TITRE : OBSERVATIONS WEIL SUR L'ALGÈBRE CHAP. V

Archives

NBL 025

118 2

OBSERVATIONS WEIL SUR L'ALGEBRE CHAP. V

§1, n°1. Je me demande si on ne gagnerait pas en clarté en ne gardant que des corps commutatifs dans ce n°, et mettant à la fin du n° une remarque comme quoi tout reste vrai s'il s'agit de corps non commutatifs. Si on laisse le n° tel quel, alors redire au début du n° 2 que maintenant tout est commutatif.

P.1, ℓ.4."C'est le sous-corps engendré par l'él.un." : je n'ai pas sous la main la définition de "sous-corps engendré par", mais il y a là quelque chose qui me gêne. Le corps premier est tout aussi bien, sauf erreur, le sous-corps engendré par la partie vide de K (et il y a lieu de le dire). Dire seulement que l'intersection P des sous-corps de K n'est pas réduite à 0 parce qu'ils contiennent tous l'unité.

P.2, fin du th.1 : "il existe des corps de toutes car." me paraît mal dit, et peut du reste être omis sans inconvénient.

Au n°1 : Observer dès maintenant qu'un corps fini est de carac. $\neq 0$. Observer aussi que tout corps, comm. ou non, peut être muni d'une structure d'algèbre sur son corps premier. On pourrait, déjà ici, mettre, en proposition, que, le corps étant muni de cette structure, toute dérivation dans le corps s'annule sur le corps premier, ce qui servira plus loin. Je note aussi, dès maintenant, à titre d'exercice à insérer en son lieu (au § 7), que, sur un corps comm. absolument algèbrique (= alg. sur son corps premier), toute dérivation s'annule (N.B. on peut formuler le th. de Wedderburn en disant que, sur un corps, comm. ou non, à un nombre fini d'éléments, toute dérivation s'annule : n'y aurait-il pas une démonstration à baser là-dessus, qu'on pourrait insérer à titre d'exercice dans le présent chapitre ?) .

P.2 : il me paraît fâcheux d'avoir, ici et dans tout le chap., la même lettre p pour la carac. et pour l'exposant carac.; pour ce dernier, je propose π .

P.2 ; l.7 du bas "on sait" (formule du binôme) : donner la référence.

P.3, prop.2 : formuler pour un corps K parfait ou non, sous la forme $(K[X])^p = K^p[X^p]$. Et voir les obs. au sujet de la p. 53 .

P.5, l.5, un membre de phrase omis dans le manuscrit.

P.5, l.7-8, "fini sur K" a-t-il été défini ? de toute manière, il vaudrait mieux dire "de rang fini" .

P.5, l.10 du bas, omettre "on sait que" . P.7, cf. ci-dessous.

P.8, l.1, supprimer "et" dans "et (f) ..." .

P.8, l.13 du bas, lire 0 au lieu de 1 .

P.8, l.6 du bas, lire "soit f le ..."

P.9, l.5 du bas, "x^{-1} devrait être..." est du charabia.

P.10, l.3, lire "Soit E = ..."

P.10, l.9,: en français, on dit "par récurrence".

Sur le début du § 3, la prop.6 p.10, et le début du § 4 (p.11-13) ; je n'ai pas ici le chap.IV, mais je présume qu'il y a été expliqué que l'idéal des relations algèbriques satisfaites, sur K , par une famille d'éléments x_ι d'une extension de K n'est autre que le module des rel.lin. satisfaites par les monomes en les x_ι . Cela posé, il convient de donner ici le premier rôle à l'idéal des relations algèbriques, et de fonder là-dessus des définitions. Donc : un élément est dit transc. (resp., une famille est dite alg. libre) si l'idéal des relations alg. est (0) . Déduire de là, comme conséquence immédiate, la condition néc. et suff. que les monomes sont lin. indép. La prop.6, p.10, doit être formulée pour une extension quelconque, non nécess. alg. (même démonstration), et reportée à la fin du § 2 (ce qui amène d'une manière naturelle l'idéal l'idéal des rel. alg., dont l'étude va être faite dans les §§ suivants), ou si l'on veut au §4. Quelque part, on insèrera que, si E est une extension de K , s'il y a un isomorphisme de E sur E', et si K' est l'image de K par cet isomorphisme, alors : si E est alg. sur K, E' l'est sur K' ; si E est de type fini sur K , E' l'est sur K' ; etc.., etc.

P.11, l.8, au lieu de "Sur E, et soit g..." lire "sur E ; soit g..."

P.11, déf. 4 : supprimer "ou que E est une ext.alg.fermée de K" , et avoir bien soin de ne jamais s'exprimer ainsi, sous peine des plus horribles confusions (jamais personne ne se souviendra de la distinction entre "fermée" et "close").

P.15, l.8, au lieu de prop.3, lire prop.2 .

P.16, l.5, mal dit : supprimer L = L .

P.16, l.10 : "la prop. étant évidente" : cela ne mérite-t-il pas un mot d'explication ? Pour la démonstration, vérifier que le parallélisme avec la démonstration correspondante pour la dimension des esp. vect. est aussi clair que possible, et mettre une remarque pour souligner l'analogie.

P.19, l.2 : lire "... dans Ω ; soit ..." <u>Ne pas</u> rédiger les l. 3-4 avec des resp., mais faire un membre de phrase séparé pour B .

P.19, à la fin de la prop.1, ajouter "et en ce cas il existe un sous-anneau de $K(E \cup F)$, isomorphe à $A \otimes B$, dont $K(E \cup F)$ est le corps des frac."

P.19, l.1 du bas, lire $E(F):E$ au lieu de ...:K

P.20, l.11 du bas, insérer "dans Ω." entre "de K" et "sont" .

P.20, l.7-4 du bas : mal rédigé (çà donne l'impression qu'on l'a déjà fait remarquer pour la disj. lin., ce qui n'est pas le cas).

P.21, l.3, insérer "(sur K)" entre "de E" et "qui soit" (ce n'est pas strictement nécessaire, mais çà facilite beaucoup les choses pour le lecteur ; de même en beaucoup d'autres lieux).

P.24, l.10 "relatifs à K": où ce terme a-t-il été défini ? en tout cas il est plus simple de dire "laissant invariants les él. de K" .

§ 6 : avec la prop.2, p.26, on perd tout le bénéfice de la méthode du produit tensoriel, et on retombe en plein dans la méthode Steinitz par adjonction successive. C'était pas la peine, assurément... Je propose donc : a) de faire remonter la prop.1, p.26, au § 2 (où elle est bien à sa place, en vertu des considérations ci-dessus sur le rôle à faire jouer dans ce § 2 à l'idéal des relations) ; b) de supprimer la prop.2, p.26, et le nom "corps de décomposition" (il n'y a aucun intérêt à avoir un mot pour cela) ; c) dégrader le th.1,p.25, au rang de proposition (il est destiné à être remplacé par le th.4, bien meilleur) ; d) supprimer le cor.2 de la prop.3 (p.28) ; e) au début du n°4, ou à la suite du n°3, démontrer la proposition suivante : Soit E une extension de K ; pour que la fermeture algèbrique F de K dans E soit algèbriquement close, il faut et il suffit que, quelle que soit l'extension K' de K de degré fini, il existe un isomorphisme de K' dans E , laissant invariants les éléments de K . Démonstration : c'est nécessaire (comme pour l'actuelle démonstration de la prop.4) ; c'est suffisant : sinon, d'après (AC"') de la prop.3, il y a une ext. alg. F' de F , non réduite à F ; soit u un élément de F', qui n'est pas dans F ; soit f le polynome minimal de u sur K,et soient $v_1,\dots,v_m$ toutes les racines distinctes de f dans F ; alors $K(u,v_1,\dots,v_m)$ est une extension de K de degré fini, contenue dans F', dans laquelle f a au moins m+1 racines ; il n'y a donc aucun K-isomorphisme de cette extension dans E , car alors f aurait m+1 racines dans E , qui seraient nécessairement dans F : mais f n'a que m racines dans F . Alors, pour démontrer l'actuel th.2, il suffit d'observer (mais c'est nécessaire !) qu'on peut définir une famille d'extensions de K , telle que toute extension de K de degré fini soit

K-isomorphe à une extension de la famille (en effet, il suffit de considérer, pour tous les entiers naturels n , toutes les tables de multiplication définissant une structure d'algèbre commutative sur un espace vectoriel de dimension n sur K ; on obtient bien ainsi, entre autres, toutes les extensions de K de degré fini, et d'ailleurs chacune une infinité de fois, ce qui n'a aucune importance).

Avant d'aller plus loin, je note : p.28, l.3-5 (rem. suivant la déf.1): remplacer par "On notera que, bien entendu, un corps algèbriquement fermé <u>dans une extension donnée de ce corps</u> n'est pas nécessairement algèbriquement clos ; cette dernière notion a un caractère absolu, c'est-à-dire qu'elle ne dépend que de la structure du corps en question, tandis que l'autre est essentiellement relative à l'extension considérée." (N.B. Se garder de tout faire rouler sur la subtile distinction entre "clos" et "fermé" ! cf. plus haut. Et, à la table des matières, au § 3, n°3, lire "Corps algèbriquement fermé dans une extension" au lieu de "Ext. alg. fermées" .

P.29, prop.4 : la combiner avec la prop. indiquée plus haut (en renforçant, dans celle-ci, la condition "nécessaire").

P.30, th.4 : formuler le théorème pour le cas où $K = K'$, et ψ est l'isom. identique ; l'énoncé actuel passe en corollaire (évident au moyen de la prop.6 p.10 modifiée comme il a été dit plus haut). Dans les énoncés, insérer le plus souvent, entre parenthèses, l'indication du corps sur lequel on prend le degré de transc. : "... une extension de K dont le degré de transcendance (sur K) soit ..." .

P.31, l.14 du bas : au lieu de "est un isom.", lire "n'est pas autre chose qu'un isom." ; c'est même comme cela qu'on aurait dû poser la définition (et on aurait dû la donner dès le § 2 !).

P.31, l.7 du bas "le seul isom. de P dans F est l'autom. identique de P": çà aurait dû être fait au § 1, n°1, et çà mérite bien une proposition. Et, aussitôt à la suite de la définition de K-isomorphisme (au § 2!), dire que tout isomorphisme est un P-isomorphisme.

P.31, l.6-5 du bas : et si l'on a plusieurs familles ??? renvoyer, non au défunt th.1 du § 6, mais au th.4 p.30 .

Avant d'aller plus loin, je répare un oubli : je propose qu'on insère, tout au moins en exercice, en ce cas insérer dans le texte un renvoi à l'exerc. (ou même dans le texte, en petits caractères) la démonstration de l'existence de la clôture algébrique que nous avions mise au point à S.Paulo (je rappelle : on considère l'ensemble L des couples (f,m) d'un polynome f, normé, irréductible sur K , et d'un entier m tel que $1 \leqslant m \leqslant \deg(f)$; on identifie avec K la partie de cet ensemble correspondans aux polynomes du 1er degré ; on considère toutes les structures de corps, prolongeant celle de K, qu'on peut mettre sur des parties de L de telle façon que tout élément soit racine du polynome qui forme sa première coordonnée ; et on Zornifie). Cette forme de la démonstration paraît généralement ignorée, et a fort intéressé MacLane et d'autres à qui je l'ai communiquée.

P.32, il revient au même, mais il est plus commode, d'énoncer comme suit : "Si le degré de transc. de E sur K est strict. inf. à celui de Ω , ou si le degré de transc. de Ω sur K est fini ..." De plus, quand l'une de ces conditions est satisfaite, il me semble qu'on peut prolonger, non seulement en un K-endomorphisme, mais en un K-automorphisme. Convient-il de rédiger la proposition ainsi ? ou, comme on ne s'en sert nulle part, cela ne risque-t-il pas de brouiller les idées (en ce cas, mettre çà en exercice, et faire suivre la prop. d'une remarque renvoyant à l'exercice).

P.35, l.11, lire p^e-ièmes ; l.12, lire $K^{p^{-\infty}}$.

P.38, l.8 , lire $\neq$ au lieu de = .

P.38, l.14-4 du bas : je ne sais pourquoi, mais, dans ce texte généralement limpide, ce laïus fait l'effet d'être incompréhensible ; et j'en dirais presque autant de l'énoncé de la prop.7. Je n'ai d'ailleurs, pour l'instant, rien de mieux à proposer.

P.41 : pour le critère de MacLane, une proposition me paraît suffisante.

P.42, l.3 du bas : supprimer le ! (mais il serait bon qu'on eût spécifié, dès la définition des ext. sép., qu'il y a des ext. insép., avec un exemple à l'appui.

P.43 : v. obs. de la p.61 .

P.43, l.1 du bas : ajouter "si un des membres est défini".

P.44, prop.13 : ceci est à bloquer avec les prop.16 et 17, p.46 : si A est un ensemble fini d'éléments de K, alors, pour que K(A) soit séparable sur K , il faut et il suffit que $K(A^p) = K(A)$. Tant qu'à faire, il ne coûterait pas plus cher (à vérifier) de démontrer la prop., qui est utile : si A est un ensemble fini d'éléments d'une extension séparable de K , alors le degré de K(A) sur $K(A^p)$ est p^d si d est le degré de transcendance de K(A) sur K (sinon, en exercice).

P.46, cor.2 de la prop.15 : çà me paraît trivial d'après les définitions.

P.48, n°8 : je propose de supprimer ce n° en tant que tel, ainsi que la définition de "base séparante", et de faire la prop.20 (sans le mot "base sép.") comme conséquence de la théorie des dérivations ; v. plus loin.

P. 50 : cf. les observations faites ci-dessus à propos du § 1,n°1 .

P. 51, l.11 du bas : ne pas se servir de la prop.14 (on n'exclut pas que K soit fini, auquel cas on ne sait pas si la prop.14 est vraie) qui n'a rien à voir. Dire : Si E est monogène, soit E = K(x)... Si E n'est pas monogène, observons d'abord que, comme tout élément x de E appartient à l'extension monogène $K(x)$, l'extension $\bar{D}$ de D à E , si elle existe, est unique. Si E est de degré fini, on peut écrire $E = K(x_1,\dots,x_n)$, et ce qui précède montre qu'on peut, par récurrence sur i, étendre D à une dérivation de $K(x_1,\dots,x_i)$, pour $1 \leqslant i \leqslant n$, donc à une dérivation de E . Enfin, si E est de degré infini, etc.

P.52, l.13, insérer "(sur K)" entre "admet" et "une dérivation".

P.53, l.13, "donc D est nulle": il aurait fallu dire (ou rappeler, si çà a été fait au chap.IV) au début du n°, qu'une dérivation D d'une extension $E = K(x_1,\dots,x_n)$ de K est complètement déterminée par la donnée des Dx_i , et s'annule si les Dx_i sont tous nuls.

P.53, prop.24 : combiner l'énoncé avec celui de la prop.20, p.48, et démontrer comme suit : soit $E = K(x_1,\dots,x_n)$ séparable sur K ; soit $D_1,\dots,D_s$ une base pour l'espace des dérivations ; après avoir fait au besoin une permutation sur les x_i , on peut supposer que $\det(D_i x_j)$ $(i,j=1,\dots,s)$ n'est pas nul. Comme les D_i sont une base, il n'y a donc pas de dérivation D dans E telle que $Dx_1 = \dots = Dx_s = 0$, donc (th.3) E est algèbrique séparable sur $F = K(x_1,\dots,x_s)$, qui est séparable sur K . Quel que soit f dans l'idéal des relations algèbriques (sur K) entre $x_1,\dots,x_s$, on a $\sum_1^s \partial f / \partial x_j . D_i x_j = 0$ $(i=1,\dots,j)$, donc $\partial f / \partial x_j = 0$, c'est-à-dire que les dérivées partielles de f sont aussi dans l'idéal ; en prenant pour f un polynome de plus petit degré $\neq 0$ (par rapport à l'ensemble des variables) dans l'idéal, il s'ensuit que les dérivées partielles de f s'annulent identiquement. En carac. 0 c'est fini : f est constant $\neq 0$, ce qui est absurde, donc l'idéal des relations est (0). En carac. p, on en conclut que f est de la forme $f = \sum c_\lambda Z_\lambda p$, où les c_λ sont des éléments de K , et les Z_λ des monomes en $X_1,\dots,X_s$; d'après le critère de MacLane, on en conclut qu'il y a, dans l'idéal des relations en $x_1,\dots,x_s$, un polynome de la forme $g = \sum c'_\lambda Z_\lambda$, contrairement à la définition de f . Donc, de toute manière, l'idéal des relations est (0), c.q.f.d. Ceci me donne l'occasion d'observer qu'il y a lieu de compléter comme suit la prop.2, p.3 : a) la donner pour les polynomes à un nombre quelconque de variables (bien entendu, c'est évident par récurrence si on l'a pour une variable, mais c'est ainsi qu'il convient de la formuler - sans supposer d'ailleurs que K soit parfait, cf. obs. de la p.3) ; b) donner la condition nécessaire et suffisante pour qu'un polynome ait toutes ses dérivées partielles nulles.

P. 54, l.3 du bas : au lieu de "on a donc f = g" , lire "donc f divise g ; d'ailleurs g divise f (réf.), et par suite f=g" . Pour la réciproque, rédiger comme suit : Réciproquement, soit $x \in E$, $x \notin K$; puisque E ne contient, par hypothèse pas d'autres éléments p-radiciels sur K que ceux de K , il existe un K-endomorphisme u de Ω tel que $u(x) \neq x$; soit v l'isomorphisme de E dans Ω induit sur E par u . Pour tout $y \in E$, v(y) est un conjugué de y sur K , donc $v(y) \in E$ (§7,prop.2) ; par suite on a $v(E) \subset E$; v est donc (prop.1) un K-automorphisme de E , pour lequel x n'est pas invariant.

P.57, l.15 du bas : insérer $f(Z) = (Z-X_1)\dots(Z-X_n)$.

P.59, l.6 du bas : "à coefficients entiers" : dire pourquoi ! (c'est en vertu de la formule de la l. 5, qu'il aurait fallu numéroter).

P.59, l.4 du bas : aller à la ligne pour "On déduit..."

P.60, déf.2 : avant de poser la définition, rappeler d'abord (avec la réf.) pourquoi il y a exactement n isomorphismes de E .

P.60,et la suite : trace et norme : personnellement je préfère $N_{E/K}(x)$, etc.

P.61, l.13-15, "En effet... distincts de F" : cela aurait dû être fait au §7, n°5, p.ex. à la suite de la prop.11 (et à ce propos, je demande qu'on énonce la prop.11 de la p.43 sans la notation $[E:K]_s$, c'est-à-dire "il faut et il suffit que le nombre des K-isom. distincts de E dans Ω soit égal au degré de E sur K , c'est-à-dire qu'on ait $[E:K]_s = [E:K]$ ").

P.63, le lemme d'Artin mérite bien un théorème.

P.64, cor.2 du th.2 : indiquer en remarque que la réciproque est vraie, avec renvoi à un exercice (cf. Artin).

P.66, cor.2 de la prop.10 : reporter à la suite du th.3, et combiner en un seul énoncé avec le cor. de celui-ci.

P.66, th.3, lire : "Soient N une extension galoisienne de K , E une extension quelconque de K , et soit L = E∩N . Les corps ...", et, dans le reste de l'énoncé, dans la démonstration, et la figure, écrire partout L au lieu de E∩N (et omettre "On peut évidemment se borner..." qui devient inutile ; écrire L au lieu de K dans la démonstration).

P.66, l.7 du bas, lire "se prolonge, d'une manière et d'une seule, en..." ; et ajouter qu'on a défini ainsi un isomorphisme entre les groupes de Galois.

P.67, l.4-5 : "l'unicité...évidente" : elle n'est pas, je crois, évidente pour les novices ; il y a là un petit raisonnement qu'on n'aperçoit pas du premier coup si on ne l'a vu au moins une fois.

P.67, l.9 : l'intervention du th. de l'élément primitif me semble indiquer que ce raisonnement n'est pas le bon ; d'ailleurs on n'a pas le droit de l'appliquer, puisqu'on n'a pas supposé L infini. J'ai l'impression qu'il y a là une question de relation primordiale, mais je ne vois pas pour l'instant la bonne démonstration.

P.67, cor. du th.3 : cf. obs. p.66 .

P.69, l.7 : donner une réf. plus précise que " §7, n°4 ".

P.69, note de bas de page : le lecteur qui a l'esprit mal tourné se demandera avec curiosité ce qu'il y a de spécifiquement géométrique à un changement linéaire de variables ! Supprimer la note.

P.70, 1.10, rétablir la phrase omise.

P.72 et suivante : il y a confusion constante entre la carac. et l'exp. car. Dire, une fois pour toutes, que "non multiple de (la carac.) p " est la même chose que "premier à (l'exp. carac.) π ", et adopter une des deux expressions dans tout ce qui suit.

P.73 : il me paraît bien préférable (et, si je ne me trompe, conforme à ce qui se fait d'ordinaire) de faire reposer le th.1 sur le lemme suivant (qui se substitue donc au lemme du texte): Pour qu'un groupe abélien fini soit cyclique, il faut et il suffit que, quel que soit n , il y ait au plus n éléments du groupe satisfaisant à $x^n=1$. (Pour la démonstration, cf. les démonstrations habituelles de l'existence des rac.prim.mod.p , p.ex. dans Hecke ; si je ne me trompe, on prend un élément d'ordre maximal, et on montre qu'il engendre le groupe).

P.74, 1.12, au lieu de "un corps $\overline{F}$" lire "le corps $\overline{F}$" (avec renvoi au n°1) ; et bien indiquer qu'on ne suppose pas $p \neq 0$.

P.74, les dernières 17 lignes paraissent assez mal rédigées.

P.76, 1.1-3, çà mérite d'être fait dans le texte.

P.76, 1.5, au lieu de "nous verrons en effet" lire "nous verrons d'ailleurs" .

P.76, 1.12 : "Le groupe... ayant q-1 él., on a $x^{q-1}=1$..." : ajouter une réf.

P.76, 1.15 : "Ceci montre à la fois l'ex. et l'un." : ni l'un ni l'autre n'est bien clair. Rédiger plus explicitement.

P.76, th.2. Ajouter la structure du groupe multipl. de $\overline{F}$ (cf.p.74), en observant que $\overline{F}^*$ est le gr. mult. des racines de l'unité.

P.77, l. 1-2 : énoncer en prop. (indispensable si l'on veut plus tard pouvoir appliquer le th. de l'él. prim. sans se borner au cas infini).

P.77, th.3 : lire : Théorème 3 (Hilbert). -

P.82,: ajouter (en prop.) la détermination du groupe de Galois, sur le corps premier : a) du corps des racines de l'unité d'ordre ℓ^n, où ℓ est un nombre premier ($\neq p$) , et n parcourt N ; b) du corps de toutes les rac. de l'unité.

J'ajoute qu'au §8, il me paraît un peu saugrenu de faire les fonc. sym. avant la th. de Galois, et que, sauf erreur, on pourrait sans inconvénient, et avec avantage, reporter le n°2 après le n° 4 actuel.

DE PROFUNDIS ...... CORPORIBUS .....
