ALGEBRE-04/09

(documents interdits)

Soit p un nombre premier et $k = \mathbb{Z}/p\mathbb{Z}$. Soit G un groupe fini. Etant donné un anneau commutatif unitaire A on définit la A-algèbre AG comme le A-module libre de base $([g]; g \in G)$ muni de la multiplication telle que $[g] \cdot [h] = [gh]$ pour tous $g, h \in G$. On rappelle qu'un AG-module est une paire (V, ρ) où V est un A-module et $\rho : AG \to \mathrm{End}_A(V)$ un morphisme de A-algèbres. On dira que (V, ρ) est de type fini si V est un A-module finiment engendré. Un définit un sous-AG-module ou un morphisme de AG-modules de la façon usuelle.

I. Soit (V, ρ) un $\mathbb{Q}G$-module de type fini. On appelle réseau de (V, ρ) un sous-$\mathbb{Z}G$-module $(V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$ de type fini de (V, ρ) tel que V est engendré par $V_{\mathbb{Z}}$ comme $\mathbb{Q}$-espace vectoriel. Démontrer qu'il existe un réseau (on commence par construire un sous-$\mathbb{Z}$-module $V'_{\mathbb{Z}}$ de type fini de V qui engendre V comme $\mathbb{Q}$-espace vectoriel, puis on construit $(V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$ à partir de $V'_{\mathbb{Z}}$). Démontrer que $V_{\mathbb{Z}}$ est un $\mathbb{Z}$-module libre de rang $\dim_{\mathbb{Q}}(V)$ (= dimension du $\mathbb{Q}$-espace vectoriel V).

II. Soient (V, ρ), $(V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$ comme ci-dessus. On pose $V_k = k \otimes_{\mathbb{Z}} V_{\mathbb{Z}}$ et $\rho_k = \mathrm{id}_k \otimes \rho_{\mathbb{Z}}$. Démontrer que (V_k, ρ_k) est un kG-module. Démontrer que $AG \simeq A[X]/(X^2 - 1)$ si $G = \mathbb{Z}/2\mathbb{Z}$ (le groupe Abélien à deux éléments). Démontrer que la classe d'isomorphisme de (V_k, ρ_k) dépend du choix du réseau $(V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$ (donner un example avec, p.ex., $G = \mathbb{Z}/2\mathbb{Z}$ et $p = 2$).

III. Soit $Rep(AG)$ l'ensemble des classes d'isomorphismes de AG-modules. Si v est un AG-module on note $\bar{v}$ sa classe d'isomorphisme. On appelle groupe de Grothendieck de AG, et on note $K(AG)$, le quotient du groupe Abélien libre $\bigoplus_{\bar{v} \in \mathrm{Rep}(AG)} A\bar{v}$ par le sous-groupe Abélien engendré par les éléments $\bar{v} - \bar{v}' - \bar{v}''$ tels qu'il existe une suite exacte de AG-modules

$$0 \to v' \to v \to v'' \to 0.$$

On note $[v]$ la classe de $\bar{v}$ dans $K(AG)$. On veut démontrer que pour tout $\mathbb{Q}G$-module $v = (V, \rho)$ la classe $[v_k]$ de $v_k = (V_k, \rho_k)$ est indépendante du choix du réseau $(V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$. On se donne donc deux réseaux $v_{\mathbb{Z}} = (V_{\mathbb{Z}}, \rho_{\mathbb{Z}})$, $v'_{\mathbb{Z}} = (V'_{\mathbb{Z}}, \rho'_{\mathbb{Z}})$.

III.a. Supposons que $pV_{\mathbb{Z}} \subset V'_{\mathbb{Z}} \subset V_{\mathbb{Z}}$. On pose $T = V_{\mathbb{Z}}/V'_{\mathbb{Z}}$. Démontrer que T admet une structure de kG module qu'on notera t. Démontrer qu'on a une suite exacte de kG-modules

$$0 \to t \to v'_k \to v_k \to t \to 0.$$

En déduire que $[v_k] = [v'_k]$.

III.b. Démonter que $[v_k] = [v'_k]$ pour tout $v_{\mathbb{Z}}$, $v'_{\mathbb{Z}}$.

Exercice n° 1 On se propose de montrer que l'extension de corps $\mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{6})})/\mathbb{Q}$ est galoisienne avec pour groupe de Galois le groupe Q des quaternions (i.e., Q est le groupe ayant huit éléments $1, s_i, s_j, s_k, t, ts_i, ts_j, ts_k$, où t est central, $t^2 = 1$, et $s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t$).

(a) Posons $K = \mathbb{Q}(\sqrt{2}, \sqrt{6})$. Expliquer pourquoi l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois produit de deux groupes cycliques d'ordre 2. On notera $\sigma_i, \sigma_j, \sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$ les trois éléments non triviaux.

(b) Posons $\alpha = (2+\sqrt{2})(3+\sqrt{6})$. Montrer que $K = \mathbb{Q}(\alpha)$.

(c) Montrer que pour chaque $\sigma = \sigma_i, \sigma_j, \sigma_k$ la quantité $\sigma(\alpha)/\alpha$ est le carré d'un élément de K que l'on précisera.

(d) Soit $\delta = \sqrt{\alpha}$ et $L = \mathbb{Q}(\delta)$. Montrer que $\delta \notin K$ (on pourra utiliser la question précédente). Quel est le groupe de Galois de L/K ? On note τ son générateur, qu'on considérera également comme un élément de $\mathrm{Gal}(L/\mathbb{Q})$ (dont $\mathrm{Gal}(L/K)$ est un sous-groupe).

(e) Définir des automorphismes $\tilde{\sigma}_i$ et $\tilde{\sigma}_j$ de $L = K(\sqrt{\alpha})$ sur $\mathbb{Q}$ qui prolongent σ_i et σ_j respectivement. On posera $\tilde{\sigma}_k = \tilde{\sigma}_i \tilde{\sigma}_j$.

(f) Calculer la loi de groupe et conclure.

(g) Combien le corps $\mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{6})})$ possède-t-il de sous-corps quadratiques (de dimension 2 sur $\mathbb{Q}$) ?