COTE : BKI 02-5.11

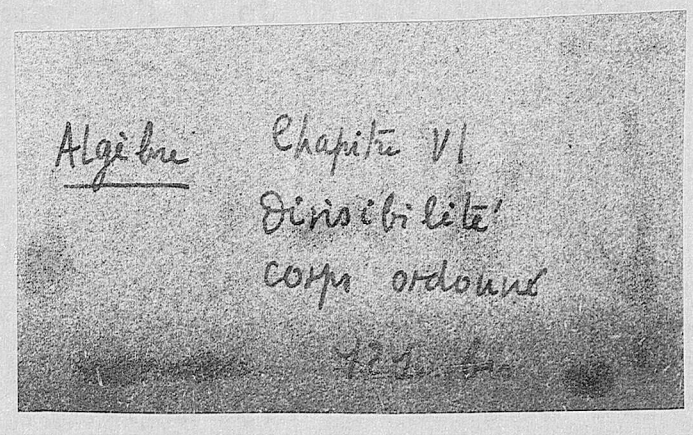
LIVRE II
CHAPITRE VI
DIVISIBILITE

Rédaction n° 121 bis

Nombre de pages : 13

Nombre de feuilles : 13

Université Henri Poincaré - Nancy I
INSTITUT ÉLIE CARTAN - UMR 7502
Bibliothèque de mathématiques
B.P. 239
54506 Vandoeuvre-Lès-Nancy



LIVRE II - CHAPITRE VI

DIVISIBILITÉ

§ 1. Corps ordonnés.

1. Anneaux ordonnés.

DÉFINITION 1.- Etant donné un anneau commutatif A, on dit qu'une structure d'ordre définie sur A est compatible avec la structure d'anneau de A si elle est compatible avec la structure de groupe additif de A, et si elle vérifie l'axiome suivant :

(AO) Les relations $x \geqslant 0$ et $y \geqslant 0$ entraînent $xy \geqslant 0$.

L'anneau A, muni d'une telle structure d'ordre, est dit anneau ordonné.

Exemples : 1) Les anneaux $\mathbb{Z}$ et $\mathbb{Q}$, ordonnés comme il a été dit au Chap.1, sont des anneaux ordonnés.

2) Un produit direct d'anneaux ordonnés, muni de la structure d'ordre produit, est un anneau ordonné. En particulier, l'anneau A^E des fonctions définies sur un ensemble E à valeurs dans un anneau ordonné A, est un anneau ordonné.

3) Un sous-anneau d'un anneau ordonné, ordonné par l'ordre induit, est un anneau ordonné.

Dans un anneau ordonné, les relations $x \geqslant y$ et $z \geqslant 0$ entraînent $xz \geqslant yz$. En effet, ces inégalités sont respectivement équivalentes à $x-y \geqslant 0$, $z \geqslant 0$ et $xz-yz \geqslant 0$. Ce résultat montre que l'ensemble des éléments positifs d'un anneau ordonné forme un monoïde multiplicatif ordonné.

On démontre de façon analogue que les relations $x \leqslant 0$ et $y \geqslant 0$ (resp. $y \leqslant 0$) entraînent $xy \leqslant 0$ (resp. $xy \geqslant 0$). Ces résultats sont

souvent invoqués sous le nom de règle des signes. Ils entraînent que tout carré est positif et, en particulier, que tout idempotent est positif.

2 Par contre, il ne faudrait pas croire que le carré d'un élément non nul est toujours strictement positif, cela peut être en défaut, même pour un anneau totalement ordonné (cf. Exerc...).

Soit P l'ensemble des éléments positifs d'un anneau ordonné A . On sait que P détermine la structure d'ordre de A . Dire que A est un anneau ordonné équivaut à dire que P jouit des propriétés suivantes :

(AP_I) $\quad P+P \subset P$

(AP_{II}) $\quad PP \subset P$

(AP_{III}) $\quad P \cap (-P) = \{0\}$.

En effet, (AP_I) et (AP_{III}) traduisent le fait que le groupe additif de A est un groupe ordonné, tandis que (AP_{II}) n'est autre que (A0).

Rappelons que pour que la relation d'ordre définie sur A soit totale, il faut et il suffit que la propriété suivante soit satisfaite :

(AP_{IV}) $\quad P \cup (-P) = A$.

Rappelons encore que, dans un groupe abélien totalement ordonné, la relation $n.x = 0$ (où n est un entier naturel non nul) entraîne $x=0$; appliqué à un anneau ordonné, cela nous donne la propriété suivante :

Proposition 1 : Un anneau totalement ordonné est de caractéristique

2. Corps ordonnés.

DEFINITION 2 : Un corps commutatif muni d'une structure d'ordre total est dit corps ordonné si sa structure d'ordre et sa structure d'anneau sont compatibles.

Exemples :

1) Le corps Q des nombres rationnels est un corps ordonné.

2) Un sous-corps d'un corps ordonné, ordonné par l'ordre induit, est un corps ordonné.

3)* Le corps des nombres réels est un corps ordonné *.

D'après la proposition 1, tout corps ordonné est de caractéristique nulle.

Dans un corps ordonné, la règle des signes se laisse préciser ainsi : Si l'on a $x>0$ et $y>0$, alors $xy>0$. En effet, on a $xy \neq 0$. Cela montre que $x>0$ équivaut à $x^{-1}>0$, puisque $xx^{-1}=1>0$. Les éléments strictement positifs du corps forment donc un groupe multiplicatif totalement ordonné.

PROPOSITION 2 : Soient A un anneau d'intégrité totalement ordonné et K son corps des quotients. Il existe sur K une structure d'ordre et une seule, induisant sur A la structure d'ordre donnée, et pour laquelle K est un corps ordonné.

Tout $x \in K$ s'écrit sous la forme $x=ab^{-1}$, avec a et b dans A. Si x est positif a et b sont de même signe et réciproquement. On voit donc que s'il existe une relation d'ordre sur K satisfaisant aux conditions prescrites, elle est unique et l'ensemble P de ses éléments positifs est identique à l'ensemble des ab^{-1} où a et b sont des éléments de A de même signe. Reste donc à montrer que cet ensemble P vérifie les conditions (AP_I) ... (AP_{IV}).

Pour (AP_I) et (AP_{II}) c'est évident, ainsi que pour (AP_{IV}).

Pour (AP_{III}), soit une égalité de la forme $ab^{-1}=-cd^{-1}$, d'où $ad+bc=0$. Si l'on suppose que a et b sont de même signe, ainsi que c et d, il en est de même de ad et bc d'après la règle des signes, ce qui montre que $ad=bc=0$, d'où $a=c=0$ et P vérifie bien (AP_{III}).

Exemple : Sur l'anneau Z , il n'existe qu'une seule structure d'ordre compatible avec la structure d'anneau, car 1 doit être >0 d'où par suite $n>0$ pour tout entier naturel $n\neq 0$, et l'on trouve ainsi la structure d'ordre définie au Chap.1. En appliquant la proposition précédente, on voit alors qu'il n'existe sur le corps Q qu'une seule structure d'ordre qui en fasse un corps ordonné.

3. Extensions de corps ordonnés.

DEFINITION 3 : Soit K un corps ordonné, L une extension de K . On dit qu'une structure d'ordre sur L définit sur L une structure d'extension ordonnée de K , si L , munie de cette structure d'ordre est un corps ordonné dont l'ordre prolonge celui de K .

Exemples :

1) Tout corps ordonné est extension ordonnée de Q .
Cela résulte de ce que tout corps ordonné, étant de caractéristique nulle, est une extension de Q , et que, d'autre part, Q ne peut être ordonné que d'une seule manière, comme nous venons de le voir.

2) Soit K un corps ordonné et K(X) le corps des fractions rationnelles d'une variable sur K . Définissons une structure d'ordre sur l'anneau des polynomes K[X] en prenant pour éléments positifs les polynomes dont le terme de plus haut degré est positif. On obtient ainsi un anneau totalement ordonné dont l'ordre prolonge celui de K . En appliquant la prop.2, on définit sur K(X) une structure d'extension ordonnée de K .
* On peut montrer que la relation d'ordre ainsi définie sur K(X) est celle de la croissance au voisinage de $+\infty$ (Cf. Prop. 4 et Livre IV - Chap ...)* .

THEOREME 1 : Pour qu'une extension L d'un corps ordonné K admette une structure d'extension ordonnée de K , il faut et il suffit qu'elle vérifie la condition suivante :

(EO) La relation $p_1x_1^2 + \ldots + p_nx_n^2 = 0$ entraîne $p_1x_1 = \ldots = p_nx_n = 0$, pour tous les systèmes d'éléments x_i de L et d'éléments positifs p_i de K .

(EO) est visiblement équivalent à :

(EO') -1 n'est pas égal à une somme d'éléments de la forme px^2 .

La condition est nécessaire, car $p_1x_1^2 + \ldots + p_nx_n^2 = 0$ entraîne $p_1x_1^2 = \ldots = 0$, puisque tous les px^2 sont positifs, et la relation $px^2 = 0$ équivaut à $px = 0$.

Pour en montrer la suffisance, nous allons définir une relation d'ordre sur L en construisant une partie P de L , satisfaisant à $(AP_I), \ldots, (AP_{IV})$ et contenant K_+ , l'ensemble des éléments positifs de K, Une telle partie P définit bien sur L une structure d'extension ordonnée de K .

Pour définir P , considérons l'ensemble $\mathcal{M}$ des parties de L qui contiennent K_+ ainsi que l'ensemble L^2 des carrés des éléments de L et qui vérifient en outre (AP_I), (AP_{II}), (AP_{III}). $\mathcal{M}$ n'est pas vide car il contient l'ensemble P_0 des $\sum p_ix_i^2$ (que P_0 vérifie (AP_{III}) résulte de (EO)) et est de caractère fini. Prenons alors pour P un élément maximal de $\mathcal{M}$. Il suffit de vérifier que P satisfait à (AP_{IV}), ce qui résulte du lemme suivant :

LEMME : Soient $P \in \mathcal{M}$ et $x \notin P$. Il existe un élément P' de $\mathcal{M}$, tel que $P \subset P'$ et que $-x \in P'$.

Prenons $P' = P - xP$ et vérifions que P' possède les propriétés requises :

Comme $0 \in L^2 \subset P$, on a $P \subset P'$. D'où $L^2 \subset P'$ et $K_+ \subset P'$.

Comme $1 \in L^2 \subset P$, on a $-x \in P'$.

On a $P'+P' = P-xP + P-xP = P+P-x(P+P) \subset P-xP = P'$

On a $P'P' = (P-xP)(P-xP) = PP+x^2PP-x(PP+PP) \subset P+L^2P-xP = P-xP = P'$.

Vérifions enfin (AP_{III}). Supposons que nous ayons une égalité :

$p-xq = -(r-xs)$, où p,q,r,s, appartiennent à P. On en déduit :

$x(s+q) = p+r$, et, si $s+q \neq 0$, $x=(s+q)^{-2}(s+q)(p+r) \in L^2PP \subset P$, contrairement à l'hypothèse ; on a donc $s+q = 0$, d'où $p+r = 0$ et, P vérifiant (AP_{III}), on a : $s=q=r=p=0$, ce qui achève la démonstration

COROLLAIRE. (Théorème d'Artin-Schreier) : Pour qu'il existe sur un corps commutatif L une structure d'ordre compatible avec la structure d'ordre de L, il faut et il suffit que la relation $x_1^2+\ldots+x_n^2 = 0$ entraîne $x_1 = \ldots = x_n = 0$.

La nécessité est évidente. Pour voir la suffisance, remarquons d'abord que la condition de l'énoncé entraîne que le corps L soit de caractéristique nulle, donc puisse être considéré comme une extension de Q. L'axiome (EO) étant vérifié il existe d'après le théorème précédent, une structure d'ordre sur L qui en fait une extension ordonnée de Q, c'est-à-dire un corps ordonné.

4. Extensions algébriques de corps ordonnés.

Soit K un corps ordonné et f(x) un polynome sur K. Nous dirons que f change de signe sur K s'il existe deux éléments $a,b \in K$ tels que $f(a)f(b) < 0$.

PROPOSITION 3 : Soit K un corps ordonné, f un polynome irréductible sur K et changeant de signe sur K. Le corps $L = K[x]/(f)$ admet une structure d'extension ordonnée de K.

Soit n le degré de f , nous raisonnerons par récurrence sur n . Pour n=1 , L = K et le théorème est évident. Supposons-le vrai jusqu'à n-1 et démontrons-le pour n . Sinon, l'on aurait d'après (LO'), une relation de la forme :

$1 + \sum_i p_i f_i^2(x) = 0 \pmod{f(x)}$, où $f_i \in K[X]$ et $p_i \in K_+$.

On peut toujours supposer que les f_i sont de degré n-1 au plus. On a alors : $1 + \sum_i p_i f_i^2(x) = h(x)f(x)$ où h est un polynome de degré inférieur à n-2 .

Si l'on remplace, dans l'égalité précédente, x par a et b , l'on voit que : $h(a)f(a) > 0$ et $h(b)f(b) > 0$. On en conclut que h change de signe en a et b , donc qu'il en est de même de l'un de ses facteurs irréductibles, soit k(x). Mais l'on a :

$1 + \sum_i p_i f_i^2(x) = 0 \pmod{k(x)}$, ce qui montre que le corps $K[X]/(k)$ n'admet pas de structure d'extension ordonnée de K , contrairement à l'hypothèse de récurrence.

Remarque. Il existe des polynomes f sur un corps ordonné K qui sont irréductibles, ne changent pas de signe sur K et sont tels que $K[X]/(f)$ admette une structure d'extension ordonnée de K (Cf.Exer...).

Pour appliquer la proposition précédente, nous aurons besoin du résultat suivant :

PROPOSITION 4 : Soient K un corps ordonné et f un polynome sur K . Il existe un intervalle de K à l'extérieur duquel f est du même signe que son terme de plus haut degré.

On peut se ramener au cas d'un polynome de la forme :

$$f(x) = x^n a_1 x^{n-1} + \ldots + a_n = x^n(1 + a_1 x^{-1} + \ldots + a_n x^{-n}) .$$

Soit $M = \mathrm{Sup}(1, |a_1| + \ldots + |a_n|)$.

Pour $|x| > M$, on a : $1+a_1x^{-1}+\ldots+a_nx^{-n} > 0$, ce qui démontre la proposition.

COROLLAIRE 1: Toute extension algèbrique de degré impair d'un corps ordonné admet une structure d'extension ordonnée.

Une telle extension étant simple d'après le théorème de l'élément primitif (Chap.5,...) est donc isomorphe à $K[X]/(f)$ où f est un polynome irréductible de degré impair. Il suffit alors de montrer que f change de signe, ce qui résulte immédiatement de la proposition précédente.

COROLLAIRE 2: Si a est un élément positif du corps ordonné K , l'extension $K(\sqrt{a})$ admet une structure d'extension ordonnée de K .

Si a est un carré dans K , la proposition est évidente. Sinon, le polynome x^2-a est irréductible et change de signe puisqu'il est négatif pour $x=0$ et du signe de x^2 , donc positif, pour x extérieur à un certain intervalle de K . On applique alors la proposition 3 .

5. Corps ordonnés maximaux.

DEFINITION 4 : Un corps ordonné K est dit maximal si toute extension algèbrique ordonnée de K est identique à K .

Exemple : *On verra plus tard que le corps R des nombres réels est un corps ordonné maximal*.

L'existence de corps ordonnés maximaux résulte du théorème plus précis suivant :

THEOREME 2 : Tout corps ordonné admet une extension algèbrique ordonnée qui soit un corps ordonné maximal.

Soit Ω la clôture algèbrique d'un corps ordonné K , et soit $\mathcal{M}$ l'ensemble des extensions ordonnées de K contenues dans Ω . Ordonnons $\mathcal{M}$ par la relation : L est une extension ordonnée de M . Munie de cette relation, $\mathcal{M}$ est un ensemble ordonné inductif. En effet, si L_i $(i \in I)$ est une famille totalement ordonnée d'éléments de $\mathcal{M}$, le corps $L = \bigcup_{i \in I} L_i$, ordonné en prenant $L_+ = \bigcup_{i \in I} (L_i)_+$, est visiblement la borne supérieure des L_i . $\mathcal{M}$ contient donc un élément maximal M qui est l'extension cherchée.

PROPOSITION 5 : Soit K un corps ordonné maximal et $f \in K[X]$ changeant de signe sur K . Le polynome f admet au moins une racine dans K .

L'un au moins des facteurs irréductibles de f change de signe sur K , soit h . Le corps $K[X]/(h)$ admettant d'après la proposition 3 une structure d'extension ordonnée de K , est confondu avec K et h est donc de degré 1 , non constant, et a une racine dans K .

Remarque : Si a et b sont deux éléments de K tels que $f(a)f(b) < 0$, f admet une racine comprise entre a et b ; pour le voir, on se ramène comme dans la démonstration précédente au cas d'un polynome du premier degré.

La proposition 5 donne en particulier :

PROPOSITION 6 : Tout élément positif d'un corps ordonné maximal a une racine carrée. Tout polynome de degré impair a au moins une racine.

COROLLAIRE : Sur un corps ordonné maximal, il n'existe qu'une seule structure d'ordre compatible avec la structure de corps.

En effet, d'après la première partie de la proposition précédente, tout élément est ou bien un carré, ou bien l'opposé d'un carré.

6. Corps ordonnés maximaux. Théorème d'Artin-Gauss-Schreier.

La propriété qu'exprime la proposition 6 caractérise les corps ordonnés maximaux. De façon plus précise, on a le théorème :

THEOREME 3 (Artin-Gauss-Schreier) : Soit K un corps ordonné. Les trois propriétés suivantes sont équivalentes :

a) Le corps K(i) est algébriquement clos (i désignant $\sqrt{-1}$).

b) Le corps K est ordonné maximal.

c) Tout élément positif de K est un carré et tout polynome de degré impair sur K a une racine dans K .

L'implication a) $\Rightarrow$ b) est évidente, car K n'a, à une isomorphie près, que deux extensions algébriques, K lui-même et K(i) qui ne peut être ordonné.

L'implication b) $\Rightarrow$ c) n'est autre que la proposition 6 .

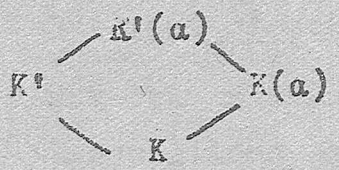
Il nous reste à démontrer que c) $\Rightarrow$ a). Cela résulte des trois propositions suivantes :

PROPOSITION 7 : Soit K un corps ordonné dans lequel tout élément positif est un carré. Alors tout élément de K(i) est un carré.

Soit $a+bi$ (a et $b \in K$) un élément quelconque de K(i). Cherchons un élément $x+yi$ tel que $(x+yi)^2 = a+bi$; cela se traduit par $x^2-y^2=a$ et $2xy = b$. On en tire : $(x^2+y^2)^2 = a^2+b^2$. Désignons par c la racine carrée positive de a^2+b^2 , c est supérieur à a et b et l'on a : $x^2+y^2=c$. D'où $x^2=1/2(c+a)$ et $y^2=1/2(c-a)$. Comme l'on a remarqué que c était supérieur à a , ces équations sont résolubles dans K et si x_o et y_o en sont des solutions, on a : $2x_oy_o = \pm b$. En changeant au besoin le signe de l'un d'eux, on voit que l'on a obtenu la racine carrée cherchée

PROPOSITION 8 : Soit K un corps commutatif (de caractéristique quelconque) tel que tout polynome sur K de degré impair ait une racine dans K . Le corps K(i) jouit de la même propriété.

Si $i \in K$, la proposition est évidente (c'est le cas si la caractéristique est deux car $i=1$). Sinon, soit $P(x)$ un polynome de degré impair n, à coefficients dans $K'=K(i)$ et irréductible sur K'. On va montrer que $n=1$.



Pour cela, soit α une racine de $P(x)$ dans une extension convenable de K' .

On a : $\begin{cases} \left[K'(\alpha):K(\alpha)\right] \leqslant \left[K':K\right] = 2 \\ \left[K'(\alpha):K\right] = \left[K'(\alpha):K'\right].\left[K':K\right] = 2n = \\ \qquad = \left[K'(\alpha):K(\alpha)\right].\left[K(\alpha):K\right] . \end{cases}$

Supposons d'abord que $\left[K'(\alpha):K(\alpha)\right] = 2$, c'est-à-dire que $i \notin K(\alpha)$. On a alors, par la deuxième équation, $\left[K(\alpha):K\right] = n$ et le polynome minimal de α sur K est un polynome irréductible sur K et de degré n , d'où $n=1$.

Supposons maintenant que $\left[K'(\alpha):K(\alpha)\right]=1$, c'est-à-dire que $i \in K(\alpha)$. On a alors $\left[K(\alpha):K\right] = 2n$ et soit $Q(x)$ le polynome minimal de α sur K . Q est irréductible et de degré $2n$. Soit $Q(x) = \prod (x-\alpha_i)$ la décomposition de Q en facteurs du premier degré dans une extension convenable de K . Posons $S(x) = \prod_{1 \leqslant i < j \leqslant 2n} (x-\alpha_i-\alpha_j)$. Les coefficients de S étant des fonctions symétriques des α_i , appartiennent au corps K ; S étant de degré $n(2n-1)$, donc impair, a une racine $u \in K$. Posons : $Q'(x)=Q(u/2+x)$. Q' a donc deux racines opposées. Le pgcd de $Q'(x)$ et de $Q'(-x)$ est donc de degré au moins 1, ce qui prouve, Q' étant irréductible, que $Q'(x) = c.Q'(-x)$ et $c=1$ comme on le voit en examinant les termes de plus haut degré et en utilisant le fait que Q' est de degré pair. On voit alors que Q' ne contient pas de puissances de x d'exposant impair, ce qui permet d'écrire $Q'(x) = R(x^2)$; R doit être irréductible, puisque Q' l'est, et comme son degré est n , donc impair, c'est que $n=1$ ce qui achève la démonstration.

PROPOSITION 9 : Soit K' un corps de caractéristique différente de deux tel que :

1°- Tout polynome de degré impair a au moins une racine.

2°- Tout élément de K' est un carré.

Alors K' est algèbriquement clos.

Nous allons montrer, par récurrence sur l'entier naturel p, que tout polynome irréductible de degré $2^p q$ (q impair) a une racine. C'est vrai si p=0 . Supposons le vrai pour p-1. Soit Q(x) un polynome irréductible de degré $2^p q=n$, et de racines a_i dans une certaine extension de K' . Formons comme précédemment le polynome S(x) qui a pour racines les a_i+a_j $(i < j)$. Il est de degré $\frac{n(n-1)}{2} = 2^{p-1}q'$ (q' impair) et a donc une racine $u \in K'$ d'après l'hypothèse de récurrence. Si nous posons $Q'(x)=Q(u/2 + x)$, nous obtenons encore un polynome de la forme $R(x^2)$, R étant de degré $2^{p-1}q$. R a alors une racine $y \in K'$, on en prend une racine carrée z et u/2 + z est une racine de Q dans K', ce qui achève la démonstration du théorème 3 .

Le théorème 3 nous permet de déterminer tous les polynomes irréductibles sur un corps ordonné maximal :

PROPOSITION 10 : Si K est un corps ordonné maximal, les seuls polynomes irréductibles sur K sont ceux du premier degré et ceux du second degré, ax^2+bx+c , tels que $b^2-4ac < 0$.

K(i) étant algèbriquemon clos, toute extension algèbrique de K est de degré 2 au plus. Tout polynome irréductible est donc de degré 1 ou 2. Pour voir quels sont les polynomes du second degré qui sont irréductibles, il suffit d'écrire l'identité : $ax^2+bx+c = a\left[(x+b/2a)^2-(b^2-4ac)/4a^2\right]$, appelée souvent forme canonique du trinôme.

Remarque - L'identité précédente donne le résultat plus fort que voici : Etant donné un corps ordonné K , pour qu'un polynome du second degré sur K , ax^2+bx+c ait un signe constant sur K , il faut et il suffit que $b^2-4ac < 0$, et le signe du polynome est alors celui de a .
