M1 Algèbre 2

Mars 2011

DM n° 1 : éléments de correction

I

1. Notons que d'après Lagrange, pour tout entier $m \geq 1$, $\mathbb{C}^\times$ possède un unique sous-groupe de cardinal m, soit $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$.
Par thm, on sait que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, où $r \geq 1$, et pour tout i, $2 \leq d_i \mid d_{i+1}$ (ceci exclut le cas trivial où $|G|=1$).
Alors d_r est l'exposant de G, et nous allons montrer que $V := \{\chi(g) \mid g \in G, \chi \in \hat{G}\}$ est le sous-groupe $\mathbb{U}_{d_r}$ de $\mathbb{C}^\times$.
On peut bien sûr supposer que $G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_r\mathbb{Z}$. Par le cours, tout caractère $\chi \in \hat{G}$ s'écrit alors de manière unique comme le produit $(\chi^{(1)}_{j_1} \circ p_1) \cdots (\chi^{(r)}_{j_r} \circ p_r)$, où $\forall \ell \in \{1, \dots, r\}$, $p_\ell : G \to \mathbb{Z}/d_\ell\mathbb{Z}$ est le morphisme de projection sur le $\ell^{\text{ième}}$ facteur, et $\chi^{(\ell)}_{j_\ell} \in \widehat{\mathbb{Z}/d_\ell\mathbb{Z}}$, $0 \leq j_\ell \leq d_\ell - 1$. Par suite V est le produit dans $\mathbb{C}^\times$ des r ensembles $V_\ell := \{\chi(\bar{k}) \mid \bar{k} \in \mathbb{Z}/d_\ell\mathbb{Z}, \chi \in \widehat{\mathbb{Z}/d_\ell\mathbb{Z}}\}$. Or par le cours $\widehat{\mathbb{Z}/d_\ell\mathbb{Z}} = \langle \chi^{(\ell)}_1 \rangle$, avec $\chi^{(\ell)}_1 : \bar{k} \mapsto e^{2\pi i k/d_\ell}$, donc $V_\ell \subset \operatorname{Im} \chi^{(\ell)}_1$ qui est le sous-groupe $\mathbb{U}_{d_\ell}$ de $\mathbb{C}^\times$. Or pour tout $\ell \in \{1, \dots, r\}$, $d_\ell \mid d_r$, donc on a $\mathbb{U}_{d_\ell} \subset \mathbb{U}_{d_r}$, et par suite $\mathbb{U}_{d_1} \cdot \mathbb{U}_{d_2} \cdots \mathbb{U}_{d_r} \subset \mathbb{U}_{d_r}$; l'autre inclusion étant claire, on conclut que $V = \mathbb{U}_{d_r}$.
(en particulier, si G n'est pas cyclique et $|G| = n$, V n'est pas $\mathbb{U}_n$!)

2. a) Les seules racines de l'unité réelles sont 1 et -1, or tout $\chi \in \hat{G}$ prend ses valeurs dans les racines de l'unité (cours). Donc si $\chi \in \hat{G}$ et $\chi \neq 1$, alors $\operatorname{Im} \chi = \{1, -1\}$ (et $\operatorname{Ker} \chi$ est un sous-groupe de G d'indice 2). Le thm. de factorisation de χ donne alors : $2 = |\operatorname{Im} \chi| \mid |G|$.

Ainsi $|G|$ est pair. Supposons réciproquement que $|G|$ est pair. Donnons deux arguments possibles : Argument 1 : on utilise le thm de structure des groupes abéliens finis pour montrer que G possède un sous-groupe H d'indice 2 (il suffit de raisonner avec $G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ ($d_i | d_{i+1}\ \forall i$), et alors $H = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times (d_r/2)\mathbb{Z}/d_r\mathbb{Z}$ convient) ; on définit alors $\chi \in \hat{G}$ comme la composée de la surjection canonique $G \to G/H$ et de l'isom. $G/H \simeq \{-1,1\}$. ($\subset \mathbb{C}^*$)
le caractère χ de G est réel et non trivial ($\ker \chi = H$).

Argument 2 : par le cours, $|\hat{G}| = |G|$ est pair, donc (par Cauchy) $\hat{G}$ possède un caractère d'ordre 2. Or si $\chi \in \hat{G}$, ord(χ) est 2 ssi χ est réel non trivial (preuve : il s'agit de montrer que $\chi^2 = 1$ ssi $\mathrm{Im}\,\chi \subset \mathbb{R}$. Or $(\mathrm{Im}\,\chi \subset \mathbb{R})$ équivaut à $(\chi = \bar{\chi})$, c.a.d à $(\chi = \chi^{-1})$, d'où le résultat).

2b) est immédiat avec l'argument 2 ci-dessus, grâce au fait (supplémentaire) que les groupes G et $\hat{G}$ sont isomorphes (cours), donc possèdent le même nombre d'éléments d'ordre 2.
(NB : on pourrait aussi mettre en bijection {sous-groupes d'ordre 2 de G} et {sous-groupes d'indice 2 de $\hat{G}$}, via l'application $H \mapsto H^\perp$ où $H^\perp = \{\chi \in \hat{G} \mid \chi_{|H} = 1\}$, qui est bijective ... ; d'où le résultat 2b) puisque ces deux ensembles sont resp. en bijection avec {éléments d'ordre 2 dans G} et $\{\chi \in \hat{G}$ tq $\underbrace{\mathrm{Im}\,\chi = \{-1,1\}}_{\text{équivaut à } "|\mathrm{Im}\,\chi| = 2" \text{ par 2a)}}\}$.)
donc à $[G : \ker \chi] = 2$

3a) C est le sous-groupe de G image du morphisme $x \overset{c}{\mapsto} x^2$ (G abélien).
Or le noyau de c est l'ensemble des racines de $X^2 - 1 \in \mathbb{F}_p[X]$, soit $\{-\bar{1}, \bar{1}\}$ (car $\mathbb{F}_p$ corps, $-\bar{1} \neq \bar{1}$ car $p \geq 3$). Ainsi $|C| = \frac{|G|}{|\ker c|} = \frac{p-1}{2}$.

3b) Si $x \in G$, on a par Lagrange $f(x)^2 = x^{p-1} = 1$, donc (voir 3a.), $\mathrm{Im} f \subset \{-\bar{1}, \bar{1}\}$. Et aussi $f(x^2) = 1$, donc $C \subset \mathrm{Ker} f$. De plus $\mathrm{Ker} f$ est l'ensemble des racines de $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$, et $\mathbb{F}_p$ corps, donc $|\mathrm{Ker} f| \leq \frac{p-1}{2}$. En comparant avec 3a, on trouve $\underline{C = \mathrm{Ker} f}$ de cardinal $\frac{p-1}{2}$, et $|\mathrm{Im} f| = \frac{p-1}{(p-1)/2} = 2$, donc $\underline{\mathrm{Im} f = \{-\bar{1}, \bar{1}\}}$.

3c) Notons f_1 le morphisme $f : G \to \mathrm{Im} f = \{-\bar{1}, +\bar{1}\}$ (f_1 est surjectif). Notons aussi Θ l'isom. de groupes $\{-\bar{1}, +\bar{1}\} \to \{-1, 1\} \subset \mathbb{C}^\times$.
$(\subset \mathbb{F}_p^\times)$
On a alors (cf 3b) : $\chi = \Theta \circ f_1 : G \to \{-1, 1\}$, morphisme surjectif, donc. Ainsi $\chi \in \widehat{\mathbb{F}_p^\times}$. On a : $\chi(-\bar{1}) = \Theta(f(-\bar{1})) = \Theta((-\bar{1})^{p-1/2})$
$= (-1)^{p-1/2} = \begin{cases} 1 & \text{si } p \equiv 1 \ (4) \\ -1 & \text{si } p \equiv 3 \ (4). \end{cases}$

3.d) Par 3.c, χ est un caractère réel non trivial de $\mathbb{F}_p^\times$, donc χ est d'ordre 2 (cf 2a), argument 2) dans $\widehat{\mathbb{F}_p^\times}$. On applique 2b) et on conclut car $-\bar{1}$ est l'unique racine autre que $\bar{1}$ de $X^2 - \bar{1}$ dans $\mathbb{F}_p$, donc l'unique élément d'ordre 2 de $\widehat{\mathbb{F}_p}$.
NB : autre argument, en utilisant que $\underline{\mathbb{F}_p^\times \text{ est cyclique}}$ (thm vu en L3) : $\chi' \in \widehat{\mathbb{F}_p^\times}$ est d'ordre 2 ssi $\mathrm{Ker}\,\chi'$ est un sous-groupe d'indice 2 (donc d'ordre $\frac{p-1}{2}$) de $\mathbb{F}_p^\times$; or $\mathbb{F}_p^\times$ cyclique de cardinal $2 \times \left(\frac{p-1}{2}\right)$ admet un $\underline{\text{unique}}$ tel sous-groupe. Si $\mathbb{F}_p^\times = \langle \zeta \rangle$, alors ce sous-groupe est $\langle \zeta^2 \rangle$, aussi égal à C, $\underline{\text{et}}$ à $\mathrm{Ker} f$! Mais alors $\chi'_{|C} = 1$, et $\chi'_{|G \setminus C}$ ne prend pas la valeur 1, mais forcément -1, puisque $\chi'^2 = 1$. Ainsi on trouve que $\underline{\chi' = \chi}$.

II

Notons i_1 et i_2 (resp^t p_1 et p_2) les injections (resp^t projections)

$V \to V \oplus V$ (resp^t $V \oplus V \to V$) associées à la somme directe $V \oplus V$. Il s'agit de 4 morphismes de représentations. Pour ℓ, j dans $\{1,2\}$, et $f \in \mathrm{End}_G(V \oplus V)$, on pose alors : $f_{\ell j} = p_\ell \circ f \circ i_j$.

On a $f_{\ell,j} \in \mathrm{End}_G(V) = \mathbb{C}\, id_V$ par le lemme de Schur.

Il existe donc $A = (a_{\ell j}) \in M_2(\mathbb{C})$ telle que $f_{\ell,j} = a_{\ell,j}\, id_V$ $\forall \ell, j$.

On définit $\Psi : \mathrm{End}_G(V \oplus V) \to M_2(\mathbb{C})$. On va montrer que Ψ est

$$f \longmapsto A$$

un isom. de $\mathbb{C}$-algèbres. En effet si B est une base de V, et $\tilde{B} = ((B,0),(0,B))$ la base de $V \oplus V$ associée, alors $\mathrm{mat}_{\tilde{B}} f = \left[\begin{array}{c|c} a_{11} I_n & a_{12} I_n \\ \hline a_{21} I_n & a_{22} I_n \end{array}\right]$.

(où $n = \dim V$)

Il est donc aisé de vérifier que Ψ est $\mathbb{C}$ linéaire, et $\Psi(id_{V \oplus V}) = I_2$; on trouve aussi que Ψ est bijective (le lemme de Schur montre qu'on définit un G-endom. de $V \oplus V$ pour <u>tout</u> choix arbitraire des quatre scalaires $a_{\ell j}$, modulo le fait (vérification aisée) que $f \in \mathrm{End}_G(V \oplus V)$ <u>ssi</u> $\forall \ell, j \in \{1,2\}$, $f_{\ell j} (= p_\ell \circ f \circ i_j) \in \mathrm{End}_G(V)$)

$(f((v_1, v_2))$ est en effet $(p_1 \circ f \circ i_1(v_1) + p_1 \circ f \circ i_2(v_2),\ p_2 \circ f \circ i_1(v_1) + p_2 \circ f \circ i_2(v_2))$

Enfin si $\Psi(f') = A'$, où $f' \in \mathrm{End}_G(V \oplus V)$, on trouve que

$$\mathrm{mat}_{\tilde{B}}(f' \circ f) = \begin{bmatrix} (a'_{11} a_{11} + a'_{12} a_{21}) I_n & (a'_{11} a_{12} + a'_{12} a_{22}) I_n \\ (a'_{21} a_{11} + a'_{22} a_{21}) I_n & (a'_{21} a_{12} + a'_{22} a_{22}) I_n \end{bmatrix}$$

(produit par blocs)

, d'où il vient que $\Psi(f' \circ f) = A' . A = \Psi(f') . \Psi(f)$. D'où le résultat.