Problème blanc
Agrégation interne 2015-2016

Partie I

1. Si $(a) \subset [b)$, a fortiori $a \in (b)$. Donc b divise a.

   Réciproquement, si b divise a, alors a est dans (b) ainsi que tous ses multiples.

   Il suffit maintenant de remarquer que si $a|b$ et $b|a$, alors il existe deux éléments u et v tels que $a = ub$ et $b = va$. On en déduit que $b = uvb$, ou encore $b(1 - uv) = 0$. L'anneau étant intègre, on en déduit que u et v sont des unités et que a et b sont associés.

   Réciproquement, si $a = ub$, où u est une unité, alors $b = u^{-1}a$. on en déduit que $a|b$ et que $b|a$.

2. a. $0 \in I$, il y a bien stabilité et présence de l'inverse : I est un sous-groupe de $(A, +)$.
      Soit $z = xa + yb$ un élément de I et $c \in A$. Alors $cz = cxa + xyb \in I$.
      I est un idéal de $(A, +, .)$.
      L'anneau est principal : cet idéal est monogène. On notera d un générateur.

   b. $a = 1a + 0b \in I$. de même pour b. Donc d est un diviseur commun à a et b.

   c. d est dans I : il existe $(u, v) \in A^2$ tel que $d = ua + vb$.
      On en déduit que si c divise a et b, alors c divise d.

3. a. Si a et b sont premiers entre eux, la question I.2.c prouve l'existence de u et v dans A tels que $1 = ua + vb$.
      Réciproquement, s'il existe (u, v) dans A^2 tel que $1 = ua + vb$, alors $1 \in I$ et $d|1$. d est une unité, et a et b sont premiers entre eux.

   b. De $1 = ua + vb$, on titre que $c = cua + vbc$.
      Or il existe $w \in A$ tel que $bc = aw$. On en déduit que $c = a(uc + vw)$.

4. On notera a_i un générateur de I_i.

   I est un sous-groupe de $(A, +)$.

   Il est non vide, puisque 0 est dans I_0.

   Soit x et y deux élements de I. Alors il existe n et p deux entiers naturels tels que $x \in I_n$ et y dasn I_p. Soit $q = max(n, p)$, alors x et y sont dans I_q qui est un idéal. $x + y$, $-x$ et $-y$ sont donc dans I.

   Soit $a \in A$, alors ax est dans I_n et donc dans I, lequel est un idéal de $(A, +, .)$.

   A étant un anneau principal, on notera d un générateur de I.

   On en déduit que $\forall n \in N, d|a_n$, et

   $\ldots |a_n|a_{n-1}|a_{n-2}| \ldots |a_1|a_0$. d est dans la réunion des I_n : il existe p tel que $d \in I_p$ et $I = I_p$.

   Comme $I_p \subset I_{p+1} \subset \ldots \subset I$, on déduit que la suite est stationnaire à partir du rang p.

5. a. La récurrence est immédiate. À chaque étape, on trouve pour d_n un diviseur non associé (on pourra dire un diviseur strict) en utilisant le fait que d_n est réductible.

   b. On considère les idéaux associés (I_n). Cette suite est croissante au sens de l'inclusion, et on peut utiliser les résultats de la question I.4.

   Tout élément de A possède un diviseur irréductible.

6. D'abord une petite remarque : il n'y a pas pour l'instant de générateur particulier pour un idéal (positif dans $\mathbb{Z}$ par exemple ou unitaire dans $K[X]$). Si un élément de A est irréductible, tous ses éléments associés le sont.

   Il n'y a donc pas besoin de faire apparaître une unité dans la décomposition. Nous aurons besoin de cette unité si nous choisissons des générateurs particuliers.

   La suite des (p_n) est une suite croissante d'idéaux. Elle est donc stationnaire, ce qui implique que la suite des $p_n)$ est finie.

   Soit n l'indice du dernier terme de la suite, alors il existe u une unité de A telle que $x = u.p_1\dot{p}_n$.

b. Montrons d'abord un premier résultat : soit $k \in \mathbb{N}^*$, si $p^k|ab$ et $p \wedge a$, alors $p^k|b$.

   On construit par récurrence une suite (b_n) telle que $b_1 = b$, et $b_{n+1} = pb_n$. On utilise le théorème de Gauss pour l'hérédité.

   Remarquons aussi si un élément irréductible divise un autre élément irréductible, ils sont associés. Ce qui implique que deux éléments irréductibles sont ou associés, ou premiers entre eux.

   Dernier résultat : si x est premier avec y et z, alors il est aussi premier avec leur produit.

   Nous allons procéder par récurrence, avec l'hypothèse de récurrence : tout élément de a qui admet une décomposition faisant intervenir n éléments irréductibles admet une décomposition en facteurs irréductibles unique, à l'ordre et aux unités prêts.

   initialisation On suppose que $x = up^a$ et $x = vq^b$. Si on suppose que p et q ne sont pas associés, en appliquant b fois le théorème de Gauss, on trouve que p divise v !. p et q sont donc associés, et donc $p^a = wp^b$, ce qui implique que $a = b$.

   Hérédité : On suppose l'hypothèse de récurrence vraie au rang $n-1$, avec $n > 1$.

   On suppose donc que pour un élément x_n donné, nous disposions de deux décompositions : $x_n = u\prod_{k=1}^{n} p_k^{\alpha_k}$ et $x_n = v\prod_{k=1}^{m} q_k^{\beta_k}$.

   Pour tout $k \in [\![1, n]\!]$, p_k divise $\prod_{j=1}^{m} q_j^{\beta_j}$. Comme p_k n'est pas premier avec le produit des q_j, il est associé à un des q_j : q_l. Comme $p_k^{\alpha_k}$ divise x_n, il divise aussi $\prod_{j=1}^{m} q_j^{\beta_j}$ et donc $q_l^{\beta_l}$.

   De même $q_l^{\beta_l}$ divise $u\prod_{k=1}^{n} p_k^{\alpha_k}$, et donc $p_k^{\alpha_k}$. Ces éléments sont associés.

   On introduit x_{n-1} tel que $x_n = p_k^{\alpha_k} x_{n-1}$ et on applique l'hypothèse de réccurence à x_{n-1}.

Si l'hypothèse de récurrence est vraie au rang $n-1$ ($n>1$), alors elle est vraie au rang n.

Conclusion : Or elle est vraie au rang 1, donc elle est vraie à tout rang.

7. a. $\mathbb{Z}$ ou encore $\mathbb{K}[X]$.

   b. i On considère d'abord $\mathcal{I} := \{\Phi(x); x \in I^*\}$. C'est une partie non vide de $\mathbb{N}$, elle admet un élément minimal p. x_0 est un des antécédents de p.

   ii Immédiat puisque $x_0 \in I$.

   iii Preuve classique.
   Soit $x \in I$. On effectue la division euclidienne de x par x_0 : il existe q et r tel que $x = qx_0 + r$ avec $r = 0$ ou $\Phi(r) < \Phi(x_0$.
   $r = x - qx_0$ est un élément de I. Or sa valeur en Phi est strictement indérieure à celle de x_0, il n'est donc pas dans I^* et par conséquent, $r = 0$. Cela implique que $x \in (x_0)$.

   c La question I.7.b indique que tout idéal de A est principal, d'où la conclusion.

Partie II

1. $(\mathbb{Z}/p\mathbb{Z}^*, .)$ est un groupe cyclique puisque p est premier. Son ordre est $p-1$ (cardinal du groupe). Donc l'ordre de tout élément divise $p-1$ (théorème de Lagrange).

2. p étant un nombre premier impair, $p = 2q+1$.

   On considère maintenant un générateur de $\mathbb{Z}/p-1\mathbb{Z}$. L'ordre de x est donc $p-1$.

   On pose $y = x^q$. Puisque l'ordre de x est $p-1$, celui de y est 2. Or les deux seuls éléments d'ordre au plus 2 sont 1 et -1.

   $y = -1$ et $x_0 = x$.

   Je laisse la preuve du fait qu'un entier est forcément premier avec un des entiers qui lui est inférieur en dehors de 1.

   On pouvait aussi passer par le quotientage du morphisme carré dans $\mathbb{Z}/p\mathbb{Z}^*$

3. Si p est de la forme $4k+1$, alors on a de la question précédente : $x^{2k} = -1$, ou encore $\left(x^k\right)^2 = -1$.

4. Une racine de -1 est une élément d'ordre 4 de $(Z/pZ^*, .)$. Ce groupe est d'ordre $p-1$. Or $p-1$ est de la forme $4k+2$. Ce n'est donc pas un multiple de 4. Il n'y a pas de racine de -1 si p est congru à 3 modulo 4.

5. On va d'abord noter que cette question est classique, mais qu'habituellement on passe par $4p_1p_1 \ldots p_n - 1$

   Ici, Bezout assure que P est premier avec tous les p_i, c'est à dire tous les entiers premiers qui lui sont inférieurs et qui sont de la forme $4p+1$.

Partie III

1. $\mathbb{Z}[i]$ est un sous-ensemble de $\mathbb{C}$ qui est intègre.

ii. Si $N(x) = 1$, alors $x \in \{1, -1, i, -i\}$. Il est bien inversible.

   Réciproquement, si x est inversible, alors $x.x^{-1} = 1$, et $N(x)N(x^{-1} = 1$. On, pour un élément z de $\mathbb{Z}[i]$, $N(z) \in \mathbb{N}^+$, et il divise 1 : c'est 1.

3. Remarquons qu'on travaille dans $\mathbb{C}$.

   Soient x et y deux éléments de $\mathbb{Z}[i]$, y non nul.

   $\frac{x}{y}$ est une élément de $\mathbb{C}$. On note α et β les parties réelles et imaginaires : $\frac{x}{y} = \alpha + i\beta$.

   Pour α, on note s l'entier le plus proche : $|\alpha - s| \leq \frac{1}{2}$. De même, pour β, en notant t l'entier le plus proche, $|\beta - t| \leq \frac{1}{2}$.

   On pose $q := s + it$, et $r := x - qy$.

$$\begin{aligned} N(r) &= N(y)N(\frac{x}{y} - q) \\ &= N(y)N(\alpha - s + i(\beta - t)) \\ &\leq N(y)(\frac{1}{4} + \frac{1}{4} \end{aligned}$$

   Il n'y a pas d'unicité.

4. Il est euclidien, il est donc principal.

Partie IV

Petite remarque : pour deux entiers z et z', z divise z' dans $\mathbb{Z}$ si et seulement si z divise z' dans $\mathbb{Z}[i]$.

1. Raisonnement par disjonction des cas : la somme de deux carrés de nombres pairs donne un reste 0 modulo 4. Pour la somme de deux nombres impairs, on trouve deux, et pour la somme d'un nombre impair et d'un nombre pair, on trouve 2.

   Donc si p est congru à 3 modulo 4, ce n'est aps la somme de deux carrés.

2. On suppose que x ne divise pas α.

   On considère I l'idéal engendré par x et α. $I := \{z_1 x = z_2\alpha; (z_1, z_2) \in \mathbb{Z}[i]^2\}$.

   I est un idéal principal : on note γ un générateur.

   γ est un diviseur commun à α et x. Mais x est irréductible. Donc γ est une unité, et $I = \mathbb{Z}[i]$. On peut donc trouver (z_1, z_2) dans $\mathbb{Z}[i]^2$ tels que $1 = z_1\alpha + z_2 x$. On multiplie cette équation par β :

$$\beta = z_1\alpha\beta + z_2 x\beta.$$

   Comme x divise $\alpha\beta$, on peut conclure que x divise β.

3. a. p est congru à 1 modulo 4, alors II.3. assure que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Notons x_0 un racine de -1. Alors $x_0^2 + 1$ est un multiple de p ce qui permet de conclure.

   b. Première remarque : les divisibilités dans $\mathbb{Z}$ et $\mathbb{Z}[i]$ se comportent différemment. Ainsi $2 = (1 + i)(1 - i)$ n'est pas premier.

   On suppose donc que p divise $x_0 + i$: il existe $q \in \mathbb{Z}[i]$ tel que $x_0 + i = p.q$. Utilisant le fait que x_0 et k sont entiers, et passant $kp = (x_0 + i)(x_0 - i)$ au conjugué, on trouve la conclusion demandée.

   p divise aussi la différence entre $x_0 + i$ et $x_0 - i$. Donc p divise $2i$. Ou encore 2 puisque $-i$ est une unité.

   Donc p divise 2 dans $\mathbb{Z}$.

c Comme p est congru à 1 modulo 4, on aboutit à une contradiction. Donc p ne divise pas $x_0 + i$.

Pour les mêmes raisons, il ne divise pas non plus $x_0 - i$.

Si p est irréductible, on peut utiliser les résultats de la question IV.2 pour p. Et on aboutit à une contradiction.

Donc p est réductible dans $\mathbb{Z}[i]$.

d. On a donc p réductible. Soit z et z' deux éléments de $\mathbb{Z}[i]$ tels que $p = zz'$ et z et z' non des unités. On passe à la norme en utilisant la multiplicativité. $p^2 = N(z)N(z')$.

On se place dans $\mathbb{Z}$. En effet $N(z)$ et $N(z')$ sont des entiers. Comme p est premier, il y a 3 possibilités : $N(z) = p^2 et N(z') = 1$, $N(z') = p^2 et N(z) = 1$ ou $N(z) = p et N(z') = p$.

Seul le dernier cas est possible car z et z' ne sont pas des unités et leur norme n'est donc pas 1.

On trouve $p = N(z)$, ce qui permet de conclure.

Partie V

1. Soit p un nombre premier réductible. On note a et b non unités tels que $p = ab$. Le même raisonnement que la question précédente montre que $p = N(a) = N(b)$ et donc que p peut s'écrire comme la somme de deux carrés. La question IV.1. assure alors qu'il n'est pas congru à 3 modulo 4. (résolution par contraposée).

2. On a donc $N(z) = a^2 + b^2$ est un nombre premier. Si z est réductible dans $\mathbb{Z}[i]$, en notant ww' sa décomposition, on trouve que $a^2 + b^2 = N(w)N(w')$. Comme $a^2 + b^2$ est premier, nécessairement z ou z' sont des unités ce qui est impossible. Donc z est irréductible dans $\mathbb{Z}[i]$.

3.

Partie VI

1. Question classique. On développe dans $\mathbb{C}$ $(a + ib)(c + id)$ et on passe au module.

   Cette question est encore valable dans la majeure partie des anneaux (expression algébrique).

2. Si x admet une telle décomposition, du fait du caractère multiplicatif de la question précédente, on regarde terme par terme.

   2 est bien la somme de deux carrés (1+1), donc 2^n aussi.

   Les $p_i^{\alpha_i}$ le sont aussi d'après V.

   $q_i^{\beta_i}$ est un carré !

3.