**Université Paris 7 - Denis Diderot** **Algèbre M1 – 2009-2010**

Examen de Mathématiques du 06/01/2010, corrigé succint

**A–**

1. (a) $\det(u,v,w) = -12$.
   (b) L'anneau $\mathbb{Z}$ étant principal, tout sous-module d'un $\mathbb{Z}$-module libre est libre, donc $M$ est libre. Le module $M$ est engendré par $u$, $v$, $w$ qui sont linéairement indépendants (déterminant non nul), $M$ est donc de rang 3.
   (c) Le rang de $M$ est égal au rang de $\mathbb{Z}^3$, donc le quotient $G$ est un module de torsion. Le groupe de torsion $G$ est de type fini, donc fini. Remarque : Le cardinal de $G = \mathbb{Z}^3/M$ est $|\det(u,v,w)| = 12$.
2. La matrice $A = \begin{pmatrix} 8 & 18 & 30 \\ 7 & 16 & 26 \\ 12 & 26 & 40 \end{pmatrix}$ représente l'inclusion du module libre $M$ dans $\mathbb{Z}^3$. La forme normale de Smith de $A$ est $S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$. La matrice $S$ représente l'inclusion de $M$ dans $\mathbb{Z}^3$ après changement des bases. Le groupe $G$ est isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/6$, donc les facteurs invariants sont 6 et 2.
3. Par le théorème chinois
$$G \simeq \mathbb{Z}/2 \times \mathbb{Z}/6 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \ .$$

**B–**

1. Le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$. Le corps $K$ est une extension quadratique de $\mathbb{Q}$ c'est à dire $[K : \mathbb{Q}] = 2$. Le groupe $\mathrm{Gal}(K : \mathbb{Q})$ a deux éléments : l'identité et l'involution $\sigma$ qui envoit $a + b\sqrt{2}$, $a$ et $b$ rationnels, sur $a - b\sqrt{2}$.
2. (a) Pour tout $z = a + b\sqrt{2} \in K$, $a$ et $b$ rationnels, on a : $N(a + b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}$.
   (b) Si $z \in K$ est un carré, alors $N(z) = N(u)^2$ est un carré dans $\mathbb{Q}$.
   (c) $N(4 + 2\sqrt{2}) = 8$ n'est pas un carré dans $\mathbb{Q}$, sinon 2 serait aussi est carré. D'après la question précédente $4 + 2\sqrt{2}$ n'est pas un carré dans $K$.
3. (a) Le polynôme minimal de $\alpha$ sur $K$ est $x^2 - (4 + 2\sqrt{2})$ : d'après ce qui précède il est irréductible. On a : $[L : K]$=2, et donc $[L : \mathbb{Q}] = 4$.
   (b) On a $(\alpha^2 - 4)^2 = 8$. Le polynôme $Q = X^4 - 8X^2 + 8$ annulle $\alpha$. Le degré du polynôme minimal de $\alpha$ est $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Le calcul de $\alpha^2$ montre que $K \subset \mathbb{Q}(\alpha)$, donc $\mathbb{Q}(\alpha) = K(\alpha) = L$ ; le degré est 4 et $Q = X^4 - 8X^2 + 8$ est le polynôme minimal.
   (c) $L$ contient $\alpha$ et $\sqrt{2}$, donc contient $\beta = \frac{2\sqrt{2}}{\alpha}$.
   (d) Les racines de $Q$ sont : $\pm\alpha$, et $\pm\beta$ qui sont dans $L$. Les racines : $\pm\beta$, avec $\beta = \sqrt{4 - 2\sqrt{2}} = \frac{2\sqrt{2}}{\alpha}$ sont dans $L$. Le corps $L$ est corps de décomposition sur $\mathbb{Q}$ du polynôme (séparable) $Q$ : l'extension $(L : \mathbb{Q})$ est galoisienne, en particulier elle est normale.
4. (a) D'après la question 3b, on a $\mathbb{Q}(\alpha) = L$.
   (b) L'extension $(L : \mathbb{Q})$ est primitive : $L = \mathbb{Q}(\alpha)$. Un automorphisme de Galois est déterminé par l'image de $\alpha$ qui est parmi les racines de $Q$. Le groupe $\mathrm{Gal}(L : \mathbb{Q})$ a quatre éléments correspondants aux quatre racines de $Q$. En particulier il existe un unique élément $h \in \mathrm{Gal}(L : \mathbb{Q})$ tel que : $h(\sqrt{4 + 2\sqrt{2}}) = \sqrt{4 - 2\sqrt{2}}$.
   (c) $h(\alpha^2) = \beta^2 = 4 - 2\sqrt{2}$, donc $h(\sqrt{2}) = -\sqrt{2}$ ; $h(\beta) = h(\frac{2\sqrt{2}}{\alpha}) = -\alpha$. L'ordre de $h$ divise 4. On a :
$$h^2(\alpha) = h(\beta) = \frac{2h(\sqrt{2})}{h(\alpha)} = -\alpha \ .$$
   L'automorphisme $h$ est d'ordre 4.
   (d) Le groupe $\mathrm{Gal}(L : \mathbb{Q})$ est cyclique. Il contient trois sous-groupes : le trivial, le sous-groupe engendré par $h^2$, et lui-même. Les sous-corps fixes correspondants sont $L$, $K$ et $\mathbb{Q}$. Le théorème de Galois montre que ce sont les seuls sous-corps.

**C–**

1. Le groupe additif $\mathbb{F}$ est produit de trois groupes cyclique d'ordre 3 ; les facteurs invariants sont $(3,3,3)$. Le groupe multiplicatif $\mathbb{F}^*$ est cyclique de cardinal 26.
2. Le groupe de Galois de $\mathbb{F}$ est cyclique, engendré par l'automorphisme de Frobenius qui est d'ordre 3.
3. (a) Le polynôme $X^{13}-1$ est séparable sur $\mathbb{F}_3$ car il n'a pas de racine commune avec son polynôme dérivé $X^{12}$. Le corps $\mathbb{F}$ est corps de décomposition d'un polynôme séparable, donc l'extension $(\mathbb{F}:\mathbb{F}_3)$ est normale et séparable ; elle est galoisienne.
   (b) Le groupe des racines 13-ièmes de 1 dans $\mathbb{K}$ est d'ordre 13 (il est formé des racines de $P$ qui est séparable et scindé sur $\mathbb{K}$). L'ordre est premier, donc tout élément autre que 1 engendre ; c'est le cas de $\alpha$. Le corps $\mathbb{F}_3(\alpha)$ est donc le corps de décomposition de $X^{13}-1$, c'est à dire $\mathbb{F}=\mathbb{F}_3(\alpha)$.
   (c) Un automorphisme de $\mathbb{K}$ est déterminé par l'image de $\alpha$. Notons $\psi$ l'automorphisme de Frobenius de $\mathbb{K}$. On a $\psi^k(\alpha)=\alpha^{3^k}$. L'ordre de $\psi$ est celui de 3 dans le groupe multiplicatif $(\mathbb{Z}/13)^\times$. On a $3^2=9$ et $3^3\equiv 1\ (13)$. L'ordre de $\psi$ est égal à 3. On a $[\mathbb{K}:\mathbb{F}_3]=3$. Le corps $\mathbb{K}$ contient 27 éléments ; il est isomorphe à $\mathbb{F}$.
   (d) Le polynôme minimal de $\alpha$ est de degré $[\mathbb{F}_3(\alpha):\mathbb{F}_3]=3$.
4. Le polynôme cyclotomique à coefficients réduits modulo 3 : $\overline{\phi}_{13}\in\mathbb{Z}/3[X]$ annule toutes les racines de $X^{13}-1$ distinctes de 1. Il n'est pas irréductible ; ce qui précède montre qu'il se décompose en quatre polynômes irréductibles de degré 3. ($P=(X^3+2X+2)(X^3+X^2+2)(X^3+X^2+X+2)(X^3+2X^2+2X+2)$.)
5. Le corps de rupture d'un polynôme irréductible de degré 3 sur $\mathbb{F}_3$ est isomorphe à $\mathbb{F}_{27}$. Donc tout polynôme irréductible de degré 3 divise $X^{26}-1=(X-1)(X+1)(X^{13}-1)(X^{13}+1)$. Le facteur $X^{13}+1=-P(-X)$ se décompose aussi en quatre polynômes irréductibles de degré 3. On obtient huit polynômes irréductibles de degré 3.

   Remarque : le nombre de générateurs de $\mathbb{F}^*$ est $27-3=24$. Sous l'action du groupe de Galois ces générateurs se regroupent en huit orbites de 3 éléments, qui correspondent aux huit polynômes irréductibles de degré 3.

**D–**

1. (a) Pour tout $x\in\mathbb{F}_p^*$, on a $(x^{\frac{p-1}{2}})^2=x^{p-1}=1$ (petit théorème de Fermat). Donc : $x^{\frac{p-1}{2}}=\pm 1$.
   (b) Si $x\in\mathbb{F}_p^*$ est un carré, $x=y^2$, alors : $x^{\frac{p-1}{2}}=y^{p-1}=1$. Soit $\alpha$ un générateur du groupe cyclique $\mathbb{F}_p^*$. Si $x=\alpha^k$ et $x^{\frac{p-1}{2}}=\alpha^{\frac{k(p-1)}{2}}=1$, alors $p-1$ divise $\frac{k(p-1)}{2}$, donc $k$ est pair et $x=(\alpha^{\frac{k}{2}})^2$ est un carré.
2. Notons $x_i$, $0\le i\le 12$, les racines de $Q$ dans le corps de décomposition ; on a $\prod_i x_i=1$. Le discriminant de $Q$ est $D=(-1)^{\frac{r(r-1)}{2}}\mathrm{Res}(Q,Q')=(-1)^{\frac{r(r-1)}{2}}\prod_i Q'(x_i)$.
   On a $r$ impair, et $Q'=rX^{r-1}$, donc $D=(-1)^{\frac{r-1}{2}}r^r\prod_i x_i^{r-1}=(-1)^{\frac{r-1}{2}}r^r$.
3. On a :

$$D^{\frac{p-1}{2}}=(-1)^{\frac{(p-1)(r-1)}{4}}r^{\frac{r(p-1)}{2}}=(-1)^{\frac{(p-1)(r-1)}{4}}L(r,p)^r=\ (-1)^{\frac{(p-1)(r-1)}{4}}L(r,p)\ \ (r\text{ est impair}).$$

4. Soit $m$ l'ordre de $p$ dans $(\mathbb{Z}/r)^\times$ ; $m$ divise $r-1$ qui est l'ordre du groupe $(\mathbb{Z}/r)^\times$. Le polynôme $Q$ a $r-1$ racines primitives (générateurs du groupe des racines $r$-ièmes de 1) qui se répartissent en $\frac{r-1}{m}$ cycles. La permutation $\sigma$ est composée de $\frac{r-1}{m}$ cycles disjoints d'ordre $m$.
5. Ecrivons $r-1$ sous la forme $2^\nu q$, avec $q$ impair ($\nu\ge 1$) ; $L(p,r)$ est égal à $-1$ si et seulement si $2^\nu$ divise $m$, ce qui équivaut à $\frac{r-1}{m}$ impair. La signature de $\sigma$ est égale à $(-1)^{(m-1)\frac{r-1}{m}}=\epsilon_\sigma$. Dans le cas $L(p,r)=1$, $\frac{r-1}{m}$ est pair et $\epsilon_\sigma=1$. Dans le cas $L(p,r)=-1$, $m-1$ et $\frac{r-1}{m}$ sont impairs et $\epsilon_\sigma=-1$. La signature de $\sigma$ est égale à $L(p,r)$.
6. Démontrons la *loi de réciprocité quadratique*. Le discriminant $\overline{D}\in\mathbb{F}_p$ du polynôme $\overline{Q}\in\mathbb{F}_p[X]$ est un carré si et seulement si $L(D,p)=1$. D'autre part, ce discriminant est un carré si et seulement si le groupe de Galois ne définit que des permutations de signature 1. Ici le groupe de Galois est engendré par l'automorphisme de Frobenius. D'après la question précédente on a $L(p,r)=L(D,p)$ ; avec la question 3 :

$$L(p,r)=(-1)^{\frac{(p-1)(r-1)}{4}}L(r,p)\ .$$