DS 3 de mathématiques – Reprise

1 Structure des groupes abéliens finis

1.1 Ordres et exposant

1. Dans les cas les plus simples, exhiber la bijection réciproque (et vérifier qu'elle l'est) est souvent le plus rapide pour montrer qu'une application est bijective.

2. Argument classique, vu en arithmétique, avec un formalisme légèrement différent. On généralisera cette propriété au cas non abélien plus tard.

3. (a) Dire que $(ab)^{\omega(a)\omega(b)}$ ne montre pas que $\omega(ab) = \omega(a)\omega(b)$, mais que $\omega(ab) \mid \omega(a)\omega(b)$. L'autre sens est un peu plus délicat.

   (b) Les deux premières égalités sont obtenues de la même façon. On peut écrire *De même* pour la deuxième, après avoir justifié convenablement la première.

   (c) RAS

4. **Un exemple.** RAS

1.2 Prolongement de caractères

5. Il faut absolument justifier que l'ensemble est non vide. L'équivalence se démontre ensuite de façon analogue à ce qui a été fait plusieurs fois dans le cours (ne pas oublier le sens trivial) !

6. On note K le sous-groupe de G engendré par $H \cup \{a\}$.

   (a) Rédaction souvent confuse. On pouvait au choix utiliser la formule générale pour un sous-groupe engendré et justifier proprement que les éléments ainsi écrits étaient exactement les ha^k ; ou bien montrer directement que le membre de droite est un sous-groupe de G contenant H et a et minimal pour cette propriété (c'est-à-dire refaire une preuve du cours dans un cadre simplifié). La deuxième rédaction est sans doute la plus simple.

   (b) Beaucoup disent que $\omega = \chi(a)$ convient ; attention à bien comprendre la structure de la preuve. L'objectif est justement de prolonger un caractère, qui n'est pas défini en a pour le moment !

(c) La *bonne définition* a été mal comprise. Quand on demande de montrer qu'une application est bien définie, il y a essentiellement trois problèmes potentiels (qui peuvent se recouper) :

- L'expression a un sens (pas de division par 0 par exemple).
- On arrive dans le bon ensemble d'arrivée (question 2.2.6 du problème par exemple).
- Quand la fonction est définie à partir d'une écriture non unique d'un élément de l'espace de départ, la formule donnée pour l'image ne dépend pas de cette écriture.

C'était ici le 3ème point qu'il fallait vérifier.

7. On attend une démonstration propre. On renvoie au corrigé pour une rédaction raisonnable. Il est aussi envisageable de considérer le plus grand groupe contenant H sur lequel χ se prolonge et de montrer que ce groupe doit être G entier en raisonnant par l'absurde ; c'est sans doute un point de vue plus abstrait.

1.3 Théorème de structure

8. Essentiellement une question de cours.

9. De même, il s'agit essentiellement de rappeler que le groupe additif $\mathbb{Z}/e\mathbb{Z}$ est isomorphe au groupe multiplication $\mathbb{U}_e$.

10. L'inclusion $\hat{\chi}(G) \subset \mathbb{U}_e$ n'est pas automatiquement : on n'a pas explicitement dit qu'on pouvait rester dans le même groupe de racines de l'unité quand on prolonge le caractère (et c'est faux en général) ; le point était de rappeler que l'ordre de tout élément divise e.

11. RAS

12. Ici aussi, on attend une démonstration par récurrence un minimum formalisée. Ce n'est d'ailleurs pas si compliqué à rédiger et ça clarifie l'argumentation ; notamment les liens de divisibilité entre les d_k.

2 Convolution de Dirichlet et fonction de Möbius

2.1 Anneau des fonctions arithmétiques

1. Question de cours. Il est mieux de redonner l'argument pour se préparer à un vrai écrit. On peut dire que la commutativité et l'associativité de la loi + se déduisent immédiatement de celles sur $\mathbb{C}$.

2. Question plus délicate, notamment l'associativité. Il est plus simple d'utiliser la première forme donnée du produit de convolution pour faire un calcul convaincant.

3. RAS

4. D'une part, ne pas oublier la distributivité (même si elle est évidente). D'autre part, rappeler tous les axiomes à vérifier, même s'ils viennent d'être démontrés (vous voulez montrer que vous connaissez vos définitions).

5. L'implication directe s'obtient en évaluant en 1 l'égalité $f * f^{-1} = \mathbb{1}$. Pour la réciproque, il faut *construire* l'inverse ; une construction par récurrence fonctionne.

2.2 Fonctions multiplicatives

6. Le fait que ϕ est bien définie est à peu près trivial. Mais il est mieux d'écrire qqch du genre $m = d_1k_1$; $n = d_2k_2$ donc $mn = (d_1d_2)(k_1k_2)$. Affirmer qu'elle est bien définie parce que $m \wedge n = 1$ dénote une certaine paresse intellectuelle ; cette hypothèse n'étant pas nécessaire à ce stade...
   Pour la surjectivité, on ne doit pas se contenter d'une paraphrase du type : comme $m \wedge n = 1$, tout diviseur de mn s'écrit comme le produit d'un diviseur de m et d'un diviseur de n. Il n'y a pas d'argument dans une telle reformulation de la question.

7. RAS

8. RAS

9. La stratégie pour ces questions a été mal comprise en général.

   (a) Une analyse-synthèse était pertinente.

   (b) RAS

   (c) RAS

2.3 Fonction de Möbius

10. Souvent une mauvaise rédaction. Faire une disjonction de cas est normal mais il faut être clair sur quoi. Ou bien sur la valeur de $\mu(nm)$, ou bien sur celle de $\mu(n)\mu(m)$; si on mélange tout en même temps, ça devient très vite confus. On renvoie au corrigé.

11. (a) Beaucoup affirment que $\mu(p^i)$ est toujours nul. Or $\mu(1) = (-1)^0$ et $\mu(p) = (-1)^1$. Si on a du mal à accepter la première égalité (en considérant que 1 est un produit de 0 nombre premier), on peut au moins remarquer que c'est une conséquence de $\mu \in \mathcal{M}$, d'après les calculs faits précédemment.

    (b) RAS

12. L'objectif était d'obtenir cette formule d'inversion en utilisant les propriétés formelles établies du produit de convolution. On pouvait bien sûr la démontrer directement ; ce qui revient essentiellement à refaire la preuve de l'associativité de $*$ dans ce cas.

2.4 Produits eulériens

13. On invite les élèves ayant du mal à comprendre ce *gros développement* à écrire explicitement ce qui se passe avec $N = 2$ et 3 nombres premiers.

14. Il s'agit de passer à la limite dans une somme de termes géométriques.

15. Corollaire de la formule précédente et de ce qui est admis sur les limites.

2.5 Probabilité que deux entiers soient premiers entre eux

16. RAS

17. On a bien sûr envie d'appliquer la formule d'inversion de Möbius ; mais elle ne va pas dans le bon sens. Il fallait privilégier un calcul direct.

18. Quelques élèves se trompent pour la deuxième inégalité et donnent une inégalité qui semble meilleure. Toujours se méfier quand on obtient mieux que l'énoncé.

19. RAS