Université Cheikh Anta Diop de Dakar
Faculté des Sciences et Techniques
(UCAD-FST)
Département de Mathématiques et Informatique
(DMI)
Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications
(LACGAA)
Licence 03 Mathématiques et Informatique

Cours Algèbre Licence III

Chargé du cours : **Pr Amadou Lamine FALL**
Assistants TD : **Dr Ousmane NDIAYE**
Dr Kande DIABY
Dr Jean Belo KLAMTI

Table des matières

1 Généralités sur les groupes **7**

1.1 Groupes et sous-groupes 7

1.2 Groupes quotients 10

1.2.1 Sous-groupe normal et groupe quotient 10

1.2.2 Théorème d'isomorphisme 13

1.3 Groupes cyciques 17

2 GROUPES DES PERMUTATIONS D'UN ENSEMBLE FINI **23**

2.1 Orbite d'un élélment de S_n - Cycles - Transpositions 23

2.1.1 Orbite suivant une permutation 25

2.1.2 Cycles - Transpositions 26

2.2 Générateurs de $\mathcal{S}_n$ 27

2.2.1 Décomposition canonique d'une permutation 27

2.2.2 Ordre d'une permutation - Inverse d'une permutation 28

2.2.3 Décomposition d'une permutation en transposition 29

2.3 Signature d'une permetation - Groupe Alterné 30

2.3.1 Signature d'une permutation 30

2.3.2 Groupes alternés 33

2.3.3 Générateurs de $\mathcal{A}_n$ 34

3 Actions de groupes sur un ensemble **37**

3.1 Généralités sur les actions de groupes 37

3.2 Orbites et Stabilisateurs d'une action de groupes 39

3.3 Dénombrement des orbites 40

3.4 Applications aux p-groupes 45

3.5 Produit semi - direct de groupes 46

3.5.1 Produit direct de deux sous - groupes d'un groupe G 47

3.5.2 Produit semi - direct de deux sous - groupes d'un groupe 48

3.5.3 Produit semi- direct des groupes (Produit semi - direct externe 49

4 Les Théorèmes de Sylow 53

4.1 Les Théorèmes de Cauchy 53

4.1.1 Théorèmpe de Cauchy abélien 53

4.1.2 Théorème de Cauchy non abélien 54

4.2 Les Théorèmes de Sylow 55

4.3 Applications des théorèmes de Sylow 60

5 Groupes résolubles 61

5.1 Suite de décomposition et de Jordan-Holder 61

5.1.1 Groupes résolubles 66

5.2 Caractérisation de la résolubilité des groupes dérivés 68

5.3 Résolubilité du groupe symétrique 70

6 Anneaux et Corps 73

6.1 Anneaux - Sous - anneaux et idéaux 73

6.2 Morphismes et Anneaux quotients 77

6.2.1 Morphismes 77

6.2.2 Anneaux quotients 78

6.3 Idéal Premier et Idéal maximal 81

6.4 Caractéristique d' un anneau 83

6.5 Corps de Fraction d'un anneau intègre 85

7 Anneaux Factoriels - Anneaux Principaux 93

7.1 Anneau de Polynômes 93

7.1.1 Anneau de Polynômes à une indéterminée 93

7.1.2 Anneau de Polynôme à plusieurs indéterminées 102

7.2 Anneaux Factoriels 107

7.2.1 Divisibilité et éléments irréductibles 107

7.2.2 Anneaux factoriels 109

7.3 Anneaux Principaux 113

7.4 Anneaux Euclidiens 115

8 Polynômes irréductibles 121

9 Extensions de corps 131

9.1 Généralités sur les extensions 131

9.2 Extension obtenue par adjonction 133
9.3 Éléments algébriques - Extensions algébriques 135
9.3.1 Éléments algébriques 135
9.3.2 Extensions algébriques 141

10 Corps de rupture - Corps de décomposition **145**
10.1 Corps de rupture 145
10.2 Corps de décomposition 147
10.3 Corps de décomposition 148
10.4 Corps finis 152

11 Extensions Galoisiennes **157**
11.1 Groupe de Galois d'une extension 157
11.2 Polynômes séparables et extensions séparables 162

Chapitre 1

Généralités sur les groupes

1.1 Groupes et sous-groupes

Définition 1.1.1. *Un groupe est un ensemble non vide muni d'une loi de composition interne* $\star$ *vérifiant :*

1. *Pour tout* $(x, y, z) \in G^3$, $(x \star y) \star z = x \star (y \star y)$ *(Associativité)*
2. *il existe* $e \in G$ *tel que pour tout* $x \in G$, $x \star e = e \star x = x$ *(Élément neutre)*
3. *Pour tout* $x \in G$, *il existe* $x' \in G$ *tel que* $x \star x' = x' \star x = e$ *(tout élément admet un symétrique)*

Exemple 1.1.2.

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$, $(\mathcal{S}_n, \circ)$ et $(GL_n(\mathbb{R}), *)$ sont des groupes.

Définition 1.1.3. *Lorsque la loi de composition interne* $\star$ *est commutative, on dira que le groupe* G *est commutatif ou abélien.*

Notation 1.1.4.

Soit G un groupe muni d'une loi de composition intere $\star$

1. Si la loi $\star$ est multiplicative (respectivement additive), alors on désigne par e (respectivement par 0) l'élément neutre de G. Pour tout élément $x \in G$ on désigne par x^{-1} (respectivement $-x$) le symétrique de x
2. Si la loi $\star$ est multiplicative, pour tout $x \in G$, on définit par récurrence $x^0 = e$, $x^1 = x$ et pour tout $n \geq 2$, $x^n = x^{n-1}$. Pour tout $m \in \mathbb{Z}$, $x^m = (x^{-1})^{-m}$
3. Le cardinal de G sera noté $|G|$ ou $Card(G)$

Définition 1.1.5. *Soit* G *un groupe et* H *une partie de* G. *On dit que* H *est un sous*groupe de* G, *si* H *muni de la loi de composition interne de* G *est un groupe.*

Proposition 1.1.6. *Soit G un groupe et H une partie de G. Alors H est un sous-groupe de G si et seulement si les deux propriétés suivantes sont vérifiées.*

1. $H \neq \varnothing$
2. *Pour tout* $(x, y) \in G^2$, $xy^{-1} \in H$

Démonstration

Soit H un sous-groupe de G alors $e \in H$ donc $H \neq \varnothing$.

Soit $(x, y) \in H^2$. Comme H est un sous-groupe de G alors $y^{-1} \in H$ et $xy^{-1} \in H$

Ainsi 1. et 2. sont vérifiées.

Réciproquement supposons que 1. et 2. sont vérifiées. Soit $x \in H$ alors d'après 2. $xx^{-1} = e \in H$ et on déduit que $x^{-1} = ex^{-1} \in H$.

Soient $(x, y) \in H^2$. on a $y^{-1} \in H$ et $x(y^{-1})^{-1} = xy \in H$.

Loi de G étant associative, il en résulte que $(H; \cdot)$ est un groupe.

Théorème 1.1.7. *Soit G un groupe et S une partie de G. Alors il existe un plus petit sous-groupe de G qui contient S. Ce sous-groupe est appelé sous-groupe engendré par S et on le note $< S >$*

Démonstration

Posons $\mathcal{F}$ l'ensemble des sous-groupes de G de contenant S. L'ensemble $\mathcal{F}$ n'est pas vide car $G \in \mathcal{F}$. Soit $L = \bigcap_{H \in \mathcal{H}} H$. On a $e \in L$ et $S \subset L$ donc $L \neq \varnothing$.

Soit $(x, y) \in L$. Pour tout $H \in \mathcal{F}$, x, $y \in H$. Comme $H \in \mathcal{F}$, H est un groupe alors $H \in \mathcal{F}$, $xy^{-1} \in H$ donc $xy^{-1} \in L$. Il en résulte que L est un sous-groupe de G.

Soit H'un sus-groupe de G contenant S. Alors $H' \in \mathcal{F}$ donc $L \subset H'$. Ainsi L est le plus petit sous groupe de G contenant S

Théorème 1.1.8. *Soit G un groupe et H une partie non vide de G. Alors*

$$< S >= \{x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n} tel\ que \quad n \in \mathbb{N}^*, \quad x_1, ..., x_n \in S, \quad \epsilon_i \in \{-1; 1\}\ \}$$

Démonstration

Posons $L = \{x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n} tel\ que \quad n \in \mathbb{N}^*, \quad x_1, ..., x_n \in S, \quad \epsilon_i \in \{-1; 1\}\ \}$. Alors $S \subset L$ donc $L \neq \varnothing$ et de plus $L \subset < S >$.

Pour montre que $L =< S >$ il suffit de montrer maintenant que L est un sous-groupe de G. Soient x, et $y \in L$. Alors il existe n, et $m \in \mathbb{N}^*$ tels que $x = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$ et $y = y_1^{\epsilon'_1} y_2^{\epsilon'_2} ... y_m^{\epsilon'_m}$. On a

$$xy^{-1} = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n} y_m^{-\epsilon'_m} ... y_1^{-\epsilon'_1} \in L$$

En conclusion L est un sous-groupe de G. D'où $L =< S >$

Remarque 1.1.9.

1. Si $S = \varnothing$ alors $< S >= \{e\}$
2. Si la loi de composition de G est additive alors

$$< S >= \{\epsilon_1 + \epsilon_2 x_1 x_2 + ... + \epsilon_n x_n tel\ que\ \ n \in \mathbb{N}^*,\ \ x_1, ..., x_n \in S,\ \ \epsilon_i \in \mathbb{Z}\ \}$$

3. Si $S = \{x\}$ alors

$$< S >= \left\{x^k\ \ tel\ que\ \ k \in \mathbb{Z}\ \right\}$$

Définition 1.1.10. *L'ordre d'un groupe G est son cardinal $|G|$. Lorsque le cardinal du groupe G est fini , on dit que G est un groupe fini et dans le cas contraire on dira que G est infini*

Définition 1.1.11. *Soit G un groupe et $x \in G$. On appelle l'ordre de x l'ordre $| < x > |$ du sous-groupe $< x >$ engendré par x et on le note $O(x)$.*

Théorème 1.1.12. *Soit G un groupe et $x \in G$ un élément d'ordre fini alors*

$$O(x) = | < x > | = \min \left\{k \in \mathbb{N}^*\ \ tel\ \ x^k = e\right\}$$

Démonstration

Soit $x \in G$ un élément d'ordre fini. Alors le sous-groupe $< x >= \left\{x^k\ \ tel\ que\ \ k \in \mathbb{Z}\ \right\}$ est d'ordre fini donc l'ensemble $\left\{x^k\ \ tel\ que\ \ k \in \mathbb{N}^*\ \ \right\}$ est fini.

Soit $N = \left\{k \in \mathbb{N}^*\ \ tel\ \ que\ \ x^k = e\right\}$. Alors N est non vide te admet un plus petit élément n. Soit $y \in < x >$. Alors il existe $m \in \mathbb{Z}$ tel que $y = x^m$.

En faisant la division euclidienne de m par n, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $m = qn + r$ avec $0 \leq r < n$. Donc

$$y = x^m = x^{qn+r} = x^{qn} x^r = x^r$$

On en déduit donc que

$$< x >= \left\{x^k\ \ tel\ que\ \ 0 \leq k \leq n - 1\right\}$$

Soient k_1 et $k_2 \in \mathbb{N}$ tels que $0 \leq k_1 \leq k_2 \leq n - 1$ et $x^{k_1} = x^{k_2}$.

On a

$$x^{k_1} = x^{k_2} \Longrightarrow x^{k_2 - k_1} = e$$

or $0 \leq k_2 - k_1 \leq n - 1 - k_1 \leq n - 1$ la minimalité de n implique que $k_2 - k_1 = 0$ donc $k_1 = k_2$. Ainsi

$$< x >= \left\{e, x, x^2, x^3, ..., x^{n-1}\ \right\}$$

d'où $O(x) = n$

Théorème 1.1.13. *Soit G un groupe et x un élément de G d'ordre fini n. Alors pour tout $m_i n\mathbb{Z}$, $x^m = e$ si et seulement si $m \in n\mathbb{Z}$*

Démonstration

Soit $m \in \mathbb{Z}$ tel que $x^m = e$. En faisant la division euclidienne de m il existe un unique couple d'entier (q, r) tel que $m = nq + r$ avec $0 \leq r < n$. Supposons $r \neq 0$ alors

$$x^m = x^{nq+r} = x^r = e \;\; absurde$$

car $r < n$ donc $r = 0$ d'où $m = nq$ ainsi $m \in n\mathbb{Z}$.

Reciproquement si $m \in n\mathbb{Z}$ alors il existe $k \in \mathbb{Z}$ tel que $m = kn$ donc

$$x^m = x^{kn} = e$$

Théorème 1.1.14. *Soit G un groupe et soient x et y deux élément de G tels que*

1. $O(x) = n$ *et* $O(y) = m$ *avec* n *et* $m \in \mathbb{N}^*$
2. $xy = yx$
3. $< x > \cap < y >= \{e\}$

Alors $O(xy) = ppcm(n, m)$

Démonstration Posons $\ell = ppcm(n, m)$ alors il existe q_1 et $q_2çin\mathbb{Z}$ tels que $\ell = q_1 n$ et $\ell = q_2 m$. Comme $xy = yx$ alors on a

$$(xy)^\ell = x^{q_1 n} y^{q_2 m} = ee = e$$

donc $O(xy)$ est fini. Posons $s = O(xy)$. D'après ce qui précède s divise ℓ alors $s \leq \ell$

On a $s = O(xy)$ implique que

$$(xy)^s = e \Longrightarrow x^s = y^{-s} \in < x > \cap < y >= \{e\} \Longrightarrow x^s = y^{-s} = e$$

donc s est un multiple comme de n et m alors $s \geq \ell$

D'où $s = \ell$

1.2 Groupes quotients

1.2.1 Sous-groupe normal et groupe quotient

Soit G un groupe et H un sous-groupe de G. On définit sur G les deux relations binaires suivantes :

1. Pour tout $(x, y) \in G^2$, $x\mathcal{R}_g y \Longleftrightarrow x^{-1}y \in H$

2. Pour tout $(x, y) \in G^2$, $x\mathcal{R}_d y \Longleftrightarrow yx^{-1} \in H$

Les relations $\mathcal{R}_d$ et $\mathcal{R}_g$ qont des relations d'équivalence sur G appelées relations d'équivalence à droite et à gauche modulo H.

La classe à gauche (respectivement à droite) de x modulo H est

$$xH = \{xh \ \ tel\ que \ \ h \in H\}\,(respectivement \ \ Hx = \{hx \ \ tel\ que \ \ h \in H\})$$

Soit $(G/H)_g$ l'ensemble des classes à gauche modulo H et $(G/H)_d$ l'ensemble des classes à droite modulo H.

Lemme 1.2.1. *Soient G un groupe et H un sous-groupe de G. Soient x, $y \in G$. Les conditions suivantes sont équivalentes :*

1. $x^{-1}y \in H$
2. $xH = yH$
3. $Hx^{-1} = Hy^{-1}$

Démonstration

2.$\Longrightarrow$ 1. Supposons que $xH = yH$

On a

$$xH = yH \Longrightarrow H = x^{-1}yH \Longrightarrow x^{-1}ye = x^{-1}y \in H$$

1.$\Longrightarrow$ 3. Supposons que $x^{-1}y \in H$ Soit $h \in H$ on a :

$$hx^{-1} = (hx^{-1}y)y^{-1} \in Hy^{-1} \Longrightarrow Hx^{-1} \subset Hy^{-1}$$

De même on montre que $Hy^{-1} \subset Hx^{-1}$. D'où $Hx^{-1} = Hy^{-1}$

3. $\Longrightarrow$ 1. On a

$$Hx^{-1} = Hy^{-1} \Longrightarrow (Hx^{-1})^{-1} = (Hy^{-1})^{-1} \Longrightarrow xH = yH$$

Lemme 1.2.2. *Soient G un groupe et H un sous-groupe de G. Pour tout $x \in G$, $|xH| = |H| = |Hx|$*

Démonstration

Considérons l'application $\varphi : H \longrightarrow xH$ telle que pour tout $h \in H$, $\varphi(h) = xh$.

φ est surjective par construction. Soient h_1 et $h_2 \in H$ tels que $\varphi(h_1) = \varphi(h_2)$. On a :

$$\varphi(h_1) = \varphi(h_2) \Longleftrightarrow xh_1 = xh_2 \Longrightarrow h_1 = h_2$$

donc φ est injective. Donc φ est bijective. Ainsi $|xH| = |H|$

Lemme 1.2.3. *oient G un groupe et H un sous-groupe de G. On a*

$$|(G/H)_g| = |(G/H)_d|$$

Démonstration

Considérons l'application $\varphi : (G/H)_g \longrightarrow (G/H)_d$ telle que pour tout $xH \in (G/H)_g$, $\varphi(xH) = Hx^{-1}$.

Soit $Hy \in (G/H)_d$. On a $Hy = \varphi(y^{-1}H)$ donc φ est surjective. On en déduit du 1.2.1, φ que φ est injective. D'où φ est bijective. Ainsi, $|(G/H)_g| = |(G/H)_d|$

Définition 1.2.4. *Soit G un groupe et H un sous-groupe de G. Le cardinal commun à $(G/H)_g$ et $(G/H)_d$ est appelé indice ou index de H dans G et se note $[G : H]$*

Théorème 1.2.5. *(Lagrange Soit G un groupe fini et H un sous-groupe de G Alors*

$$|G| = |H| \times [G : H]$$

C'est-à-dire l'ordre et l'indice de H sont des diviseurs de l'ordre de G.

Démonstration

Posons $x_1, ..., x_t$ les représentants des classes distinctes. Alors on aura

$$G = \bigcup_{i=1}^{t} x_i H \Longrightarrow |G| = |\bigcup_{i=1}^{t} x_i H|$$

Or pour tout $i \neq j$ $x_iH \cap x_jH = \varnothing$ et $|x_iH| = |x_jH| = |H|$ donc

$$|G| = \sum_{i=1}^{t} |H| = t \times |H| = [G : H]|H|$$

Définition 1.2.6. *Soit G un groupe et H un sous-groupe de G. On dit que H est un sous-groupe normal ou distingué de G si et seulement si pour tout $x \in G$, $xH = Hx$. On note dans ce cas $H \lhd G$*

Remarque 1.2.7.

Soit G un groupe et H un sous-groupe normal de G. Soit x, x', y et $y' \in G$ tels que $xH = x'H$ et $yH = y'H$. On a

$$xyH = x(yH) = x(y'H) = x(Hy') = (xH)y' = (x'H)y' = x'y'H$$

Donc si H est normal dans G , les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont compatible avec la loi du groupe G.

On peut définir sur G/H une loi de composition interne suivante :

$$(xH).(yH) = (xy)H$$

G/H muni de cette loi est un groupe appelé groupe quotient de G par H.

1.2.2 Théorème d'isomorphisme

Définition 1.2.8. *Soient G et G' deux groupes. On appelle morphisme de groupes de G dans G', toute application $\varphi : G \longrightarrow G'$ vérifiant pour tout x, $y \in G$,*

$$\varphi(xy) = \varphi(x)\varphi(y)$$

Lorsque φ est bijective, on dira que φ est un isomorphisme de groupes.

Définition 1.2.9. *On appelle endomorphisme d'un groupe G, tout morphisme de groupes de G dans G lui même.*

Un automorphisme de G est un endomorphisme bijectif

Remarque 1.2.10.

1. Soit $f : G \longrightarrow G'$ un morphisme de groupes. Si e est l'élément neutre de G et e' celui de G' alors $f(e) = e'$ et pour tout $x \in G$ on a $f(x^{-1}) = [f(x)]^{-1}$
2. Soit G un groupe et H un sous-groupe normal de G. L'injection canonique $i : H \longrightarrow G$ et la surjection canonique $\pi : G \longrightarrow G/H$ telles que $i(x) = x$ et $\pi(g) = gH$ sont des morphismes de groupes.
3. Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors $ker\ f = \{x \in G \ \ tel \ \ que \ \ f(x) = e'\}$ est un sous-groupe normal de G et $Im\ f = f(G)$ est un sous-groupe G'.

   f est injectif si et seulement si $ker\ f = \{e\}$ et f est surjectif si et seulement si $Im\ f = G'$

Le théorème suivant est appelé théorème de factorisation des morphismes de groupes ou propriété universelle du groupe quotient.

Théorème 1.2.11. *Soit $f : G \longrightarrow G'$ un morphisme de groupes et H un sous-groupe normal de G tel que $H \subset ker\ f$ et $\pi : G \longrightarrow G/H$ la surjection canonique. Alors :*

1. *Il existe un unique morphisme de groupes $\varphi : G/H \longrightarrow G'$ tel que $\varphi \circ \pi = f$*
2. *Le morphisme φ est injectif si $H = ker\ f$.*
3. *Le morphisme φ est surjectif si et seulement si f est surjectif.*

Démonstration

1. Posons

$$\varphi : G/H \longrightarrow G'$$

$$xH \longrightarrow \varphi(xH) = f(x)$$

Montrons que φ est bien défini. Soient x_1H et $x_2H \in G/H$ tel que $x_1H = x_2H$. On a :

$$x_1H = x_2H \Longrightarrow x_1^{-1}x_2 \in H \Longrightarrow \varphi(x_1^{-1}x_2H) = f(x_1^{-1}x_2) = e'$$

$$\Longrightarrow f(x_1) = f(x_2) \Longrightarrow \varphi(x_1H) = \varphi(x_2H)$$

Donc φ est bien définie. Montrons que φ est un morphisme de groupes.

Soient x_1H et $x_2H \in G/H$. On a :

$$\varphi[(x_1H)(x_2H)] = \varphi[(x_1x_2)H] = f(x_1x_2) = f(x_1)f(x_2) = \varphi(x_1H)\varphi(x_2H)$$

Soit $x \in G$. On a :

$$f(x) = \varphi(xH) = \varphi(\pi(x)) = (\varphi \circ \pi)(x)$$

Donc $f = \varphi \circ \pi$.

Soit $g : G/H \longrightarrow G'$ tel que $f = g \circ \pi$. Soit $xH \in G/H$. On a :

$$\varphi(xH) = f(x) = g(\pi(x)) = g(xH)$$

donc $\varphi = g$

2. Supposons que φ est injectif. Soit $x \in ker\ f$. On a :

$$x \in ker\ f \Longrightarrow f(x) = e' \Longrightarrow \varphi \circ \pi(x) = e' \Longrightarrow xH \in ker\ \varphi = eH = H$$

Réciproquement supposons que $H = Ker\ f$. Montrons que φ est injectif. Soient x_1H, $x_2H \in G/H$ tel que $\varphi(x_1H) = \varphi(x_2H)$. On a

$$\varphi(x_1H) = \varphi(x_2H) \Longrightarrow f(x_1) = f(x_2) \Longrightarrow f(x_1^{-1}x_2) = e'$$

$$\Longrightarrow x_1^{-1}x_2 \in ker\ f = H \Longrightarrow x_1H = x_2H.$$

Ainsi φ est injectif.

3. Évident

Corollaire 1.2.12. *(Premier théorème d'isomorphisme)*

Soit $f : G \longrightarrow G'$ un morphisme de groupes alors les groupes $Im\ f$ et $G/ker\ f$ sont isomorphes.

Démonstration

Il suffit d'appliquer les théorème précédent à l'application $g : G \longrightarrow Im\ f$ telle que pour tout $x \in G$, $g(x) = f(x)$.

Lemme 1.2.13. *Soit G un groupe. Soient H et K deux sous-groupe de G tels que $H \lhd G$. Alors*

1. *HK est un sous-groupe de G et $H \lhd HK$*
2. *$H \cap K \lhd K$ ($H \cap K$ est normal dans K)*

Démonstration

1. Comme KH est un sous-groupe de G si et seulement $KH = HK$. Pour montrer que HK est un sous-groupe de G il suffit de montrer que KH est un groupe.
   (a) On $e \in KH$
   (b) Soit $x = k_1h_1$ et $y = k_2h_2 \in KH$. On a

$$xy^{-1} = k_1h_1h_2^{-1}k_2^{-1} = k_1k_2^{-1}l(k_2h_1h_2^{-1}k_2^{-1}) \in KH$$

   Donc KH est un sous-groupe de G. Ainsi HK est un sous-groupe de G. On a HK est un sous-groupe de$G$ et $H \lhd G$ donc $H \lhd HK$
2. Soit $k \in K$ et $t \in H \cap K$. On a

$$t \in H \cap K \Longrightarrow ktk^{-1} \in K$$

   De plus $H \lhd G$ donc $ktk^{-1} \in H$. Donc $ktk^{-1} \in H \cap K$. Ainsi $H \cap K \lhd K$

Théorème 1.2.14. *(deuxième théorème d'isomorphisme)*

Soit G un groupe. Soient H et K deux sous-groupes de G tels que $H \lhd G$. Alors les groupes quotients $K/H \cap K$ et HK/H sont isomorphes.

Démonstration

Considérons l'application $\pi : G \longrightarrow G/H$ et $f : K \longrightarrow HK/H$ la restriction de π à K. Alors f est morphisme de groupes. Montrons que $Im\ f = HK/H$ et $ker\ f = H \cap K$

Soit $x \in H \cap K$, on a

$$x \in H \cap K \Longleftrightarrow x \in H \ \ et \ \ x \in K \Longleftrightarrow x \in K \ \ et \ \ f(x) = \overline{x} = \overline{e}$$

donc $ker\ f = H \cap K$.

Soit $y \in Im\ f$. On a :

$$y \in Im\ f \Longrightarrow \exists\ k \in K \ \ tel \ \ que f(k) = y \Longrightarrow y = f(k) = \overline{k} = \overline{ek} \in HK/H$$

donc $Im\ f \subset HK/H$

Réciproquement soit $y \in HK/K$. On a

$$y \in HK/H \Longrightarrow \exists (h, k) \in H \times K \ \ tel \ \ que \ \ y = \overline{hk} = \overline{hk} = \overline{k} = f(k)$$

donc $HK/H \subset Im\ f$. Ainsi $HK/H = Im\ f$.

Alors d'après le théorème d'isomorphisme, les groupes $K/H \cap K$ et HK/H sont isomorphes.

Théorème 1.2.15. *(Troisième théorème d'isomorphisme) Soit G un groupe. Soient H et K deux sous-groupes normaux de G tels que $K \subset H$. Alors*

1. *H/K est normal dans G/K*
2. *Les groupes G/K et $(G/k)/(H/K)$ sont isomorphes*

Démonstration

1. Soit $\overline{x} \in G/K$ et $\overline{h} \in H/K$. On a

$$\overline{x}\overline{h}\overline{x}^{-1} = \overline{xhx^{-1}} \in H/K$$

car $H \lhd G$ donc $H/K \lhd G/K$

2. Soit $f : G/K \longrightarrow G/H$ l'application définie par : pour tout $xK \in G/K$, $f(xK) = xH$. f est un morphisme surjectif de groupes. Soit $xKinker\ f$. On a :

$$xK \in ker\ f \Longleftrightarrow xH = \overline{e} = H \Longleftrightarrow x \in H \Longleftrightarrow xK \in H/K$$

Alors d'après le premier théorème d'isomorphisme, les groupes quotient G/H et $(G/K)/(H/K)$ sont isomorphes.

Théorème 1.2.16. *(De correspondance) Soient G un groupe, K un sous-groupe normal de K et $\pi : G \longrightarrow G/K$ la surjection canonique. On désigne par Γ_K l'ensemble des sous-groupes de G contenant K et par $\mathcal{S}_{G/K}$ l'ensemble des sous-groupes de G/K. Alors*

1. *L'application*

$$\varphi : \Gamma_K \longrightarrow \mathcal{S}_{G/K}$$
$$H \longrightarrow \varphi(H) = H/K = \pi(H)$$

est bijective

2. *$H' = H/K$ est normal dans G/K si et seulement si $H \lhd G$*

Démonstration

1. Soit

$$\varphi : \Gamma_K \longrightarrow \mathcal{S}_{G/K}$$
$$H \longrightarrow \varphi(H) = H/K = \pi(H)$$

(a) Soient H_1 et $H_2 \in \Gamma_K$ tels que $\varphi(H_1) = \varphi(H_2)$. On a :

$$\varphi(H_1) = \varphi(H_2) \Longrightarrow H_1/K = H_2/K$$

Montrons dans ce cas que $H_1 = H_2$. Soit $a \in H_1$. on a :

$$a \in H_1 \Longrightarrow \overline{a} \in H_1/K = H_2/K \Longrightarrow \exists b \in H_2 \ \ tel \ \ que \ \ \overline{a} = \overline{b}$$

$$\Longrightarrow ab^{-1} \in K \Longrightarrow a = (ab^{-1})b \in H_2 \Longrightarrow H_1 \subset H_2$$

On montre de la même façon que $H_2 \subset H_1$. D'où $H_1 = H_2$ et donc φ est injective.

(b) Soit $H^* \in \mathcal{S}_{G/K}$. Posons $H = \pi^{-1}(H^*)$. Alors H est un sous-groupe de G contenant K et $\varphi(H) = H^*$ donc φ est surjective.

En conclusion φ est bijective.

2. Si H est normal dans G, le théorème d'isomorphisme entraine que H/K est normal dans G/K.

Supposons que H/K est normal dans G/K. Montrons que H est normal dans G. Soit $h \in H$ et $g \in G$. On a :

$$H/K \lhd G/K \Longrightarrow \overline{ghg^{-1}} = \overline{g}\overline{h}\overline{g}^{-1} \in H/K \Longrightarrow \exists t \in H \ \ tel \ \ que \ \ \overline{ghg^{-1}} = \bar{t} \Longrightarrow a = \overline{ghg^{-1}t^{-1}} \in K \subset$$

donc $ghg^{-1} = at \in H$ d'où $H \lhd G$

Exemple 1.2.17.

Sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$

1.3 Groupes cyciques

Définition 1.3.1. *Soit G un groupe. On dit que G est groupe monogène s'il existe $a \in G$ tel que $G =< a >$.*

Le groupe G sera dit cyclique lorsqu'il est monogène et fini

Définition 1.3.2. *Soit G un goupe fini. On appelle exposant de G le maximum d des ordres des éléments de G*

$$d = \max\{O(x) \ \ tel \ \ que \ \ x \in G\}$$

Exemple 1.3.3.

L'exposant de $\mathcal{S}_3$ est 3, celui de $\mathbb{Z}/4\mathbb{Z}$ est 4 et de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est 2.

Théorème 1.3.4. *Soit G un groupe fini d'exposant d. Alors pour tout $x \in G$, on a $x^d = e$*

Démonstration :

Soit $y \in G$ tel que $O(y) = d$. Supposons qu'il existe $x \in G$ dont l'ordre $n = O(x) = p_1^{\alpha_1}...p_t^{\alpha_t}$ ne divise pas d. Alors il existe $1 \leq i \leq t$ tel que $p_i^{\alpha_i}$ ne divise pas d. On peut alors écrire $d = p_i^{\beta} q_1$ avec $0 \leq \beta < \alpha_i$ et $pgcd(p_i, q_1) = 1$ puis $n = p_i^{\alpha_i} q_2$ où $q_2 = \prod\limits_{j \neq t} p_j^{\alpha_j}$. On a $O(x^{q_2}) = p_i^{\alpha_i}$ et $O(y^{p_i^{\beta}}) = q_1$. Comme $pgcd(p_i, q_1) = 1$, $< x^{q_2} > \cap < y^{p_i^{\beta}} >= \{e\}$ de plus comme G est abélien on aura $O(x^{q_2}, y^{p_i^{\beta}}) = ppcm(p_i^{\alpha_i}, q_1) = p_i^{\alpha_i} q_1 > d$ ce qui est absurde par définition de d. Ainsi d est multiple de n donc de multiple l'ordre de tout élément G.

Théorème 1.3.5. *Soit G un groupe monogène*

1. *Si G est d'ordre infini alors G est isomorphe à $\mathbb{Z}$*
2. *Si G est d'ordre fini n alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration

Soit x le générateur de G. Alors

$$G = \{x^m \ \ tel \ \ que \ \ m \in \mathbb{Z}\}$$

Considérons

$$\varphi : \mathbb{Z} \longrightarrow G$$

$$m \longrightarrow \varphi(m) = x^m$$

l'application φ est surjective. Soient m_1 et $m_2\mathbb{Z}$ tel que

$$\varphi(m_1 + m_2) = x^{m_1+m_2} = x^{m_1}x^{m_2} = \varphi(m_1)\varphi(m_2)$$

1. Supposons que G est infini.

   Comme G est infini, pour tout $m \in \mathbb{Z} \setminus \{0\}$, on a $x^m \neq e$ donc φ est injectif
2. Supposons G fini d'ordre n. Soit $m \in ker\ \varphi$. On a

   $$m \in ker\ \varphi \Longleftrightarrow x^m = e \Longleftrightarrow m \in n\mathbb{Z}$$

   Donc $ker\ \varphi = n\mathbb{Z}$ alors d'après le théorème d'isomorphisme, $G \simeq \mathbb{Z}/n\mathbb{Z}$

Remarque 1.3.6.

Tout groupe monogène est abélien

Théorème 1.3.7. *Soit G un groupe. Alors tout sous-groupe de G est monogène*

Soient x le générateur de G et H un sous-groupe de G.

1. Si $H = \{e\}$ alors $H =< e >$

2. Sinon si $H = G$ alors $H =< x >$
3. Sinon soit k le plus petit entier naturel tel que $x^k \in H$. Soit $y \in H$ alors il existe n tel que $y = x^n$. Alors la division euclidiène de n par k nous donne $n = qk + r$ avec $0 \leq r < k$. Si $r \neq 0$, on a

$$(x^k)^q \in H \Longrightarrow x^r = y(x^k)^{-q} \in H$$

absurde par définition de k donc $r = 0$ d'où $H =< x^k >$

Théorème 1.3.8. *Soit G un groupe cyclique d'ordre n. Soit d un entier naturel tel que d soit un diviseur de n. Alors il existe un unique sous-groupe de G d'ordre d.*

Démonstration

Soit x un générateur de G. Posons $\ell = n/d$ et $H =< x^\ell >$. Soit H' un sous groupe de G d'ordre d. Alors H' est cyclique et $H' =< x^m >$. Comme l'ordre de H' est d, on a :

$$x^{md} = e \Longrightarrow \exists k \in \mathbb{Z} \ \ tel \ \ que \ \ dm = nk$$

Donc $m = \frac{nk}{d}$ alors

$$x^m = x^{\frac{nk}{d}} = (x^{\frac{n}{d}})^k \Longrightarrow x^m \in H$$

Ce qui implique finalement $H' \subset H$ or $|H'| = |H|$ alors $H = H'$

Théorème 1.3.9. *Soit $G =< x >$ u groupe cyclique d'ordre n. Soit k un entier naturel. Alors*

1. $O(x^k) = \frac{n}{pgcd(n,k)}$
2. *$G =< x^k >$ si et seulement si n et k sont premier entre eux.*

Démonstration

1. Posons $m = pgcd(n, k)$ alors il $k' \in \mathbb{Z}$ tel que $k = mk'$. On a

$$x^k = x^{mk'} = (x^m)^{k'} \Longrightarrow x^k \in < x^m >$$

donc $< x^k > \subset < x^m >$

Comme $m = pgcd(k, n)$ d'après le théorème de Bezout, il existe un unique couple d'entiers (α, β) tel que $m = \alpha k + \beta n$. Alors on a

$$x^m = x^{\alpha k + \beta n} = x^{\alpha k} x^{\beta n} = x^{\alpha k} = (x^k)^\alpha \Longrightarrow x^m \in < x^k >$$

donc $< x^m > \subset < x^k >$.

En conclusion $< x^k > = < x^m >$. Comme m divise n, il existe m' tel que $n = mm'$ donc

$$O(x^m) = O(x^k) = m' = \frac{n}{pgcd(n, k)}$$

2. On a

$$G =< x^k > \Longleftrightarrow |G| = O(x^k) \Longleftrightarrow n = \frac{n}{pgcd(n,k)} \Longrightarrow pgcd(n,k) = 1$$

Lemme 1.3.10. *Soient G et G' deux groupes d'élément neutre respectivement e et e'. Soient $(x, y) \in G \times G'$ alors*

$$O((x, e')) = O(x) \quad et \quad O((e, y)) = O(y)$$

démonstration

Supposons que x est d'ordre infini alors pour tout $k \in \mathbb{Z}$, $(x, e')^k = (x^k, e') \neq (e, e')$ donc (x, e') est d'ordre infini. Inversement supposons que (x, e') est d'ordre infini alors pour tout $k \in \mathbb{Z}$, $(x, e')^k = (x^k, e') \neq (e, e')$ donc pour tout $k \in \mathbb{Z}$,$x^k \neq e$ implique que x est d'ordre infini.

Supposons que x est d'ordre fini k alors

$$(x, e')^k = (x^k, e') = (e, e')$$

donc (x, e') est d'ordre fini et son ordre est inferieur ou égal à k. Inversement supposons que (x, e') est d'ordre fini n alors

$$(x, e')^n = (x^n, e') = (e, e') \Longrightarrow x^n = e$$

donc x est d'ordre fini et son ordre est inférieur ou égal à n.

On vient ainsi de montrer que x est d'ordre fini si et seulement (x, e') est d'ordre fini et $O(x) = O((x, e'))$. On procède de la même manière pour (e, y)

Théorème 1.3.11. *Soient G et G' deux groupes d'élément neutre respectivement e et e'. Alors pour tout $(x, y) \in G \times G'$:*

1. *(x, y) est d'ordre infini si et seulement si x est d'ordre infini ou y est d'ordre infini.*
2. *Si $O(x) = n$ et $O(y) = m$,$O((x, y)) = ppcm(n, m)$*

Démonstration

1. Supposons (x, y) est d'ordre infini. Alors pour tout $k \in \mathbb{Z}$, on a :

$$(x, y)^k = (x^k, y^k) \neq (e, e') \Longleftrightarrow x^k \neq e \quad ou \quad y^k \neq e'$$

donc (x, y) est d'ordre infini si et seulement si x est d'ordre infini ou u est d'ordre infini.

2. Supposons que $O(x) = n$ et $O(y) = m$ alors

$$\left\{\begin{array}{l} (O((x,e')) = n \;\; et \;\; O((e,y)) = m \\ \\ \quad (x,e')(e,y) = (e,y)(x,e')) \end{array}\right. \Longrightarrow O((x,y)) = ppcm(O((x,e')), O((e,y)))$$

Donc $O((x,y)) = ppcm(O((x,e')), O((e,y))) = ppcm(O(x), O(y)) = ppcm(n,m)$

Théorème 1.3.12. *Soient $G =< x >$ et $G' =< y >$ deux groupes cycliques d'ordre respectivement n et m alors $G \times G'$ est cyclique si et seulement si n et m sont premiers entre eux.*

Démonstration

Supposons que $G \times G'$ est cyclique de générateur (a,b). Alors $|G| \times |G'| = |G \times G'| = O((a,b)) = ppcm(O(a), O(b))$. On a $O(a)$ divise $|G|$ et $O(b)$ divise $|G'|$ donc

$$|G| \times |G'| = ppcm(O(a), O(b)) \leq O(a) \times O(b) \leq |G| \times |G'|$$

Alors $G| \times |G'| = ppcm(O(a), O(b)) = O(a) \times O(b)$

or $ppcm(O(a), O(b)) \times pgc(O(a), O(b)) = O(a) \times O(b)$ donc $pgc(O(a), O(b)) = 1$

On a

$$\left\{\begin{array}{l} O(a) \; divise \; |G| \\ \\ O(b) \; divise \; |G'| \end{array}\right. \Longrightarrow \left\{\begin{array}{l} |G| = O(a)\ell_1 \\ \\ |G'| = O(b)\ell_2 \end{array}\right.$$

donc

$$|G| \times |G'| = O(a) \times O(b)\ell_1\ell_2 = O(a) \times O(b) \Longrightarrow \ell_1\ell_2 = 1 \Longrightarrow \ell_1 = \ell_2 = 1$$

Ainsi $pgcd(n,m) = pgcd(O(a), O(b)) = 1$ donc m et n sont premier entre eux.

Réciproquement supposons que m et n sont premiers entre eux. On a

$$O((x,y)) = ppcm(O(a), O(b)) = ppcm(n,m) = mn = |G \times G'|$$

donc $G \times G'$ est cyclique

Chapitre 2

GROUPES DES PERMUTATIONS D'UN ENSEMBLE FINI

Soit $n \in \mathbb{N}$, le groupe symétrique d'ordre n est le groupe S_n des permutations de l'ensemble $X = \{1, 2, 3, \cdots, n\}$. Comme tout ensemble fini de cardinal n est en bijection avec X, S_n est aussi le groupe des permutations d'un ensemble fini de cardinal n, $|S_n| = n!$ et S_n n'est pas abélien pour $n \geq 2$.

2.1 Orbite d'un élélment de S_n - Cycles - Transpositions

Définition 2.1.1. *Soit $\sigma \in S_n$ une permutation d'ordre n, le support de σ est l'ensemble*

$$\mathrm{Supp}(\sigma) = \{x \in X / \sigma(x) \neq x\}.$$

Soit $\sigma \in S_n$, $\mathrm{Supp}(\sigma) = \emptyset$ si et seulement si $\sigma = e$ est l'élément neutre de S_n

- Si $\sigma \neq e$, la restriction de σ où support de σ est une permutation de $\mathrm{Supp}(\sigma)$: $x \in \mathrm{Supp}(\sigma) \Longrightarrow \sigma(x) \neq x \Longrightarrow \sigma(\sigma(x)) \neq \sigma(x) \Longrightarrow \sigma(x) \in \mathrm{Supp}(\sigma)$.
- $k \in \mathbb{Z}$, $\mathrm{Supp}(\sigma^k) \subseteq \mathrm{Supp}(\sigma)$, en effet sont $x \in X$, et $k \in \mathbb{Z}$, $\sigma(x) = x \Longrightarrow \sigma^k(x) = x$, donc par contraposée $\sigma^k(x) \neq x \Longrightarrow \sigma(x) \neq x$. Ainsi $x \in \mathrm{Supp}(\sigma^k) \Longrightarrow x \in \mathrm{Supp}(\sigma)$.

Exemple 2.1.2.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 8 & 2 & 7 & 5 & 11 & 4 & 3 & 12 & 10 & 6 & 9 \end{pmatrix}$$

$supp(\sigma) = \{2, 3, 4, 6, 7, 8, 9, 11, 12\}$

Définition 2.1.3. *Soient σ et $\sigma^{'} \in S_n$, on dit que σ et $\sigma^{'}$ sont disjoints si*

$$\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma^{'}) = \emptyset.$$

Les supports de σ et $\sigma^{'}$ sont disjoints.

Deux éléments quelconques σ et $\sigma^{'}$ de S_n ne commutent pas en général. La proposition suivante montre que si σ et $\sigma^{'}$ sont disjoints, alors ils commutent.

Théorème 2.1.4. *Soient σ et $\sigma^{'}$ deux éléments de S_n. Si σ et $\sigma^{'}$ sont disjoints alors,*
$\sigma \circ \sigma^{'} = \sigma^{'} \circ \sigma$ *et* $<\sigma> \cap <\sigma^{'}>= \{e\}$.

Démonstration :

Si $n = 1$, la proposition est immédiate. On suppose $n > 1$. Soient σ et $\sigma^{'} \in S_n$, si $\sigma = e$ ou $\sigma^{'} = e$ alors $\sigma \circ \sigma^{'} = \sigma^{'} \circ \sigma$ et $<\sigma> \cap <\sigma^{'}>= \{e\}$.
Supposons $\sigma \neq e$ et $\sigma^{'} \neq e$. Soit $x \in X$, on a trois cas :

1 **cas :** $x \in \mathrm{Supp}(\sigma)$ et $x \notin \mathrm{Supp}(\sigma^{'})$: $x \in \mathrm{Supp}(\sigma) \Longrightarrow \sigma(x) \in \mathrm{Supp}(\sigma)$.
Comme $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma^{'}) = \emptyset$, on a $\sigma(x) \notin \mathrm{Supp}(\sigma^{'})$, donc $\sigma^{'}(\sigma(x)) = \sigma(x)$, d'où $\sigma^{'} \circ \sigma(x) = \sigma(x)$. De plus $\sigma \circ \sigma^{'}(x) = \sigma(\sigma^{'}(x)) = \sigma(x)$. Ainsi, $\sigma \circ \sigma^{'}(x) = \sigma^{'} \circ \sigma(x) = \sigma(x)$.

2 **cas :** $x \notin \mathrm{Supp}(\sigma)$ et $x \in \mathrm{Supp}(\sigma^{'})$: On a $\sigma(\sigma^{'}(x)) = \sigma(\sigma^{'}(x)) = \sigma^{'}(x)$ car $\sigma^{'} \in \mathrm{Supp}(\sigma^{'})$ et $\sigma^{'} \notin \mathrm{Supp}(\sigma)$. Ainsi, $\sigma \circ \sigma^{'}(x) = \sigma(\sigma^{'}(x)) = \sigma^{'}(x)$

3 **cas :** $x \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma^{'})$: $\sigma \circ \sigma^{'}(x) = \sigma(\sigma^{'}(x)) = \sigma(x) = x$ et $\sigma \circ \sigma^{'}(x) = \sigma^{'}(\sigma(x)) = \sigma^{'}(x) = x$.

Dans tous les cas nous avons $\sigma \circ \sigma^{'}(x) = \sigma^{'}(\sigma(x))$, $\forall x \in X$, d'où $\sigma \circ \sigma^{'} = \sigma^{'} \circ \sigma$.

Montrons que $<\sigma> \cap <\sigma^{'}>= \{e\}$, soit $\gamma \in <\sigma> \cap <\sigma^{'}>$.

$\gamma \in <\sigma> \cap <\sigma^{'}> \Longrightarrow \gamma \in <\sigma>$ et $\gamma \in <\sigma^{'}> \Longrightarrow \exists k_1 \in \mathbb{Z}$ et $k_2 \in \mathbb{Z}$ tels que $\gamma = \sigma^{k_1} = \sigma^{k_2}$, donc $\mathrm{Supp}(\gamma) \subset \mathrm{Supp}(\sigma)$ et $\mathrm{Supp}(\gamma) \subset \mathrm{Supp}(\sigma^{'})$, d'où
$\mathrm{Supp}(\gamma) \subset \mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma^{'})$. Comme $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma^{'}) = \emptyset$, on a $\mathrm{Supp}(\gamma) = \emptyset$ d'où $\gamma = e$. Ainsi

$$<\sigma> \cap <\sigma^{'}>= \{e\}.$$

Remarque 2.1.5.

La démonstration ci dessus montre que si σ et $\sigma^{'}$ sont disjoints alors $\mathrm{Supp}(\sigma \circ \sigma^{'}) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma^{'})$ et

$$\sigma \circ \sigma^{'}(x) = \sigma^{'}\sigma(x) = \begin{cases} \sigma(x) \text{ si } x \in \mathrm{Supp}(\sigma) \\ \sigma^{'}(x) \text{ si } x \in \mathrm{Supp}(\sigma^{'}) \\ x \text{ si } x \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma^{'}) \end{cases}$$

2.1.1 Orbite suivant une permutation

Soit $\sigma \in S_n$, on associe à σ la relation $\mathcal{R}_\sigma$ définie par $x, y \in X$, $x\mathcal{R}_\sigma y \Longleftrightarrow \exists k \in \mathbb{Z}$ tel que $y = \sigma^k(x)$. La relation $\mathcal{R}_\sigma$ est une relation d'équivalence sur X.

Définition 2.1.6. *Soit $\sigma \in S_n$ et $x \in X$, la classe d'équivalence de x modulo $\mathcal{R}_\sigma$ est appelée orbite de x suivant la permutation σ. On la note par $\Theta_\sigma(x) = \{\sigma^k(x)/k \in \mathbb{Z}\}$*

Exemple 2.1.7.

1.
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$$
Les orbites suivant σ sont $\Theta_\sigma(1) = \{1, 5, 3\}$, $\Theta_\sigma(2) = \{2\}$ et $\Theta_\sigma(4) = \{4, 6\}$

2.
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 8 & 2 & 7 & 9 & 11 & 1 & 3 & 12 & 6 & 10 & 5 \end{pmatrix}$$
Les orbites suivant β sont $\Theta_\beta(1) = \{1, 4, 7\}$, $\Theta_\beta(2) = \{2, 8, 3\}$, $\Theta_\beta(5) = \{5, 9, 12\}$ et $\Theta_\beta(6) = \{6, 11, 10\}$.

Pour tout $\sigma \in S_n$, l'ensemble des orbites suivant σ constituent une partition de X. Le théorème suivant donne la description de l'orbite d'un élément $x \in X$.

Théorème 2.1.8. *Soit $\sigma \in S_n$ et Θ une orbite suivant σ de cardinal $l > 1$. Alors $\forall x \in \Theta$, on a $\sigma^l(x) = x$ et*
$$\Theta = \{x, \sigma(x), \cdots, \sigma^{l-1}(x)\}.$$

démonstration

Soit $x \in \Theta = \{\sigma^k(x)/k \in \mathbb{Z}\}$.

Comme Θ est fini, $\exists i, j \in \mathbb{Z}$, $i < j$ tel que $\sigma^i(x) = \sigma^j(x)$.

$\sigma^i(x) = \sigma^j(x) \Longrightarrow \sigma^{j-i}(x) = x$, on en déduit que l'ensemble des entiers $m \in \mathbb{N}^*$ tel que $\sigma^m(x) = x$, n'est pas vide, donc admet un plus petit élément l.

Posons $L = \{x, \sigma(x), \cdots, \sigma^{l-1}(x)\}$, on a $L \subseteq \Theta$ (1). Montrons que $\Theta \subseteq L$.

Soit $y \in \Theta, \exists k \in \mathbb{Z}$ tel que $y = \sigma^k(x)$. La division euclidienne de k par l, donne $k = ql + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < l$. On a

$$\begin{aligned} y &= \sigma^k(x) \\ &= (\sigma^{lq} \circ \sigma^r)(x) \\ &= (\sigma^r \circ \sigma^{lq})(x) \\ &= \sigma^r((\sigma^l)^q(x)) \\ &= \sigma^r(x). \end{aligned}$$

Donc $y \in L$, d'où $\Theta \subseteq L$ (2). Les inclusions (1) et (2) entraînent $\Theta = L = \{x, \sigma(x), \cdots, \sigma^{l-1}(x)\}$. Montrons que $\text{card}(\Theta) = l$.

Soit r et $r^{'}$ deux éléments de $\{0, 1, \cdots, l-1\}$, avec $r \leq r^{'}$ tel que $\sigma^r(x) = \sigma^{r^{'}}(x)$. $\sigma^r(x) = \sigma^{r^{'}}(x) \Longrightarrow \sigma^{r-r^{'}}(x) = x$. Comme $0 \leq r^{'} - r < l$ et que l est le plus petit entier strictement positif tel que $\sigma^l(x) = x$, on a $r^{'} - r = 0$ par suite $r = r^{'}$. Ainsi les éléments $x, \sigma(x), \cdots, \sigma^{l-1}(x)$ sont deux à deux distincts. D'où $l = \text{card}(\Theta)$.

2.1.2 Cycles - Transpositions

Définition 2.1.9. *Soit $\sigma \in S_n$, on dit que σ est un cycle s'il existe une et une seule orbite qui ne sont pas réduite à un élément. Cet orbite est le support du cycle.*

Une permutation σ est un cycle s'il existe un entier $r, 1 \leq r \leq n$, des éléments $a_1, a_2, \cdots, a_r \in X$ tel que

$$\begin{cases} \sigma(a_i) = a_{i+1} \ 1 \leq i \leq r-1 \\ \sigma(a_r) = a_1 \\ \sigma(x) = x & si \ x \neq a_j, 1 \leq j \leq r. \end{cases}$$

On note le cycle σ par $\sigma = (a_1, a_2, \cdots, a_r)$, l'entier r est appelé la longueur du cycle σ. Un cycle de longueur 1 est égal à l'identité. Un cycle de longueur r est appelé r-cycle.

Exemple 2.1.10.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} \in S_6$, $\text{Supp}(\sigma) = \{2, 4, 5, 6\}$. Il y a une seule orbite non réduite à un point, donc $\sigma = (2, 4, , 6, 5)$ est un cycle de longueur 4.

Définition 2.1.11. *Un cycle de longueur 2, est appelé transposition. Une permutation $\tau \in S_n$ est une transposition s'il existe $i, j \in X$ tel que $\tau(i) = j$, $\tau(j) = i$ et $\tau(k) = k$ si $k \neq i$ et $k \neq j$. Une telle transposition est notée $\tau = (i, j)$.*

Le théorème suivant montre que l'ordre d'un cycle de longueur r est égal à r.

Théorème 2.1.12. *Soit c un cycle de longeur $r \leq n$ dans $\mathcal{S}_n$. Alors l'ordre de c est égal à r.*

Démonstration

Soit c un cycle de longueur r, si $r = 1$ alors $r = e$ et $o(c) = 1$. Si $r > 1$, c ne possède qu'une seule orbite Θ non réduite à un point et $\text{card}(\Theta) = r$. Soit $x \in \Theta$, d'après le théorème 2.1.8 on a

$$c^l(x) \neq x \text{ pour } 0 < l < r \text{ et } c^r(x) = x.$$

Comme $c(y) = y$ si $y \notin \Theta$. On a $c^r(x) = x, \quad \forall x \in X$ par suite $c^r = e$ et $c^l \neq e$ si $0 < l < r$. On en déduit que $o(c) = r$.

En particulier une transposition est d'ordre 2.

2.2 Générateurs de $\mathcal{S}_n$

2.2.1 Décomposition canonique d'une permutation

Soit $\sigma \in \mathcal{S}_n$ et $r \neq e$, le théorème suivant montre que σ se décompose de manière unique sous forme de cycles disjoints.

Théorème 2.2.1. *Toute permutation $\sigma \in \mathcal{S}_n$ est soit un cycle, soit un produit de cycles disjoints. Le groupe $\mathcal{S}_n$ est engendré par les cycles qu'il contient.*

Démonstration

Soient $\sigma \in S_n$, $S = \mathrm{Supp}(\sigma)$ et $p = |S|$. On fait la décomposition par récurrence sur p. Si $p = 0$, $|S| = 0 \Longrightarrow \sigma = e$ est un 1-cycle. Supposons $p > 0$ et soit $a_1 \in S$ et soit $\Theta = \Theta_\sigma(a_1) = \{a_1, a_2, \cdots, a_r\}$ l'orbite de a_1 suivant σ et $c_1 = (a_1, a_2, \cdots, a_r)$ le cycle de longueur r dont le support est Θ. Nous avons :

- si $r = n$, alors $\sigma = c_1$ est un cycle de longueur n.
- si $r < n$, Posons $Y = X \setminus \Theta$, on a $c_1(y) = y$, $\forall y \in Y$ et $c_1(x) = \sigma(x), x \in \Theta$ et la restriction de σ à Y est une permutation de Y. On considère

$$\begin{array}{rcl} \sigma' : X & \longrightarrow & X \\ x & \longmapsto & \sigma^{'}(x) = \begin{cases} x, & \text{si } x \in \Theta \\ \sigma(x), & \text{si } x \in Y \end{cases} \end{array}$$

Les permutations $\sigma^{'} \in S_n, \sigma^{'}$ et c_1 sont disjoints. Montrons que $\sigma = c_1\sigma^{'}$.

Soit $x \in X$, si $x \in Y$ alors $c_1\sigma^{'}(x) = \sigma^{'}(c_1(x)) = \sigma'(x) = \sigma(x)$.

Si $x \in \Theta, c_1 \circ \sigma^{'}(x) = c_1(x) = \sigma(x)$. Ainsi $c_1\sigma^{'}(x) = \sigma(x) \quad \forall x \in X$ d'où $\sigma = c_1\sigma^{'}$, $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma^{'}) = \emptyset$

$\mathrm{card}(\mathrm{Supp}(\sigma^{'})) \leq \mathrm{card}(\mathrm{Supp}(\sigma)) - r \leq p - 1$, par hypothèse de récurrence, il existe des cycles disjoints $c_2, c_3, \cdots, c_t$ tel que $\sigma^{'} = c_2 \cdots c_t$ d'où $\sigma = c_1c_2 \cdots c_t$

Exemple 2.2.2.

1. $$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$$

$\sigma_1 = (1,6,3)(2,4)(5)(7,8,9) = (1,6,3)(2,4)(7,8,9)$, (5) est un cycle de longueur 1, donc est à l'identité. Les cycles de longueur 1 sont omis dans la décomposition en cycles.

2.
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix} \in S_8$$

$\sigma_2 = (1,4,6)(2)(3,5,8)(7)$

3.
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 2 & 1 & 8 & 7 & 9 & 11 & 12 & 10 & 5 & 6 \end{pmatrix} \in S_{12}$$

$\sigma_3 = (1,3,2,4)(5,8,11)(6,7,9,12)(10)$

Définition 2.2.3. *Soit $\sigma \in S_n, \sigma \neq e$, la décomoposition de σ en cycles disjoints est unique. Cette décomposition est appelée décomposition canonique de de σ produit de cycles.*

Le théorème 2.2.1 montrent que l'ensemble des cycles de $\mathcal{S}_n$ constitue une famillie génératrice de $\mathcal{S}_n$.

Définition 2.2.4. *Une permutation $\sigma \in S_n$, est dite régulière si elle est décomposée en cycles disjoints de même longueur.*

Exemple 2.2.5.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 8 & 2 & 7 & 9 & 11 & 1 & 3 & 12 & 6 & 10 & 5 \end{pmatrix} \in S_{12}$$

$\sigma = (1,4,7)(2,8,3)(5,9,12)(6,11,10)$ est une permutation régulière

2.2.2 Ordre d'une permutation - Inverse d'une permutation

Soit $\sigma \in S_n$, une permutation avec $\sigma \neq e$, la décomposition de σ en cycles disjoints, permet de calculer plus facilement l'ordre de σ comme de montre le théorème suivant :

Théorème 2.2.6. *Soit $\sigma \in \mathcal{S}_n, n \geq 2$, $\sigma \neq e$ et $\sigma = c_1 c_2 \cdots c_t$ est la décomposition canonique de σ. Alors l'ordre de σ le groupe $\mathcal{S}_n$ est égal au* ppcm *des longueurs des cycles c_i, $1 \leq i \leq t$*

Démonstration

La démonstration se fait par récurrence sut t. Si $t = 2$, $\sigma = c_1 c_2$ où c_1 et c_1 sont disjioints. $\sigma = c_1 c_2$, c_1 et c_2 étant disjoints, on a $c_1 c_2 = c_2 c_1$ et $< c_1 > \cap < c_2 >= \{e\}$,

on en déduit que $o(\sigma) = o(c_1 c_2) = \text{ppcm}(o(c_1), o(c_2))$

$o(c_1) = l_1$=longueur de c_1, $o(c_2) = l_2$=longueur de c_2, d'un $o(\sigma) = \text{ppcm}(l_1, l_2)$

Supposons la propriété vraie á l'ordre $t-1$ et soit $\sigma = c_1c_2\cdots c_{t-1}c_t$ la décomposition de σ en cycles disjoints. On a $\sigma = \sigma' c_t$ et $\text{Supp}(\sigma') = \bigcup_{i=1}^{t-1}\text{Supp}(c_i)$ où $\sigma' = c_1c_2\cdots c_{t-1}$.

Donc $\text{Supp}(c_i)\cap\text{Supp}(c_t) = \bigcup_{i=1}^{t-1}\text{Supp}(c_i)\cap\text{Supp}(c_t) = \emptyset$, ainsi

$$o(\sigma) = \text{ppcm}(o(\sigma'), o(c_t)) = \text{ppcm}(o(c_1), o(c_2), \cdots, o(c_{t-1}), o(c_t))$$

cqfd.

Exemple 2.2.7.

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix} \in S_9$$

On a $\sigma_1 = (1,6,3)(2,4)(7,8,9) = c_1c_2c_3$ avec $c_1 = (1,6,3)$, $c_2 = (2,4)$ et $c_3 = (7,8,9)$

$$o(\sigma_1) = \text{ppcm}(3,2,3) = 6$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix} = (1,4,6)(3,5,8)$$

$$o(\sigma_2) = \text{ppcm}(3,3) = 3$$

$\sigma_1^{-1} = c_3^{-1}c_2^{-1}c_1^{-1} = (9,8,7)(4,2)(3,6,1)$, $\quad \sigma_2^{-1} = (8,5,3)(4,6,1)$

2.2.3 Décomposition d'une permutation en transposition

Soit $\sigma \in S_n$ une permutation. Les théorèmes suivants montrent que σ peut être décomposée en produit de transpositions et que $\mathcal{S}_n$ est engendré par les transpositions qu'il contient.

Théorème 2.2.8. *Toute permutation de $S_n (n \geq 2)$ se décompose en produit de transpositions.*

Démonstration

Comme toute permutation se décompose en produit de cycles, il suffit de montrer que tout cycle se décompose en produit de transpositions.

Soit $c = (a_1, a_2, \cdots, a_p)$ un cycle de longueur p, on a $c = (a_1,a_2)(a_2,a_3)(a_3,a_4)\cdots(a_{p-1},a_p)$ d'où le résultat

Exemple 2.2.9.

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix} = (1,6,3)(2,4)(7,8,9) = (1,6)(6,3)(2,4)(7,8)(8,9)$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix} = (1,4,6)(3,5,8) = (1,4)(4,6)(3,5)(5,8)$$

Théorème 2.2.10. *Pour $n \geq 2$, le groupe symétrique S_n est engendré par les transpositions*

$$(i, i+1) \quad 1 \leq i \leq n-1.$$

Démonstration Comme toute permutation est un produit de transposition il suffit de montrer qu'une transposition (p,q), $1 \leq p < q \leq n$ est le produit de transpositions de la forme $(i, i+1)$.

On fait la démonstration par récurrence sur $q - p$.
Si $q - p = 1$, on a $(p,q) = (p, p+1)$ le résultat est vrai. Supposons $q - p > 1$. on a $(p,q) = (q-1,q)(p,q-1)(q-1,q)$.

Par hypothèse de récurrence, $(p, q-1)$ est un produit de transpositionss de la forme $(i, i+1)$, on en déduit que (p,q) est produit de transpositions de la forme $(i, i+1)$.

Exemple 2.2.11.

1.
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} = (2,4,6,5) = (2,4)(4,6)(6,5)$$

$(2,4) = (3,4)(2,3)(3,4)$, $(4,6) = (5,6)(4,5)(5,6)$. Donc,

$$\sigma = (3,4)(2,3)(3,4)(5,6)(4,5)(5,6) = (3,4)(2,3)(3,4)(5,6)(4,5)$$

2.

$$\begin{aligned} (1,8) &= (7,8)(1,7)(7,8) = (7,8)(6,7)(1,6)(6,7)(7,8) \\ &= (7,8)(6,7)(5,6)(1,5)(5,6)(6,7)(7,8) \\ &= (7,8)(6,7)(5,6)(4,5)(1,4)(4,5)(5,6)(6,7)(7,8) \\ &= (7,8)(6,7)(5,6)(4,5)(3,4)(1,3)(3,4)(4,5)(5,6)(6,7)(7,8) \end{aligned}$$

2.3 Signature d'une permetation - Groupe Alterné

2.3.1 Signature d'une permutation

Définition 2.3.1. *Soit $\sigma \in \mathcal{S}_n$ et m le nombre d'orbite suivant σ. On appelle signature de σ l'entier $\varepsilon(\sigma) = (-1)^{n-m}$.*

Nous avons les cas particuliers suivants :

— Si $\sigma = e$, $\varepsilon(\sigma) = 1$, $m = n$

— Si $\sigma = \tau$ est une transposition, $m = n - 1$, $\varepsilon(\tau) = (-1)^{n-(n-)} = (-1)^1 = -1$

— Si σ est un l-cycle $m = n - l + 1$, $\varepsilon(\sigma) = (-1)^{n-(n-l+1)} = (-1)^{l-1}$

Dans le cas général les résultats suivants permettent de calculer la signature d'une permutation.

Théorème 2.3.2. *Soient $\sigma \in \mathcal{S}_n$ et τ une transposition, alors*

$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma).$$

Démonstration

Notons $\tau = (a, b)$, etv $\sigma' = \sigma\tau$ et m le nombre d'orbites suivant σ. Déterminons le nombre m' d'orbites suivant σ'. Toute σ-orbite qui ne contenant ni a, ni b est une σ'-orbite. Seules les σ-orbites contenant a ou b sont modifiées par l'action de τ. Soit $\Theta_\sigma(a)$ et $\Theta_\sigma(b)$ les orbites de a et b suivant σ. Posons $p = \text{card}(\Theta_\sigma(a))$ et $q = \text{card}(\Theta_\sigma(b))$. On a deux cas, ou bien $\Theta_\sigma(a)$ et $\Theta_\sigma(b)$ sont confondues ou bien elles sont disjointes.

1er **cas** $\Theta_\sigma(a) = \Theta_\sigma(b)$, $\quad a = \sigma^p(a)$ et $\Theta_\sigma(a) = \Theta_\sigma(b) = \{a, \sigma(a), \cdots, \sigma^{r-1}(a)\} = \Theta$

$b \in \Theta \Longrightarrow \exists r, 1 \leq r \leq r-1$ tel que $b = \sigma^r(a)$. on a $\Theta_{\sigma'}(a) = \{a, \sigma^{r+1}(a), \cdots, \sigma^{p-1}\}$ et $\Theta_{\sigma'}(a) = \{b, \sigma(a), \cdots, \sigma^{r-1}\}$ d'où $\Theta = \Theta_{\sigma'}(a) \cup \Theta_{\sigma'}(b)$ avec $\Theta_{\sigma'}(a) \cap \Theta_{\sigma'}(b) = \emptyset$. L'orbite communu de a et b suivant σ s'est scindée en deux orbites suivant σ'. On en déduit que $m' = m+1$, d'où $(-1)^{n-m'} = (-1)^{n-m-1} = -(-1)^{n-m}$ d'où $\varepsilon(\sigma') = -\varepsilon(\sigma)$ dans ce cas.

2 **cas** $\Theta_\sigma(a) \cap \Theta_\sigma(b) = \emptyset$

$\Theta_{\sigma'}(a) = \{a, \sigma(a), \cdots, \sigma^{q-1}(b), b, \sigma(a)\} = \Theta_{\sigma'}(b) = \Theta_\sigma(a) \cup \Theta_\sigma(b)$

Les orbites distinctes $\Theta_\sigma(a)$ et $\Theta_\sigma(b)$ de a et b suivant σ sont unifiées en une seule orbite $\Theta_{\sigma'}(a)$ de a suivant σ'. On déduit que $m' = m-1$, d'où $(-1)^{n-m'} = (-1)^{n-(m-1)} = -(-1)^{n-m}$ donc $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Dans tous les cas nous avons

$$\varepsilon(\sigma') = -\varepsilon(\sigma).$$

Corollaire 2.3.3. *Soit $\sigma \in \mathcal{S}_n$. Si σ est produit de p transposition alors*

$$\varepsilon(\sigma) = (-1)^p.$$

Démonstration

La démonstration se fait par récurrence sur le nombre p de transpositions. Si $p = 1$, σ est une transposition $\varepsilon(\sigma) = -1$. Supposons la priopriété vraie à l'ordre $p \geq 2$. Soit $\sigma = t_1 t_2 \cdots t_p t_{p+1}$ ou les t_i sont des transpositions. Posons $\gamma = t_1 t_2 \cdots t_p$, on a $\sigma = \gamma t_{p+1}$, d'après le théorème 2.3.2, $\varepsilon(\sigma) = -\varepsilon(\sigma) = -(-1)^p = (-1)^{p+1}$

Exemple 2.3.4.

Soit
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \in S_6$$
Les orbites sont $\Theta_{\sigma_1}(1) = \{1, 5, 3\}, \Theta_{\sigma_2}(1) = \{2\}, \Theta_{\sigma_1}(1) = \{4, 6\}$

Il y a trois orbites distinctes $\varepsilon(\sigma_1) = (-1)^{6-3} = (-1)^3 = -1$

$\sigma_1 = (1, 5, 3)(4, 5) = (1, 5)(5, 3)(4, 6)$,
$$\varepsilon(\sigma) = -1$$

Exemple 2.3.5.

Soit
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 8 & 2 & 7 & 9 & 11 & 1 & 3 & 12 & 6 & 10 & 5 \end{pmatrix}$$
$\Theta_{\sigma_2}(1) = \{1, 4, 7\}, \Theta_{\sigma_2}(2) = \{2, 8, 3\}, \Theta_{\sigma_2}(5) = \{5, 9, 12\}, \Theta_{\sigma_2}(6) = \{6, 11, 10\}$.

D' après le théorème 2.3.2
$$\varepsilon(\sigma_2) = (-1)^{12-4} = (-1)^8 = 1.$$
$\sigma_2 = (1, 4, 7)(2, 8, 3)(5, 9, 12)(6, 11, 10) = (1, 4)(4, 7)(2, 8)(8, 3)(5, 9)(9, 12)(6, 11)(11, 10)$.

D' après le corollaire 2.3.3,
$$\varepsilon(\sigma) = (-1)^8 = 1.$$

Corollaire 2.3.6. *L'application*
$$\begin{array}{rcl} \varepsilon : (\mathcal{S}_n, \circ) & \longrightarrow & (\{-1, 1\}, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$
est un homomorphisme surjectif de groupes.

Démonstration Soient σ et $\sigma^{'}$ deux éléments de $\mathcal{S}_n$, σ et $\sigma^{'}$ sont produit de p et q transpositions respectivement. $\sigma\sigma\prime$ est produit de $p + q$ transpositions, donc
$$\varepsilon(\sigma\sigma') = (-1)^{p+q} = (-1)^p(-1)^q = \varepsilon(\sigma)\varepsilon(\sigma^{'}).$$

Théorème 2.3.7. *Soit $n \in \mathbb{N} \setminus \{1\}$, et $\sigma \in \mathcal{S}_n$. Montrer*
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Définition 2.3.8. *Soit $\sigma \in \mathcal{S}_n$ et $i \in X$ et $j \in X$. On dit que i et j sont en inversion pour σ, si $i < j$ et $\sigma(i) > \sigma(j)$.*

Théorème 2.3.9. *Soit $\sigma \in \mathcal{S}_n$.*

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

où I_σ est le nombre total d'inversion de σ.

Théorème 2.3.10. *Soit $\sigma \in \mathcal{S}_n$ et $\sigma = c_1 c_2 \cdots c_t$ la décomposition de σ en cycles disjoints. Montrer que*

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{t}(\ell_i - 1)}$$

où ℓ_i est la longueur de c_i.

2.3.2 Groupes alternés

Définition 2.3.11. *Soit $\sigma \in S_n$, on dit que σ est permutation paire si $\varepsilon(\sigma) = 1$, σ est une permutation impaire si $\varepsilon(\sigma) = -1$.*

σ est une permutation paire si elle est décomposée en un nombre pair de transpositions. σ est impair si elle est décomposée en un nombre impair de transpositions.

Exemple 2.3.12.

1. Soit
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 8 & 2 & 7 & 9 & 11 & 1 & 3 & 12 & 6 & 10 & 5 \end{pmatrix}$$
La décomposition de σ en transposition donne
$$\sigma = (1,4)(4,7)(2,8)(8,3)(5,9)(9,12)(6,11)(11,10).$$
La permutation σ est paire.

2. $$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} = (1,5)(5,3)(4,6).$$
La permutation γ est impaire

Définition 2.3.13. *Soit $n \in \mathbb{N}^*$, l'ensemble des permutations paires est appelé groupe alterné d'ordre n et se note $\mathcal{A}_n$.*

$\mathcal{A}_n$ est le noyau de l'homomorphisme ε, il est donc un sous groupe normal de S_n. D'après le premier théorème d'isomorphisme le groupe $S_n/\mathcal{A}_n$ est isomorphe au groupe multiplicatif $(\{-1,1\}, \times)$. On en déduit que $|\mathcal{S}_n/\mathcal{A}_n| = 2$, d'où $|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{2} = \frac{n!}{2}$.
Soit $c = (a_1, a_2, \cdots, a_r) \in \mathcal{S}_n, p \leq n$, un cycle de longueur r et $\sigma \in \mathcal{S}_n$, on a le théorème suivant appelé principe de conjugaison.

Conjoncture 2.3.14. *Soit $c = (a_1, a_2, \cdots, a_r) \in \mathcal{S}_n$ un cycle de longueur r. Alors $\forall \sigma \in \mathcal{S}_n$, on a $\sigma c \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_r))$*

Démonstration Posons $c' = \sigma c \sigma^{-1}$

— Soit $1 \leq i < r$. On a $c'(\sigma(a_i)) = \sigma c \sigma^{-1}(\sigma(a_i)) = \sigma c(a_i) = \sigma(a_{i+1})$. De plus

$$c'(\sigma(a_r) = \sigma c \sigma^{-1}(\sigma(a_r)) = \sigma(c(a_r)) = \sigma(a_1).$$

— Si $x \in X$ et $x \notin \{\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_r)\}$ alors $\sigma^{-1}(x) \notin \{a_1, a_2, \cdots, a_r\}$ car σ est une bijection. Donc

$$c'(x) = \sigma c \sigma^{-1}(x) = \sigma(c\sigma^{-1}(x)) = \sigma(\sigma^{-1}(x)) = x.$$

Ainsi

$$\begin{cases} c'(\sigma(a_i)) = \sigma(a_{i+1}) \ 1 \leq i \leq r-1 \\ c'(\sigma(a_r)) = \sigma(a_1) \\ c'(x) = x \quad si \quad x \notin \{\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_r)\}. \end{cases}$$

On en déduit que $c' = (\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_r)$ d'où

$$\sigma c \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_r)).$$

2.3.3 Générateurs de $\mathcal{A}_n$

Dans $\mathcal{S}_n$ un cycle de longueur 3 est une permutation paire. Les résultats suivants montrent que le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles.

Lemme 2.3.15. *Dans $\mathcal{S}_n$, le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles.*

Démonstration. Soit $i < j < k < l$. Nous avons d'une part $(i, j)(j, k) = (i, j, k)$ et d'autre part $(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, j, k)(j, k, l)$.

Théorème 2.3.16. *Soit $n \geq 3$ un entier. Alors le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles de $\mathcal{S}_n$.*

Démonstration. Soit $\sigma \in \mathcal{A}_n$ une permutation paire, σ est le produit d'un nombre pair de transpositions. Or d'après le lemme 2.3.15 le produit de deux transpositions distinctes est, soit un 3-cycle si ces deux transpositions ont des supports non disjoints, sinon un produit de deux 3-cycles. On en déduit que σ est un produit de 3-cycles, d'où $\mathcal{A}_n$ est engendré par les 3-cycles de $\mathcal{S}_n$.

Théorème 2.3.17. *Soit $n \geq 3$ un entier. Alors le groupe alterné $\mathcal{A}_n$ est engendré par les $(n-2)$ 3-cycles de la forme $(1, 2, k)$ pour $3 \leq k \leq n$.*

Démonstration. Soit $\sigma \in \mathcal{A}_n$, comme $\mathcal{A}_n$ est engendré par les 3-cycles, σ est un produit de 3-cycles de la forme (i, j, k). D'après le principe de conjugaison on a

$$(i, j, k) = (1, 2, i)(2, j, k)(1, 2, i)^{-1} \text{ et } (2, j, k) = (1, 2, j)(1, 2, k)(1, 2, j)^{-1}.$$

On en déduit que le groupe alterné $\mathcal{A}_n$ est engendré par les $(n-2)$ 3-cycles de la forme

$$(1, 2, k) \text{ pour } 3 \leq k \leq n.$$

Chapitre 3

Actions de groupes sur un ensemble

3.1 Généralités sur les actions de groupes

Définition 3.1.1. *Soient G un groupe et X un ensemble non vide. On appelle action à gauche (opération) de G sur X une application*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longrightarrow g.x \end{aligned}$$

vérifiant les deux propriétés suivantes :

1. $\forall (g_1, g_2) \in G^2, \quad \forall x \in X, \quad g_1.(g_2.x) = (g_1 g_2).x$
2. $\forall x \in X, \quad e.x = x$ *où e est un l'élément neutre de G.*

Remarque 3.1.2. *On définit une action à droite de G sur X par*

$$\begin{aligned} X \times G &\longrightarrow X \\ (x, g) &\longrightarrow x.g \end{aligned} \quad \textit{vérifiant}$$

- $(x.g_1).g_2 = x.(g_1 g_2) \quad \forall (g_1, g_2) \in G^2$ et $\forall x \in X$
- $x.e = x$.

<u>Convention</u> : Dans la suite du cours, on appelle action d'un groupe G sur un ensemble non vide X, toute action à gauche de G sur X. On dit que G opère sur l'ensemble X.

Définition 3.1.3. *Soit G un groupe et X un ensemble non vide.*
Si G opère sur X on dit que X est un G-ensemble.

Définition 3.1.4. *Soit X un ensemble non vide, on appelle permutation de X, toute bijection de X dans X. On note $\mathcal{S}_X$ l'ensemble des permutations de X.*
Soit G un groupe et X un ensemble non vide, les résultats suivants montrent que la donnée d'une action de G sur X équivaut à la donnée d'un morphisme de G dans $\mathcal{S}_X$.

Proposition 3.1.5.

Proposition 3.1.6. *Soit G un groupe, X un ensemble non vide. Alors à tout morphisme de groupe $\varphi : G \longrightarrow \mathcal{S}_X$ on peut associer une action de G sur X.*

Démonstration. Soit $\varphi : G \longrightarrow \mathcal{S}_X$ un morphisme de groupe. On considère

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longrightarrow \varphi(g)(x) = g.x \end{aligned}$$

Montrons que cette application définit une action de G sur X.

1. Soit $(g_1, g_2) \in G^2$, $g_1.(g_2.1) = \varphi(g_1)(g_2.1) = \varphi(g_1)(\varphi(g_2(x))$
   $= (\varphi(g_1) \circ \varphi(g_2))(x) = \varphi(g_1 g_2)(x) = (g_1 g_2).x$
   donc $g_1.(g_2.x) = (g_1 g_2).x$
2. $\forall x \in X$, $e.x = \varphi(e)(x) = id_X(x) = x$.

1) et 2) entraînent que φ définit une action de G sur X. □

Définition 3.1.7. *Soit G un groupe opérant sur un ensemble X. Len oyau de l'action est le noyau du morphisme de groupe $\varphi : G \longrightarrow \mathcal{S}_X$.*

<u>Exemples</u> :

1. G opère sur lui - même par les translations

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longrightarrow g.x = gx \end{aligned}$$

2. Un groupe G opère sur lui-même par conjugaison

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longrightarrow g.x = gxg^{-1} \end{aligned}$$

   est une opération de G sur lui-même appelée **opération par conjugaison**.

3. Soit $n \in \mathbb{N}^*$, $\mathbb{K}$ un corps commutatif et unitaire $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre n et $GL_n(\mathbb{K})$ le groupe linéaire d'ordre n c'est-à-dire le groupe des matrices carrées d'ordre n inversibles.

   a) L'application

$$\begin{aligned} GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) &\longrightarrow \mathcal{M}_n(\mathbb{K}) \\ (P, M) &\longrightarrow PMP^{-1} \end{aligned}$$

   définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ par conjugaison.

b) L'application

$$\begin{aligned} GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) &\longrightarrow \mathcal{M}_n(\mathbb{K}) \\ (P, M) &\longrightarrow P^t M P \end{aligned}$$

définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ par congruence.

4. Soit G un groupe et S l'ensemble des sous - groupes de G, G opère sur S par conjugaison.

3.2 Orbites et Stabilisateurs d'une action de groupes

Définition 3.2.1. *Soit G un groupe et X un G-ensemble, $x \in X$.*
L'ensemble $G_x = \left\{ g \in g \ / \ g.x = x \right\}$ est un sous-groupe de G appelé stabilisateur de x ou sous groupe d'isotropie de x.

Soit G un groupe et X un G-ensemble.
On définit sur X la relation $\mathcal{R}_G$ suivante :

$$\forall x \in X, \ \forall y \in X \ x\mathcal{R}_G y \Longleftrightarrow \exists g \in G \ / \ y = g.x$$

$\mathcal{R}_G$ est une relation d'équivalence sur X.

Définition 3.2.2. *Soit G un groupe et X un G-ensemble.*
La classe d'équivalence de $x \in X$ modulo $\mathcal{R}_G$ est appelé orbite de x suivant G ou G-orbite de x.
On note par $\theta(x)$ la G-orbite de x

$$\theta(x) = \left\{ g.x \ / \ g \in G \right\}$$

Exemples :

1. Soit G un grope on considère l'action de G sur lui-même par translation à gauche.
$\forall x \in G, \quad G_x = \left\{ g \in G \ / \ gx = x \right\} = \{e\}$ e étant l'élément neutre de G

$$\theta(x) = \left\{ g.x \ / \ g \in G \right\} = G_x = G$$

2. Soit G un groupe on considère l'action de G sur lui-même par conjugaison.

$$G_x = \left\{ g \in G \ / \ gxg^{-1} = x \right\} = \left\{ g \in G \ / \ gx = xg \right\} = C_G(x)$$

centralisation de x dans G.
$\theta(x) = \left\{ gxg^{-1} \ / \ g \in G \right\}$ la classe de conjugaison de x, c'est aussi l'ensemble des conjugues de x.

3. Soit G un groupe et S_G l'ensemble des sous - groupes de G, on considère l'action de G sur S_G par conjugaison.

   Soit $H \in S_G$ un sous - groupe de G

   $G_H = \left\{ g \in G \ / \ gHg^{-1} = H \right\} = N_G(H)$ le normalisateur de H dans G.

   $\theta(H) = \left\{ gHg^{-1} \ / \ g \in G \right\}$ l'ensemble des conjugues de H.

3.3 Dénombrement des orbites

Soit G un groupe et X un G-ensemble, le théorème suivant montre que les stabilisateurs de deux éléments d'une même orbite sont des sous - groupes conjugués
de G.

Théorème 3.3.1. *Soient G un groupe et X un G-ensemble, alors*

$$\forall x \in X, \quad \forall y \in X, \quad x\mathcal{R}_G y \Longrightarrow G_x \ \ \textit{et} \ \ G_y \ \ \textit{sont conjugués}$$

Donc $|G_x| = |G_y|$, si x et y sont dans la même orbite, les stabilisateurs de x et y ont le même nombre d'éléments.

Démonstration :

On considère l'action de G sur X

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longrightarrow g.x \end{aligned}$$

$x\mathcal{R}_G y \Longleftrightarrow \exists g \in G \ / \ y = g.x$, montrons que $G_y = gG_xg^{-1}$
$t \in G_y \Longrightarrow t.y = yt(g.x) = g.x \Longrightarrow g^{-1}.(t.g.x) = x$
$\Longrightarrow (g^{-1}tg).x = x \Longrightarrow g^{-1}tg \in G_x \Longrightarrow t \in gG_xg^{-1}$
$\Longrightarrow G_y \subset g \ G_xg^{-1} \qquad (*)$
$b \in g \ G_xg^{-1} \Longrightarrow \exists a \in G_x \ / \ b = gag^{-1}$.
$y = g.x \Longrightarrow x = g^{-1}.y$ et $a \in G_x \Longrightarrow a.x = x = x$, donc
$b.y = (gag^{-1}).y = (ga).(g^{-1}.y) = (ga).x = g.(a.x) = g.x = y$
d'où $b \in G_y$, ainsi $gG_xg^{-1} \subset G_y \qquad (**)$
$(*)$ et $(**) \Longrightarrow G_y = gG_xg^{-1}$.
Le théorème suivant montre que le cardinal de l'orbite d'un élément $x \in X$ est égal à l'indexe du stabilisateur de x.

Théorème 3.3.2. *Soient G un groupe, X un G-ensemble et $x \in X$, alors*
$|\theta(x)| = \left[G : G_x \right]$.

Démonstration :

Soit $x \in X$ et G_x le stabilisateur de x.
On considère l'ensemble quotient de G par la relation d'équivalence à gauche modulo G_x, G/G_x et

$$\begin{array}{l} f : \theta(x) \longrightarrow G/G_x \\ y = ax \longrightarrow a.G_x \end{array},$$

montrons que f est une bijection.
Soit $b.G_x \in G/G_x$, posons $t = bx$, on a $f(t) = b/G_x$ donc f est surjective.
Soit $y_1 = a_1x \in \theta(x)$ et $y_2 = a_2x \in \theta(x)$ / $f(y_1) = f(y_2)$
$f(y_1) = f(y_2) \Longrightarrow a_1G_x = a_2G_x \Longrightarrow G_x = a_1^{-1}a_2G_x$
$\Longrightarrow a_1^{-1}a_2 \in G_x \Longrightarrow (a_1^{-1}a_2).x = x \Longrightarrow a_1.x = a_2.x \Longrightarrow y_1 = y_2$ donc f est injective.
f injective et surjective $\Longrightarrow f$ bijective. On en déduit que

$$\left|\theta(x)\right| = \left|G/G_x\right| = \left[G : G_x\right]$$

Corollaire 3.3.3. *Soit G un groupe fini et X un G-ensemble.
Le cardinal de chaque orbite suivant G est un diviseur de l'ordre $|G|$ de G.*

Corollaire 3.3.4. *Soit G un groupe fini et $x \in G$, le nombre de conjugues de x dans G est égal à $\left[G : C_G(x)\right]$.
L'indexe du centralisateur de x dans G.*

Démonstration :

On considère l'action de G sur lui-même par conjugaison. $\forall x \in G$, $\theta(x) = \{gxg^{-1} \;/\; g \in G\}$ est l'ensemble des conjugyes de x.

$$\begin{array}{l} G_x = \left\{g \in G \;/\; gxg^{-1} = x\right\} = \left\{g \in G \;/\; gx = xg\right\} \\ \left|\theta(x)\right| = \left[G : G_x\right] = \left[G : C_G(x)\right] \end{array}$$

Corollaire 3.3.5. *Soit G un groupe fini et H un sous - groupe de G alors le nombre de conjugues de H dans G est $\left[G : N_G(H)\right]$.
L'indexe du normalisateur de H dans G.*

Démonstration :

On considère l'action de G sur l'ensemble de ses sous - groupes S_G.

$$H \in S_G, \quad G_H = \left\{g \in G \;/\; gHg^{-1} = H\right\} = N_G(H)$$

normalisateur de H dans G et $\theta(H) = \left\{gHg^{-1} \;/\; g \in G\right\}$ l'ensemble des conjugues de H.

$$\left|\theta(H)\right| = \left[G : G_H\right] = \left[G : N_G(H)\right]$$

Théorème 3.3.6. *Soit* G *un groupe et* X *un* G*-ensemble fini.*
Si $(x_i)_{1\leq i\leq r}$ *est un ensemble de représentants des* G*-orbites alors*

$$|X| = \sum_{i=1}^{r}\Big[G : G_{x_i}\Big]$$

<u>**Démonstration**</u> **:**

Soit G un groupe et X un G-ensemble fini. Le nombre des G-orbites est fini. Comme les G-orbites sont les classes d'équivalences modulo R_G, les G-orbites distinctes constituent une partition de X. Soit $(x_i)_{1\leq i\leq r}$ une famille de représentatn des G-orbites distinctes.

$$X = \bigcup_{i=1}^{r}\theta(x_i) \ \text{ et } \ \theta(x_i)\cap\theta(x_j) = \phi \ \text{ si } \ i\neq j.$$

Donc $\qquad |X| = \left|\bigcup_{i=1}^{r}\theta(x_i)\right| = \sum_{i=1}^{r}|\theta(x_i)|.$

Comme pour tout $\quad i\in[[1,r]], \quad |\theta(x_i)| = [G : G_{x_i}]$, on a $|X| = \sum_{i=1}^{r}[G : G_{x_i}]$.

Corollaire 3.3.7. *Soit* G *un groupe fini et* $(x_i)_{1\leq i\leq r}$ *une famille de représentants des classes de conjugaison,*

$$\forall x\in G,\ \theta(x) = \Big\{gxg^{-1}\ /\ g\in G\Big\}$$

est la classe de conjugaison de x, $\quad G_x = C_G(x)$.
Soit $(x_i)_{1\leq i\leq r}$ *une famille de représentants des classes de conjugaison*

$$|G| = \sum_{i=1}^{r}[G : G_{x_i}] = \sum_{i=1}^{r}\Big[G : C_G(x_i)\Big].$$

Equation aux classes et Lemme de Burnside

Soit G un groupe opérant sur lui-même par conjugaison et $Z(G)$ le centre de G, $\quad Z(G) = \Big\{x\in G\ /\ ax = xa, \quad \forall a\in G\Big\}$

$x\in Z(G)\Longleftrightarrow C_G(x) = G$, donc $x\in Z(G)\Longleftrightarrow\Big[G : C_G(x)\Big] = 1$

$x\in Z(G)\Longleftrightarrow\theta(x) = \{x\}$

Définition 3.3.8. *Soit* G *un groupe et* X *un* G*-ensemble, on appelle orbite ponctuelle, toute* G*-orbite réduite à un point.*

Théorème 3.3.9. *(Equation aux classes)*

Soit G *un groupe fini de centre* $Z(G)$ *et* $(x_i)_{1\leq i\leq \ell}$ *un ensemble de représentants des classes de conjugaison distinctes et non ponctuelles de* G*. Alors*

$$|G| = |Z(G)| + \sum_{i=1}^{\ell}\Big[G : C_G(x_i)\Big].$$

Démonstration :

On fait opérer G sur lui-même par conjugaison.
Si G est abélien, les classes de conjugaison sont ponctuelles et $G = Z(G)$. Donc la forme est vraie dans ce cas
Supposons G non abélien donc $Z(G) \neq G$.
Soit $(x_i)_{1 \leq i \leq r}$ un ensemble des représentants de G-orbites.
Soit ℓ l'ensemble de ces représentants non ponctuels, $1 \leq \ell \leq r$.
On suppose que les $(x_i)_{1 \leq i \leq p}$ sont les représentants non ponctuels

$$x_i \notin Z(G), \text{ pour } 1 \leq i \leq \ell \text{ et } x_i \in Z(G), \quad \ell + 1 \leq i \leq r.$$

D'après le théorème 3, $|G| = \sum_{i=1}^{r} [G : G(x_i)] = \sum_{i=1}^{r} [G : C_G(x_i)]$

$$|G| = \sum_{i=1}^{\ell} [G : C_G(x_i)] + \sum_{i=\ell+1}^{r} [G : C_G(x_i)] = \sum_{i=1}^{\ell} [G : G(x_i)] + \sum_{x \in Z(G)} \{x_i\}$$

$$|G| = |Z(G)| + \sum_{i=1}^{\ell} [G : C_G(x_i)].$$

Définition 3.3.10. *Un G-ensemble X est dit fini si G et X sont finis.*

Définition 3.3.11. *Soit GF un groupe et X un G-ensemble*

1. *On dit que G opère transitivement sur X si*

$$\forall x \in X \; et \; \forall y \in X, \quad \exists g \in G \; / \; y = g.x$$

2. *On dit que G opère fidèlement sur X si le morphisme $\varphi : G \longrightarrow \mathcal{S}_X$ est injectif.*

Donc si G opère transitivement sur X, il ya une seule orbite suivant cette action.

Définition 3.3.12. *Un G-ensemble X est homogène si G opère transitivement sur X.*

Exemples :

1. Un groupe G opère transitivement et fidèlement sur lui-même par translation à gauche.
2. Soit $G \neq \{e\}$ un groupe, l'opération de G sur lui-même par conjugaison n'est ni transitive, ni fidèle.
3. Soit X un G-ensemble, alors G opère transitivement sur chaque orbite.

Définition 3.3.13. *Soit X un G-ensemble. L'ensemble $X^G = \left\{x \in X, g.x \quad \forall g \in G\right\}$ est appelé ensemble de points fixes sous l'action de G.*

Pour $g \in G$, *on note* $X^g = \Big\{x \in X, g.x = x\Big\}$ *l'ensemble des éléments de* X *fixes par* g *et par* $F(g) = |X^g| = card(X^g)$.
La formule suivante de Burnside est très utile en combinatoire elle donne le nombre des G*-orbites suivant l'action de* G.

Théorème 3.3.14. *(Formules de Burnside) Soit* X *un* G*-ensemble fini,* N *le nombre des* G*-orbites,*

$$X^g = \Big\{x \in X, g.x = x\Big\} \quad et \qquad F(g) = |X^g|. \text{ Alors on a :}$$

$$N = \frac{1}{|G|} \sum_{g \in G} F(g).$$

<u>**Démonstration**</u> **:**

Posons $E = \Big\{(g, x) \in G \times X \ / \ g.x = x\Big\}$

$$E = \bigcup_{g \in G} \Big\{(g, x) \ / \ x \in X^g\Big\} = \Big\{\bigcup_{g \in G} (\{g\} \times X^g)\Big\}.$$

les $\{g\} \times X^g$ sont deux à deux disjoints, donc

$$|E| = \sum_{g \in G} |\{g\} \times X^g| = \sum_{g \in G} |X^g| = \sum_{g \in G} F(g) \tag{3.1}$$

$E = \bigcup_{x \in X} \Big\{(g, x) \ / \ g \in G_x\Big\}$ G_x étant le stabilisateur de x.

Les ensembles $\Big\{(g, x) \ / \ g \in G_x\Big\} = G_x \ X\{x\}$ sont deux à deux disjoints donc

$$|E| = \sum_{x \in X} |G_x \ X\{x\} = \sum_{x \in X} |X|.$$

Soit $\theta(x_1), \ \theta(x_2), \cdots, \theta(x_N)$ les G-orbites distinctes.
comme $X = \bigcup_{i=1}^{N} \theta(x_i)$, on a

$$|E| = \sum_{i=1}^{N} \sum_{x \in \theta(x_i)} |G_x|.$$

Or $\forall x \in \theta(x_i)$ et $\forall y \in \theta(x_i)$, G_x et G_y sont conjugués dans G donc, $|G_x| = G_y|$. D'où $\sum_{x \in \theta(x_i)} |G_x| = |\theta(x)|.|G_x|$. Comme $|\theta(x)| = [G : G_x]$, on a

$$\sum_{x \in \theta(x_i)} |G_x| = |G_x|.[G : G_x] = |G| \qquad \text{d'après Lagrange). Donc}$$

$$E| = \sum_{i=1}^{N} |G| = N \times |G| \tag{3.2}$$

(1.1) et **(1.2)** $\Longrightarrow N|G| = \sum_{g \in G} F(g) \Longrightarrow N = \frac{1}{|G|} \sum_{g \in G} F(g)$ d'où la formule de Burnside.

3.4 Applications aux p-groupes

Définition 3.4.1. *Soit* p *un nombre premier. Un groupe* G *est un* p*-groupe si* $|G|$ *est une puissance de* p. $|G| = p^n \quad n \in \mathbb{N}^*$.

Lemme 3.4.2. *Soit* G *un p-groupe opérant sur un ensemble fini* X *et soit* X^G *l'ensemble des points fixes de* X *sour l'action de* G $X^G = \left\{ x \in X \ / \ \forall g \in G, \ g.x = x \right\}$. *Alors* $|X| \equiv |X^G|$ *(modulo p).* $|X|$ *est conjugué à* $|X^G|$ *(modulo p).*

<u>Démonstration</u> :

D'après le théorème 3, $|X| = \sum_{i=1}^{r} [G : G_{x_i}] = \sum_{i=1}^{r} |\theta(x_i)|$ où $(x_i)_{1 \leq i \leq r}$ est un ensemble de représentatnts des G-orbites distinctes $\theta(x_i)$ l'orbite de x_i

$$|X| = \sum_{x \in X^G} |\theta(x)| + \sum_{x \notin X^G} |\theta(x)|$$

or $x \in X^G \Longleftrightarrow \theta(x) = \{x\}$ et $x \notin X^G \Longrightarrow |\theta(x)| > 1$.
Comme $|\theta(x)|$ divise $|G| = p^n, \ n \in \mathbb{N}^* \left| \sum_{x \notin X^G} |\theta(x)| \right| = k_p = |X| = \sum_{x \in X^G} |\theta(x)| + \sum_{x \notin X^G} |\theta(x)| = |X^G| \sum_{x \notin X^G} |\theta(x)| = |X^G| + k_p$.
Donc $\quad |X| \equiv |X^G|$ *mod p.*

Théorème 3.4.3. *(Burnside)*

Soit G *un* p*-groupe d'ordre* p^n *où* p *est un nombre premier et* $n \in \mathbb{N}^*$. *Alors* $Z(G) \neq \{e\}$. *Le centre de* G *n'est pas réduit à* $\{e\}$ e *étant l'élément neutre de* G.

<u>Démonstration</u> :

On fait opèrer G sur G par conjugaison. L'ensemble des points fixes de G pour cette action est $Z(G)$.
D'après le lemme ci - dessus $|G| \equiv |Z(G)| modulo \ p, \quad \exists \lambda \in \mathbb{N}^*$ tel que

$$|G| = |Z(G)| + \lambda_p, \quad |Z(G)| = |G| - \lambda_p = p^n - \lambda_p = (p^{n-1} - \lambda)_p \Longrightarrow |Z(G)|$$

est un multiple de $p \Longrightarrow |Z(G)| \geq p \Longrightarrow Z(G) \neq \{p\}$.

Corollaire 3.4.4. *Soit* G *un groupe d'ordre* p^2 *où* p *est un nombre premier. Alors* G *est abélien.*

<u>Démonstration</u> :

$|G| = p^2$ G est un p-groupe, d'après le théorème 6 de Burnside $|G(G)| \geq p$. Comme $|Z(G)|$ divise $|G|$ on a

$$|Z(G)| = p \ \text{ ou } \ |Z(G)| = p^2.$$

. Si $|Z(G)| = p$, $\left|G/Z(G)\right| = p$ premier $\Longrightarrow G/Z(G)$ est un groupe cyclique $\Longrightarrow G$ est abélien donc $|G| = p$. Donc $|Z(G)| = p^2$ d'où $Z(G) = G$ et G est abélien.

Exercice :

Soit $n \geq 1$, p un nombre premier et $q \in \mathbb{N}^* \ / \ 0 \leq q \leq n$.
Montrer que tout groupe non abélien G d'ordre p^n possède un sous - groupe normal H d'ordre p^q.

Indication : On raisonnera par récurrence forte sur n et on applique l'hypothèse de récurrence à $G/Z(G)$.

Exercice : Soit G un groupe fini et H un sous - groupe de G tel que $[G : H] = p$ est le plus petit nombre premier divisant $|G|$. Montrer que H est un sous - groupe normal de G.

Indication : Utiliser l'action de H sur (G/H) par translation à gauche et l'équation aux classes associée à cette action.

3.5 Produit semi - direct de groupes

Soient G un groupe et N et H deux groupes.

Définition 3.5.1. *Une suite de morphismes de groupes est la donnée de groupes N, G, H et de deux morphismes $f : N \longrightarrow G$ et $g : G \longrightarrow H$. Cette situation est représentée ainsi : $N \xrightarrow{f} G \xrightarrow{g} H$.*
Cette suite est dite exacte si $Imf = kerg$.
Soit G un groupe et N un sous - groupe normal de G $N \lhd G$ et G/N le groupe quotient. On cherche à reconstituer G en connaissant N et G/N. De façon générale soit G, N et H trois groupes. On cherche tous les groupes G tels qu'on ait une suite exacte $\{e_N\} \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow \{e_H\}$.

Définition 3.5.2. *Soit N et H deux groupes. Un groupe G s'appelle extension de N par H par N) si on a une suite exacte de morphismes de groupes*

$$\{e\} \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow \{e_H\}.$$

e_N et e_H étant les éléments neutres de N et H respectivement.

Soient N et H deux groupes, la notion de produit direct et produit semi - direct permettent de déterminer une extension de N par 'H pour des cas particuliers.

3.5.1 Produit direct de deux sous - groupes d'un groupe G

Définition 3.5.3. *Soient G un groupe, N et H deux sous - groupes normaux de G ($N \lhd G$ et $H \lhd G$). On dit que G est produit direct de N et H. si :*

1. $G = N_H$
2. $N \cap H = \{e\}$ *e étant l'élément neutre de G.*

Théorème 3.5.4. *Soient G un groupe, N et H deux sous - groupes normaux de G. Si G est produit direct de N et H alors G est isomorphe à $N \times H$.*

<u>Démonstration</u> :

On suppose $G = NH$ et $N \cap H = \{e\}$. On considère

$$\begin{array}{l} f : G \longrightarrow N \times H \\ x = nh \longrightarrow f(x) = (n, h) \end{array}.$$

Soit $x_1 = n_1h_1$ et $x_2 = n_2h_2$ deux éléments de G tels que $x_1 = x_2$

$$\begin{array}{l} x_1 = x_2 \Longrightarrow n_1h_1 = n_2h_2 \Longrightarrow n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H \Longrightarrow n_1 = n_2 \text{ et } h_1 = h_2 \\ \Longrightarrow (n_1, h_1) = (n_2, h_2) = (n_2, h_2) \Longrightarrow f(x_1) = f(x_2). \end{array}.$$

Donc f définit une application. De plus f est surjective. **(1)**.

Soit $n \in \mathbb{N}$ et $h \in H$, montrons que $nh = hn$, (tout élément n de N commute avec tout élément de h de H).

$x = nhn^{-1}h^{-1} = (nhn^{-1})h^{-1} \in H$ car $H \lhd G$ de même $x = n(hn^{-1}h^{-1}) \in N$ car $N \lhd G$.

donc $x = nhn^{-1}h^{-1} \in N \cap H = \{e\} \Longrightarrow nhn^{-1}h^{-1} = e$

$\Longrightarrow (nh)(hn)^{-1} = e \Longrightarrow nh = hn.$

Montrons que f est un morphisme de groupes.

Soient $x_1 = n_1h_1 \in G$ et $x_2 = n_2h_2 \in G$ tel que

$$\begin{aligned} f(x_1, x_2) = f(n_1h_1\ n_2h_2) = f(n_1n_2\ h_1h_2) &= n_1n_2\ h_1h_2 \\ &= n_1h_1\ n_2h_2 \\ &= f(x_1)\ f(x_2) \end{aligned}$$

donc f est un morphisme de groupes. **(2)**

Soit $x = nh \in Kerf$, $f(x) = (e, e) \Longrightarrow (n, h) = (e, e) \Longrightarrow x = e$ et $****$

$\Longrightarrow x = e$ donc f est injective **(3)**

(1), **(2)** et **(3)** entraînent que f est un isomorphisme de groupes.

<u>Exemple</u> :

Soit G le sous - groupe du groupe symétrique $\mathcal{S}_4$ constitue l'élément neutre de e, et des doubles transpositions

$a = (1, 2)(3, 4)$, $b = (1, 3)(2, 4)$ et $c = (1, 4)(2, 3)$

$G = \{e, a, b, c\}$, $N = \{e, a\}$ et $H = \{e, b\}$

G est produit direct de N et H.

3.5.2 Produit semi - direct de deux sous - groupes d'un groupe

Définition 3.5.5. *Soient G un groupe, N et H deux sous - groupes de G. On dit que G est le produit semi - directe de N par H si :*

1. $N \lhd G$ *N est un sous - groupe normal de G*
2. $G = NH$
3. $N \cap H = \{e\}$

On note $G = N \lhd H$

Définition 3.5.6. *Soient G un groupe et $N \rtimes G$ un sous - groupe normal de G. Si H est un sous - groupe de G tel que $G = N \rtimes H$. On dit que H est un complément de N dans G.*

Exemples : Groupes d'idéaux de degré n avec $n \geq 3$

Soit $n \geq 3$ un entier naturel et D_n le groupe d'ordre $2n$ engendré par deux éléments r et s vérifiant $0(r) = n,\ 0(s) = 2,\ 0(rs) = 2,\ \ 0(sr) = 2.$

Lemme 3.5.7. *$\forall j \in \mathbb{Z}$ et $\forall h \in \mathbb{Z}$, on a $s^k r^j s^{-k} = r^{(-1)}j.$*

Démonstration :

$0(sr) = 2 \Longrightarrow srsr = e \Longrightarrow srs = r^{-1} \Longrightarrow srs^{-1} = r^{-1}$
$\Longrightarrow \forall j \in \mathbb{Z}\ \ sr^j s^{-1} = (srs^{-1})^j = r^{-1}$ donc la propriété est vraie par $k = 1$.
Supposons la vraie à l'ordre $k-1$ avec $k \geq 1$.

$$s^k r^j s^{-k} = s(s^{k-1} r^j s^{-k+1})s^{-1} = qe^{(-1)k-1}j)s = r^{-(-1)^{k-1}j} = r^{(-1)^k j}.$$

Donc la propriété est vraie à l'ordre k. En posant $\ell = -k$. On montre de même que la propriété est vraie pour $k < 0$ d'où elle est vraie $\forall k \in \mathbb{Z}$ et $\forall j \in \mathbb{Z}$.

Théorème 3.5.8. *Soit G un groupe d'ordre $2n$ engendre par deux éléments a et b vérifiant $0(a) = n,\ 0(b) = 2,\ 0(ab) = 0(ba) = 2$. Alors G est isomorphe à D_n.*

Démonstration :

On considère $D_n = \langle r, s \rangle,\ 0(r) = n,\ 0(s) = 2.$
Posons $N = \langle r \rangle$ H est un sous - groupe cyclique de D_n

$$[D_n : N] = \frac{|D_n|}{|N|} = \frac{2n}{n} = 2, \text{ donc } N \text{ est normal dans } D_n$$

On a deux classes à droite modulo N, N et M_s

$$D_n = M \cup N_s = \left\{ e, r, r^2, \cdots, r^{n-1}, s, rs, r^2 s, \cdots a^{n-1} s \right\}.$$

De même $G = \left\{e, a, \cdots, a^{n-1}, b, ab, \cdots, a^{n-1}b\right\}$ tout élément $x \in D_n$ est de la forme $x = r^j s^k$ avec $0 \leq j \leq n-1$ et $0 \leq k \leq 1$.
De même un élément de G est de la forme $a^j b^k$.
On considère l'application

$$\begin{aligned} f : D_n &\longrightarrow G \\ x = r^j s^k &\longrightarrow f(x) = a^j b^k \end{aligned}$$

Montrons que f est un morphisme de groupe.
Soit $x = r^j s^k \in D_n$, $x' = r^{j'} s^{k'} \in D_n$.
$xx' = r^j s^k r^{j'} s^{k'} = r^j (s^k r^{j'} s^{j'}) s^{k+k'} = r^j r^{(-1)^{k'} j} \; s^{k+k'} = r^{(-1)^{k'} j'} \; s^{k+k'}$
$f(xx') = a^{j+(-1)^{k'} j'} \; b^{k+k'}$.
$f(x)f(x') = a^j b^k \; a^{j'} b^{k'} = a^{j+(-1)^{k'} j'} \; b^{k+k'}$
ainsi $f(xx') = f(x)\; f(x')$, f est un morphisme surjectif de groupe. Comme $|D_n| = |G| = 2n$, f est un isomorphisme.

Définition 3.5.9. *Le groupe D_n d'ordre $2n$ engendre par deux éléments r et s vérifiant $(0(r) = n,\ 0(s) = 2,\ 0(sr) = 2$ est applé groupe du dual de degré n.*

Remarque 3.5.10. *Soit $n \geq 3$ et $\mathcal{P}_n$ un polynôme régulier à n sommets dans le plan. D_n est l'ensemble des isométries du plan qui fassent invariant le polynôme $\mathcal{P}_n$. Les éléments de D_n laissent globalement invariant l'ensemble des n sommets du polynôme. Ces isométries sont constituées des n rotations de centre 0, centre du polygone, d'angles $\dfrac{2k\pi}{n}$, $0 \leq k \leq n-1$ et les n symétries par rapport aux axes du polygones.*
r est la rotation de cnetre 0 et d'angle $\dfrac{2\pi}{n}$, s est la symétrie d'axe (A_1) où A_1 est l'un des sommets qui situe sur l 'axe des abscisses.
$D_n = \langle r, s\rangle$, $0(r) = n,\ 0(s) = 2$ $N = \langle r\rangle$ et $H = \langle s\rangle$
D_n est le produit semi - dirct de N par H.

3.5.3 Produit semi- direct des groupes (Produit semi - direct externe

Soient N et H deux groupes et *Aut* N le groupe des automorphismes de groupes de N. Un morphisme

$$\begin{aligned} \varphi : H &\longrightarrow Aut\ N \\ h &\longrightarrow \varphi(h) = \varphi_n \end{aligned}$$

définit sur le produit cartésien $N \times H$ la loi suivante

$$(n, h)(n', h') = (n(h.n'),\ hh')$$

Proposition 3.5.11. *La loi* $(n,k)(n',h') = (n(h.n'),\ hhj')$ *définit sur* $N \times H$ *une structure de groupe noté* $N \rtimes_\varphi H$.

<u>Démonstration</u> : La loi est interne

1. Soient $(n,h), (n',h')$ et (n'',h'') trois éléments de $N \times H$

$$
\begin{aligned}
\Big[(n,h)(n',h')(n'',h'')\Big] &= (n(h.n'), hh')(n'',h'') \\
&= (n(h.n')(hh'.n''), (hh')h'') \\
&= (n(h.n')(h.(h'.n''), (hh')h'') \\
&= (n - \varphi_h(n')(\varphi_h(h'.n''), (hh')h'') \\
&= (n\varphi_h(n'(h'.n''), (hh')h'') \\
&= (n,h)(n'(h'.n''), h'h'') \\
&= (n,h)\Big[(n',h')(n'',h'')\Big]
\end{aligned}
$$

   donc on a l'associativité.

2. Soit e_N l'élément neutre de N et e_H celui de H.
   (e_N, e_H) est l'élément neutre de $N \times H$ pour cette loi

3. Soit $(n,h) \in N \times H$, on considère $n' = \varphi_h^{-1}(n^{-1}$ et $h' = h^{-1}$
   (n',h') est l'inverse de (n,h).

Définition 3.5.12. *Le groupe* $N \rtimes_\varphi H$ *est appelé semi - direct du groupe* N *par le groupe* H *relativement à* φ.

Proposition 3.5.13. *Soit* N *et* H *deux groupes,* $\varphi : H \longrightarrow Aut(N)$ *définissant une action de* H *et* $G = N \rtimes_\varphi H$ *le produit semi - direct de* N *par* H *relativement à* φ. *Alors :*

1. les applications

$$
f : \begin{array}{l} H \longrightarrow G \\ h \longrightarrow (e_N, h) \end{array} \quad et \quad g : \begin{array}{l} N \longrightarrow G \\ x \longrightarrow (x_1, e_H) \end{array}
$$

   sont des morphismes injectifs de groupes.

2. Si $H' = Imf$ *et* $N' = Img$, *alors* G *est produit semi - direct du sous - groupe* N' *par le sous - groupe* H'.

<u>Démonstration</u> :

1. Soit $h_1, h_2 \in H$, $f(h_1h_2) = (e_N, h_1h_2)$

$$
\begin{aligned}
&(e_N, h_1)(e_N, h_2) && = (e_N(h_1.e_N), h_1h_2) \\
&h_1.e_N = \varphi_{h_1}(e_N) && = e_N \ \text{ car } \ \varphi_{h_1} \in Aut(N) \\
&\text{donc } (e_N, h_1).(e_N, h_2) && = (e_N, h_1h_2) \Longrightarrow f(h_1h_2) = f(h_1)f(h_2)
\end{aligned}
$$

f est un morphisme de groupes.

$h \in Kerf \Longleftrightarrow f(h) = (e_N, e_H) \Longleftrightarrow (e_N, h) = (e_N, e_H) \Longrightarrow h = e_H$

$\Longleftrightarrow Kerf = \{e_H\}$

Soit $x_1, x_2 \in N$, $g(x, x_2) = (x_1x_2, e_H)$

$$\begin{aligned}(x_1, e_H).(x_2, e_H) = (x_1(e_H.x_2),\ e_H.x_2),\ e_He_H) &= (x_1\ \varphi_{e_H}(x_2), e_H) \\ &= (x_1x_2, e_H)\end{aligned}$$

Donc $g(x_1x_2) = g(x_1)\ g(x_2)$, g est un morphisme de groupes

$x \in Kerg \Longleftrightarrow g(x) = (e_N, e_H) \Longleftrightarrow (x = e_N \quad Kerg = \{e_N\}$ g est injectif.

2. Posons $H' = Imf$, $N' = Img$. H' et N' sont des sous - groupes de G.

   $H' = \Big\{(e_N, h)\ /\ h \in H\Big\}$ et $N' = \Big\{(n, e_H)\ /\ n \in N\Big\}$

   a) Soient $(n, e_H) \in N'$ et $(x, h) \in G$

$$\begin{aligned}(x,h)(n,e_H)(x,h)^{-1} &= (x,h)\Big[(n,e_H)(\varphi_h^{-1}(x^{-1}), h^{-1})\Big] \\ &= (x,h)(n(e_H.\varphi_h^{-1}(x^{-1}), \varphi_h^{-1}) \\ &= (x,h)(n, \varphi_h^{-1}(x^{-1}), h^{-1}) \\ &= (x(h.(n\ \varphi_h^{-1}(x^{-1}), hh^{-1} \\ &= (x\ \varphi_h(n\ \varphi_h^{-1}(x^{-1})), e_H) \\ &= (x\ \varphi_h(n)x^{-1},\ e_H) \in N'.\end{aligned}$$

Donc N' est normal dans G

b) $(x, h) \in N' \cap H' \Longleftrightarrow (x, h) \in N'$ et $(x, h) \in H' \Longleftrightarrow x = e_N$ et $h = e_H$.

Donc $N' \cap H' = \Big\{(e_N, e_H)\Big\}$

c) $$\begin{aligned}\forall x \in N' \text{ et } \forall h \in H,\quad (x, e_H).(e_N, h) &= (x(\varphi_{\varphi_{e_H}}(e_N), e_Hh) \\ &= (x, h)\end{aligned}$$

a) et **b)** et **c)** entraînent que $G = N' \rtimes H'$.

Critère de décomposition en produit semi - direct

Soient N, H, G trois groupes d'éléments neutres e_N, e_H et e.

Soit $\{e_N\} \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow \{e_H\}$ une suite exacte i est injectif, p surjectif et $Imi = Kerp$.

Posons $N' = i(N) = Kerp$ et on suppose qu'il existe un sous - groupe H' de G tel que la restriction f de p à H' soit un isomorphisme de H' à H.

On dit que H' est relèvement de H.

Théorème 3.5.14. *Si on a une suite exacte*

$$\{e_N\} \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow \{e_H\}$$

et s'il existe un relèvement H' *de* H; *alors* G *est isomorphe au produit semi - direct* $N \rtimes H$.

Démonstration :

Posons $N' = i(N) = Kerp$. Comme i est un morphisme de plus $N' = Kerp$,
$N' \lhd G$. **(1)**

Soit H' un relèvement de H, $f = p/H' : H' \longrightarrow H$ est un isomorphisme. Pour montrer que G est isomorphe $N \rtimes H$ il suffit de montrer que G est le produit semi - direct de ses sous - groupes N' et H'.

Soit $g \in G$, $p(g) \in H \Longrightarrow \exists h \in H' \;/\; p(g) = p(h)$
$p(g) = p(h) \Longrightarrow p(gh^{-1}) = e_H \Longrightarrow gh^{-1} \in Kerp = N' \Longrightarrow \exists n \in N' \;/$
$gh^{-1} = n \Longrightarrow g = nh \in N'H' \Longrightarrow G = N'H'$ **(2)**
$x \in N' \cap H' \Longrightarrow x \in N'$ et $x \in H'$
$x \in N' = Kerp \Longrightarrow p(x) = e_H = p(e) \Longrightarrow f(x) = f(e) \Longrightarrow x = e$
donc $N' \cap H' = \{e\}$ **(3)**.
(1), **(2)** et **(3)** entraînent que $G = N' \rtimes G'$.

Exemples :

1. Soient $C_n = \langle a \rangle$ un groupe cyclique d'ordre n et $C_2 = \langle b \rangle$ un groupe cyclique d'ordre 2.
   On considère $\varphi : C_2 \longrightarrow Aut(C_n)$ défini par
   $$\varphi(e) = \varphi_e = id_{C_n} \text{ et } \varphi(b) = \varphi_b, \text{ avec } \varphi_b(x) = x^{-1} \quad \forall x \in c_n$$
   φ est un morphisme de groupes. $D_n = C_n \rtimes_\varphi C_2$ le produit semi - direct de C_n par C_2 relativement à φ s'identifie au groupe d'idéal de degré n.
2. Soit $n \in \mathbb{N}^*$, $\mathcal{S}_n$ et $\mathcal{A}_n$ les groupes symétriques et alterné.
   Soit $(\{-1, 1\}, X)$ le groupe multiplicatif isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
   Soit ε la signature, on a la suite exacte
   $$\{id\} \longrightarrow \mathcal{A}_n \xrightarrow{i} \mathcal{S}_n \xrightarrow{\varepsilon} \{-1, 1\} \longrightarrow \{1\}$$
   i est l'injection canonique de $\mathcal{A}_n$ dans $\mathcal{S}_n$.
   Soit $\tau \in \mathcal{S}_n$, une transposition, $H' = \{e, \tau\} = \langle \tau \rangle$ est la relation de ε à H' est un isomorphisme de H' vers $\{-1, 1\}$.
   D'après le théorème ci- dessus $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \{-1, 1\} \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

Chapitre 4

Les Théorèmes de Sylow

Soit G un groupe fini. L'ordre de tout élément de G est un diviseur de l'ordre de G mais la réciproque n'est pas vraie.
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est l'ordre 4 mais ne contient pas d'élément d'ordre 4.
De même le groupe symétrique $\mathcal{S}_3$ est d'ordre 6, mais ne contient pas d'élément d'ordre 6.
Cependant les théorème de Cauchy montrent que si un nombre premier p divise l'ordre de 6, alors G contient un élément d'ordre p.
Si H est un sous - groupe de G, d'après le théorème de Lagrange l'ordre de H est un diviseur de l'ordre de G. La réciproque n'est pas vraie si d est un diviseur de l'ordre de G, G ne contient pas forcément un sous - groupe d'ordre d. Par exemple le groupe Alterné A_4 est d'ordre 12 mais ne contient pas un sous - groupe d'ordre 6. Cependant les théorèmes de Sylow montrent que si d est une puissance d'un nombre premier p, alors G contient un sous - groupe d'ordre d.

4.1 Les Théorèmes de Cauchy

4.1.1 Théorèmpe de Cauchy abélien

Théorème 4.1.1. *Soit G un groupe abélien et p un nombre premier.*
Si p divise $|G|$ alorse G contient un élément d'ordre p.

<u>Démonstration</u> :

On pose $|G| = pm$ avec $m \geq 1$.
La démonstration se fait par récurrence forte sur m.
• Si $m = 1$, $|G| = p$, donc G est cyclique et par suite contient un élément d'ordre p.
Supposons la propriété vraie pour tout entier $1 \leq k < m$. Soit $x \in G$ tel que $0(x) = t > 1$.
• Si p divise t, $t = p\lambda$, $x_o = x^A$ est d'ordre p. Donc G contient un élément d'ordre

p. Supposons que p ne divise pas t.

Comme G est abélien, $\langle x\rangle$ est normal dans G et $G/_{\langle x\rangle}$ est un groupe abélien d'ordre $p\,\dfrac{m}{t}$.

Comme p ne divise pas t, p et t sont premiers entre eux d'après le théorème de Gauss, t divise m et $\dfrac{m}{t}$ est un entier strictement plus petit que m.

Par hypothèse de récurrence $G/_{\langle x\rangle}$ contient un élément $\overline{y}$ d'ordre p avec $\overline{y} = \pi(y)$ ou $\pi : G \longrightarrow G/_{\langle x\rangle}$ est la surjection canonique $0(\overline{y}) = o \Longrightarrow p$ divise $0(y) \Longrightarrow \exists\beta \in \mathbb{N}^* \;/\; 0(y) = p^{\beta}$.

$y_o = y^{\beta}$ est un élément de G d'ordre p.

4.1.2 Théorème de Cauchy non abélien

Théorème 4.1.2. *Soit G un groupe fini d'ordre n et p un diviseur premier de n. Alors G contient un élément d'ordre p.*

Démonstration :

Elle se fait par récurrence forte sur n.

Si $A = 2$, G est cyclique et le résultat est vrai. On suppose que la propriété est vraie $\forall m < n$ avec $n > 2$. Soit p un nombre premier divisant n. Si $G = Z(G)$, G est abélien, donc G contient un élément d'ordre p. Supposons $G \neq Z(G)$. Deux cas sont possibles.

1ère cas : $\exists x \in G\backslash Z(G)$ tel que p divise $|C_G(x)|$ où $C_G(x)$ est le centralisateur de x dans G. $x \notin Z(G) \Longrightarrow C_G(x)$ est un sous - groupe propre de $G \Longrightarrow |C_G(x)| < |G|$. Par hypothèse de récurrence $C_G(x)$ contient un élément d'ordre p, donc G contient un élément d'ordre p.

2ème cas : $\forall x \in G\backslash Z(G)$, p ne divise pas $|C_G(x)|$.

p divise $|G| = [G : C_G(x)] \setminus C_G(x)|$.

Comme p et $|C_G(x)|$ sont premiers entre eux, d'après le théorème de Gauss, p divise $[G : C_G(x)]$, $\forall x \in G\backslash Z(G)$.

D'après l'équation aux classes $|Z(G)| = |G| - \sum\limits_{x\notin Z(G)} [G : C_G(x)]$, donc p divise $|Z(G)|$, le théorème de Cauchy abélien montre que $Z(G)$ contient un élément d'ordre p, par suite G possède un élément d'ordre p.

4.2 Les Théorèmes de Sylow

Définition 4.2.1. *Soit G un groupe fini et p un nombre premier divisant $|G|$. Un sous - groupe H de G est un p- sous - groupe de ylow de G.*
Si H est maximal dans l'ensemble des p- sous - groupes de G ordonné par l'inclusion.

Théorème 4.2.2. *Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors tout p- sous - groupe de G est includ ans un p-sous - groupe de Sylow de G.*

Démonstration :

Soit G un groupe fini et p un nombre premier divisant $|G|$ et H un p-sous - groupe de G tel que $H \supsetneqq H_1$.
Si H_1 est maximal, la démonstration est terminée sinon il existe un p-sous - groupe H_2 de G tel que $H \subsetneqq H_1 \subsetneqq H_2$. Comme G est fini le processus de construction des H_i est fini et le théorème est démontré.

Corollaire 4.2.3. *Soit G un groupe fini et p un nombre premier divisant $|G|$, alors G possède un p-sous-groupe de Sylow.*

Démonstration :

Soit G un groupe fini et p un nombre premier divisant $|G|$, d'après le théorème de Cauchy._ G contient un élément x d'ordre p, $H = \langle x \rangle$ est un p-groupe d'après le théorème ci-dessus, H est contenu dans un p-groupe de Sylow de G.

Théorème 4.2.4. *Soit G un groupe fini et p un nombre premier divisant $|G|$.*

1. *Tout sous - groupe conjugué d'un p- sous - groupe de Sylow de G est un p- sous - groupe de Sylow de G.*
2. *Si G possède un unique p- sous - groupe de Sylow H alors H est normal dans G.*

Démonstration :

1. Soit H un p- sous - groupe de Sylow de G et K un conjugé de H, $\exists g \in G / K = gHg^{-1} = \varphi_g(H)$ où φ_g est l'automorphisme intérieur associé à g.
   $|K| = |gHg^{-1}| = |H|$, donc K est un p-sous - groupe de G, montrons qu'il est maximal.
   Soit K' un p- sous- groupe G telq ue $H \subset \varphi_g^{-1}(K')$.
   Comme H est un p - sous - groupe de Sylow, on a $H = \varphi_g^{-1}(K')$ d'où $K = \varphi_g(H) = K'$, par suite K est maximal.

2. Si G possède un seul p- sous - groupe H, comme les conjugués de H sont des p - sous - groupes de Sylow de G on a

$$gHg^{-1} = H \qquad \forall g \in G, \text{ d'où } H \lhd G.$$

Lemme 4.2.5. *Soit p un nombre premier et $n \in \mathbb{N}^*$. 8 Alors pour tous entiers s et r tel que p et s soient premiers et $1 \leq r \leq n$, on a $C_{sp^n}^{p^r} = \lambda p^{n-r}$ où λ est un entier premier avec p.*

__**Démonstration**__ **:**

On a

$$C_{sp^n}^{p^r} = \frac{(sp^n!}{p^r!(sp^n - p^r)!} = \frac{(sp^n(sp^n-1)(sp^n-2)\cdots(sp^n-p^r+1)}{p^r(p^r-1)p^r-2)\cdots 2\times 1}$$

$$= sp^{n-r} - \left(\frac{sp^n-1}{1}\right)\left(\frac{sp^n-2}{2}\right)\cdots\frac{sp^n-(p^r-k)}{p^r-k}\Bigg)\cdots\left(\frac{sp^n-(sp^r-1)}{p^r-1}\right)$$

Posons $\lambda = s\left(\frac{sp^n-1}{1}\right)\left(\frac{sp^n-2}{2}\right)\cdots\frac{sp^n-(p^r-k)}{p^r-k}\Bigg)\cdots\left(\frac{sp^n-(sp^r-1)}{p^r-1}\right).$

Comme p ne divise pas s, pour montrer que p ne divise pas λ, il suffit de montrer que pour tout entier $k', 1 \leq k' \leq p^r - 1$ la fraction $\dfrac{sp^n - k'}{k'}$ est égal à une fraction irréductible dont p ne divise ni le numérateur, ni le dénominateur.

Posons $k' = qp^t$ avec $t \geq 0$ et p premier avec q.

$\dfrac{sp^n - k'}{k'} = \dfrac{sp^n - qp^t}{qp^t} = \dfrac{sp^{n-t} - q}{q}$, comme p ne divise pas q, p ne divise pas $sp^{n-t} - q$, d'où le résultat.

Théorème 4.2.6. *(Sylow)*

Soit G un groupe fini d'ordre sp^n, $n \in \mathbb{N}^*$, $s \in \mathbb{N}^*$ et p un nombre premier ne divisant pas s. alors pour tout entier r $1 \leq r \leq n$, il existe un sous - groupe H de G d'ordre p^r.

__**Démonstration**__ **:**

Soit G un groupe, $|G| = sp^n$, $n \in \mathbb{N}^*, s \in \mathbb{N}^*$, p un nombre premier ne divisant pas s.

Soit $r \in \mathbb{N}$ tel que $1 \leq r \leq n$ et soit E_r l'ensemble des parties à rp^r éléments de G

$$E_r = \left\{X \in \mathcal{P}(G) \ / \ |X| = p^r\right\}, \quad |E_r| = C_{sp^n}^{p^r} = \lambda p^{n-r}$$

où λ est un entier premier avec p.

Comme les translations à gauche sont des bijections de G sur G, on a :

$$\forall g \in G, \quad \forall X \in E_r, \quad |gX| = |X| = p^r,$$

donc G opère sur E_r par translation à gauche. Soit $(X_i)_{1\leq i\leq d}$ l'ensemble des orbiteqs distinctes et $(x_i)_{1\leq i\leq d}$ une famille de représentants de ces orbites.
D'après l'équation aux classes $\ell,\ 1\leq \ell\leq d$ tel que p^{n-r+1} ne divise pas $\Big[G:G_{x_\ell}\Big]$.
Supposons le contraire c'est-à-dire p^{n-r+1} divise $\Big[G:G_{x_i}\Big]$ $\forall i,\ 1\leq i\leq d$

$$\Big[G:G_{x_i}\Big]=\lambda_i\ p^{n-r+1}\Longrightarrow\sum_{i=1}^{d}\Big[G:G_{x_i}\Big]=\sum_{i=1}^{d}\lambda_i\ p^{n-r+1}=p^{n-r+1}\left(\sum_{i=1}^{d}\right)$$

$$\Longrightarrow\lambda p^{n-r}=p^{n-r+1}\left(\sum_{i=1}^{d}\lambda_i\right)\Longrightarrow\lambda=p\left(\sum_{i=1}^{d}\lambda_i\right)$$

donc p divise λ, ce qui est contraire à la définition de λ.
Ainsi, $\exists\ell,\ 1\leq\ell\leq$ tel que p^{n-r+1} ne divise pas $[G:G_{x_\ell}]$.
Posons $H=G_{x_\ell}$, H est un sous - groupe de G, montrons que $|H|=p^r$. Soit $x\in X_\ell$, l'orbite de x_ℓ et

$$\begin{aligned}\varphi_x:\ \ & H\longrightarrow X_\ell\\ & h\longrightarrow\varphi_x(h)=h_x\end{aligned}$$

φ_x est bien définie.
Soit $h_1,h_2\in H$ tel que $h_1\neq h_2$.

$$h_1\neq h_2\Longrightarrow h_1x\neq h_2x\Longrightarrow\varphi_x\text{ est injective }\Longrightarrow|H|\leq|X_\ell|=p^r.\tag{4.1}$$

Posons $[G:H]=s'p^t$ avec $t\geq 0$ et s' premier avec p.
Comme p^{n-r+1} ne divise pas $[G:H]=s'p^t$, on a $0\leq g\leq n-r$.
D'après le théorème de Lagrange $[G:H]$ divise $|G|=sp^n$, donc $\exists a\in\mathbb{N}^*\ /\ sp^n=as'p^t$, ce qui implique $as'=sp^{n-t}$.
De plus s' étant premier avec p, s' divise s et $\exists s''\in\mathbb{N}^*$ tel que

$$s=s's''\textbf{.}\ H=\frac{|G|}{[G:H]}=\frac{s'ns''p^n}{s'p^t}=s''\ p^{n-t}.$$

Comme $0\leq t\leq n-r$ on a

$$r\leq n-t,\quad\text{d'où }\ p^r\leq p^{n-t}\leq s''p^{n-t}\Longrightarrow p^r\leq|H|\tag{4.2}$$

(1) et **(2)** $\Longrightarrow|H|=p^r$.

Exercice :

Soit G un groupe fini d'ordre sp^n, $s\in\mathbb{N}^*$, p un nombre premier divisant $|G|$. (p^n est la plus grande puissance de p divisant $|G|$.) Montrer que les p - sous - groupes de Sylow sont les p - sous - groupes de de G d'ordre p^n.

Soit G un groupe opérant sur un ensemble E et K un sous - groupe de G. K opère sur E par la restriction de l'action de G. Soit $x \in E$, on désigne par K_x le stabilisateur de x dans K et G_x le stabilisateur de x dans G.
E^K l'ensemble des points fixes de E sous l'action de K.

Lemme 4.2.7. *On a :*

1. $K_x = G_x \cap K$
2. $x \in E^K \Longleftrightarrow K$ *est un sous - groupe de* G_x.

<u>Démonstration</u> :

1. $k \in K_x \Longleftrightarrow k \in K$ et $k \,\text{.}\, x = x \Longleftrightarrow k \in K$ et $k \in G_x \Longleftrightarrow k \in K \cap G_x$ donc $K_x = K \cap G_x$
2. $E^K = \left\{ x \in E / \ k \,\text{.}\, x = x, \quad \forall k \in K \right\}$, donc
   $x \in E^k \Longleftrightarrow k \,\text{.}\, x = x \quad \forall x \in K \Longleftrightarrow K_x = K \Longleftrightarrow K \cap G_x = K \Longleftrightarrow K \subset G_x$.

Lemme 4.2.8. *Soit* G *un groupe,* H *et* K *deux sous - groupes de* G *tel que* $[G : H] = r \in \mathbb{N}^*$ *et* $|K| = p^n$, $n \in \mathbb{N}^*$ *et* p *un nombre premier ne divisant pas* r. *Alors* K *est inclu dans un conjugue de* G.

<u>Démonstration</u> :

Posons $E = (G/H)_g$ l'ensemble des classes à gauche modulo H. G et K opère sur E par les translations à gauche. On désigne par E^K l'ensemble des points fixes de E sous l'action de K, comme K est un p - sous - groupe, on a
$|E| = |E^K|$ modulo p, $|E| = [G : H] \equiv |E^K|$ modulo p
$\Longrightarrow$ $|E^K| \equiv r$ modulo p, comme p ne divise pas r, on a :
$E^K \neq \varnothing \Longrightarrow \exists x_o \in G \ / \ x_oH \in E^K$. Soit G_{x_o} le stabilisateur de x_oH sous l'action de G sur E. Montrer que $G_{x_o} = x_oH_{x_o}^{-1}$
$y \in G_{x_o}H \Longrightarrow y(x_oH) = x_oH \Longrightarrow \exists h \in H \ / \ yx_o = x_oh$
$\Longrightarrow y = x_ohx_o^{-1} \Longrightarrow y \in x_o \ Hx_o^{-1} \Longrightarrow G_{x_o}H \subset x_o \ Hx_o^{-1}$ $\qquad (i)$
$y \in x_o \ Hx_o^{-1} \Longrightarrow \exists t \in H \ / \ y = x_otx_o^{-1} \Longrightarrow yx_o = x_ot$
$y(x_oH) = (yx_o)H = x_otH = x_oH \Longrightarrow y \in G_{x_o}H \Longrightarrow x_oHx_o^{-1} \subset G_{x_o}H$ $\qquad (ii)$
(i) *et* $(ii) \Longrightarrow G_{x_o}H = x_oHx_o^{-1}$.
D'après le lemme 1 ci-dessus, $x_oH \in E^K \Longrightarrow K \subset G_{x_o}H = x_oHx_o^{-1}$ donc K est inclu dans un conjugue de H.

Lemme 4.2.9. *Soit* G *un groupe fini,* p *un nombre premier divisant* $|G|$ *et* H *un* p *- sous - groupe de Sylow de* G. *Alors* H *est l'unique* p*- sous - groupe de Sylow de son normalisateur dans* G, $N_G(H)$.

Démonstration :

Soit H un p- sous - groupe de Sylow de $N_G(H)$.
Posons $|N_G(H)| = s'p^n$ avec s' et p premiers entre eux.
Soit K un p- sous - groupe de Sylow de $N_G(H)$, on a :

$$|K| = |H| = p^n, \quad [N_G(H) : H] = \frac{N_G(H)|}{|H|} = \frac{s'p^n}{p^n}.$$

Comme p ne divise pas s', d'après le lemme 2, K est inclu dans un conjugue de H dans $N_G(H)$, donc $\exists x \in N_G(H)$ tel que $K \subset xHx^{-1} = H$.
$(K \subset H$ et $|K| = |H|) \Longrightarrow K = H$, ainsi H est l'unique p- sous - groupe de Sylow de $N_G(H)$.

Théorème 4.2.10. *(Sylow)*

Soit G un groupe fini et p un nombre premier divisant $|G|$.

1. *les p- sous - groupe de Sylow de G sont conjugues dans G*
2. *le nombre n_p des sous - groupes de Sylow de G est un diviseur de $|G|$, conjugue à 1 modulo p.*

Démonstration :

1. $|G| = sp^n$, s et p premier entre eux.

   Soient H et K deux p- sous - groupe de Sylow de p ne divise pas s.

   $$|H| = |K| = p^n, \quad [G : H] = s \ , \quad |K| = p^n,$$

   d'après le lemme 2 K est inclus dans un conjugue de H, $\exists x \in G \ / \ K \subset xHx^{-1}$.
   $|xHx^{-1} = |H| = p^n = |K|$. Comme $K \subset xHx^{-1}$, on a $K = Hx^{-1}$ ainsi H et K sont conjugués dans G.

2. Soit E l'ensemble des p-sous-groupes de Sylow de G.

   Comme les p-sous-groupes de Sylow sont deux à deux conjugués, G opère transitivement par conjugaisons sur E, on a une seule orbite suivant cette action, θ_H où $H \in E$. Soit n_p le nombre de p-sous-groupes de Sylow de G.

   $$n_p = |E| = |\theta_H| = [G : N_G(H)],$$

   donc n_p divise $|G|$. H opère sur E par conjugaison, soit E^H l'ensemble des points fixes de E sous l'action de H.
   Comme H est un p - groupe, $|E| \equiv |E^H|$ modulo p, donc $n_p \equiv |E^H|$ modulo p.
   De plus

   $$\begin{aligned} HK \in E^H & \Longleftrightarrow hK = K \qquad \forall h \in H \\ & \Longleftrightarrow hKh' = K \qquad \forall h \in H \\ & \Longleftrightarrow H \subset N_G(K) \end{aligned}$$

D'après le lemme 3, $N_G(K)$ ne contient qu'un seul p-sous-groupe de Sylow qui est K, donc $K = H$ et $|E^H| = 1$, on en déduit que $n_p \equiv 1$.

Remarque 4.2.11. $|G| = sp^n$, $n \in \mathbb{N}$, *p - premier ne divisant pas s, si H est un p-sous-groupe de Sylow de G, alors* $[G : H] = s$.

Corollaire 4.2.12. *Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors G a un unique p- sous-groupe de Sylow H si et seulement si H est normal dans G.*

Corollaire 4.2.13. *Soit G un groupe abélien fini, pour tout nombre premier p divisant $|G|$, G ne possède qu'un seul p- sous-groupe de Sylow.*

4.3 Applications des théorèmes de Sylow

Définition 4.3.1. *Un groupe G est dit simple si les seuls sous-groupes normaux de G sont $\{e\}$ et G.*

1. **Aucun groupe d'ordre 63 n'est simple**

   Soit G un groupe d'ordre 63
   $63 = 3^2 \times 7$, le nombre n_7 de 7-sous - groupe de Sylow de G.
   $n_7 \equiv 1$ modulo 7 et n_7 divise 9, donc $n_7 \equiv 1$.
   G contient un unique 7 - sous - groupe de Sylow H, $H \lhd G$ donc G n'est pas simple.

2. **Groupe G d'ordre 200**

$$|G| = 200 = 5^2 \times 8 = 5^2 \times 2^3.$$

   Soit n_5 le nombre de 5- sous - groupe de Sylow de G.

   $n_5 \equiv 1$ modulo 5 et n_5 divise 8, donc $n_5 = 1$ donc G possède un unique 5-sous - groupe de Sylow H et $H \lhd G$ donc G n'est pas simple.

3. **Groupe d'ordre 30**

$$|G| = 30 = 2 \times 3 \times 5.$$

   Soit n_5, n_3 et n_2 les nombres du 5-sous- groupe de Sylow, de 3-sous-groupe de Sylow et 2-sous-groupe de Sylow respectivement.

Chapitre 5

Groupes résolubles

5.1 Suite de décomposition et de Jordan-Holder

Définition 5.1.1. *SoitG un groupe. On appelle suite normale de G , une suite* $(G_i)_{0 \leq i \leq n}$ *de sous-groupe de G tels que*

1. $G = G_0 \supset G_1 \supset .... \supset G_n = \{e\}$
2. $G_{i+1} \lhd G_i$

La suite est dite de composition si $G_{i+1} \subsetneqq G_i$ *pour tout* $1 \leq i \leq n$.

L'entier n est la longueur de la suite et les groupes G_i *sont appelés facteurs de cette suite.*

Exemple 5.1.2.

1. Pour tout $n \in \mathbb{N}^*$, $\mathcal{S}_n \supsetneqq \mathcal{A}_n \supsetneqq \{e\}$
2. $\mathbb{Z}/24\mathbb{Z} \supsetneqq 3\mathbb{Z}/24\mathbb{Z} \supsetneqq 6\mathbb{Z}/24\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$
3. $\mathbb{Z}/30\mathbb{Z} \supsetneqq 5\mathbb{Z}/30\mathbb{Z} \supsetneqq 10\mathbb{Z}/30\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$

Définition 5.1.3. *Soient* $\Sigma_1 : G = G_0 \supset G_1 \supset .... \supset G_n = \{e\}$ *et* $\Sigma_2 : G = H_0 \supset H_1 \supset .... \supset H_\ell = \{e\}$ *deux suite de décomposition d'un groupe G. On dit que* Σ_2 *est un raffinement du* Σ_1 *si et seulement si pour tout* $i \in \{0, 1, ..., n\}$ *il existe* $j \in \{0, 1, ..., \ell\}$ *tel que* $G_i = H_j$. *C'est-à-dire on peut obtenir* Σ_2 *à partir de* Σ_1 *en insérant des groupes entre les* G_i.

Σ_2 *est dit raffinement propre de* Σ_1 *si et seulement s'il existe* $j \in \{0, 1, ..., \ell\}$ *tel que* $H_j \neq G_i$ *pour tout* $i \in \{0, 1, ..., n\}$

Exemple 5.1.4.

1. Considérons les suites

$$\Sigma_1 : \mathbb{Z} \supsetneqq 8\mathbb{Z} \supsetneqq 72\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

et

$$\Sigma_2 : \mathbb{Z} \supsetneqq 4\mathbb{Z} \supsetneqq 8\mathbb{Z} \supsetneqq 24\mathbb{Z} \supsetneqq 72\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

Σ_2 est un raffinement de Σ_1

2. Considérons les suites

$$\Sigma_1' : \mathbb{Z}/24\mathbb{Z} \supsetneqq 6\mathbb{Z}/24\mathbb{Z} \supsetneqq 12\mathbb{Z}/24\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

et

$$\Sigma_2' : \mathbb{Z}/24\mathbb{Z} \supsetneqq 3\mathbb{Z}/24\mathbb{Z} \supsetneqq 6\mathbb{Z}/24\mathbb{Z} \supsetneqq 12\mathbb{Z}/24\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

Σ_2' est un raffinement de Σ_1'

Définition 5.1.5. *Deux suites de décompositions* $\Sigma_1 = (G_i)_{0\leq i\leq n}$ *et* $\Sigma_2 = (H_i)_{0\leq i\leq \ell}$ *d'un groupe* G *sont dites équivalentes si et seulement :*

1. $\ell = n$
2. *Il existe* $\sigma \in \mathcal{S}_n$ *tel que pour tout* $0 \leq i \leq n$, $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$

Exemple 5.1.6.

Considérons les deux suites de décomposition de $\mathbb{Z}/30\mathbb{Z}$

$$\Sigma_1 : \mathbb{Z}/30\mathbb{Z} \supsetneqq 5\mathbb{Z}/30\mathbb{Z} \supsetneqq 10\mathbb{Z}/30\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

et

$$\Sigma_2 : \mathbb{Z}/30\mathbb{Z} \supsetneqq 2\mathbb{Z}/30\mathbb{Z} \supsetneqq 6\mathbb{Z}/24\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$$

les facteurs de

— Σ_1 sont $\overline{G_3} = (10\mathbb{Z}/30\mathbb{Z})/\left\{\bar{0}\right\} \simeq \mathbb{Z}/3\mathbb{Z}$, $\overline{G_2} = (5\mathbb{Z}/30\mathbb{Z})/(10\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ et $\overline{G_1} = (\mathbb{Z}/30\mathbb{Z})/(5\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$

— Σ_2 sont $\overline{H_3} = (6\mathbb{Z}/30\mathbb{Z})/\left\{\bar{0}\right\} \simeq \mathbb{Z}/5\mathbb{Z}$, $\overline{H_2} = (2\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$ et $\overline{H_1} = (\mathbb{Z}/30\mathbb{Z})/(2\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

Soit $\sigma = (1, 3, 2)$ alors $\overline{G_1} = \overline{H_{\sigma(1)}} = \overline{H_3}$, $\overline{G_2} = \overline{H_{\sigma(2)}} = \overline{H_1}$ et $\overline{G_3} = \overline{H_{\sigma(3)}} = \overline{H_2}$

Remarque 5.1.7.

De manière générale, le théorème de *Schreier* montre que deux suites de décompositions d'un groupes admettent de raffinement équivalents. La démonstration du théorème de *Schreier* utilise le résultat suivant

Théorème 5.1.8. *Soient* A_1, A_2, B_1 *et* B_2 *quatre sous-groupes d'un groupe* G *tels que* $A_2 \lhd A_1$ $B_2 \lhd B_1$. *Alors*

1. $A_2(A_1 \cap B_2) \lhd A_2(A_1 \cap B_1)$
2. *Les groupes quotients* $A_2(A_1 \cap B_1)/A_2(A_1 \cap B_2)$ *et* $B_2(A_1 \cap B_1) \lhd B_2(A_2 \cap B_1)$ *sont isomorphes.*

Démonstration

Comme $A_2 \lhd A_1$ et $B_2 \lhd B_1$, on a $A_2 \cap B_1 \lhd A_1 \cap B_1$ et $A_1 \cap B_2 \lhd A_1 \cap B_1$. Posons $D = (A_2 \cap B_1)(A_1 \cap B_2)$ alors D est un sous-groupe de $A_1 \cap B_1$. Montrons que D est normal dans $A_1 \cap B_1$.

Soit $x \in A_1 \cap B_1$ et $ab \in D$. On a

$$xabx^{-1} = (xax^{-1})(xbx^{-1}) \in D \Longrightarrow D \lhd A_1 \cap B_1$$

Soit

$$f : A_2(A_1 \cap B_1) \longrightarrow (A_1 \cap B_1)/D$$
$$xy \longmapsto f(xy) = \bar{y} = yD$$

Soient x et $a \in A_2$, y et $b \in A_1 \cap B_1$ tels que $xy = ab$. On a

$$xy = ab \Longrightarrow a^{-1}x = by^{-1} \in A_2 \cap B_1 \subset (A_2 \cap B_1)(A_1 \cap B_2) = D \Longrightarrow bD = yD \Longrightarrow f(xy) = f(ab)$$

donc f est bien définie. Montrons que f est un morphisme de groupes.

Soient x et $a \in A_2$, y et $b \in A_1 \cap B_1$. On a

$$(xy)(ab) = c(yay^{-1})(yb)$$

posons $a_1 = yay^{-1} \in A_2$ alors

$$(xy)(ab) = (xa_1)(yb) \Longrightarrow f[(xy)(ab)] = ybD = yDbD = f(xy)f(ab)$$

donc f est un homomorphisme de groupes qui est de plus surjectif.

Soit $xy \in ker\ f$. On a

$$xy \in ker\ f \Longrightarrow f(xy) = \bar{e} = D \Longrightarrow y \in D \subset A_2(A_1 \cap B_2) \Longrightarrow xy \in A_2(A_1 \cap B_2)$$

donc $ker\ f \subset A_2(A_1 \cap B_2)$

Soit $xy \in A_2(A_1 \cap B_2)$. On a

$$y \in A_1 \cap B_2 \Longrightarrow y \in (A_2 \cap B_1)(A_1 \cap B_2) = D \Longrightarrow yD = D = \bar{e} \Longrightarrow f(xy) = yD = \bar{e}$$

donc $A_2(A_1 \cap B_2) \subset ker\ f$

Alors on n déduit que $A_2(A_1 \cap B_2) = ker\ f$. D'après le théorème d'isomorphisme, les groupes $A_2(A_1 \cap B_1)/A_2(A_1 \cap B_2)$ et $(A_1 \cap B_1)/D$ sont isomorphes.

En considérant

$$g : B_2(A_1 \cap B_1) \longrightarrow (A_1 \cap B_1)/D$$
$$xy \longmapsto f(xy) = \bar{y} = yD$$

on montre de la même manière que les groupes $B_2(A_1 \cap B_1)/B_2(A_2 \cap B_1)$ et $(A_1 \cap B_1)/D$.

On en déduit finalement que $A_2(A_1 \cap B_1)/A_2(A_1 \cap B_2)$ et $B_2(A_1 \cap B_1) \lhd B_2(A_2 \cap B_1)$ sont isomorphes.

Théorème 5.1.9. *(Schreier)*

Deux suites normales d'un groupes ont des raffinements équivalents.

Démonstration

Soit $\Sigma_1 : G = G_0 \supset G_1 \supset .... \supset G_n = \{e\}$ et $\Sigma_2 : G = H_0 \supset H_1 \supset .... \supset H_\ell = \{e\}$ deux suites normales de G. Soit $i \in \{0, 1, ..., n\}$ et $j \in \{0, 1, ..., \ell\}$.

Dans Σ_1, insérons entre les groupes G_{i+1} et G_i les groupes

$$G_i \supsetneqq G_{i+1}(G_i \cap H_1) \supsetneqq G_{i+1}(G_i \cap H_2) \supsetneqq ... \supsetneqq G_{i+1}(G_i \cap H_\ell) = G_{i+1}$$

D'après le Lemme de *Zassenhauss* $G_{i+1}(G_i \cap H_{j+1}) \lhd G_{i+1}(G_i \cap H_j)$. On obtient ainsi une suite normale σ_1' de longueur mn qui est un raffinement de Σ_1.

Dans Σ_2, on insère entre les groupes H_j et H_{j+1} les groupes

$$H_j = H_{j+1}(H_j \cap G_1) \supsetneqq H_{j+1}(H_j \cap G_1) \supsetneqq H_{j+1}(H_j \cap G_2) \supsetneqq ... \supsetneqq H_{j+1}(H_i \cap G_n) = H_{j+1}$$

D'après le Lemme de *Zassenhauss* $H_{j+1}(H_j \cap G_{i+1}) \lhd H_{J+1}(H_j \cap G_i)$. On obtient ainsi une suite normale σ_2' de longueur mn qui est un raffinement de Σ_2.

D'après le Lemme de *Zassenhauss*

$$H_{J+1}(H_j \cap G_i)/H_{j+1}(H_j \cap G_{i+1}) \quad et \quad G_{i+1}(G_i \cap H_j)/G_{i+1}(G_i \cap H_{j+1})$$

sont isomorphes.

Σ_1' et Σ_2' ont une même longueur et chaque facteur de Σ_1' est isomorphe à un facteur de Σ_2' donc Σ_1' et Σ_2' sont équivalents.

Définition 5.1.10. *Une suite normale d'un groupe est dite de Jordan-Holder si les facteurs sont des groupes simples.*

Exemple 5.1.11.

1. $\Sigma_1 : \mathbb{Z}/30\mathbb{Z} \supsetneqq 5\mathbb{Z}/30\mathbb{Z} \supsetneqq 10\mathbb{Z}/30\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$
   Les facteurs de Σ_1 sont $\overline{G_3} = (10\mathbb{Z}/30\mathbb{Z})/\left\{\bar{0}\right\} \simeq \mathbb{Z}/3\mathbb{Z}$, $\overline{G_2} = (5\mathbb{Z}/30\mathbb{Z})/(10\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ et $\overline{G_1} = (\mathbb{Z}/30\mathbb{Z})/(5\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$

   Ces groupes simples donc Σ_1 est une suite de Jordan-Holder
2. $\Sigma_2 : \mathbb{Z}/30\mathbb{Z} \supsetneqq 2\mathbb{Z}/30\mathbb{Z} \supsetneqq 6\mathbb{Z}/24\mathbb{Z} \supsetneqq \left\{\bar{0}\right\}$
   Les facteurs de Σ_2 sont $\overline{H_3} = (6\mathbb{Z}/30\mathbb{Z})/\left\{\bar{0}\right\} \simeq \mathbb{Z}/5\mathbb{Z}$, $\overline{H_2} = (2\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$ et $\overline{H_1} = (\mathbb{Z}/30\mathbb{Z})/(2\mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. Ces groupes simples donc Σ_2 est une suite de Jordan-Holder.
3. La suite $\Sigma_3 : \mathcal{S}_4 \supsetneqq \mathcal{A}_4 \supsetneqq H_4 \supsetneqq K \supsetneqq \{e\}$ est une suite de Jordan-Holder.

Proposition 5.1.12. *Soit G un groupe. Une suite normale Σ de G est une suite de Jordan-Holder si et seulement si elle n'admet pas de raffinement propre.*

démonstration

Soit $\Sigma : G = G_0 \supset G_1 \supset .... \supset G_n = \{e\}$ une suite normale de G Le quotient G_i/G_{i+1} est simple si et seulement tout sous groupe normal de G_i contenant G_{i+1} est égal à G_i ou à G_{i+1}. Donc Σ est de Jordan-Holder si et seulement si Σ n'admet aucun raffinement propre.

Théorème 5.1.13. *(Jordan-Holder)*

Soit G un groupe admettant une suite de Jordan-Holder Σ_0. Alors

1. *Toutes suite normale Σ de G admet un raffinement qui est de Jordan-Holder.*
2. *Deux suites de Jordan-Holder de G sont équivalentes.*

Démonstration

1. Soit Σ_0 une suite de Jordan-Holder de G et Σ_1 une suite de décomposition de G. D'après le Théorème de Schreier Σ_0 et Σ_1 sont admettent des raffinements équivalents Σ_0' et Σ_1' qui sont équivalents. Comme Σ_0 est de Jordan-Holder on a $\Sigma_0 = \Sigma_0'$ d'où Σ_1' est équivalente à Σ_0 donc Σ_1' est Jordan-Holder
2. Soient Σ_1 et Σ_2 deux suites de Jordan-Holder de G alors d'après le Théorème de Schreier Σ_1 et Σ_2 sont admettent des raffinements équivalents Σ_1' et Σ_2' qui sont équivalents. Comme Σ_1 et Σ_2 sont de Jordan-Holder on a $\Sigma_1 = \Sigma_1'$ et $\Sigma_2 = \Sigma_2'$ d'où Σ_1 et Σ_2 sont équivalentes.

Théorème 5.1.14. *Tout groupe fini G possède une suite de Jordan-Holder.*

Démonstration

Elle se fait par récurrence sur $|G| = n$ Si $n = 1$ le resultat est vrai. Supposons $n \geq 2$ et le resultat vrai pour $m < n$ et soit G un groupe de carinal n.

Si G est simple $G \supsetneqq \{e\}$ est une suite de Jordan-Holder.

Supposons que G est non simple. Comme G est fini, G possède un nombre fini de sous-groupes normaux propre.

Soit G_1 un élément maximal dans l'ensemble des sous-groupes normaux propre de G par inclusion. Alors $|G_1| < |G| = n$ et par hypothèse de récurrence G_1 admet une suite de Jordan-Holder

$$G_1 \supsetneqq G_2 \supsetneqq ... \supsetneqq G_m = \{e\}$$

Par la maximalité de G_1, la suite

$$G = G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq ... \supsetneqq G_m = \{e\}$$

5.1.1 Groupes résolubles

Définition 5.1.15. *On appelle suite résoluble d'un groupe G une suite normale de G dont les facteurs sont abéliens. Un groupe G est dit résoluble s'il possède une suite résoluble.*

Théorème 5.1.16. *Soit G un groupe résoluble. Alors tout sous-groupe H de G est résoluble*

Démonstration

Soit $G = G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq ... \supsetneqq G_n = \{e\}$ une suite résoluble de G. Soit H un sous-groupe de G. Posons pour tout $i = 0, 1..., n$ $H_i = H \cap G_i$ alors

$$H = H_0 \supsetneqq H_1 \supsetneqq H_2 \supsetneqq ... \supsetneqq H_n = \{e\}$$

D'après le théorème d'isomorphisme $H_{i+1} = G_{i+1} \cap H = (H \cap G) \cap G_{i+1}$ est normal dans $H \cap G_i = Hi$. De plus $H_i/H_{i+1} = H \cap G_i/H \cap G_{i+1} \simeq G_{i+1}(H \cap G_i)/G_{i+1}$ qui est un sous-groupe de G_i/G_{i+1} qui est abélien donc la suite

$$H = H_0 \supsetneqq H_1 \supsetneqq H_2 \supsetneqq ... \supsetneqq H_n = \{e\}$$

est une suite résoluble ainsi H est résoluble.

Théorème 5.1.17. *Soit G un groupe résoluble et H un sous-groupe normal de G. Alors le groupe quotient G/H est résoluble*

Démonstration

Soient $G = G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq ... \supsetneqq G_n = \{e\}$ une suite résoluble de G, H un sous-groupe normal de G et $\pi : G \longrightarrow G/H$ la surjection canonique. Posons $\overline{H_i} = \pi(G_i)$ alors $\overline{H_{i+1}}$ est un sous-groupe de $\overline{H_i}$. Montrons que $\overline{H_{i+1}}$ est normal dans $\overline{H_i}$

Soient $\bar{x} = \pi(x) \in \overline{H_i}$ et $\bar{a} = \pi(a) \in \overline{H_{i+1}}$ avec $x \in G_i$ et $a \in G_{i+1}$. On a

$$\bar{x}\bar{a}\bar{x}^{-1} = \pi(xax^{-1}) \in \pi(G_{i+1}) = \overline{H_{i+1}}$$

donc $\overline{H_{i+1}} \lhd \overline{H_i}$. On a ainsi une suite normale de G/H donnée par

$$G/H = \overline{H_0} \supsetneqq \overline{H_1} \supsetneqq ... \supsetneqq \overline{H_n} = \{\bar{e}\}$$

montrons que les facteurs $\overline{H_i}/\overline{H_{i+1}}$ sont abéliens.

Considérons

$$\varphi : G_i/G_{i+1} \longrightarrow \overline{H_i}/\overline{H_{i+1}}$$

$$xG_{i+1} \longmapsto \varphi(tG_{i+1}) = \pi(x)\overline{H_{i+1}}$$

Soient x_1G_{i+1}, $x_2G_{i+1} \in G_i/G_{i+1}$ tels que $x_1G_{i+1} = x_2G_{i+1}$. On a

$$x_1G_{i+1} = x_2G_{i+1} \Longrightarrow x_2^{-1}x_1G_{i+1} = G_{i+1} \Longrightarrow x_2^{-1}x_1 \in G_{i+1} \Longrightarrow \pi(x_2^{-1}x_1) \in \overline{H_{i+1}}$$

$$\Longrightarrow \pi(x_1)\overline{H_{i+1}} = \pi(x_2) \in \overline{H_{i+1}} \Longrightarrow \varphi(x_1G_{i+1}) = \varphi(x_2G_{i+1})$$

donc φ_i est bien définie. De plus pour tout $\bar{y} \in \overline{H_i}$, il existe $y \in G_i$ tel que $\bar{y} = \pi(y)$, $\varphi(\bar{y}) = \varphi(yG_{i+1}) = \pi(y)\overline{H_{i+1}}$ donc φ_i surjectif. Soit aG_{i+1}, $bG_{i+1} \in G_i/G_{i+1}$. On a

$$\varphi[(aG_{i+1})(bG_{i+1})] = \varphi[abG_{i+1}] = \pi(ab)G_{i+1} = \pi(a)\overline{H_{i+1}}\pi(b)\overline{H_{i+1}} = \varphi(aG_{i+1})\varphi(bG_{i+1})$$

Donc φ est un morphisme de groupe. D'près le premier théorème d'isomorphisme $\overline{H_i}/\overline{H_{i+1}}$ est isomorphe à $(G_i/G_{i+1})/ker\ \varphi$

Donc $\overline{H_i}/\overline{H_{i+1}}$ est abélien. Alors on en déduit que G/H est résoluble.

Théorème 5.1.18. *Soit G un groupe et H un sous-groupe normal de G. Si H et G/H sont résolubles alors G est résoluble.*

Démonstration

Comme H et G/H sont résolubles, ils admettent chacun une suite résoluble

$$H = H_0 \supsetneq H_1 \supsetneq .... \supsetneq H_n = \{e\}$$

$$G/H = K_0^* \supsetneq K_1^* \supsetneq ... \supsetneq K_m^* = \{e\}$$

D'après le théorème de correspondance pour tout $i = 0, 1..., m$ il existe un sous-groupe K_i de G tel que $K_i^* = K_i/H$. de plus $K_{i+1}^* \lhd K_i^*$ donc on a $K_{i+1} \lhd K_i$ puis K_i^*/K_{i+1}^* et K_i/K_{i+1} sont isomorphes or K_i^*/K_{i+1}^* est abélien donc K_i/K_{i+1} est abélien par conséquent la suite

$$G = K_0 \supsetneq K_1 \supsetneq ... \supsetneq k_m = H \supsetneq H_1 \supsetneq .... \supsetneq H_n = \{e\}$$

est une suite résoluble de G d'où G est résoluble.

Corollaire 5.1.19. *Soient H et K deux groupes résolubles. Alors $H \times K$ est résoluble.*

Démonstration

Soient e et e' les éléments neutres respectivement de H et K. posons $H' = H \times e'\{\}$ et $K' = \{e\} \times K$. Alors H' et K' sont des sous-groupes de $G = H \times K$ isomorphes à respectivement à H et K. Montrons que H' est normal dans G.

Soient $x = (x_1, x_2) \in G$ et $y = (a, e') \in H'$ On a

$$xyx^{-1} = (x_1ax_1^{-1}, e') \in H'$$

donc H' est normal dans G. H' est résoluble, K' est résoluble et isomorphe à G/H' donc on en déduit que $G = H \times K$ est résoluble.

Théorème 5.1.20. *Soit $p \in \mathbb{N}$ un nombre premier et G un p-groupe. Alors G est résoluble.*

Démonstration

Elle se fait par récurrence sur $|G| = n$

Si $|G| = 2$ alors G est abélien donc résoluble.

Supposons que la propriété est vraie pour tout p-groupe de cardinal $m < n$. Comme G est un p-groupe, $Z(G) \neq \{e\}$ et $G/Z(G)$ sont des p-groupe tels que $|G/Z(G)| < n$ et $|Z(G)| < n|$ donc par hypothèse de récurrence $G/Z(G)$ et $Z(G)$ sont résoluble d'où G est résoluble.

5.2 Caractérisation de la résolubilité des groupes dérivés

Définition 5.2.1. *Soit G un groupe. Soient a, $b \in G$. le commutateur de a et b est l'élément*

$$[a, b] = aba^{-1}b^{-1}$$

Le sous-groupe dérivé de G est le sous-groupe engendré par les commutateurs de G. On le note $D(G)$.

Le sous-groupe $D(G)$ est normal dans G.

Définition 5.2.2. *Soit G un groupe. On appelle la suite dérivée de G, la suite $(D^n(G))_{n\in\mathbb{N}}$ définie par*

$$D^0(G) = G, \quad D^1(G) = D(G) \quad et \quad \forall\ n \geq 2, \quad D^n(G) = D(D^{n-1}(G))$$

On a

$$G = D^0(G) \supset D^1(G) \supset ... \supset\supset D^n(G)$$

Théorème 5.2.3. *Soit G un groupe. Alors $D(G) \lhd G$ et $G/D(G)$ est abélien*

Démonstration

Soient $x \in G$ et $h \in D(G)$. On a

$$[x, h] = xhx^{-1}h^{-1} \in D(G) \Longrightarrow xhx^{-1} \in D(G) \Longrightarrow D(G) \lhd G$$

Soient $\bar{x}$ et $\bar{y} \in G/D(G)$. On a

$$[x, y] = xyx^{-1}y^{-1} \in D(G) \Longrightarrow \overline{[x, y]} = \bar{e} \Longrightarrow \bar{x}\bar{y} = \bar{y}\bar{x}$$

d'où $G/D(G)$ est abélien

Théorème 5.2.4. *Soit G un groupe et H un sous-groupe de G. Alors les propriétés sont équivalentes*

1. $D(G) \subset H$
2. $H \triangleleft G$ *et* G/H *est abélien*

Démonstration

Supposons que $D(G) \subset H$. Soit $x \in G$ et $h \in H$. On a :

$$[x,h] = xhx^{-1}h^{-1} \in D(G) \subset H \Longrightarrow xhx^{-1} \in H$$

Soient $\bar{x}$ et $\bar{y} \in G/H$. On a

$$[x,y] = xyx^{-1}y^{-1} \in D(G) \subset H \Longrightarrow \overline{[x,y]} = \bar{e} \Longrightarrow \bar{x}\bar{y} = \bar{y}\bar{x}$$

Réciproquement supposons que $H \triangleleft G$ et G/H est abélien. Soit x, $y \in G$. On a

$$[x,y] = xyx^{-1}y^{-1} \in D(G)$$

Au passage aux classe on aura

$$\overline{[x,y]} = \overline{xyx^{-1}y^{-1}} = \bar{e} \Longrightarrow xyx^{-1}y^{-1}H \Longrightarrow D(G) \subset H$$

Lemme 5.2.5. *Soit G un groupe résoluble et $G = G_0 \supsetneqq\supsetneqq G_1 \supsetneqq ... \supsetneqq G_n$ une suite résoluble de G. Alors pour tout $i = 0, 1, ..., n$,*

$$D^i(G) \subset G_i$$

Démonstration

Elle se fait par récurrence sur i. Si $i = 0$, on a

$$D^0(G) = G_0 = G$$

Supposons que $D^i(G) \subset G_i$. On a

$$D^{i+1} = D(D^i(G)) \subset D(G_i)$$

Comme G_i/G_{i+1} est abélien on a $D(G_i) \subset G_{i+1}$

Théorème 5.2.6. *Un groupe G est résoluble si et seulement s'il existe $n\mathbb{N}^*$ tel que $D^n = \{e\}$.*

Démonstration

SSupposons qu'il existe $n\mathbb{N}^*$ tel que $D^n = \{e\}$. Alors

$$G = D^0(G) \supset D^1(G) \supset ... \supset\supset D^n(G) = \{e\}$$

est une suite normale dont les quotients sont abélien donc G résoluble.

Réciproquement si G est résoluble, G admet une suite normale

$$G_0 = G \supsetneqq G_1 \supsetneqq \dots \supsetneqq G_n = \{e\}$$

dont les facteurs sont abélien. Alors d'après le lemme précédent, $D^n(G) \subset G_n = \{e\}$ donc $D^n = \{e\}$

Lemme 5.2.7. *Soit $G \neq \{e\}$ un groupe simple et résoluble. Alors G est monogène*

Démonstration

Comme G est simple les seuls sous-groupes normaux de G sont G et $\{\}$ or $D(G)$ est normal dans G donc $D(G) = G$ ou bien $D(G) = \{e\}$.

L'égalité $D(G) = G$ entraine que $\forall\ n \in \mathbb{N}$, $D^n = G$. Comme G est résoluble, on a nécessairement $D(G) = \{e\}$ donc G abélien. Soit $x \in G \setminus \{e\}$. Posons $H =< e >$ alors $H \lhd G$ et comme G est simple on a finalement $H = G$ d'où G est monogène.

Théorème 5.2.8. *Soit $G \neq \{e\}$ un groupe fini. Alors G est résoluble si te seulement si G possède une suite de Jordan-Holder dont les facteurs sont cycliques d'ordre premier.*

Démonstration

Si G possède une suite de Jordan-Holder dont les facteurs sont cycliques d'ordre premier alors G est résoluble.

Réciproquement supposons que G est fini et résoluble. Alors G possède une suite de Jordan-Holder

$$G = G_0 \supsetneqq G_1 \supsetneqq \dots \supsetneqq G_n = \{e\}$$

les quotients G_i/G_{i+1} sont simple et résolubles, d'après le Lemme précédent G_i/G_{i+1} est cyclique.

Soit $i = 1, ..., n-1$ et $n_i = O(G_i/G_{i+1})$ et d un diviseur de n_i. Alors il existe un sous-groupe de G_i/G_{i+1} d'ordre d. La simplicité de G_i/G_{i+1}implique que ce sous-groupe est égal à G_i/G_{i+1} ou à $\{e\}$ donc $d = 1$ ou $d = n_i$ ce qui implique n_i est premier

5.3 Résolubilité du groupe symétrique

Théorème 5.3.1. *Pour tout $n \leq 4$, le groupe symétrique $\mathcal{S}_n$ est résoluble*

Lemme 5.3.2. *Pour tout $n \geq 3$ le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles*

Démonstration

Soit $i < j < k < \ell$ des éléments de $\{1, ..., n\}$ alors

$$(i, j)(j, k) = (i, j, k) \quad et \quad (i, j)(k, \ell) = (i, j, k)(j, k, \ell)$$

Donc le produit deux transposition est un produit de deux 3-cycle ou est un 3-cycle. Comme tout élément $\sigma \in \mathcal{A}_n$ est un produit en un nombre pair des transpositions on en déduit que σ est un produit de 3-cycles.

Lemme 5.3.3. *Pour tout $n \geq 5$ les 3-cycles sont conjugués dans $\mathcal{A}_n$*

Lemme 5.3.4. *Pour tout $n \geq 5$,*

$$D(\mathcal{A}_n) \subset \mathcal{A}_n \quad et \quad D(\mathcal{S}_n) = \mathcal{A}_\backslash$$

Démonstration

On a $D(\mathcal{A}_n) \subset \mathcal{A}_n$ comme $\mathcal{A}_n$ est engendré par les 3-cycles pour montrer que $D(\mathcal{A}_n)$, il suffit de montrer que $D(\mathcal{A}_n)$ contient les 3-cycles.

Soit $c = (a_1, a_2, a_3)$ un 3-cycle alors $c^2 = (a_1, a_3, a_2)$ est un 3-cycle donc c et c^2 sont conjugués dans $\mathcal{A}_n$ alors il existe $\sigma \in \mathcal{A}_n$ tel que

$$c^2 = \sigma c \sigma^{-1} \Longrightarrow c = \sigma c \sigma^{-1} c^{-1} = [\sigma, c] \in D(\mathcal{A}_n)$$

d'où $D(\mathcal{A}_n) = \mathcal{A}_n$

Théorème 5.3.5. *Pour tout $n \geq 5$, $\mathcal{S}_n$ n'est pas résoluble.*

Démonstration

Pour tout $m \in \mathbb{N}^*$, $D^m(\mathcal{S}_n) = \mathcal{A}_n \neq \{e\}$ donc $\mathcal{S}_n$ n'est pas résoluble.

Théorème 5.3.6. *(Feit-Thompson) Tout groupe fini d'ordre d'ordre impair est résoluble.*

Chapitre 6

Anneaux et Corps

6.1 Anneaux - Sous - anneaux et idéaux

Définition 6.1.1.

Un anneau est un groupe abélien $(A, +)$ *muni d'une loi de composition interne notée* $\times$

$$A \times A \longrightarrow A$$
$$(a, b) \longrightarrow ab$$

vérifiant les propriétés suivantes :

1. $\forall\ (a, b, c) \in\ A^3,\ \ a(b + c) = ab + ac$ *et* $(b + c)a = ba + ca$
2. $a(bc) = (ab)c\ \ \forall(a, b, c)\ \ \in\ A^3$

Définition 6.1.2.

- *L' anneau* A *est dit commutatif si la loi* $\times$ *est commutative c'est à dire si*

$$ab = ba \quad \forall\ (a, b) \in A^2$$

- *L'anneau* A *est dit unitaire s'il existe un élément* $1_A \in\ A$ *appelé unité tel que* $\forall a\ \in A$, $1_A a = a 1_A = a$.

Exemple 6.1.3.

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ et muni de l' addition et de la multiplication usuelles sont des anneaux
2. Soit E un $\mathbb{K} - ev$, l'ensemble $\mathcal{L}_{\mathbb{K}}(E)$ des endomorphismes de E muni de l'addition et de la composition des applications est un anneau unitaire.
3. L'ensemble $M_n(\mathbb{K})$ des matrices carrées d'ordre $n \geq 2$ muni de l'addition et de la multiplication matricielle est un anneau unitaire.

4. Soit $n \in \mathbb{N}^\star$. $(\mathbb{Z}/n\mathbb{Z}, \ + \ , \times)$, $\overline{a} + \overline{b} = \overline{a+b}$ *et* $\overline{a}\overline{b} = \overline{ab}$ est un anneau commutatif et unitaire.
5. Soient $A_1 ..., A_n$ des anneaux commutatifs et unitaires.

   On pose A $= A_1 \times A_2 \times .... \times A_n$, on munit A des deux lois :
   $a = (a_1, ..., a_n)$, $b = (b_1, ..., b_n)$ on définit $a + b = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$ et $ab = (a_1b_1, a_2b_2, ..., a_nb_n)$ le triplet $(A, +, \times)$ est un anneau commutatif et unitaire appelé anneau produit des anneaux $A_1, ..., A_n$, $1_A = (1_{A_1}, ..., 1_{A_n})$

Définition 6.1.4.

Soit A un anneau unitaire et $A^\star = A \setminus \{0\}$. Un élément $a \in A^\star$ tel que $ab = 0$ (resp $ba = 0$) est dit diviseur de zéro à gauche (resp à droite). Il est dit diviseur de zéro, s' il est diviseur de zéro à gauche et à droite.

Exemple 6.1.5.

1. $A = \mathbb{Z}/6\mathbb{Z}$, $a = \overline{2}$ et $b = \overline{3}$, $ab = \overline{b} = \overline{0}$
2. $A = M_2(\mathbb{R}), a = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

Définition 6.1.6.

Un anneau A est dit intègre s'il est commutatif et unitaire et sans diviseurs de zéro . Autrement dit
$\forall \ (a, b) \in A^2, ab = 0 \quad \Longrightarrow \quad a = 0 \ \textit{ou} \ \ b = 0$

Définition 6.1.7.

Soit A un anneau unitaire . Un élément $a \in A$ est dit Unitaire s'il existe $a^{'} \in$ telque $aa^{'} = a^{'}a = 1_A$.
On note par a^{-1} l'inverse de A et par $\mathfrak{U}(A)$ l' ensemble des éléments inversible de A.

Proposition 6.1.8.

Soit $n \in \mathbb{N}, n \geq 2$, alors $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si n et k sont premiers entre eux .

Définition 6.1.9.

Un corps est un anneau non réduit à $\{0\}$ tel que tout élément non nul $a \in A$ soit inversible.

Remarque 6.1.10.

Dans tout ce chapitre le mot anneau désigne un anneau commutatif et unitaire d' élément unité $1 \neq 0$.

Définition 6.1.11.

Soit A un anneau et B une partie de A. On dit que B est un sous anneau de A si les conditions suivantes sont vérifiées.

1. $1_A \in B$
2. $(B, +)$ *est un sous groupe de* $(A, +)$
3. $\forall\ x \in B$ *et* $\forall\ y \in B, \quad xy \in B$

Définition 6.1.12.

Soit A un corps et B une partie de A est un sous corps si B est un sous anneau de A et est un corps.

Définition 6.1.13.

On dit qu'une partie I d'un anneau A est un idéal de A si :

1. $I \neq \emptyset$
2. $x + y \in I, \ \forall\ x \in I$ *et* $\forall\ y \in I$
3. $ax \in I \ \ \forall\ x \in I$ *et* $\forall\ a \in A$

Exemple 6.1.14.

Les idéaux de $\mathbb{Z}$ sont de la forme $n\,\mathbb{Z}$ ou $n \in \mathbb{N}$

Remarque 6.1.15.

Soit A un anneau et I un idéal de A

1. *Si* $1_A \in\ I$ *alors* $I = A$
2. *Si I contient un élément inversible u alors $I = A$*

Soit A un anneau , I et J deux idéaux de A . On pose $I \cap J = \{x \in A \ /x \in I$ et $x \in J\}, I + J = \{x_1 + x_2 \ /x_1 \in I$ et $x_2 \ \in J\}$ et IJ l' ensemble de toutes les sommes finies de la forme $\sum_{i=1}^{n} x_i y_i$ ou $x_1, ..., x_n \in I$ etIet $y_1, ..., y_n \in J$.

Proposition 6.1.16.

Soit I et J deux idéaux d'un anneau A. Alors les ensembles $I \cap J$, $I + J$ et IJ sont des idéaux de A.

<u>Démonstration</u>

1. $0 \in I \cap J$, donc $I \cap J \neq \emptyset$

   Soit $x \ \in I \ \cap J, \quad y \in I \cap J$ et $a \in \ A$

   Comme I et J sont des idéaux de A ,on a $x + y \in I$, $x + y \in J$, $ax \in I$ et $ax \in J$, donc $x + y \in I \ \cap J$. On en déduit que $I \cap J$ est un idéal de A.

2. $0 = 0 + 0 \in \ I + J \implies I + J \neq \phi$

   Soit $x = x_1 + x_2 \in I + J$, $y = y_1 + y_2 \ \in I + J$ et $a \in \ A$.

   On a $x + y = (x_1 + y_1) + (x_2 + y_2) \in I + J$ et $ax = ax_1 + ax_2 \in I + J$ donc $I + J$ est un ideal de A.

3. $0 = 0 + 0 \in IJ,$ donc $IJ \neq \phi$

   Soit $x \in \ IJ,\ y \ \in IJ$ et $a \in A$

   x s'écrit $x = \sum_{i\in k}^{n} x_i y_i$ *avec* $x_i \in$ et $y_i \in J$ et y $= \sum_{j\in l}^{m} x_j y_j, x_j \in I,\ y_j \in J,\ l$et k sont des ensembles finis $x + y = \sum_{i\in k}^{n} x_i y_i + \sum_{j\in\ l}^{m} x_j y_j \in IJ$ et $ax = \sum_{i\in k}(ax_i)\ y_i \in IJ$.

Définition 6.1.17.

Soit A un anneau et S une partie idéal de A , on appelle idéal de A engendre par S , l' intersection des idéaux de A contenant S . Cet idéal est le plus petit idéal de A contenant S, on le note < S >.

Proposition 6.1.18. *Soit A un anneau et S une partie non vide de A. Alors < S > est l'ensemble des combinaisons linéaires finies d' éléments de S à coefficients dans A.*

Démonstration

Posons $I = \left\{ \sum_{k\in L} a_k x_k \ /\ \text{L est un ensemble fini}, a_k \ \in A \ et \ x_k \ \in S \right\}$

1. (a) Soit $x \ \in S,\ x = 1.x \ \in \ I,$ donc I $\neq \emptyset$

   (b) Soit $x = \sum_{k\in L_1} a_k x_k,$ ou L_1 est un ensemble fini, $a_k \in \ A$ et $x_k \in \ S$

   $y = \sum_{k\in L_2} a_k x_k$ L_2 est un ensemble fini, $a_l \ \in A$ et $x_l \in S$ et $a \ \in \ A$, x + y = $\sum_{k\in L_2} a_k x_k \in \ I$ *et* $ax = \sum_{k\in L_1} (aa_k) x_k \in \ I$.

   Donc I est un idéal de A et $S \subset I$.

2. Soit J un idéal de A contenant S , J contient toute somme finie d'éléments de la forme ax où $a \in A \ et \ x \in \ S \ donc \ I \subset J$.On en deduit que $I =< S >$

Corollaire 6.1.19.

Soit A un anneau et $S = \{a_1, a_2, ..., a_n\}$ *une partie finie de A , alors*

$$< a_1, a_2, \cdots, a_n >= Aa_1 + Aa_2 + \cdots + Aa_n.$$

Définition 6.1.20.

Un idéal I d' un anneau A est dit principal s'il existe $a \in A$ *tel que* $I =< a >$.

Définition 6.1.21.

Un idéal d'un anneau A est dit propre si $I \neq 0$ *et* $I \neq A$

Proposition 6.1.22.

Soit A un anneau commutatif et unitaire.

A est un corps si et seulement si A ne possède aucun idéal propre.

Démonstration

On suppose que A est un corps et soit I un idéal non nul de A, il existe $a \in A$ tel que $a \neq 0$ *et* $a \in I$, comme a est un corps a est inversible et donc on a $I = A$.

Réciproquement supposons que A est un anneau commutatif sans idéal propre et soit $a \neq 0$ un élément de A. L'idéal $I =< a >= Aa$, est non nul , donc $I = A$, par conséquence $1_A \in I = Aa$, donc il existe $b \in A$ tel que $ba = 1$, donc a est inversible d' où A est un corps.

6.2 Morphismes et Anneaux quotients

6.2.1 Morphismes

Définition 6.2.1.

soient A et B deux anneaux. On appelle morphisme de A dans B (ou homomorphisme) toute application $f : A \longrightarrow B$ *vérifiant :*

1. $f(x + y) = f(x) + f(y) \ \forall \ x, y \in \ A$
2. $f(xy) = f(x)f(y) \ \forall \ x, y \in \ A$
3. $f(1_A) = 1_B$

Définition 6.2.2.

Soit $f : A \longrightarrow B$ *un morphisme d'anneaux. f est un isomorphisme si f est bijectif.*

Définition 6.2.3.

Deux anneaux A et B sont dits isomorphes et on note $A \cong B$ *s'il existe un isomorphisme de A sur B.*

Définition 6.2.4.

Soit A un endomorphisme . On appelle endomorphisme de A , tout morphisme de A sur lui même .Un endomorphisme bijectif de A est appelé automorphisme de A.

Théorème 6.2.5.

Soit $f : A \longrightarrow B$ un morphisme d' anneaux.

1. *Si N est un sous anneau de A alors $f(N)$ est un sous anneau de B. En particulier $Imf = f(A)$ est un sous anneau de B.*
2. *Si D est un sous-anneau de B alors $f^{-1}(D)$ est un sous anneau de A.*
3. *Si J est un idéal de B , alors $f^{-1}(J)$ est un idéal de A en particulier $kerf = f^{-1}(0)$ est un ideal de A.*
4. *Si I est un idéal de A et f surjectif , alors $f(I)$ est un idéal de B.*

Démonstration

1. (a) $1_A \in N \Longrightarrow 1_B = f(1_A) \in f(N) \Longrightarrow f(N) \neq \emptyset$

   (b) Soit $y_1, y_2 \in f(N)$, il existe $x_1, x_2 \in N$ tel que / $y_1 = f(x_1)$ et $y_2 = f(x_2)$. On a $y_1 - y_2 = f(x_1) - f(x_2) = f(x_1 - x_2) \in f(N)$ et $y_1y_2 = f(x_1)f(x_2) = f(x_1x_2) \in f(N)$, donc $f(N)$ est un sous anneau de B.

2. (a) $0_B \in D \Longrightarrow f(0_A) = 0_B \in D \Longrightarrow 0_A \in f^{-1}(D) \neq \phi$

   (b) Soit $x_1, x_2 \in f^{-1}(D)$, on a $f(x_1) \in D$ et $f(x_2) \in D$, donc $f(x_1) - f(x_2) \in D$ et $f(x_1)f(x_2) \in D$, donc $f(x_1 - x_2) \in D$ et $f(x_1x_2) \in D$ d 'ou $x_1 - x_2 \in f^{-1}(D)$ et $x_1x_2 \in f^{-1}(D)$. Ainsi $f^{-1}(D)$ est un sous anneau de A.

3. Soit J un idéal de B, nous avons

   (a) $f(0_A) = 0_B \in J \Longrightarrow 0_A \in f^{-1}(J) \Longrightarrow f^{-1}(J) \neq \emptyset$

   (b) Soient $x_1, x_2 \in f^{-1}(J)$ on a $f(x_1) \in J$ et $f(x_2) \in J$, donc $f(x_1 + x_2) = f(x_1) + f(x_2) \in J$ d'où $x_1 + x_2 \in J$.

   (c) Soit $x \in f^{-1}(J)$ et $a \in A$, on a $f(x) \in J$ et $f(a) \in B$, donc $f(ax) = f(a)f(x) \in J$ d'où $ax \in f^{-1}(J)$. On en déduit que $f^{-1}(J)$ est un idéal de A.

4. Soit I un idéal de A et on suppose f surjectif. On a $0_B = f(0_A) \in f(I) \Longrightarrow f(I) \neq \emptyset$ Soient y_1, $y_2 \in f(I)$ et $b \in B$, Alors il existe x_1, $x_2 \in I$ et $a \in A$ tel que $y_1 = f(x_1)$, $y_2 = f(x_2)$ et $b = f(a)$. On a $y_1 + y_2 = f(x_1) + f(x_2) = f(x_1 + x_2) \in f(I)$ et $by_1 = f(a)f(x_1) = f(ax_1) \in f(I)$ donc $f(I)$ est un idéal de A.

6.2.2 Anneaux quotients

Soit A un anneaux et I un idéal de A , on définit sur A la relation d'équivalence suivante $xR_Iy \Longrightarrow x - y \in I$. si x $\in$ A , on note$\overline{x}$ la classe de x *modulo* R_I et parA/I

l'ensemble quotientA/R_I.On definit sur A/I les deux lors suivantes $\overline{x}+\overline{y}= \ \overline{x+y}$ et $\overline{x}\cdot\overline{y}=\overline{xy},(A/I,+,\times)$ est un anneaux et

$$\Pi : A \longrightarrow A/I$$
$$x \longrightarrow \Pi(x)=\overline{x}$$

est un morphisme d' anneaux

On a le théorème de factorisation des morphismes d'anneaux suivant.

Théorème 6.2.6. *Soient A, B deux anneaux et $f : A \longmapsto B$ un morphisme d'anneaux. Si I est un idéal de A tel que $I \subset \ker f$, alors il existe un unique morphisme d'anneaux $g : A/I \longmapsto B$, tel que $f = \overline{f}\circ\pi$. De plus* $\ker g = \ker f/I$.

Démonstration : Soit

$$g : A/I \longmapsto B$$
$$\overline{x} \longmapsto g(\overline{x}) = f(x)$$

Montrons que g est bien défini.

Soit $\overline{x},\overline{y}\in A/I$ tel que $\overline{x}=\overline{y}$

$$\begin{aligned}\overline{x}=\overline{y} &\Longrightarrow x-y\in I \Longrightarrow x-y\in\ker f\\ &\Longrightarrow f(x-y)=0 \Longrightarrow f(x)=f(y)\\ &\Longrightarrow g(\overline{x})=g(\overline{y})\\ &\Longrightarrow g \text{ est bien définie}\end{aligned}$$

Soit $\overline{x}$ et $\overline{y}\in A/I$, on a alors :

$$\begin{aligned}g(\overline{x}+\overline{y}) &= g(\overline{x+y}) = f(x+y) = f(x)+f(y) = g(\overline{x})+g(\overline{y})\\ g(\bar{x}\overline{y}) &= g(\overline{xy}) = f(x)f(y) = g(\overline{x})g(\overline{y})\\ g(\overline{1_A}) &= f(1_A) = 1_B\end{aligned}$$

Donc g est un morphisme d'anneaux.

$\forall x\in A$, on a $g\circ\pi(x)=g(\overline{x})=f(x)$, d'où $f=g\circ\pi$. Montrons que $\ker g=\ker f/I$:

$$\begin{aligned}\overline{x}\in\ker g &\iff g(\overline{x})=0 \iff g\circ\pi(x)=0 \iff f(x)=0\\ &\iff x\in\ker f\end{aligned}$$

d'où $\ker g = \ker f/I$.

Théorème 6.2.7 (Le théorème de correspondance)**.** *Soit A un anneau, I un idéal de A et $\pi : A \longmapsto A/I$ la surjection canonique. Soit $\mathcal{F}_{A/I}$ l'ensemble des idéaux de A/I et Γ_I l'ensemble des idéaux de A contenant I. Alors L'application φ définie comme suit*

$$\begin{aligned} \varphi : \mathcal{F}_{A/I} &\longmapsto \Gamma_I \\ X &\longmapsto \varphi(X) = \pi^{-1}(X) \end{aligned}$$

est une bijection.

<u>Démonstration</u> : Soit $X_1 \in \mathcal{F}_{A/I}$ et $X_2 \in \mathcal{F}_{A/I}$ tel que $\varphi(X_1) = \varphi(X_2)$

$$\begin{aligned} \varphi(X_1) = \varphi(X_2) &\implies \pi^{-1}(X_1) = \pi^{-1}(X_2) \\ &\implies \pi(\pi^{-1}(X_1)) = \pi(\pi^{-1}(X_2)) \\ &\implies X_1 = X_2 \end{aligned}$$

d'où φ est injective.

Soit $J \in \Gamma_I$ un idéal de A contenant I, et soit $x \in J + I$, donc $\exists\, a \in J$ et $b \in I$ tel que $x = a + b$. On a alors :

$$\pi(x) = \pi(a) + \pi(b) = \pi(a) \in \pi(J) \implies x \in \pi^{-1}(\pi(J))$$

d'où

$$J + I \subset \pi^{-1}(\pi(J)) \tag{$*$}$$

Soit $z \in \pi^{-1}(\pi(J))$, alors $\pi(z) \in \pi(J)$, donc $\exists t \in J$ tel que $\pi(z) = \pi(t)$. Par suite, $i = z - t \in I$ et donc $z = t + i \in J + I$ ce qui implique que :

$$\pi^{-1}(\pi(J)) \subset J + I \tag{$**$}$$

$(*)$ et $(**)$ $\implies \pi^{-1}(\pi(J)) = J + I$.

Comme $I \subset J$, on a $\pi^{-1}(\pi(J)) = J$. Ainsi $\forall J \in \Gamma_I$, $J = \varphi(\pi(J))$ donc φ est surjectif, on en déduit que φ est une bijection.

Définition 6.2.8.

Deux idéaux I et J d'un anneau A sont dit comaximaux ou étrangers si $I + J = A$

Lemme 6.2.9.

Soient A un anneau , I et J deux idéaux de A

1. *$IJ \subset I \cap J$*
2. *Si $IetJ$ sont comaximaux alors $IJ = I \cap J$*

<u>Démonstration</u> :

1. soient $a \in I$ et $b \in J$, $ab \in I$ et $ab \in J$, donc $ab \in I \cap J$. Alors on en déduit que I ∩ J contient tous les éléments de la forme $\sum_{i \in K} a_i b_i$, où K est un ensemble fini , $a_i \in I$ et $b_i + J$, donc IJ ⊂ I ∩ J
2. On suppose I + J = A.

   Comme I + J = A , ∃ x ∈ I et ∃ y ∈ J tel que $x + y = 1$

   Soit a ∈ I ∩ J , a = a.1 = ax + ay

   $ax \in IJ$, $ay \in IJ$, donc $a = ax + ay \in IJ$, d'où $I \cap J \subset IJ$.

   comme $IJ \subset I \cap J$, on a $IJ = I \cap J$

Théorème 6.2.10. *(Lemme Chinois)*

Soit A un anneau , I et J deux idéaux comaximaux de A. Alors les anneaux A/IJ et $A/I \times A/J$ sont isomorphes

Démonstration : I et J deux idéaux comaximaux de A, on considère $\pi_1 : A \longrightarrow A/I$, $\pi_2 : A \longrightarrow A/J$ les surjections canoniques et

$$\begin{aligned} f : A &\longmapsto A/I \times A/J \\ x &\longmapsto f(x) = (\pi_1(x), \pi_2(x)) \end{aligned}$$

f est un morphisme d' anneaux, montrons que $\ker f = I \cap J = IJ$.
$x \in kerf$ si et seulement s $\pi_1(x) = 0$ et $\pi_2(x) = 0$, si et seulement si $x \in I$ et $x \in J$ si et seulement si $x \in I \cap J$, donc $\ker f = I \cap J = IJ$. Montrons que f est surjective.
Soit $(a, b) \in A^2$, Comme $I + J = A$, , il existe $u \in I$ et $v \in J$ tel que $u + v = 1$, nous avons $a = au + av$ et $b = ba + bv$ et $\pi_1(a) = \pi_1(av)$, $\pi_2(b) = \pi_2(bu)$. Posons $x = bu + av$, $\pi_1(x) = \pi_1(av) = \pi_1(a)$ et $\pi_2(x) = \pi_1(bv) = \pi_2(b)$, donc $(\pi_1(x), \pi_2(x)) = (\pi_1(a), \pi_1(b))$. Ainsi f est surjective, d'après le premier théorème d'isomorphisme A/IJ et $A/I \times A/J$ sont isomorphes.

Proposition 6.2.11.

Si A corps et B un anneau , alors tout morphisme $f : A \longrightarrow B$ est injectif

6.3 Idéal Premier et Idéal maximal

Définition 6.3.1.

Soit A un anneau et $\mathfrak{p}$ un idéal de A . On dit que $\mathfrak{p}$ est un idéal premier de A si :

1. $\mathfrak{p} \neq A$
2. $\forall (a, b) \in A^2, ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p}$ *ou* $b \in \mathfrak{p}$

Proposition 6.3.2.

Soit $\mathfrak{p}$ un idéal d'un anneau A . Alors $\mathfrak{p}$ est premier si et seulement si l'anneau quotient $A/\mathfrak{p}$ est intègre.

Démonstration :
supposons $\mathcal{P}$ premier
$\mathfrak{p} \neq A \Longrightarrow A/\mathfrak{p} \neq (0)$. Soit $\overline{a} \in A/\mathfrak{p}$ et $\overline{b} \in A/\mathfrak{p}$ telque $\overline{a}.\ \overline{b} = \overline{0}$ .On a $\overline{a}.\ \overline{b} = \overline{0}$ $\Longrightarrow \overline{ab} = 0 \Longrightarrow ab \ \in \mathfrak{p} \Longrightarrow a \ \in \mathfrak{p}$ ou $b \in \mathfrak{p} \ \Longrightarrow \overline{a} = \overline{0}$ *ou* $\overline{b} = \overline{0},$ *donc* $A/\mathfrak{p}$ est intègre.
Réciproquement supposons $A/\mathfrak{p}$ intègre
$A/\mathfrak{p} intégre \ \Longrightarrow A/\mathfrak{p} \neq (0) \ \Longrightarrow A \neq \mathfrak{p}$.
Soit $a \in A$ et $b \in A$ tel que $ab \in \mathfrak{p}$. On a $ab \in \mathfrak{p} \Longrightarrow \overline{ab} = \overline{0}$, donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, ainsi $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$, donc $\mathfrak{p}$ est un idéal premier de A.

Proposition 6.3.3.

Soit $f : A \longrightarrow B$ un morphisme d'anneaux si $\mathfrak{q}$ est un idéal pour de B alors $f^{-1}(\mathfrak{q})$ est un idéal premier de A.

Démonstration :

Soit $f : A \longrightarrow B$ un morphisme d'anneaux et $\mathfrak{q}$ un idéal premier de B , posons $\mathfrak{p} = f^{-1}(\mathfrak{q})$ $f(1_A) = 1_B \notin \mathfrak{q} \ \Longrightarrow 1_A \notin \mathfrak{p} \ \Longrightarrow \mathfrak{p} \neq A$. Soit $a \in A$, $b \in B$ tel que $ab \in \mathfrak{p}$, on a $f(a)f(b) = f(ab) \in \mathfrak{q}$ donc $f(a) \in \mathfrak{q}$ ou $f(b) \in \mathfrak{q}$, d'où $a \in \mathfrak{p}$ ou $a \in \mathfrak{p}$. On en déduit que $\mathfrak{p}$ est un idéal premier de A.
Exemple Les idéaux premier de $\mathbb{Z}$ sont les idéaux de la forme $p\mathbb{Z}$
avec p premier ou $p = 0$

Définition 6.3.4.

Soit A un anneau et $\mathfrak{m}$ un idéal de A . On dit que $\mathfrak{m}$ est un idéal de A si :

1. $\mathfrak{m} \neq A$
2. *les seuls idéaux de A qui contiennent $\mathfrak{m}$ sont $\mathfrak{m}$ et A*

Proposition 6.3.5.

Soit $\mathfrak{m}$ un idéal d'un anneau A. Alors $\mathfrak{m}$ est un idéal maximal de A si et seulement si l'anneau quotient $A/\mathfrak{m}$ est un corps.

Démonstration :
Supposons que l'anneau quotient $A/\mathfrak{m}$ est un corps. Comme $A/\mathfrak{m}\ \mathfrak{m}$ est un corps, $A/\mathfrak{m} \neq (0)$, donc $\mathfrak{m} \neq A$. Soit J un idéal de A contenant $\mathfrak{m}$, si $J = \mathfrak{m}$, la démonstration est terminée. Supposons que $\mathfrak{m} \neq J$; il existe $a \in J$ tel que $a \notin \mathfrak{m}$, donc $\bar{a} \neq \bar{0}$. comme $A/\mathfrak{m}$ est un corps $\bar{a}$ est inversible et il existe $b \in A$ tel que $\bar{a}\bar{b} = \bar{1}$.
Ce qui implique $ab - 1 \in \mathfrak{m} \subset J$, ainsi $1 = ab - (ab - 1) \in J$, par conséquent $J = A$, on en

déduit que $\mathfrak{m}$ est un idéal maximal de A.
Réciproquement supposons que $\mathfrak{m}$ est un idéal maximal de A. Comme $\mathfrak{m}$ est maximal l'anneau quotient $A/\mathfrak{m}$ n'est pas nul. Soit $\bar{x} \in A/\mathfrak{m}$ tel que $\bar{x} \neq \bar{0}$, on a $x \notin \mathfrak{m}$ et l'idéal $\mathfrak{m} + xA$ contient strictement $\mathfrak{m}$, donc $\mathfrak{m} + xA = A$.Par conséquent il existe $m \in \mathfrak{m}$ et $a \in A$ tel que $1 = m + xa$ ce qui implique que $\bar{x}\bar{a} = \bar{1}$ donc $\bar{x}$ est inversible d'où $A/\mathfrak{m}$ est un corps.

Remarque 6.3.6.

1. *Tout idéal maximal $\mathfrak{m}$ d'un anneau A est un idéal premier*
2. *Soit $f : A \longrightarrow B$ un morphisme d'anneau. Si $\mathfrak{q}$ est un idéal maximal de B , $f^{-1}(\mathfrak{q})$ n'est pas en général un idéal maximal de A comme le montre l'exemple suivant :*
   $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, $\mathfrak{q} = (0)$ est un idéal maximal de $\mathbb{Q}$ mais $i^{-1}(\mathfrak{q})$ n 'est pas maximal dans $\mathbb{Z}$.

6.4 Caractéristique d' un anneau

soit A un anneau , on considère l'application
$\varphi : \mathbb{Z} \longrightarrow A$

$$k \longrightarrow \varphi(k) = k.1_A = \begin{cases} 1_A + ... + 1_A \quad (k \textit{ termes}) \ si \ k > 0 \\ \varphi(0) = 0 \\ -\varphi(-k) \quad si \quad k < 0 \end{cases}$$

Lemme 6.4.1.

L'application φ est un morphisme d'anneaux

Démonstration :

1. Montrons que $\varphi(n + m) = \varphi(n) + \varphi(m)$ pour cela destinguons quatre cas.

   Premier cas $n > 0$ *et* $m \geq 0$

   $$\varphi(n + m) = \underbrace{1_A + 1_A + ... + 1_A}_{n+m} = \underbrace{1_A + 1_A + ... + 1_A}_{n} + \underbrace{1_A + 1_A + ... + 1_A}_{m}$$
   $$= \varphi(n) + \varphi(m)$$

   Deuxième cas $n < 0$ et m ≤ 0

   $$\varphi(n + m) = -\varphi(-(n + m)) = -\varphi((-n) + (-m)) = -\varphi(-n) - \varphi(-m)$$
   $$= \varphi(n) + \varphi(m)$$

   Troisième cas $n > 0$, m ≤ 0 et n + m ≥ 0

   $$\varphi(n + m) = \underbrace{1_A + 1_A + ... + 1_A}_{n+m} = \underbrace{1_A + 1_A + ... + 1_A}_{n} + \underbrace{1_A + 1_A + ... + 1_A}_{-m}$$

$$= \varphi(n) - \varphi(-m)$$
$$= \varphi(n) + \varphi(m)$$

Quatrième cas $n \geq 0$, m < 0 et n + m ≤ 0

$$\begin{aligned}\varphi(n+m) &= -\varphi[-(n+m)] \\ &= -\varphi[(-m)+(-n)] \\ &= -\varphi(-m) - \varphi(-n) \\ &= -\varphi(m) + \varphi(n)\end{aligned}$$

Ainsi $\forall (m,n) \in \mathbb{Z}^2, \varphi(n+m) = \varphi(m) + \varphi(n)$

2. Montrons que $\varphi(nm) = \varphi(m)\varphi(n)$
   Si m = 0 ou n = 0 alors $\varphi(nm) = \varphi(m)\ \varphi(n)$. Supposons n $\neq 0$ et m $\neq 0$
   Distinguons trois cas :
   Premier cas $n > 0$ *et* $m > 0$
   $$\varphi(n\ m) = \underbrace{1_A + 1_A + ... + 1_A}_{nm} = \underbrace{1_A + 1_A + ... + 1_A}_{n} + \underbrace{1_A + 1_A + ... + 1_A}_{m}$$
   $$= \varphi(n)\ \varphi(m)$$
   Deuxième cas $n < 0$ *et* $m < 0$
   $\varphi(n\ m) = \varphi[(-m)(-n)] = \varphi(-n)\varphi(-m) = [-\varphi(n)][-\varphi(m)] = \varphi(n)\varphi(m).$
   Troisième cas $n > 0$ *et* $m < 0$
   $\varphi(n\ m) = -\varphi(n(-m)) = -\varphi(n)\varphi(-m) = \varphi(n)[-\varphi(nm)] = \varphi(n)\varphi(m).$
3. On a $\varphi(1) = 1_A$, donc φ est un morphisme d'anneaux.

Définition 6.4.2. *kerφ est un idéal de $\mathbb{Z}$, donc $\exists\ n \in \mathbb{N}$ tel que ker $\varphi = n\mathbb{Z}$. L'entier n est appelé caractéristique de l'anneau A. On le note caract(A).*

Remarque 6.4.3.

1. *Si φ est injectif , caract(A) = 0 , $\mathbb{Z} \simeq \mathrm{Im}\,\varphi$ l' anneau A contient un sous anneau isomorphe à $\mathbb{Z}$. Ce sous-anneau est appelé sous-anneau premier de A . Ce sous-anneau est souvent noté $\mathbb{Z}$*

2. *Si φ n' est un pas injectif , $\ker\varphi = n\ \mathbb{Z}$,caract(A) = $n > 0$ alors $\mathrm{Im}\,\varphi \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. A contient un anneau isomorphisme à $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Ce sous anneau est appelé sous anneau premier de A on le note souvent pas $\mathbb{Z}_n$.*

Exemple 6.4.4.

1. Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique zéro.

2. $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.
3. Un anneau fini ne peut être de caractéristique 0.

Théorème 6.4.5.

Soit A un anneau intègre. Alors $caract(A) = 0$ ou $caract(A) = p$ est un nombre premier

Démonstration

Comme A est intègre , le sous anneau $Im\varphi$ l' est aussi. or $Im\varphi$ est isomorphisme à $\mathbb{Z}/caract(A)\mathbb{Z}, donc \quad \mathbb{Z}/caract(A)\mathbb{Z}$ est un anneau intègre , donc $caract(A)\mathbb{Z}$ est un idéal premier d'ou $caract(A) = 0$ ou $caract(A) = p$ est un nombre premier.

Corollaire 6.4.6.

La caractéristique d' un corps est ou bien nulle ou bien un nombre premier.

Démonstration :

Il suffit de montrer qu'un corps est un anneau intègre. Soit k un corps et $(a, b) \in k^2$ tel que $ab = 0$, si $a \neq 0$, a est inversible , donc $b = 0$.

Théorème 6.4.7.

Soit p un nombre premier et A un anneau de caractéristique p alors

$$\forall (a, b) \in A^2, (a + b)^p = a^p + b^p.$$

Démonstration :

Soit $k \in [1, p - 1]$, p est premier avec tous les entiers $1, 2, ...$, donc p est premier avec $k!$ Comme p divise $k!\ C_p^k$, d'après Gauss , p divise $C_p^k = \alpha_k\ p$ où α_k est un entier.

$$(a + b)^p = \sum_{k=0}^{p} C_p^k\ a^k\ b^{n-k} = a^p + b^p + \sum_{k=1}^{p-1} p\ \alpha_k\ a^k\ b^{n-k}$$
$$= a^p + b^p$$

6.5 Corps de Fraction d'un anneau intègre

Soit A un anneau intègre et $S = A\star = A \setminus \{0\}$, on définit sur $A \times S$ la relation d'équivalence suivante :

$$(a, s)\ \mathcal{R}\ (b, t) \iff at - bs = 0.$$

, on note par $\dfrac{a}{s}$ la classe de (a, s) et par $S^{-1}A$ l'ensemble quotient de $A \times S$ par la relation d'équivalence $\mathcal{R}$. On définit sur $S^{-1}A$ les deux lois suivantes $\dfrac{x}{s} \in S^{-1}A$ et $\dfrac{y}{t} \in S^{-1}A$, on pose $\dfrac{x}{s} + \dfrac{y}{t} = \dfrac{xt + ys}{st}$ et $(\dfrac{x}{s})(\dfrac{y}{t}) = \dfrac{xy}{st}$

Lemme 6.5.1.

Les deux lois définies ci dessus ne dépendent pas des représentants (x, s) *et* (y, t)

<u>**D**émonstration</u> :

Soient $(x_1, s_1), (x_2, s_2),\ (y_1, t_1),\ (y_2, t_2)\ \in\ A\ \times\ S$ tel que $\frac{x_1}{s_1} = \frac{x_2}{s_2}$ *et* $\frac{y_1}{t_1} = \frac{y_2}{t_2}$ montrons que
$\frac{x_1}{s_1} + \frac{x_1}{s_1} = \frac{x_2}{s_2} + \frac{y_2}{t_2}$ et $\frac{x_1}{s_1} \cdot \frac{y_1}{t_1} = \frac{x_1}{s_1} \cdot \frac{y_1}{t_1}$, d'une part , on a :

$$\begin{aligned} s_2t_2\ (x_1t_1 + y_1s_1) -\ s_1t_1\ (x_2t_2 + y_2s_2) &= x_1s_2t_1t_2 + y_1t_1s_1s_2\ -\ x_2s_1t_1t_2 - y_2t_1s_1s_2 \\ &= t_1t_2(x_1s_2 - x_1s_1) +\ s_1s_2(y_1t_2 - y_2t_1) \\ &= 0 \end{aligned}$$

donc on en déduit que $\frac{x_1}{s_1} + \frac{y_1}{t_1} = \frac{x_2}{s_2} + \frac{y_2}{t_2}$.
D'autre part

$$\begin{aligned} 0 &= (x_1s_2 - x_2s_1)(y_1t_2 - y_2t_1) \\ &= x_1y_1s_2t_2\ -\ x_2y_2s_1t_1 \end{aligned}$$

donc, $\frac{x_1}{s_1} \cdot \frac{y_1}{t_1} = \frac{x_2}{s_2} \cdot \frac{y_2}{t_2}$

Lemme 6.5.2.

$(S^{-1}A, +)$ *est un groupe abélien.*

<u>**D**émonstration</u> :

1. Soit $\frac{x_1}{s_1}, \frac{x_2}{s_2}$ *et* $\frac{x_3}{s_3} \in S^{-1}A$
   $\left(\frac{x_1}{s_1} + \frac{x_2}{s_2}\right) + \frac{x_3}{s_3} = \frac{x_1\ s_2\ +\ x_2\ s_1}{s_1\ s_2} + \frac{x_3}{s_3} = \frac{x_1\ s_2\ s_3\ +\ x_2\ s_1\ s_3\ +\ x_3\ s_1\ s_2}{s_1\ s_2\ s_3}$
   $= \frac{x_1(\ s_2\ s_3)\ +\ (x_2\ s_3\ +\ x_3\ s_2)s_1}{s_1\ (s_2\ s_3)} = \frac{x_1}{s_1} + \frac{x_2\ s_3\ +\ x_3\ s_2}{s_2\ s_3}$
   $= \frac{x_1}{s_1} + \left(\frac{x_2}{s_2} + \frac{x_3}{s_3}\right)$ donc la loi est associativité.

2. Soit $\frac{x_1}{s_1} \in\ S^{-1}\ A$ *et* $\frac{x_2}{s_2}\ S^{-1}\ A$
   $\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{x_1\ s_2\ +\ x_2\ s_1}{s_1\ s_2} = \frac{x_1\ s_2\ +\ x_2\ s_1}{s_1\ s_2} = \frac{x_2}{s_2} + \frac{x_1}{s_1}$
3. Soit $\frac{x_1}{s_2} \in S^{-1}A,\quad \frac{x}{s} + \frac{0}{1} = \frac{x \times 1 + 0 \times s}{s \times 1} = \frac{x}{s}$.
   $\frac{0}{1}$ est l'élément neutre de $S^{-1}A$.

4. Soit $\frac{x}{s} \in S^{-1}A$, $\frac{x}{s} + \left(-\frac{x}{s}\right) = \frac{xs - xs}{ss} = \frac{0}{s^2} = \frac{0s^2}{s^2} = \frac{0}{1}$.

Théorème 6.5.3.

$(S^{-1}A, +, \times)$ *est un corps.*

Démonstration :

D'après les lemmes ci - dessus $(S^{-1}A, +)$ est un groupe.

i) Soit $\frac{x_1}{s_1}$, $\frac{x_2}{s_2}$ et $\frac{x_3}{s_3} \in S^{-1}A$.

$$\left(\frac{x_1}{s_1}.\frac{x_2}{s_2}\right).\frac{x_3}{s_3} = \left(\frac{x_1\ x_2}{s_1\ s_2}\right).\frac{x_3}{s_3} = \frac{(x_1\ x_2)x_3}{(s_1 s_2)s_3} = \frac{x_1(x_2\ x_3)}{s_1(s_2\ s_3)}$$

$$= \frac{x_1}{s_1}.\frac{x_2\ x_3}{s_2\ s_3} = \frac{x_1}{s_1}.\left(\frac{x_2}{s_2}.\frac{x_3}{s_3}\right) \quad \text{d'où l'associativité}$$

ii) Soit $\frac{x_1}{s_1}, \frac{x_2}{s_2} \in S^{-1}A$, $\frac{x_1}{s_1}.\frac{x_2}{s_2} = \frac{x_1\ x_2}{s_1\ s_2} = \frac{x_2\ x_1}{s_2\ s_1} = \frac{x_2}{s_2}.\frac{x_1}{s_1}$

donc la loi $\times$ est la commutativité

iii) Soit $\frac{x_1}{s_1}$, $\frac{x_2}{s_2}$ et $\frac{x_3}{s_3} \in S^{-1}A$

$$\frac{x_1}{s_1}\left(\frac{x_2}{s_2} + \frac{x_3}{s_3}\right) = \frac{x_1}{s_1}\left(\frac{x_2\ s_3 + x_3\ s_2}{s_2\ s_3}\right) = \frac{x_1\ x_2\ s_3 + x_1\ x_3\ s_2}{s_1\ s_2\ s_3}$$

$$= \frac{[(s_1 x_2)s_3 + (x_1\ s_3)s_2]}{s_1(s_1 s_2\ s_3)} = \frac{(x_1\ x_2)s_1\ s_3 + (x_1\ x_3)s_1\ s_2}{(s_1\ s_2)(s_1\ s_3)}$$

$$= \frac{x_1\ x_2}{s_1\ s_2} + \frac{x_1\ x_3}{s_1\ s_3} = \frac{x}{s_1}.\frac{x_2}{s_2} + \frac{x_1}{s_1}.\frac{x_3}{s_3}$$

donc $\times$ est distributive par rapport à $+$.

iv) $\forall\ \frac{x}{s} \in S^{-1}A$, $\frac{x}{s}.\frac{1}{1} = \frac{x \times 1}{s \times 1} = \frac{x}{s}$, $\frac{1}{1}$ est l'unité de $S^{-1}A$

v) Soit $\frac{x}{s} \in S^{-1}A$ tel que $\frac{x}{s} \neq \frac{0}{1}$. On a $x \neq 0$, donc

$$\frac{x}{s} \in S^{-1}A \ \text{ et } \ \frac{x}{s}.\frac{s}{x} = \frac{x_1}{s_1} = \frac{1}{1}.$$

i), ii), iii), iv) et v) entraîne que $(S^{-1}A, +, \times)$ est un corps.

Lemme 6.5.4. *L'application*

$$i : A \longrightarrow S^{-1}A$$
$$a \longrightarrow i(a) = \frac{a}{1}$$

est un morphisme injectif d'anneaux.

Démonstration :

Soit $a, b \in A$, on a

- $i(a+b) = \dfrac{a+b}{1} = \dfrac{a}{1} + \dfrac{b}{1} = i(a) + i(b)$
- $i(ab) = \dfrac{ab}{1} = \dfrac{a}{1}.\dfrac{b}{1} = i(a)\ i(b)$
- $i(1_A) = \dfrac{1}{1}$ donc i est un morphisme d'anneaux.

Soient a et $b \in A$ tel que $i(a) = i(b)$

$$i(a) = i(b) \Longrightarrow \frac{a}{1} = \frac{b}{1} \Longrightarrow a.1 = b.1 \Longrightarrow a = b.$$

Remarque 6.5.5.

1. *le morphisme i permet d'identifier A au sous-anneau $i(A) = \left\{\dfrac{a}{1}\ /\ a \in A\right\}$ de $S^{-1}A$.*
2. *Les éléments de S sont inversibles dans $S^{-1}A$*
   $\forall s \in S,\quad i(s) = \dfrac{s}{1}$ est inversible dans $S^{-1}A$ d'inverse $\dfrac{1}{s}$.

Propriété universelle de $(S^{-1}A, +, \times)$:

Théorème 6.5.6.

Soit A un anneau intègre et $S = A\setminus\{0\}$. Alors le couple $(S^{-1}A, i)$ vérifie la propriété universelle suivante.
Pour tout corps L et tout morphisme injectif d'anneaux $f : A \longrightarrow L$, il existe un unique morphisme d'anneaux $g : S^{-1}A \longrightarrow L$ tel que $f = g \circ i$.

Démonstration :

Soit A un anneau intègre, $S = A\setminus\{0\}$ et soit L un corps et $f : A \longrightarrow L$ un morphisme injectif d'anneaux. Notons que $\forall s \in S$, $f(s)$ est inversible dans L. On considère

$$\begin{aligned} &g : S^{-1}A \longrightarrow L \\ &\frac{a}{1} \longrightarrow g(\frac{a}{s}) = f(a)(f(s))^{-1}. \end{aligned}$$

- Montrons que g est bien définie, soit $\dfrac{a}{s}$ et $\dfrac{b}{t} \in S^{-1}A$ tel que $\dfrac{a}{s} = \dfrac{b}{t}$

$$\begin{aligned} \frac{a}{s} = \frac{b}{t} &\Longrightarrow at = bs \Longrightarrow f(at) = f(bs) \Longrightarrow f(a)\ f(t) = f(b)\ f(s) \\ &\Longrightarrow f(a)(f(s))^{-1} = f(b)(f(t))^{-1} \Longrightarrow g(\frac{a}{s}) = g(\frac{b}{t}) \end{aligned}$$

- Montrons que g est un morphisme d'anneaux (de corps)

$$\begin{aligned} g\left(\frac{a}{s} + \frac{b}{t}\right) &= f(at+bs)[f(st)]^{-1} \\ &= \Big[f(a)\ f(t) + f(b)\ f(s)\Big]\ (f(s)^{-1}\ f(t)^{-1}) \\ &= f(a)(f(s))^{-1} + f(b)(f(t))^{-1} \\ &= g(\frac{a}{s}) + g\left(\frac{b}{t}\right) \end{aligned}$$

$$\begin{aligned} g\left(\frac{a}{s}\,\frac{b}{t}\right) = f(ab)\ (f(st))^{-1} &= f(a)\ f(b)\ (f(s))^{-1}\ (f(t))^{-1} \\ &= f(a)\ (f(s))^{-1}\ f(b)\ (f(t))^{-1} \\ &= g(\frac{a}{s}))g(\frac{b}{t}) \end{aligned}$$

$g\left(\dfrac{1}{1}\right) = f(1)\ \Big[f(1)\Big]^{-1} = f(1) = 1_L$

g est donc un morphisme de corps.

De plus

$$\begin{aligned} \forall a \in A, \quad g \circ i(a) = g(i(a)) = g\left(\frac{a}{1}\right) &= f(a)\ (f(1))^{-1} \\ &= f(a) \end{aligned}$$

d'où $f = g \circ i$. Soit $h : S^{-1}A \longrightarrow L$ un morphisme de corps tel que $h \circ i = f$.

$$\begin{aligned} &\forall\ a \in A, \quad h\left(\frac{a}{1}\right) = h \circ i(a) = f(a) \\ &\forall\ s \in S, \quad h\left(\frac{1}{s}\right) = h\left[\left(\frac{s}{1}\right)^{-1}\right] = \left[h\left(\frac{s}{1}\right)\right]^{-1} = \Big[h \circ i(s)\Big]^{-1} = \Big[f(s)\Big]^{-1}. \end{aligned}$$

Donc $\forall a \in A$ et $\forall s \in S$,

$$h\left(\frac{a}{s}\right) = h\left(\frac{a}{1}.\frac{1}{s}\right) = h\left(\frac{a}{1}\right)\ h\left(\frac{1}{s}\right) = f(a)\Big[f(s)\Big]^{-1} = g\left(\frac{a}{s}\right).$$

donc $h = g$. On dit que g est l'unique morphisme $S^{-1}A \longrightarrow L$ qui prolonge i.

Théorème 6.5.7. *$S^{-1}A$ est l'unique corps (à isomorphisme près) vérifiant la propriété universelle du théorème ci-dessus.*

__**Démonstration :**__ Soit A un anneau intègre, $S = A \setminus \{0\}$ $i : A \longrightarrow S^{-1}A$. Soit F un corps et $j : A \longrightarrow F$ un morphisme injectif d'anneaux vérifiant la propriété universelle ci - dessus. Montrons que F et $S^{-1}A$ sont isomorphes. On a $id_{S^{-1}A} \circ i = i$ et $id_F \circ j = j$

$$i : A \longrightarrow S^{-1}A \qquad a \longrightarrow i(a) = \frac{a}{1}$$

On a $id_{S^{-1}A} \circ i = i$ et $id_F \circ\ j = j$

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[d, "i"'] & S^{-1}A \\ S^{-1}A \arrow[ur, "id_{S^{-1}A}"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "j"] \arrow[d, "j"'] & F \\ F \arrow[ur, "id_F"'] & \end{tikzcd}$$

$id_{S^{-1}A}$ est l'unique endomorphisme de corps de $S^{-1}A$ qui prolonge i , de même id_F est l'unique endomorphisme de corps de F qui prolonge j.

Comme $i : A \longrightarrow F$ est injective , il existe un unique morphisme de corps, $l : F \longrightarrow S^{-1}A$ tel que $l \circ j = i$ ce qui se traduit par le diagramme suivant :

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[d, "j"'] & S^{-1}A \\ F \arrow[ur, "l"'] & \end{tikzcd}$$

De même comme $j : A \longrightarrow F$ est injectif , il existe un unique morphisme de corps $k : S^{-1}A \longrightarrow F$ tel que $k \circ i = j$

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[d, "j"'] & F \\ S^{-1}A \arrow[ur, "k"'] & \end{tikzcd}$$

On a $(k \circ l) \circ j = k \circ (l \circ j) = k \circ i = j$ et $(l \circ k) \circ i = l \circ (k \circ i) = l \circ j = i$, ainsi , $k \circ l = id_F$ et $(l \circ k) = id_{S^{-1}A}$, donc l et k sont des isomorphismes de corps d'où F et $S^{-1}A$ sont isomorphes.

Définition 6.5.8.

Le corps $S^{-1}A$ est appelé corps des fractions anneau intègre A et se note $Fr(A)$.

Exemple 6.5.9.

$Fr(\mathbb{Z}) = \mathbb{Q}$

Définition 6.5.10.

Soit A un anneau et S une partie de A. On dit que S est une partie multiplicative de A si :

i) $1 \in S$

ii) $\forall \ (s_1, s_2) \in S^2$ *on a* $s_1 s_2 \in S$.

Exemple 6.5.11.

1. Si A est un anneau intègre $S = A \setminus \{0\}$ est une partie multiplicative de A.
2. Soit A un anneau et $s \in A$, $S = \{s^n \ \backslash n \in \mathbb{N}\}$ est une partie multiplicative de A
3. Soit A un anneau et $\mathfrak{p}$ un idéal premier de A alors $S = A \setminus \mathfrak{p}$ est une partie multiplicative de A.

<u>Exercice</u> :

Soit A un anneau et S une partie multiplicative de A on définit sur $A \times S$ la relation d' équivalence suivan
$(a, s) \ \mathcal{R} \ (b, t) \Longleftrightarrow \exists u \ \in \ S \setminus u(at - bs) = 0,$ on note par $S^{-1}A$ l'ensemble quotient de

$A \times S$ *par* $\mathcal{R}$ *on* note par $\dfrac{a}{s}$ la classe $\overline{(a, s)}$ et on définit sur $S^{-1}A$ les deux lois suivantes :
$\dfrac{a}{s} + \dfrac{a}{s} = \dfrac{at + bs}{st}$ *et* $\dfrac{a}{s} \cdot \dfrac{b}{t} = \dfrac{ab}{st}$

Chapitre 7

Anneaux Factoriels - Anneaux Principaux

7.1 Anneau de Polynômes

7.1.1 Anneau de Polynômes à une indéterminée

a) <u>Construction et Définitions</u>

Définition 7.1.1.

Soit A un anneau, on appelle polynôme à une indéterminée à coefficients dans A, une suite d'éléments de A n'ayant qu'un nombre fini de termes non nuls.

On note un tel polynôme par $P = (a_i)_{i\in\mathbb{N}} = (a_0, \cdots, a_n, \cdots)$ les éléments non nuls a_i sont appelés les coefficients du polynôme P.

Définition 7.1.2.

Soit A un anneau et $P = (a_i)_{i\in\mathbb{N}}$ un polynôme à coefficients dans A et $n = max\{i/a_i \neq 0\}$, le coefficient a_n est appelé coefficient dominant de P.

Si $a_n = 1$, on dit que P est un polynôme unitaire ou normalisé.

On définit dans l'ensemble B des polynômes à une indéterminée à coefficients dans A les deux opérations suivantes :

1. ***<u>Addition</u>*** *:* $P = (a_i)_{i\in\mathbb{N}}$ *et* $Q = (b_i)_{i\in\mathbb{N}}$
   $P + Q = (s_i)_{i\in\mathbb{N}}$ *avec* $s_i = a_i + b_i$, *la loi* $+$ *est interne dans* B.
2. ***<u>Multiplication</u>*** *:* $P = (a_i)_{i\in\mathbb{N}}$ *et* $Q = (b_i)_{i\in\mathbb{N}}$, $PQ = (c_n)_{i\in\mathbb{N}}$ *avec*
   $c_n = \sum_{i+j=n} a_i b_j$.

Théorème 7.1.3.

Le triplet $(B, +, \times)$ *est un anneau et*

$$\begin{aligned} i : A &\longrightarrow B \\ A &\longrightarrow (a, 0, \cdots) \end{aligned}$$

est un morphisme injectif d'anneaux.

Démonstration :

1. (a) Il est clair que $(B, +)$ est un groupe abélien

   ii. Commutativité de $\times$ On a

$$P = (b_i)i \in \mathbb{N}, \quad Q = (b_i)i \in \mathbb{N}, \quad PQ = \left(\sum_{p+q=n} a_p b_q\right)_{i\in\mathbb{N}} = \left(\sum_{p+q=n} b_q a_p\right)_{i\in\mathbb{N}} = QP$$

   La loi $\times$ est commutative.

   (b) associativité de $\times$

   Soit $P = (a_i)_{i\in\mathbb{N}}, \quad Q = (b_i)_{i\in\mathbb{N}}$ et $R = (c_i)_{i\in\mathbb{N}}$

$$PQ = (d_s)_{s\in\mathbb{N}} \quad \text{avec} \quad d_s = \sum_{p+q=s} a_p b_q$$
$$(PQ)R = (e_i)_{i\in\mathbb{N}} \quad \text{avec} \quad e_n = \sum_{s+r=n} d_s c_r$$

$$e_n = \sum_{s+r=n} a_s \left(\sum_{p+q=s} a_p b_q\right) c_r = \sum_{s+r=n} \left(\sum_{+q=s} a_p b_q c_r\right) = \sum_{p+q+r=s} a_p b_q c_r$$

   $P(QR) = (PQ)R = (f_i)_{i\in\mathbb{N}}$

$$f_n = \sum_{p+q+r=n} b_q c_r a_p = \sum_{p+q+r=n} a_p b_q c_r = e_n$$

   donc $(PQ)R = P(QR)$ d'où $\times$ est associative.

   (c) Distributivité de $\times$ par rapport à $+$: Soit $(P = (a_i)_{i\in\mathbb{N}}, \quad Q = (b_i)_{i\in\mathbb{N}}$ et $R = (c_i)_{i\in\mathbb{N}}$.

$$P \centerdot (Q + R) = (d_n)_{i\in\mathbb{N}} \quad \text{avec} \quad d_n = \sum_{p+q=n} a_p(b_q + c_q)$$

$$d_n = \sum_{p+q=n} (a_p b_q + a_p c_q) = \sum_{p+q=n} a_p b_q + \sum_{p+q=n} a_p c_q$$

   donc $P(Q + R) = PQ + PR$, la multiplication est distributive par rapport à l'addition.

(d) L'élément neutre pour la loi $\times$: Notons

$$\begin{aligned} 1_B &= (1, 0, \cdots, 0, \cdots) \\ &= (a_0, a_1, \cdots) \end{aligned} \qquad \text{et} \quad P = (b_i)_{i \in \mathbb{N}}$$

$$P \cdot 1_B = (d_n)_{i \in \mathbb{N}} \quad \text{avec} \quad d_n = \sum_{p+q=n} a_p b_q = a_n$$

car le seul terme non nul de cette somme est celui pour lequel $p = 0$ et $q = n$ donc $P 1_B = P$, 1_B est l'élément unité de B.

2. Soit

$$\begin{aligned} (a, b) \in A^2,\ i(a+b) \quad &= (a+b, 0, \cdots 0, \cdots) \\ &= i(a) + i(b) \\ i(ab) = (a, 0, \cdots, 0, \cdots) \quad &= i(a)\ i(b) \\ i(1) = (1, 0, \cdots) \quad &= 1_B \end{aligned}$$

donc i est un morphisme d'anneaux, de plus i est injectif.

<u>**Notations :**</u> Posons $X = (0, 1, 0, \cdots, 0, \cdots)$

$$X^2 = (0, 0, 1, 0, \cdots), \cdots, \quad X^k = (\overbrace{0, \cdots, 0}, 1, 0, \cdots, 0)$$

$P = (a_o, a_1, \cdots, a_n, 0, \cdots) = a_o(1, 0, \cdots, 0) + a_1(0, 1, 0, \cdots) + \cdots + a_n(0, \cdots, 1, \cdots)$
$= \sum_{k \in \mathbb{N}} a_k X^k$, on note $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$.

Définition 7.1.4.

$P = (a_i)_{i \in \mathbb{N}}$ est le polynôme nul si $a_i = 0 \quad \forall i \in \mathbb{N}$

Définition 7.1.5.

Soit $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$ un polynôme non nul.

On appelle degré de P, le nombre $n = max\{i / a_i \neq 0\}$ on le note $\deg(P)$.

On appelle valuation de P, le nombre $min\{i / a_i \neq 0\}$ on le note $Val(P)$.

Remarque 7.1.6.

1. *Si P est le polynôme nul, on pose* $\deg(P) = -\infty$ *et $Val(P) = +\infty$.*
2. *Si P est non nul et si $n = \deg(P)$ alors $P(X) = \sum_{k=0}^{n} a_k X^k$*
   a_n est appelé coefficient dominant de P.

Proposition 7.1.7.

1. $\deg(P+Q) \leq max(\deg(P), \deg(Q))$
2. *Si* $\deg(P) \neq \deg(Q)$ *alors* $\deg(P+Q) = max(\deg(P), \deg(Q))$
3. $deg(PQ) \leq deg(P) + deg(Q)$
4. *Si* A *n'a pas de diviseur de zéro, alors*

$$\deg(PQ) = \deg(P) + \deg(Q).$$

En particulier si A *est intègre alors* $A[X]$ *est intègre.*

Démonstration :

1. $n > max(\deg(P), \deg(Q)) \Longrightarrow \begin{cases} n > \deg(P) \\ n > \deg(Q) \end{cases} \Longrightarrow \begin{cases} a_n = 0 \\ b_n = 0 \end{cases}$

   $\Longrightarrow a_n + b_n = 0$, donc $\deg(P+Q) \leq max(\deg(P), \deg(Q)$
2. Notons $\deg(P) = m$ et $\deg(Q) = \ell$, on suppose $m < \ell$

$$N = max(M, \ell) = \ell, \quad a_N + b_N = a_\ell + b_\ell = b_\ell \neq 0, \text{ donc}$$

$$\deg(P+Q) = \ell = max(\deg(P), \deg(Q))$$

3. $P = (a_i)_{i\in\mathbb{N}}$, $a_p = 0$ si $p > m$, $Q = (b_i)_{i\in\mathbb{N}}$, $b_q = 0$ si $q > \ell$

$$PQ = (c_n)_{i\in\mathbb{N}}, \quad c_n = \sum_{p+q=n} a_p b_q$$

   $\forall n \in \mathbb{N}, \quad n > \ell + m \Longrightarrow a_p = 0$ et $b_q = 0 \Longrightarrow c_n = 0$
   donc $deg(PQ) \leq m + \ell = deg(P) + deg(Q)$
4. $PQ = (C_n)_{i\in\mathbb{N}}$, $C_n = \sum_{p+q=n} a_p b_q$

$$C_{n+\ell} = \sum_{p+q=m+\ell} a_p b_q = a_m b_\ell \neq 0 \text{ car } a_m \neq 0 \text{ et } b_\ell \neq 0$$

   et A intègre, donc $\deg(PQ) = \deg(P) + \deg(Q)$. Soit $P = (a_i)_{i\in\mathbb{N}} \neq 0$, $Q = (b_i)_{i\in\mathbb{N}} \neq 0$

$$m = \deg(P), \qquad \ell = \deg(Q), \qquad PQ = (C_n)_{i\in\mathbb{N}},$$

$$\deg(PQ) = m + \ell, \qquad C_{m+\ell} = a_m b_\ell \neq 0, \text{ donc } PQ \neq 0$$

   Ainsi $A[X]$ est intègre

Notation :

Soit A un anneau, on note $\mathcal{U}(A)$ l'ensemble des éléments inversibles de A.

Corollaire 7.1.8.

Soit A un anneau intègre, alors $\mathcal{U}(A[X])$ est l'ensemble des éléments de la forme $(a, 0, \cdots, 0, \cdots)$ où $a \in \mathcal{U}(A)$.

Démonstration :

Soit $P \in A[X]$ avec A intègre.

P est inversible $\Longrightarrow \exists Q \in A[X] \;/\; PQ = 1$

$$PQ = 1 \Longrightarrow deg(P) + deg(Q) = deg(PQ) = 0$$
$$\Longrightarrow deg(P) = 0 \text{ et } deg(Q) = 0$$
$$\Longrightarrow P = (a, 0, \cdots, 0, \cdots) \text{ et } Q = (b, 0, \cdots, 0, \cdots)$$

$$PQ = 1 \Longrightarrow (ab, 0, \cdots) = (1, 0, \cdots) \Longrightarrow ab = 1 \Longrightarrow a \in \mathcal{U}(A).$$

Théorème 7.1.9. *Soit A un anneau et $P = \sum_{i=0}^{n} a_i X^i$ un polynôme à coéficients dans A. Alors :*

1. *Le polynôme P est un diviseur de zéro dans $A[X]$ si et seulement si il existe $b \in A$ non nul tel que $bP = 0$.*
2. *Le polynôme P est nilpotent si et seulement si les coéficients $a_0, a_1, \cdots, a_n$ sont nilpotents.*
3. *Le polynôme P est inversible dans $A[X]$ si et seulement si a_0 est inversible dans A et les $a_1, \cdots, a_n$ sont nilpotents.*

Démonstration :

Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme à coéficients dans A.

1. S'il existe $b \in A$ non nul tel que $bP = 0$ alors P est un diviseur de zéro. Réciproquement si que P est un diviseur de zéro, il existe $H \in A[X]$ non nul tel que $PH = 0$. L'ensemble
$$\{\deg(H) / H \neq 0 \text{ et } PH = 0\}$$
est une partie non vide de $\mathbb{N}$, donc admet un minimum m. Soit $Q = \sum_{j=0}^{m} b_i X^i \in A[X]$ tel que $PQ = 0$. On a $PQ = b_m a_n X^{m+n} + (b_m a_{n-1} + b_{m-1} a_n) X^{m+n-1} + \cdots = 0$, donc $b_m a_n = 0$, montrons que $b_m P = 0$. Si $b_m P \neq 0$, il existe un entier i tel que $0 \leq i \leq n$ et $b_m a_i \neq 0$. Soit a_{n-k} le premier des coéficients de P tel que $b_m a_{n-k} \neq 0$, on a $b_m a_n = b_m a_{n-1} = \cdots = b_m a_{n-k+1} = 0$.
Comme $(a_l Q)P = 0$ et $\deg(a_l Q) < \deg(Q)$ pour $n-k+1 \leq l \leq n$, nous avons $a_l Q = 0$

à cause de la minimalité de $\deg(Q)$. En posant $P_1 = a_nX^n + \cdots + a_{n-k+1}X^{n-k+1}$ et $P_2 = a_{n-k}X^{n-k} + \cdots + a_0X^{n-k+1}$, nous avons $P = P_1 + P_2$ et $P_1Q = 0$, donc $0 = PQ = P_1Q + P_2Q = P_2Q$, ainsi $b_ma_{n-k} = 0$. Ce qui contredit le choix a_{n-k}, n en déduit que $b_mP = 0$.

2. Si les coéfficients a_i de P sont nilpotents alors P est nilpotent. Réciproquement supposons que P est nilpotent montrons par récurrence sur $n = \deg(P)$ que les coéfficients a_i sont nilpotents. La propriété est vraie pour $n = 0$, supposons $n \geq 1$ et la propriété vraie pour polynôme de degré strictement inférieur à n. Posons $P_1 = P - a_nX^n$, comme P est nilpotent, il existe $m \in \mathbb{N}$ tel que $P^m = (P_1 + a_nX^n)^m = \sum_{i=0}^{m} \binom{m}{i} P_1^i a_n^{m-i} X^{n(m-i)} = 0$. Ce qui implique $a_n^m X^{mn} + \sum_{i=1}^{m} \binom{m}{i} a_n^{m-i} X^{n(m-i)} P_1^i = 0$, donc $a_n^m = 0$ et a_n est nilpotent, ainsi P_1 est nilpotent. Comme $\deg(P_1) < n$, l'hypothèse de récurrence entraîne que les coéfficients $a_0, \cdots a_{n-1}$ sont nilpotents.

3. Supposons que a_0 inversible, les $a_1, \cdots a_n$ sont nilpotents et posons $P = a_0 + P_1$, d'après 2) le polynôme P_1 est nilpotent. Soit d l'indice de nilpotence de P_1 et $Q_1 = a_0^{-1}P_1$, on a $Q_1 = a_0^{-1}P = 1 - Q_1$ donc

$$a_0^{-1}P(1 + Q_1 + \cdots + Q_1^{d-1}) = 1 - Q_1^d = 1$$

donc le polynôme P est inversible. Réciproquement supposons que P est inversible montrons par récurrence sur $n = \deg(P)$ que a_0 inversible et les coéfficients $a_1, \cdots a_n$ sont nilpotents. Si $n = 0$ alors $P = a_0$ est inversible, supposons $n \geq 1$ et la propriété vraie pour polynôme inversible de degré strictement inférieur à n. Comme P est inversible, il existe un polynôme $Q = \sum_{j=0}^{m} b_iX^i \in A[X]$ tel que $PQ = \sum_{k=0}^{m+n} \sum_{i+j=k} a_ib_jX^k = 1$. On a

$$\begin{array}{rcl} a_nb_m & = & 0 \\ a_nb_{m-1} + a_{n-1}b_m & = & 0 \\ a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m & = & 0 \\ \vdots & & \\ a_1b_0 + a_0b_1 & = & 0 \\ a_0b_0 & = & 1 \end{array}$$

La dernière équation montre que a_0 et b_0 sont inversibles. En multipliant la seconde équation par a_n et la troisième par a_n^2 on obtient $a_n^2b_{m-1} = 0$ et $a_n^3b_{m-2} = 0$. En rítérant le procedé on a $a_n^{m+1}b_0 = 0$, d'où $a_n^{m+1} = 0$ ainsi a_n est nilpotent. On considère l'anneau quotient $A[X]/\langle X^n \rangle$, on a $\bar{P} = \sum_{i=0}^{n-1} a_i\bar{X}^i$. La relation $PQ = 1$ implique $\bar{P}\bar{Q} = 1$, donc $\bar{P}$ est inversible. Par hypothèse de récurrence les coéfficients $a_1, \cdots, a_{n-1}$ sont nilpotents ainsi nous avons le résultat.

b) Division euclidienne

Théorème 7.1.10.

Soit A un anneau, $Q \in A[X]$ non nul dont le coefficient dominant est inversible dans A. Alors $\forall P \in A[X]$ il existe un unique couple $(H, R) \in (A[X])^2$ tel que

$$P = HQ + R \quad avec \quad \deg(R) < \deg(Q)$$

Démonstration :

Elle se fait par une récurrence forte sur $n = \deg(P)$. Quitte à multiplier par l'inverse du coefficient dominant de Q on peut supposer que Q est unitaire (normalisé).

Posons $\deg(Q) = m$. Si $\deg(P) < \deg(Q)$, on pose $H = 0$ et $R = P$. Supposons $\deg(P) = n \geq m = \deg(Q)$. Si $n = 0$ alors $R = 0$; la propriété est vraie pour $n = 0$.

Supposons le résultat vrai pour tout polynôme de degré $< n$. Soit $P = \sum_{k=0}^{n} a_k X^k$, $\qquad a_n X^{n-m}$ est de degré n et sont coefficient dominant est a_n. Posons $T = P - a_n Q X^{n-m}$ $deg(T) < n$.

Par hypothèse de récurrence, $\exists (H_1, R_1) \in (A[X])^2$ tel que $T = H_1 Q + R_1$ avec $\deg(R_1) < \deg(Q)$.

$$\begin{aligned} P = T + a_n Q\ X^{n-m} &= H_1 Q + R_1 + a_n\ X^{n-m} Q \\ &= (H_1 + a_n\ X^{n-m}) Q + R_1 \ \text{ avec } \ \deg(R_1) < \deg(Q) \end{aligned}.$$

Posons $\qquad H = H_1 + a_n\ X^{n-m}$ et $R = R_1$

On a $\qquad P = HQ + R$ et $\deg(R) < \deg(Q)$.

Unicité :

$$P = H_1 Q + R_1 = H_2 Q + R_2 \ \text{ avec } \ \deg(R_1) < \deg(Q) \ \text{ et } \ \deg(R_2) < \deg(Q)$$

$$0 = (H_1 - H_2) Q + R_1 - R_2 \Longrightarrow R_2 - R_1 = (H_1 - H_2) Q.$$

Si $H_1 - H_2 \neq 0$. Comme le coefficient dominant de Q est 1

$$\begin{aligned} &\deg(R_2 - R_1) = \deg\Big[(H_1 - H_2) Q\Big] \geq deg(Q) \ \text{ or} \\ &\deg(R_2 - R_1) \leq max(\deg(R_1), \deg(R_2)) < \deg(Q). \end{aligned}$$

Ainsi, $R_1 = R_2$ et $H_1 = H_2$, d'où l'unicité.

Théorème 7.1.11. *Soit A un anneau, $P \in A[X]$ non nul dont le coefficient dominant est a. Alors pour tout $F \in A[X]$, il existe $k \in \mathbb{N}$ et $Q, R \in A[X]$ tels que*

$$a^k F = PQ + R \quad avec \quad \deg(R) < \deg(Q).$$

On peut poser $k = \max\{0, 1 + \deg(F) - \deg(P)\}$

Démonstration : Posons $P = \sum_{i=0}^{n} a_i X^i$ avec $a_n = a$ et $F = \sum_{j=0}^{m} b_j X^j$.
Si $\deg(F) < \deg(P)$ alors on prend $k = 0$, $Q = 0$ et $R = F$. Supposons $\deg(F) \geq \deg(P)$ et montrons la propriété par récurrence sur $m = \deg(F)$. Si $m = 0$ alors $n = 0$ et le résultat est vrai. Supposons $m \geq 1$ et la propriété vraie pour tout polynôme de degré strictement inférieur à m. Posons $F_1 = aF - b_m X^{m-n} P$, on a $\deg(F_1) < m$, par hypothèse de récurrence, il existe un entier naturel $k_1 \in \mathbb{N}$, Q_1 et R deux polynômes à coéfficients dans A tels que $a^{k_1} F_1 = PQ_1 + R$ avec $\deg(R) < \deg(Q)$ et $k_1 = \max\{0, 1 + \deg(F_1) - \deg(P)\}$. En posant $k = k_1 + 1$, $Q = Q_1 + a^{k_1} b_m X^{m-n}$, on a $a^k F = PQ + R$.

Exemples :

1. $A = \mathbb{Z}/4\mathbb{Z}$, $\quad P(X) = X^4 + \overline{3}X^3 + \overline{2}X$ et $\varphi = \overline{3}X^3 + \overline{1}$
   $\overline{3} \in \mathcal{U}(\mathbb{Z}/4\mathbb{Z})$, il existe un unique couple (H, R) tel que

$$P = HQ + R, \qquad H = \overline{3}X + \overline{1} \text{ et } R = \overline{3}X + \overline{3}$$

2. $A = \mathbb{Z}/4\mathbb{Z}$, $\quad A[X] = \mathbb{Z}/4\mathbb{Z}[X]$

c) Fonction polynomiale ou évaluation

Définition 7.1.12.

Soit A un anneau, $x_o \in A$ et $P \in A[X]$.
$P(X) = a_o + a_1 X + \cdots + a_n X^n$. On appelle évaluation de P en x_o
$eval_{x_o}(P) = a_o + a_1 x_o + \cdots + a_n x_o^n$, on note $eval_{x_o}(P) = P(x_o) = a_o + a_1 x_o + \cdots + a_n x_o^n \in A$.
Si B est un anneau contenant A comme sous - anneau

$$Q \in A[X], \qquad P(Q) = a_o + a_1 Q + \cdots + a_n Q^n.$$

Proposition 7.1.13.

Soit A un anneau, $x_o \in A$ alors l'application

$$\begin{aligned} eval_{x_o} : A[X] &\longrightarrow A \\ P &\longrightarrow eval_{x_o}(P) \end{aligned}$$

est un morphisme d'anneaux

Démonstration :

$$eval_{x_o}(P + Q) = (P + Q)(x_o) = P(x_o) + Q(x_o) = eval_{x_o}(P) = eval_{x_o}(Q)$$

$$P = (a_i)_{i\in\mathbb{N}}, \quad Q = (b_i)_{i\in\mathbb{N}}, \quad P_\alpha = (c_n)_{n\in\mathbb{N}}, \quad c_n = \sum_{p+q=n} a_p b_q$$

$$\begin{aligned} eval_{x_o}(PQ) = c_n\ x_o^n &= \sum_{n\in\mathbb{N}} \left(\sum_{p+q=n} a_p b_q \right) x_o^{p+q} \\ &= \sum_{n\in\mathbb{N}} \sum_{p+q=n} (a_p x_o^p)(b_q x_o^q) \\ &= \sum_p \sum_q a_p x_o^p\ b_q x_o^q \\ &= \left(\sum_{q\in\mathbb{N}} a_p x_o^p \right) \left(\sum_{q\in\mathbb{N}} b_p x_o^q \right) \\ &= eval_{x_o}(P) eval_{x_o}(Q) \end{aligned}$$

$eval_{x_o}\left(1_{A[X]}\right) = 1_{A[X]}(x_o) = 1_A$.

Définition 7.1.14.

Soit A un anneau et $P \in A[X]$, une racine de P est un élément $a \in A$ (ou d'un anneau contenant A) tel que $P(a) = 0$.

Proposition 7.1.15.

Soit $a \in A$ et $P \in A[X]$, alors P est un multiple de $X - a$ si et seulement si $P(a) = 0$.

Démonstration :

La division euclidienne de P par $X \longrightarrow a$ donne

$$P(X) = (X - a)\ Q(X) + R(X) \ \text{ avec } \ d \circ R < 1 \Longrightarrow d \circ R \leq 0$$

R est une constante et $R = P(a)$.

$$\begin{gathered} P(X) = (X - a)\ Q(X) + P(a) \\ P(a) = 0 \Longleftrightarrow P = (X - a)Q \end{gathered}$$

Définition 7.1.16.

Soit $P \in A[X]$ et a une racine de P, la multiplicité de a est le plus grand entier m tel que $(X - a)^m$ divise P, a une racine simple si $m = 1$.

Définition 7.1.17.

Soit $P \in A[X]$, $P(X) = \sum_{k\in\mathbb{N}} a_n X^n$. La dérivée formelle de P est $P'(X) = \sum_{n\geq 1} n a_n\ X^{n-1}$.

Proposition 7.1.18.

Soit $a \in A$ *et* $P \in A[X]$, a *une racine simple de* P *si et seulement si* $P'(a) \neq 0$.

Démonstration :

Si a est une racine de P de multiplicité m alors

$$P(X) = (X-a)^m\, Q(X) \quad \text{avec} \quad Q(a) \neq 0.$$

Théorème 7.1.19. *(changement de l'anneau de base)*

Soit $f : A \longrightarrow B$ *un morphisme non nul d'anneaux.*
alors il existe un et un seul morphisme d'anneaux $\varphi : A[X] \longrightarrow B[Y]$ *qui prolonge* f *et transforme l'indéterminée* X *de* $A[X]$ *en indéterminée* Y *de* $B[Y]$.

Démonstration :

$$\varphi : A[X] \longrightarrow B[Y]$$
$$P = \sum_{n\in\mathbb{N}} a_n X^n \longrightarrow \varphi(P) = \sum_{n\in\mathbb{N}} \varphi(a_n) Y^n$$

répond à la question.

7.1.2 Anneau de Polynôme à plusieurs indéterminées

a) Construction et Définition

Soit A un anneau $B = A[X]$ l'anneau des polynômes à une indéterminée X. Soit V une indéterminée, $C = B[Y]$ l'anneau des polynômes à une indéterminée à coefficients dans B. $P \in B[Y]$ s'écrit d

$$P(X) = \sum_{j=0}^{m} b_j\, Y^j, \qquad b_j \in B = A[X], \qquad b_j = \sum_{j=0}^{n} a_{i,j}\, X^i$$

avec $a_{ij} \in A$, donc $P = \sum_{i=0}^{n} a_{i,j} X^i) Y^j = \sum_{j=0}^{m}\sum_{i=0}^{n} a_{i,j} X^i Y^j$.
On note par $A[X,Y]$, l'anneau $C = B[Y] = A[X][Y]$.
Si T est une indéterminée, on définit $C[X]$

$$Q \in C[X], \quad \text{s'écrit} \quad Q = \sum_{k=0}^{\ell} P_k T^k, \quad P_k \in C = A[X,Y]$$

$P_k = \sum_{j=0}^{m}\sum_{i=0}^{n} a_{i,k,k}\, X^i Y^j$, donc

$Q = \sum_{k=0}^{\ell}\sum_{j=0}^{m}\sum_{i=0}^{n} a_{i,k,k}\, X^i Y^j T^k$ on note

$C[T]$ par $C[T] = A[X,Y,Z]$

Définition 7.1.20.

Soit A *un anneau et* $n \geq 1$ *un entier.*
On définit par récurrence sur n *l'anneau* $A[X_1, \cdots, X_n]$ *des polynômes à* n *déterminées* $X_1, \cdots, X_n$ *par :*

- Si $n \geq 2$, $A[X_1, \cdots, X_{n-1}, X_n] = A[X_1, \cdots, X_{n-1}][X_n]$ *est l'anneau des polynômes à une indéterminée* X_n *à coefficients dans* $A[X_1, \cdots, X_{n-1}]$.
Un élément $P \in A[X_1, \cdots, X_n]$ *s'écrit sous la forme*

$$P(X_1, \cdots, X_n) = \sum_{\alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n} a_{\alpha_1}, \alpha_n \; X_1^{\alpha_1} \; X_2^{\alpha_2} \cdots X_n^{\alpha_n}.$$

Les $a_\alpha = a_{\alpha_1,\cdots,\alpha_n}$ *étant nuls sauf pour un nombre fini.*

Remarque 7.1.21.

1. *Pour* $\alpha = (\alpha_1, \cdots, \alpha_n)$, *on note* $|\alpha| = \alpha_1 + \cdots + \alpha_n$
2. *Soit* $\sigma \in \mathcal{S}_n$, *une permutation,* $A[X_1, \cdots, X_n] = A[X_{\sigma_{(1)}}, \cdots, X_{\sigma_{(n)}}]$
3. *Soit* $m \in \mathbb{N}$ *tel que* $m \leq n$, $A[X_1, \cdots, X_n] = A[X_1, \cdots, X_m] = A[X_{m+1}, \cdots, X_m]$.

Définition 7.1.22.

Un élément de $A[X_1, \cdots, X_n]$ *de la forme* $a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ *est monôme et si* $a_\alpha \neq 0$, *son degré total est* $|\alpha| = \sum_{i=1}^{n} \alpha_i$. *Les* α_i *sont les degrés partiels.*

Définition 7.1.23.

Soit $P = \sum_{\alpha\in\mathbb{N}} a_\alpha \; X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ *un polynôme non nul, le degré total de* P *est le maximum des degrés des monômes non nuls dont il est la somme,*

$$deg(P) = max\left\{\sum_{i=1}^{n} \alpha_i = |\alpha| \; / \; a_\alpha \neq \right\}$$

$$deg(0) = -\infty \quad et \quad deg(P+Q) \leq sup\Big(deg(P) + deg(Q)\Big)$$

Définition 7.1.24.

Un polynôme $P = \sum_{\alpha\in\mathbb{N}^n}^{n} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha}$ *est dit homogène de degré* s *si* $P \neq 0$ *et si tous les monômes* $\alpha_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ *ont le même degré* $|\alpha| = s$.

Proposition 7.1.25.

Soit P *et* Q *deux polynômes homogènes de degré* s *et* t. *Si* $PQ \neq 0$ *alors* PQ *est homogène de degré* $s + t$.

Démonstration :

$$P = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} \; , \quad \sum_{i=1}^{n} \alpha_i = s.$$

$$Q = \sum_{\beta \in \mathbb{N}^n} b_\beta X_1^{\beta_1} \cdots X_n^{\beta_n} \ , \quad \sum_{j=1}^{n} \beta_j = s.$$

Si $PQ \neq 0$, il existe au moins un terme.
$C_\gamma = \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta$ non nul et chaque C_j non nul est le coefficient du monôme

$$C_\gamma \ X_1^{\alpha_1+\beta_1} \ X_2^{\alpha_2+\beta_2} \cdots X_n^{\alpha_n+\beta_n} \text{ de degré } \sum_{i=1}^{n} (\alpha_i + \beta_i) = s + t.$$

Proposition 7.1.26.

Un polynôme P de degré m s'écrit de manière unique comme somme de Polynômes $P = P_o + P_1 + \cdots + P_m$ ou P_s est soit nul soit homogène de degré s et ou $P_m \neq 0$.

Démonstration :

$P = \sum a_\alpha \ X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, somme de monômes deux à deux distincts. On définit P_s comme étant 0 ou la somme de tous les monômes de degré s. On a $P_m \neq 0$.
La décomposition est unique car si deux polynômes homogènes sont égaux, ils ont même degré.

Corollaire 7.1.27.

Soient P et $Q \in A[X_1, \cdots, X_n]$ et si $P_\alpha \neq 0$ alors

$$deg(Q) \leq deg(P) + deg(Q).$$

Démonstration :

$$P = P_o + P_1 + \cdots + P_s \ et \ \text{ et } \ Q = Q_o + Q_1 + \cdots + Q_r.$$

Q_i est homogène de degré i et Q_j est homogène de degré j. On a

$$PQ = P_o Q_o + \cdots + \sum_{i+j=h} P_i Q_j + \cdots + P_s Q_r, \quad \text{avec}$$
$$P_o Q_o, \sum_{i+j=1} P_i Q_j, \cdots, \sum_{i+j=h} P_i Q_j, \cdots, P_s Q_r$$

sont soit nuls soit homogènes de degré $0, 1, \cdots, h, \cdots, s + t$, donc

$$\deg(PQ) \leq s + t.$$

b) **Propriété universelle de** $A[X_1, \cdots, X_n]$.

Théorème 7.1.28.

Soit $f : A \longrightarrow B$ un morphisme d'anneaux.
Soient $y_1, y_2, \cdots, y_n \in B$. Alors il existe un morphisme unique d'anneaux $\varphi : A[X_1, \cdots, X_n] \longrightarrow B$ tel que la restriction de φ à A soit égale à f $(\varphi/A = f)$ et $\varphi(X_i) = y_i$.

Démonstration :

Soit $P = \sum_{\alpha\in\mathbb{N}^n} a_\alpha \; X_1^{\alpha_1}\cdots X_n^{\alpha_n}$, on définit l'application

$$\begin{aligned} \varphi : AX_1, \cdots, X_n] &\longrightarrow b \\ P &\longrightarrow \varphi(P) = \sum_{\alpha\in\mathbb{N}^n} f(a_\alpha) y_1^{\alpha_1}\cdots y_n^{\alpha_n} \end{aligned}$$

$$\begin{aligned} \varphi(X_i) &= y_i \;, \text{ on a } \; \varphi(P+Q) = \varphi\left(\sum_{\alpha\in\mathbb{N}^n} a_\alpha \; X_1^{\alpha_1}\cdots X_n^{\alpha_n} + \sum_{\alpha\in\mathbb{N}^n} b_\alpha \; X_1^{\alpha_1}\cdots X_n^{\alpha_n}\right) \\ &= \sum_{\alpha\in\mathbb{N}^n} f(a_\alpha + b_\alpha) y_1^{\alpha_1}\cdots y_n^{\alpha_n} = \sum_{\alpha\in\mathbb{N}^n} f(a_\alpha) y_1^{\alpha_1}\cdots y_n^{\alpha_n} + \sum_{\beta\in\mathbb{N}^n} f(b_\alpha) y_1^{\alpha_1}\cdots y_n^{\alpha_n} = \varphi(P) + \varphi(Q) \end{aligned}$$

$\varphi(a) = f(a) \qquad \forall a \in A.$

Posons $H = PQ = \sum_\gamma C_\gamma \; X_1^{\alpha_1}\cdots X_n^{\alpha_n}$

$$C_r = \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta, \quad \varphi(H) = \sum_{\gamma\in\mathbb{N}^n} f(C_\gamma) \; y_1^{\gamma_1}\cdots X_n^{\gamma_n}$$

$$f(C_\gamma) = \sum_{\alpha+\beta=\gamma} f(a_\alpha) \; f(b_\beta), \quad \text{donc}$$

$$\begin{aligned} \varphi(H) &= \sum_{\gamma\in\mathbb{N}^n}\left(\sum_{\alpha+\beta=\gamma} f(a_\alpha) f(b_\beta)\right) y_1^{\alpha_1}\cdots y_n^{\alpha_n} \\ &= \sum_{\gamma\in\mathbb{N}^n}\left(\sum_{\alpha+\beta=\gamma} f(a_\alpha) f(b_\beta) \; y_1^{\alpha_1+\beta_1} \; y_2^{\alpha_2+\beta_2}\cdots y_n^{\alpha_n+\beta_n}\right. \\ &= \sum_{\gamma\in\mathbb{N}^n} f(a_\alpha) y_1^{\alpha_1}\cdots y_n^{\alpha_n} \centerdot \sum_{\gamma\in\mathbb{N}^n} f(b_\alpha) y_1^{\beta_1} \; y_2^{\beta_2}\cdots y_n^{\alpha_n} \\ &= \varphi(P) \; \varphi(Q), \end{aligned}$$

donc φ est un morphisme d'anneaux.

L'unicité de φ découle de la définition.

Définition 7.1.29.

Soient k un corps et A un anneau, on dit que A est une k - algèbre si k est un sous - anneau de A.

Définition 7.1.30.

Soient k un corps, A et B deux k - algèbres.
On appelle morphisme de k - algèbre de A vers B, tout morphisme d'anneaux $f : A \longrightarrow B$ telle que $f(\lambda) = \lambda \qquad \lambda \in K$.

Remarque 7.1.31. *Une expression du type $\sum_{\alpha\in\mathbb{N}^n} a_\alpha \; y_1^{\alpha_1}\cdots y_n^{\alpha_n}$ est appelée expression polynomiale des éléments $y_1, \cdots, y_n$.*

Remarque 7.1.32. *(Algèbre sur un anneau)*

Soit k *un anneau. Une* k *- algèbre est un couple* (A, i) *où* A *est un anneau et* $i : k \longrightarrow A$ *est un morphisme d'anneaux. Soient* (A, i) *et* (B, j) *deux* k *- algèbres.*
Un morphisme de k *- algèbres est un morphisme d'anneaux* $f : A \longrightarrow B$ *tel que* $f(i(\lambda)) = j(\lambda) \quad \forall \lambda \in k$.

c) **Sous - anneau engendré**

Soit A un anneau, X une partie quelconque de A, le sous - anneau B de A engendré par X est l'intersection des sous - anneaux de A contenant X, c'est le plus petit sous - anneau de A contenant $X.L'anneau$ B contient 0 et 1_A, donc B contient le sous - anneau premier $\mathbb{Z}_n$ $(n \in \mathbb{N})$ de A.
L'anneau B est le plus petit sous - anneau de A contenant X et $\mathbb{Z}_n$.

Soit I un ensemble et $D = \{X_i \ / \ i \in I\}$ un ensemble d'indéterminées indexé par I. Pour toute partie $K = \{i_1, i_2, \cdots, i_t\}$ $(t \in \mathbb{N}^*)$ finie de I, on note $A_K = A[X_{i_1}, \cdots, X_{i_t}]$ l'anneau des polynômes à coefficients dans A où $t = card\ K$ et $X_{i_1}, \cdots, X_{i_t}, \quad i_k \in K$ sont les indéterminées.
Si K et L sont deux parties finies de I, $A_K \subset A_{K \cup L}$ et $A_L \subset A_{K \cup L}$. Notons $\mathcal{F}(I)$ l'ensemble des parties finies non vides de I et $A[D] = A[X_i/i \in I] = \bigcup\limits_{K \in \mathcal{F}(I)} A_K$.
$P, Q \in A[X_i/i \in I]$, il existe une partie finie non vide K de I tel que $P \in A_K$ et $Q \in A_K$.
On définit $P + Q$ et PQ dans $A[X_i/i \in I]$, ou comme étant la somme $P + Q$ et le produit PQ dans A_K. L'ensemble $A[X_i/i \in I]$ est un anneau contenant A comme sous - anneau. De plus l'anneau A_K est un sous - anneau de $A[X_i/i \in I]$.

Théorème 7.1.33. *Soit* A *un anneau de sous - anneau premier* $\mathbb{Z}_n$ $(= \mathbb{Z}$ *si* $n = 0$ *ou si* $\mathbb{Z}/n\mathbb{Z}$ *si* $n > 0)$ *et* $\wedge$ *une partie non vide de* A.
Alors le sous - anneau de A *engendré par* $\wedge$ *est l'ensemble de toutes les expressions polynomiales d'éléments de* $\wedge$ *à coefficients dans* $\mathbb{Z}_n$

Démonstration :

Soit $\{X_\alpha/\alpha \in \wedge\}$ un ensemble d'indéterminée indexées par $\wedge$. Considérons l'application

$$\begin{aligned} \varphi : \mathbb{Z}_n[X_\alpha/\alpha \in \wedge] &\longrightarrow A \\ P &\longrightarrow \varphi(P) = P(\alpha_{i_1}, \cdots, \alpha_{i_t}) \end{aligned}$$

où $P \in \mathbb{Z}_n[X_{\alpha_{i_1}}, X_{\alpha_{i_2}}, \cdots, X_{\alpha_{i_t}}]$, $\alpha_{i_k} \in A$, $1 \leq k \leq t$.
Dans l'expression de P ne figurent que les indéterminées $X_{\alpha_{i_1}}, X_{\alpha_{i_2}}, \cdots, X_{\alpha_{i_t}}$ indexées par les éléments $\alpha_{i_1}, \cdots, \alpha_{i_t}$ de $\wedge$.
$\varphi(P) = P(\alpha_{i_1}, \cdots, \alpha_{i_t})$ où l'on substitue α_{i_k} à X_{i_k}.

Soit $P(X_{\alpha_{i_1}}, X_{\alpha_{i_2}}, \cdots, X_{\alpha_{i_t}})$ et $Q(X_{\beta_{j_1}}, X_{\beta_{j_2}}, \cdots, X_{\beta_{j_s}}) \in \mathbb{Z}_n[X_\alpha/\alpha \in \wedge]$.

$$\begin{aligned} Q(P+Q) &= P(\alpha_{i_1}, \cdots, \alpha_{i_t}) + Q(\beta_{j_1}, \cdots, \beta_{j_s}) \\ &= \varphi(P) + \varphi(Q) \\ \varphi(PQ) &= \varphi(P)\ \varphi(Q) \ \text{ et } \ \varphi(1_{\mathbb{Z}_n}) = 1_A. \end{aligned}$$

φ est un morphisme d'anneaux, $\operatorname{Im}\varphi$ est un sous - anneau de A.

Soit $\alpha \in \wedge$ et $P = X_\alpha$, $\varphi(P) = \alpha$, donc $\wedge \subset Im\varphi$.

Soit B un sous -anneau de A contenant $\wedge$, comme $1_A \in B$, B contient toute expression polynomiale d'éléments de $\wedge$ à coefficients dans $\mathbb{Z}_n$, donc $\operatorname{Im}\varphi \subset B$. Par conséquent $\operatorname{Im}\varphi$ est le sous - anneau de A engendré par $\wedge$.

Notation :

Soit A un anneau et $\wedge$ une partie de A, on note $\mathbb{Z}_n[\wedge]$ le sous - anneau de A engendré par $\wedge$.

Corollaire 7.1.34. *Soit $\wedge = \{s_1, \cdots, s_t\}$ une partie finie d'un anneau A.*
Alors $\mathbb{Z}_n[\wedge] = \left\{ P(s_1, \cdots, s_t) \ / \ P \in \mathbb{Z}_n[X_1, \cdots, X_t] \right\}$.

Définition 7.1.35.

Soit A un anneau, $B \supset A$ une A- algèbre, on dit que B est une A-algèbre de type fini s'il existe $b_1, \cdots, b_n \in B$ tel que

$$B = A[b_1, \cdots, b_n] = \left\{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha \ b_1^{\alpha_1} \cdots b_2^{\alpha_2} \ / \ a_\alpha \in A \right\}$$

l'ensemble des expressions polynomiales à coefficients dans A.

7.2 Anneaux Factoriels

7.2.1 Divisibilité et éléments irréductibles

Définition 7.2.1.

Soit A un anneau intègre, $(a, b) \in A^2$, non nuls. On dit que b divise a (ou que a est divisible par b) et on note b/a s'il existe $c \in A$ tel que $a = bc$.

Remarque 7.2.2.

La relation b/a équivaut à dire que a appartient à l'idéal Ab engendré par b c'est à dire $b \backslash a \Longleftrightarrow \langle a \rangle \subset \langle b \rangle$.

Définition 7.2.3.

Soit A un anneau intègre, $(a,b) \in A^2$, non nuls. On dit que b et a sont associés s'il existe un élément inversible $u \in A$ tel que $b = ua$.

Définition 7.2.4.

Soit A un anneau intègre, $p \in A$ un élément non nul. On dit que p est irréductible si :

1. *p n'est pas inversible dans A.*
2. *Si $p = ab$, avec $a, b \in A$, alors a est inversible ou b est inversible.*

Remarque 7.2.5.

1. *Si p est irréductible et $u \in A$ inversible, alors up est irréductible*
2. *Si p est irréductible, les seuls diviseurs de p, sont les éléments inversibles et les associés de p.*

Définition 7.2.6. *Soit A un anneau intègre, $a, b \in A$. On dit que a et b sont premiers entre eux si on a : $\forall d \in A$, si d divise a et d divise b alors d est inversible dans A.*

Proposition 7.2.7.

Soit A un anneau intègre, $a \in A$, $a \neq 0$. Si l'idéal $\langle a \rangle = aA$ est premier, alors l'élément a est irréductible.

<u>Démonstration</u> :

On suppose $\langle a \rangle = aA$ est premier

aA premier $\Longrightarrow aA \neq A \Longrightarrow a$ est non inversible.

Soit $b, c \in A$ tel que $a = bc$.

$a = bc \in aA \Longrightarrow b \in aA$ ou $c \in aA$.

$b \in aA \Longrightarrow \exists uA \ / \ b = ua \Longrightarrow a = uac \Longrightarrow 1 = uc \Longrightarrow c$ est inversible de la même manière, $c \in aA \Longrightarrow b$ est inversible.

Remarque 7.2.8.

L'implication réciproque de l'énoncé de la proposition ci - dessus est en général fausse. Comme le montre l'exemple suivant.

Exemple 7.2.9.

Soit $A = \mathbb{Z}[i\sqrt{5}]$ le sous - anneau de c engendré par $\mathbb{Z}$ et $i\sqrt{5}$

1. Montrer que $A = \left\{ m + i\sqrt{5} \ / \ (m,n) \in \mathbb{Z}^2 \right\}$
2. Déterminer les éléments inversibles de A
3. Montrer que les éléments $2, 3, 1 + i\sqrt{5}$ sont irréductibles.

4. Montrer que l'idéal engendré par 2 dans A n'est pas premier.

Solution :

1. $\mathbb{Z}[i\sqrt{5}]$ est l'ensemble des expressions polynomiales de $i\sqrt{5}$ à coefficients dans $\mathbb{Z}$, donc $A = \mathbb{Z}[i\sqrt{5}] = \left\{ m + in\sqrt{5} \ / \ (m,n) \in \mathbb{Z}^2 \right\}$
2. Soit $z = m + in\sqrt{5}$. Posons $N(z) = |z|^2 = m^2 + 5n^2$
   z inversible $\Longrightarrow \exists z' \in A \ / \ zz' = 1 \Longrightarrow N(z) = 1$
   $\Longrightarrow m^2 + 5n^2 = 1 \Longrightarrow m^2 = 1$ et $n^2 = 0 \Longrightarrow z = 1$ ou $z = -1$
   $\mathcal{U}(A) = \{1, -1\}$.
3. Soit $z_1 = a + ib\sqrt{5}$ et $z_2 = c + id\sqrt{5}$ tel que $2 = z_1 z_2$
   $2 = z_1 z_2 \Longrightarrow N(2) = N(z_1)\ N(z_2) \Longrightarrow 4 = (a^2 + 5b^2)(c^2 + 5d^2)$
   $\Longrightarrow a^2 + 5b^2$ divise 4.
   $\Longrightarrow a^2 + 5b^2 = 1$ ou $a^2 + 5b^2 = 2$ ou $a^2 + 5b^2 = 4$
   on a $a^2 + 5b^2 \neq 2$
   . Si $a^2 + 5b^2 = 1$ alors $a = 1$ ou $a = -1$ et $b = 0$, donc
   $z_1 = 1$ ou $z_1 = -1$ est inversible
   . $a^2 + 5b^2 = 4 \Longrightarrow c^2 + 5d^2 = 1 \Longrightarrow z_2$ est inversible.
   Ainsi 2 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$.
4. Posons $a = 1 + i\sqrt{5}$, $\qquad b = 1 - i\sqrt{5}$
   $ab = 6 = 2 \times 3$, mais $1 + i\sqrt{5} \notin \langle 2 \rangle$ et $1 - i\sqrt{5} \notin \langle 2 \rangle$
   donc $\langle 2 \rangle$ n'est pas premier.
   Les anneaux factoriels sont les anneaux pour lesquels la réciproque est vraie.

7.2.2 Anneaux factoriels

Définition 7.2.10. *Soit A un anneau. On dit que A est factoriel s'il vérifie les trois propriétés suivantes*

1. *A est intègre*
2. *Tout élément non nul a est produit d'un nombre fini d'éléments irréductibles*
3. *Si $a \in A$ est non nul et non inversible et si*

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

où $q_1, q_2, \cdots, q_n$ et $p_1, \cdots, p_m$ sont des éléments irréductibles de A,
alors $m = n$ et il existe $\sigma \in \mathcal{S}_n$, $u_i \in \mathcal{U}(A)$ tel que $p_i = u_i\ q_{\sigma(i)}$, $1 \leq i \leq n$.

Théorème 7.2.11. *Soit A un anneau intègre. alors A est factoriel si et seulement si les deux conditions suivantes sont vérifiées :*

i) Chaque élément non nul et non inversible de A est produit d'un nombre fini d'éléments irréductibles de A.

ii) Soit $a \in A$ un élément irréductible et si a divise b produit de bc de deux élements a, c de A alors a divise b ou a divise c.

<u>Démonstration</u> :

$\Longrightarrow$) Soit A un anneau factoriel, la condition i) est vérifiée.

Soit $a \in A$ un élément irréductible et soit $(b,c) \in A^2$ tel que a divise bc. il existe $d \in A$ tel que $bc = ad$.

Si b est inversible, alors $c = adb^{-1}$, donc a divise c,. De même si c est inversible alors a divise b. Supposons b et c non inversibles. On peut alors écrire $b = p_1p_2\cdots p_t$, $c = p_{t+1}\cdots p_{t+s}$ et, $d = q_1q_2\cdots q_r$. La relation $bc = ad$ entraîne que $p_1p_2\cdots p_t\ p_{t+1}\cdots p_{t+s} = aq_1q_2\cdots q_r$.

Comme a est irréductible, il existe $i_o \in \{1,..,t+s\} = \{1,..,t\} \cup \{t+1,..,t+s\}$ et $u_o \in A$ inversible tel que $a = u_{i_o}\ p_{i_o}$.

Si $i_o \in \{1,..,t\}$, a divise b et si $i_o \in \{t+1,..,t+s\}$, a divise c d'où le résultat.

$\Longleftarrow$) Réciproquement supposons que les conditions $i)$ et $ii)$ sont vérifiées et montrons que A est factoriel.

Par hypothèse A intègre et la condition 2°) de la définition est vérifiée.

Soit $a \in A$ non nul et non inversible, tel que $a = p_1p_2\cdots p_m = q_1q_2\cdots q_n$ avec les p_i et q_j irréductibles.

Supposons que $m \leq n$ et montrons par récurrence sur m que 3°) est vérifiée.

Si $m = 1$, q_1 divise p_1, donc $\exists u_1 \in A$ inversible tel que $q_1 = u_1p_1$, donc $n = 1$ donc la propriété est vraie pour $m = 1$. Supposons $m \geq 2$ et le résultat vrai pour $m - 1$.

Comme p_1 divise $p_1(p_2\cdots q_1q_2\cdots q_m)$, d'après la propriété $ii)$ il existe $i \in \{1,..,n\}$ tel que p_1 divise q_i, c'est à dire $q_i = u_ip_1$ ou $u_i \in \mathcal{U}(A)$. On a

$$p_1(p_2\cdots p_m) = u_ip_1(q_1\cdots q_{i-1}\ q_{i+1}\cdots q_n) \Longrightarrow p_2\cdots p_m = u_iq_1\cdots q_{i-1}\ q_{i+1}\cdots q_n.$$

Par hypothèse de récurrence $m-1 = n-1$ et $p_2 = u_2q_{\gamma(2)}$, $p_3 = u_3\ q_{\gamma(3)}, \cdots, p_m = u_m\ q_{\gamma(m)}$, les $u_2, \cdots, u_m$ étant inversibles et

$$\gamma : \{2,\cdots,m\} \longrightarrow \{1,\cdots,i-1,i+1,\cdots,m\} \text{ est une bijection.}$$

Posons $\sigma : \{1,\cdots,m\} \longrightarrow \{1,2,\cdots,m\}$ définie par

$$\sigma(k) = \begin{cases} \gamma(k) & \text{si } k \neq 1 \\ i & \text{si } k = 1, \end{cases}$$

On a $\sigma \in \mathcal{S}_m$ et $p_j = u_j\ q_{\sigma(j)}$ d'où le résultat.

Corollaire 7.2.12. *Soit A un anneau factoriel et $a \in A$, $a \neq 0$.*
alors a est irréductible si et seulement si l'idéal $\langle a \rangle = aA$ est premier.

<u>Démonstration</u> :

Si $\langle a \rangle$ est premier alors a est irréductible.
Supposons a irréductible et soit $(b,c) \in A^2$ tel que $bc \in \langle a \rangle$. $bc \in \langle a \rangle$ entraîne que a divise bc, comme A est factoriel, a divise b ou a divise c, d'où $b \in \langle a \rangle$ ou $c \in \langle a \rangle$,, donc $\langle a \rangle$ est un idéal premier.

Remarque 7.2.13.

1. *Soit $a = u = u\prod_{i=1}^{n} p_i^{\alpha_i}$, $b = v\prod_{i=1}^{n} p_i^{\beta_i}$, l'élément a divise l'élément b si et seulement si $\alpha_i \leq \beta_i$*
2. *Soit A un anneau intègre, on définit sur A la relation d'équivalence suivante :*

$$\forall (a,b) \in A^2, \quad a\mathcal{R}b \Longleftrightarrow \exists u \in \mathcal{U}(A) \text{ tel que } b = ua.$$

   C'est à dire $a\mathcal{R}b$ si et seulement si a et b sont associés.

3. *Soit A un anneau factoriel et on considère la relation d'équivalence ci - dessus. Soit $\mathcal{P}$ un ensemble de représentants des irréductibles de A c'est -à-dire :*

   i) Si $p, q \in \mathcal{P}$, $p \neq q$ alors p et q ne sont pas associés

   ii) Chaque élément irréductible de A est associé à un unique élément de $\mathcal{P}$.

4. *Soit $a \in A$, $a \neq 0$, a s'écrit de manière unique sous la forme*

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \quad u \in \mathcal{U}(A),\ p_i \in \mathcal{P}, \quad \alpha_1, \cdots, \alpha_n \in \mathbb{N}, \quad \alpha_1 \geq 1.$$

   On dit que p_i divise a avec la multiplicité α_i, on notera $V_{p_i}(a) = \alpha_i$ et $V_{p_i}(a) = 0$ si p_i ne divise pas a.

Définition 7.2.14. *Soit A un anneau, a et b deux éléments non nuls de A. Un élément $d \in A$ est un plus grand diviseur commun de a et b si*

1. *d divise a et d divise / b.*
2. *$\forall x \in A$, si x divise a et x divise b alors x divise d. On note $d = \operatorname{pgcd}(a,b)$.*

Définition 7.2.15. *Soit A un anneau, a et b deux éléments non nuls de A. Un élément $m \in A$ est un plus petit multiple commun de a et b si*

1. *a divise m et b divise / m.*
2. *$\forall x \in A$, si a divise x et b divise x alors m divise x. On note $m = \operatorname{ppcm}(a,b)$.*

Proposition 7.2.16. *Soit A un anneau intègre, a et b deux éléments non nuls de A. Si d et d' (resp. m et m') sont deux* pgcd *(resp.* ppcm*) de a et b, alors il existe $u \in \mathcal{U}(A)$ (resp. $v \in \mathcal{U}(A)$ tel que $d' = ud$ (resp. $m' = vm$).*

<u>Démonstration</u> : $(a, b) \in A^2$ non nuls

Soient d et d' deux pgcd de a et b. Comme d pgcd de a et b et d' divise a et divise b, alors d' divise d, donc il existe $u' \in A$ tel que $d = u'd'$, de même, $\exists u \in A$ tel que $d' = ud$. Par conséquent, $d = u'd' = u'(ud) = uu'd$ ce qui implique $d(1 - uu') = 0$. Comme A est intègre et $d \neq 0$, on a $1 = uu'$, donc u et u' sont inversibles d'où, d' = ud,*donc*d et d' sont associés. On montre de la même manière que $m' = vm$.

Proposition 7.2.17. *Soit A un anneau factoriel, $a, b \in A$, $a \neq 0$, $b \neq 0$.*
Alors, a et b possèdent un pgcd, d et un ppcm, m, de plus

$$\exists u \in \mathcal{U}(A) \ \textit{tel que} \ ab = umd, \quad \textit{et} \ aA \cap bA = mA.$$

<u>Démonstration</u> :

Posons $a = u_1 = \prod_{i=1}^{n} p_i^{V_{p_i(a)}}$, $\qquad b = v_1 \prod_{i=1}^{n} p_i^{V_{p_i(b)}}$ où les p_i sont dans $\mathcal{P}$.

Posons $\gamma_i = min\Big(V_{p_i}(a), V_{p_i}(b)\Big)$ et d= $\prod_{i=1}^{n} p_i^{\gamma_i}$. Nous avons $\forall i \in \{1, .., n\}$, p_i divise a et b, donc d divise a et b. Soit $x = \omega \prod_{i=1}^{n} p_i^{t_i} \in A$ tel que x/a et x/b. Puisque x divise a et x divise b on a $t_i \leq \alpha_i$ et $t_i \leq \beta_i$, donc $t_i \leq min(\alpha_i, \beta_i)$, x divise d d'où $d = pgcd(a, b)$.

Posons $\delta_i = max(V_{p_i}(a), V_{p_i}(b))$ et $m = \prod_{i=1}^{n} p_i^{\delta_i}$. Les éléments a et b divisent m. Soit $y = u' \prod_{i=1}^{n} p_i^{\lambda_i}$ tel que a divise y et b divise y. Comme a divise y et b divise y on a $\alpha_i \leq \lambda_i$ et $\beta_i \leq \lambda_i$, on en déduit que $max(\alpha_i, \beta_i) \leq \lambda_i$, ainsi m divise y d'où $m = \text{ppcm}(a, b)$.
$u_1 v_1 md = u_1 v_1 \prod_{i=1}^{n} p_i^{max(\alpha_i, \beta_i) + min(\alpha_i, \beta_i)} = u_1 v_1 \prod_{i=1}^{n} p_i^{\alpha_i + \beta_i} = ab$
Comme a divise m et b divise m, on a $m \in aA \cap bA$, donc $mA \subset aA \cap bA$.
Soit $x \in aA \cap bA$ on a a divise x et b divise x, donc m divise x d'où $x \in mA$, ainsi $aA \cap bA \subset mA$. On en déduit que $aA \cap bA = mA$.

Exemple 7.2.18.

1. Si A est un anneau factoriel, $A[X]$ est factoriel
2. Si A est factoriel, $A[X_1, \cdots, X_n]$ est un anneau factoriel, en particulier si k est un corps $k[X_1, \cdots, X_n]$ est un anneau factoriel.

7.3 Anneaux Principaux

Définition 7.3.1. *Un anneau commutatif* A *est dit principal s'il est intègre et si tous ses idéaux sont principaux*

Définition 7.3.2. *Soit* A *un anneau et* I *un idéal de* A.
On dit que I *est un idéal principal s'il existe* $a \in A$ *tel que* $I = \langle a \rangle = aA$.

Exemple 7.3.3.

1. L'anneau $\mathbb{Z}$ est principal
2. L'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \Big\{a + ib \ /a, b \in \mathbb{Z}\Big\} \text{ est un anneau principal.}$$

Théorème 7.3.4. *Soit* k *est un corps, alors l'anneau des polynômes* $k[X]$ *est principal.*

Démonstration :

$k[X]$ est un anneau intègre, montrons que tout idéal de $k[X]$ est principal, l'idéal nul est principal. Soit I un idéal non nul de $k[X]$ et soit $\wedge = \Big\{\deg P /\ P \in I \setminus \{0\}\Big\}$ où $\deg P$ est le degré de P, l'ensemble $\wedge$ est une partie non vide de $\mathbb{N}$, donc admet un minimum d_o. Soit $P_o \in I \ / \deg P_o = d_o$, montrons que $I = \langle P_o \rangle$.
Comme

$P \in I$, on a $\langle P_o \rangle \subset I$ (1). La division euclidienne de P par P_0 donne
$P = P_oQ + R$ avec $\deg(R) < \deg(P_o)$. Comme $P \in I$, $P_o \in I$ on a $R = P - P_oQ \in I$. comme de plus $\deg(R) < \deg(P_o)$, on a $R = 0$ donc $P = P_oQ \in \langle P_o \rangle$ d'où $I \subset \langle P_o \rangle$ (2).
Les inclusions **(1)** et **(2)** entraînent que $I = \langle P_o \rangle$ est principal.
Réciproquement nous avons le résultat suivant :

Théorème 7.3.5. *Soit A un anneau alors $A[X]$ est un anneau principal si et seulement si A est un corps.*

Démonstration :

Si l'anneau A est un corps le théorème ci-dessus montre que $A[X]$ est un anneau principal. Réciproquement supposons que l'anneau $A[X]$ est principal. l'anneau $A[X]$ est intègre donc l'anneau A est intègre. Comme X est irréductible et l'anneau est principal, l'idéal $\langle X \rangle$ est maximal d'où l'anneau quotient $A[X]/\langle X \rangle$ est un corps, on en déduit que A est un corps puisqu'il est isomorphe à $A[X]/\langle X \rangle$.

Théorème 7.3.6. *Dans un anneau principal A , toute suite croissante d'idéaux est stationnaire.*

Démonstration :

Soit A un anneau principal, $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots \subset$ une suite croissante d'idéaux de A, $I = \bigcup_{i=1}^{\infty} I_n$ est un idéal de A. Comme A est principal, $\exists a \in A$ tel que $I = \langle a \rangle = aA$. De $a \in I = \bigcup_{i=1}^{\infty} I_n$ il résulte qu'il existe $q \in \mathbb{N}^*$ tel que $a \in I_q$, comme $I = \langle a \rangle$, on a $I \subset I_q$, or $I_q \subset I_n$ pour tout $n \geq q$, donc $\forall n \geq q$, on a $I_q \subseteq I_n \subseteq I \subsetneqq I_q$, d'où $I_n = I_q$ pour tout $n \geq q$. Ainsi la suite $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ est stationnaire.

Proposition 7.3.7. *Soit A un anneau principal et $p \in A$ un élément irréductible de A. Alors l'idéal $\langle p \rangle = pA$ est maximal.*

Démonstration :

Soit I un idéal de A tel que $pA = \langle p \rangle \subset I$. Comme A est principal, il existe $b \in A$ tel que / $I = bA$. Comme $p \in I$, $\exists a \in A$ tel que $p = ab$, l'Íément p étant irréductible, on a $a \in \mathcal{U}(A)$ ou $b \in \mathcal{U}(A)$, donc $I = A$ ou $I = pA$. On en déduit que l'idéal pA est maximal.

Théorème 7.3.8. *Dans un anneau principal A, tout idéal premier propre de A, et non nul est maximal*

Démonstration :

Soit $\mathfrak{p}$ un idéal premier non nul de A, $\mathfrak{p} = pA$ ou p est un élément premier de A, l'élément p est irréductible, donc $\mathfrak{p} = pA$ est maximal.

Théorème 7.3.9. *Tout anneau anneau principal A est factoriel.*

Démonstration :

Soit $x \in A$ un élément non nul et non inversible

1. Supposons que x n'est pas produit fini d'élément irréductibles de A. D'après le théorème de Krull l'idéal $\langle x \rangle$ est inclu dans un idéal maximal $\mathfrak{m}$ de A. Comme A est principal il existe un élément irréductible b_1 tel que $\mathfrak{m} = \langle b_1 \rangle$. L'idéal $\langle x \rangle$ est inclu dans $\langle b_1 \rangle$, donc il existe $a_1 \in A$ tel que $x = a_1 b_1$. Par hypothèse a_1 n'est pas produit fini d'élément irréductibles, de la même manière il existe $a_2 \in A$ et $b_2 \in A$ tel que $a_1 = a_2 b_2$. On fabrique ainsi une suite infinie $a_1, a_2, \cdots$, d'éléments de l'anneau A, cette suite engendre une suite strictement croissante $a_1 A \subsetneqq a_2 A \subsetneqq \cdots$ d'idéaux principaux de A ce qui contredit le théorm̀e ci dessus. On en déduit que x est produit déléments irréductibles.

2. Supposons que x admette deux décompositions en éléments irréductibles

$$x = up_1 p_2 \cdots p_m = vq_1 q_2 \cdots q_n.$$

Montrons par récurrence sur m que $m = n$ et il existe $\sigma \in \mathfrak{S}_n$ et $u_i \in \mathcal{U}(A)$ tel que $p_i = u_i q_{\sigma(i)}$. Comme p_1 divise $q_1 q_2 \cdots q_n$, on a $q_1 q_2 \cdots q_n \in \langle p_1 \rangle$, comme de plus l'idéal $\langle p_1 \rangle$ est premier, il existe $j \in \{1, .., n\}$ tel que $q_j \in \langle p_1 \rangle$, donc il existe $v_j \in A$ tel que $q_j = v_j p_1$. L'irréductibilité de q_j entraîne que $v_j \in \mathcal{U}(A)$, par simplification on a $p_2 \cdots p_m = u_j q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_n$. Par hypothèse de récurrence $m - 1 = n - 1$ et il existe $\gamma \in \mathfrak{S}_{n-1}$ tel que $p_i = u_i q_{\gamma(i)}$. Posons $\sigma : \{1, \cdots, \} \longrightarrow \{1, 2, \cdots, n\}$ définie par

$$\sigma(k) = \begin{cases} \gamma(k) & \text{si } k \neq 1 \\ j & \text{si } k = 1, \end{cases}$$

On a $\sigma \in \mathcal{S}_n$ et $p_j = u_j \; q_{\sigma(j)}$.

On déduit de 1) et 2) que A est un anneau factoriel.

7.4 Anneaux Euclidiens

Définition 7.4.1. *Un anneau A est dit euclidien s'il vérifie les propriétés suivantes :*

1. *L'anneau A est intègre.*
2. *L'anneau A est muni d'une division euclidienne $\varphi : A \backslash \{0\} \longrightarrow \mathbb{N}$ appelée stathme telle que si $(a, b) \in (A \setminus \{0\})^2$, il existe $(q, r) \in (A)^2$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.*

Exemple 7.4.2.

1. Soit k un corps l'anneau des polynômes $k[X]$ est euclidien avec
$$\begin{aligned} \varphi : k[X] \setminus \{0\} &\longrightarrow \mathbb{N} \\ P &\longrightarrow \varphi(P) = \deg(P). \end{aligned}$$
2. L'anneau $\mathbb{Z}$ est euclidien avec
$$\begin{aligned} \varphi : \mathbb{Z}^* &\longrightarrow \mathbb{N} \\ k &\longrightarrow \varphi(k) = |k|. \end{aligned}$$
3. L'anneau $\mathbb{Z}\left[\dfrac{1 + i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

Théorème 7.4.3. *Un anneau euclidien A est principal.*

<u>**Démonstration**</u> **:** Soit A un anneau euclidien, $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ le stathme associé et soit I un idéal non nul de A. L'ensemble $\Gamma = \{\varphi(t) \;\; / \;\; t \in I \setminus \{0\}$ est une partie non vide de $\mathbb{N}$ donc admet un minimum d. Soit $b \in I \setminus \{0\}$ tel que $\varphi(b) = d$, montrons que $I = \langle b \rangle$. Comme $b \in I$, on a $\langle b \rangle \subset I$. Soit $a \in I$, la division euclidienne de a par b donne $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$, comme $a \in I$ et $b \in I$, on a $r = a - bq \in I$ la minimalité de $\varphi(b)$ entraîne $r = 0$, d'où $a = bq \in \langle b \rangle$, ainsi $I \subset \langle b \rangle$. On en déduit que $I = \langle b \rangle$

Exercices

Exercice 1.

Soit $(A,+,\centerdot)$ un anneau unitaire non commutatif.

1. Soient a, b deux éléments de A tels que $ab+ba=1$ et $a^2b+ba^2=a$. Montrer que

$$a^2b-ba^2=0, \quad 2aba=a \ ; \ ab-ba=0 \text{ et } 2ba=1.$$

2. On suppose qu'il existe dans A deux éléments c et d tels que $c.d=1$ et $d.c\neq 1$.

Montrer que c et d sont des diviseurs de zéro dont on précisera le côté et un diviseur de zéro associé pour chacun d'eux

Exercice 2.

Soit A un anneau tel que tout élément de A soit idempotent c'est à dire $x^2=x$, $\forall x\in A$.

1. Montrer que si $x\in A$ alors $2x=0$ et que A est commutatif.
2. Montrer que $\forall x,y\in A$, $xy(x+y)=0$.
3. Montrer que si A est intègre alors $\text{card}(A)\leq 2$

Exercice 3.

Soit A un anneau non commutatif et non unitaire. On munit $\tilde{A}=\mathbb{Z}\times A$ les opérations suivantes :

$$(m,a)+(n,b)=(m+n,\ a+b), \quad \forall(m,n)\in\mathbb{Z}^2, \quad \forall(a,b)\in A^2$$

$$(m,a)\centerdot(n,b)=(mn,\ na+mb+ab).$$

1. Montrer que $(\tilde{A},+,\centerdot)$ est un anneau unitaire.
2. A quelle condition $\tilde{A}$ est commutatif.

Exercice 4.

Exercice 5.

Soit A un anneau commutatif et unitaire, on note $\sqrt{I}=\{x\in A|\exists n\in\mathbb{N}^*, x^n\in I\}$.

1. Monter que $\sqrt{I}$ est un idéal contenant I
2. Pour tout idéal I de A, on a $\sqrt{\sqrt{I}}=\sqrt{I}$.
3. Montrer que : $I\subset J\Rightarrow\sqrt{I}\subset\sqrt{J}$.
4. Montrer que $\sqrt{I}\cap\sqrt{J}=\sqrt{I\cap J}$.

5. Un idéal propre I de A est dit radical ou semi-premier si $\sqrt{I} = I$ et l'anneau A non nul est dit réduit si 0 est le seul élément nilpotent de A.
   Montrer que les conditions suivantes sont equivalentes :
   (a) L'idéal I est radical.
   (b) Si $x \in A$ et $x^2 \in I$ alors $x \in I$.
   (c) L'anneau quotient A/I est réduit.
6. Montrer qu'un idéal premier est radical.
7. Soit $\mathbb{Z}$ l'anneau des entiers relatifs et p un nombre premier. Déterminer l'idéal $\sqrt{p\mathbb{Z}}$
8. Soit $\alpha \in \mathbb{N}$, montrer que $\sqrt{p^\alpha \mathbb{Z}} = p\mathbb{Z}$.
9. Déterminer l'idéal $\sqrt{m\mathbb{Z}}$ avec $m \geq 2$ est un entier naturel.

Exercice 6.

Soit A un anneau et X une partie non vide de A. On pose

$$L(X) = \{r \in A/rx = 0, \forall x \in X\}$$

et

$$R(X) = \{r \in A/xr = 0, \forall x \in X\}.$$

1. Montrer que $L(X)$ est un idéal à gauche de A et que $R(X)$ est un idéal à droite de A.
2. Montrer que si X est un idéal à gauche alors $L(X)$ est un idéal bilatère.

Exercice 7.

Soit A un anneau commutatif et unitaire. Un élément $e \in A$ est appelé idempotent si $e^2 = e$. Soit $e \neq 1$ un idempotent.

1. Montrer que eA est un anneau unitaire.
2. Montrer que $1 - e$ est un idempotent.
3. Montrer que A est isomorphe à l'anneau produit $eA \times (1 - e)A$.
4. Généraliser cette décomposition, si $e_1, e_2, ..., e_n$ sont des idempotents tels que $\sum_{i=1}^n e_i = 1$

Exercice 8. *Théorème chinois.*

Soit A un anneau et $I_1, I_2, ..., I_n$ $(n \geq 2)$ des idéaux de A tels que $I_i + I_j = A$ si $i \neq j$ (on dit que I_1 et I_2 sont deux idéaux étrangers).

1. Montrer que pour tout n-uplet $(x_1, ..., x_n) \in A^n$, il existe $x \in A$ tel que $x = x_i[I_i]$ $1 \leq i \leq n$.

2. En déduire que
$$\frac{A}{\prod_{i=1}^{n} I_i} \simeq \prod_{i=1}^{n} \frac{A}{I_i}$$

Exercice 9. *Idéal Maximal dans un anneau.*

Soit A un anneau fini ou infini dénombrable.

1. Montrer que A possède idéal maximal.
2. En déduire que tout idéal propre de A est contenu dans un idéal maximal.

Exercice 10. *Anneau local*

Soit A un anneau commutatif. A est dit local s'il a un seul idéal maximal.

1. Montrer que A est local si et seulement si l'ensemble des éléments non-inversible forme un idéal.
2. Soit p un nombre premier, E_p l'ensemble des des rationnels de la forme $\frac{a}{b}$ avec $\gcd(b, p) = 1$.
   (a) Montrer E_p est sous anneau de $\mathbb{Q}$
   (b) Montrer que E_p est local.

Exercice 11.

Soient K un corps,a et b deux éléments de K.

1. Montrer que l'anneau quotient $\dfrac{K[X]}{\langle X-a\rangle}$ est isomorphe à K.
2. Montrer que l'anneau quotient $\dfrac{K[X,Y]}{\langle Y-b\rangle}$ est isomorphe à $K[X]$.
3. Montrer que l'anneau quotient $\dfrac{K[X,Y]}{\langle X-a, Y-b\rangle}$ est isomorphe à K.

Exercice 12.

Soient K un corps. On pose $A = \dfrac{K[X,Y]}{\langle X^2, XY, Y^2\rangle}$

1. Déterminer les éléments inversibles de A.
2. Déterminer tous les idéaux principaux de A.
3. Déterminer tous les idéaux de A.

Exercice 13.

Soit
$$\begin{array}{rccc} \varphi : & \mathbb{C}[X,Y] & \longrightarrow & \mathbb{C}[X] \\ & P(X,Y) & \longmapsto & P(X,X^2) \end{array}$$

1. Montrer que φ est un morphisme surjectif d'anneaux et que $\langle Y - X^2\rangle \subset \ker(\varphi)$.

2. Soit $P \in \ker(\varphi)$. En faisant la division euclidienne de P par $Y - X^2$ dans l'anneau $\mathbb{C}[X][Y]$ montrer que $P \in \langle Y - X^2 \rangle$.
3. Montrer que l'anneau quotient $A = \dfrac{\mathbb{C}[X,Y]}{\langle Y - X^2 \rangle}$ est principal.

Exercice 14. *L'anneau des entiers de Gauss*

On considère le sous-ensemble de $\mathbb{C}$ constitué des éléments de la forme $a+ib$ où $a, b \in \mathbb{Z}$.

1. Montrer que c'est un sous-anneau de $\mathbb{C}$.
   On l'appelle l'anneau des entiers de Gauss et on le note $\mathbb{Z}[i]$.
2. Montrer que $\mathbb{Z}[i]$ un anneau est principal.
3. Déterminer l'ensemble des éléments inversibles de cet anneau.
4. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien.

Exercice 15. *Construction de $\mathbb{C}$.*

Soit F un corps et d un éléments de F qui n'est pas carré parfait. Soit $E = F[X]/(X^2 - d)$ et $\eta = [X] \mod X^2 - d$.

1. Montrer que $E = \{a + b\eta \mid a, b \in F\}$.
2. Monter que l'anneau quotient E est un corps et donner l'inverse d'un élément $a+b\eta \in E$.
3. Monter l'application qui envoie $a + b\eta \in E$ à $a - b\eta$ est un automorphisme involutif de E.
4. montrer $\mathbb{Z}[i]$,$\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Q}(i)$ et $\mathbb{C}$ peuvent être construits de cette manière.
5. En remarquant que $2 \times 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, montrer que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Exercice 16. *Une Application de l'anneau des entiers de Gauss.*

On veut déterminer tous les nombres n pour lesquels l'équation $x^2+y^2 = n$ a des solutions entières .i.e $S = \{x^2 + y^2 | x, y \in \mathbb{Z}\}$.

1. (a) Quels sont les nombres premiers p tels que -1 est un carré dans $\mathbb{Z}_p$
   (b) En déduire que, si p est un nombre premier congru à 3 modulo 4 et n un élément non nul de S, alors la valuation $v_p(n)$(.i.e l'exposant de p dans la décomposition en facteurs premiers de n) est paire.
2. (a) Montrer qu'un nombre premier p est dans S si, et seulement si, il n'est pas irréductible dans $\mathbb{Z}[i]$.
   (b) En déduire qu'un nombre premier impair p est dans S si, et seulement si, il est congru à 1 modulo 4.

3. Montrer qu'un entier naturel n est dans S si, et seulement si, pour tout premier p congru à 3 modulo 4, la valuation $v_p(n)$ est paire.

Exercice 17. *L'équation de Pell-Fermat : le groupe des solutions.*

On veut étudier l'équation de Pell-Fermat $x^2 - 2y^2 = 1$ et déterminer ses solutions dans $\mathbb{Z}$.

1. On se place dans $\mathbb{Z}[\sqrt{2}]$
   (a) Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau et donner l'expression de ces éléments
   (b) Caractériser les éléments inversibles et remarquer qu'ils se répartissent sur une hyperbole.
2. On considère l'affixe $(3 + 2\sqrt{2}$ d'une solution particulière. Montrer que parmi les solution $a + b\sqrt{2}$, avec $a, b > 0$ c'est celle pour laquelle a est minimum, puis si on multiplie une solution $a + b\sqrt{2}$ par $3 - 2\sqrt{2}$ on obtient une solution $\alpha + \beta\sqrt{2}$ avec $\alpha > 0$ et $\alpha < a$. En déduire que toutes les solutions sont au signe près puissance de $3 + 2\sqrt{2}$
3. En déduire tous les entiers k pour lesquels $\frac{k(k+1)}{2}$ est un carré parfait.

Chapitre 8

Polynômes irréductibles

Définition 8.0.1.

Soit A un anneau, un polynôme $P \in A[X]$ est dit irréductible dans $A[X]$ si $P \in A$ est irréductible ou si :

1. $d^\circ P \geq 1$
2. *Les seuls diviseurs de P dans $A[X]$ sont les polynômes uP où $u \in \mathcal{U}(A)$ et les éléments de $\mathcal{U}(A)$.*

Théorème 8.0.2.

Soit K un corps et $\mathbb{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$. alors :

1. *Tout polynôme de degré 1 est irréductible dans $\mathbb{K}[X]$*
2. *Tout polynôme irréductible de degré > 1 n'a pas de racine dans $\mathbb{K}$.*
3. *Un polynôme de degré 2 ou 3 dans $\mathbb{K}[X]$ est irréductible si et seulement si il n 'a pas de racines dans $\mathbb{K}$.*

Démonstration :

1. Soit $P \in \mathbb{K}[X]$ de degré 1, si $P = QR$ alors $d^\circ P = 1 = deg(Q) + deg(R)$, donc $d^\circ Q = 0$ ou $d^\circ R = 0$, donc l'un des éléments R de Q est inversible. Ainsi les polynômes de degré 1 sont irréductibles.
2. Soit P un polynôme de degré > 1, si P a une racine x_o, alors P est divisible par $X - a$, donc est réductible.
3. Soit P un polynôme de degré 2 ou 3. Si P est irréductible, d'après 2)) P n'a pas de racine dans $\mathbb{K}$.
   Réciproquement soit P un polynôme de degré 2 ou 3. Si P est réductible, il existe

deux polynômes non constants Q et R tel que $P = QR$, on a

$$\begin{cases} deg\ Q \geq 1 \\ deg\ R \geq 1 \\ deg\ Q + deg\ R = deg\ P \leq 3 \end{cases} \Longrightarrow d°Q = 1 \text{ ou } d°Q = 1 \text{ ou } d°R = 1$$

donc P admet nécessairement un diviseur $\alpha X + \beta$ de degré 1 dans $\mathbb{K}[X]$, donc $-\beta/\alpha \in K$ est racine de P.

Remarque 8.0.3.

1. *$P(X) = (X^2 + 1)^2$ n'a pas de racines dans Q, mais est réductible dans Q.*
2. *Si k est un sous - corps de K, si $P \in k[X]$ alors $P \in K[X]$*

   Si P est irréductible dans $K[X]$ alors P est irréductible dans $k[X]$, mais la réciproque est fausse.

   $P(X) = X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais $P(X) = (X - i)(X + i)$ est irréductible dans $\mathbb{C}[X]$.
3. *Soit A un anneau factoriel, K son corps de fractions*

   Soit $P \in K[X] \backslash \{0\}$. $P(X) = \dfrac{a_o}{s_o} + \dfrac{a_1}{s_1}X + \cdots + \dfrac{a_n}{s_n}X^n$.

   Posons $a = ppcm(s_o, s_1, \cdots, s_n)$, le dénominateur commun $a \in A^*$, $aP(X) \in A[X]$, l'irréductibilité de $aP(X)$ dansn $A[X]$. L'étude d'irréductibilité dans $A[X]$ où A est un anneau factoriel se ramène à l'étude de l'irréductibilité dans $K[X]$ où K est le corps des fractions de A.

Proposition 8.0.4.

Soit $P(X) = a_o = a_1X + \cdots + a_n \in \mathbb{Z}[X]$ avec $a_o \neq 0$ et $a_n \neq 0$. Si $x_o = \dfrac{p}{q}$ (avec $pgcd(p, q) = 1$) est racine de $P(X)$ alors p divise a_o et q divise a_n.

Démonstration :

$P(x_o) = 0 \Longrightarrow a_o\dfrac{p}{q} + a_1\dfrac{p}{q} + \cdots + a_n\dfrac{p^n}{q^n}$

$\Longrightarrow q^n p(x_o) = a_o q^n + a_1 p q^{n-1} + \cdots + a_{n-1}\ p^{n-1} q \Longrightarrow p$ divise $a_o\ q^n$.

Comme p et q sont premiers entre eux, p divise a_o de même q divise $a_o q^n + a_1 p p^{n-1} + \cdots + a_{n-1}\ p^{n-1} q = -a_n p^n$.

Comme $pgcd(p, q) = 1$, q divise a_n.

Exercice 8.0.5.

1. Étudier l'irréductibilité de $P(X) = 2X^3 - 8X^2 - 9X - 5$ $a_o = -5$, $a_3 = 2$.

Soit $x_o = \dfrac{p}{q} \in Q$ avec $(p,q)=1$ une racine de P dans $\mathbb{Z}$. p divise 5 et q divise 2. Donc

$$x_o \in \left\{5,-5,1,-1,\frac{1}{2},-\frac{1}{2},\frac{5}{2},-\frac{5}{2}\right\}$$

2. Étudier l'irréductibilité de $P(X) = 30X^3 + 277X^2 - 31X - 28$ dans $Q[X]$.

Définition 8.0.6.

Soit A un anneau factoriel, $P(X) = a_o + a_1X, \cdots, a_nX^n$.
On appelle contenu de P et on note $C(P)$, le pgcd des coefficients de P, $C(P) = pgcd(a_o, a_1, \cdots, a_n)$.
Le pgcd étant pris sur les coefficients non nuls à un élément inversible près.

Définition 8.0.7.

Soit A un anneau factoriel et $P \in A[X]$. On dit que P est primitif si $C(P) = 1$ à un inversible près.

Lemme 8.0.8. *(Gauss)*

Soit A un anneau factoriel, alors

1. *Le produit de deux polynômes primitifs est primitif*
2. $\forall (P,Q) \in (A[X] \setminus \{0\})^2, \qquad C(PQ) = C(P)C(Q)$

Démonstration :

1. Soient P et Q deux éléments non nuls de $A[X]$ avec $C(P) = C(P) = 1$. On suppose $C(PQ) \neq 1$ il existe un élément irréductible $p \in A$ divisant tous les coefficients de PQ, comme p est irréductible et A factoriel.
   L'idéal $\langle P\rangle = pA$ est premier, donc l'anneau quotient $B = A/\langle p\rangle$ est intègre, d'où $B[X]$ est aussi intègre.
2. Soit $\pi : A \longrightarrow B = A/\langle p\rangle$ la surjection canonique et

$$\begin{aligned} \varphi : A[X] &\longrightarrow B[X] \\ f = \sum a_kX^k &\longrightarrow \varphi(f) = \sum \pi(a_k)X^k = \sum \overline{a}_kX^k \end{aligned}$$

   φ est un morphisme d'anneau.
   Comme p divise tous les coefficients de PQ, on a

$$0 = \varphi(PA) = \varphi(P)\ \varphi(Q), \quad \text{d'où} \quad \varphi(P) = 0 \quad \text{où} \quad \varphi(Q) = 0$$

   ce qui contredit $C(P) = C(Q) = 1$
3. $\exists R, S \in A[X]$ tel que $P = C(P)$ et $Q = C(Q)S$ avec $C(R) = C(S) = 1$, $PQ = C(P)\ C(Q)\ RS$, d'après 1°) $C(RS) = 1$ donc $C(PQ) = C(P)\ C(Q)$.

Théorème 8.0.9.

Soit A un anneau factoriel $K = Frac(A)$ son corps de fractions. Soit P un polynôme de degré ≥ 1 à coefficients dans A. Alors les conditions suivantes sont équivalentes :

1. *P est irréductible dans $A[X]$.*
2. *P est irréductible dans $K[X]$ et $C(P) = 1$ (P est primitif).*

Démonstration :

Soit $P \in A[X]$, $deg(P) \geq 1$

$1°) \Longrightarrow 2°)$. Supposons que P est irréductible dans $A[X]$.

Le contenu $C(P)$ divise P dans $A[X]$, comme P est irréductible dans $A[X]$, $C(P) \in \mathcal{U}(A)$, donc $C(P) = 1$.

En effet si $C(P) \neq 1$ (ou $C(P) \notin \mathcal{U}(A)$, $P = C(P)P_1$, $P_1 \in A[X]$ non inversible, ce qui contredit l'irréductibilité de P dans $A[X]$. Montrons que P est irréductible dans $K[X]$.

Supposons $P = QR$ ou Q et $R \in K[X]$ sont de degré ≥ 1.

Soit a un multiple commun à tous les dénominateurs des coefficients non nuls de Q et R, $a \in A^*$

$$a^2 P = (aQ)(aR) = UV \qquad (*) \quad \text{ou } U = aQ,\ V = aR$$
$$a^2 C(P) = C(a^2 P) = C(UV) = C(U)C(V).$$

Posons $U = C(U)U_1$ et $V = C(V)V_1$, avec U_1 et $V_1 \in A[X]$ et $C(V_1) = C(U_1) = 1$.

$(*) \Longrightarrow a^2 P = C(U)C(V)U_1V_1 = a^2\ C(P)U_1V_1$

$\Longrightarrow P = C(P)U_1V_1$ ce qui est absurde car $C(P)U_1$ et V_1 sont de degré ≥ 1 dans $A[X]$.

Ainsi P est irréductible dans $K[X]$.

$2°) \Longrightarrow 1°)$ Supposons P primitif et irréductible dans $K[X]$.

Si $P = QR$ avec $Q, R \in A[X]$ (donc $Q, R) \in K[X]$).

Comme P est irréductible dans $K[X]$, on a $deg(Q) = 0$ ou $deg(R) = 0$ c'est-à-dire $Q \in K^*$ ou $R \in K^*$.

- Si $Q \in K^*$ on a $Q \in A^*$, comme Q divise P, Q divise $C(P) = 1$ d'où $Q \in \mathcal{U}(A)$, de même $R \in K^* \Longrightarrow R \in \mathcal{U}(A)$.

Ainsi P est irréductible dans $A[X]$.

Théorème 8.0.10. *(Critère d'Einstein)*

Soit A un anneau factoriel, $K = Frac(A)$ le corps des fractions de A et $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ de degré $n \geq 1$.

Soit $p \in A$ un élément irréductible. On suppose

1. *p ne divise pas a_n*

2. p divise a_k $\forall k \in \{0,..,n-1\}$

3. p^2 ne divise pas a_o.

Alors $P(X)$ est irréductible dans $K[X]$.

Démonstration :

Posons $B = A/pA$ et $\begin{array}{c} \pi : A \longrightarrow B \\ a \longrightarrow \pi(a) = \overline{a} \end{array}$.

Si P n'est pas irréductible dans $K[X]$, $\exists U, V \in K[X]$ tel que $P = UV$, en raisonnant comme dans l'implication $1°) \Longrightarrow 2°)$ du théorème ci-dessus, on montre qu'il existe $Q, R \in A[X]$ tel que $P = QR$, $deg(Q) < deg(P)$ et $deg(R) < deg(P)$,
$Q(X) = \sum_{i=0}^{r} b_i\ X_i^i$, $R(X) = \sum_{j=0}^{s} c_j\ X^j$, $b_i, c_j \in A$ $1 \leq r \leq n-1$ et $1 \leq s \leq n-1$.

Notons que $a_k = \sum_{i=0}^{k} b_i\ c_{k-i}$.

On considère le morphisme d'anneaux

$$\begin{array}{ll} \varphi : A[X] & \longrightarrow B[X] \\ S = \sum \lambda_k X^k & \longrightarrow \varphi(S) = \sum \overline{\lambda}_k\ X^k = \overline{S} \end{array}$$

$\varphi(P) = \varphi(Q)\ \varphi(R) = \overline{Q}\ \overline{R}$. Comme a_k divise p $\mathcal{U} \in \{0,..,n-1\}$

$$\overline{p} = \overline{a}_n\ X^n = \left(\overline{b}_o + \cdots + \overline{b}_r\ X^r\right)\left(\overline{c}_o + \overline{c}_1\ X + \cdots + \overline{c}_s\ X^s\right) \quad (*).$$

Le terme de degré 0 de $(*)$ est nul, donc $\overline{b}_o\ \overline{c}_o = \overline{0}$ d'où $\overline{b}_o = \overline{0}$ ou $\overline{c}_o = \overline{0}$.
Notons que $\overline{b}_o$ et $\overline{c}_o$ ne sont pas simultanément nuls.
En effet si $\overline{b}_o = \overline{c}_o = \overline{0}$, alors p divise b_o et c_o, donc p^2 divise $a_o = b_o c_o$ ce qui est contraire aux hypothèses.

Supposons pour simplifier que $\overline{b}_o = \overline{0}$ et $\overline{c}_o \neq \overline{0}$.
Les $\overline{b}_i$ ne sont pas tous nul sinon $\overline{a}_n = \overline{b}_r \overline{c}_s = \overline{0}$.
Soit ℓ le plus petit des indices i tel que $\overline{b}_i \neq \overline{0}$ $(pX\ b_\ell)$. On a

$$\overline{b}_o = \cdots = \overline{b}_{\ell-1} = \overline{0} \text{ et } \overline{b}_\ell \neq \overline{0}, \qquad \ell \in \{0,..,r-1\}$$

$\overline{a}_\ell = \sum_{i=0}^{\ell} \overline{b}_i\ \overline{b}_{\ell-i} = \overline{b}_\ell\ \overline{c}_o \neq \overline{0}$ ce qui contredit le fait que p divise a_ℓ. On en déduit que P est irréductible dans $K[X]$.

Exemple 8.0.11.

1. Étudier l'irréductibilité dans $Q[X]$ de $P(X) = X^5 - 4X + 2$, on applique le critère d'Einstein dans $\mathbb{Z}[X]$ pour $p = 2$.

Si $P = QR$ avec $Q, R \in A[X]$ (donc $Q, R \in K[X]$).

Comme P est irréductible dans $K[X]$, on a $deg(Q) = 0$ ou $deg(R) = 0$ c'est à dire $Q \in K^*$.

- Si $Q \in K^*$, on a $Q \in A^*$. Comme Q divise P, Q divise $C(P) = 1$, d'où $Q \in \mathcal{U}(A)$, de même $R \in K^* \Longrightarrow R \in \mathcal{U}(A)$.

ainsi P est irréductible dans $A[X]$.

Théorème 8.0.12. *(Critère d'Einstein)*

Soit A un anneau factoriel, $K = Frac(A)$, le corps des fractions de A et $P(X) = \sum_{k=0}^{n} a_k\ X^k$ un polynôme de degré $n \geq 1$ à coefficients dans A. On suppose qu'il existe un élément $p \in A$ irréductible tel que p divise a_k, $\forall k \in \{0, .., n-1\}$, p ne divise pas a_n et p^2 ne divise pas a_o. Alors P est irréductible dans $K[X]$.

<u>**Démonstration :**</u>

$P(X) = \sum_{k=0}^{n} a_k\ X^k$, $p \in A$ irréductible tel que p divise a_k, $\forall k \in \{0, .., n-1\}$, p ne divise pas a_n et p^2 ne divise pas a_o. Soit $B = A/pA$ l'anneau quotient et

$$\begin{array}{l} \pi : A \longrightarrow B = A/pA \text{ la surjection canonique} \\ a \longrightarrow \pi(a) = \overline{a}, \quad \pi(a_k) = \overline{a}_k = 0 \quad \forall k \in \{0, .., n-1\}. \end{array}.$$

On suppose $P = QR$, $Q, R \in K[X]$ de degré ≥ 1

$\exists U, V \in A[X]$ tel que $P = UV$, $U, V \in A[X]$ de degré ≥ 1.

$U(X) = \sum_{k=0}^{r} b_i\ X^i$, $V(X) = \sum_{j=0}^{s} c_j\ X^j$ avec $b_r c_r = a_n \neq 0$ $r \geq 1$, $s \geq 1$, $r+s = n$,

on a $1 \leq r \leq\leq n-1$, $1 \leq s \leq n-1$.

On considère le morphisme d'anneaux

$$\begin{array}{c} \varphi : A[X] \longrightarrow B[X] \\ S(X) = \sum \lambda_k X^k \longrightarrow \varphi(S) = \sum \overline{\lambda}\ X^k \end{array}$$

$$\begin{aligned} \varphi(P) = \varphi(UV) &= \varphi(U)\ \varphi(V) \\ &= \left(\sum_{i=0}^{r} \overline{b}_i\ X^i\right)\left(\sum_{j=0}^{s} \overline{c}_j\ X^j\right) \qquad (*) \end{aligned}.$$

Comme $\overline{a}_k = 0$ $\forall k \in \{0, .., n-1\}$, on a $\varphi(p(X)) = \overline{a}_n\ X^n$ donc le terme de degré 0, de $(*)$ est nul, donc $\overline{b}_o \overline{c}_o = 0$, donc $\overline{b}_o = \overline{0}$ ou $\overline{c}_o = \overline{0}$ mais on a pas simultanément $\overline{b}_o = \overline{0}$ et $\overline{c}_o = \overline{0}$ sinon b_o et c_o seraient divisibles par p, donc $a_o = b_o c_o$ serait divisible par p^2.

- Supposons $\overline{b}_o = \overline{0}$ et $\overline{c}_o = \overline{0}$. Si $\overline{b}_i = 0$ $\forall i \in \{0, .., r-1\}$, on aurait $\overline{b}_r = \overline{0}$, donc $\overline{a}_n = \overline{b}_r\ \overline{c}_s = \overline{0}$ ce qui est contraire à p ne divise pas a_n. Soit ℓ le plus grand des entiers $i \in \{0,..,r-1\}$ tel que $\overline{b}_\ell = 0$, quitte à changer la numérotation, on peut supposer que $\overline{b}_o = \overline{b}_1 = \cdots = \overline{b}_\ell = \overline{0}$ et $\overline{b}_{\ell+1} \neq \overline{0}$

$$P = UV \Longrightarrow a_{\ell+1} = \sum b_k\ c_{\ell+1-k}$$

$\overline{a}_{\ell+1} = \sum_{k=0}^{\ell+1} \overline{b}_k\ c_{\ell+1-k} = \overline{b}_{\ell+1}\ \overline{c}_o \neq 0$ ce qui contredit $a_o = 2$, $a_1 = -4$ et $a_2 = 1$.
p divise a_o et a_1 ne divise pas $a_2 = 1$ et p^2 ne divise pas a_o, donc d'après Einstein $P(X)$ est irréductible dans $Q[X]$.
Comme $C(P) = 1$, $P(X)$ est irréductible dans $\mathbb{Z}[X]$

2. $P(X) = X^3 + 3X^2 - 6X + 3$ sur $Q[X]$ et $Z[X]$.

Définition 8.0.13.

Soit $p \in \mathbb{Z}$ un nombre premier, on appelle polynôme cyclotomique, le polynôme

$$\phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-2} + X^{p-1}.$$

Corollaire 8.0.14.

Pour tout nombre premier p, le polynôme cyclotomique ϕ_p est irréductible sur Q.

<u>**Démonstration :**</u> Il suffit de montrer que $\phi_p(X+1)$ est irréductible

$$\begin{aligned}
\phi_p(X+1) &= \frac{(X+1)p - 1}{X} = \frac{\sum_{k=0}^{p} C_p^k\ X^k - 1}{X} = \frac{\sum_{k=1}^{p} C_p^k\ X^k}{X} \\
\phi_p(X+1) &= \sum_{k=1}^{p} C_p^k\ X^k - 1 = \sum_{k=0}^{p} C_p^{i+1}\ X^i
\end{aligned}$$

$\forall i \in \{0,..,p-2\}$, p divise C_p^{i+1}, p^2 ne divise pas le terme constant $C_p' = p$, p ne divise pas le coefficient dominant $C_p^p = 1$, d'après Einstein $\phi_p(X+1)$ est irréductible sur Q, donc ϕ_p est irréductible sur Q.

Corollaire 8.0.15. *Soit $a \notin \{-1, 1\}$ un entier sans carrée, alors $\forall n \geq 2$, $X^n - a$ est irréductible sur Q.*

Exemple 8.0.16.

1. Étudier l'irréductibilité sur Q de $X^3 - 10$
2. $P(X) = X^3 + 3X^2 - 6X + 9$
3. $P(X) = X^4 + X^3 + X + 1 \in \mathbb{Z}[X]$, $P(X+1) = X^4 + 5X^3 + 10X^2 + 10X + 5$, $P = 5$.

Théorème 8.0.17. *(Réduction modulo p)*

Soit A un anneau factoriel et $K = Frac(A)$ le corps des fractions de A. Soit I un idéal premier de A et $B = A/I$, L le cors des fractions de B. On suppose $a_n \notin B$ avec

$$P(X) = \sum_{i=0}^{n} a_i X^i \in A[X] \quad et \quad \overline{P}(X) = \sum_{i=0}^{n} \overline{a}_i X^i$$

sa réduction modulo I. Si $\overline{P}(X)$ est irréductible sur $L[X]$ alors $P(X)$ est irréductible sur $K[X]$.

Démonstration :

Supposons que $P(X) = Q(X)\ R(X)$ dans $A[X]$,

$$P(X) = \sum_{k=0}^{n} a_k X^k, \quad Q(X) = \sum_{i=0}^{r} b_i X^i, \quad r \neq s = n$$

$R(X) = \sum_{j=0}^{s} c_j\ X^j\ , \quad b_i, c_j \in A, \quad 1 \leq r \leq n-1, \quad 1 \leq s \leq n-1$
$a_k = \sum_{i=0}^{k} b_i\ c_{k-i} \neq \overline{0} \Longrightarrow \overline{b}_r \neq 0$ et $\overline{c}_s \quad \overline{P} = \overline{Q}\ \overline{R}$
$\overline{a}_n = \overline{b}_r\ \overline{c}_s \neq \overline{0} \Longrightarrow \overline{b}_r \neq \overline{0}$ et $\overline{c}_s \neq \overline{0}$
$\Longrightarrow deg(\overline{Q}) = r$ et $deg(\overline{R}) = s$.
Comme $\overline{P}$ est irréductible dans $L[X]$, on a $deg(\overline{Q}) = r = 0$ ou $deg(\overline{R}) = s = 0$
$\Longrightarrow deg(Q) = 0$ ou $deg(R) = 0 \Longrightarrow P(X)$ est irréductible dans $K[X]$.

Exercice 8.0.18.

Étudier l'irréductibilité des polynômes suivants :

1. $P(X) = X^3 - 127X^2 + 3608X + 19 \in \mathbb{Z}[X]$
2. $P(X) = X^5 - 12X^3 + 36X - 12 \in \mathbb{Z}[X]$
3. $P(X) = 6X^3 + 10X^2 + 8X + 2 \in \mathbb{Q}[X]$
4. $P(X, Y) = X^3 + Y^3 + 1 \in \mathbb{C}[X, Y]$
5. $P(X, Y) = X^2 + Y^6 + 7Y^4 + XY^3 + 2X^2Y^2 + 5Y + X + 1 \in \mathbb{Q}[X, Y]$

Solution :

1. $A = \mathbb{Z}, \qquad I = 2\mathbb{Z}$, la réduction modulo 2
   $P(X) = X^3 - 127X^2 + 3608X + 19$
   $\overline{P}(X) = X^3 - X^2 + \overline{1}$ est irréductible dans $\mathbb{F}_2[X] = \mathbb{Z}/2[X]$
   donc $P(X)$ est irréductible dans $\mathbb{Q}[X], .$ Comme P est primitif, P est irréductible dans $\mathbb{Z}[X]$.
2. $P = 3$ et on utilise le critère d'Einstein

3. $P(X) = 2(3X^3 + 5X^2 + 4X + 1) = 2\mathbb{Q}[X]$
   $P(X) = 3X^3 + 5X^2 + 4X + 1$, $P(X)$ et $P_1(X)$ sont associés dans $\mathbb{Q}[X]$. Etudions l'irréductibilité de $P_1(X)$ par la réduction modulo 2, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

$$\overline{P}_1(X) = X^3 + X^2 + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$$

   est irréductible dans $\mathbb{Q}[X]$, comme P_1 est primitif, P_1 est irréductible dans $\mathbb{Z}[X]$.

4. $P(X,Y) = X^3 + Y^3 + 1 \in \mathbb{C}[X,Y] = \mathbb{C}[X]\ [Y]$
   $P(X,Y) = P(Y) = Y^3 + (X^3 <= 1)$, $P = X + 1$ est irréductible dans $\mathbb{C}[X]$ qui est factoriel, p divise $X^3 + 1$ mais p^2 ne divise pas 1, d'après Einstein $P(Y) = P(X,Y)$ est irréductible.

5. $P(X,Y) = (1 + 2Y^2)X^2 + (Y^3 + 1)X + Y^6 + 7Y^4 + 5Y + 1$
   $P(X,Y) = P(X) \in \mathbb{Q}[X,Y] = \mathbb{Q}[X]\ [Y]$
   $\mathbb{Q}[Y]$ est factoriel et $P(X)$ primitif ?
   Posons $d = C(P)$ le contenu de P
   d divise $1 + 2Y^2$, $Y^3 + 1$ et $Y^6 + 7Y^4 + 5Y + 1$.
   Comme $1 + 2Y^2$ est irréductible dans $\mathbb{Q}[Y]$, d est inversible ou d est associé à $1 + 2Y^2$. Supposons d associé à $1 + 2Y^2$, on a $1 + 2Y^2$ divise $Y^3 + 1$, ce qui est faux donc $d = 1$.
   $P = Y \in \mathbb{Q}[Y]$ est irréductible, on applique la réduction modulo p, à $P(X)$,
   $\overline{P} \in \mathbb{Q}[X,Y]/_{\langle Y \rangle} \simeq \mathbb{Q}[X]$

$$\overline{P}(X) = X^2 + X + 1 \in \mathbb{Q}[X,Y]/_{\langle Y \rangle} = \mathbb{Q}[X]$$

   est irréductible dans $\mathbb{Q}[X]$, donc $P(X,Y)$ est irréductible dans $\mathbb{Q}[X,Y]$.

Chapitre 9

Extensions de corps

9.1 Généralités sur les extensions

Définition 9.1.1.

Soit K *un corps. Une extension de* K *est la donnée d'un couple* (L, j) *où* L *est un corps et où* $j : K \longrightarrow L$ *est un morphisme de corps de* K *dans* L. *On note* L/K.

Remarque 9.1.2.

Comme un morphisme de corps $j : K \longrightarrow L$ *est injectif. On identifie* K *à* $j(K)$, *de sorte que* K *est considéré comme un sous - corps de* L.

Exemple 9.1.3.

1. Le corps des nombres complexes $\mathbb{C}$ est une extension de $\mathbb{R}$
2. $\mathbb{C}$ est une extension de $\mathbb{Q}$ et $\mathbb{R}$ est une extension de $\mathbb{Q}$.
3. Soit k un corps, $k(X)$ le corps des fractions de l'anneau des polynômes $k[X]$, $k(X)$ est une extension de k.
4. Soit k un corps, l'image $im\varphi$ du morphisme

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow k \\ n &\longrightarrow \varphi(n) = n\ 1_k \end{aligned} \quad \text{est un sous - anneau intègre de } k$$

$Im\varphi \simeq \mathbb{Z}/ker\ \varphi$.

— Si $Caract(k) = 0$, alors, $Im\varphi \simeq \mathbb{Z}$; on dira que k contient $\mathbb{Z}$ et donc k contient $\mathbb{Q}$. $\mathbb{Q}$ est le plus petit sous corps de k, on dit que $\mathbb{Q}$ est le sous - corps premier de k.

— Si K est de caractéristique p où p est premier, alors $Ker\varphi \simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, on dira que K contient $\mathbb{F}_p$.

$\mathbb{F}_p$ est le plus petit sous corps de K, $\mathbb{F}_p$ est le sous corps premier de K.

Tout corps est une extension de son sous - corps premier.

Définition 9.1.4.

Soit K un corps et L une extension de K
La dimension de L sur K et est noté, $dim_K\ L = [L : K]$.
Si $[L : K]$ est fini, on dira que L est une extension de degré fini de K, dans le cas contraire, on dira que L est une extension de degré infinie de K.

Exemple 9.1.5.

1. $[\mathbb{C} : \mathbb{R}] = 2$
2. $[\mathbb{R} : \mathbb{Q}] = +\infty$ car $\mathbb{Q}$ est dénombrable et $\mathbb{R}$ ne l'est pas.

Théorème 9.1.6. *(de la base télescopique)*

Soit $K \subset L \subset M$ des corps.
Si $S = \{a_i\ /\ i \in I\}$ est une base de L sur K, $S' = \{b_j\ /j \in J\}$ est une base de M sur L alors $S'' = \{a_i b_j\ /(i, j) \in I \times J\}$ est une base de M sur K.

Si les degrés sont finis, on a $[M : K] = [M : L][L : K]$.

<u>**Démonstration :**</u>

Soit $x \in M$, comme S' est une base de M sur L, x est combinaison dans L, c'est - à - dire qu'il existe $b_1, \cdots, b_n \in S'$

$$\ell_1, \cdots, \ell_n \in L\ /\ x = \sum_{k=1}^{n} \ell_k b_k.$$

$\forall k \in \{1, ..., n\}$, ℓ_k est combinaison linéaire finie d'éléments de S à coefficients dans K, il existe $a_1, \cdots, a_m \in S$,

$$d_t k, d_{2,k}, \cdots, d_{m,k} \in K \text{ tel que } \ell_k = \sum_{i=1}^{m} d_{i,k} a_i \text{ donc}$$

$$x = \sum_{k=1}^{n} \left(\sum_{i=1}^{m} d_{i,k} a_i \right) b_k = \sum_{k=1}^{n} \sum_{i=1}^{m} d_{i,k}\ a_i\ b_k$$

donc $S'' = \left\{ a_i b_j\ /\ (i, j) \in I \times J \right\}$ est une famille génératrice de M sur K. Montrons que S'' est libre.

Soit $\left\{ a_i b_k\ /a_i \in S,\ b_k \in S',\ \ 1 \leq i \leq m,\ \ 1 \leq i \leq n \right\}$ une famille finie de S'' et $d_{i,k}$ $(1 \leq i \leq m,\ \ 1 \leq i \leq n)$ des éléments de K tel que $\sum_{k=1}^{n} \sum_{i=1}^{m} d_{i,k}\ a_i b_k = 0$.

$\sum_{k=1}^{n} \left(\sum_{i=1}^{m} d_{i,k} \right) a_i = 0$ et de plus comme S est libre sur K, on a $d_{i,k} = 0$, $\forall i \{1, ..., m\}$.

Ainsi S'' est libre sur K. On en déduit que S'' est une base de M sur K.
De plus si I et J sont finies, on a $|I \times J| = |I|.|J|$ d'où

$$[M : K] = [L : K][M : L].$$

Corollaire 9.1.7.

Soit $K_o \subset K_1 \cdots \subset K_{n-1} \subset K_n$ *une suite finie croissante de sous corps d'un corps* K, $n \geq 2$. *Si* $\forall i \in \{0, ..., n-1\}$. *L'extension* K_{i+1}/K_i *est de degré fini alors*

$$[K_n : K_o] = [K_n, : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_o].$$

Démonstration :

Elle se fait par récurrence forte sur n.
Si $n = 2$, le résultat est vrai d'après le théorème ci - dessus.
Supposons $n > 2$ et le résultat vrai pour tout $m \in \{2, ..., n\}$
$[K_n : K_o] = [K_n : K_m] = [K_m : K_o]$. Par hypothèse de récurrence
$[K_n : K_m] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}]$
$[K_m : K_o] = [K_m : K_{m-1}][K_{m-1} : K_{m-2}]$
donc $[K_n : K_o] = [K_n : K_{n-1}][K_{m-1} : K_{m-2}] \cdots [K_{m+1} : K_m]$ et
$[K_m : K_o] = [K_m : K_{m-1}][K_{m-1} : K_{m-2}] \cdots\cdots\cdots [K_1 : K_o]$
donc $[K_n : K_o] = [K_n : K_{n-1}][K_{m-1} : K_{m-2}] \cdots\cdots [K_1 : K_o]$.

Définition 9.1.8.

On appelle tour d'extension une suite croissante pour l'inclusion
$K_o \subset K_1 \subset \cdots \subset K_n$.

Définition 9.1.9.

Soit L *une extension d'un corps* K, *on appelle corps intermédiaire de l'extension* L/K *ou sous extension de l'extension* L/K, *tout sous corps* H *de* L *tel que* $K \subset H \subset L$.

9.2 Extension obtenue par adjonction

Définition 9.2.1.

Soit L *une extension d'un corps* K *et* S *une partie de* L, *l'ensemble des sous corps de* L *qui contiennent* K *et* S *admet au sens de l'inclusion un plus petit élément ce plus petit élément est noté* $K(S)$ *et est appelé sous extension de* L/K *engendré par* S *ou* $R(S)$ *est l'extension de* K *obtenue par adjonction de* S *à* K.

Exemple 9.2.2.

Soit K un corps, $K(\phi) = K$.

Si K est un corps et $S \subset K$ alors $K(S) = K$, $\mathbb{R}(i) = \mathbb{C}$.

Remarque 9.2.3.

Soit K un corps, L une extension de K, $K[S]$ la $K[S]$ la K-algèbre engendré par S, $K(S)$ est le corps des fractions de l'anneau intègre $K[S]$.
Si $S \neq \phi$,
$f \in K(S) \Longleftrightarrow \exists s_1, \cdots, s_n \in S, \quad \exists g, h \in K[X_1, \cdots, X_n]$
tel que $f = \dfrac{g(s_1, \cdots, s_n)}{h(s_1, \cdots, s_n)}$ *avec* $h(s_1, \cdots, s_n) \neq 0$

Définition 9.2.4. *Une extension $> L$ d'un corps K est dite de type fini s'il existe une partie finie $S = \{a_1, \cdots, a_)\}$ de L tel que $L = K(S) = K(a_1, \cdots, a_n)$.*
On dit que l'extension L de K est simple ou monogène s'il existe $a \in L$ tel que $L = K(a)$, a est appelé élément primitif de L.

Théorème 9.2.5.

Soit L une extension d'un corps K et $a \in L$.
L'extension simple $K(a)$ est ou bien isomorphe au corps des fractions $K(X)$ de $K[X]$ ou bien à un corps de la forme $K[X]/\langle p(X)\rangle$ où $P(X)$ est un polynôme irréductible de $K[X]$.

<u>Démonstration :</u>

Soit $K[a]$ le plus petit sous - anneau de L contenant K et a, $K[a]$ est l'ensemble des éléments de la forme

$$\sum_{i=0}^{n} \lambda_i a^i \text{ où } n \in \mathbb{N},\ \lambda_o, \cdots, \lambda_n \in K.$$

On considère l'application

$$\begin{aligned} \varphi : K[X] \quad & \longrightarrow K[a] \\ P = \sum_{i=0}^{n} \lambda_i X^i \quad & \longrightarrow \varphi(P) = \sum_{i=0}^{n} \lambda a^i = P(a). \end{aligned}$$

φ est un morphisme surjectif, d'anneaux

a) Si φ est injectif c'est à dire si $\forall P \in K[X]$ non nul $P(a) \neq 0$, φ est un isomorphisme de $K[X]$ et $K(a)$ sont isomorphes.

b) Si φ n'est pas injectif, c'est à dire s'il existe $Q \in K[X]$, non nul tel que $\varphi(P) = P(a) = 0$.
$I = Ker\varphi$ est un idéal non nul de $K[X]$. Comme $K[X]$ est principal, I est principal, $\exists P_o \in K[X]$ tel que $I = \langle P_o\rangle$, comme $K[X]/I$ est isomorphe à l'anneau intègre $K[a]$, I est un idéal premier et P est irréductible. De plus comme I est un idéal maximal, donc $K[X]/\langle P_o\rangle$ et par conséquent $K[a]$ sont des corps, d'où $K[a] \simeq K[a] \simeq K[X]/I$.

Remarque 9.2.6.

1. *Il découle du Théorème ci - dessus que s'il existe un polynôme non nul* $P \in K[X]$ *tel que* $P(a) = 0$, *il existe un polynôme irréductible* $P_o(X) \in K[X]$ *tel que* $K_o(a) = 0$.
2. *Si* H *est un polynôme irréductible tel que* $H(a) = 0$, *alors* $Ker\varphi = \langle H \rangle$.
3. *Soit le morphisme*
$$\varphi : K[X] \longrightarrow K[a]$$
$$P \longrightarrow \varphi(\rho) = P(a)$$
on a $\varphi(X) = a$ *et* $\varphi(\lambda) = \lambda \quad \forall \lambda \in K$.
φ *est un morphisme de* K*-algèbres et de* K*-espaces vectoriels (application linéaire).*

Proposition 9.2.7.

Soit L *une extension de degré fini d'un corps* K, *alors* L *est de type fini sur* K.

Démonstration :

Soit L une extension de degré fini de K $n = [L : K] = dim_K(L)$ et $a_1, \cdots, a_n$ une base de L on a $K(a_1, \cdots, a_n) \subset L$ de plus $\forall x \in L$, $\exists \lambda_1, \cdots, \lambda_n \in K$ tel que

$$x = \sum_{i=1}^{n} \lambda_i a_i \in K(a_1), \cdots, a_n) \text{ donc } L = K(a_1, \cdots, a_n).$$

Remarque 9.2.8.

La réciproque de la proposition est fausse $K(X)$ *le corps des fractions de l'anneau* $K[X]$. $K(X)$ *est de type fini sur* K *mais n'est pas de degré fini sur* K. *Cependant si* L *est de type fini et algébrique sur* K *alors* L *est de degré fin sur* K.

9.3 Éléments algébriques - Extensions algébriques

9.3.1 Éléments algébriques

Définition 9.3.1.

Soit L *une extension d'un corps* K *et* $\alpha \in L$ *on dit que* α *est algébrique sur* K *s'il existe un polynôme* $P \in K[X]$ *non nul tel que* $P(\alpha) = 0$.
Si α *n'est pas algébrique sur* K, *on dit que* α *est transcendant sur* K.

Exemple 9.3.2.

1. Si K est un corps, tout élément de K est algébrique sur K
2. Tout élément de $\mathbb{C}$ est algébrique sur $\mathbb{R}$.
$\forall Z \in \mathbb{C}$, Z est racine du polynôme
$$P(X) = X^2 - 2reel(Z)X + |Z|^2$$

3. $\sqrt{2}$ est algébrique sur Q

4. $\alpha = \sqrt{2} + \sqrt{3}, \quad \alpha^2 = 5 + 2\sqrt{6}$

$$\begin{array}{l} (\alpha^2 - 5)^2 = 24 \Longrightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \\ P(\alpha) = 0 \qquad \text{ou} \qquad P(X) = X^4 - 10X^2 + 1. \end{array}$$

α est algébrique sur Q.

Remarque 9.3.3.

Soit L une extension d'un corps K, $\alpha \in L$

$$\begin{array}{ll} \varphi : K[X] \longrightarrow K[\alpha] & \textit{si } I = Ker\varphi = (0) \textit{ alors} \alpha \textit{ est trascendant sur } K \\ P \longrightarrow P(\alpha) & \alpha \textit{ est algébrique sur } K. \end{array}$$

Définition 9.3.4.

Soit L une extension d'un corps K.
Si $\alpha \in L$ est algébrique sur K, il existe un unique polynôme unitaire irréductible P tel que $P(\alpha) = 0$.
On dit que P est le polynôme minimal de α sur K. Le degré de α est le degré de P.

Théorème 9.3.5.

Soit L une extension d'un corps K, $\alpha \in L$. Les conditions suivantes sont équivalentes

1. *α est algébrique sur K*
2. *L'extension $K(\alpha)/K$ est de degré fini*
3. *$K(\alpha) = K[\alpha]$.*

Démonstration :

On considère le morphisme surjectif

$$\begin{array}{r} \varphi : K[X] \longrightarrow K[\alpha] \\ P \longrightarrow P(\alpha) \end{array}$$

$1°) \Longrightarrow 2°)$ Soit $\alpha \in L$ algébrique sur K et soit P le polynôme minimal de α et $n = deg(P)$.
D'après le théorème 2, il existe un isomorphisme $\overline{\varphi}$:

$$\begin{tikzcd} K[X] \arrow[r, "\varphi"] \arrow[d, "\pi"'] & K[\alpha] = K(\alpha) \\ K[X]/\langle P \rangle \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

Soit $\beta \in K(\alpha)$, $\exists H \in K[X]$ tel que $\beta = \overline{\varphi}(\pi(H)) = \varphi(H) = H(\alpha)$.
La division euclidienne de $H(X)$ par $P(X)$ donne

$$H(X) = P(X)\ Q(X) + R(X) \qquad \text{avec} \qquad d^\circ R < d^\circ P.$$

$$d^\circ R < d^\circ P \Longrightarrow R(X) = \sum_{i=0}^{n-1} \lambda_i\ X^i$$

$$\beta = H(\alpha) = P(\alpha)\ Q(\alpha) + R(\alpha) = R(\alpha) = \sum_{i=0}^{n-1} \lambda_i\ \alpha^i$$

donc la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est génératrice du K-espace vectoriel $K(\alpha)$. Il en résulte que $[K(\alpha) : K] = dim_K(K(\alpha)) \leq n$.
$2^\circ) \Longrightarrow 3^\circ)$ On suppose que $K(\alpha)/K$ est de degré fini.
Posons $m = [K(\alpha) : K]$, la famille $\{1, \alpha, \cdots, \alpha^m\}$ est une famille liée du K-espace vectoriel $K(\alpha)$ il existe $\lambda_o, \lambda_1, \cdots, \lambda_m \in K$ tel que $\sum_{i=0}^{m} \lambda_i\ \alpha^i = 0$. Posons $P(X) = \sum_{i=0}^{m} \lambda_i\ X^i \in K[X]$ est non nul vérifiant $P(\alpha) = 0$. D'après la remarque 3 du théorème 2, il existe $h(X) \in K[X]$, irréductible tel que $h(\alpha) = 0$ et $Ker\varphi = \langle h(X) \rangle$ où

$$\begin{aligned} \varphi : K[X] &\longrightarrow K[\alpha] \\ P &\longrightarrow \varphi(P) = P(\alpha), \quad \text{on a un isomorphisme} \end{aligned}$$

$K[X]/\langle h(X) \rangle \simeq K[\alpha]$. Comme $K[X]/\langle h(X) \rangle$ est un corps, $K[\alpha]$ est un corps et on a $K[\alpha] = K(\alpha)$ d'où $2^\circ) \Longrightarrow 3^\circ)$.

$3^\circ) \Longrightarrow 1^\circ)$ On suppose $K[\alpha] = K(\alpha)$

$$\alpha^{-1} \in K(\alpha) = K[\alpha] \Longrightarrow \exists g \in K[X]\ /\ \alpha^{-1} = \varphi(g) = g(\alpha) \text{ où}$$

$$\begin{aligned} \varphi : K[X] &\longrightarrow K[\alpha] \\ P &\longrightarrow \varphi(P) = P(\alpha) \end{aligned}$$

$$\alpha^{-1} = g(\alpha) \Longrightarrow 1 = \alpha g(\alpha) \Longrightarrow 1 - \alpha g(\alpha) = 0.$$

Posons $P(X) = 1 - Xg(X) \in K[X]$, on a $P(\alpha) = 0$ donc α est algébrique sur K.

Corollaire 9.3.6.

Soit L *une extension d'un corps* K, $\alpha \in L$ *un élément algébrique sur* K, m_α *son polynôme minimal, et* $n = dom_{\alpha,K}$. *Alors* $\{1, \alpha, \cdots, \alpha^{n-1}\}$ *est une base de* $K(\alpha)$ *sur* K *et* $[K(\alpha) : K] = n$.

Démonstration :

Soit $\alpha \in L$, algébrique sur K, $m_{\alpha,K}$ son polynôme minimal sur K et $n = d^\circ m_{\alpha,K}$ d'après la démonstration de $1^\circ) \Longrightarrow 2^\circ)$ du théorème 3, la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est génératrice du K-espace vectoriel $K(\alpha)$.

Soit $\lambda_o, \cdots, \lambda_{n-1} \in K$ tel que $\sum_{i=0}^{n-1} \lambda_i \ \alpha^i = 0$.

Posons "$P(X) = \sum_{i=0}^{n-1} \lambda_i \ X^i$, on a $P(\alpha) = 0$,

$$P \in Ker\varphi = \langle m_\alpha(X) \rangle, \text{ donc } \exists S \in K[X] \text{ tel que } P(X) = S(X) \ m_\alpha(X).$$

Comme $deg(m_\alpha(X)) = n$ et $deg(P(X)) \leq n-1$, le polynôme $P(X)$ est identiquement nul d'où $\lambda_o = \lambda_1 = \cdots = \lambda_{n-1} = 0$ donc la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est libre et par suite est une basse du K- ev $K(\alpha)$.
On en déduit que $[K(\alpha) : K] = n = deg(m_\alpha(X))$.

Exemple 9.3.7.

1. Déterminer $[Q[\sqrt{2}] : Q]$

$$\alpha = \sqrt{2} \Longrightarrow \alpha^2 - 2 = 0, \qquad P(X) = X^2 - 2.$$

$P(X)$ est irréductible, unitaire et $P(\alpha) = 0$, donc $P(X) = m_\alpha(X) = X^2 - 2$ est le polynôme minimal de $\sqrt{2}$ sur Q, d'où $[Q[\sqrt{2}] : Q] = 2$ et $\{1, \sqrt{2}\}$ est une base du Q-ev $Q[\sqrt{2}]$.

2. Déterminer $[Q[\sqrt{2}, \sqrt{2}] : Q[\sqrt[3]{2}, \sqrt{2}]]$,

$$[Q[\sqrt[3]{2}, \sqrt{2}] : Q(\sqrt{2})] \quad \text{et} \quad [Q(\sqrt[3]{2}, \sqrt{2}) : Q]$$

et une base de $Q(\sqrt[3]{2}, \sqrt{2}] : Q(\sqrt{2})$ sur Q.
On a

$$Q \subset Q[\sqrt[3]{2}] \subset Q[\sqrt[3]{2}, \sqrt{2}] \quad \text{et} \quad Q \subset Q[\sqrt{2}] \subset Q[\sqrt[3]{2}, \sqrt{2}]$$

$$\begin{aligned} \text{donc } \left[Q[\sqrt[3]{2}, \sqrt{2}] : Q\right] &= \left[Q[\sqrt[3]{2}, \sqrt{2}] : Q[\sqrt[3]{2}\right]\left[Q[\sqrt[3]{2}, \sqrt{2}] : Q\right] \\ &= \left[Q(\sqrt[3]{2}, \sqrt{2}) : Q(\sqrt{2})\right]\left[Q(\sqrt{2}) : Q\right] \end{aligned}$$

$[Q(\sqrt{2}) : Q] = 2$ et $\{1, \sqrt{2}\}$ est une base du Q-ev
$Q(\sqrt{2})$; $\left[Q(\sqrt[3]{2} : Q\right] = 3$ et $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$ est une base du Q-ev $Q(\sqrt[3]{2})$.
$Q[\sqrt[3]{2}, \sqrt{2}] = Q[\sqrt[3]{2}] \ [\sqrt{2}]$. Posons $\beta = \sqrt{2}$, $\beta \notin Q[\sqrt[3]{2}]$.
$\beta^2 - 2 = 0$, $P(X) = X^2 - 2 \in Q[\sqrt[3]{2}][X]$ est irréductible sur $Q[\sqrt[3]{2}]$, donc $m_\beta(X) = X^2 - 2$ est le polynôme minimal de β sur $Q[\sqrt[3]{2}]$, d'où

$$[Q[\sqrt[3]{2}, \sqrt{2}] : Q\sqrt[3]{2}] = 2. \text{ Ainsi}$$

$\{1, \sqrt{2}\}$ est une base du $Q[\sqrt[3]{2}]$ - ev $Q[\sqrt[3]{2}, \sqrt{2}]$.

Ainsi $[Q[\sqrt[3]{2}, \sqrt{2}] : Q] = 6$ et

$$\left\{1, \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{4}, 2^{2/6} \ , \ 2^{7/6}\right\}$$

est une base du Q - espace vectoriel $Q[\sqrt[3]{2}, \sqrt{2}]$.

3. Déterminer $[Q(\sqrt{3}, \sqrt{2}) : Q(\sqrt{3})]$; $[Q(\sqrt{3}, \sqrt{2}) : Q(\sqrt{2})]$ et $[Q(\sqrt{3}, \sqrt{2}) : Q]$.

   On a $Q \subset Q(\sqrt{3}) \subset Q(\sqrt{3}, \sqrt{2})$ et $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{3}, \sqrt{2})$

   donc $[Q(\sqrt{3}, \sqrt{2}) : Q] = [Q(\sqrt{3}, \sqrt{2}) : Q(\sqrt{3})][Q(\sqrt{3}) : Q]$
   $= [Q(\sqrt{3}, \sqrt{2}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q]$

   $Q(\sqrt{3}, \sqrt{2}) = Q(\sqrt{3})(\sqrt{2})$, $X^2 - 2$ est irréductible sur $Q(\sqrt{3})$ donc $X^2 - 2$ est le polynôme minimal de $\sqrt{2}$ sur $Q(\sqrt{3})$ donc $[Q(\sqrt{3}, \sqrt{2}) : Q(\sqrt{3})] = 2^{1,\sqrt{2}}$ de même $X^2 - 3$ est le polynôme minimal de $\sqrt{3}$ sur Q d'où $[Q(\sqrt{3}) : Q] = 2$, $\{1, \sqrt{3}\}$ base de $Q(\sqrt{3})$ sur Q.

   d'où $[Q(\sqrt{3}, \sqrt{2}) : Q] = 2 \times 2 = 4$ et $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une base de $Q(\sqrt{3}, \sqrt{2})$ sur Q.

Représentation matricielle

Soit L une extension de degré fini d'un corps K, $n = [L : K]$. Soit $\mathcal{A} = \{e_1, e_2, \cdots, e_n\}$ une base de L sur K, pour $\beta \in L$, on note

$$\begin{aligned} \eta_\beta : L &\longrightarrow L \\ x &\longrightarrow f_\beta(x) = \beta_x \end{aligned}$$

la multiplication par β.

Soit $M(\beta)$ la matrice de f_β relativement à la base $\mathcal{A}$, $M(\beta) \in M_n(K)$.

Lemme 9.3.8.

1. $\forall \beta \in K, \quad f_\beta = \beta.id_L$ *et* ${}_M(B) = \beta.I_n$
2. $\forall \alpha, \beta \in L, \quad f_\alpha + f_\beta = f_{\alpha+\beta}, \quad f_\alpha \circ f_\beta = f_{\alpha\beta}$

$$M(\alpha) + M(\beta) = M(\alpha\beta) \quad ; \quad M(\alpha\beta) = M(\alpha)\ M(\beta)$$

3. $(\forall \alpha, \beta \in L), \quad \alpha = \beta \Longleftrightarrow f_\alpha = f_\beta \Longleftrightarrow M(\alpha) = M(\beta)$.

Proposition 9.3.9.

Soit $\beta \in L$, *le polynôme caractéristique de* f_β, *ne dépend pas de la base* $\mathcal{A}$.

$$P_{f_\beta} = P_\beta(X) = det(-M(\beta) + XI_n) \quad et \quad P_\beta(\beta) = 0.$$

Si β *est algébrique sur* K, *le polynôme minimal de* β *sur* K *est le polynôme minimal de* f_β.

Exemple 9.3.10.

1. Comparer $Q(\sqrt{3}, \sqrt{2})$ et $Q(\sqrt{3}+\sqrt{2})$ puis déterminer le polynôme minimal de $\sqrt{2}+\sqrt{2}$ sur Q.
   On a $Q(\sqrt{3}+\sqrt{2}) \subset Q(\sqrt{3}, \sqrt{2})\alpha = \sqrt{3}+\sqrt{2}$, $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 1 \Longrightarrow$ $\sqrt{3}-\sqrt{2} = (\sqrt{3}+\sqrt{2})^{-1} \in Q(\sqrt{3}+\sqrt{2})$
   $\sqrt{3} = \frac{1}{2}(\sqrt{3}+\sqrt{2}) + \frac{1}{2}(\sqrt{3}-\sqrt{2})$ et $\sqrt{2} = \frac{1}{2}(\sqrt{3}+\sqrt{2}) - \frac{1}{2}(\sqrt{3}-\sqrt{2})$.
   donc $\sqrt{3} \in Q(\sqrt{3}+\sqrt{2})$ et $\sqrt{2} \in Q(\sqrt{3}-\sqrt{2})$, d'où $Q(\sqrt{3}, \sqrt{2}) \subset Q(\sqrt{3}+\sqrt{2})$ et par suite $Q(\sqrt{3}, \sqrt{2}) = Q(\sqrt{3}+\sqrt{2})$.
   Posons $\alpha = \sqrt{3}+\sqrt{2}$, déterminer la matrice de la multiplication par α relativement à la base $\mathcal{A} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ du Q- ev $Q(\sqrt{3}, \sqrt{2}) = Q((\sqrt{3}+\sqrt{2})$.

   $$f_\alpha(e_1) = \alpha \ , \quad f_\alpha(e_2) = \alpha e_2 = 2+\sqrt{6}, \quad f_a(e_3) = 3+\sqrt{6}$$
   $$f_\alpha(e_a) = 3\sqrt{2}+2\sqrt{3}$$

   $$M_{(\beta)} = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad P_M(X) = X^4 - 10X^2 + 1.$$

   Comme $[Q(\sqrt{3}+\sqrt{2}) : Q] = 4$, on a $m_\alpha(X) = X^4 - 10X^2 + 1$.

2. Déterminer le polynôme minimal de $1 + \sqrt[3]{2} + 3\sqrt[3]{4}$

   $$[Q(\sqrt[3]{2}) : Q] = 3 \quad \text{et} \quad \{1, \sqrt[3]{2}, \sqrt[3]{4}\} \text{ est une base du } Q - \textit{espace vectoriel}.$$

   Posons $\beta = 1 + \sqrt[3]{2} + 3\sqrt[3]{4}$. Déterminer la matrice de l'endomorphisme obtenu par multiplication de β.

   $$f_\beta(1) = \beta = 1 + \sqrt[3]{2} + 3\sqrt[3]{4}, \quad f_\beta(\sqrt[3]{2}) = \sqrt[3]{2} + \sqrt[3]{4} + 6 = 6 + \sqrt[3]{2} + \sqrt[3]{4}$$

   $$f_\beta(\sqrt[3]{4}) = \sqrt[3]{4}(1 + \sqrt[3]{2} + 3\sqrt[3]{4}) = \sqrt[3]{4} + 2 + 6\sqrt[3]{2} = 2 + 6\sqrt[3]{2} + \sqrt[3]{4}$$

   $$M = \begin{pmatrix} 1 & 6 & 2 \\ 1 & 1 & 6 \\ 3 & 1 & 1 \end{pmatrix}$$

   $$\begin{aligned} P_M(X) &= -X^3 + 3X^2 - \omega_2 X + d\acute{e}t\ M \\ &= -X^3 + 3X^2 - 15X + 93 \end{aligned}$$

   $\beta = 1 + \sqrt[3]{2} + 3\sqrt[3]{4} \notin Q$. Son polynôme minimal est de degré 3, donc le polynôme minimal de β est $m_\beta(X) = X^3 - 3X^2 + 15X - 93$.

9.3.2 Extensions algébriques

Définition 9.3.11.

Une extension L d'un corps K est dite algébrique sur K si tout élément de L est algébrique sur K.

Proposition 9.3.12.

Soit L une extension de degré fini d'un corps K. Alors L est algébrique sur K.

Démonstration :

On pose $n = [L : K]$ et soit $\alpha \in L$.
La famille $S = \{1, \alpha, \cdots, \alpha^n\}$ est une famille de $n+1$ vecteurs du K - espace vectoriel L. Comme $dim_K(L) = [L : K] = n$, S est liée, donc il existe $\lambda_o, \cdots, \lambda_n \in K$ tel que $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$. Posons $P(X) = \sum_{i=0}^{n-1} \lambda_i X^i$, on a $P(\alpha) = 0$ et α est algébrique sur K.

Remarque 9.3.13.

La réciproque de la proposition est fausse comme le montre l'exemple suivant :

Soit $i \in \mathbb{N}^*$, on pose $K_i = Q(2\sqrt[i]{2})$, le polynôme $P(X) = X^{2^i} - 2 \in Q[X]$ est irréductible et $P_i(\sqrt[2^i]{2}) = 0$.
P_i est le polynôme minimal de $2\sqrt[i]{2}$ sur Q, donc

$$[Q((\sqrt[2^i]{2}) : Q] = 2^i \qquad (*)$$

On a : $a : \left((\sqrt[2^i]{2})\right)^2 = (\sqrt[2^i]{2})$, donc $K_{i-1} \subseteq K_i$.
D'après $(*)$ $[K_i : Q] = 2^i$ et $[K_{i-1} : Q] = 2^{i-1}$, on a $Ki - 1 \subsetneqq K_i$.
Posons $K = \bigcup_{i \in \mathbb{N}^*} K_i$, K est une extension de Q. D'une part :

Soit $\alpha \in K$, $\exists i \in \mathbb{N}^* \ / \ \alpha \in K_i$. Comme $[K_i : Q]$ est fini, α est algébrique sur Q, donc K est une extension algébrique de Q.
D'autre part, $\forall n \in \mathbb{N}$, on a $n < 2^n = [K_n : Q] < [K : Q]$, donc l'extension K/Q n'est pas de degré fini.

Proposition 9.3.14.

Soit $L = K(\alpha_1, \cdots, \alpha_s$ une extension de type fini d'un corps K. Si les α_i sont algébriques sur K, alors L est de degré fini sur K.

Démonstration :

Posons $K_o = K$ et pour $1 \leq i \leq s$, $K_i = K(\alpha_1, \cdots, \alpha_i)$, on a la tour d'extension $K = K_o \subseteq K_1 \subseteq \cdots \subseteq K_s = L$. Pour $1 \leq i \leq d$, $K_i = K_{i-1}(\alpha_i)$ et α_i est algébrique sur K, donc est algébrique sur k_{i-1} donc $[K_i : K_{i-1}]$ est fin et $K_i = K_{i-1}[\alpha_i]$.
$[K_o : K] = \prod_{i=1}^{s} [K_i : K_{i-1}]$ est fini, donc L est de degré fini sur K.

Proposition 9.3.15.

Soit K une extension algébrique d'un corps k et L une extension algébrique de K. Alors L est une extension algébrique de k.

Démonstration :

Soit $\alpha \in L$. Comme L est algébrique sur K, il existe un polynôme non nul $g(X) = \sum_{i=0}^{n} b_i X^i$ à coefficients dans K tel que $g(\alpha) = 0$.
$g(X)$ est aussi à coefficients dans $k(b_o, \cdots, b_n) = K_n$ donc α est algébrique sur $K_n = k(b_o, \cdots, b_n)$.
Comme $b_i \in K$ et l'extension K/k est algébrique, les b_i sont algébriques sur k. D'après la proposition ci-dessu, K_n/k est de degré fini. Comme α est algébrique sur k_n, l'extension $K_n(\alpha)/K_n$ est de degré fini, d'où $K_n(\alpha)/k$ est de degré fini et α est algébrique sur k.

Lemme 9.3.16.

Soit L une extension d'un corps K. L'ensemble F des éléments de L qui sont algébriques sur K forme un sous corps de L.

Démonstration :

Notons d'aborde que 0 et 1 sont algébriques sur K. Soient $\alpha, \beta \in F$.
Soit $K[\alpha, \beta]$ le sous anneau de L engendré par α et β $K[\alpha, \beta], = K[\alpha]\ [\beta]$, β est algébrique sur K donc sur $K[\alpha]$, le théorème 3 entraîne que $K[\alpha]$ et $K[\alpha, \beta]$ sont des corps, la proposition 4 entraîne que $K[\alpha, \beta]$ est de degré fini sur K et donc algébrique sur K, $K[\alpha, \beta] = K(\alpha, \beta)$ or $\alpha - \beta$, $\alpha\beta$ et α^{-1} (si $\alpha \neq 0$) sont des éléments de $K(\alpha)(\beta) = K(\alpha, \beta)$, donc ils sont algébriques sur K.
Ainsi $\alpha - \beta, ;$ $\alpha\beta \in F$ et si $\alpha \neq 0$, $\alpha^{-1} \in F$. On en déduit que F est un sous corps de L.

Définition 9.3.17.

Le corps F est appelé clôture (Fermeture) algébrique de K dans L et on note $\mathcal{C}_L(K) = F$.

Exemple 9.3.18.

1. Si L/K est algébrique alors $\mathcal{C}_L(K) = L$.
2. $\mathcal{C}_K(K) = K$
3. $\mathcal{C}_{\mathbb{C}}(K) = \mathbb{C}$.

Définition 9.3.19.

La clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est appelé corps des nombres algébriques. Ce corps est noté souvent par $\overline{\mathbb{Q}}$.

Définition 9.3.20.

Soit L une extension d'un corps K. On dit que K est algébriquement clos dans L si $\mathcal{C}_L(K) = K$.

Exemple 9.3.21.

$\overline{\mathbb{Q}}$ est algébriquement clos dans $\mathbb{C}$.

Définition 9.3.22.

Un corps K est dite algébriquement clos s'il est algébriquement clos dans toute extension de K.
Le théorème suivant donne une caractérisation des corps algébriquement clos.

Théorème 9.3.23.

Soit K un corps, les conditions suivantes sont équivalentes

1. *K est algébriquement clos*
2. *Si L est une extension algébrique de K alors $L = K$*
3. *Tout polynôme non constant admet une racine dans K*
4. *Tout polynôme non constant de $K[X]$ s'écrit sous forme de produit de polynôme de degré 1*
5. *Les seuls polynômes irréductibles de $K[X]$ sont les polynômes de $K[X]$ de degré 1.*

<u>Démonstration :</u>

$1°) \Longrightarrow 3°)$ Soit $P \in K[X]$ un polynôme non constant et soit $Q(X)$ un facteur irréductible de $P(X)$, $\langle Q(X)\rangle$ un idéal maximal, donc l'anneau quotient $K[X]/\langle Q(X)\rangle$ est un corps et $K[X]/\langle Q(X)\rangle = K(\overline{X})$ où $\overline{X}$ est la classe de X modulo $\langle Q(X)\rangle$.
$K(\overline{X})$ est une extension algébrique de K.
Par hypothèse $K = K(\overline{X})$. Posons $\alpha = \overline{X}$ $\alpha \in K$, et on a $Q(\alpha) = Q(\overline{X}) = \overline{Q(X)} = 0$.
Comme $Q(X)$ est un facteur de $P(X)$, $\exists H(X) \in K(X)$ tel que $P(X) = Q(X)\ H(X)$.
$P(\alpha) = Q(\alpha)\ H(\alpha) = 0$, donc α est une racine de P dans K.

$3°) \Longrightarrow 4°)$ Soit P un polynôme non constant de $K[X]$, on raisonne par récurrence sur $n = deg(P)$. Si $n = 1$, $P(X) = a + b]$ avec $a \neq 0 \in K$, $b \in K$ le résultat est vérifié.
Supposons le résultat vérifie pour tout polynôme de degré $< n-1$ avec $n \geq 2$.

Soit α une racine de $P(X)$ dans K, $\exists Q_1(X) \in K[X]$ tel que $P(X) = (X-\alpha)\ Q_1(X)$ avec $deg(Q) = n-1$.
Par hypothèse de récurrence $Q_1(X) = \prod_{i=2}^{n}(a_iX + b_i)$ $a_i \in K\backslash\{0\}$ et $b_i \in K$, d'où
$P(X) = (X - \prod_{i=2}^{n}(a_iX + b)$ donc le résultat est vrai au rang n.

4°) $\Longrightarrow$ 5°) Soit $P(X)$ un polynôme non constant de degré $n > 1$. Par hypothèse $P(X)$ s'écrit sous la forme $\prod_{i=1}^{n}(a_iX + b_i)$, donc $P(X)$ n'est pas irréductible dans K. On en déduit que les seuls polynômes irréductibles de $K[X]$ sont les polynômes de degré 1.

5°) $\Longrightarrow$ 1°) Soit L une extension de K et $\alpha \in L$ un élément de L algébrique sur K. Le polynôme minimal $m_\alpha(X)$ étant irréductible, il est par hypothèse de la forme $X + a$ où $a \in K$

$$m_\alpha(\alpha) = 0 \Longrightarrow \alpha + a = 0 \Longrightarrow \alpha = -a \in K.$$

Il en découle que $\mathcal{C}_L(K) = K$, d'où K est algébriquement clos.

Exemple 9.3.24.

1. $\mathbb{C}$ est algébriquement clos
2. Un corps fini K n'est jamais algébriquement clos

$$K = \{a_1, \cdots, a_n\}, \quad P(X) = \prod_{i=i}^{n}(X - a_i) + 1 \text{ n'a pas de racines dans } K$$

Chapitre 10

Corps de rupture - Corps de décomposition

10.1 Corps de rupture

Définition 10.1.1.

Soit K un corps et $P \in K[X]$ un polynôme irréductible. Une extension $L \supset K$ de K est appelé corps de rupture de P sur K si $L = K(\alpha)$ est une extension simple (monogène) avec $P(\alpha) = 0$.

Exemple 10.1.2.

1. $K = Q$ et $P(X) = X^3 - 2$.
   $P(X) = 2\left(\left(\frac{X}{\sqrt{2}}\right)^3 - 1\right)$, les racines de $P(X)$ dans $\mathbb{C}$ sont $\rho = \sqrt[3]{2}$, ρj, ρj^2 où $j = e^{\frac{2i\pi}{3}}$.
   Le polynôme $P(X)$ a trois corps de rupture distincts dans $\mathbb{C}$, $Q(\rho), Q(\rho j)$ et $Q(\rho j^2)$
2. $P(X) = \dfrac{X^5 - 1}{X - 1}$. Posons $\omega = e^{\frac{2i\pi}{5}}$, les racines de P dans $\mathbb{C}$ sont $\omega, \omega^2, \omega^3, \omega^4$. $\forall p$, $\omega^p \in Q(\omega)$, les corps de rupture $Q(\omega), Q(\omega^2), Q(\omega^3)$ et $Q(\omega^4)$ sont égaux. P n'a qu'un seul corps de rupture dans $\mathbb{C}$.

Remarque 10.1.3.

Les exemples 1°) et 2°) montrent qu'il peut y avoir plusieurs corps de rupture d'un même polynôme irréductible de $K[X]$. Cependant le théorème suivant montre que ces corps de rupture sont isomorphes entre eux.

Théorème 10.1.4.

Soit K *un corps et* $P(X) \in K[X]$ *un polynôme irréductible. Alors il existe un corps de rupture* $K(\alpha)$ *de* $P(X)$ *sur* K *avec* $P(\alpha) = 0$. *Si* $K(\beta)$ *est un autre corps de rupture de* $P(X)$ *sur* K *tel que* $P(\beta) = 0$.
Alors il existe un isomorphisme de corps $f : K(\alpha) \longrightarrow K(\beta)$ *tel que*

$$f(\alpha) = \beta \quad et \quad f(\lambda) = \lambda \qquad \forall \lambda \in K.$$

Démonstration :

1. **Existence d'un corps de rupture**
   On considère l'anneau quotient $K[X]/\langle P(X)\rangle = K(\overline{X})$ est une extension simple de K, de plus $P(\overline{X}) = \overline{P(X)} = 0$. Posons $\alpha = \overline{X}$, $K(\alpha)$ est un corps de rupture de $P(X)$ et $K(\alpha) = K[X]/\langle P(X)\rangle$.

2. **Isomorphisme entre les corps de rupture**
   Soit $K(\beta)$ un autre corps de rupture de $P(X)$, $P(\beta) = 0$. β est algébrique sur K, donc $K(\beta) = K[\beta]$, on considère

$$\begin{aligned} \varphi : K[X] &\longrightarrow K[\beta] = K(\beta) \\ Q &\longrightarrow \varphi(Q) = Q(\beta) \end{aligned}$$

   φ est un morphisme surjectif, d'anneaux. Comme $P(\beta) = 0$, on a $P \in Ker\varphi$ et comme P est irréductible on a $Ker\varphi = \langle P(X)\rangle$ donc φ passe au quotient en un isomorphisme

$$\begin{aligned} f : K(\alpha) = K[X]/\langle P(X)\rangle &\longrightarrow K(\beta) \\ \overline{Q(X)} &\longrightarrow f(\overline{Q(X)} \; = \varphi(Q(X)) \\ & \qquad\qquad\quad = Q(\beta) \end{aligned}$$

   $f(\alpha) = f(\overline{X}) = \varphi(X) = \beta.$
   Si $\lambda \in K$, $\qquad f(\lambda) = \varphi(\lambda) = \lambda$

Remarque 10.1.5.

1. *D'après la démonstration ci - dessus* $P(\alpha) = 0$, P *irréductible sur* $K[X]$, *si* P *est unitaire,* P *est le polynôme minimal de* α *sur* K *donc* $[K(\alpha) : K] = deg(P)$, *et* $\{\overline{1}, \alpha, \cdots, \alpha^{deg(P)-1}\}$ *est une base de* $K(\alpha)$ *sur* K.
2. *La méthode de construction d'un corps de rupture est du à Cauchy et Kronecker. On l'appelle méthode "d'adjonction symbolique".*

Exemple 10.1.6.

1. Construction de $\mathbb{C}$, $P(X) = X^2 + 1$.
   $P(X) \in \mathbb{R}[X]$ est irréductible, $\mathbb{R}[X]/\langle X^2+1\rangle$ est un corps de rupture de $P(X) = X^2 + 1$.
   On note $\overline{X} = i$.
   $Q(X) \in \mathbb{R}[X]$, la division euclidienne de $Q(X)$ par $P(X) = X^2 + 1$, donne $Q(X) = (X^2+1)\ H(X) + R(X)$ avec $deg(R) \leq 1$, $R(X) = aX + bX$,
   $$\overline{Q(X)} = \overline{R(X)} = a\overline{X} + b\overline{X} = a^\circ ib, \quad (a,b) \in \mathbb{R}^2$$
   $P(i) = 0 \Longrightarrow i^2 = -1$, un élément $\overline{Q(X)}$ de $\mathbb{R}[X]/\langle X^2+1\rangle$ s'écrit de manière unique sous la forme $z = a + ib$.
   On a $\mathbb{R}[X]/\langle X^2+1\rangle = \mathbb{C}$ est un corps de rupture du polynôme $X^1 + 1$.
2. $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $P(X) = X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$, on considère la surjection canonique
   Posons $j = \pi(X) = \overline{X}$, $\mathbb{F}_2(j)$ est isomorphe à $\mathbb{F}_2[X]/\pi(X)$
   $$[\mathbb{F}_2(j) = deg(X^2 + X + 1) = 2, \qquad \mathbb{F}_2(j)$$
   est une base de $mathbbF_2(j)$ sur $\mathbb{F}_2$,
   $$\begin{aligned} \mathbb{F}_2(j) &= \left\{ a + b_j \ / \ (a,b) \in \mathbb{F}_2 \right\} \\ &= \left\{ \overline{0}, \overline{1}\}, j, j^2 \right\} \end{aligned}$$

10.2 Corps de décomposition

Définition 10.2.1.

Soit K un corps et $P(X) \in K[X]$ de degré $n \geq 1$. On appelle corps de décomposition de $P(X)$ une extension L de K contenant n racines de P et qui est minimal pour cette propriété.

Remarque 10.2.2.

Soit K un corps, $P(X) \in K[X]$ et L un corps de décomposition de $P(X)$ et $n = deg(< p)$.

Soient $\alpha_1, \cdots, \alpha_n$ les n racines de $P(X)$, chaque racine étant comptée un nombre α_r fois égal à sa multiplicité $K \subset K(\alpha_1, \cdots, \alpha_n) \subset L$, la minimalité de L entraîne que $L = K(\alpha_1, \cdots, \alpha_n)$.

Exemple 10.2.3.

1. Le corps de décomposition dans $\mathbb{C}$ de X^3-2 est

$$Q\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right) = Q\left(\sqrt[3]{2}, j\right) \ \omega = j = e^{i\frac{2\pi}{3}}$$

2. Le corps de décomposition de $\dfrac{X^5-1}{X-1}$ dans $\mathbb{C}$ est $Q\left(e^{i\frac{2\pi}{3}}\right)$.

3. $P(X) = X^2+17, \qquad X^2+7=0 \Longrightarrow 7\left(\left(\dfrac{X}{\sqrt{7}}\right)^2+1\right)=0$

$$t = \frac{X}{\sqrt{t}}\ , \quad t^2+1=0 \Longrightarrow t = \pm i \Longrightarrow X = \pm i\sqrt{7}.$$

   Le corps de décomposition de $P(X) = X^2+7$ dans $\mathbb{C}$ est $Q(i\sqrt{7})$.

4. $P(X) = X^4-7$, P est irréductible sur Q
   $P(X)=0 \Longrightarrow \left(\dfrac{X}{4\sqrt{t}}\right)^4 - 1 = 0, \quad t = \dfrac{X}{4\sqrt{t}}$
   $t^4-1=0 \Longrightarrow (t^2-1)(t^2+1)=0 \Longrightarrow t \in \{-1,1,i,-i\}$
   $X \in \left\{-\sqrt[4]{7}, \sqrt[4]{7}, -i\sqrt[4]{7}, i\sqrt[4]{7}\right\}$
   Le corps de décomposition de X^4-7 est donc

$$Q(-\sqrt[4]{7}, \sqrt[4]{7}, -i\sqrt[4]{7}, i\sqrt[4]{7}) = (\sqrt[4]{7}, i\sqrt[4]{7}) = Q(\sqrt[4]{7}, i).$$

Remarque 10.2.4.

Soit $\tau : K_1 \longrightarrow K_2$ *un isomorphisme de corps,* τ *induit une application*

$$\tilde{\tau} : K_1[X] \longrightarrow K_2[X]$$
$$h(X) = \sum_{i=0}^{n} a_i\ X^i \longrightarrow \tilde{\tau}(h(X)) = \sum_{i=0}^{n} \tilde{\tau}(a_i)\ X^i$$

1. $\tilde{\tau}$ *est un isomorphisme d'anneaux et* $\tilde{\tau}(a) = \tau(a) \quad \forall a \in K_1$.
2. *Si* $P(X)$ *est un polynôme irréductible dans* $K_1[X]$ *alors* $\tilde{\tau}(P(X)$ *est irréductible dans* $K_2[X]$
3. *Soit* $h(X) \in K_1[X]$, $\pi_1 : K_1[X] \longrightarrow K_1[X]/\langle h(X)\rangle$
   $\pi_2 : K_2[X] \longrightarrow K_2[X]/\langle \tilde{\tau}(h(X)\rangle$ *les surjections canoniques*

10.3 Corps de décomposition

Définition 10.3.1.

Soit K *un corps et* $P(X) \in K[X]$ *degré* $n \geq 1$. *On appelle corps de décomposition de* $P(X)$ *une extension* L *de* K *contenant n racines de* P *et qui est minimal pour cette propriété.*

Remarque 10.3.2.

Soit K *un corps,* $P(X) \in K[X]$ *et* L *un corps de décomposition de* $p(X)$ *et* $n = deg(P)$.
$\alpha_1, \cdots, \alpha_n$ *les* n *racines de* $P(X)$, *chaque racine étant comptée un nombre de fois égale à sa multiplicité* $K \subset K(\alpha_1, \cdots, \alpha_n) \subset L$, *la minimalité de* L *entraîne que* $L = K(\alpha_1, \cdots, \alpha_n)$.

Exemple 10.3.3.

1. Le corps de décomposition dans $\mathbb{C}$ de $X^3 - 2$ est $Q\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right) = Q(\sqrt[3]{2}, j)$ $\omega = j = e^{\dfrac{i2\pi}{3}}$.

2. Le corps de décomposition de $\dfrac{X^5-1}{X-1}$ dans $\mathbb{C}$ est $Q\left(e^{\dfrac{2i\pi}{5}}\right)$.

3. $P(X) = X^2 + 7$, $\qquad X^2 + 7 = 0 \Longrightarrow 7\left(\left(\dfrac{X}{\sqrt{7}}\right)^2 + 1\right) = 0$

$$t = \frac{X}{\sqrt{t}} \quad t^2 + 1 \Longrightarrow t = \pm i \Longrightarrow X = \pm i\sqrt{7}$$

Le corps de décomposition de $P(X) = X^2 + 7$ dans $\mathbb{C}$ est $Q(i\sqrt{7})$.

4. $P(X) = X^4 - 7$, P est irréductible sur Q
$P(X) = 0 \Longrightarrow \left(\dfrac{X}{\sqrt[4]{7}}\right)^4 - 1 = 0, \quad t = \dfrac{X}{\sqrt[4]{7}}$
$t^4 - 1 = 0 \Longrightarrow (t^2 - 1)(t^2 + 1) = 0 \Longrightarrow t \in \{-1, 1, i, -i\}$
$X \in \left\{-\sqrt[4]{7},\ \sqrt[4]{7},\ i\sqrt[4]{7},\ i\sqrt[4]{7}\right\}$
Le corps de décomposition de $X^4 - 7$ est donc

$$Q\left(-\sqrt[4]{7},\ \sqrt[4]{7},\ i\sqrt[4]{7},\ i\sqrt[4]{7}\right) = Q\left(\sqrt[4]{7},\ i\sqrt[4]{7}\right) = Q\left(\sqrt[4]{7}, i\right)$$

Remarque 10.3.4. *Soit* $\tau : K_1 \longrightarrow K_2$ *un isomorphisme de corps,* τ *induit une application*

$$\tilde{\tau} : K_1[X] \longrightarrow K_2[X]$$
$$h(X) = \sum_{i=0} a_i\ X^i \longrightarrow \tilde{\tau}(h(X)) = \sum_{i=0} \tau(a_i)\ X^i$$

1. $\tilde{\tau}$ *est un isomorphisme d'anneaux et* $\tilde{\tau}(a) = \tau(a) \quad \forall a \in K_1$

2. *Si* $P(X)$ *est un polynôme irréductible dans* $K_1[X]$ *alors* $\tilde{\tau}(P(X))$ *est irréductible dans* $K_2[X]$

3. *Soit* $h(X) \in K_1[X]$, $\quad \pi_1 : K_1[X] \longrightarrow K_1[X]/\langle h(X)\rangle$, $\pi_2 : K_2[X] \longrightarrow K_2[X]/\langle\tilde{\tau}(h(X))\rangle$ *les surjections canoniques.*

Lemme 10.3.5.

Soit $\tau : K_1 \longrightarrow K_2$ *un isomorphisme de corps,* $P_1(X)$ *un polynôme irréductible dans* $K_1[X]$*,* L_1 *un corps de rupture de* $P_1(X)$ *sur* K_1 *engendré par une racine* α_1 *de* $P(X)$*,* L_2 *un corps de rupture de* $P_2(X) = \tilde{\tau}(P_1(X))$ *sur* $\tilde{\tau} : K_1[X] \longrightarrow K_1[X]$ *est l'isomorphisme induit par* τ*. Alors il existe un isomorphisme de corps* $f : L_1 \longrightarrow L_2$ *tel que* $f(\alpha_1) = \alpha_2$ *et*
$\forall f(a) = \tau(a) \qquad \forall a \in K_1.$

<u>**Démonstration :**</u>

D'une part l'isomorphisme τ induit un isomorphisme $\tilde{\tau} : K_1[X] \longrightarrow K_2[X]$ qui passe au soutient en un isomorphisme $g : \dfrac{K_1[X]}{\langle P_1(X)\rangle} \longrightarrow \dfrac{K_2[X]}{\langle P_2(X)\rangle}$ rendant commutatif le diagramme suivant :

$$\begin{tikzcd}
K_1[X] \arrow[r, "\tilde{\tau}"] \arrow[d, "\pi_1"'] & K_2[X] \arrow[d, "\pi_2"] \\
\dfrac{K_1[X]}{\langle P_1(X)\rangle} \arrow[r, "g"'] & \dfrac{K_2[X]}{\langle P_2(X)\rangle}
\end{tikzcd}$$

π_1 et π_2 étant les surjections canoniques

D'autre part, le théorème d'adjonction symbolique montre qu'on a des isomorphismes.

$$\varphi_1 : \frac{K_1[X]}{\langle P_1(X)\rangle} \longrightarrow K_1(\alpha_1) = L_1 \quad \text{et}$$

$$\varphi_2 : \frac{K_2[X]}{\langle P_2(X)\rangle} \longrightarrow K_2(\alpha_2) = L_2 \quad \text{tel que}$$

$\varphi_1(\overline{X}) = \alpha_1$ et $\varphi_2(\overline{X}) = \alpha_2$, on pose $f = \varphi_2 \circ g \circ \varphi_1^{-1}$

$$\begin{tikzcd}
K_1[X] \arrow[r] \arrow[d, "\varphi_1"'] & K_2[X] \arrow[d, "\varphi_2"] \\
K_1(\alpha_1) \arrow[r, "f"'] & K_2(\alpha_2)
\end{tikzcd}$$

$$f(a) = \varphi_2 \circ g \circ \varphi_1^{-1}(a) = \varphi_2(g(a)) = \varphi_2(\tau(a)) = \tau(a)$$

$$f(\alpha_1) = \varphi_2 \circ g \circ \varphi_1^{-1}(\alpha_1) = \varphi_2(g(\overline{X})) = \varphi_2(\overline{X}) = \alpha_2$$

Lemme 10.3.6.

Soit $\tau : K_1 \longrightarrow K_2$ *un isomorphisme de corps,* $h(X) \in K_1[X]$ *un polynôme non constant.*
D_1 *un corps de décomposition de* $P_1(X)$ *sur* K_1 *et* D_2 *un corps de décomposition de* $P_2(X) = \tilde{\tau}(P_1(X)$ *sur* K_2 *où* $\tilde{\tau} : K_1[X] \longrightarrow K_2[X]$ *est l'isomorphisme induit par* τ. *Alors il existe un isomorphisme de corps* $f : D_1 \longrightarrow D_2$ *tel que* $f(a) = \tau(a), \quad \forall a \in K_1$.

Démonstration :

Elle se fait par récurrence sur $n = [D_1 : K_1]$.

Si $n = 1$, on a $D_1 = K_1$, les racines $\alpha_1, \cdots, \alpha_m$ de $P_1(X) = \lambda \prod_{i=1}^{m}(X - \tau(\alpha_i))$, donc les racines de $P_2(X)$ dans D_2 sont toutes dans K_2, d'où $D_2 = K_2$ et $f = \tau$.
Supposons $n > 1$ et la propriété vraie pour tout isomorphisme de corps $\sigma : K_1' \longrightarrow K_2'$, pour tout corps de décomposition D_1' d'un polynôme $P_1'(X) \in K_1'[X]$ sur K_1' et tout corps de décomposition de $\tilde{\sigma}(P_1'(X))$ sur K_2' tel que $[D_1' : K_1'] < n$.

Soit $Q_1(X)$ un facteur irréductible de $P_1(X)$ dans $K_1[X]$, n'ayant pas de racines dans K_1, soit α_1 une racine de $Q_1(X)$ dans D_1, β_1 une racine de $\tilde{\tau}(Q_1(X))$ dans D_2. D'après le lemme 1, il existe un isomorphisme de corps $\tau_1 : K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$ qui prolonge τ, $(\tau_1(a) = \tau(a) \quad \forall a \in K_1)$ et tel que $\tau_1(\alpha_1) = \beta_1$.

Soit

$$\begin{aligned} \tilde{\tau} : K_1(\alpha_1)[X] &\longrightarrow K_2(\beta_1)[X] \\ \sum a_i X^i &\longrightarrow \sum \tau(a_i)\ X^i. \end{aligned}$$

L'isomorphisme d'anneaux induit par τ_1

- Dans $K_1(\beta_1)[X]$, $P_2(X) = (X - \beta_1)\ h_2(X)$

$$\begin{aligned} P_2(X) &= \tilde{\tau}(P_1(X)) = \tilde{\tau}(P_1(X)) = \tilde{\tau}\Big[(X - \alpha_1)\ h_1(X)\Big] \\ &= (X - \tilde{\tau}_1(\alpha_1))\ \ \tilde{\tau}_1(h_1(X)) = (X - \beta_1)\ \ \tilde{\tau}_1(h_1(X)) \end{aligned}$$

donc $\quad h_2(X) = \tilde{\tau}_1(h_1(X))$.
D_1 est un corps de décomposition de $h_1(X)$ sur $K_1(\alpha_1)$, D_2 est un corps de décomposition de $h_2(X)$ sur $K_2(\beta_1)$, de plus la relation

$$n = [D_1 : K_1] = [D_1 : K_1(\alpha_1)]\ [K_1(\alpha_1) : K_1] \text{ entraîne}$$

$$[D_1 : K_1(\alpha_1)] < n \quad \text{car} \quad [K_1(\alpha) : K] > 1 \quad (\alpha_1 \notin K_1).$$

Par hypothèse de récurrence, il existe un isomorphisme de corps $f : D_1 \longrightarrow D_2$ prolongeant τ_1, comme τ_1 prolonge τ, f prolonge τ.

Théorème 10.3.7. *Soit* K *un corps. Tout polynôme* $P(X) \in K[X]$, *non constant admet sur* K *un corps de décomposition unique à isomorphisme près.*

Démonstration :

a) **Existence :**

Elle se fait par récurrence sur $n = d^\circ P$.

Si $n = 1$, P admet et/une racine dans K et K est un corps de décomposition de P. Supposons $n > 1$ et la propriété vraie pour tout polynôme non constant de degré strictement inférieur à n.

Soit $Q(X)$ un facteur irréductible de $P(X)$, α une racine de $Q(X)$ et $K(\alpha)$ un corps de rupture de $Q(X)$.

Dans $K(\alpha)K[X]$, $P(X) = (X - \alpha)\ g(X)$ avec $g(X) \in K(\alpha)K[X]$.

b) **Unicité :**

En appliquant le lemme 2 à $P(X)$ et à $i_k : K \longrightarrow K$ (identité) on obtient l'unicité à isomorphisme près.

Définition 10.3.8.

Soit K un corps, on appelle clôture algébrique de K, toute extension algébrique de K qui est algébriquement clos.

Théorème 10.3.9. *(Steimtz)*

Tout corps admet une clôture algébrique.

10.4 Corps finis

Théorème 10.4.1.

Soit K un corps fini. Alors K est de caractéristique p un nombre premier et $\exists n \in \mathbb{N}^*$ tel que $|K| = p^n$.

Démonstration :

Si K est un corps fini alors $Carc(K) = p$ est premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est le sous corps premier de K.

K est une extension de $\mathbb{F}_p$. Comme K est fini, K est un $\mathbb{F}_p$ - espace vectoriel de dimension finie. Posons $n = [K : \mathbb{F}_p] = dim_{\mathbb{F}_p}(K)$. K est isomorphe à $\mathbb{F}_p^n$, d'où $|K| = |\mathbb{F}_p|^n = p^n$.

Proposition 10.4.2. *Soit K un corps de caractéristique $p > 0$.*
L'application

$$f : K \longrightarrow K$$
$$x \longrightarrow f(x) = x^p$$

est un morphisme de corps, appelé morphisme de Frobenius.

<u>Démonstration :</u>

On considère

$$\begin{array}{l} f : K \longrightarrow K \\ x \longrightarrow f(x) = x^p \end{array}.$$

Soit $x, y \in K$, on a $f(x,y) = (xy)^p = x^p y^p = f(x)f(y)$

$$f(x+y) = (x+y)^p = \sum_{k=0}^{p} C_p^k \ x^{p-k} y^k = x^p + \sum_{k=0}^{p-1} C_p^k \ x^{p-k} y^k + y^p$$

or $\forall \ 1 \leq k \leq p-1$, p divise C_p^k, donc $\sum\limits_{k=0}^{p-1} C_p^k \ x^{p-k} y^k = 0$.

D'où $f(x+y) = x^p + y^p = f(x) + f(y)$, $f(1_K) = 1_K$.

Ainsi, f est un morphisme de corps, donc injectif. Si K est fini, f est un isomorphisme.

- Si $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, K^* est un groupe multiplicatif d'ordre $p-1$ et on a $x^{p-1} = 1$ $\forall x \in K^*$, d'où $x^p = x$. Ainsi $f = id_{\mathbb{F}_p}$.

Théorème 10.4.3. *Soit p un nombre premier et $n \in \mathbb{N}^*$, on pose $q = p^n$. Alors*

1. *Il existe un corps K à q éléments qui est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$*

2. *Deux corps finis à $q = p^n$ éléments sont isomorphes entre eux.*

<u>Démonstration :</u>

1. **<u>Existence</u> :** On considère le corps de décomposition du polynôme $f(X) = X^q - X$ sur $\mathbb{F}_p$ La dérivée de $f(X)$ est $f'(X) = qX^{q-1} - 1 = p^n \ X^{q-1} - 1 = -1$.
   $f'(X) \neq 0$, donc les racines de $f(X)$ sont distinctes f q racines distinctes $x_1, \cdots, x_q$.
   Montrons que $K = \{x_1, x_2, \cdots, x_q\}$ est un corps.
   $K \subset D_{\mathbb{F}_p}(f(X))$, il suffit de montrer que K est un sous corps de $D_{\mathbb{F}_p}(f)$ (corps de décomposition de $f(X) = X^q - X$), $1 \in K$.
   Soit $x, y \in K$, on a $x^q = x$ et $y^q = y$.

   $$\begin{array}{l} (x+y)^q = x^q + y^q = x + y \ \text{ et } \ (xy)^q = x^q \ y^q = xy \\ 0 = x + (-x) \Longrightarrow 0 = (x + (-x))^q = x^q + (-x)^q \Longrightarrow (-x)^q = -x^q = -x \end{array}.$$

   Donc K est un sous corps de $D_{\mathbb{F}_p}$.
   K est un corps et $|K| = q = p^n$.
   Montrons que $K = D_{\mathbb{F}_p}(f(X)) = \mathbb{F}_p(x_1, \cdots, x_q)$ pour cela il suffit de montrer que $\mathbb{F}_p \subset K$
   $-x \in \mathbb{F}_p \Longrightarrow x^p = x \Longrightarrow (x^p)^p = x^p = x$, c'est à dire $x^{p^2} = x$ et par récurrence sur n, on a $x^{p^n} = x$, d'où $\mathbb{F}_p \subset K$ et $K = \mathbb{F}_p(x_1, \cdots, x_q) = D_{\mathbb{F}_p}(X^q - X)$.

Montrons que $Caract(K) = P$.

Si $Caract(K) = p'$ avec p' premier. Soit $\mathbb{F}_{p'}$ est le sous corps premier de K, et $t = [K : \mathbb{F}_{p'}]$, $|K| = p^n = p^{ir}$.

Comme p et p' sont premiers, on a $p' = p$ et $n = r$.

2. **Unicité :**

Soit F un corps à $q = p^n$ éléments, on a $Caract(F) = p,$. Les éléments de F sont racines du polynôme $X^q - X \in \mathbb{F}_p[X]$. Or les racines de $X^q - X$ sont distinctes et par suite F coïncide avec le corps K des racines $X^q - X \in \mathbb{F}_p[X]$. L'unicité du corps de décomposition (à isomorphisme près) entraîne le résultat.

Notation : On note par $\mathbb{F}_p$ un corps à $q = p^n$ éléments.

Deux critères d'irréductibilité

Nous terminons ce chapitre par les deux critères d'irréductibilité suivants :

Théorème 10.4.4.

Soit K un corps, $P \in K[X]$ de degré $n > 0$.
Alors $P(X)$ est irréductible sur $K[X]$ si et seulement si $P(X)$ n'a pas de racines dans les extensions L de K e degré $[L : K] \leq \frac{n}{2}$.

Démonstration :

$\Longrightarrow$ On suppose P irréductible sur $K[X]$.
Soit L une extension de K. Si $\alpha \in L$ est une racine de $P(X)$, alors $K(\alpha)$ est un corps de rupture de P sur K, donc $[K(\alpha) : K] = n$ d'où $[L : K] \geq n$

$\Longleftarrow$ Réciproquement, procédons par contraposée en supposant que P n'est pas irréductible.

$$\exists (R, Q) \in (K[X])^2 \ / \ P = RQ \quad \text{avec} \quad deg(Q) \leq \frac{n}{2} \ \text{ où } \ deg(R) \leq \frac{n}{2}.$$

Sans perte de généralité, on peut supposer que $deg(Q) \leq \frac{n}{2}$. Soit Q' un facteur irréductible de Q, α une racine de Q' et $K(\alpha)$ un corps de rupture de Q' sur K, $Q'(\alpha) = 0 \Longrightarrow Q(\alpha) = 0 \Longrightarrow P(\alpha) = 0$, donc P admet une racine dans $K(\alpha)$ avec $[K(\alpha) : K] = deg(Q') \leq deg(Q) = \frac{n}{2}$.
D'où le résultat.

Exemple 10.4.5.

Étudier l'irréductibilité dans $\mathbb{Z}$ de $P(X) = x^4 = 8Xr + 17X - 1$.

Utilisons la réduction modulo 2.

Sur $\mathbb{F}_2[X]$, $\overline{P}(X) = X^4 + X + \overline{1}$, pour montrer que $\overline{P}$ est irréductible, il suffit de montrer que $\overline{P}$ n'a pas de racine sur une extension L de $\mathbb{F}_2$ de degré $\leq \dfrac{4}{2} = 2$ c'est-à-dire sur les extensions de degré 1 ou 2 de $\mathbb{F}_2$.

Si $[L : \mathbb{F}_2 = 1$ alors $L = \mathbb{F}_2$. Si $[L : \mathbb{F}_2] = 2$ alors $|L| = 2^2 - 4$, L est isomorphe à $\mathbb{F}_4 = \mathbb{F}_{2^2}$.

$\overline{P}$ n'a pas de racines dans $\mathbb{F}_2$.
Soit $x \in \mathbb{F}_4$, si $x \in \mathbb{F}_2$, x n'est pas racine de $\overline{P}$.

$x \in \mathbb{F}_4 \backslash \mathbb{F}_2 \quad x \neq 0 \ , \ x^4 - x = 0 \Longrightarrow x^4 = x$
$\Longrightarrow x^4 + x + T = \overline{2}x + \overline{1} = 1 \neq 0$, donc x n'est pas racine de $\overline{P}(X) = X^4 + X + \overline{1}$.
$\overline{P}$ n'a aucune racine dans une extension de $\mathbb{F}_2$ vérifiant $[K : \mathbb{F}_2] \leq \dfrac{n}{2}$, d'où $\overline{P}$ est une dualité dans $\mathbb{F}_2$ et par suite P est irréductible dans $\mathbb{Z}$.

Théorème 10.4.6.

Soit K un corps, $P \in K[X]$ un polynôme irréductible de degré n et L une extension de K de degré m. Si m et n sont premiers entre eux, alors P est irréductible sur L.

Démonstration :

Supposons $P = QR$, $Q, R \in K[X]$ avec ^{Q} irréductible de degré q avec $0 < q < n$.
Soit $M \simeq L[X]/\langle Q \rangle = K(\alpha)$ un corps de rupture de Q sur L.
On a :

$$[M : K] = [M : L][L : K] = qm \tag{10.1}$$

$$[M : K] = [M : K(\alpha)][K(\alpha) : K]$$

Comme $K(\alpha)$ est un corps de rupture de P sur K, on a

$$[K(\alpha) : K] = n \ \text{ et } \ [M : K] = rn \ \text{ avec } \ r = [M : K(\alpha)] \tag{10.2}$$

(1) et (2) $\Longrightarrow rn = qm \Longrightarrow n$ divise $qm,$. Comme $(m, n) = 1$, on a n divise q ce qui est absurde donc P est irréductible sur L.

Chapitre 11

Extensions Galoisiennes

11.1 Groupe de Galois d'une extension

Définition 11.1.1.

Soit L *et* M *deux extensions d'un corps* K. *On appelle* K*- morphisme de* L *dans* M, *tout morphisme de corps de* L *dans* M, $f : L \longrightarrow M$ *tel que* $f(\lambda) = \lambda \quad \forall \lambda \in K$. *Lorsque* $L = M$, *on dit que* f *est un* K *- endomorphisme de* L. *Si* f *est bijective, on dit que* f *est un* K*-isomorphisme.*

Remarque 11.1.2.

1. f *est un* K*-morphisme de* L *dans* K *si et seulement si* f *est un morphisme de* K*-algèbre*
2. *Un automorphisme de corps* K *est un morphisme bijectif, de* K *dans* K,. *L'ensemble* $Aut(K)$ *des automorphismes de* K *forme un groupe pour la loi* $\circ$ *de composition des applications,* $(Aut(K), \circ))$ *est un groupe.*

Définition 11.1.3.

Soit K *un corps et* L *une extension de* K.

On appelle K*-automorphisme de* L, *tout* K*-endomorphisme bijectif de* L.

Exemple 11.1.4.

1. $\mathbb{C}$ est une extension de degré 2 de $\mathbb{R}$

$$\sigma : \mathbb{C} \longrightarrow \mathbb{C}$$
$$x = a + ib \longrightarrow \sigma(x) = \overline{x} = a - ib \text{ est un } \mathbb{R} - \text{automorphisme}$$

2.

$$\sigma : Q(\sqrt{2}) \longrightarrow Q(\sqrt{2})$$
$$x = a + b\sqrt{2} \longrightarrow \sigma(x) = a - b\sqrt{2} = a - b\sqrt{2} \text{ est un } Q - automorphisme.$$

Définition 11.1.5.

Soit K *un corps et* L *une extension de* K.
L'ensemble des K*- automorphismes du corps* L *est un groupe pour loi* $\circ$ *de composition des applications. Ce groupe, est appelé groupe de Galois de l'extension* L/K *et se note* $Gal(L/K)$.

Démonstration :

$f(1) = 1$, donc $1 \in Fix(f)$.
Soit $(a, b) \in Fix(f)^2$, $f(a - b) = f(a) - f(b) = a - b$ donc

$$a - b \in Fix(f), \quad f(a, b) = f(a)\ f(b) = ab, \quad \text{donc} \quad ab \in Fix(f) \quad \forall x \in\in Fix(f),$$

avec $x \neq 0$, $f(x^{-1}) = [f(x)]^{-1} = x^{-1}$ donc $x^{-1} \in Fix(f)$. Ainsi $Fix(f)$ est un sous - corps de K.

Proposition 11.1.6.

Soit K *un corps de sous - corps premier* P. *Alors* $Aut(K) = Gal(K/P)$.

Démonstration :

On a $Gal(K/P) \subset Aut(K)$.
Réciproquement soit $f \in Aut(K)$, d'après le lemme ci - dessus $Fix(f)$ est un sous - corps de K. Comme P est le plus sous - corps de K, on a $P \subset Fix(f)$, c'est à dire $\forall x \in P$, $f(x) = x$, d'où $f \in Gal(K/P)$ et $Aut(K) \subset Gal(K/P)$.

Exemple 11.1.7.

$Aut(\mathbb{R}) = Gal(\mathbb{R}/Q) = \{id_{\mathbb{R}}\}$.
Comme Q est le sous - corps premier de $\mathbb{R}$, on a $Aut(\mathbb{R}) = Gal(\mathbb{R}/Q)$, montrons que $Gal(Q) = \{id_{\mathbb{R}}\}$.
Soit $f \in Gal(\mathbb{R}/Q)$, f est Q-automorphisme de $\mathbb{R}$

$$\forall x > 0, \quad f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 > 0 \quad x \neq 0, \quad f \text{ injectif}$$

donc $x > 0 \Longrightarrow f(x) > 0$. Montrons que f est strictement croissante. Soient a et $b \in \mathbb{R}\ /a < b$

$$b > a \Longrightarrow f(b) - f(a) = f(b - a) > 0.$$

Soit $x \in \mathbb{R}$ si $x \in Q$, on a $f(x) = x$.
Soit $x \in \mathbb{R} \backslash Q$, si $f(x) < x$, $\exists r \in Q/\ f(x) < r < x \Longrightarrow f(f(x)) < f(r) < f(x)$

$$\Longrightarrow r < f(x)$$

Donc $f(x) < r$ et $r < f(x)$ absurde.
Si $x < f(x)$, $\exists r_1 \in Q\ /\ x < r_1 < f(x)$

$x < r_1 < f(x) \Longrightarrow f(x) < f(r_1) < f(f(x)) \Longrightarrow f(x) < r_1$
donc $r_1 < f(x) < r_1$, absurde, d'où $\forall x \in \mathbb{R}\backslash Q \ f(x) = x$ et comme f est un Q-automorphisme, on a $f = id_{\mathbb{R}}$.

Lemme 11.1.8. *(Lemme de Dedekind)*

Soient G un groupe, K un corps. Soit $(\sigma_i)_{i\in\{1,\dots,m\}}$ une famille de morphismes de groupes de G dans K^* tous distincts. Alors la famille $(\sigma_i)_{1\le i\le m}$ est libre sur K (c'est-à-dire si $(\lambda_i)_{1\le i\le m} \in K^m$. vérifie $\forall g \in G, \ \sum_{i=1}^{m}\lambda_i \ \sigma_i(g) = 0$ alors $\lambda_i = 0 \quad \forall i$.

<u>**Démonstration**</u> **:**

Elle se fait par récurrence sur m.

Si $m = 1$, $\lambda_1\sigma_1(g) = 0 \quad \forall g \in G \Longrightarrow \lambda_1\sigma_1(e) = 0$

e étant l'élément neutre de G alors $\lambda_1\sigma_1(e) = 0 \Longrightarrow \lambda_1 = 0$.

Supposons la propriété vraie à l'ordre $m-1$.

Soit $(\lambda_1, \cdots, \lambda_m) \in K^m$ tel que $\sum_{i=1}^{m}\lambda_i \ \sigma_i(g) = 0 \ \ \forall g \in G$.

Si l'un des λ_i est nul alors par hypothese de récurrence tous les autres sont nuls.

$$\forall (x, y) \in G^2, \ \sum_{i=1}^{m}\lambda_i \ \sigma_i(xy) = 0 \Longrightarrow \sum_{i=1}^{m}\lambda_i \ \sigma_i(x) \ \sigma_i(y) = 0$$

Donc $\sum_{i=1}^{m}\lambda_i \ \sigma_i(x) \ \sigma_i(y) = 0 \qquad \forall (x, y) \in G^2$

$$\Longrightarrow \sum_{i=1}^{m-1}\lambda_i \ \sigma_i(x) \ \sigma_i(y) + \lambda_m \ \sigma_m(x) \ \sigma_m(y) = 0 \tag{11.1}$$

D'autre part $\sum_{i=1}^{m}\lambda_i \ \sigma_i(x) = 0 \Longrightarrow \sigma_m(y)\sum_{i=1}^{m}\lambda_i \ \sigma_i(x) = 0$

$$\Longrightarrow \sum_{i=1}^{m-1}\lambda_i \ \sigma_i(x) \ \sigma_m(y) + \lambda_m \ \sigma_m(x) \ \sigma_m(y) = 0 \tag{11.2}$$

$(1) - (2) \Longrightarrow \sum_{i=1}^{m}\lambda_i \ \sigma_i(x)(\sigma_i(y) - \sigma_m(y)) = 0 \Longrightarrow \sum_{i=1}^{m-1}\lambda_i(\sigma_i(y) - \sigma_m(y)) \ \sigma_i(x) = 0.$

Par hypothèse de récurrence $\lambda_i(\sigma_i(y) - \sigma_m(y)) = 0 \quad \forall i \in \{1, ..., m-1\}$

Comme $\sigma_i \neq \sigma_m$, on a $\lambda_i = 0$. Ainsi

$$0 = \sum_{i=1}^{m}\lambda_i \ \sigma_i(g) = \sum_{i=1}^{m-1}\lambda_i \ \sigma_i(g) + \lambda_m \ \sigma_m(g) = \lambda_m \ \sigma_m(g) \Longrightarrow \lambda_m = 0.$$

La famille $(\sigma_i)_{1\le i\le m}$ est donc libre.

Théorème 11.1.9.

Soit K un corps et L une extension de K de degré fini. Alors $Gal(L/K)| \le [L : K]$.

Démonstration :

Posons $n = [L : K]$ et raisonnons par l'absurde en supposons que $|Gal(L/K)| > n$. Il existe $n + 1$, K-automorphismes distincts $\sigma_1, \sigma_2, \cdots, \sigma_{n+1}$ de L.

Soit $\{e_1, \cdots, e_n\}$ une base du K-ev L, on considère la matrice $M = (\sigma_j(e_i))_{\substack{1\leq i\leq n\\ 1\leq j\leq n+1}} \in M_{n,n+1}(L)$.

Comme $dim_L(L^n) = n$, les vecteurs colonnes $c_1, \cdots, c_{n+1}$ sont linéairement dépendants alors $\exists(\lambda_1, \cdots, \lambda_{n+1}) \in L^{n+1} \setminus\{0\}$ tel que $\sum_{j=1}^{n+1} \lambda_j c_j = 0$

$c_j =^t (\sigma_j(e_1), \sigma_j(e_2), \cdots, \sigma_j(e_n))$. Donc on a $\sum_{j=1}^{n+1} \lambda_j\ \sigma_j(e_i) = 0 \qquad \forall i \in \{1, .., n\}$.

Posons $\sigma = \sum_{j=1}^{n+1} \lambda_j\ \sigma_j$, σ est un K-endomorphisme de L, nul sur la base $\{e_1, \cdots, e_n\}$, donc $\sigma = 0$ la famille $\{\sigma_j\}_{1\leq\leq j\leq n+1}$ est liée ce qui contredit le lemme de Dedekind. On en déduit que $|Gal(L/F)| \leq [L : K]$.

Définition 11.1.10.

Soit K un corps. On appelle extension Galoisienne finie de K, toute extension L de K de degré fini vérifiant $|Gal(L/K)| = [L : K]$.

Exemple 11.1.11.

1. Tout corps K est une extension galoisienne fini de lui - même
2. $\mathbb{R}$ n'est pas une extension galoisienne de Q.

Définition 11.1.12.

Soit K un corps et H une partie non vide de l'ensemble des endomorphismes de corps K.

$Fix(H) = \{x \in K\ / f(x) = x\}$ st un sous - corps de K appelé corps fixe de H.

Définition 11.1.13.

Soit K un corps et L une extension de K.

L'ensemble $F = \Big\{x \in L\ /\ \sigma(x) = x\} \quad \forall\sigma \in Gal(L/K)\Big\}$ est un sous - corps de L, appelé corps fixe de $Gal(L/K)$.

Notons que $K \subset F \subset L$.

Lemme 11.1.14.

Soit K un corps et L une extension de K. On a $Gal(L/K) = Gal(L/F)$.

Démonstration :

Soit $\sigma \in Gal(L/F)$.

Comme $K \subset F$, on a $\sigma(a) = a$, $\forall a \in K$. Donc $\sigma \in Gal(L/K)$, d'où $Gal(L/F) \subset Gal(L/K)$.

$\sigma \in Gal(L/K)$, par définition de F, et on a $\sigma(x) = x, \ \ \forall x \in F$ donc

$$\sigma \in Gal(L/F), \quad \text{d'où } \ Gal(L/K) \subset Gal(L/F)$$

par suite $Gal(L/K) = Gal(L/F)$.

Théorème 11.1.15.

Soit K un corps, L une extension de degré fini de K, F le corps fixe de $Gal(L/K)$. Alors

1. $|Gal(L/K)| = |Gal(L/F)| = [L : F]$
2. *L est une extension galoisienne de K si et seulement si $K = F$.*

Démonstration :

Posons $n = [L : F]$

1. Supposons $|Gal(L/F)| < [L : F] = m$.
   Soit $(e_1, \cdots, e_n)$ une base du F- ev L <;
   Posons $Gal(L/F) = Gal(L/K) = \{\sigma_1, \cdots, \sigma_m\}$.
   On considère la matrice $M = (\sigma_j(e_i))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$.
   Soit V le sous - espace vectoriel du L-ev L^m engendré par les vecteurs lignes $L_1, L_2, \cdots, L_n$ de M et $r = dim\ V$ on a $1 \leq r \leq m < n$. Extrayons une base $L_1, \cdots, L_r$ à partir de cette famille génératrice.
   $L_{r+1} \in V = Vect(L_1, , \cdots, L_r \Longrightarrow \exists (\lambda_1, \cdots, \lambda_r) \in L^r$ tel que
   $L_{r+1} = \sum_{i=1}^{r} \lambda_i \ L_i \Longrightarrow \forall j \in \{1, .., m\}, \ g_j(e_{r+1}) = \sum_{i=1}^{r} \lambda_i \ g_j(e_i)$
   c'est-à-dire
   $$g(e_{r+1}) = \sum_{i=1}^{r} \lambda_i \ g(e_i) \quad \forall g \in Gal(L/K). \tag{11.3}$$
   Soit $f \in Gal(L/K)$ et $g \in Gal(L/K)$, en composant par f les deux membres de (1.3), on a
   $$f \circ g(e_{r+1}) = f(g(e_{r+1})) = \sum_{i=1}^{r} f(\lambda_i) \ f \circ g(e_i) \quad \text{pour } f \text{ fixe.}$$
   L'application
   $$\begin{aligned} \varphi_f : Gal(L/K) &\longrightarrow Gal(L/K) \\ g &\longrightarrow \varphi_f(g) = f \circ g \end{aligned}$$
   est une bijection, donc $\forall f \in Gal(L/K), \ \ \forall g \in Gal(L/K)$
   $$g(e_{r+1}) = \sum_{i=1}^{r} f(\lambda_i) \ g(e_i) \tag{11.4}$$

$(2)-(1) \Longrightarrow \sum_{i=1}^{r}(f(\lambda_i)-\lambda_i)\ g_i(e_i)=0 \Longrightarrow \sum_{i=1}^{r}(f(\lambda_i)-\lambda_i)L_i=0\ \ \forall f\in Gal(L/K)$.
Comme $L_1, L_2, \cdots, L_r$ sont linéairement indépendants on a

$$f(\lambda_i)=\lambda_i \quad \forall i\in\{1,..,r\}, \quad \forall f\in Gal(L/K).$$

Ainsi $\lambda_i \in F \quad i\in\{1,..,r\}$. En appliquant (1.3) pour $g=id_L$, on a $e_{r+1} = \sum_{i=1}^{r}\lambda_i\ e_i$ ce qui contredit le fait que $\{e_1, e_2, \cdots, e_n\}$ est une base d'où

$$|Gal(L/K)| = |Gal(L/F)| = [L:F]$$

2. Comme $K\subset F\subset L$, on a $[L:K]=[L:F][F:K]$
$\Longrightarrow |Gal(L/F)| = [L:K] \Longleftrightarrow [F:K]=1 \Longleftrightarrow F=K$.

11.2 Polynômes séparables et extensions séparables

Définition 11.2.1.

Soit K un corps et $P(X)\in K[X]$ un polynôme irréductible. On dit que $P(X)$ est séparable si toutes les racines de $P(X)$ dans une clôture algébrique de K sont simples.

Un polynôme non constant est dit séparable si tous ses facteurs irréductibles sont séparables.

Si un polynôme n'est pas séparable on dit qu'il est inséparable.

Exemple 11.2.2.

$X^2+1\in\mathbb{R}[X]$ est séparable, $(X-1)^3(X^2+3)^4\in\mathbb{R}[X]$ est séparable.

Lemme 11.2.3.

Soit K un corps $P(X)\in K[X]$ un polynôme non constant. Alors $P(X)$ possède une racine multiple dans son corps de décomposition L sur K si et seulement si dans $L[X]$ le degré du pgcd(P,P) de $P(X)$ et de son polynôme dérive $P'(X)$ est strictement positif.

Démonstration :

$\Longrightarrow$) Soit α une racine d'ordre de multiplicité $m>1$ de $P(X)$ dans le corps de décomposition L de $P(X)$.

Dans $L[X]$, $P(X)=(X-\alpha)^m\ Q(X)$ avec $Q(\alpha)\neq 0$.
$P'(X)=m(X-\alpha)^{m-1}\ Q(X)+(X-\alpha)^m\ Q'(X)$
$P'(\alpha)=0 \Longrightarrow X-\alpha$ divise
donc $X-\alpha$ est un diviseur commun à $P(X)$ et $P'(X)$, d'où $X-\alpha$ divise $D(X) = pgcd(P,P')$. Ainsi

$$deg(D(X)) \geq deg(X-\alpha)=1.$$

$\Longleftarrow$) Soit $D = pgcd(P, P')$ et supposons $deg(D) \geq 1$
Soit α une racine de $D(X)$ dans le corps de décomposition L de $P(X)$ sur K.
Comme D divise P et P' et $D(\alpha) = 0$, on a $P(\alpha) = P'(\alpha) = 0$.
Soit $m \geq 1$ l'ordre de multiplicité de α comme racine de $P(X)$ dans $L[X]$, on a $P(X) = (X - \alpha)^m\, Q(X)$ avec $Q(\alpha) \neq 0$ montrons que $m > 1$.
Si $m = 1$ alors $P'(X) = Q(X) + (X - \alpha)\, Q'(X)$ et $P'(\alpha) = Q(\alpha) \neq 0$ ce qui est absurde.
Donc $m > 1$.

Lemme 11.2.4.

Soit K un corps, $P \in K[X]$ tel que $P' = 0$. Alors
(i) Si $Car(K) = 0$, P est constant
(ii) Si $Car(K) = p > 0$, il existe $Q \in K[X]$ tel que $P(X) = Q(X^p)$.

<u>Démonstration</u> :

Soit $P(X) = \sum_{i=0}^{n} a_i\, X^i$

$P'(X) = \sum_{i=1}^{n} i a_i\, X^{i-1}$, donc $P' = 0 \Longleftrightarrow i a_i = 0$ pour $1 \leq i \leq n$.

i) Si $Car(K) = 0$, on a $a_i = 0$, $1 \leq i \leq n$, donc P est constant.

ii) Si $Car(K) = p > 0$, $i a_i = 0$ signifie que i est un multiple de p dès que $a_i \neq 0$

$$i = jp \Longrightarrow P(X) = \sum_{i=0}^{n} a_i\, X^{jp} = \sum_{j=0}^{[\frac{n}{p}]} a_{jp}\, (X^p)^j$$

$$P(X) = Q(X^p) \text{ avec } Q(X) = \sum_{j=0}^{[\frac{n}{p}]} b_j\, X^j, \quad b_j = a_{jp}$$

Proposition 11.2.5.

Soit K un corps et $P(X) \in K[X]$ un polynôme irréductible

1. *Si $Car(K) = 0$ alors $P(X)$ est séparable*
2. *Si $Car(K) = p > 0$ est premier alors P est séparable si et seulement si $P(X) \notin K[X^p]$.*

<u>Démonstration</u> :

1. Soit $P(X) \in K[X]$ irréductible.
   Comme $Car(K) = 0$, $P'(X) \neq 0$, $P' \neq 0$.
   Soit $\overline{K}$ une clôture algébrique de K et $\alpha \in \overline{K}$ une racine de $P(X)$. Comme P est irréductible quitte à multiplier $P(X)$ par l'inverse de son coefficient dominant, onpeut supposer que P est le polynôme minimal de α sur K. De plus, comme

$d^\circ P' < d^\circ P$ et $P' \neq 0$, on a $P'(\alpha) \neq 0$, d'où α est une racine simple de P et P est séparable.

2. $\Longrightarrow$) Supposons P séparable. D'après le lemme 3 le degré de $D = pgcd(P, P')$ est inférieur ou égal à 0, $P(X)$ étant irréductible, on a $deg(P) \geq 1$, donc $D \neq P$. Par conséquent $P' \neq 0$, donc $P(X) \notin K[X^p]$ d'après le lemme 4.

$\Longleftarrow$) Réciproquement, supposons que $P(X) \notin K[X^p]$.

$P(X) = \sum_{i=0}^{n} a_i\ X^i$, $n \geq 1$, $a_n \neq 1$, $a_n \neq 0$, comme $P(X) \notin K[X^p]$.

$\exists i_o \in \{1, .., n\}$ tel que $a_{i_o} \neq 0$ et $i_o \notin p\mathbb{Z}$

$$P'(X) = \sum_{i=1}^{n} i a_i\ X^{i-1}\ X^{i-1} \neq 0 \ \text{ car } \ i_o\ a_{i_o}\ X^{i_o - 1} \neq 0,$$

$P(X)$ étant irréductible, $P(X)$ et $P'(X)$ sont premiers entre eux car $deg(P') < deg(P)$, d'après le lemme 3.

$P(X)$ n'admet pas de racines multiples, il est donc séparable.

Exercices

Anneaux

Polynômes irréductibles

Corps et extensions