+1$.

Par récurrence le lemme est vrai.

Par récurence sur n on montre alors sans mal que ϕ_n est à coefficients entiers. L'initialisation est sans malice. Supposons que ϕ_1, ϕ_2,..., ϕ_{n-1} soient éléments de $\mathbf{Z}[X]$, pour un entier $n \geq 2$. Alors par (c), ϕ_n est le quotient de $X^n - 1$ par le polynôme unitaire $\prod_{k \in D_n \setminus \{n\}} \phi_k$ qui est grâce à l'hypothèse de récurrence à coefficients entiers ($\mathbf{Z}$ est un anneau), donc, par le lemme, ϕ_n est à coefficients entiers.

Les polynômes cyclotomiques sont éléments de $\mathbf{Z}[X]$.