DM 9 - Sommes de deux carrés – Ordres dans un groupe - Reprise

1 Entiers de Gauss et sommes de deux carrés

1.1 $\mathbb{Z}[i]$ est un anneau euclidien.

1. Traité le plus souvent de façon efficace.
2. RAS
3. Pour le sens $N(z) = 1$ implique z inversible dans $\mathbb{Z}[i]$, on préfère dans beaucoup de copies dire que $a^2 + b^2$ doit diviser a et b. C'est bien sûr correct, mais l'utilisation de la norme (cf.corrigé) est plus efficace et fonctionne dans davantage de situations.
4. Deux problèmes à éviter : 1) ne pas remarquer que prendre les parties entière des parties réelle et imaginaire ne fonctionne pas toujours : il faut prendre les entiers les plus proches pour gagner en proximité ; 2) Multiplier les cas pour pas grand chose. Il suffit de remarquer que tout réel est à distance $\leq 1/2$ d'un entier (ce qui peut être affirmé directement) et de travailler avec ces entiers.
5. Un contre-exemple vaut mieux qu'un long discours.

1.2 Lemme d'Euclide dans $\mathbb{Z}[i]$

6. Des réponses souvent trop longues. Il suffit de dire que l'ensemble considéré est une partie non vide de $\mathbb{N}$.
7. Bien en général. Le passage de d divise a à d inversible est souvent un peu confus.

1.3 Nombres premiers sommes de deux carrés

8. On peut aller vite sur ces questions. Pas besoin de traiter 16 cas : dire qu'un carré modulo 4 vaut 0 ou 1 et donc que la somme de deux carrés modulo 4 vaut 0, 1 ou 2 suffit largement.
9. Le fait que p ne divise pas $x + i$ dans $\mathbb{Z}[i]$ est souvent bâclé.
10. RAS
11. Ne pas oublier de donner un argument pour $N(b), N(c) \neq 1$.

1.4 Théorème de Fermat de Noël

12. RAS
13. RAS ; voir cependant le corrigé et méditer sur cette identité.
14. Il faut dire ce qui se passe avec les puissances de 2.

15. RAS

16. Bien compris en général

17. RAS

2 Ordres dans un groupe

2.1 Théorème de Lagrange

1. RAS

2. Pour ce genre d'égalités *faciles*, il est souvent plus rapide de raisonner par équivalence, plutôt que de faire une double inclusion où on écrit essentiellement deux fois la même chose. On peut aller vite sur le fait que $H \to xH, h \mapsto xh$ est une bijection (par exemple, en donnant simplement son inverse).

3. Il faut dire très clairement que l'ensemble des classes d'équivalence est une partition de G.

4. Souvent mal traitée. Il est souvent affirmé un peu vite que puisque G est fini, il existe nécessairement un entier $n > 0$ tel que $x^n = e_G$. C'est vrai, mais uniquement parce qu'on est dans un groupe ; ceci devrait figurer de façon claire dans la justification.
   De plus, l'égalité $\langle x \rangle = \{e, x, \dots, x^{\omega(x)-1}\}$ mérite une démonstration (l'inclusion droite-gauche est claire, gauche-droite vient d'une division euclidienne). Enfin, il ne faut pas oublier de dire pouquoi $\{e, x, \dots, x^{\omega(x)-1}\}$ est bien de cardinal $\omega(x)$ (il pourrait y avoir des doublons, mais non).

5. RAS

6. **Application.** Pour tout x, $\omega(x)$ divise p. Attention ! on peut avoir $\omega(x) = 1$ (exactement pour $x = e$). Bien dire qu'on prend un élément x différent de e et qu'alors $\langle x \rangle = G$.

7. **Exemple des groupes cycliques.** Rédigé de façon plus ou moins propre. Il ne suffit pas de dire que $\frac{n}{n \wedge k} \times \overline{k} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$; il faut encore dire que $\frac{n}{n \wedge k}$ est l'entier minimal pour cette propriété. Un raisonnement par équivalence comme dans le corrigé est pertinent.

8. **Exemple des groupes symétriques.** Soit $n \geq 1$. On note S_n le groupe des permutations de $[\![1, n]\!]$.

   (a) RAS

   (b) RAS

   (c) Un exemple a souvent été donné. Attention ! il est parfois affirmé de façon plus ou moins explicite que l'ordre d'un produit de deux éléments est le ppcm de l'ordre de ces éléments. Ceci est faux, y compris dans un contexte commutatif. (*mais si deux éléments commutent et ont des ordres premiers entre eux, alors l'ordre du produit est le produit des ordres*)

2.2 Théorème de Cauchy

Partie peu traitée. En général bien comprise de celles et ceux qui s'y sont essayé.