Corrigé pour la Fiche 4, exos. 3(c), 4(c) et 4(d) et la démonstration du critère d'Eisenstein
2016-2017

3(c) Si a^2+b^2 est impair, alors il est congru à 1 modulo 4. En effet, si a^2+b^2 est impair, alors, quitte à permuter les variables, on peut supposer que a est pair et b est impair. Si $a=2n$ et $b=2m+1$, alors $a^n+b^n=4(n^2+m^2+m)+1$. Comme p est premier et $p\geq 3$, p est impair. Donc si p est la somme de deux carrés, alors p est congru à 1 modulo 4.

Pour la réciproque, on suppose p congru à 1 modulo 4. Alors par la partie b, il existe un $x\in\mathbf{Z}$ tel que x^2+1 est divisible par p. On pose $x^2+1=np^k$ où $k\geq 1$, et $p\not| n$. On utilise maintenant l'exercice 2 : $A=\mathbf{Z}[i]$ est un anneau principal donc factoriel. En plus, si z_1 divise z_2 dans A, alors $s(z_1)$ divise $s(z_2)$, et $s(z)\in\mathbf{N}$ est ≥ 2 si et seulement si z n'est pas inversible.
On va montrer par l'absurde que p n'est pas premier (ou irréductible) dans $\mathbf{Z}[i]$. On suppose que p est premier dans A. On a que $(x+i)(x-i)=np^k$. D'abord, p ne divise pas $2i$, car $s(p)=p^2>4=s(2i)$. Donc p ne divise pas à la fois $(x+i)$ et $(x-i)$. Maintenant, comme p^k divise le produit, si p est premier, comme A est factoriel, p^k divise un des facteurs. Ceci implique que $p^{2k}=s(p^k)$ divise $np^k=s(x+i)=s(x-i)$ dans $\mathbf{Z}$. Ceci n'est pas possible, car $k\geq 1$ et p est premier.

4(c) (Rappel : Dans A, comme dans $\mathbf{Z}$, un élément est irréductible si et seulement s'il est premier.) Si $a\in\mathbf{N}$ est irréductible dans A, alors il est irréductible dans $\mathbf{Z}$. En plus, par l'exercice 3(c), a n'est pas congru à 1 modulo 4, et par l'exercice 4(b), $a\neq 2$. Donc a est premier et congru à 3 modulo 4.
Pour la réciproque, si $p\in\mathbf{N}$ est premier dans $\mathbf{Z}$ et congru à 3 modulo 4, on va montrer, en utilisant la "norme" s, que p est irréductible (donc premier) dans A. On suppose que $p=(a+ib)(c+id)\in A$ où $a+ib$ et $c+id\in A$. Alors $p^2=s(p)=s(a+ib)s(c+id)$. Si $s(a+ib)=p$, alors $p=a^2+b^2$ est une somme de deux carrés. Ceci est impossible par l'exercice 3(c). Donc $s(a+ib)=1$ ou p^2, auquel cas $s(c+id)=1$. On a donc démontré que $a+ib$ ou $c+id$ est inversible.

4(d) Soit $z=a+ib\in A$ avec $a\neq 0$ et $b\neq 0$. Supposons d'abord que $a^2+b^2=p$ est premier (et , par l'exercice 3(c), p n'est pas congru à 3 modulo 4). On va montrer que z est premier dans A. Il suffit de montrer que z est irréductible. Si $z=(c+id)(c'+id')$, alors $p=s(z)=(c^2+d^2)(c'^2+d'^2)\in\mathbf{Z}$. Comme p est premier, un des facteurs est p, et l'autre facteur est 1. Donc un $c+id$ ou $c'+id'$ est inversible. Ceci montre que z est irréductible.
Maintenant, la réciproque : Soit $z=a+ib\in A$ premier. On a que $(a+ib)(a-ib)=a^2+b^2$. On peut décomposer a^2+b^2 en produit de nombres premiers dans $\mathbf{Z}$. Comme z est premier dans A, il divise un tel facteur. Autrement dit, il existe un nombre premier p, tel que $a+ib$ divise p. Donc $a^2+b^2=s(a+ib)$ divise $s(p)=p^2$. Ceci implique que $s(z)=a^2+b^2=1, p$ ou p^2. Cette norme ne peut pas être 1, car z n'est pas inversible ($a\neq 0$, et $b\neq 0$). On montre maintenant, par l'absurde, que $a^2+b^2\neq p^2$. On suppose que $(a+ib)(a-ib)=p^2$. Si p est congru à 3 modulo 4, alors, par l'exercice 4(c), p est premier dans A, et donc la décomposition unique un produit d'éléments premiers de $(a+ib)(a-ib)=p^2$ est p^2. Comme $a\neq 0$ et $b\neq 0$, $a+ib$ n'est pas un facteur premier. Si p n'est pas congru à 3 modulo 4, alors p est la somme de deux carrées : $p=c^2+d^2=(c+id)(c-id)$. Si $a+ib$ est premier, $a+ib$ divise $c+id$ ou $c-id$. Donc $p^2=a^2+b^2$ divise $c^2+d^2=p$. Contradiction.
Ceci montre que l'unique possibilité est que $a^2+b^2=p$, avec p premier, et $p=2$ ou $p\equiv 1(\mod 4)$.

Exercice supplémentaire : Décomposer en produit d'éléments premiers : 5 et $3+4i$. (On remarque que $5^2=(3+4i)(3-4i)$.)

Deux démonstrations du critère d'Eisenstein

Théorème 1 *(Critère d'Eisenstein) Soit A un anneau factoriel, et $P=\sum_{i=0}^{d}a_i\in A[X]$ un polynôme de contenu $c(P)=1$. S'il existe un élément premier p de A tel que $p|a_i$ pour $i=0,\ldots,d-1$ et $p^2\not| a_0$, alors P est un polynôme irréductible de $A[X]$ (et donc de $K[X]$, où K est le corps de fractions de A).*

On utilisera les résultats suivants :
(a) Un polynôme $Q \in A[X]$ est inversible si et seulement si $\deg(Q) = 0$ et $c(Q) = 1$;
(b) $\deg(QR) = \deg(Q) + \deg(R)$, car A est intègre.

Pour les deux démonstrations, on suppose que $P = QR$. On sait que le degré du polynôme P est d. On montrera que le degré de Q ou de R est zéro. Par les résultats ci-dessus et le fait que le contenu de Q et R sont forcément 1, ceci implique que Q ou R est inversible, et donc P est irréductible.

Soit $Q = \sum_{j=0}^{n} q_j X^j$, et $R = \sum_{k=0}^{m} r_k X^k$ avec $\deg(Q) = n$ et $\deg(R) = m$. On a $n + m = d$.

Notons que $p \not| a_d$, car le contenu $c(P) = 1$, et p divise tous les autres coefficients. Ceci implique aussi que $p \not| q_n$ et $p \not| r_m$, car $a_d = q_n r_m$.

Maintenant considérons le terme constante $a_0 = q_0 r_0$. Comme $p|a_0$ mais $p^2 \not| a_0$, on peut conclure que $p|q_0$ ou r_0, mais pas les deux. Quitte à échanger Q et R, on va supposer que $p|q_0$ et $p \not| r_0$. Le but dans les deux démonstrations est de montrer que $m = 0$ (et $n = d$).

Démonstration 1 : On considère l'anneau intègre $B = A/(p)$. (Intègre, car p est un élément premier de A.) On construit l'homomorphisme $\varphi : A[X] \to B[X]$, tel que $\varphi(\sum_{i=0}^{s} c_i X^i) = \sum_{i=0}^{s} \overline{c_i} X^i$, où $\overline{c_i}$ est la classe de c_i dans B. Notation : $\varphi(Q) = \overline{Q}$.

On remarque que $X \in B[X]$ est premier, car $B[X]/(X) \cong B$ est intègre.

On applique φ à $P = QR$. On a $\overline{P} = \overline{Q}\,\overline{R}$. Comme les coefficients de plus haut degré de P, Q et R ne sont pas divisibles par p, les degrés ne changent pas. Autrement dit, $\deg(P) = \deg(\overline{P})$, $\deg(Q) = \deg(\overline{Q})$ et $\deg(R) = \deg(\overline{R})$.

Maintenant on voit que $\overline{P} = \overline{a_d} X^d = \overline{Q}\,\overline{R}$. Par l'hypothèse, $p \not| r_0$, et donc $X \not| \overline{R}$. Comme X est premier dans $B[X]$, ceci implique que X^d divise $\overline{Q}$, qui doit être de degré au moins d. Mais ce degré est $n \leq d$. Donc $n = d$, et $m = 0$.

Démonstration 2 : Comme dans la démonstration 1, on suppose que p divise q_0 mais p ne divise pas r_0. En plus, on sait que $p \not| q_n$. Donc on peut choisir j_0 minimal tel que $p \not| q_{j_0}$. Autrement dit, $p|q_0, \ldots, q_{j_0-1}$, mais $p \not| q_{j_0}$. On calcule $a_{j_0} = \sum_{k=0}^{j_0} q_k r_{j_0-k}$. Tous les termes sont divisibles par p sauf $q_{j_0} r_0$, qui n'est pas divisible par p. Donc p ne divise pas a_{j_0}. Par l'hypothèse du théorème, $j_0 = d$. Mais $j_0 \leq n$, le degré de Q. Donc l'unique possibilité est $j_0 = n = d$, et $m = 0$.