ALGÈBRE: LE GRAND COMBAT

ERRATA ET COMMENTAIRES (VERSION DU 18 SEPTEMBRE 2019)

Introduction

p.xx, seconde moitié. $\mathrm{GL}(K)$ doit être remplacé par $\mathrm{GL}_n(K)$.

1. Ch. I - Théorie des ensembles

Définition 1.8. Il faut bien entendu lire « $f(E') = \{f(x') \mid x' \in E'\}$. »

Définition 2.1. La classe d'équivalence est plutôt le sous-ensemble des éléments en relation avec x (et non pas « équivalents à x »).

2. Ch. II - Arithmétique dans $\mathbb{Z}$

Remarques 1.2. (2). Il faut lire « l'antisymétrie découle du point (1). »

Remarques 1.4. (2). Il faut lire « $a' \in \mathbb{Z}$ ».

Algorithme d'Euclide, p.25. Il faut lire « où q_i et r_{i+1} »

Exercice 4. p.34. Le théorème de Gauss auquel on se réfère est bien entendu le lemme de Gauss.

3. Ch. IV - Déterminant

Proposition 5.8. Point (1′). Il faut lire « d'au plus une dilatation ».

4. Ch. V - Un peu de géométrie

Lemme 2.13, démo. En fait, il ne faut pas supposer F non nul, sinon on loupe le résultat suivant : si u est normal/etc..., alors u^* aussi. Ceci dit la démonstration fonctionne très bien, même si F est nul, puisque dans ce cas M se réduit à la matrice C.

Lemme 4.2. Pour coller aux notations des énoncés qui suivent ce lemme, il aura mieux valu échanger les places de b et c dans la matrice M, pour finalement obtenir $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

5. Ch. VI - Propriétés élémentaires des groupes

Démo du lemme 4.7. Pour « (1) $\Longrightarrow$ (2) », il serait plus judicieux d'écrire : « Supposons que H soit distingué dans G, et soit $x \in G$. Pour tout $h \in H$, on a $[\cdots]$ »

Théorème 4.9. Pour enfoncer le clou, il serait peut-être bon de rajouter dans l'énoncé que $|G/H| = [G : H] = \dfrac{|G|}{|H|}$.

6. Ch. VII - Groupes opérants sur un ensemble

Définition 1.8. Il faut bien entendu lire « pour la relation d'équivalence sur E ».

Proposition 1.12. La première application de l'énoncé s'appelle f, bien entendu.

Démo du lemme 1.14. Il faut mieux utiliser x' plutôt que x (qui est déjà utilisé) dans la définition de l'action de $\mathbb{Z}$ sur E.

7. Ch. VIII - Groupe symétrique, groupe alterné

Lemme 1.5. Dans (2) et (3), il manque « Pour tout $\sigma \in \mathfrak{S}(E)$ ».

p.205, Notation. Il faut lire « le p-cycle de l'exemple précédent ».

Début de la section 2. Il vaudrait mieux remplacer x par a, par souci de cohérence de notations.

Démo du lemme 2.5. Il vaudrait peut-être mieux récrire le début de l'argument comme suit. Soit $a' \in E$. Si $a' \in E \setminus \{a, \sigma(a), \ldots, \sigma^{p-1}(a)\}$, alors $a' \notin \omega[\cdots]$.

Il reste aussi à démontrer que le support de σ_ω est ω, mais cela provient de l'égalité et de l'exemple 2.3. (on peut aussi le démontrer par des arguments directs, sans passer par l'égalité précédente).

Remarque 2.8. Il vaudrait mieux dire (pour éviter les répétitions) : « Les deux résultats précédents fournissent l'égalité suivante ».

Lemme 2.17. Pour des soucis de cohérence de notation avec ce qui suit, il serait plus judicieux d'utiliser τ, au lieu de σ.

Théorème. 2.18. Il est bien entendu que les listes sont avec répétition.

Exemple 2.22. Pour des soucis de cohérence dans l'ouvrage, il faut écrire « cinq », en toutes lettres.

Remarque 2.24 et Exemple 2.25. Il serait plus cohérent de les échanger.

Remarque 2.24. Peut-être que quelques explications supplémentaires ne seraient pas de trop.

Connaître les longueurs des p-cycles à supports disjoints composant σ revient à connaître les cardinaux des σ-orbites non réduites à un singleton. Or, le nombre de σ-orbites réduites à un élément, c'est le nombre de points fixes,

c'est-à-dire le nombre d'éléments qui ne sont pas dans le support. Mais, le nombre d'éléments du support est la somme des cardinaux des σ-orbites non réduites à un singleton. Bref, connaître les longueurs des p-cycles à supports disjoints composant σ équivaut à connaître les cardinaux de toutes les σ-orbites, i.e. connaître le type de σ.

Le théorème 2.18 se retraduit donc de la manière suivante : deux permutations de $\mathfrak{S}(E)$ sont conjuguées si, et seulement si, elles sont de même type.

Démo du théorème 5.3. La première phrase aurait plus sa place après le cas $n = 4$.

Exercice 26. Question **d.** Il faut lire « On écrit $|G| = 2^m s$ », avec s impair et $m \geq 0$. D'autre part, dans la suite de la question, il faut lire « $|G|$ est impair ».

8. Ch. IX - Groupes quotient

Après l'exemple 1.1. La phrase « l'élément neutre de G/H est un 1_G »est superflue. Il suffit d'utiliser la définition de la loi pour avoir l'égalité souhaitée.

9. Ch. X - Produits directs et semi-directs

Proposition 3.1 et Lemme 3.4. Il serait peut-être plus judicieux de noter explicitement la loi de groupe $*$ dans les calculs.

Exemple 3.7. (2). Il serait plus exact de dire $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes D$, où D est le sous-groupe de $\mathrm{GL}_n(K)$ formé des matrices de dilatation et de la matrice identité.

10. Ch. XI - Actions de groupe et structure des groupes finis

Exercice 16. Dans les questions **e.** et **f.**, il est sans doute plus judicieux de demander de démontrer qu'il existe un groupe abélien fini A d'ordre premier à p tel que $Z(G) = (S \cap Z(G)) \odot A$, puis que $G = S \odot A$.

11. ch. XII - Thèmes et variations sur les groupes abéliens

p.380. La remarque « Les exercices ci-après, etc. » doit être placée avant l'exercice 11.

12. Ch. XIV - Propriétés élémentaires des anneaux et des corps

Exemples 3.3. (2). La conclusion manque : l'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est donc pas intègre.

Exemples 3.6. On pourrait rajouter un quatrième exemple. Pour tout $d \in \mathbb{Z} \setminus \{0\}$ sans facteurs carrés, $\mathbb{Q}[\sqrt{d}]$ est un corps (exercice laissé au lecteur).

p.417, haut de page. Dans la définition de e_n, c'est plutôt le terme d'indice n qui vaut 1 (donc le $(n+1)$-ième.

De plus, il faut bien entendu lire $\Big(\sum_{\substack{i,j\geq 0\\ i+j=n}} a_i b_j\Big)_{n\geq 0}$, dans la définition de ss'.

p.417, bas de page. L'écriture $S = \sum_{n\geq 0} a_n X^n$ est un peu cavalière, et ne provient pas « de ce qui précède ». En fait, ce qui précède donne envie d'écrire une telle chose...Il n'y aurait pas de problème si on se limitait aux suites $(a_n)_{n\geq 0}$ à support fini (i.e. aux polynômes). En revanche, il y en a un ici a priori. En fait, la somme $S = \sum_{n\geq 0} a_n X^n$ est à prendre au sens « formel ».

Ce n'est pas une vraie somme (contrairement au cas des polynômes), mais simplement une commodité d'écriture introduite pour pouvoir visualiser un peu mieux les lois définies plus haut. Si on veut donner un vrai sens mathématique, il faudrait introduire une topologie, ce que l'on fait dans le chapitre XXII.

Lemme 6.3. Fin de l'énoncé, il faut lire « est un sous-anneau de $A[[X]]$ ».

Lemme 6.8. et Théorème 6.10. L'hypothèse de commutativité est superflue.

Thm 6.10, démonstration. Juste après l'énoncé de la propriété (H_n), la phrase suivante est superflue. Le cas $f = 0$ ne peut se produire, puisque l'on a supposé $\deg(f) \geq \deg(g) \geq 0$.

D'autre part, pour démontrer l'unicité du reste et du quotient, il y a un argument plus court que celui qui est proposé. Au lieu de supposer $R_2 - R_1 \neq 0$, supposons plutôt que $Q_2 - Q_1 \neq 0$. Alors, on a la même contradiction sur le degré de $R_2 - R_1$, et on obtient directement que $Q_2 - Q_1 = 0$ (sans utiliser l'injectivité de la multiplication par g). On en déduit alors que $R_2 - R_1 = 0$.

Enfin, on s'aperçoit que, si l'on écrit « $a_{n+1}b_m^{-1}$ » partout, l'énoncé devient valable dans n'importe quel anneau, commutatif ou non. D'autre part, en remplaçant « $a_{n+1}b_m^{-1}$ »par « $b_m^{-1}a_{n+1}$ » dans la démonstration, on montre aussi l'existence de polynômes $\tilde{Q}, \tilde{R} \in A[X]$ uniques tels que $f = g\tilde{Q} + \tilde{R}$ et $\deg(\tilde{R}) < \deg(g)$.

Définition 6.18. Stricto sensu, il faudrait rajouter l'hypothèse que A est commutatif, puisque le morphisme d'évaluation n'a été défini que dans ce cadre. Ceci est un peu embêtant au vu de la remarque 6.21, qui utilise la notion de zéro de polynôme à coefficients dans l'anneau non commutatif $\mathbb{H}$.

Pour pallier ce petit écueil, si A est un anneau quelconque et $f \in A[X]$, il suffit de définir $f(a)$ comme suit : si $f = \sum_{n\geq 0} a_n X^n$ et $a \in A$, on pose

$$f(a) = \sum_{n\geq 0} a_n a^n \in A.$$

Attention ! L'évaluation en a n'est plus un morphisme d'anneaux en général si A n'est pas commutatif.

13. Ch. XV - Anneaux quotient

Exemples 2.2. Dans l'exemple (1), on peut aussi rajouter que (0) est maximal si, et seulement si, A est un corps. Dans l'exemple (2), pour démontrer que l'idéal $p\mathbb{Z}$ est maximal, il faut aussi dire que $p\mathbb{Z} \neq \mathbb{Z}$.

Thm 3.13. La phrase « Pour tout $i \in [\![1, n]\!]$, on note $\pi_i : A \longrightarrow A/\mathfrak{a}_i$. » n'a rien à faire dans l'énoncé.

E11, p.477. Il faut bien entendu lire « $\Delta = a^2 - 4b$ ».

E12. Il faut lire ε au lieu de $\overline{\varepsilon}$ dans tout l'énoncé.

14. Ch XVII - Divisibilité dans les anneaux

Lemme 1.11. Il vaut mieux dire « un » pgcd et « un » ppcm partout dans l'énoncé.

Remarque 1.14. De manière générale, si a et b sont deux éléments de A associés, alors a est irréductible si, et seulement si, b l'est. Dans ce cas, on a nécessairement $b = ua$, avec $u \in A^\times$ (ce qui n'est pas nécessairement le cas si a et b sont quelconques, cf. exercice 18).

En effet, supposons que a et b soient associés, i.e. $(a) = (b)$, et supposons que a soit irréductible. Comme a est non nul est non inversible, (a) est non nul et distinct de A. Il en est donc de même de (b), et b est alors non nul et non inversible. Puisque $a \in (a) = (b)$, il existe $c \in A$ tel que $a = bc$. Puisque b est non inversible et a est irréductible, on a $c \in A^\times$.

Il reste donc à montrer le fait suivant : si π est irréductible et $u \in A^\times$, alors $u\pi$ est irréductible. Ceci est laissé en exercice au lecteur.

Définition 1.20. Remarquons que, si a et b sont deux éléments de A associés, alors a est premier si, et seulement si, b l'est (puisque $(a) = (b)$!).

En particulier, si π est premier et $u \in A^\times$, alors $u\pi$ est premier.

Lemme 1.26. Notons que la conclusion du lemme implique que les éléments $\pi'_1, \ldots, \pi'_s$ sont alors premiers, puisqu'associés à des éléments premiers.

Proposition 2.1. L'anneau A doit bien entendu être supposé principal.

Thm 2.4. La phrase « Pour tout $i \in [\![1, n]\!]$, on note $\pi_i : A \longrightarrow A/(a_i)$. » n'a rien à faire dans l'énoncé.

Lemme 2.5. L'hypothèse d'intégrité est superflue. De plus, à la fin de la démonstration, le fait que π soit premier provient plutôt de la **définition** d'un élément premier, et non pas du lemme 1.19.

Lemme 2.9., démo. La démonstration est deux fois trop longue, car prise par le mauvais bout. Voici une version plus courte, qui évite de dire deux fois la même chose.

Soit $a \in A$ un élément non nul et non inversible. Puisque a est non inversible, on a $(a) \neq A$. L'idéal (a) est donc contenu dans un idéal maximal $\mathfrak{m}$ par le théorème de Krull. En particulier, $\mathfrak{m}$ est un idéal premier, non nul (sinon $(a$ serait nul). Écrivons $\mathfrak{m} = (\pi)$. Alors, π est premier, donc irréductible puisqu'un anneau principal est intègre. Mais alors, comme $(a) \subset (\pi)$, on a $\pi \mid a$, et π est un diviseur irréductible de A. Le second point est alors clair.

Algorithme d'Euclide. Il faut lire « on définit des éléments q_i et r_{i+1} ».

Exercice 21 Question b iii). Il faut plutôt lire : montrer que $2(k+2)$ et $(k+2)(2+i\sqrt{d})$ n'ont pas de pgcd.

15. Ch. XVIII- Matrices à coefficients dans un anneau euclidien

Définition 3.17. Dans la définition d'une base, dans la combinaison linéaire, il faut remplacer x_i par e_i.

16. Ch. XXI - Séries formelles

Proposition 3.1., démonstration. En bas de la page 708, il faut lire « $B_k S^{(k)}$ », et non pas $tB_k S^{(k)}$.

17. Ch. XXIV - Polynômes et racines

Thm. 4.12 L'équivalence entre (1) et (3) est fausse. Voici un contre-exemple. On prend $A = \mathbb{Z}[i\sqrt{13}], P = 2X^2 + 2X + 7$. On peut montrer que A intégralement clos. Alors, P est irréductible dans $A[X]$, mais on a

$$P = \frac{1}{2}(2X + 1 + i\sqrt{13})(2X - 1 + i\sqrt{13}) \in K_A[X].$$

Le bon énoncé est donc :

4.12. Théorème. Soit A un anneau intègre. Alors, tout polynôme unitaire irréductible de $A[X]$ reste irréductible dans $K_A[X]$ si, et seulement si, A est intégralement clos.

La première partie de la remarque qui suit est également fausse : le polynôme P précédent fournit un contre-exemple.

18. Ch. XXVII - Nul n'est censé ignorer Galois

p. 931, premier paragraphe . Il y a un « le » en trop dans « dont le groupe de Galois est [...] ».

Exemple 3.3. Il manque un s à « complexe ».

19. Ch. XXVIII - Réduction des endomorphismes

p. 944, Lemme 1.2. Dans le point (1), il faut lire « Id_E » au lieu de « Id_u. »

Proposition 1.19, démo. Il faut lire « $\mu_u(M) = 0$ ».

Thm 3.3. Il faut bien entendu lire « $\lambda_1, \ldots, \lambda_r \in K$ ».

p.971 Démo du thm 3.10.

Juste avant la démonstration de l'unicité, le paragraphe montrant que δ et ν sont des polynômes en u est redondant. Pour la démonstration de l'unicité, il vaut mieux dire « Soit $u = \delta' + \nu'$ une autre décomposition ». En effet, la décomposition $u = \delta + \nu$ est celle construite précédemment, et non pas une décomposition arbitraire.

p. 979, haut de la page. La forme de Jordan de u appartient plutôt à $\mathrm{M}_n(K)$, où $n = \dim_K(E)$ (et non pas à $\mathrm{M}_r(K)$).

p.981. Lorsque l'on explique comme construire une base F_i, il y a un « est une base » en trop.

p. 985 fin du point (2). On répète le procédé jusqu'à avoir une de $\mathrm{Ker}(u - \lambda\mathrm{Id}_E)$ que l'on dispose « à l'étage 1 », et non pas au rez-de-chaussée.

p.1005, Exercice 19. L'indication finale est plutôt « considérer $\mathrm{Ker}(\pi(u))$ » (et non pas $\mathrm{Ker}(P)$).

Cette indication est d'ailleurs plutôt laconique. Plus précisément, considérer $v \in \mathrm{Ker}(\pi(u)) \setminus \{0\}$, et justifier que $E = \mathrm{Vect}_K(v, u(v), \dots, u^{d-1}(v))$, où $d = \deg(\pi)$. Comparer alors les dimensions pour en déduire que $\ell = 1$.

D'ailleurs, une alternative serait démontrer tout d'abord que si $v \in E \setminus \{0\}$, alors $(v, u(v), \dots, u^{n-1}(v))$ soit une base de E (où $n = \dim(E)$, bien sûr), puis que l'on a $\mu_u = \chi_u$. Il est alors aisé de démontrer que μ_u est irréductible en utilisant le lemme des noyaux et la simplicité de u.

p.1010, Exercice 29 b. Il manque un point final.

20. Ch. XXIX - Décomposition de Frobenius

Exercice 6 Question c. Le cas d'une matrice compagnon n'est pas si immédiat. On peut par exemple traduire l'égalité $SM = M^t S$ en termes de coefficients, et montrer que toute solution S est nécessairement symétrique. Justifier alors qu'il y a au moins une solution S inversible (comparer les invariants de similitude de M et M^t), nécessairement symétrique par ce qui précède.

Il existe aussi une solution plus conceptuelle. Si $E = K[X]/(P)$, où P est un polynôme unitaire de $K[X]$, alors la matrice représentative de la multiplication par $\overline{X}$ dans la base $(\overline{1}, \overline{X}, \dots, \overline{X^{n-1}})$ est C_P.

D'autre part, si $P = X^n + a_{n-1}X^{n-1} + \cdots = a_0$, on peut définir des polynômes $H_0, \dots, H_{n-1}$ par

$$H_0 = 1 \text{ et } H_k = XH_{k-1} + a_{n-k} \text{ pour tout } k \in [\![0, n-1]\!].$$

Vérifier alors que $(\overline{H}_{n-1}, \dots, \overline{H}_0)$ est une base de E, que la matrice représentative de la multiplication par $\overline{X}$ dans cette nouvelle base est C_P^t, et que la matrice de passage est symétrique.

21. Ch. XXXII - Théorie des caractères

Exemple 3.6. Il faut lire ≪ la seule décomposition de douze en somme de carrés contenant exactement trois termes égaux à un ≫.