.LA TRIBU

(Bulletin oecuménique apériodique et bourbachique)

N° 16 - 15 Novembre 1948

COMPTE-RENDU DU CONGRÈS DU FIL DIRECTEUR

(Nancy : 27-30 Octobre 1948)

Présents : Cartan, Chabauty, Chevalley, Dieudonné, Godement, Pisot, Roger, Samuel, Schwartz, et plusieurs cobayes.

Pleurez, chers lecteurs, pleurez ! Le Siva destructeur du complexe bourbachique a démembré les corps ; et il a fallu plus de trois jours pour les remembrer. Pleurez, jeunes cobayes, et fidèles sympathisants, pleurez ! Aucune nourriture imprimée ne sortira de ce Congrès pour apaiser votre fringale de vraie Mathématique.

Tel qu'en Grand Oméga l'isomorphie le plonge
Le surcorps transcendant, séparable, infini,
Voit l'exposant p tû , le critère vomi,
MacLane repoussé. Que le ver noir les ronge !

Car Dieudonné têtu, d'une main sûre longe
Le Grand Fil Conducteur, sans trêve et sans répit,
Car Chevalley rétif s'est à l'instant soumis ;
Cartan ne dit plus rien, et le cobaye songe.

De base et dérivée hostiles, ô grief,
Que notre Fil avec, nous sculpte un bas-relief
Dont l'oeuvre de Steinitz éblouissante s'orne ;

Que tous, dans Oméga, soient immergés, encor
Que Dedekind du moins montre à jamais sa borne
Au ~~xxx~~ nombre d'isomorphe(s), épars dans le Grand Corps.

Le Congrès fut surtout consacré aux Corps commutatifs. Dieudonné s'accrocha obstinément au "fil directeur des isomorphismes" , et joua à maintes reprises la scène classique : "Ttout est rompu, mon gendre!...". Après de laborieuses médiations, l'accord finit par se faire sur un nouveau plan donnant satisfaction à tous les Congressistes. On nota une recrudescence de l'action des démons ennemis de Bourbaki : l'un d'eux n'avait-il pas réussi à troubler les idées de Samuel au point de lui faire confondre un produit d'espaces vectoriels avec une somme directe, d'où un énoncé inexact de la fameuse prop.7 du § 7 ; un autre, par le canal de Chevalley, tenta de prouver au Congrès que le lemme d'Artin était trivial, et il fallut plusieurs heures aux Congressistes abrutis pour s'apercevoir du canular !

Le chapitre "O et o" (ou plutôt son premier paragraphe) subit quelques modifications, exigeant une nouvelle rédaction. Quant aux Equations différentielles, elles furent renvoyées au Congrès de Février, faute de temps.

CORPS COMMUTATIFS .

Nouveau plan :

§ 1. Caractéristique ; corps premiers (avec la formule $(x+y)^p=x^p+y^p$, mais rien d'autre sur les calculs en carac. p).

§ 2. Extensions (avec un n° sur les extensions linéairement disjointes).

§ 3. Extensions algèbriques.

§ 4. Théorèmes d'existence des extensions algèbriques.

§ 5. Extensions transcendantes (où rentre la disjonction algèbrique)

§ 6. Isomorphismes (conjugués, th. de Dedekind, définition des ext. séparables, transitivité des ext. séparables, ext. algèbriques séparables).

§ 7. Théorie de Galois.

§ 8. Applications : racines de l'unité, corps finis, extensions cycliques.

§ 9. Eléments radiciels ; critères de séparabilité ; dérivations (calcul en carac. p , critère de MacLane, bases séparantes).

Appendice I : Fonctions symétriques.

Appendice II : Extensions galoisiennes infinies.

Commentaires généraux : La substance du chapitre est restée pratiquement inchangée : il y a eu très peu d'expulsions et d'additions et seulement sur des points tout à fait secondaires. Par contre, le plan de l'Etat 4 a fait l'objet de très vives critiques : la plupart des Congressistes sont choqués du perpétuel mélange des extensions transcendantes et algèbriques, et trouvent abusif de devoir avaler le critère de MacLane, et tous les calculs où intervient la caractéristique p , pour accéder à la théorie de Galois. On a donc repoussé le plus loin possible tout ce qui a trait à la caractéristique, à l'exception de la formule $(x+y)^p=x^p+y^p$, indispensable pour les exemples d'extensions inséparables, les racines de l'unité et corps finis. L'inconvénient est qu'on ne peut pas démontrer tout de suite que toute extension d'un corps de caract. 0, ou d'un corps fini, est séparable (on le dira naturellement dès le § 6, en renvoyant pour la démonstration au § 9 ; ce sont seulement des exemples, qui ne servent pas aux démonstrations des §§ 6,7 et 8) ; cela ne semble pas un obstacle sérieux, car on peut parfaitement dérouler toutes les propriétés des ext. séparables qui se déduisent de la définition (en particulier la théorie de Galois) sans avoir de critère pratique pour décider si une extension est séparable. Cette manière de faire accentue encore le caractère linéaire des (nouveaux) §§ 6 et 7, puisque la propriété $(x+y)^p = x^p+y^p$ n'y intervient plus ; en particulier, Chevalley a remarqué qu'on peut démontrer la transitivité des extensions séparables (générales) par un raisonnement purement linéaire sur les isomorphismes (qui serait applicable même à des corps non commutatifs, et est donc préférable au raisonnement s'appuyant sur le critère de MacLane).

Détail :

§ 1 : Corps premiers. Caractéristique. Signaler que le corps premier est engendré par $\emptyset$ (en petites lettres, car çà ne sert à rien). Ne pas parler de corps non commutatifs dans le texte du n°1 ; supprimer la dernière phrase du th.1, mais ajouter 4 remarques : 1) il existe des corps de toutes les caractéristiques possibles ; 2) tout corps fini est de caractéristique $\neq 0$; 3) tout sous-corps et tout surcorps a même caractéristique ; 4) extension aux corps non commutatifs. On ne garde du n°2 que la prop.1 et son corollaire ; remarquer que les coefficients du multinôme sont divisibles par p , d'où extension de l'identité à un anneau commutatif de carac. p ; un $\supsetneq$ pour les corps non commutatifs (x et y doivent permuter).

§ 2 : Extensions. Signaler en note de bas de page qu'on change la terminologie du chap.I (où extension = surcorps). Au th.1, dire : "si l'un des membres de (1) est défini, l'autre aussi, et ils sont égaux" Conformément au principe du début du chapitre, énoncer la prop.1 et son corollaire pour une algèbre commutative ; une remarque pour l'extension au cas non commutatif, en signalant que dans les hypothèses de la prop.1, a admet un inverse tout court. Au n°2, la notation KK' est vidée, on admettra K(A,A') au lieu de $K(A \cup A')$; une note de bas de page pour la prop.3 : ça marche pour toutes les structures algèbriques à cause de leur "caractère fini". Introduire la terminologie "sous-extension" ou "corps intermédiaire" et la notion de K-isomorphisme dès le n°1 ; dire aussi que l'inclusion $K \subset L$ pour 2 corps implique que la structure de corps de K est induite par celle de L . Introduire les diagrammes (au n°2) avec des flèches, sans convention de haut et bas, $K \to L$ remplaçant $K \subset L$. Au n°1 dire que tout corps est extension de son sous-corps premier.

Un nouveau n° (3), sur la disjonction linéaire. Commencer par des rappels du chap.III sur la disjonction linéaire et l'isomorphie avec le produit tensoriel ; puis la dernière partie de la prop.2 p. 19 (cas $[F:K]$ fini) bloquée avec le corollaire p.20 ; ensuite, la partie c) de la prop.1, p.19 (la partie a) n'a rien à voir avec la disjonction linéaire, et b) est devenu un rappel du chap.III).

§ 3 : <u>Extensions algèbriques</u>. Dans la déf.1, donner le pas à l'idéal des relations algèbriques, les monomes ensuite. Dire tout de suite après qu'algèbrique signifie $a_0+a_1x+\ldots+a_nx^n=0$. Diviser le th.1 en alinéas ; n'y rien dire des éléments transcendants. Donner la déf. du polynome minimal <u>après</u> le th.1 et non dans le théorème ; préciser que l'isomorphie de K(x) sur $K[X]/(f)$ est une K-isomorphie. Dans la prop.1, dire que le pol. minimal de x sur F divise le pol. minimal sur K .

Au n°2, prop.2 , il aura fallu dire au chap.IV que $K[X]$ n'est pas un corps. On vide la prop.6 qui est une trivialité sur les structures ; de même, les remarques de Weil à ce sujet "si E et E' isomorphes, K' image de K dans E' , E alg. sur K , alors E' alg. sur K' , etc." sont repoussées comme étant de fâcheux américanismes (s'il faut encore dire ces choses-là après avoir fait un chapitre sur les transports de structure, c'était pas la peine, assurément...). N°3 , dans le titre, dire "corps algèbriquement fermé dans un surcorps" et supprimer la parenthèse dans la déf. 4 .

§ 4 : <u>Théorèmes d'existence</u>. On adopte le plan suivant, inspiré des observations Weil.

1) Propriétés des corps algèbriquement clos (prop.3, p.27 et cor.1 ; le cor.3 est repoussé au § 9 , avec les corps parfaits).

2) Le th.1 (th. d'immersion) qui passe en proposition (on commencera par un laïus : "Pour former des corps alg.clos, on va chercher à former des surcorps alg. clos d'un corps donné, et pour cela on va voir qu'on

qu'on peut plonger dans une même extension toutes les extensions de degré fini" . Vider la déf. d'extension composée et la remarque 1 , remanier la remarque 2 .

3) Extensions algèbriquement closes d'un corps. On remplace le cor.2 de la prop.3 et les prop.1 et 2 par l'unique prop. de Weil :
Pour que E soit une ext. alg. close de K , il faut et il suffit qu'on puisse plonger dans E toute extension algèbrique de degré fini de K . La condition nécessaire donne le th. d'unicité de E , la condition suffisante donne le th. d'existence par l'immersion de toutes les ext. algèbriques dans un même corps. Définir le corps des racines d'une équation dans une ext. alg. close (noter qu'il est en général distinct de $K(x_i)$). Le th. de prolongement est réduit aux ext. algèbriques ; ne pas oublier de dire qu'un automorphisme de K se prolonge à sa cloture algèbrique.

§ 5 : Extensions transcendantes. Dans la déf.1, parler d'abord de l'idéal des rel. algèbriques, puis des monômes. La prop.1 passe après la déf.1 . Les 2 lignes qui suivent la déf.2 passent dans cette définition. Pour la terminologie, on dira "extension pure" au lieu de "transcendante pure" , parce que K est extension pure de lui-même, mais non transcendante ; "transcendante pure" signifiera "transcendante et pure" . Définir une "base pure" d'une extension pure comme partie alg. libre B telle que E=K(B) (avec la déf. 2) .

Au n°2 , suivre de plus près l'analogie avec les espaces vectoriels et la souligner ; un peu plus d'explications dans la fin de la prop.2 . Dire que si des éléments sont alg. liés, l'un au moins est algèbrique sur le corps engendré par les autres : c'est indispensable pour la prop.3 . Vider la deuxième phrase de la remarque p.16 .

Au n°3 , on ne fera le th. d'équipotence que pour le cas fini, Chevalley assurant que le th. ne sert jamais dans le cas infini. P.17 dire (avec Z) qu'une extension de degré de transcendance fini n'est pas toujours de type fini. Remonter la remarque du bas de page après la déf.4 . Des corollaires au th.3 (bases, systèmes de générateurs) en conservant le parallélisme avec les espaces vectoriels. On introduit la notation $\dim.\mathrm{al}_K E$ pour éviter toute confusion, $\dim_K E$ par abus de langage. Dans le th.4, dire "si l'un des membres est défini, l'autre aussi ..." .

On insère en nouveau n° à ce § , les extensions alg. disjointes. Définition ; critère symétrique : existence de deux bases de transcendance A,B telles que $A \cap B = \emptyset$, $A \cup B$ alg.libre. Cor.3 de la p.22. Puis critère dissymétrique (prop.3, p.21) et ses cor.1 et 2 . Prop.5 de la p.24 et ses corollaires. Le critère de Chevalley (prop.4 de la p.23) et son corollaire sont vidés sur proposition de leur auteur, qui les déclare inutiles.

Dire qu'on peut toujours immerger dans une ext. alg. close de dimension alg. infinie sur K , deux extensions de K de dim.alg. finie, de sorte qu'elles soient alg. disjointes.

§6. <u>Isomorphismes</u>. <u>Extensions séparables</u>. Nouveau plan :

1) On ne considère, parmi les K-isomorphismes des sous-extensions de Ω , que ceux qui sont des restrictions d'automorphismes de Ω . Dire qu'ils laissent invariant le corps premier. Prop.1 (p.32) pour les extensions E de degré de transcendance fini (avec "automorphisme" de Ω). Corps conjugués, éléments conjugués ; prop.2 de la p.33 , prop.1 de la p. 54 .

2) Nombre de K-isomorphismes d'une sous-extension, notion $[E:K]_s$.
Si $K \subset E \subset F$, σ_i K-isomorphismes de E, τ_j E-isomorphismes de F, les $\sigma_i \tau_j$ sont les K-isomorphismes de F. Corollaire : $[F:K]_s = [F:E]_s [E:K]_s$

3) Th. de Dedekind, avec application $[E:K]_s \leqslant [E:K]$.

4) Définition de la séparabilité (comme p.40) ; cas algèbrique fini : $[E:K]_s = [E:K]$. La séparabilité est de caractère fini ; toute sous-extension est séparable. Dire (avec renvoi au § 9) que toute extension d'un corps de car.0 ou d'un corps fini est séparable. Exemple d'extension non séparable. Transitivité de la séparabilité par la dém.Chevalley (voir ci-dessous).

5) Eléments algèbriques séparables ; tout élément d'une extension alg. séparable est séparable. Equivalence avec "racine simple d'un polynome de $K[X]$" et cor.2 de la p.46. Prop.17 de la p.46, éléments séparables d'une extension algèbrique (prop.19).

6) Th. de l'élément primitif.

<u>Démonstration Chevalley de la transitivité de la séparabilité</u>.
On définit la notion de s-esp. vectoriel séparable V de Ω (toute application K-linéaire de V dans Ω est combinaison linéaire de K-automorphismes de Ω). Remarquer que tout s-esp. de V est séparable, et que si V est séparable, αV aussi pour tout K-automorphisme α de Ω.

Soit $K \subset E \subset F$, E séparable sur K, F séparable sur E. Soit $V \subset F$ un s-esp. de dimension finie sur K, $(v_i)_{1 \leqslant i \leqslant n}$ une base de V sur K, $(v_i)_{1 \leqslant i \leqslant m}$ un système libre maximal <u>sur</u> E extrait de cette base ; soit $v_{m+k} = \sum_k a_{kj} v_j$, $a_{kj} \in E$. Les a_{kj} et K engendrent sur K un s-esp. vectoriel de dimension finie, de base $(\omega_h)_{1 \leqslant h \leqslant s}$. Soit $W = \sum_{h,j} K\omega_h v_j$; ce sous-espace sur K contient V. Il suffira donc de montrer que W est séparable sur K, et pour cela de montrer que l'application linéaire φ telle que $\varphi(\omega_1 v_1)=1$, $\varphi(\omega_h v_j)=0$ pour $(h,j) \neq (1,1)$ est combinaison linéaire de K-automorphisme de Ω . Comme $\sum_j Ev_j$ est séparable sur E , l'application E-linéaire α telle que $\alpha v_1=1$, $\alpha v_j=0$ pour $j\neq 1$ est combinaison linéaire de E-automorphismes. Comme E est séparable sur K , l'application linéaire β telle que $\beta\omega_1=1$, $\beta\omega_h=0$ pour $h\neq 1$, est combinaison linéaire de K-automorphismes ; on a $\varphi=\beta\alpha$, d'où la proposition.

§ 7. Théorie de Galois. On conserve le plan du n°1 ; dans la prop.3, ajouter qu'une extension normale est identique à ses conjuguées, et que deux isomorphismes d'une extension normale N dans un autre corps Ω' appliquent N sur un même corps. Faire aussi la prop.4 pour des extensions galoisiennes ; dire que la plus petite extension normale n'est pas galoisienne si E est non séparable. Faire aussi le cor.2 de la prop.5 pour les extensions galoisiennes. Ajouter le groupe de Galois d'une équation comme groupe de permutations des racines (oublié par le rédacteur). Le n°2 actuel, qui coupe fâcheusement le § , est repoussé plus loin, la norme et trace avant la base normale, et les fonctions symétriques en Appendice.

Au n°2 nouveau (ancien 3), dire en proposition que N est galoisienne sur tout corps intermédiaire. Le lemme d'Artin en théorème avec référence au chap.II, puis énoncer le th. fondamental en calquant sur le chap.II (plus de groupes et corps "associés") (il aura fallu dire au n°1 que $[N:K]$ est l'ordre du gr. de Galois). Le cor.2 de la p. 64 en proposition, vider la remarque qui suit. Remettre en français les prop.9 et 10 et leur démonstration (plus de $k(\Delta)$ ni $g(E)$) ; les démonstrations doivent être évidentes. Le cor.2 de la p.66 combiné avec le th.3 et son corollaire en un seul énoncé ; dans l'énoncé du th.3 , écrire L au lieu de $E\cap N$. La dém. du th.3 comme suit : E(N) étant galoisienne sur E , soit Γ son groupe de Galois ; si les $x_i \in E$

étaient linéairement indépendants sur L et non sur N , il y aurait une relation primordiale $\sum a_i x_i = 0$ à coefficients dans N , d'où pour $\sigma \in \Gamma$, $\sum_i a_i^\sigma x_i = 0$, et comme la relation est primordiale, $a_i^\sigma = a_i$ donc $a_i \in E$, contradiction. En petits caractères, démonstration lorsque $[N:K]$ fini (considèrer le corps des invariants des restrictions à N des automorphismes de Γ , ce qui donne l'isomorphie de Γ et du groupe de Galois de N sur K , d'où la disjonction linéaire).

N° 4 : norme et trace, comme faits, ajouter qu'il y a un élément de trace $\neq 0$ (par Dedekind).

N° 5 : on commence par le th. d'indépendance <u>algèbrique</u> des automorphismes (lorsque K infini) : si $P(\sigma_1(x),\ldots,\sigma_n(x))=0$ pour tout $x \in N$ alors $P=0$: on prend une base (a_i) de N sur K , et $x = \sum_i a_i y_i$, $y_i \in K$, d'où $\sigma_j(x) = \sum_i \sigma_j(a_i) y_i$; on pose $X_j = \sum_i \sigma_j(a_i) Y_i$, substitution linéaire inversible par Dedekind, d'où $P(X)=Q(Y)$; par hypothèse $Q(y_1,y_2,\ldots,y_n)=0$ pour tout $(y_i) \in K^n$, donc $Q=0$ puisque K est infini d'où $P=0$.

On en déduit la base normale en remarquant d'abord que pour que les $\sigma_i(x)$ soient linéairement indépendants sur K , il faut et suffit que $\mathrm{Det}(\sigma_i\sigma_j(x)) \neq 0$ (c'est suffisant à cause de l'existence d'un élément de trace non nulle) ; mais $\mathrm{Det}(\sigma_i\sigma_j(x))$ provient d'un polynome $P(X_1,\ldots,X_n) \neq 0$ par substitution de $\sigma_k(x)$ à X_k , d'où le th. de la base normale.

§ 8 . <u>Applications</u> : <u>racines de l'unité, corps finis, extensions cycliques</u>. Le Congrès, écoeuré par les "rappels" (enticipés!) sur la divisibilité des entiers, se prononce en grosse majorité pour le retour à la dém. Chevalley. Cartan seul tient à une démonstration de type plus classique et propose une version qu'on trouvera en Appendice à ce Compte-rendu. Expliquer davantage la construction des a_n (p. 74) .

La lecture des corps finis et extensions cycliques est ajournée au Congrès de Février.

§ 9. <u>Eléments radiciels ; critères de séparabilité ; dérivations</u>.

Nouveau plan :

1) L'isomorphisme $x \to x^p$. (Contrairement aux propositions de Weil, on conserve p pour la caractéristique et l'exposant caractéristique, en faisant attention, notamment au § 8, de ne pas parler de l'un au lieu de l'autre). Rappel de $(x+y)^p = x^p + y^p$. Corps parfaits (ils sont mieux à leur place ici, où on va les caractériser au n° suivant comme les corps n'ayant que des ext. séparables. Exemples : caract. 0, corps finis, corps alg. clos. Formules $(K[A])^p = K^p[A^p]$, $(K(A))^p = K^p(A^p)$; corollaire : les polynomes de $K[X_1^p, \dots, X_n^p]$ sur un corps parfait sont les puissances p-èmes de polynomes de $K[X_1, \dots, X_n]$. Caractérisation des polynomes de $K[X_1^p, \dots, X_n^p]$: toutes les dérivées partielles nulles. Si (a_i) est une base de $K[A]$ sur K, les a_i^p forment un système de générateurs (linéaire) de $K[A^p]$ sur K, donc de $K(A^p)$ quand A algèbrique sur K.

2) Eléments radiciels (Contrairement à l'avis de Weil, on préfère "radiciel" à "p-radiciel" pour les raisons suivantes : 1° personne n'a jamais appelé "radiciel" un élément racine de $X^k - a$ pour k quelconque, donc aucune confusion n'est possible ; 2° si on introduisait une telle terminologie, on dirait "k-radiciel" et alors "p-radiciel" voudrait dire racine de $X^p - a$). D'abord la prop.3 de la p.33, puis la définition. La prop.3 est elle-même conséquence de la suivante : si x est algèbrique sur K, il existe m tel que x^{p^m} soit racine simple d'un polynome de $K[X]$. Prop. 4,5,6 inchangées ; dire que tout élément d'une extension algèbrique E de K est radiciel sur la plus grande extension séparable contenue dans E, avec l'ordre d'inséparabilité dans le cas fini.

3) Critère de MacLane. Commencer par la prop.7, réduite au cas où elle est vraie (c.-à-d. au cor.2) ; on rappellera la notion de rang d'une partie d'un espace vectoriel. Bloquer le critère de MacLane et son corollaire (il faut que toute partie libre ..., il suffit qu'une base ...). Caractérisation des corps parfaits comme ayant toutes leurs extensions séparables. La prop.12, p.43 en exercice ; son cor.2 en proposition, le démontrer par le critère de MacLane ; en déduire le cor.1 de la p.44 ; le cor.3 a déjà été fait. Bloquer la prop.13 et la prop.16.

4) Dérivations. Il aura fallu, au chap.IV, définir les dérivations d'une sous-algèbre B d'une algèbre A , qui prennent leurs valeurs <u>dans</u> A : p.ex., toute restriction à B d'une dérivation de A (dans A) est une dérivation de B dans A . Alors les prop.21, 22, 23 doivent être faites pour les dérivations de E dans Ω ; corollaire : une dérivation d'une extension E de K est nulle dans toute extension algèbrique séparable de K contenue dans E . Autre corollaire : si E est algèbrique séparable sur K , D une dérivation de E , $\sigma D\sigma^{-1}$ est une dérivation de E pour tout K-isomorphisme σ de E dans Ω , comme elle coïncide avec D sur K , elle est identique à D , d'où D(Tr x)=Tr(D x) pour tout x séparable sur K . Faire la prop.20 et la prop.24 bloquées par la méthode Weil.

<u>Appendice I</u> . Ce qui est fait actuellement dans le texte est jugé insuffisant ; on demande le fait que les polynomes symétriques ont des coefficients entiers par rapport aux S_j , et les questions d'isobares ; les formules de Newton développées ont peu d'intérêt, on préfère les formules récurrentes.

<u>Appendice II</u> . Lecture renvoyée en Février.

SÉRIES FORMELLES.

P.1, rappeler ce qu'est la condition (D). Définir l'algèbre avant ses éléments, dans la déf.1 ; ne pas se borner au cas où $I=[1,p]$ pour le nom "séries formelles à p indéterminées" . P.3, faire d'abord l'application de A dans B , puis application à un sous-anneau (représentation identique de A' dans A). P.4, dire que l'ordre d'un polynome n'est pas son degré, et que 0 a tous les ordres. Avant la substitution de séries formelles dans une autre, définit une somme infinie de séries formelles (d'ordre tendant vers $+\infty$), et l'utiliser dans tout ce qui suit. P.7, donner la formule $1/(1-T) = \sum_{n=0}^{\infty} T^n$ en proposition. Corollaire : dans $K[[X]]$ il n'y a qu'un seul idéal maximal si K est un corps. Introduire la notation $K((X_1,\dots,X_n))$ pour le corps des fractions ; un pour dire qu'on ne peut développer les fractions rationnelles de plus d'une variable, exemple $1/(X+Y)$. P.9 , écrire $D(\prod_i X_i^{n_i}) = \sum_j n_j X_1^{n_1}\dots X_j^{n_j-1}\dots \cancel{X_p^{n_p}} \dots X_p^{n_p} DX_j$. En déduire la formule $\omega(DG) \geqslant \omega(G)-1$ (en lemme aux prop.3 et 4). Bloquer les prop.3 et 4 (existence et unicité du prolongement de D). Pour l'existence, si $F=\sum_{n=0}^{\infty} u_n$ (u_n forme de degré n) on pose $DF = \sum_{n=0}^{\infty} Du_n$, ce qui a un sens puisque $\omega(Du_n) \geqslant n-1$; on vérifie ensuite que $F \rightarrow DF$ est bien une dérivation.

Après le Congrès est arrivée une lettre de Weil demandant qu'on ajoute à cet Appendice le th. des fonctions implicites pour les séries formelles.

On décide de mettre un dernier n° où sera introduite la topologie et où les prop. antérieures seront traduites en langage topologique (complétion de l'anneau de polynomes, sommes infinies, une dérivation est uniformément continue). Exercice d'Eilenberg : extraction de la racine k-ème d'une série inversible si k non multiple de la caractéristique :

par le développement de $(1-X)^{1/k}$ (méthode Pisot : écrire $1-X=(1+a_1X+\ldots+a_nX^n+\ldots)^k$ et montrer par récurrence que $k^{2n-1}a_n$ est entier).

ETUDE LOCALE DES FONCTIONS.

Le Congrès s'aperçoit que le premier relève, non de la technique des groupes, mais bien de celle des anneaux et modules : il n'y a aucune raison de supposer les f. de comparaison strictement positives tant qu'on ne prend pas d'inverses. D'autre part, on se ridiculiserait fatalement en enveloppant toutes ces choses extrêmement simple d'un langage algèbrique savant (bien que certains algèbristes impénitents affirment ne rien comprendre sans ce jargon) ; les relations avec l'algèbre seront donc faites en petits caractères ("gammes bourbachiques"!). On change le signe $\prec$ en $\prec\prec$ (signe des physiciens) pour éviter toute confusion fâcheuse avec $\leqslant$ (les 2 signes n'ont rien à voir). Définir $f \sim g$ pour des fonctions vectorielles, par $\|f-g\| \prec\prec \|g\|$ (et aussi $\prec\prec \|f\|$ ce qui est équivalent et doit être dit).

Au § 2, renverser l'ordre des indices pour se conformer aux applications usuelles. Les fonctions de comparaison g_α prendront leurs valeurs dans $\mathbb{R}$ ou $\mathbb{C}$, les coefficients a_α seront dans un espace vectoriel sur ce corps ; la condition pour l'échelle est $|g_\alpha| \prec\prec |g_\beta|$ si $\alpha > \beta$. Faire la multiplication plus généralement pour une fonction bilinéaire (comme au chap. I).

N-B.- La rédaction rappelle aux membres de Bourbaki que l'emplacement du Congrès de Pâques 1949 doit être fixé en Février, et qu'ils doivent s'occuper d'ici là de recueillir tous renseignements relatifs à cette question (logement, nourriture, tableau noir et salle de travail).

A tous, salut et bénédiction.

Notes de CARTAN
sur le groupe multiplicatif des racines de l'unité
(pour le Chap. V d'Algèbre)

Soit G un groupe abélien, noté multiplicativement, et dont tous les éléments sont d'ordre fini. Notons, pour chaque entier premier p , G_p le sous-groupe des éléments dont l'ordre est une puissance de p .

Lemme.- Le groupe G est somme directe de ses sous-groupes G_p ; l'ordre d'un élément de G est égal au produit des ordres de ses composantes dans les G_p .

Démonstration : la somme des G_p est directe, car si l'ordre d'un élément divise deux entiers premiers entre eux (ici : une puissance de p , et un produit de puissances d'entiers premiers $\neq p$), cet ordre est un, autrement dit l'élément est l'unité du groupe G . Les G_p engendrent le groupe G tout entier : il suffit de montrer que si l'ordre n d'un élément est produit de 2 entiers a et b premiers entre eux, cet élément x est produit d'un élément y tel que $y^a=1$, et d'un élément z tel que $z^b=1$; or il existe 2 entiers λ et μ tels que $\lambda a+\mu b=1$; on a $x=yz$, avec $y=x^{\mu b}$ et $z=x^{\lambda a}$. Reste enfin à montrer que l'ordre d'un élément x de G est égal au produit des ordres de ses composantes x_p dans les G_p ; il suffit de montrer que cet ordre n est un multiple de l'ordre de chaque x_p ; or $x^n=1$ montre que $(x_p)^n$ appartient à la somme des G_q pour $q\neq p$, donc est égal à 1 . C.Q.F.D.

Si G est le groupe multipliant des racines de l'unité dans un corps algèbriquement clos de caractéristique p , alors, pour tout entier premier $q\neq p$, le nombre des éléments dont l'ordre divise q^k est égal à q^k , et cela pour tout k. On va voir que cette propriété détermine brièvement la structure du groupe G . Dans le groupe des éléments dont l'ordre divise q^k , le sous-groupe des éléments d'ordre $\neq q^k$ est celui des éléments d'ordre q^{k-1} ; il a q^{k-1} éléments ; il y a donc $q^k(1-1/q)$

- Suite -

éléments d'ordre q^k exactement ; le groupe $G_{q,k}$ des éléments dont l'ordre divise q^k est donc cyclique ; sa structure est ainsi complètement déterminée. Il en résulte que la structure de G_q est entièrement déterminée : car si on a 2 tels groupes G_q et G'_q , on obtient un isomorphisme de $G_{q,k}$ sur $G'_{q,k}$ par choix d'un générateur dans chacun d'eux, et cet isomorphisme peut se prolonger en un isomorphisme de $G_{q,k+1}$ sur $G'_{q,k+1}$. L'unicité de structure montre, par exemple, que G_q est isomorphe au groupe quotient du groupe additif des fractions dont le dénominateur est une puissance de q , par le sous-groupe des entiers.

Si la caractéristique du corps est nulle, le groupe G des racines de l'unité est isomorphe à la somme directe de tous les G_q précédents, pour toutes les valeurs de q premiers ; si la caractéristique est $p \neq 0$, G est isomorphe à la somme directe de tous les G_q relatifs aux q premiers $\neq p$. Tout groupe jouissant de la propriété que le nombre des éléments dont l'ordre divise n est n (resp. est 1 si n est une puissance de p, n si n est premier à p) est isomorphe au groupe G ; tel le groupe quotient du groupe $\mathbb{Q}$ par le sous-groupe $\mathbb{Z}$ (resp. du groupe additif des fractions de dénominateur premier à p par le groupe $\mathbb{Z}$) .

En particulier, le sous-groupe des éléments dont l'ordre divise n a des éléments d'ordre n (si n non divisible par la caractéristique p quand celle-ci est $\neq 0$) ; il est cyclique ; le nombre de ses générateurs est égal au produit $\prod_i p_i^{\lambda_i}(1-1/p_i)$ si $n = \prod_i p_i^{\lambda_i}$ est la décomposition de n en un produit de puissances de nombres premiers. Ainsi le nombre $\varphi(n)$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est $n\prod_i(1-1/p_i)$.

<u>Remarque</u> sur la rédaction actuelle : on n'y a pas donné l'identité permettant de calculer, de proche en proche, le polynome distingué $F_n(X)$ ayant pour racines les racines primitives n-ièmes de l'unité : (pour n premier à la caractéristique)

$$X^n-1 = \prod_{d/n} F_d(X) .$$

Cette formule est à donner à côté de $n = \sum_{d/n} \varphi(d)$, qui traduit l'égalité des degrés des 2 membres.
