RÉSUMÉ DU COURS D'ALGÈBRE LC5 (2002 – 2003): PRINCIPAUX THÉORÈMES ET DÉFINITIONS.

A.PAJITNOV

CHAPITRE 1. THEORIE DE GROUPES

Groupes, sous-groupes, homomorphismes

Définition. On appelle *groupe* un ensemble G muni d'une application $\mu : G \times G \to G$ vérifiant les trois conditions ci-dessous:

$$\forall x, y \in G : \mu(x, \mu(y, z)) = \mu(\mu(x, y), z) \tag{1}$$

$$\exists e \in G : \forall x \in G : \mu(x, e) = \mu(e, x) = x \tag{2}$$

$$\forall x \in G\ \exists y \in G : \mu(x, y) = \mu(y, x) = e \tag{3}$$

L'élement e est appelé *l'élement neutre*. L'élément y vérifiant (3) est appelé *l'inverse de* x. Si $\mu(x, y) = \mu(y, x)$ pour tout x, y on dit que G est *abélien*.

On utilise souvent la notation $x \cdot y$ ou xy au lieu de $\mu(x, y)$. L'élément neutre est noté 1. L'élément inverse à x est noté x^{-1}. Pour un groupe G abélien, on utilise souvent la notation $x + y$ au lieu de $\mu(x, y)$, l'élément neutre est noté 0, et l'élément inverse à x est noté $-x$.

Exemple. L'ensemble de toutes les bijections de l'ensemble $[[1, n]]$ sur lui-même est un groupe par rapport à la loi de composition $\mu(f, g) = f \circ g$. Ce groupe est noté S_n et appelé *groupe symétrique*.

Définition.
1. Un sous-ensemble H d'un groupe G est dit *sous-groupe de* G si $1 \in H$, pour tous $x, y \in H$ on a $xy \in H$, et pour tout $x \in H$ on a $x^{-1} \in H$.
2. Une application $f : G \to H$ est dite *homomorphisme* si pour tout $x, y \in G$ on a $f(xy) = f(x)f(y)$.
3. Un homomorphisme injectif est aussi appelé *monomorphisme*; un homomorphisme surjectif est aussi appelé *épimorphisme*; un homomorphisme qui est injectif et surjectif est appelé *isomorphisme*; on dit que deux groupes G, H sont *isomorphes* et on écrit $G \approx H$, s'il existe un isomorphisme $G \to H$.

4. Soit $\phi : G \to H$ un homomorphisme. On appelle *noyau de* ϕ et on note $\operatorname{Ker}\phi$ le sous-groupe $\{x \in G \mid \phi(x) = 1\}$. On appelle *l'image de* ϕ le sous-groupe $\phi(G)$ de H.
5. Soit G un groupe. S'il est fini, la cardinalité de G est appelée *ordre* de G, et noté $|G|$.

Proposition. $|S_n| = n!$.

Théorème (Lagrange). *L'ordre d'un sous-groupe d'un groupe fini divise l'ordre du groupe.*

Définition. Soit G un groupe et $x \in G$. *L'ordre de* x est le plus petit entier n positif non nul, tel que $x^n = 1$. L'ordre de x est noté $|x|$. Si un tel entier n'existe pas, on dit que *x est d'ordre infini.*

Proposition. *Soit G un groupe fini. Alors tout élément x de G et d'ordre fini, et l'ordre de x divise l'ordre de G.*

Définition. Soit G un groupe, $K \subset G$ un sous-ensemble. Le plus petit sous-groupe de G contenant K est appelé *le sous-groupe engendré par* K, et noté $\langle K \rangle$. S'il existe un sous-ensemble fini $K \subset G$ tel que $\langle K \rangle = G$ on dit que G est *de type fini.* S'il existe un sous-ensemble $K \subset G$ de cardinalité 1 tel que $\langle K \rangle = G$ on dit que G est *cyclique* ou *monogène.*

Définition. Soit G un groupe, $H \subset G$ un sous-groupe.

1. L'ensemble quotient de G par rapport à la relation d'équivalence
$$x \sim y \Leftrightarrow x^{-1}y \in H$$
est appelé *l'ensemble des classes à gauche de G modulo H* et noté G/H.
2. On dit que H est *normal* (ou *distingué*) si pour chaque $g \in G$ on a $gHg^{-1} \subset H$.

Théorème. *Soit $H \subset G$ un sous-groupe normal. Alors*

1. *G/H a une structure de groupe telle que la projection $\pi : G \to G/H$ est un homomorphisme.*
2. *Soit $\phi : G \to G'$ un homomorphisme tel que $H \subset \operatorname{Ker}\phi$. Alors il existe un unique homomorphisme $\phi' : G/H \to G'$ tel que $\phi' \circ \pi = \phi$.*

Proposition. *Tout groupe cyclique est isomorphe au groupe quotient $\mathbf{Z}/n\mathbf{Z}$ pour un certain $n \in \mathbf{Z}$ (le cas $n = 0$ correspond au groupe cyclique infini).*

Groupes abéliens de type fini

Définition. 1. Un groupe abélien est dit un *groupe de torsion* si tout élément de G est d'ordre fini.

2. Soit G un groupe abélien. Une suite finie $(e_1, ..., e_n)$ des éléments $e_i \in G$ est appelée *base* de G, si pour chaque $x \in G$ il existe un unique n-uplet $(a_1, ..., a_n) \in \mathbf{Z}^n$, tel que
$$x = \sum_{i=1}^{n} a_i e_i.$$
On dit qu'un groupe abélien est *groupe abélien libre de type fini* s'il a une base.

Théorème. *Tout sous-groupe d'un groupe abélien libre de type fini est un groupe abélien libre de type fini. Tout groupe abélien libre de type fini est isomorphe à $\mathbf{Z}^n$ pour un certain entier n. Si $\mathbf{Z}^n \approx \mathbf{Z}^m$, alors $m = n$.*

Définition. Soit G un groupe abélien libre de type fini. Le nombre n tel que $G \approx \mathbf{Z}^n$ est appelé *rang de G*.

Théorème. *Tout groupe abélien de type fini est isomorphe à la somme directe $L \oplus T$ où L, T sont des groupes abéliens de type fini, et L est libre, T est de torsion.*

Définition. Soit G un groupe abélien, soit p un nombre premier. On note G_p le sous-groupe de G constitué par tous les éléments dont l'ordre est une puissance de p.

Théorème. *Soit G un groupe fini abélien. Alors*
$$G \approx \bigoplus_{p||G|} G_p. \tag{4}$$

Définition. La décomposition (4) est appelée *décomposition primaire* du groupe G.

Théorème. *Soit G un groupe abélien fini. Alors il existe une unique suite finie des entiers $a_i > 1$, tels que $a_i | a_{i+1}$ pour tout i, et*
$$G \approx \mathbf{Z}/a_1\mathbf{Z} \oplus \mathbf{Z}/a_2\mathbf{Z} \oplus ... \oplus \mathbf{Z}/a_m\mathbf{Z}. \tag{5}$$

Définition. La décomposition (5) est appelée *décomposition canonique*.

Action de groupes sur les ensembles.

Définition. Soit G un groupe, X un ensemble. Une application ϕ : $G \times X \to X$ vérifiant les deux conditions ci-dessous est appelée *action à gauche de G sur X*:

$$\phi(gh, x) = \phi(g, \phi(h, x)) \quad \forall x \in X,\ \forall g, h \in G;$$
$$\phi(1, x) = x \quad \forall x \in X.$$

On écrit souvent gx au lieu de $\phi(g, x)$. Un ensemble X muni d'une action d'un groupe G est appelé *G-ensemble.*

Exemple. Soit G un groupe, $H \subset G$ un sous-groupe. La formule $\phi(g, [x]) = [gx]$ définit une action de G sur l'ensemble G/H.

Définition. Soit $\phi : G \times X \to X$ une action de G sur X.

1. Pour $x \in X$ l'ensemble $\{\phi(g, x) \mid g \in G\}$ est appelé *orbite de x*, il est noté $\mathcal{O}_x$.
2. Un ensemble $Y \subset X$ est dit *invariant* si pour tout $y \in Y$ et tout $g \in G$ on a: $\phi(g, y) \in Y$.
3. Un élément $x \in X$ est dit *point fixe* de l'action, si $\phi(g, x) = x$ pour tout $g \in G$.
4. On dit que l'action ϕ est *transitive* si X est l'orbite d'un point $x \in X$.
5. Pour $x \in X$ le sous-groupe $\{g \in G \mid \phi(g, x) = x\} \subset G$ est appelé *stabilisateur de x* et noté $St_G(x)$.

Exemple. Soit G un groupe. La formule $\phi(g, x) = gxg^{-1}$ définit une action de G sur lui-même qui est appelé *l'action par conjugaison.* Les orbites de cette action sont appelés *classes de conjugaison.*

Théorème (Cayley)**.** *Soit G un groupe fini. Alors il existe n, tel que G soit isomorphe à un sous-groupe de S_n.*

Définition. Deux G-ensembles X, X' sont dits *isomorphes* s'il existe une bijection $A : X \to X'$ qui vérifie $A(\phi(g, x)) = \phi'(g, A(x))$ pour tout $g \in G$ et tout $x \in X$.

Proposition. *Chaque G-ensemble transitif est isomorphe au G-ensemble G/H pour un certain sous-groupe $H \subset G$.*

Théorème (Formule des classes)**.** *Soit G un groupe fini. Alors*

1. $$|G| = |Z(G)| + \sum_{C \in \mathcal{A}} \text{card } C$$
   où $\mathcal{A}$ est l'ensemble de toutes les classes de conjugaison C avec card $C \neq 1$.

2. *Pour chaque classe de conjugaison C on a*

$$\text{card } C = \frac{|G|}{|C_G(x)|}$$

où x est un élément quelconque de C, et $C_G(x)$ est son stabilisateur par rapport à l'action par conjugaison.

Théorème. *Soit G un groupe fini non trivial, dont l'ordre est une puissance d'un nombre premier p. Alors le centre de G est non trivial.*

Théorème. *Soit p un nombre premier. Alors tout groupe d'ordre p^2 est abélien.*

Définition. Soit G un groupe fini. Soit p^n la plus grande puissance de p divisant $|G|$. On appelle *p-sous-groupe de Sylow de G* un sous-groupe dont l'ordre est p^n.

Théorème. *Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Alors il existe au moins un p-sous-groupe de Sylow dans G.*

Groupes symétriques

Définition. Une permutation $\sigma \in S_n$ est appelée *cycle* s'il existe un sous-ensemble

$$A = \{a_1, a_2, ..., a_k\} \subset [[1, n]] \quad \text{avec} \quad k > 1$$

tel que

$$\sigma(x) = x \quad \text{pour} \quad x \in [[1, n]] \setminus A$$

et

$$\sigma(a_i) = a_{i+1} \quad \text{pour} \quad 1 \leqslant i < k; \quad \sigma(a_k) = a_1.$$

Le nombre k est appelée *longueur* ou *l'ordre* du cycle σ. L'ensemble A est appelé *support de σ.*

Définition. 1. Les cycles d'ordre 2 sont dits *transpositions.*
2. Deux cycles σ_1, σ_2 sont dits *disjoints* si supp $\sigma_1 \cap$ supp $\sigma_2 = \emptyset$.

Théorème. *Soit $\sigma \in S_n$. Alors il existe une partition $[[1, n]] = X_0 \sqcup X_1 \sqcup X_2 \sqcup ...X_k$ et des cycles $\sigma_1, ..., \sigma_k$, tels que*

1. $\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_k$;
2. $\sigma|X_0 = id|X_0$ *et* supp $\sigma_i = X_i$;
3. σ_i *commute avec* σ_j *pour tout* i, j;
4. $|\sigma| = PPCM(|\sigma_1|, ..., |\sigma_k|)$.

Définition. Soit $\sigma \in S_n$. On dit que σ *présente une inversion en* (i,j) (où $i,j \in [[1,n]]$) si $i<j$ et $\sigma(i)>\sigma(j)$. Le nombre

$$\varepsilon(\sigma) = (-1)^{\nu(\sigma)},$$

où $\nu(\sigma)$ est le nombre des inversions de σ, s'appelle *signature de* σ.

Une permutation $\sigma \in S_n$ est dite *paire* si $\varepsilon(\sigma)=1$, elle est dite *impaire* si $\varepsilon(\sigma)=-1$.

Proposition.

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau);$$

$$\varepsilon(\sigma) = \operatorname{sgn} \prod_{i<j} \Big(\sigma(i)-\sigma(j)\Big).$$

CHAPITRE 2. ANNEAUX ET CORPS

Anneaux, sous-anneaux, idéaux, corps

Définition. *Un anneau* est un ensemble A muni de deux lois de composition, la première appelée *addition* et notée $+$, la seconde appelée *multiplication* et notée $\cdot$, vérifiant les propriétés suivantes:

1. L'addition définit sur A une structure d'un groupe abélien.
2. La multiplication vérifie les propriétés suivantes:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \ \forall x, y, z \in A$$
$$\exists e \in A : e \cdot x = x \cdot e, \ \forall x \in A$$
$$x \cdot (y + z) = x \cdot y + x \cdot z, \ \forall x, y, z \in A$$
$$(y + z) \cdot x = y \cdot x + z \cdot x, \ \forall x, y, z \in A$$

On écrit souvent xy au lieu de $x \cdot y$. L'élément neutre pour l'addition est noté 0, et l'élément e est souvent noté 1.

On dit qu'un anneau A est *commutatif*, si $xy = yx$ pour tout $x, y \in A$. Par la suite nous ne considérerons que des anneaux commutatifs.

Définition. Un élément $x \in A$ est dit *inversible* s'il existe un élément $y \in A$ avec $xy = 1$. Un anneau A est appelé *corps* si $1 \neq 0$ et chaque élément non-nul est inversible.

Définition.
1. Soit A un anneau. Un sous-ensemble $B \subset A$ est dit *sous-anneau* de A si B est un sous-groupe de A par rapport à la loi d'addition, $1 \in B$ et $x, y \in B \Rightarrow xy \in B$.
2. Soit A, A' des anneaux. Une application $\phi : A \to A'$ est dite *homomorphisme d'anneaux* si $\phi(x+y) = \phi(x)+\phi(y)$ $\forall x, y \in A$, et $\phi(1_A) = 1_{A'}$, et $\phi(xy) = \phi(x)\phi(y)$ $\forall x, y \in A$.
3. Un homomorphisme injectif est aussi appelé *monomorphisme*; un homomorphisme surjectif est aussi appelé *épimorphisme*; un homomorphisme qui est injectif et surjectif est appelé *isomorphisme*;
4. On dit que deux anneaux A, A' sont *isomorphes* et on écrit $A \approx A'$, s'il existe un isomorphisme $A \to A'$.
5. Un élément x d'un anneau A est dit *diviseur de zéro* si $x \neq 0$ et il existe $y \in A, y \neq 0$ avec $xy = 0$.
6. Un anneau est appelé *intègre* si $1 \neq 0$ et s'il n'a pas de diviseurs de zéro.

Théorème et Définition. Soit A un anneau intègre. On définit une relation d'équivalence sur l'ensemble $Z = A \times (A \setminus \{0\})$ par la formule suivante:

$$(p, q) \sim (p', q') \quad \text{si} \quad pq' = p'q$$

On définit deux lois de composition sur Z:

$$(p,q)+(p',q')=(pq'+p'q,qq'), \quad (p,q)\cdot(p',q')=(pp',qq').$$

Ces deux lois déterminent une structure d'anneau sur l'ensemble quotient $Z/\sim$. Cet anneau est appelé *corps des quotients* de A. L'application de l'anneau A dans son corps des quotients K qui associe à chaque a la classe d'équivalence de $(a,1)$ dans K est injective.

Corollaire. *Soit A un anneau intègre. Alors il existe un monomorphisme de A dans un corps.*

Définition. Soit A un anneau.

1. Un sous-ensemble $I\subset A$ est appelé *idéal* de A, si pour tout $x\in I$ et tout $y\in A$ on a $xy\in I$.
2. Soit $x\in A$. L'ensemble $\{yx \mid y\in A\}$ est appelé *idéal principal engendré par x*, et noté Ax ou encore (x).
3. Soit $x_1,...,x_k\in A$. Le plus petit idéal contenant tous les x_i est appelé *l'idéal engendré par $x_1,...,x_k$*, et noté $(x_1,...,x_k)$.
4. Soit $I\subset A$ un idéal, tel que $I\neq A$. On dit que I est *maximal*, s'il n'existe pas d'idéal J de A avec $I\subset J\subset A$ et $I\neq J$, $J\neq A$.
5. Soit $I\subset A$ un idéal, tel que $I\neq A$. On dit que I est *premier* si $xy\in I$ implique $x\in I$ ou $y\in I$.

Proposition. *Tout idéal maximal est premier.*

Théorème. *Soit I un idéal d'un anneau A. Alors le groupe quotient A/I (par rapport à l'addition) a une structure d'anneau, tel que la projection $A\to A/I$ est un homomorphisme d'anneaux. Pour tout homomorphisme d'anneaux $\phi: A\to B$ tel que $I\subset \mathrm{Ker}\ \phi$ il existe un unique homomorphisme $\psi: A/I\to B$ tel que le diagramme suivant soit commutatif:*

$$\begin{tikzcd} A \arrow[rr, "\phi"] \arrow[dr] & & B \\ & A/I \arrow[ur, "\psi"'] & \end{tikzcd}$$

Proposition. *Soit I un idéal de A.*

1. *I est maximal si et seulement si A/I est un corps.*
2. *I est premier si et seulement si A/I est un anneau intègre.*

Proposition. *Soit $I=n\mathbf{Z}$ un idéal de $\mathbf{Z}$, et $n\in\mathbf{N}$. Alors trois propriétés sont équivalentes:*

1. *I est premier.*
2. *I est maximal.*

3. *n est un nombre premier.*

Définition. 1. Soit A un anneau. Soit $a, b \in A, a \neq 0, b \neq 0$. On dit que a divise b et on écrit $a|b$), s'il existe $c \in A$, tel que $b = ac$. Un élément $c \in A$ est appelé *pgcd* de a, b si $c|a, c|b$ et pour chaque $d \in A$ avec $d|a, d|b$ on a $d|c$.
2. Deux éléments $a, b \in A$ sont appelés équivalents, et on écrit $a \sim b$, s'il existe un élément $y \in A$ inversible, tel que $a = by$.

Proposition. *Soit c un pgcd de deux éléments a, b. Soit c' un autre pgcd de a, b. Alors $c \sim c'$.*

Si c est pgcd de a et b, on écrit $c \sim pgcd(a, b)$.

Anneaux principaux

Définition. L'anneau A est dit *principal* si A est intègre et chaque idéal de A est principal.

Soit A un anneau principal.

Proposition. *Soit $a, b \in A,\ a \neq 0, b \neq 0$. Soit $(c) = (a, b)$. Alors $c \sim pgcd(a, b)$. Il existe $x, y \in A$ tels que $c = ax + by$.*

Proposition. *Soit $c, x, y \in A$ des éléments non nuls. Si $c|xy$ et $pgcd(c, x) \sim 1$, alors $c|y$.*

Définition. Un élément $x \neq 0$ est dit *irréductible*, si x n'est pas inversible, et

$$x = ab \;\Rightarrow\; a \quad \text{ou} \quad b \quad \text{inversible.}$$

Théorème. *Soit $x \in A, x \neq 0$ un élément non-inversible. Alors il existent des éléments irréductibles $p_1, ..., p_k \in A$ tels que*

$$x = p_1 \cdot ... \cdot p_k. \tag{6}$$

Anneaux euclidiens

Définition. Un anneau A est appelé *euclidien* si A est intègre et il existe une fonction $g : A \setminus \{0\} \to \mathbf{N}$, telle que

1. $g(ab) \geqslant g(a)$ pour tout $a, b \in A \setminus \{0\}$.
2. Pour tout $a \in A$ et tout $b \in A \setminus \{0\}$ il existent $q, r \in A$ tels que a) $a = bq + r$ et b) $r = 0$ ou $g(r) < g(b)$.

La fonction g est appelée *norme euclidienne.*

Théorème. *Tout anneau euclidien est un anneau principal.*

Proposition. *L'anneau des nombres de Gauss*

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$$

(où $i = \sqrt{-1}$) est un anneau euclidien par rapport à la norme $g(a + bi) = a^2 + b^2$.

L'Anneau de polynômes en une variable

Définition. 1. Soit A un anneau. On appelle *polynôme* à coefficients dans A une suite $(a_0, a_1, ..., a_n, ...)$ d'éléments de A, telle que tous les éléments a_i sauf un nombre fini, sont nuls. L'ensemble de tous les polynômes est noté $A[x]$.

2. On introduit la loi d'addition sur $A[x]$ par la formule suivante:

$$(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n, ...) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...).$$

3. On introduit la loi de multiplication sur $A[x]$ de la façon suivante: soit $P = (a_0, a_1, ..., a_n, ...)$, $Q = (b_0, b_1, ..., b_n, ...)$. On pose $R = (c_0, c_1, ..., c_n, ...)$ où

$$c_r = \sum_{i=0}^{r} a_i b_{r-i} \quad \text{pour tout} \quad r.$$

Proposition. *L'ensemble $A[x]$ muni de ces lois est un anneau.*

Définition. L'anneau $A[x]$ est appelé *l'anneau de polynômes en une variable à coefficients dans A.*

Définition. Un polynôme $P = (a_0, ..., a_n, 0, ...)$ s'écrit aussi $P = a_0 + ... + a_n x^n$. L'entier positif maximal $n \in \mathbf{N}$ tel que $a_n \neq 0$ est appelé *degré* du polynôme P.

Théorème. *Soit K un corps. Alors l'anneau de polynômes $K[x]$ en une variable à coefficients dans K est un anneau euclidien par rapport à la norme $g(P) = \deg P$.*

Corollaire. *Soit K un corps. L'anneau de polynômes $K[x]$ est principal.*

Définition. Soit K un corps. Le corps de quotients de $K[x]$ est appelé *corps de fractions rationnelles sur K* et noté $K(x)$.

Théorème. (Décomposition des fractions rationnelles en éléments simples). *Soit K un corps. Toute fraction rationnelle $R \in K(x)$ s'écrit sous la forme*

$$R = A + \frac{C_1}{P_1^{\alpha_1}} + ... + \frac{C_k}{P_k^{\alpha_k}}$$

où A, C_i, P_i sont des polynômes, α_i sont des entiers positifs et $\deg C_i < \deg P_i$ *pour tout i.*

Théorème. (Théorème de D'Alembert-Gauss). *Soit $P \in \mathbf{C}[x]$ un polynôme non-constant. Alors P a au moins une racine dans $\mathbf{C}$.*

Corollaire. *Un polynôme $P \in \mathbf{C}[x]$ est irréductible si et seulement si* $\deg P = 1$.

Théorème.
1. *Chaque polynôme $P \in \mathbf{R}[x]$ linéaire non constant est irréductible dans $\mathbf{R}[x]$.*
2. *Un polynôme à coefficients réels de degré 2 est irréductible dans $\mathbf{R}[x]$ si et seulement s'il n'a pas de racines réelles.*
3. *Tous les polynômes irréductibles de $\mathbf{R}[x]$ sont de degré $\leqslant 2$.*

Anneaux de polynômes en plusieurs variables

Définition. L'anneau de polynômes à n variables à coefficients dans A est défini par récurrence comme étant l'anneau des polynômes en une variable x_n sur l'anneau des polynômes à $n-1$ variables, soit $A[x_1, ..., x_{n-1}][x_n]$. Il est noté $A[x_1, ..., x_n]$.

Définition.
1. L'action du groupe symétrique S_n sur $A[x_1, ...x_n]$ est définie par la formule suivante:
$$(\sigma P)(x_1, ...x_n) = P(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$
2. Un polynôme $P \in A[x_1, ...x_n]$ est appelé *symétrique* si $\sigma P = P$ pout tout $\sigma \in S_n$.

Définition. Soit $i \leqslant n$. Le polynôme symétrique
$$\sigma_{i,n} = \sum_{(a_1, ..., a_n) | a_1 < a_2 ... < a_n} x_{a_1} \cdot ... \cdot x_{a_n}$$
est appelé *polynôme symétrique élémentaire.*

Théorème. (Théorème de Viète) *Soit K un corps,*
$$P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in K[x]$$
un polynôme. Supposons que P soit décomposable dans $K[x]$ en un produit des polynômes linéaires: $P(x) = (x-\alpha_1) \cdot (x-\alpha_2) \cdot ... \cdot (x-\alpha_n)$. Alors on a
$$a_i = (-1)^{n-i} \sigma_{n-i,n}(\alpha_1, ..., \alpha_n) \quad \textit{pour tout} \quad i$$

Théorème. *Soit $P \in K[x_1, ..., x_n]$ un polynôme symétrique. Alors il existe un polynôme $Q \in K[x_1, ..., x_n]$ tel que*
$$P(x_1, ..., x_n) = Q\big(\sigma_{1,n}, ..., \sigma_{n,n}\big)$$
où $\sigma_{i,n} = \sigma_{i,n}(x_1, ..., x_n)$ sont les polynômes symétriques élémentaires.

Bibliographie.

- B.L.Wan der Waerden, *Algebra,* Springer.
- S.Lang, *Algebra,* Addison-Wesley.
- L.Schwartz, *Algèbre,* Dunod, Mathématiques pour la Licence.