L3 Mathématiques, Structures algébriques

Epreuve du 21 Janvier 2009

1. Cours Donner la définition d'un anneau principal. Donner la définition d'un élément irréductible.
Démontrer que si A est un anneau principal et si $a \in A$ est un élément (non-nul, non-inversible) les trois conditions suivantes sont équivalentes : l'élément a est irréductible, l'idéal (a) est premier, l'idéal (a) est maximal.

2. Montrer que le polynôme $P = X^2 + \bar{3}X + \bar{3}$ dans le corps $\mathbf{F}_5$ est irréductible.
Puisque c'est un polynôme de degré 2 il suffit de vérifier qu'il n'a pas de racines. Or $P(0) = 3$, $P(\bar{1}) = \bar{2}$, $P(\bar{2}) = \bar{3}$, $P(\bar{3}) = \bar{1}$, $P(\bar{4}) = \bar{1}$.
Quel est le nombre d'éléments de $k = \mathbf{F}_5[X]/(P)$?
C'est $|k|^{\deg(P)} = 5^2 = 25$.
Soit $\alpha = \bar{X} \in k = \mathbf{F}_5[X]/(P)$. Montrer que α est d'ordre 24 dans le groupe k^*.
Les ordres possibles sont les diviseurs de 24, or

- $\alpha^2 = 2\alpha + 2$,
- $\alpha^3 = \alpha + 4$,
- $\alpha^4 = \alpha + 2$,
- $\alpha^6 = 3$,
- $\alpha^8 = \alpha + 1$,
- $\alpha^{\mathbf{12}} = 4$**.**

Combien y a t'il d'éléments d'ordre 2, 3, 4, 6, 8, 12, 24 dans $\mathbf{Z}/24\mathbf{Z}$ (on rappelle que dans $\mathbf{Z}/n\mathbf{Z}$ l'ordre de $\bar{k}$ est $\frac{n}{pgcd(k,n)}$).
On trouve

- $\mathrm{ord}(\bar{k}) = 24$ est équivalent à $pgcd\big)(k, 24) = 1$. Donc k n'est pas divisible par 2 et 3. On trouve $\varphi(24) = 8$ éléments : $1, 5, 7, 11, 13, 17, 19, 23$.
- $\mathrm{ord}(\bar{k}) = 12$ est équivalent à $pgcd(k, 24) = 2$. Donc k n'est pas divisible par 3, et l'est par 2 mais pas par 4. On trouve 4 éléments : $2, , \ 10, 14, 22$.
- $\mathrm{ord}(\bar{k}) = 8$ est équivalent à $pgcd(k, 24) = 3$. Donc k n'est pas divisible par 2, et l'est par 3. On trouve 4 éléments : $3, 9, 15, 21$.
- $\mathrm{ord}(\bar{k}) = 6$ est équivalent à $pgcd(k, 24) = 4$. Donc k n'est pas divisible par 3, et l'est par 4 mais pas par 8. On trouve 2 éléments : $4, 20$.
- $\mathrm{ord}(\bar{k}) = 4$ est équivalent à $pgcd(k, 24) = 6$. Donc k est divisible par 3, et l'est par 2 mais pas par 4. On trouve 2 éléments : $6, 18$.

- $\text{ord}(\bar{k}) = 3$ est équivalent à $pgcd(k, 24) = 8$. Donc k n'est pas divisible par 3, et l'est par 8 . On trouve 2 éléments : $8, 16$.

- $\text{ord}(\bar{k}) = 2$ est équivalent à $pgcd(k, 24) = 12$. Donc On trouve 1 élément : 12.

Donner la liste des d'éléments d'ordre 2, 3, 4, 6, 8, 12, 24 dans k^* (cette dernière question est répétitive et un peu longue, on pourra donc se contenter de donner le nombre d'éléments d'ordre 2, 3, 4, 6, 8, 12, 24 et des exemples).
Puisqu'il y a un élément d'ordre 24 dans k^* ce groupe qui a 24 éléments est isomorphe à $\mathbf{Z}/24\mathbf{Z}$. Il y a donc autant d'éléments d'ordre 2, 3, etc que dans $\mathbf{Z}/24\mathbf{Z}$.
En particulier α est d'ordre 24, $\alpha^2 = 2\alpha + 2$ est d'ordre 12, $\alpha^3 = \alpha + 4$ d'ordre 8, ..., 4 d'ordre 2.

3. Donner la liste des polynômes irréductibles sur le corps $\mathbf{F}_2$ de degré inférieur ou égal à 2, 3 et 4.
En degré 2 et 3 ceux qui n'ont pas de racines, ce sont X^2+X+1, X^3+X+1, X^3+X^2+1 (on devait donner quelques précisions).
En degré 4 on a montré en cours qu'il fallait éliminer, outre les polynômes qui ont des racines, ceux qui sont le produit de deux polynômes irréductibles de degré 2. Ce qui revient à éliminer $(X^2 + X + 1)^2 = X^4 + X^2 + 1$.
La condition sur les racines pour $X^4 + aX^3 + bX^2 + cX + d$ s'écrit $d \neq 0$, donc $d = 1$, et $1 + a + b + c + 1 \neq 0$. il reste donc la condition $a + b + c \neq 0$. On trouve (éliminant $X^4 + X^2 + 1$) $X^4 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^3 + X^2 + X + 1$.
On pourra admettre dans la suite que le polynôme $P = X^4 + X^3 + 1$ est irréductible. Quel est le nombre d'éléments du corps $L = \mathbf{F}_2[X]/(X^4 + X^3 + 1)$. On notera comme il est d'usage α la classe $\bar{X}$, si bien que $\{1, \alpha, \alpha^2, \alpha^3\}$ est une base de L sur $\mathbf{F}_2$.
Calculer l'inverse de $\alpha + 1$ et celui de $\alpha^2 + 1$ dans cette base (on partira soit de P, soit on cherchera à résoudre un système linéaire approprié) et celui de $\alpha^2 + 1$ dans cette base.
Soit $\alpha^4 + \alpha^3 = 1$ donc $\alpha^3(\alpha + 1) = 1$, et $\alpha^6(\alpha^2 + 1) = 1$, $\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1$.

J'ai du mal à comprendre les calculs qui suivants (est-ce que tu veux dire que $\alpha^6 = a\alpha^3 + b\alpha^2 + c\alpha + d$ *et calculer* a, b, c *et* d*?) Mais je suis d'accord :* $\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1$. *A mon avis le mieux pour le trouver serait de faire une division de polynômes et de prendre le reste. Il y a donc des corrections à faire dans ce qui suit, mais je ne sais pas exactement lesquelles :*

Soit on résout le système linéaire $(\alpha^2 + 1)\big(\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1\big) = 1$, $a, b, c, d \in \mathbf{F}_2$, soit $c = 0$, $b + c = 0$, $a + b = 0$, $a + d = 1$.

Soit (utilisant Fermat) (ce n'est pas aussi agéable, et est juste donné pour mémoire) on note que $(1+\alpha)^{15} = 1$ et donc l'inverse est $(1+\alpha)^{14}$ qui est égal à $(1+\alpha)^8(1+\alpha)^4(1+\alpha)^2 = (1+\alpha^8)(1+\alpha^4)(1+\alpha^2)$ qui, comme $\alpha^4 = \alpha^3+1$, est encore égal à $(1+\alpha^8)(1+\alpha^4)(1+\alpha)^2 = \alpha^6\alpha^3(1+\alpha^2) = \alpha^9(1+\alpha)^2$. Mais $\alpha^9 = \alpha^8\alpha = (\alpha^6+1)\alpha = \alpha^7+\alpha$, on calcule $\alpha^7 = \alpha^2+\alpha+1$. Il suit que $\alpha^9 = \alpha^2 + 1$. Donc $\alpha^9(1 + \alpha)^2 = (1 + \alpha)^4 = 1 + \alpha^4 = \alpha^3$.
Quel est l'ordre de α dans L^*? Donner les éléments d'ordre 3, 5 et 15 dans L^*.
On a fait des calculs plus haut, les ordres possibles sont 3, 5 et 15, or α^3 est dans la base et $\alpha^5 = \alpha^3+\alpha+1$. Donc α est d'ordre 15. Comme plus haut on trouve les éléments de la forme

α^i, avec $pgcd(1,15) = 1$ d'ordre 15, il y en a $\varphi(15) = 8 : \alpha, \alpha^2, \alpha^4 = \alpha^3+1, \alpha^8 = \alpha+\alpha^2+\alpha^3$, et $\alpha^7 = 1+\alpha+\alpha^2$ (voir plus haut), $\alpha^{11} = 1+\alpha+\alpha^3$, $\alpha^{13} = \alpha+\alpha^2$, $\alpha^{14} = \alpha^2+\alpha^3$.
Egalement α^3, α^6, α^9, α^{12} sont d'ordre 5 (on laisse l'écriture dans la base à faire).
Trouver dans L une racine du polynôme $X^4+X^3+X^2+X+1$ (on pourra se servir de l'identité $(X+1)(X^4+X^3+X^2+X+1) = 1 = X^5+1$).
A cause de l'identité on voit que l'on cherche un élément d'ordre 5, α^3 convient.
Trouver dans L une racine du polynôme X^2+X+1. A cause de $(X+1)(X^2+X+1) = 1 = X^3+1$ on cherche un élément d'ordre 5, $\alpha^5 = 1+\alpha+\alpha^3$ convient.

4. On admet dans la suite que l'anneau $\mathbf{Z}[i]$ des entiers de Gauss est principal. Décomposer $x = 5+3i$ en produit d'éléments irréductibles. (N'était pasz dans l'épreuve)
On a $N(x) = 5^2+3^2 = 34 = 2\times 17$. D'où $x\bar{x} = (1+i)(1-i)(4+i)(4-i)$. Les éléments $1+i$, $1-i$, $4+i$ et $4-i$ sont irréductibles dans $\mathbf{Z}[i]$ car ils sont de la forme $a+ib$ avec a^2+b^2 premiers. Par unicité de la décomposition en irréductibles dans un anneau principal, on sait que x (ainsi que $\bar{x}$) est un produit de certains d'entre eux. On voit immédiatement que $5+3i = (1+i)(4-i)$ (ou bien que $5+3i = (1-i)(4+i)$ - ce qui donne la même réponse du fait que $(1+i)$ et $(1-i)$ sont associés).

5. Soit l'entier de Gauss $3+2i$. On cherche à montrer que $\mathbf{Z}[i]/(3+2i)$ est isomophe à $\mathbf{F}_{13}$. A cette fin, montrer que l'application ϕ de $\mathbf{Z}[i]$ dans $\mathbf{F}_{13}$, donnée par $a+ib \mapsto \overline{a+5b}$ est un homomorphisme d'anneaux, dans la formule $\overline{a+5b}$ désigne la classe de congruence modulo 13 de $a+5b$. On vérifiera en particulier que $\phi(xx') = \phi(x)\phi(x')$.
Pour cette dernière formule il faut montrer que si on a $x = a+ib$ et $x' = a'+ib'$, alors

$$aa' - bb' + 5(ab'+a'b) \cong (a+5b)(a'+5b') \mod 13$$

soit $-bb' \cong 25bb' \mod 13$.
Montrer qu'elle est surjective sur $\mathbf{F}_{13}$.
Il suffit de prendre la classe de $a \in \mathbf{Z}$.
Montrer que $3+2i$ est dans son noyau,
$3+2\times 5 = 13$
puis que ce noyau est l'idéal $(3+2i)$ (on pourra se servir du fait que $3+2i$ est irréductible, en le justifiant).
Un élément $a+ib$ de $\mathbf{Z}[i]$ tel que a^2+b^2 est premier (dans $\mathbf{Z}$!) est irréductible. Le noyau de ϕ contient l'idéal maximal $(3+2i)$ (citer le cours, voir 1!) , n'est pas égal à $\mathbf{Z}[i]$ et est égal à $(3+2i)$.
En déduire que que $\mathbf{Z}[i]/(3+2i)$ est isomorphe à $\mathbf{F}_{13}$.
Théorème d'isomorphisme.