Université Paris 7 - Denis Diderot **Algèbre M1**

Examen partiel, Lundi 15 novembre 2010

Corrigé succint

A–

1. Il y a quatre polynômes de degré 2 sur $\mathbb{F}_2$: X^2+aX+b, $a\in\mathbb{F}_2$, $b\in\mathbb{F}_2$. Seul X^2+X+1 n'a pas de racine et donc est irréductible.
2. Dans $\mathbb{F}_2[X]$, $X^5+1=(X+1)(X^4+X^3+X^2+X+1)$. Le polynôme $X^4+X^3+X^2+X+1$ n'a pas de racine et n'est pas divisible par X^2+X+1. Il n'a donc pas de facteur irréductible de degré 1, ni de degré 2 : il est irréductible. Dans $\mathbb{F}_2[X]$, $X^5+X+1=(X^2+X+1)(X^3+X^2+1)$. Le polynôme X^3+X^2+1, de degré 3, n'a pas de racine : il est irréductible.
3. La réduction modulo 2 du polynôme $X^5-82X+43$ est X^5+1. D'après la question précédente, une réduction sur $\mathbb{Z}$ aurait un facteur de degré 1. Par arithmétique élémentaire, 43 étant premier, les seules possibilités seraient $\pm X\pm 43$. Il n'y a donc pas de réduction sur $\mathbb{Z}$. Le polynôme est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.
4. Si le polynôme X^5+X-1 avait une racine dans $\mathbb{Q}$, il aurait sur $\mathbb{Z}$ un facteur de degré 1. Les seules possibilités seraient $\pm X\pm 1$. On a $X^5+X-1=(X^2-X+1)(X^3+X^2-1)$. (On peut remarquer que $-e^{\frac{i2\pi}{3}}$ est racine.)

B–

1. L'anneau $\mathbb{Z}[i]/(i+1)$ est de caractéristique 2 : $(2=(1+i)(1-i)$. C'est un corps car $1+i$, de norme l'entier premier 2, est irréductible dans l'anneau $\mathbb{Z}[i]$. Notons que $a+bi$ s'identifie à $a+b$ mod 2 dans le quotient. Le corps $\mathbb{Z}[i]/(i+1)\approx\mathbb{Z}/2$ a deux éléments.
2. (a) Le noyau du morphisme d'anneau $\mathbb{Z}\to\mathbb{Z}[i]/(q)$ est engendré par q qui est la caractéristique de l'anneau $\mathbb{Z}[i]/(q)$.
   (b) On a des isomorphismes $\mathbb{Z}[X]/(X^2+1,q)\approx\mathbb{Z}[i]/(q)$ et $\mathbb{Z}[X]/(X^2+1,q)\approx\mathbb{F}_q[X]/(X^2+1)$. L'anneau $\mathbb{Z}[i]/(q)\approx\mathbb{F}_q[X]/(X^2+1)$ compte q^2 éléments.
   (c) L'anneau $\mathbb{Z}[i]/(q)$ est un corps si et seulement si X^2+1 est irréductible sur $\mathbb{F}_q$, c'est à dire si et seulement -1 n'est pas un carré modulo q. Les carrés dans le groupe multiplicatif $\mathbb{F}_q$ sont les éléments dont l'ordre divise $\frac{q-1}{2}$. La condition requise est $(-1)^{\frac{q-1}{2}}\equiv -1$ mod. q, soit $q\equiv 3$ mod. 4.
   (d) Si X^2+1 n'est pas irréductible, il y a une réduction $X^2+1=(X-\alpha)(X-\beta)$. Par le théorème chinois, $\mathbb{F}_q[X]/(X^2+1)$ est alors isomorphe $\mathbb{F}_q[X]/(X-\alpha)\times\mathbb{F}_q[X]/(X-\beta)\approx\mathbb{F}_q^2$. L'anneau $\mathbb{Z}[i]/(q)$ est isomorphe à $\mathbb{F}_q^2$ pour q impair congru à 1 modulo 4, et pour $q=2$.

C–

1. On calcule le déterminant de la mutiplication par $(Y-X)^2-2$ modulo X^3-7.

$$\mathrm{Res}_X(X^3-7,(Y-X)^2-2)=(-1)^{2\times 3}\begin{vmatrix} Y^2-2 & 7 & -14Y \\ -2Y & Y^2-2 & 7 \\ 1 & -2Y & Y^2-2 \end{vmatrix}$$

$$\mathrm{Res}_X(X^3-7,(Y-X)^2-2)=Y^6-6Y^4-14Y^3+12Y^2-84Y+41\ .$$

2. Pour $Y = \sqrt{2} + \sqrt[3]{7}$ les polynômes $X^3 - 7$ et $(Y - X)^2 - 2$ ont $\sqrt[3]{7}$ comme racine commune, d'où l'annulation du résultant.
3. Pour α et β dans $\mathcal{O}$, on a des polynômes unitaires P et Q à coefficients entiers de racines respectives α et β. On utilise l'argument précédent : Soit $R = \mathrm{Res}_X(P, Q(Y - X))$. A un éventuel changement de signe près, le polynôme R est unitaire : si on calcule comme précédemment, le monôme dominant sort du produit des termes diagonaux. Il s'annulle pour $Y = \alpha + \beta$ (racine commune α). Soit $T = \mathrm{Res}_X(P, X^{\deg(Q)}Q(Y/X))$. Pour la même raison que pour R, le polynôme T est unitaire et s'annulle pour $Y = \alpha\beta$ (racine commune α). L'ensemble $\mathcal{O}$ est stable par somme et produit : c'est un sous-anneau.

D–

1. L'anneau $\mathbb{Z}[X]/(X - 2)$ est isomorphe à $\mathbb{Z}$. L'anneau $\mathbb{Z}[X]/(2X - 1)$ est isomorphe à $\mathbb{Z}[\frac{1}{2}] = S^{-1}\mathbb{Z}$, avec $S = 2^n,\ n \geq 0$.
2. Soit $s = \sum_{n \geq n_0} a_n X^n$ une série formelle à coefficients entiers, et $\overline{s}$ sa classe dans $\mathbb{Z}_2$. Si le premier coefficient est pair : $a_{n_0} = 2k$, alors $\overline{s}$ est représenté par $(k + a_{m+1})X^{m+1} + \sum_{n \geq n_0+2} a_n X^n$. En réitérant le procédé tant que le premier coefficient est pair, on obtient :
   soit que $\overline{s}$ a un représentant de la forme $X^m + \sum_{n>m} b_n X^n$;
   soit que le procédé se prolonge indéfiniment et dans ce cas $X - 2$ divise s, i.e. $\overline{s}$ est nul.
   Notons que dans le premier cas $\overline{s}$ n'est pas nul. Une série divisible par $X - 2$ a nécessairement son premier coefficient pair.
   On déduit que le produit de deux éléments non nuls de $\mathbb{Z}_2$ est non nul :
   $$\overline{(X^m + \sum_{n>m} b_n X^n)}\,\overline{(X^{m'} + \sum_{n>m'} c_n X^n)} = \overline{X^{m+m'} + \sum_{n>m+m'} d_n X^n}\ .$$
   L'anneau $\mathbb{Z}_2$ est intègre. Le noyau du morphisme $\mathbb{Z} \to \mathbb{Z}_2$ est trivial : aucun entier n'est divisible par $X - 2$. La caractéristique est nulle.
3. En reprenant le procédé précédent, on construit par récurrence des suites $a_k \in \{0, 1\}$, $b_k \in \mathbb{Z}$, $R_n \in \mathbb{Z}[X]$ telle que :
   $$\forall n \quad s = \sum_k a_k X^k = \sum_{k \leq n} a_k X^k \quad + (X - 2) \sum_{k \leq n} b_k X^k \ + \ X^{n+1} R_n$$
   On déduit : $s = \sum_k a_k X^k \quad + (X - 2) \sum_k b_k X^k$, ce qui donne le représentant demandé.
   Si $s = \sum_k a_k X^k$ et $s' = \sum_k a'_k X^k$, avec des coefficients a_k, a'_k dans $\{0, 1\}$, représentent les mêmes éléments de $\mathbb{Z}_2$, alors les $a'_k - a_k$ sont pairs, donc pour tout k on a $a_k = a'_k$.
4. Un entier impair est représenté dans $\mathbb{Z}_2$ par une série de premier terme 1 qui est inversible.
5. Les éléments de $\mathbb{Z}_2$ dont la représentation canonique précédente commence par $a_0 = 0$ forme un idéal dont le complément est formé d'inversibles : l'anneau est local.
6. Soit I un idéal non trivial de $\mathbb{Z}_2$, et soit k le plus petit entier pour lequel il existe un élément dans I dont la forme canonique commence avec X^k, alors I est engendré par X^k.
7. Le polynôme $2Y^2 - Y + 2$ n'a pas de racine dans $\mathbb{Q}$: il est irréductible sur $\mathbb{Q}$. Par contre il a une racine y dans $\mathbb{Z}_2$ et n'est donc pas irréductible sur $\mathbb{Q}_2$. On cherche y sous la forme canonique : $y = \sum_k a_k X^k$, avec les a_k dans $\{0, 1\}$. En posant $y_n = \sum_{k=0}^n a_k X^k = y_{n-1} + a_n X^n$, on obtient a_n par récurrence :
   $$a_n X^n \equiv 2y_{n-1}^2 - y_{n-1} + 2 \bmod (X - 2, X^{n+1})$$