Université Claude Bernard Lyon 1

CORRECTION DE L'EXAMEN PARTIEL

M1-Algèbre 2017

Problème 1.

1. On veut montrer que $\mathbb{Z}[i]$ est euclidien. Utilisons comme stathme la norme de $\mathbb{Z}[i]$ donnée par
$$N(a+ib) = a^2 + b^2,\ a, b \in \mathbb{Z}.$$
On se fixe z, z' non nuls dans $\mathbb{Z}[i]$. On pose alors [1]
$$\frac{z'}{z} = x + yi,\ x, y \in \mathbb{R}.$$
On peut trouver a, b dans $\mathbb{Z}$ tels que
$$|x-a| \leq \frac{1}{2},\ |y-b| \leq \frac{1}{2}.$$
Il en résulte que
$$N\left(\frac{z'}{z} - (a+ib)\right) = N\left((x-a) + i(y-b)\right) \leq \frac{1}{4} + \frac{1}{4} < 1.$$
Si l'on pose $q := a + ib$ et $r := z' - qz$, on a donc bien
$$z' = qz + r,\ N(r) = N(z)N(\frac{z'}{z} - q) < N(z).$$
Conclusion, $\mathbb{Z}[i]$ est euclidien.
2. Les éléments ± 1, $\pm i$ sont clairement inversibles dans $\mathbb{Z}[i]$. Réciproquement, si $u := a + ib$ est inversible dans $\mathbb{Z}[i]$, alors il existe u' dans $\mathbb{Z}[i]$ tel que $uu' = 1$. Comme la norme d'un élément de $\mathbb{Z}[i]$ est dans $\mathbb{N}$, il vient que $N(u)N(u') = 1$ implique $N(u) = 1$. On a donc $a^2 + b^2 = 1$, ce qui donne bien $(a, b) = (\pm 1, 0)$ ou $(a, b) = (0, , \pm 1)$ comme voulu.
3. Supposons x pair. On a alors $y^2 \equiv -1$ modulo 4. Or, -1 n'est pas un carré modulo 4. Donc, x est impair. Du coup, y^2 est pair, donc y est pair.
4. Supposons que $1+i$ divise $y \pm i$ dans $\mathbb{Z}[i]$. Alors, en prenant la norme, on aurait $2 = N(1+i)$ divise $y^2 + 1 = N(y \pm i)$. Absurde, car y est pair.
5. Par l'absurde, supposons $1 + i = zz'$, avec z et z' non inversibles. On a alors
$$2 = N(1+i) = N(z)N(z'),$$
ce qui oblige, par exemple, $N(z) = 1$. Mais dans ce cas $z\overline{z} = 1$ et donc z est inversible, absurde. De même, $1 - i$ est irréductible.

1. En fait, a et b sont dans $\mathbb{Q}$, mais ce n'est pas très important ici.

6. Montrons que $y+i$ et $y-i$ sont premiers entre eux. Pour cela, on peut supposer, par l'absurde, $d \in \mathbb{Z}[i]$ premier divisant $y+i$ et $y-i$. En particulier, d divise $(y+i)-(y-i) = 2i$. Donc, $N(d)$ divise $N(2i) = 4$. Cela implique $N(d) = 4$ ou $N(d) = 2$. Le premier cas donne $d = 2$ modulo les unités, donc $d = (1+i)(1-i)$, absurde car d est premier ; donc irréductible. Le second cas donne $d = 1+i$ modulo les unités. Absurde par ce qui précède.

   Maintenant, comme $(y+i)(y-i) = x^3$ et que $y+i$ et $(y-i)$ sont premiers entre eux dans l'anneau factoriel $\mathbb{Z}[i]$, il en résulte que $y+i$ est un cube, à unité près. Or, les inversibles de $\mathbb{Z}[i]$ sont tous des cubes (par exemple, car $\mathbb{Z}[i]^*$ est d'ordre $'$ qui est premier avec 3). Donc, $y+i$ est un cube.
7. Il existe donc a et b dans $\mathbb{Z}$ tels que $(y+i) = (a+ib)^3$. La partie imaginaire donne $1 = 3a^2b - b^3$, donc, soit $b = 1$ avec $3a^2 - b^2 = 1$, soit $b = -1$ avec $3a^2 - b^2 = -1$. Le premier cas est impossible, le second donne $(a, b) = (0, -1)$. On a alors $y = 0$, puis, $x = 1$.

Problème 2.

1. Le nombre n_p de p-Sylow divise q et il est différent de 1 car G est simple. Donc, $n_p = q$, or $q < p$, donc q ne peut pas être congru à 1 modulo p.
2. (a) Le nombre n_q de q-Sylow divise p^2 et est différent de 1. Donc, $n_q = p$ ou p^2. Or $p < q$, donc p ne peut pas être congru à 1 modulo q. Conclusion, $n_q = p^2$.
   (b) Deux q-Sylow sont d'ordre q premier. Donc, leur intersection est triviale et de plus tous les éléments non triviaux d'un q-Sylow sont d'ordre q, par Lagrange. Il y a donc $n_q(q-1) = p^2(q-1)$ éléments d'ordre q.
   (c) Comme le groupe G est simple, il ne peut contenir qu'un seul p-Sylow. Or, un p-Sylow contient p^2 éléments, dont $p^2 - 1$ d'ordre divisible par p. Conclusion, G contient au poins p^2 éléments dont l'ordre est divisible par p.
   (d) Faisons le bilan : il y a l'élément neutre, plus, au moins p^2 éléments d'ordre divisible par p, et $p^2(q-1)$ éléments d'ordre q. Comme p et q sont des premiers distincts, ces ensembles sont disjoints et cela fait en tout au moins $1+p^2+p^2(q-1) = p^2q+1 > p^2q$ éléments. Absurde.

Problème 3.

1. Une orbite est en bijection avec un quotient de G. Donc, les orbites d'un p-groupe sont de cardinal 1 ou divisible par p. Par la formule des classes, comme le cardinal de X n'est pas divisible par p, il existe forcément une orbite de cardinal 1, donc forcément, un élément x de X fixé par tout G.
2. (a) Le groupe G est un sous-groupe de $\mathrm{GL}(V)$. A ce titre, il agit sur V et comme $\{0\}$ est une orbite singletonne, il agit sur $X := V - \{0\}$. Or, X est de cardinal $p^n - 1$, donc, non divisible par p. Conclusion, G possède un point fixe dans X.
   (b) Le morphisme de groupe provient du calcul par blocs : Si l'on multiplie g et g', on multiplie $\mathrm{mat}_b(g)$ et $\mathrm{mat}_b(g')$, et donc $\mathrm{mat}_{b'}(g)$ et $\mathrm{mat}_{b'}(g')$.
   (c) On montre l'initialisation en 1. Si V de dimension 1, $\mathrm{GL}(V) \simeq \mathbb{F}_p^*$ est de cardinal $p-1$, qui n'est pas divisble par p. Donc G est réduit à un élément neutre (un p-groupe trivial !).

   L'hérédité provient directement de la question précédente en changeant b' en une base de trigonalisation, obtenue par récurrence.