Université d'Évry Val d'Essonne 2009-2010

M54 algèbre et arithmétique

Indications pour le partiel de 2009

Exercice 1.1 à 3. Cours.

4. L'idéal $(2, X)$ n'est pas principal : s'il était engendré par P, ce P diviserait 2 et $X\ldots$
5. Cours.
6. $\mathbf{Z}$.
7. Pas traité en cours cette année.
8. Les polynômes de degré 1, et ceux de degré 2 à discriminant strictement négatif.
9. Cet anneau est principal, donc les idéaux maximaux sont ceux engendrés par les éléments irréductibles, donnés à la question précédente.

Exercice 2. 1. $\mathbf{F}_2$ est un corps, et le cours dit que l'anneau des polynômes sur un corps est euclidien, donc principal.

2. Il est de degré 2 et n'a pas de racine.
3. Ce sont les $a + b\overline{X}$ avec a et b dans $\mathbf{F}_2$.
4. Fait en TD.
5. Polynôme de degré 2 : il est irréductible si et seulement si il n'a pas de racine.
6. Par la question précédente, P est irréductible, dans l'anneau principal $\mathbf{F}_p[X]$ il engendre donc un idéal maximal : le quotient est corps.
7. D'après la question précédente, on peut voir $\mathbf{F}_9$ comme $F_3[X]/(X^2+1)$.
8. Polynôme de degré 3 sans racine. $\mathbf{F}_8 = \{a + b\overline{X} + c\overline{X} \text{ avec } a, b, c \in \mathbf{F}_2\}$. Règles de calcul données par $\overline{X}^3 = \overline{X}^2 + 1$.

Exercice 3. 1. Voir feuille 5.

2. Fait en TD.
3. On résout $a^2 + b^2 = 2$ dans $\mathbf{Z}$, on trouve $(1, 1)$. Pour 3, il n'y a pas de solution.
4. Application directe de la définition.
5. En clair : montrer que x est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$. Puis calculer le nombre de solutions de $X^{\frac{p-1}{2}} = 1$. Voir feuille 1.
6. Voir feuille 1.
7. Erreur dans l'énoncé : il faut montrer que $\mathbf{Z}[X]/(p, X^2+1)$ est isomorphe à $\mathbf{Z}[i]/(p)$. On commence comme l'indication, il faut ensuite montrer que $\ker \phi = (p, X^2 + 1)$. Une inclusion est évidente. Pour l'autre on prend P dans le noyau, on fait sa division euclidienne par $X^2 + 1$ et on montre que le reste doit être nul modulo p.

8. À la question précédente, on peut voir que $\mathbf{F}_p[X]/(X^2+1) \equiv \mathbf{Z}[i]/(p)$. Si p est congru à 1 modulo 4, alors X^2+1 n'est pas irréductible sur $\mathbf{F}_p$, donc l'idéal qu'il engendre n'est pas maximal, et le quotient n'est pas un corps. Ainsi $\mathbf{Z}[i]/(p)$ non plus, donc (p) n'est pas maximal et p n'est pas irréductible (on est dans des anneaux principaux).
9. p est le produit de deux éléments de $\mathbf{Z}[i]$. Comme à l'exercice 6 de la feuille 5, on montre ce ces éléments sont forcément conjugués.
10. X^2+1 est de degré 2 et n'a pas de racine. L'idéal qu'il engendre est maximal ; le quotient est un corps, donc $\mathbf{Z}[i]/(p)$ aussi et p est irréductible dans $\mathbf{Z}[i]$.
11. Si z est irréductible, on l'écrit $z = xy$ avec x et y non inversibles. On $\phi(z) = \phi(x)\phi(y)$, et on aboutit à une contradiction.
12. $p \mid \phi(z) = z\bar{z}$. Comme p est irréductible dans $\mathbf{Z}[i]$, il divise soit z soit $\bar{z}$. Or, s'il divise $\bar{z}$ il divise aussi z. Donc p divise z, mais les deux sont irréductibles, l'un est donc un multiple de l'autre par un inversible (unicité de la décomposition en facteurs irréductibles).
13. Il existe q tel que $p = q\bar{q}$. Ainsi $q\bar{q}$ divise $z\bar{z}$, qui est le produit de deux irréductibles. On a donc $z = uq$ ou $z = u\bar{q}$ avec u inversible.
14. ...

Exercice 4.
1. On écrit $P = (X^2+2)Q + R$ la division euclidienne de P par X^2+2, avec R de degré 1. On voir que $P(i\sqrt{2}) = R(i\sqrt{2})$.
2. Voir exercice précédent.
3. Pas traité en cours cette année.
4. Ce sont les x tels que $\phi(x)$ est inversible dans $\mathbf{Z}$. On trouve seulement 1 et -1.
5. Oui, car son image par ϕ l'est dans $\mathbf{Z}$.
6. On trouve $c = 0$ et $d = \pm 1$. Irréductibilité : voir question précédente.
7. On a $2i\sqrt{2} = -(i\sqrt{2})^3$, décomposition en facteur premiers. Les diviseurs sont $\pm(i\sqrt{2})^\alpha$ avec α entre 0 et 3 ; ils sont irréductibles pour $\alpha = 1$.
8. Si l'un est pair, l'autre doit l'être aussi. S'ils étaient pairs, on aurait $4 \mid y^2$, donc $4 \nmid y^2+2$, or $8 \mid x^3$.
9. S'ils ont un facteur premier commun f, alors f divise leur différence $2i\sqrt{2}$, donc $f = \pm i\sqrt{2}$ par la question précédente. Mais alors $f^2 = \pm 2$ diviserait x^3, or x est impair.
10. Dans la décomposition de x est produit d'irréductibles dans $\mathbf{Z}[i\sqrt{2}]$, chaque facteur divise soit $y + i\sqrt{2}$ soit $y - i\sqrt{2}$. On choisit pour $a + ib\sqrt{2}$ le produit de ceux qui divisent $y + i\sqrt{2}$.
11. On a donc $y + i\sqrt{2} = (a + ib\sqrt{2})^3 = a(a^2 - 6b^2) + b(3a^2 - 2b^2)i\sqrt{2})$. Par identification, $1 = b(3a^2 - 2b^2)$. Ainsi, b est inversible dans $\mathbf{Z}$, donc $b = \pm 1$. On voit que seul $b = 1$ est possible, avec $a = \pm 1$. On trouve alors $y = \pm 5$ et $x = 3$.