Licence de mathématiques

Mohamed Aqalmoun
ⵎⵓⵃⴰⵎⴻⴷ ⴰⵇⴰⵍⵎⵓⵏ

Structures algébriques

Module *M*353 (S5)

Cahier-Cours

ENS-FES

Table des matières

Chapitre 1

Groupes

ᴏlΛ§ , ... let's go

1.1 Groupes

1.1.1 Définitions et exemples

Définition 1.1.

Un groupe est un couple $(G,*)$ où G est un ensemble et $*: G\times G\to G$ est une loi de composition interne vérifiant les propriétés suivantes :

1. *La loi $*$ est associative ; $\forall (x,y,z)\in G^3$,*
$$x*(y*z)=(x*y)*z$$
2. *La loi $*$ possède un élément neutre ; il existe $e\in G$ tel que pour tout $x\in G$,*
$$x*e=e*x=x$$
3. *Tout élément de G possède un symétrique, c'est-à-dire pour tout $x\in G$, il existe $x'\in G$ tel que*
$$x*x'=x'*x=e$$

Remarque : Par un simple jeu logique avec ces axiomes, on vérifie que si $(G,*)$ est un groupe alors

1. L'élément neutre e est unique.

2. Le symétrique d'un élément x est unique et on le note $\mathrm{sym}(x)$.

Exemples :

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes.
2. $(\{-1,1\},\times)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes.

Définition 1.2.

Un groupe $(G,*)$ est dit abélien ou commutatif, lorsque la loi $*$ est commutative c'est-à-dire pour tout $(x,y)\in G^2$,

$$x*y=y*x$$

Exemple : Les groupes cités dans l'exemple précédent sont tous abéliens.

1.1.2 Groupe produit

Soit $(G,*)$, $(G',.)$ deux groupes. On rappel que la loi produit sur $G\times G'$ est définie par

$$(x,y)\top(x',y')=(x*x',y.y')$$

Théorème 1.3. (et définition)

Soient $(G_1,*)$, $(G_2,.)$ deux groupes. Alors $G_1\times G_2$ muni de la loi produit est un groupe, dit le groupe produit de $(G_1,*)$ et $(G_2,.)$.

Démonstration : $(G_1\times G_2,\top)$ est un monoïde où $\top$ est la loi produit, si $(x,y)\in G_1\times G_2$, notons x' et y' respectivement le symétrique de x respectivement de y, alors $(x,y)\top(x',y')=(x*x',y.y')=(e_1,e_2)=(x'*x,y'.y)=(x',y')\top(x,y)$ donc (x,y) est symétrisable et $\mathrm{sym}(x,y)=(x',y')$.

1.1.3 Sous-groupes

Soit $(G,*)$ un groupe. Lorsque la loi du groupe G est notée multiplicativement, l'élément$x*y$ sera noter xy et le symétrique de x sera notée également x^{-1}. Lorsque la loi est notée additivement l'élément $x*y$ sera noter $x+y$ et le symétrique de x sera noter aussi $-x$. Souvent, les groupes sont notés multiplicativement.
On rappel qu'une partie H d'un groupe G est dite stable si, pour tout $x,y\in H$, $xy\in H$.

Définition 1.4.

Soit G un groupe et H une partie de G. On dit que H est un sous groupe de G, si H est stable par la loi de G et H muni de la loi induite est un groupe.

Exemple : .....

Théorème 1.5.

Soit H une partie d'un groupe G. Les propriétés suivantes sont équivalentes :

1. *H est un sous groupe de G,*
2. *H est non vide, et $\forall x, y \in H$, $xy \in H$ et $x^{-1} \in H$.*

Démonstration : voir cours *S*1.

Théorème 1.6.

Soit H une partie d'un groupe G, on a équivalence entre :

1. *H est un sous groupe de G,*
2. *H non vide, et $\forall x, y \in H$; $xy^{-1} \in H$.*

Démonstration : Voir cours *S*1.

Exemple : .....

Proposition 1.7.

Soit G un groupe. Si $(H_i)_{i\in I}$ est une famille de sous-groupes de G, alors $\cap_{i\in I} H_i$ est un sous groupe de G.

Démonstration : Voir cours *S*1.

1.1.4 Sous groupe engendré par une partie

Définition 1.8.

Soit G un groupe et A une partie de G. Le sous groupe $\cap_{A\subseteq H} H$ (l'intersection de tous les sous groupes de G contenant A) est appelé le sous groupe engendré par A et se note $\langle A\rangle$. C'est le plus petit sous groupe de G contenant A.

Remarque : Le plus petit sous groupe de G contenant l'ensemble vide est le sous groupe $\{e\}$, donc .....

Théorème 1.9.

Soit G un groupe et A une partie non vide de G. Alors

$$\langle A\rangle = \{x_1 \dots x_n \quad / \quad n \geq 1, x_i \in A \text{ ou } x_i^{-1} \in A\}$$

Démonstration : On pose $H_1 = \{x_1 \dots x_n \quad / \quad n \geq 1, x_i \in A \text{ ou } x_i^{-1} \in A\}$ .....

Corollaire 1.10.

Soit G un groupe et $g \in G$. Si $A = \{g\}$, alors $\langle A\rangle = \{g^n \in / \ n \in \mathbb{Z}\}$ noté aussi $\langle g\rangle$.

Démonstration : D'après le théorème précédent.

Définition 1.11.

Soit G un groupe. On dit que que G est un groupe monogène si G est engendré par un seul élément c'est-à-dire il existe $g \in G$ tel que $G = \langle g\rangle$.

Exemple : Le groupe $\mathbb{Z}$ est un groupe monogène engendré par 1.

Proposition 1.12.

Tout groupe monogène est abélien.

Démonstration : .....

Théorème 1.13.

Tout sous groupe d'un groupe monogène est monogène.

Démonstration : .....

Corollaire 1.14. (Sous groupe de $\mathbb{Z}$)

Les sous groupe de $\mathbb{Z}$ sont les partie de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Démonstration : .....

1.1.5 Morphisme de groupes

Définition 1.15.

Soient G , G' deux groupes, et $f : G \to G'$ une application. On dit que f est un morphisme de groupes si ; pour tous $x, y \in G$, on a $f(xy) = f(x)f(y)$.

Propriétés 1.16.

Soit $f : G \to G'$ un morphisme de groupes.

1. $f(e) = e'$,
2. $f(x^{-1}) = f(x)^{-1}$.

Démonstration : .....

Proposition 1.17.

1. *Si $f : G \to G'$ et $g : G' \to G''$ sont deux morphismes de groupes alors $g \circ f : G \to G''$ l'est aussi.*
2. *Si $f : G \to G'$ est un morphisme de groupes bijectif. Alors $f^{-1} : G' \to G$ est un morphisme de groupes.*

Démonstration : .....

Définition 1.18.

1. *Un morphisme de groupes $f : G \to G'$ est dit isomorphisme si f est bijective.*
2. *Un endomorphisme de G est un morphisme de G dans lui même. L'ensemble des endomorphismes de G se note* $\mathrm{End}(G)$.
3. *Un automorphisme de G est un isomorphisme de G dans lui même ou encore est un endomorphisme bijectif. L'ensemble des automorphismes de G se note* $\mathrm{Aut}(G)$.

Proposition 1.19.

Soit G un groupe. Alors $(\mathrm{Aut}(G), \circ)$ *est un groupe.*

Démonstration : .....

Proposition 1.20.

Soit $f : G \to G'$ un morphismes de groupes.

1. *Si H est un sous groupe de G alors $f(H)$ est un sous groupe de G'.*
2. *Si K est un sous groupe de G' alors $f^{-1}(K)$ est un sous groupe de G.*

Démonstration : .....

Définition 1.21.

Soit $f : G \to G'$ un morphisme de groupes.

1. *On appelle noyau de f le sous groupe* $\ker f := f^{-1}(\{e'\})$ *où e' est le neutre de G'.*
2. *On appelle image de f le sous groupe* $\mathrm{Im}\, f := f(G)$.

Proposition 1.22.

Soit $f : G \to G'$ un morphisme de groupes.

1. *f injectif si, et seulement si, $\ker f = \{e\}$.*
2. *f est surjectif si, et seulement si, $\mathrm{Im}\, f = G'$.*

Démonstration : .....

1.2 Groupe fini

Définition 2.1.

Un groupe G est dit fini, lorsque l'ensemble G est fini, son cardinal est dit l'ordre du groupe et se note $o(G)$ ou $\mathrm{ord}(G)$ ou $|G|$.

Exemple : Soit $n \in \mathbb{N}^*$, on pose $\mathbb{U}_n = \{z \in \mathbb{C} \ / \ z^n = 1\}$ ensemble des racines n-ème de l'unité .....

Définition 2.2.

Un groupe cyclique est un groupe monogène et fini.

Exemple : $\mathbb{U}_n$ est un groupe cyclique d'ordre (de cardinal) n.

Définition 2.3.

Soit G un groupe et $g \in G$. On dit que g est d'ordre fini si le groupe $\langle g \rangle$ est fini, dans ce cas l'ordre de g est noté $o(g)$ est le cardinal de $\langle g \rangle$.

Exemple : .....

Théorème 2.4.

Soit G un groupe et g un élément d'ordre fini. Alors $o(g) = \min\{k \in \mathbb{N}^* \mid g^k = e\}$ et $\langle g \rangle = \{e, g, \ldots, g^{o(g)-1}\}$.

Démonstration : .....

1.3 Groupe quotient

1.3.1 Relation modulo un sous groupe

Définition 3.1.

Soit G un groupe et H un sous groupe de G.

1. *La relation définie par $x \sim_g y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence. La classe d'équivalence de x est l'ensemble xH (classe d'équivalence à gauche modulo H), l'ensemble quotient se note G/H.*
2. *La relation définie par $x \sim_d y \Leftrightarrow xy^{-1} \in H$ est une relation d'équivalence. La classe d'équivalence de x est l'ensemble Hx (classe d'équivalence à droite modulo H), l'ensemble quotient se note $H\backslash G$.*

Justification : .....

Proposition 3.2.

Soit G un groupe et H un sous groupe de G.

1. *Les ensembles xH, Hx et H sont équipotents, si de plus H est fini, $|xH| = |Hx| = |H|$.*
2. *G/H et $H\backslash G$ sont équipotents, si de plus G est fini $|G/H| = |H\backslash G|$.*

Démonstration : .....

Définition 3.3.

Soit G un groupe et H un sous groupe de G. On appelle indice de H dans G noté $[G:H]$ le cardinal (éventuellement infini) de G/H (c'est aussi le cardinal de $H\backslash G$).

Théorème 3.4. (Théorème de Lagrange)

Soit G un groupe fini et H un sous groupe de G. Alors $|H|[G:H] = |G|$, en particulier $|H|$ divise $|G|$.

Démonstration : .....

Corollaire 3.5.

Soit G un groupe fini d'ordre n et $g \in G$. On a $o(g)$ divise n, et $g^n = e$.

Démonstration : .....

1.3.2 Sous groupe distingué

Définition 3.6. (Sous groupe distingué)

Soit G un groupe et H un sous groupe de G. On dit que H est un sous groupe distingué (ou normal) de G et on note $H \lhd G$ si, pour tout $x \in G$, $xHx^{-1} \subseteq H$.

Exemples :

1. Les sous groupes d'un groupe abélien sont distingués.
2. $\{e\}$ et G sont des sous groupes distingués de G.
3. $\mathrm{SL}_n(\mathbb{K}) := \{A \in \mathrm{Gl}_n(\mathbb{K}) \ / \ \det(A) = 1\}$ est un sous groupes distingués de $\mathrm{GL}_n(\mathbb{K})$. En effet ; .....

Proposition 3.7.

Soit G un groupe et H un sous groupe de G. Les propriétés suivantes sont équivalentes :

1. *H sous groupe distingué de G,*
2. *Pour tout $x \in G$, $xHx^{-1} = H$,*
3. *Pour tout $x \in G$, $xH = Hx$.*

Démonstration : .....

Proposition 3.8.

Soit $f : G \to G'$ un morphisme de groupes. Alors $\ker f$ est un sous groupe distingué de G.

Démonstration : .....

Proposition 3.9.

Soit $(H_i)_{i\in I}$ une famille de sous groupes distingués de G. Alors $\cap_{i\in I} H_i$ est un sous groupe distingué de G.

Démonstration : .....

1.3.3 Groupe quotient

Soit G un groupe et H un sous groupe distingué de G. Dans ce cas $G/H = H\backslash G$.

Théorème et définition 3.10.

Soit G un groupe et H un sous groupe distingué de G. L'application $G/H \times G/H \to G/H$, $(\overline{x},\overline{y}) \mapsto \overline{xy}$ définie une loi de composition interne sur G/H, et muni de cette loi G/H est un groupe dit groupe quotient de G par H. De plus l'application $\pi : G \to G/H$, $x \mapsto \overline{x}$ est un morphisme de groupe surjectif, dit morphisme canonique.

Démonstration : .....

Remarques :

1. Si $H = \{e\}$, alors G/H et G sont isomorphes.
2. Si $H = G$, alors G/H est réduit à un singleton.

Théorème 3.11.

Soit $f : G \to G'$ un morphisme de groupes et H un sous groupe distingué de G tel que $H \subseteq \ker f$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ vérifiant $f = \overline{f} \circ \pi$ (i.e $\forall x \in G$, $\overline{f}(\overline{x}) = f(x)$).

Démonstration : .....

1.3.4 Théorème d'isomorphisme

Théorème 3.12.

Soit $f : G \to G'$ un morphisme de groupes. Alors

$$\begin{array}{rcl} \overline{f} : G/\ker f & \to & \operatorname{Im} f \\ x & \mapsto & f(x) \end{array}$$

est un isomorphisme de groupes.

Démonstration : .....

Remarque : Si G est fini alors $o(G/\ker f) =$ .....

Corollaire 3.13.

Soit G un groupe monogène. Alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ ou G est isomorphe à $\mathbb{Z}$.

Démonstration : .....

Théorème 3.14.

Soit G un groupe et H, K deux sous groupes distingués dans G tels que $H \subseteq K$. Alors $(K/H) \lhd (G/H)$ et $(G/H)/(K/H)$ est isomorphisme à G/K.

Démonstration : .....

1.4 Groupe symétrique

1.4.1 Groupe symétrique

Théorème et définition 4.1.

Soit X un ensemble non vide. L'ensemble des applications bijectives de X vers X muni de la composition des applications est un groupe appelé groupe symétrique de X et se note $S(X)$. Un élément de $S(X)$ est appelé une permutation de X.

Notations : pour $n \geq 1$, on note S_n le groupe symétrique de $X = \{1,2,\ldots,n\}$. Si $\sigma \in S_n$ avec $\sigma(i) = a_i$, alors σ se note $\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$, ainsi $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.
Si $\sigma, \sigma' \in S_n$, on note $\sigma\sigma'$ au lieu de $\sigma \circ \sigma'$.

Remarque : S_n est fini et $\text{Card}(S_n) = n!$.

Exemple : S_2 et S_3 : .....

Exemple : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 4 & 1 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 3 & 1 \end{pmatrix}$:
$\sigma\sigma'$ .....
σ^{-1} .....

Définition 4.2.

Soit $n \geq 2$. Une transposition de S_n est une permutation de S_n qui échange deux éléments distincts de $[\![1,n]\!]$ et en fixant les autres éléments.
Soit $(i,j) \in [\![1,n]\!]^2$ avec $i \neq j$. La transposition qui échange i et j se note τ_{ij}. Elle est définie par : $\tau_{ij}(i) = j$ et $\tau_{ij}(j) = i$ et $\tau_{ij}(k) = k$, si $k \notin \{i,j\}$.

Proposition 4.3.

Soit $\tau \in S_n$ une transposition. Alors $\tau^2 = \text{Id}$ et $\tau^{-1} = \tau$.

Démonstration : .....

Théorème 4.4.

Toute permutation est le produit d'un nombre fini de transpositions. En d'autres termes le groupe S_n est engendré par ses transpositions.

Démonstration : .....

1.4.2 Signature

Définition 4.5.

Soit $n \geq 2$ un entier. On appelle nombre d'inversions $\sigma \in S_n$ l'entier :

$$I(\sigma) = \text{card}\left\{(i,j) \in [\![1,n]\!]^2 \;\middle|\; i<j \text{ et } \sigma(j)<\sigma(i)\right\}$$

On appelle signature de σ l'entier valant -1 ou 1 défini par : $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Exemple : .....

Proposition 4.6.

Soit $n \geq 2$ et $\tau \in S_n$ une transposition. Alors $\varepsilon(\sigma) = -1$.

Démonstration : .....

Théorème 4.7.

La signature est un morphisme de groupes de S_n dans $(\{-1,1\},\times)$. Autrement dit, $\forall \sigma,\sigma' \in S_n$, $\epsilon(\sigma\sigma') = \epsilon(\sigma)\epsilon(\sigma')$.

Démonstration : .....

Corollaire 4.8.

Soit $\sigma \in S_n$ $(n \geq 2)$.

1. *Si σ se décompose d'une part en un produit de m transpositions, d'autre part en un produit de m' transpositions, alors les entiers naturels m et m' sont de même parité.*
2. *On a $\varepsilon(\sigma) = (-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions.*

Démonstration : .....

Exemples : .....

Définition 4.9.

Soit $n \geq 2$. Le noyau de ε est est appelé le nième groupe alterné. On le note A_n.

Remarque : A_n est un sous groupe de S_n.

Proposition 4.10.

A_n est de cardinal $\frac{n!}{2}$, en particulier A_n est un sous-groupe distingué de S_n.

Démonstration : .....

1.4.3 Support et orbite

Définition 4.11.

Soit $\sigma \in S_n$. On appelle support de σ l'ensemble $\text{supp}(\sigma) = \{k \in [\![1, n]\!] \ / \sigma(k) \neq k\}$.

Remarque : $\text{supp}(\sigma) = \emptyset$ si, et seulement si, ...

Proposition 4.12.

Pour toute $\sigma \in S_n$ non triviale, la restriction de σ à $\text{supp}(\sigma)$ *est une permutation. de* $\text{supp}(\sigma)$.

Démonstration : .....

Proposition 4.13.

Deux permutations de S_n dont les supports sont disjoints commutent.

Démonstration : .....

Définition 4.14.

Pour toute $\sigma \in S_n$ et tout $i \in \{1,2,...,n\}$, on appelle σ-orbite de i l'ensemble des images de i par les différents éléments du groupe cyclique $\langle\sigma\rangle$; on le note

$$\Omega_\sigma(i) = \{\sigma^k(i) \mid k \in \mathbb{Z}\}$$

On dit que $\Omega_\sigma(i)$ est une orbite ponctuelle si $\Omega_\sigma(i) = \{i\}$.

Exemple : .....

Proposition 4.15.

Soit $\sigma \in S_n$ $(n \geq 2)$ et $i \in [\![1,n]\!]$.

1. *$\Omega_\sigma(i) = \{i\}$ si, et seulement si, $i \notin \text{supp}(\sigma)$.*
2. *Les différentes σ-orbites forme une partition de $[\![1,n]\!]$.*

Démonstration : .....

Définition 4.16.

Une permutation $\sigma \in S_n$ est appelée un cycle lorsqu'il existe une σ-orbite et une seule qui n'est pas ponctuelle.

Exemple : .....

Proposition 4.17.

Soit $\sigma \in S_n$ un cycle. On note p l'ordre de σ dans S_n.

1. *L'unique σ-orbite non ponctuelle est égale au support de σ.*
2. *Le cardinal du support de σ est égal à p.*
3. *Il existe $i_1, i_2, \ldots, i_p$ distincts dans $\{1,2,...,n\}$ tels que :*
   $\sigma(i_1) = i_2, \ldots, \sigma(i_{p-1}) = i_p, \sigma(i_p) = i_1$ et $\sigma(i) = i$ si $i \notin \{i_1, \ldots, i_p\}$.

On dit alors que σ est un p-cycle, et on note $\sigma = (i_1\ i_2\ \ldots\ i_p)$.

Démonstration : .....

Remarque : L'inverse d'un p-cycle est un p-cycle .....
Les 2-cycles sont .....

Proposition 4.18.

Si $\sigma \in S_n$ est un p-cycle alors $\varepsilon(\sigma) = (-1)^{p-1}$

Démonstration : .....

Théorème 4.19. (Décomposition en produit de cycles disjoints)

Soit $\sigma \in S_n$ une permutation non triviale.

1. *σ se décompose en un produit de cycles à supports disjoints.*
2. *Les cycles dans une telle décomposition commutent deux à deux.*
3. *Cette décomposition est unique à l'ordre près des facteurs.*

Démonstration : .....

1.5 Exercices

Exercice 1.1

Soit G un groupe de neutre e tel que $\forall x \in G,\ x^2 = e$. Montrer que G est un groupe abélien.

Exercice 1.2

Soit G un groupe et H un sous groupe de G. Soit $x \in G$ on pose

$$xHx^{-1} = \{xhx^{-1}\ ,\ \ h \in H\}$$

Montrer que xHx^{-1} est un sous groupe de G.

Exercice 1.3

Soit G un groupe. On pose $Z(G) = \{x \in G\ \ ,\ \ \forall y \in G\ \ xy = yx\}$.
Montrer que $Z(G)$ est un sous groupe de G (appelé le centre de G)

Exercice 1.4

Soit G un groupe et H une partie finie non vide de G. On suppose que H est stable par la loi de G.

1. *Montrer que si $h \in H$, alors il existe $N \in \mathbb{N}^*$ tel que $h^N = e$.*
2. *En déduire que H est un sous groupe de G.*

Exercice 1.5 (Union de deux sous groupes)

Soit G un groupe, H et K deux sous groupes de G.
Montrer que $H \cup K$ est un sous groupe de G si, et seulement si, $H \subseteq K$ ou $K \subseteq H$.

Exercice 1.6

Soit G un groupe fini d'ordre pair. Montrer qu'il existe un élément $x \in G$ tel que $x \neq e$ et $x^2 = e$

Exercice 1.7 (Les sous groupes de $\mathbb{R}$)

Soit G un sous groupe de $(\mathbb{R}, +)$. On suppose que $G \neq \{0\}$

1. *Montrer que $G \cap \mathbb{R}_+^*$ admet une borne inférieure a.*
2. *Montrer que $a \in G$. (Distinguer les deux cas $a = 0$ et $a \neq 0$).*
3. *On suppose que $a > 0$. Montrer que $G = a\mathbb{Z}$*
4. *On suppose que $a = 0$. Montrer que G est dense dans $\mathbb{R}$*
5. *Soit $f : \mathbb{R} \to \mathbb{R}$ périodique non constante continue sur $\mathbb{R}$. Montrer que f admet une plus petite période. c-a-d : $\{T \in \mathbb{R}_+^*, \quad \forall x \in \mathbb{R} \ \ f(x+T) = f(x)\}$ à un plus petit élément.*
6. *Soi $H = \{n + p\sqrt{2}, \quad n, p \in \mathbb{Z}\}$. Montrer que H est un sous groupe de $(\mathbb{R}, +)$. De quel type est-il ?*
7. *Montrer que $\{\cos n \quad / \quad n \in \mathbb{N}\}$ est une partie dense dans $[-1, 1]$.*

Exercice 1.8

Soit G un groupe de neutre e et H une partie de G contenant e. Pour $g \in G$ on définit

$$gH := \{gh \ / h \in H\}$$

1. *Montrer que si H est un sous groupe de G, alors la famille $(gH)_{g\in G}$ forme une partition de G.*
2. *Montrer que si la famille $(gH)_{g\in G}$ forme une partition de G alors H est un sous groupe de G.*

Exercice 1.9

Soit G un groupe. H et K deux sous groupes de G, on note

$$HK = \{hk \ / h \in H \ , k \in K\}$$

Montrer que les propriétés suivantes sont équivalentes.

1. *HK est un sous groupe de G,*
2. *KH est un sous groupe de G,*
3. *$HK \subseteq KH$,*
4. *$KH \subseteq HK$.*

Exercice 1.10

Soit G un groupe. Pour tout $g \in G$ on note $i_g : G \to G$ l'application définie par $i_g(x) = g^{-1}xg$

1. *Montrer que pour tout $g \in G$, i_g est automorphisme de G.*
   On pose $\mathrm{Fix}(i_g) = \{x \in G \mid i_g(x) = x\}$
2. *Montrer que $\mathrm{Fix}(i_g)$ est un sous groupe de G*
3. *Démontrer que $\bigcap_{g\in G} \mathrm{Fix}(i_g) = Z(G)$*

Exercice 1.11

Montrer que les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ne sont pas isomorphes.

Exercice 1.12

Soit G un groupe.

1. *Montrer que si $x \mapsto x^2$ est un morphisme de groupes, alors G est commutatif.*
2. *Montrer que si $x \mapsto x^{-1}$ est un morphisme de groupes, alors G est commutatif.*
3. *Montrer que si $x \mapsto x^3$ est un morphisme de groupes surjectif, alors G est commutatif.*

Exercice 1.13

Soit G un groupe commutatif fini d'ordre impair. Montrer que $x \mapsto x^2$ est surjectif.

Exercice 1.14

Soit G un groupe. On appelle commutateur de x et y l'élément

$$[x, y] = xyx^{-1}y^{-1}$$

On appelle sous groupe dérivé de G noté $D(G)$ le sous groupe engendré par l'ensemble des commutateurs.

1. *Décrire $D(G)$ lorsque G est commutatif.*
2. *Montrer que si f est un endomorphisme de G, alors $f(D(G)) \subseteq D(G)$.*

Exercice 1.15

Soit G un groupe et A une partie de G. On désigne par $Z(A)$ le centralisateur de A c'est-à-dire $Z(A) = \{g \in G \ . \ \forall a \in A, \quad ga = ag\}$

1. *Montrer que $Z(A)$ est un sous groupe de G.*
2. *Montrer que $Z(A) = Z(\langle A \rangle)$.*

Exercice 1.16

Soit G un groupe et H un sous groupe de G d'indice 2. Montrer que H est distingué dans G.

Exercice 1.17

Soit G un groupe.

1. *Montrer que $Z(G)$ est un sous groupe distingué de G.*
2. *Montrer que si $G/Z(G)$ est monogène alors G est abélien.*

Exercice 1.18

Soit G un groupe et $a, b \in G$ deux éléments d'ordre fini tels que $ab = ba$.

1. *Montrer que si $o(a) \wedge o(b) = 1$, alors $o(ab) = o(a)o(b)$.*
2. *Soit $\tau = \tau_{12}, \tau' = \tau_{23} \in S_n$ où $n \geq 3$. Quel est l'ordre de τ, τ' et $\tau\tau'$?*

Exercice 1.19

Montrer que A_3 est engendré par le 3-cycle (1 2 3)

Exercice 1.20

Soit $n \geq 2$ un entier naturel.

1. *Soit $(i_1 \ \dots \ i_p)$ un p-cycle de S_n et $\sigma \in S_n$. Montrer que*

$$\sigma(i_1 \ \dots \ i_p)\sigma^{-1} = (\sigma(i_1) \ \dots \ \sigma(i_r))$$

2. *En déduire que deux p-cycles sont conjugués.*

Exercice 1.21

Pour $n \geq 2$.

1. *Pour $i \neq j$ et $\sigma \in S_n$. Montre que $\sigma\tau_{ij}\sigma^{-1} = \tau_{kl}$ où $k = \sigma(i)$ et $l = \sigma(j)$.*

2. *En déduire que deux transpositions de S_n sont conjuguées.*
3. *Déterminer tous les morphismes de groupes de S_n dans $\mathbb{C}^*$.*

Exercice 1.22

Soit G un groupe, H et H' deux sous-groupes finis de G. Montrer que si $o(H)$ et $o(H')$ sont premiers entre eux alors $H \cap H' = \{e\}$.

Exercice 1.23

Soit n un entier > 1.

1. *Vérifier que $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication est un monoïde.*
2. *On note M_n l'ensemble des éléments inversible de $\mathbb{Z}/n\mathbb{Z}$. Montrer que $M_n = \{\overline{k} \ / \ k \wedge n = 1\}$.*
3. *Déterminer M_p lorsque p est un nombre premier.*
   Soit $G = \langle g \rangle$ un groupe monogène.
4. *Montrer que pour tout $f \in \mathrm{Aut}(G)$, $f(g)$ est un générateur de G.*
5. *On suppose dans cette question que G est cyclique d'ordre n.*
   (a) *Soit k un entier premier avec n avec $1 \leq k \leq n-1$. Montrer que l'application $h : G \to G$ définie par $h(x) = x^k$ est un automorphisme de G.*
   (b) *Soit h un automorphisme de G. Montrer que montrer qu'il existe k un entier premier avec n tel que $1 \leq k \leq n-1$ et $h(g) = g^k$. En déduire que pour tout $x \in G$, $h(x) = x^k$.*
   (c) *Montrer que $\mathrm{Aut}(G)$ est isomorphisme à M_n.*
   (d) *En déduire que $\mathrm{Aut}(G)$ est groupe abélien.*
6. *On suppose dans cette question que G monogène infini. Montrer que le groupe $\mathrm{Aut}(G)$ est cyclique d'ordre 2.*

Exercice 1.24

Soit G un groupe et H un sous groupe distingué de G.
On suppose que le groupe quotient G/H est fini d'ordre n.

1. *Montrer que pour tout $x \in G$, $x^n \in H$.*
2. *Montrer que si k est un entier premier avec n et $x \in G$ tel que $x^k \in H$ alors $x \in H$.*

Exercice 1.25

Soit G un groupe. Pour $g \in G$, on note $i_g : G \to G$ l'application définie par $i_g(x) = gxg^{-1}$.

1. *Pour $g \in G$. Montrer que i_g est un automorphisme de G.*
   Un automorphisme de la forme i_g s'appelle un automorphisme intérieur de G, l'ensemble des automorphismes intérieurs de G se note $\mathrm{Int}(G)$.
2. *Montre que $\mathrm{Int}(G)$ est un sous groupe de $\mathrm{Aut}(G)$ (pour la loi de composition).*
3. *Montrer que l'application $\varphi : G \to \mathrm{Int}(G)$ définie par $\varphi(g) = i_g$ est un morphisme de groupes.*
4. *En déduire que $G/Z(G)$ et $\mathrm{Int}(G)$ sont isomorphismes.*

Exercice 1.26

Soit G un sous groupe fini de $\mathrm{GL}_n(\mathbb{K})$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) de cardinal r. On pose $B = \frac{1}{r}\left(\sum_{A \in G} A\right)$.

1. *Montrer que pour tout $A \in G$, $AB = B$.*
2. *Montrer que B est la matrice d'un projecteur dans la base canonique de $\mathbb{K}^n$..*
3. *Montrer que $\sum_{A \in G} \mathrm{tr}(A)$ est un entier divisible par r.*
4. *Montrer que si $\sum_{A \in G} \mathrm{tr}(A) = 0$, alors $\sum_{A \in G} A = 0$.*
5. *Montrer que toute matrice $A \in G$ est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$.*

Exercice 1.27

On muni $\mathbb{R}^n$ *de la forme quadratique* $q(x) = \sum_{k=1}^{n} x_i^2$, *où* $x = (x_1, \ldots, x_n)$ *et* φ *sa forme polaire. Soit* G *un sous groupe fini de* $\mathrm{GL}(\mathbb{R}^n)$.

1. *Montrer que l'application* $\psi : (x, y) \mapsto \psi(x, y) = \sum_{g \in G} \varphi(g(x), g(y))$ *est une forme bilinéaire symétrique définie positive.*
2. *Montrer que pour tout* $g \in G$ *et tous* $x, y \in \mathbb{R}^n$,
$$\psi(g(x), y) = \psi(x, g^{-1}(y))$$
3. *Montrer que si* F *est un sous espace vectoriel de* $\mathbb{R}^n$ *stable par tous les éléments de* G, *alors il admet un supplémentaire stable par tous les éléments de* G.

Chapitre 2

Anneaux et corps

2.1 Anneaux et sous anneaux

Définition 1.1.

Un anneau est un triplet $(A,+,\times)$ *vérifiant :*
- $(A,+)$ *est un groupe abélien (de neutre* 0 *).*
- *La multiplication* $\times$ *est associative c'est-à-dire pour tous* $a,b,c\in A$, $a(bc)=(ab)c$.
- *La multiplication* $\times$ *est distributive par rapport à l'addition* $+$ *c'est-à-dire ; pour tous* $a,b,c\in A$, $(a+b)\times c=a\times c+b\times c$ *et* $a\times(b+c)=a\times b+a\times c$.

L'anneau A *est dit unitaire si* $\times$ *admet un élément neutre appelé unité et se note* 1_A *ou* 1.
L'anneau A *est dit commutatif si la multiplication* $\times$ *est commutative.*

Notation : Si $a,b\in A$, l'élément $a\times b$ sera noter ab.

Exemples :

1. $(\mathbb{Z},+,\times)$ est un anneau commutatif et unitaire,
2. $(\mathscr{M}_n(\mathbb{K}),+,\times)$ est un anneau unitaire (non commutatif si $n\geq 2$).

Propriétés 1.2.

Soit A *un anneau.*

1. *Pour tout* $a\in A$, $a.0=0.a=0$,
2. *Pour tous* $a,b\in A$, $(-a)b=a(-b)=-ab$,

3. Pour tous $a,b,c \in A$, $a(b-c) = ab-bc$ et $(a-b)c = ac-bc$.

Démonstration :

1. $a0 = a(0+0) = a0 + a0$, donc $a0 = 0$. De même $0a = 0$.
2. $(-a)b + ab = (-a+a)b = 0b = 0$, donc $(-a)b = -ab$, de même pour $a(-b) = -ab$.
3. $a(b-c) = ab + a(-c) = ab - ac$, de même $(a-b)c = ac - bc$.

Proposition 1.3.

Soit A un anneau $a,b \in A$ tels que $\underline{ab = ba}$ et $n \in \mathbb{N}^*$.

1. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
2. $a^n - b^n = (a-b)\left(\sum_{k=0}^{n} a^k b^{n-1-k}\right)$.

Par convention, si $x,y \in A$, $x^0 y = y$ et $xy^0 = x$.

Démonstration : Par récurrence sur n.

Définition 1.4. (Anneau produit)

Soit A_1, A_2 deux anneaux et $A = A_1 \times A_2$, alors muni des deux lois produits, A est un anneau appelé anneau produit.

Remarque :

1. Les lois de A sont définies de la façon suivantes : $(a,b) + (a',b') = (a+a', b+b')$ et $(a,b)(a',b') = (aa', bb')$.
2. Plus généralement si $A_1, \ldots, A_n$ sont des anneaux, alors muni des lois produits,
$$A := A_1 \times \ldots \times A_n$$
est un anneau.

Définition 1.5.

Soit A un anneau et B une partie de A. On dit que B est un sous anneau de A si $(B,+)$ est un sous groupe de $(A,+)$ et B stable par la multiplication.
Si A est un anneau unitaire un sous anneau unitaire de A est un sous anneau B contenant 1_A.

Exemple :

1. Pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous anneau de $\mathbb{Z}$.
2. Si A est un anneau l'ensemble $Z(A) = \{a \in A \ / \ \forall b \in A, \ \ ab = ba\}$ est un sous anneau de A.

Remarque : Soit A un anneau et B une partie non vide de A. Alors B est un sous-anneau de A si, et seulement si, pour tout $(x,y) \in B^2$, $x - y \in B$ et $xy \in B$.

Remarque : Si B est un sous anneau de A, alors B lui aussi est un anneau.

Proposition 1.6.

Si $(B_i)_{i\in I}$ est une famille de sous anneaux de A alors $\cap_{i\in I} B_i$ est un sous anneau de A.

2.2 Éléments particuliers

Définition 2.1.

Soit A un anneau unitaire. Un élément $a \in A$ est dit inversible s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles de A se note $\mathcal{U}(A)$.

Proposition 2.2.

Soit A un anneau unitaire et $a \in A$. Alors a est inversible si, et seulement si, il existe un unique $b \in A$ tel que $ab = ba = 1$. Si c'est les cas l'élément b s'appelle l'inverse de a et se note a^{-1}.

Démonstration : Si a est inversible et $b, b' \in A$ tels que $ab = ba = 1 = ab' = b'a$. Alors $b = 1b = (b'a)b = b'(ab) = b'1 = b'$.

Exemples :

1. $\mathscr{U}(\mathbb{Z}) = \{-1, 1\}$,
2. $\mathscr{U}(\mathbb{Q}) = Q^*$.

Proposition 2.3.

Soit A un anneau unitaire. Alors $\mathscr{U}(A)$ muni de la multiplication est un groupe.

Démonstration : Clairement 1 est inversible. Si a et a' sont inversibles alors aa' est aussi inversible et on a de plus $(aa')^{-1} = a'^{-1}a^{-1}$. De plus si a est inversible alors a^{-1} est inversible c'est-à-dire $a^{-1} \in \mathscr{U}(A)$. Ainsi $\mathscr{U}(A)$ stable par la multiplication (on a aussi l' associativité), possède un élément neutre , et tout élément est inversible. Il s'agit alors d'un groupe.

Définition 2.4.

Soit A un anneau.
Un élément a non nul de A est dit diviseur de zéro à gauche (respectivement à droite), s'il existe un élément non nul b tel que $ab = 0$ (respectivement $ba = 0$).
On dit que a est un diviseur de zéro dans A si a est un diviseur de zéro à gauche ou à droite dans A.
On dit que a est un élément régulier à gauche (respectivement à droite), s'il est non nul et s'il n'est pas un diviseur à gauche (respectivement à droite).
Un élément a de A est dit régulier s'il n'est pas nul et n'est pas un diviseur de zéro.

Remarque : Si a est inversible alors a n'est pas un diviseur de zéro.

Proposition 2.5.

Soit A un anneau et $a \in A$ un élément non nul.

1. *a est régulier à gauche si, et seulement si, l'application $x \mapsto ax$*

est injective,

2. *a est régulier à droite si, et seulement si, l'application $x \mapsto xa$ est injective,*

Démonstration :

1. Si a est régulier à gauche, et $x, x' \in A$ tels que $ax = ax'$, alors $a(x-x') = 0$, et donc $x - x' = 0$, d'où $x = x'$.
   Réciproquement, si l'application $x \mapsto ax$ est injective, et b un élément de A tel que $ab = 0$, donc $ab = a.0$, ainsi $b = 0$.

Définition 2.6.

Un anneau A est dit intègre s'il est commutatif et $A \neq \{0\}$ et pour tous $x, y \in A$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$

Remarque : Un anneau intègre est un anneau commutatif sans diviseurs de zéro.

Exemples :

1. $\mathbb{Z}$ est un anneau intègre.
2. L'anneau $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ n'est pas intègre, car $(1,0)(0,1) = (0,0)$.

Définition 2.7.

Soit A un anneau. On dit que $a \in A$ est un élément nilpotent, s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

Proposition 2.8.

Soit A un anneau.

1. *Si $a, b \in A$ sont nilpotents et $ab = ba$, alors ab est nilpotent.*
2. *Si $a, b \in A$ sont nilpotents et $ab = ba$, alors $a + b$ est nilpotent.*

Démonstration :

1. Soit $n, m \in \mathbb{N}^*$ tels que $a^n = b^m = 0$, on a $(ab)^{n+m} = a^{n+m}b^{n+m} = 0$, donc ab est nilpotent.
2. Soit $n, m \in \mathbb{N}^*$ tels que $a^n = b^m = 0$. Pour $N = \max(n, m)$, on a $a^N = b^N = 0$. En utilisant la formule du binôme de Newton, on obtient $(a+b)^{2N} = \sum_{k=0}^{n} \binom{k}{2N} a^k b^{2N-k}$. Pour $0 \leq k \leq N$, si $k \geq N$ alors $a^k = 0$. Si $0 \leq k < N$ alors $2N - k > N$ donc $b^{2N-k} = 0$. Dans les deux cas $a^k b^{2N-k} = 0$, par conséquent $(a+b)^{2N} = 0$, et donc $a+b$ est nilpotent.

Remarque : Soit A un anneau unitaire. Si a est nilpotent alors $1-a$ est inversible.

2.3 Corps

Définition 3.1.

Soit A un anneau unitaire non réduit à un élément. On dit que A est un corps si tout élément non nul est inversible. Si de plus la multiplication est commutative, on dit que A est un corps commutatif.

Exemples :

1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ muni des lois usuelles sont des corps.
2. $\mathbb{Z}$ n'est pas un corps, car $2 \in \mathbb{Z}$ mais $2^{-1} \notin \mathbb{Z}$.

Remarque :

1. Si K est un corps alors $K \setminus \{0\}$ (muni de la multiplication) est un groupe.
2. Si A est un corps commutatif alors A est intègre.

Définition 3.2.

Soit K un corps et K' une partie de K. On dit que K' est un sous corps de K si c'est un sous anneau unitaire de K et pour tout $x \in K' \setminus \{0\}$, $x^{-1} \in K'$.

Remarque :

1. Soit K un corps et K' une partie non vide de K. Alors K' est un sous corps de K si, et seulement si, pour tout $x, y \in K'^2$, $x - y \in K'$ et pour tout $(x, y) \in K' \times (K' \setminus \{0\})$, $xy^{-1} \in K'$.
2. Si K' est un sous corps de K, alors K' lui aussi est un corps.

2.4 Idéaux et anneaux quotient

Définition 4.1.

Soit A un anneau et I une partie de A.

1. *On dit que I est un idéal à gauche de A si $(I, +)$ est un sous groupe de $(A, +)$ et pour tout $a \in A$ et $x \in I$, $ax \in I$.*
2. *On dit que I est un idéal à droite de A si $(I, +)$ est un sous groupe de $(A, +)$ et pour tout $a \in A$ et $x \in I$, $xa \in I$.*
3. *Un idéal bilatère est un idéal à gauche et à droite.*

Exemples :

1. $\{0\}$ et A sont des idéaux bilatères de A dits idéaux triviaux de A.
2. $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ est un idéal bilatère de $\mathbb{Z}$.

Remarque :

1. Soit A un anneau unitaire et I un idéal de A. Alors $1 \in I$ si, et seulement si, $I = A$.
2. Si A est un anneaux commutatif, alors I est un idéal bilatère de A si, et seulement si, I est un idéal à gauche de A si, et seulement si, I est un idéal à droite de A. Ainsi, lorsque A est un anneau commutatif, il n'y a pas de différence entre idéal à gauche, à droite et bilatère.

Proposition 4.2.

Soit A un anneau.

1. *Si $(I_i)_{i \in X}$ est une famille d'idéaux à gauche (respectivement à droite) de A, alors $\cap_{i \in X} I_i$ est un idéal à gauche (respectivement*

à droite) de A.

2. *Si I et J sont deux idéaux à gauche (respectivement à droite) de A, alors $I+J=\{i+j \ / i\in I \ \text{ et } \ j\in J\}$ est un idéal à gauche (respectivement à droite) de A appelé la somme de I et J.*

Démonstration :

1. Le cas des idéaux à gauche : Notons d'abord que $\cap_{i\in X} I_i$ est un sous groupe de $(A,+)$ comme intersection de sous groupe de $(A,+)$. Soit $a\in A$ et $x\in\cap_{i\in X} I_i$. On a $\forall i\in X,\ i\in I_i$, donc $ax\in I_i$, par suite $ax\in\cap_{i\in X} I_i$.
2. Cas d'idéaux à gauche : On a $0=0+0\in I+J$. Soit $x=i+j\in I+J$ et $y=i'+j'\in I+J$ avec $i,i'\in I$ et $j,j'\in J$. On a $x-y=(i-i')+(j-j')\in I+J$, donc $I+J$ est un sous groupe de $(A,+)$.
   Soit $a\in A$ et $x=i+j\in I+J$ avec $i\in I$ et $j\in J$. On a $ax=ai+aj\in I+J$. Il vient alors que $I+J$ est un idéal à gauche de A.

Définition 4.3.

Soit A un anneau commutatif unitaire et S une partie de A. L'intersection de tous les idéaux de A contenant S est appelé l'idéal engendré par S et se note (S). Ainsi (S) est le plus petit idéal de A contenant S.

Remarques : Soit A un anneau commutatif.

1. $(\emptyset)=(\{0\})=\{0\}$.
2. $(A)=A$.

Proposition 4.4.

Soit A un anneau commutatif unitaire et S une partie non vide de A. Alors

$$(S)=\{\sum_{i=1}^{n} a_i s_i \ / \ n\in\mathbb{N},\ 1\leq\forall i\leq n,\quad a_i\in A, s_i\in S\}$$

Démonstration : Notons $J=\{\sum_{i=1}^{n} a_i s_i \ / \ n\in\mathbb{N},\ 1\leq\forall i\leq n,\quad a_i\in A, s_i\in S\}$.

Soit A un anneau commutatif unitaire et I,J deux idéaux de A. L'idéal engendré par les éléments de la forme ij où $i\in I$ et $j\in J$ est appelé l'idéal

produit de I et J et se note IJ.

Proposition 4.5.

Soit A un anneau commutatif unitaire et I, J deux idéaux de A. Alors

$$IJ = \left\{ \sum_{k=1}^{m} i_k j_k \ / \ m \geq 1, i_k \in I, \ j_k \in J \right\}$$

Définition 4.6.

Un idéal I d'un anneau commutatif unitaire A est dit principal s'il est engendré par un élément.
Un anneau est dit principal s'il est commutatif unitaire intègre et tout idéal de A est principal.

Exemple : $\mathbb{Z}$ est un anneau principal : Si I est un idéal de $\mathbb{Z}$, alors I est un sous groupe de $(\mathbb{Z}, +)$, comme les sous groupe de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, il existe alors $n \in \mathbb{N}$ tel que $I = n\mathbb{Z} = (n)$, donc I est principal.

Définition 4.7.

Soit A un anneau commutatif unitaire. Un idéal I de A est dit premier si $I \neq A$ et pour tout $(x, y) \in A^2$, $xy \in I \Rightarrow x \in I$ ou $y \in I$.

Exemples :

1. Soit p un nombre premier. Alors $p\mathbb{Z}$ est un idéal premier de Z : Clairement $p\mathbb{Z}$ est un idéal de $\mathbb{Z}$, soit $x, y \in \mathbb{Z}$ tels que $xy \in p\mathbb{Z}$, alors il existe $k \in \mathbb{Z}$ tel que $xy = kp$, en d'autres termes p divise xy, comme p premier alors p divise x ou p divise y, c'est-à-dire $x = kp$ ou $y = kp$ avec $k \in \mathbb{Z}$, ou encore $x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$.
2. Si A est un anneau commutatif intègre, alors (0) est un idéal premier de A.

Définition 4.8.

Soit A un anneau commutatif unitaire et I un idéal de A. On dit I est un idéal maximal de A si $I \neq A$ et si pour tout idéal J tel que $I \subseteq J$ on a, $J = I$ ou $J = A$.

Remarque : Si K est un corps alors l'idéal $\{0\}$ est maximal.

Proposition 4.9.

Soit A un anneau commutatif unitaire et I un idéal propre de A ($I \neq A$), les propriétés suivantes sont équivalentes :

1. *I idéal maximal de A,*
2. *Pour tout $x \in A \setminus I$, $A = (x) + I$.*

Démonstration : .....

Proposition 4.10.

Soit A un anneau commutatif unitaire. Tout idéal maximal de A est un idéal premier de A.

Démonstration : .....

Lemme de Zorn : Tout ensemble non vide inductif admet au moins un élément maximal.

Théorème 4.11. (Krull)

Soit A un anneau commutatif unitaire.
Tout idéal $I \neq A$ est contenu dans un idéal maximal.
Tout anneau commutatif unitaire non réduit à un élément contient au moins un idéal maximal.

Démonstration : (Lemme de Zorn)

Théorème et définition 4.12. (Anneau quotient)

Soit A un anneau unitaire, et I un idéal bilatère. L'ensemble quotient A/I muni des deux lois de compositions internes : $\overline{x}\,\overline{y} = \overline{xy}$ et $\overline{x} + \overline{y} = \overline{x+y}$ est un anneau unitaire, dit anneau quotient (de A par I).

Démonstration : Clairement $(A/I, +)$ est un groupe abélien. La multiplication est bien définie, en effet si $x, y, x', y' \in A$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $x = x' + i$ et $y = y' + j$ où $i, j \in I$. On a $xy = xy' + x'j + iy' + ij$, puisque I est un idéal bilatère, on a donc $x'j + iy' + ij \in I$, par suite $\overline{xy} = \overline{x'y'}$. Les propriétés d'anneau sont très simples à vérifier.

Théorème 4.13.

Soit A un anneau commutatif unitaire et I un idéal de A.

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

Démonstration : .....

2.5 Morphismes d'anneaux

Définition 5.1.

Soit A et B deux anneaux et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux si : pour tout $x, y \in A$, $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$.
Si A et B sont unitaires, f est dit morphisme d'anneaux unitaires si de plus $f(1) = 1$.
Un morphisme de corps est un morphisme d'anneaux unitaires.
Un isomorphisme est un morphisme bijectif.

Exemples :

1. L'application $f : \mathbb{C} \to \mathbb{C}$ définie par $f(z) = \overline{z}$ est un morphisme d'anneaux.
2. L'application $f : \mathbb{R}[X] \to \mathbb{R}$ définie par $f(P) = P(1)$ est un morphisme d'annaux.

3. Soit A un anneau et I un idéal bilatère de A. L'application $\varphi : A \to A/I$, définie par $\varphi(x) = \overline{x}$, est un morphisme d'anneaux.

Proposition 5.2.

Soit $f : A \to B$ un morphisme d'anneaux.

1. $f(0) = 0$,
2. *Pour tous $x, y \in A$, $f(x-y) = f(x) - f(y)$.*
3. *Si $x \in A$ est inversible alors $f(x)$ est inversible et $(f(x))^{-1} = f(x^{-1})$.*

Proposition 5.3.

Soit $f : A \to B$ et $g : B \to C$ deux morphismes d'anneaux. Alors $g \circ f : A \to C$ est un morphisme d'anneaux.

Proposition 5.4.

Soit $f : A \to B$ un morphisme d'anneaux commutatifs unitaires.

1. *Si I est un idéal de B, alors $f^{-1}(I)$ est un idéal de A,*
2. *Si I est un idéal premier de B, alors $f^{-1}(I)$ est un idéal premier de A.*

Démonstration : .....

Définition 5.5.

Soit $f : A \to B$ un morphisme d'anneaux.

1. *Le noyau de f est $\ker f = \{x \in A \ f(x) = 0\}$ c'est un idéal bilatère de A,*
2. *L'image de f est $\operatorname{Im} f = f(A)$ c'est un sous anneau de B.*

Proposition 5.6.

Soit $f : A \to B$ un morphisme d'anneaux et I un idéal bilatère de A tel que $I \subseteq \ker f$. Alors il existe un unique morphisme d'anneaux

$\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$, où $\pi : A \to A/I$ est la surjection canonique.

Démonstration : .....

Théorème 5.7. (Théorème d'isomorphisme)

Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Alors f induit un isomorphisme $\overline{f} : A/\ker f \to \operatorname{Im} f$ (où $\overline{f}(\overline{x}) = f(x)$).

Démonstration : .....

Théorème 5.8.

Soit A un anneau commutatif et I un idéal de A. L'application $\pi : A \to A/I$ induit une bijection entre les idéaux de A contenant I et les idéaux de A/I (via $J \mapsto \pi(J) = \overline{J}$).

Démonstration : .....

2.6 Caractéristique d'un anneau

Soit A un anneau commutatif unitaire, il existe un unique morphisme d'anneau $f : \mathbb{Z} \to A$, ce morphisme est définie par $f(k) = k1_A$. Il existe un unique $m \in \mathbb{N}$ tel que $\ker f = (m) = m\mathbb{Z}$.

Définition 6.1.

L'entier m s'appelle la caractéristique de A et se note $\operatorname{Car}(A)$.

Remarque : Si A est un anneau de caractéristique m, alors pour tout $a \in A$, $ma = 0$.

Exemple :

1. $\operatorname{Car}(\mathbb{R}) = 0$.
2. $\operatorname{Car}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 6.2.

Soit A un anneau commutatif unitaire de caractéristique m.

1. *Si $m=0$, le morphisme $\mathbb{Z}\to A$ est injectif,*
2. *Si $m>0$, le morphisme $\mathbb{Z}\to A$, induit un morphisme injectif $\mathbb{Z}/m\mathbb{Z}\to A$.*

Proposition 6.3.

Un anneau intègre est de caractéristique nulle ou un nombre premier.

2.7 Corps des fractions d'un anneau

Soit A un anneau commutatif unitaire intègre et $S=A\setminus\{0\}$.
On définit sur $A\times S$ la relation binaire $\sim$ par :

$$(a,s)\sim(b,t)\Leftrightarrow at=bs$$

On vérifie facilement qu'il s'agit d'une relation d'équivalence. La classe d'équivalence d'un couple (a,s) est notée $\frac{a}{s}$. Ainsi $A\times S/_\sim=\{\frac{a}{s}\ /\ a\in A\ ,\ s\in S\}$. Définissons sur $A\times S/_\sim$ deux opérations :

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}\ ,\quad \text{et}\quad \frac{a}{s}\times\frac{b}{t}=\frac{ab}{st}$$

Si $s,t\in S$, alors $st\in S$ car A est intègre. C'est deux opérations sont bien définies ne dépend pas des représentations des éléments.

Théorème et définition 7.1.

$(A\times S/_\sim,+,\times)$ est un corps commutatif appelé le corps des fractions de A et se note $\mathrm{Frac}(A)$, l'application $i:A\to\mathrm{Frac}(A)$, $i(a)=\frac{a}{1}$ est un morphisme d'anneaux injectif.

Exemples :

1. $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$,
2. $\mathrm{Frac}(\mathbb{K}[X])=\mathbb{K}(X)$.

Théorème 7.2.

Soit A un anneau commutatif intègre et K un corps commutatif. Si $f : A \to K$ est un morphisme d'anneaux injectif, alors il existe un unique morphisme de corps $g : \mathrm{Frac}(A) \to K$ tel que $g \circ i = f$.

2.8 Exercices

Exercice 2.1

Soit A un anneau unitaire tel que pour tout $x \in A$, $x^2 = x$.

1. *Montrer que pour tout $x \in A$, $2x = 0$.*
2. *Montrer que A est commutatif.*
3. *Montrer que si A est intègre alors $A \simeq Z/2Z$.*

Exercice 2.2

Soit $\mathbb{K}$ un corps commutatif et $A = \mathbb{K}[X]$. Soit I un idéal non nul de $\mathbb{K}[X]$.

1. *Montrer que l'ensemble $\{\deg P \ / P \in I \setminus \{0\}\}$ admet un plus petit élément p.*
   Soit $\pi \in I$ tel que $p = \deg \pi$.
2. *Montrer que $(\pi) \subseteq I$.*
3. *Montrer que $I = (\pi)$ (Ind : on pourra effectuer la division euclidienne).*
4. *En déduire que $\mathbb{K}[X]$ est un anneau principal.*

Exercice 2.3

Soit A un anneaux commutatif unitaire . On suppose que $A[X]$ est un anneau principal.

1. *Justifier que A est intègre.*
   Soit a un élément non nul de A.
2. *Montrer qu'il existe $P \in A[X]$ tel que $(a, X) = (P)$.*

3. *Montrer que P est un polynôme constant. On note c ce polynôme constant.*
4. *Montrer que c est inversible.*
5. *En déduire que A est un corps.*

Exercice 2.4

Soit A un anneau (commutatif unitaire) intègre fini. Montrer que A est un corps.

Exercice 2.5

Soit A un anneau commutatif unitaire . Si I et J sont des idéaux de A, on note IJ l'idéal engendré par $\{ij \ / \ i \in I \ , \ j \in J\}$.

1. *Montrer que $IJ = \{i_1 j_1 + \ldots + i_n j_n \ / n \geq 1, \ \ i_k \in I \ , \ j_k \in J\}$.*
2. *Montrer que $IJ \subseteq I \cap J$.*
3. *Montrer que si $I + J = A$ alors $IJ = I \cap J$.*

Exercice 2.6 (Idéaux bilatères de $\mathscr{M}_n(\mathbb{K})$)

Soit I un idéal bilatère non nul de $\mathscr{M}_n(\mathbb{K})$.
On note E_{ij} la matrice élémentaire dont tous les coefficients sont nuls, sauf le coefficient d'indice (i,j) qui vaut 1.

1. *Que vaut $E_{ij}E_{kl}$.*
2. *Soit $A = (a_{ij})$ une matrice non nulle de I. Calculer $E_{ij}AE_{kl}$.*
3. *Montrer que pour tout i, j, $E_{ij} \in I$.*
4. *En déduire que $I = \mathscr{M}_n(\mathbb{K})$.*

Exercice 2.7

Soit A un anneau commutatif unitaire . Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A \ / \exists n \in \mathbb{N} \ \ tel \ que \ \ x^n \in I\}$.

1. *Montrer que $\sqrt{I}$ est un idéal de A contenant I.*

2. *Montrer que* $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. *Soient* I, J *deux idéaux de* A, *montrer que si* $I \subseteq J$ *alors* $\sqrt{I} \subseteq \sqrt{J}$.
4. *Monter que* $\sqrt{I} = A$ *si, et seulement si,* $I = A$.
5. *Soient* I, J *deux idéaux de* A. *Montrer que* $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
6. *Montrer que si* I *est un idéal premier alors* $\sqrt{I} = I$.
7. *Montrer que* $\overline{0}$ *est le seul élément nilpotent de* $A/\sqrt{I}$.

Exercice 2.8

Soit A *une algèbre commutative intègre de dimension* $n \geq 2$ *sur* $\mathbb{R}$. *Soit* a *un élément non nul de* A.

1. *Montrer que* $I_a = \{P \in \mathbb{R}[X] \ / P(a) = 0\}$ *est un idéal de* $\mathbb{R}[X]$. *En déduire qu'il existe un polynôme unitaire de degré minimmal* $Q_a \in \mathbb{R}[X]$ *tel que* $Q_a(a) = 0$.
2. *Montrer que* $\deg Q_a \leq 2$.
3. *Montre que* A *est un corps.*
4. *Montrer qu'il existe* $\alpha \in A$ *tel que* $\alpha \notin \text{Vect}(1)$.
5. *Montrer que* $\deg Q_\alpha = 2$.
6. *Montrer qu'il existe* $\beta \in A$ *tel que* $\beta^2 = -1$.
7. *En déduire que* A *est isomorphe à* $\mathbb{C}$.

Exercice 2.9

Soit A *un anneau principal. Montrer que tout idéal premier non nul de* A *est maximal.*

Exercice 2.10

Soit A *un anneau (commutatif unitaire) intègre de caractéristique* $p > 0$.

1. *Montrer que pour tout* $1 \leq k \leq p-1$, p *divise* C_p^k.
2. *Soient* $x, y \in A$. *Montrer que* $(x+y)^p = x^p + y^p$.

3. *En déduire que $x \mapsto x^p$ est un morphisme d'anneaux.*

Exercice 2.11 (Idéaux maximaux de $\mathscr{C}(X,\mathbb{R})$)

Soit X un espace topologique compact et $A = \mathscr{C}(X,\mathbb{R})$ l'anneau des applications continues de X dans $\mathbb{R}$.

1. *Soit $x_0 \in X$. Montrer que $M_{x_0} := \{f \in A / \ f(x_0) = 0\}$ est un idéal maximal de A.*
2. *Soit M un idéal maximal de A. On suppose que pour tout $x \in X$, il existe $f_x \in M$ telle que $f_x(x) \neq 0$.*
   (a) *Montrer que pour tout $x \in X$, il existe un voisinage V_x de x tel que f_x ne s'annule pas sur V_x.*
   (b) *Montrer qu'il existe $x_1, \ldots, x_n \in X$ tels que $V_{x_1} \cup \ldots \cup V_{x_n} = X$.*
   (c) *Soit $f = f_{x_1}^2 + \ldots + f_{x_n}^2$. Montrer que f est inversible. Puis trouver une contradiction.*
3. *Montrer que tout idéal maximal de M de A de la forme M_{x_0}.*
4. *Soit I un idéal propre de A. Montrer qu'il existe $x \in X$ tel que pour tout $f \in I$, $f(x) = 0$.*

Exercice 2.12

Soit $f : K \to K'$ un morphisme de corps commutatifs. Montrer que f est injectif.

Exercice 2.13

1. *Soit $P \in \mathbb{R}[X]$ tel que $P(i) = 0$. Montrer que $X^2 + 1$ divise P.*
2. *Montrer que $\mathbb{R}[X]/(X^2+1)$ est isomorphe à $\mathbb{C}$. (considérer l'application $P \mapsto P(i)$).*

Exercice 2.14

Soit K un corps commutatif fini de caractéristique p.

1. *Montrer que p est un nombre premier.*
   On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
2. *Montrer que K est un $\mathbb{F}_p$-espace vectoriel.*
3. *Montrer que que $\text{Card}(K) = p^n$ où n est un entier à déterminer.*

Exercice 2.15

Soit A un anneau commutatifs unitaire et I, J deux idéaux de A. Soit $f : A \to A/I \times A/J$ l'application définie par $f(x) = (\overline{x}, \overline{x})$.

1. *Montrer que f est un morphisme d'anneaux.*
2. *Déterminer $\ker f$.*
3. *On suppose que $I+J = A$, montrer que $A/(I \cap J)$ est isomorphisme à $A/I \times A/J$.*

Exercice 2.16

Soit p un nombre premier.

1. *Montrer que $\sqrt{p} \notin \mathbb{Q}$.*
2. *Soit $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{5} / \ / a, b \in \mathbb{Q}\}$. Montrer que $\mathbb{Q}[\sqrt{5}]$ est isomorphisme à $\mathbb{Q}[X]/(X^2 - 5)$.*

Exercice 2.17

Soient $A_1, \ldots, A_n$ des anneaux commutatifs unitaires et $A = A_1 \times A_2 \times \ldots \times A_n$.

1. *Montrer que si $I_1, \ldots, I_n$ sont respectivement des idéaux de $A_1, \ldots, A_n$, alors $I = I_1 \times \ldots I_n$ est un idéal de A.*
2. *Montrer que si I est un idéal de A alors ils existent $I_1, \ldots, I_n$ des idéaux respectivement de $A_1, \ldots, A_n$ tels que $I = I_1 \times \ldots \times I_n$.*
3. *Soit $P = I_1 \times \ldots \times I_n$ un idéal premier de A.*
   (a) *Montrer qu'il existe j tel que $1 \notin I_j$.*
   (b) *Montrer que si $i \neq j$, alors $I_i = A_i$.*

(c) Montrer que I_j est un idéal premier de A_j.

Chapitre 3

Arithmétique dans les anneaux commutatifs

Dans toute la suite A est un anneau commutatif unitaire intègre.

3.1 Divisibilité

Définition 1.1.

Soit $a, b \in A$. On dit que a divise b et on note $a|b$, s'il existe $c \in A$ tel que $b = ca$.

Définition 1.2.

Soit $a, b \in A$. On dit que a est associé à b et on note $a \sim b$, s'il existe $u \in U(A)$ (inversible) tel que $a = ub$.

Remarque : La relation " $\sim$ " est une relation d'équivalence sur A.

Proposition 1.3.

Soit $a, b \in A$. Les propriétés suivantes sont équivalentes :

1. *a et b sont associés,*
2. *$a|b$ et $b|a$,*
3. *$(a) = (b)$.*

Démonstration : .....

3.2 PGCD et PPCM

Définition 2.1.

Soient $a_1,\dots,a_n \in A$ et $d \in A$. On dit que d est un plus grand commun diviseur des éléments $a_1,\dots,a_n$ et on écrit $d = \text{pgcd}(a_1,\dots,a_n)$ si :

1. *Pour tout $1 \le i \le n$, $d|a_i$,*
2. *Si $a \in A$ tel que, pour tout $1 \le i \le n$, $a|a_i$, alors $a|d$.*

Remarque : Le cas de $n = 2$: d est un pgcd de a et b si, et seulement si, $d|a$, $d|b$ et pour tout $x \in A$ tel que $x|a$ et $x|b$ alors x divise d.

Proposition 2.2.

Soit $a_1,\dots,a_n \in A$. Si d et d' sont deux pgcd de $a_1,\dots,a_n$ alors d et d' sont associés. En particulier le pgcd lorsqu'il existe est unique modulo la relation " $\sim$ ".

Démonstration : Comme d' divise les éléments $a_1,\dots,a_n$, il vient que d' divise d, de même d divise d'. Donc d et d' sont associés.

Théorème 2.3.

Soit $a_1,\dots,a_n \in A$. Si l'idéal $(a_1,\dots,a_n)$ est principal alors $a_1,\dots,a_n$ admet un pgcd et dans ce cas on a, $(a_1,\dots,a_n) = (\text{pgcd}(a_1,\dots,a_n))$.

Démonstration : .....

Exemples :

1. a est un pgcd de a et 0,
2. Si u est un élément inversible 1 est un pgcd de a et u.

Définition 2.4.

Soient $a_1,\dots,a_n \in A$ et $m \in A$. On dit que m est un plus petit commun multiple des éléments $a_1,\dots,a_n$ et on écrit $m = \text{ppcm}(a_1,\dots,a_n)$ si :

1. *Pour tout $1 \le i \le n$, $a_i | m$,*
2. *Si $a \in A$ tel que, pour tout $1 \le i \le n$, $a_i | a$ alors $m | a$.*

Remarque : Le cas de $n = 2$: m est un ppcm de a et b si, et seulement si, $a|m$, $b|m$ et pour tout $x \in A$ tel que $a|x$ et $b|x$ alors m divise x.

Proposition 2.5.

Soit $a_1,\dots,a_n \in A$. Si m et m' sont deux ppcm de $a_1,\dots,a_n$ alors m et m' sont associés. En particulier le ppcm lorsqu'il existe est unique modulo la relation " $\sim$ ".

Démonstration : Puisque chaque a_i divise m', il vient que m divise m', de même m' divise m. Donc m et m' sont associés.

Théorème 2.6. (une caractérisation du ppcm)

Soient $a_1,\dots,a_n \in A$. Alors $a_1,\dots,a_n$ admettent un ppcm si, et seulement si, l'idéal $\cap_{i=1}^{n}(a_i)$ est principal. Dans ce cas on a, $\cap_{i=1}^{n}(a_i) = (\text{ppcm}(a_1,\dots,a_n))$.

Démonstration : .....

Théorème 2.7.

Soit A un anneau principal et $a_1,\dots,a_n \in A$. alors d est un pgcd de $a_1,\dots,a_n$ si, et seulement si, $(a_1,\dots,a_n) = (d)$.

Démonstration : .....

Corollaire 2.8.

Soit A un anneau principal. Toute famille $a_1,\dots,a_n$ a un pgcd et un ppcm.

Démonstration : Conséquence du fait que les deux idéaux $(a_1,\dots,a_n)$ et $\cap_{i=1}^{n}(a_i)$ sont des idéaux principaux.

Définition 2.9.

Soit $a_1,\dots,a_n \in A$. On dit que $a_1,\dots,a_n$ sont premiers entre eux si $\text{pgcd}(a_1,\dots,a_n)$ *existe et vaut* 1.

Théorème 2.10. (Bézout)

Soit A un anneau principal et $a_1,\dots,a_n \in A$. Alors $a_1,\dots,a_n$ sont premier entre eux si, et seulement si, il existe $u_1,\dots,u_n \in A$ tels que $u_1a_1+\dots+u_na_n=1$.

Démonstration :

Proposition 2.11. (Lemme de Gauss)

Soit A un anneau principal. Si a divise bc et a premier avec b, alors a divise c.

Démonstration : .....

3.3 Élément irréductible et élément premier

Définition 3.1.

Soit $a \in A$. On dit que a est irréductible si :

1. *a non nul et non inversible,*
2. *Si $a=bc$ alors b est inversible ou c est inversible, c'est-à-dire les seuls diviseurs de a sont les éléments inversible et les éléments associés à a.*

Exemples :

1. Les éléments irréductible de $\mathbb{Z}$ sont les nombres premiers.
2. Le théorème de D'Alembert-Gauss assure que les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Définition 3.2.

Soit $a \in A$. On dit que est premier si :

1. *a non nul et non inversible,*
2. *Si $a|bc$ alors $a|b$ ou $a|c$.*

Théorème 3.3.

Soit $a \in A$. Les propriétés suivantes sont équivalentes :

1. *a premier,*
2. *$a \neq 0$ et (a) est un idéal premier,*
3. *$a \neq 0$ et $A/(a)$ est intègre.*

Démonstration : .....

Proposition 3.4.

Soit $a \in A$. Si a est premier alors a est irréductible.

Démonstration : .....

Corollaire 3.5.

Dans un anneau principal, toute idéal premier non nul est maximal.

Démonstration : .....

Proposition 3.6.

Dans un anneau principal un élément est premier si et seulement s'il est irréductible.

Démonstration :

3.4 Anneau euclidien

Définition 4.1.

On dit que A est un anneau euclidien, s'il existe une application $\varphi : A\setminus\{0\} \to \mathbb{N}$, dite statheme, vérifiant : pour tout $(a,b) \in A^2$ avec $b \neq 0$, il existe un couple $(q,r) \in A^2$ tel que $a = bq + r$ et ($r = 0$ ou $\varphi(r) < \varphi(b)$).

Exemples :

1. L'anneau $\mathbb{Z}$ est euclidien ($\varphi = |.|$).
2. L'anneau $\mathbb{K}[X]$ est euclidien ($\varphi = \deg$).

Proposition 4.2.

Tout anneau euclidien est principal.

Démonstration : .....

3.5 Anneau factoriel

Définition 5.1.

Un anneau A est factoriel si :

1. *Pour tout élément non nul et non inversible a, il existent $p_1, \ldots, p_r$ irréductibles tels que $a = p_1 \ldots p_r$,*
2. *La décomposition en irréductible est unique au inversible près, c'est-à-dire : si $a = p_1 \ldots p_r = q_1 \ldots q_s$ où p_i et q_j sont irréductibles alors $r = s$ et pour tout i il existe j tel que p_i et q_j soient associés.*

Exemple : L'anneau $\mathbb{Z}$ est factoriel.

Proposition 5.2.

Soit A un anneau factoriel et $a \in A$. Alors a est irréductible si, et seulement si, a est premier.

Démonstration : Un élément premier et irréductible.
Considérons un élément irréductible x et montrons que x est premier. Par hypothèse x est non nul et non inversible. Supposons que x divise un produit ab avec a et b non nuls et non inversibles, car le cas ou l'un des éléments a et b est nul ou inversible, est trivial. Il existe donc c tel que $xc = ab$. Si l'un des éléments a ou b est nul, alors dans ce cas x divise a ou x divise b. Si a et b sont non nuls. On écrit la décomposition de a, b et c en irréductible $a = a_1 \dots a_r$, $b = b_1 \dots b_s$ et $c = c_1 \dots c_l$ où a_i, b_j et c_k sont irréductibles. On a donc $xc_1 \dots c_l = a_1 \dots a_r . b_1 \dots b_s$. On en déduit par l'unicité de la décomposition que x est associés à l'un des a_i ou à l'un des b_j, donc x divise a ou x divise b.

Théorème 5.3.

A est un anneau factoriel si, et seulement si,

1. *Toute suite croissante d'idéaux principaux et stationnaire, et*
2. *Toute élément irréductible de A est premier.*

Démonstration : Supposons que A est un anneau factoriel. D'après la proposition précédente, tout élément premier est irréductible. Considérons $(I_n)_n$ une suite croissante d'idéaux principaux de A ($I_n \subseteq I_{n+1}$) et supposons qu'il n'est pas stationnaire. Quitte à extraire de cette suite une suite strictement croissante on peut supposer qu'il est strictement croissante. Pour chaque $n \in \mathbb{N}$ il existe $a_n \in A$ tel que $I_n = (a_n)$. L'élément a_1 est non nul et non inversible, car si $a_1 = 0$ dans ce cas $a_0 = 0$ et donc $I_0 = I_1$, et si a_1 est inversible alors $I_1 = A$ et par suite $I_n = A$ pour $n \geq 1$. Comme A est un anneaux factoriel il existe $q_1, \dots, q_m$ irréductibles tel que $a_1 = q_1 \dots q_m$, on peut écrire alors a_1 sous la forme $a = p_1^{s_1} \dots p_r^{s_r}$ où $p_1, \dots, p_r$ sont irréductibles et deux à deux non associés et $s_1, \dots, s_r$ des entiers naturels. Puisque $(a_1) \subsetneq (a_2)$, a_2 est alors un diviseur de a_1, donc a_2 est de la forme $a_2 = u_2 p_1^{s_{1,2}} \dots p_r^{s_{r,2}}$, où u_2 inversible , $s_{k,2}$ sont des entiers tels que $s_{k,2} \leq s_k$ et l'une des inégalités est stricte (car a_1 et a_2 ne sont pas associés). Pour chaque n, $a_n = u_n p_1^{s_{1,n}} \dots p_r^{s_{r,n}}$. Comme $(a_n) \subsetneq (a_{n+1})$, on a donc $s_{k,n} \leq s_{k,n+1}$ et l'une des inégalités est stricte. Pour

$n \in \mathbb{N}$, si on pose $t_n = \sum_{k=1}^{r} s_{k,n}$, alors $(t_n)_n$ est une suite strictement décroissante d'entiers naturels, ce qui est absurde.
Réciproquement, on suppose que A vérifie les deux conditions 1. et 2. Soit a un élément non nul et non inversible de A, et supposons que a n'est pas décomposable en irréductibles. Alors a lui même n'est pas un élément irréductible, on peut donc le décomposé en produit $a = a_1 b_1$ avec a_1 et b_1 non inversible. Si a_1 et b_1 étaient tous deux décomposables en produits d'irréductibles, cela fournirait une telle décomposition de a, donc l'un des éléments a_1, b_1 n'admet pas non plus de décomposition, supposons qu'il s'agit de a_1. Comme $a = a_1 b_1$ et b_1 non inversible, on a donc $(a) \subsetneq (a_1)$. Et, on peut recommencer le même raisonnement avec $a_1 = a_2 b_2$, a_2, b_2 non inversibles et a_2 n'admet pas de décomposition en produit d'irréductibles. Ainsi de suite, on peut fabriquer une chaine d'idéaux $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ et donc non stationnaire.
Supposons que $a = up_1 \dots p_s = vq_1 \dots q_r$ où u, v sont inversibles et p_i, q_j sont irréductibles. De cette égalité, on déduit que p_1 divise le produit $vq_1 \dots q_r$, comme p_1 est premier, il divise alors l'un des q_j, et peut supposer que p_1 divise q_1, il existe alors u_1 inversible tel que $p_1 = u_1 q_1$. L'égalité se ramène alors, après simplification possible parce que A est intègre à $uu_1 p_2 \dots p_s = vq_1 \dots q_r$. On conclut donc par récurrence descendante sur le nombre d'irréductibles.

Proposition 5.4.

Un anneau principal est factoriel.

Démonstration : Soit A un anneau principal. Tout élément irréductible est premier. Soit $(I_n)_n$ une suite croissante d'idéaux principaux de A. Posons $I = \cup_{n\in\mathbb{N}} I_n$, c'est un idéal de A donc principal. Soit $a \in A$ tel que $I = (a)$, puisque $a \in \cup_n I_n$, il existe $m \in \mathbb{N}$ tel que $a \in I_m$. On a donc $I_m = I_{m+1} = \dots$, donc la suite est stationnaire.

Proposition 5.5.

Soit A un anneau factoriel. Toute famille $a_1, \dots, a_n$ d'éléments de A admet un pgcd et un ppcm.

Démonstration : .....

3.6 Exercices

Exercice 3.1

Soit A un anneaux commutatif unitaire intègre. Soit a un élément non nul et non inversible de A. Montrer que a est irréductible si, et seulement si, (a) est maximal parmi les idéaux principaux de A.

Exercice 3.2

Soit A un anneau commutatif intègre. Soit a et b deux éléments non nuls de A et on suppose qu'ils ont un ppcm m.

1. *Montrer que m divise ab.*
2. *Soit $d \in A$ tel que $ab = md$. Montrer que d est un pgcd de a et b.*

Exercice 3.3

Soit $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \ / \ a, b \in \mathbb{Z}\}$.

1. *Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous anneau de $\mathbb{C}$. Justifier qu'il est intègre.*
   Soit $N : \mathbb{Z}[i\sqrt{5}] \to \mathbb{N}$ l'application définie par $N(z) = z\overline{z} = |z|^2$.
2. *Soit $z = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ un élément inversible.*
   (a) *Montrer que $a^2 + 5b^2 = 1$.*
   (b) *En déduire le groupe des éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$.*
   (c) *Montrer que $2 + i\sqrt{5}$ est irréductible.*
   (d) *Montrer que $2 + i\sqrt{5}$ ne divise pas 3.*
   (e) *En déduire que $2 + \sqrt{5}$ n'est pas premier.*
   (f) *En déduire que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.*

Exercice 3.4

Soit A un anneau euclidien (qui n'est pas un corps) et $v : A \setminus \{0\} \to \mathbb{N}$ le stathme associé.

1. *Montrer que que $\{v(x) \ / \ x$ non nul et non inversible$\}$ admet un*

plus petit élément $v(a)$.

2. *Montrer que l'application $A^\times \cup \{0\} \to A/(a)$ est surjectif.*
3. *Montrer que $A/(a)$ est un corps.*

Exercice 3.5

Soit A un anneau factoriel.

1. *Soit a un élément non nul de A et p un élément irréductible. Montrer qu'il existe un entier k tel que p^k divise a et p^{k+1} ne divise pas a. Cet entier se note $v_p(a)$.*
2. *Soit $a \in A$ non nul et $p_1, \dots, p_r$ les diviseurs irréduclibles deux à deux non associés de a. Montrer que $a = u p_1^{v_{p_1}} \dots p_r^{v_{p_r}}$.*
3. *Soit $a, b \in A$ non nuls. Montrer que a divise b si, et seulement si, pour tout élément irréductible p, $v_p(a) \leq v_p(b)$.*
4. *Pour $a, b \in A$ non nuls et p irréductible. Montrer que $v_p(ab) = v_p(a) + v_p(b)$.*
5. *Soit $a, b \in A$ non nuls. Montrer que a et b sont premier entre eux si, et seulement si, pour tout élément irréductible p, $v_p(a)v_p(b) = 0$.*

Exercice 3.6

Soit A un anneaux factoriel et $K = \mathrm{Frac}(A)$.

1. *Soit $x \in K$ non nul. Montrer qu'il existe deux éléments a et b de A premiers entre eux tels que $x = \dfrac{a}{b}$.*
2. *Soit $x \in K$, et on suppose qu'il existe un polynôme unitaire P à coefficients dans A tel que $P(x) = 0$. Montrer que $x \in A$.*

Exercice 3.7

Soit A un anneau intègre tel que pour tous $a, b \in A$, a divise b ou b divise a.

1. *Montrer que l'ensemble des idéaux principaux de A est totalement ordonné par l'inclusion.*
2. *Soit $x \in K = \mathrm{Frac}(A)$. Montrer que $x \in A$ ou $x^{-1} \in A$.*
3. *Soit I et J deux idéaux de A. Montrer que $I \subseteq J$ ou $J \subseteq I$.*
4. *Montrer si I est un idéal de A engendré par un nombre fini d'éléments. Alors I est principal.*

Exercice 3.8

Soit A un anneau commutatif unitaire.

1. *On suppose que A possède un seul idéal maximal M. Montre que $M = A \setminus A^\times$.*
2. *On suppose que $A \setminus A^\times$ est un idéal de A. Montrer que $A \setminus A^\times$ est un idéal maximal de A et c'est le seul idéal maximal de A.*

Chapitre 4

Polynômes à plusieurs indéterminées

Dans tout le chapitre A désigne un anneau commutatif unitaire.

4.1 Anneau de polynômes à coefficients dans un anneau

Soit A un anneau commutatif unitaire. On appelle polynôme à une indéterminée à coefficients dans A toute suite presque nulle d'éléments de A, c'est-à-dire une suite $P = (a_n)_{n\in\mathbb{N}}$ telle qu'il existe un entier $N \in \mathbb{N}$ vérifiant $a_n = 0$ pour tout $n \geq N$. L'ensemble de ces suites est noté $A[X]$. On le munit d'une structure d'anneau au moyen des opérations suivantes :

- Addition : $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$
- Multiplication (Produit de Cauchy) : $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$ où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

Notation standard et Indéterminée :
En identifiant chaque élément $a \in A$ avec la suite $(a, 0, 0, \ldots)$, on injecte A dans $A[X]$. On définit l'indéterminée X comme la suite $(0, 1, 0, 0, \ldots)$. Par produit de Cauchy, on montre par récurrence que X^k est la suite dont le seul terme non nul vaut 1 à l'indice k.
Tout polynôme $P = (a_n)_{n\in\mathbb{N}}$ s'écrit alors de manière unique sous la forme d'une somme finie :

$$P = \sum_{k=0}^{d} a_k X^k = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Proposition 1.1.

Si A est un anneau intègre alors il en est de même pour $A[X]$.

Démonstration : .....

Degré et ses propriétés sur un anneau :

Si $P \neq 0$, le degré de P, noté $\deg(P)$, est le plus grand entier n tel que $a_n \neq 0$. Par convention, $\deg(0) = -\infty$. Le coefficient $a_{\deg(P)}$ est appelé le coefficient dominant. Si ce coefficient vaut 1, le polynôme est dit unitaire.

Proposition 1.2.

Soient $P, Q \in A[X]$.

1. $\deg(P+Q) \leq \max(\deg(P),$
2. $\deg(Q))\deg(P \cdot Q) \leq \deg(P) + \deg(Q)$.

Démonstration : .....

Remarque : Si A n'est pas intègre, l'inégalité du produit peut être stricte. Par exemple, dans $\mathbb{Z}/4\mathbb{Z}[X]$, si $P = 2X$ et $Q = 2X$, on a $\deg(P) = 1$ et $\deg(Q) = 1$, mais $P \cdot Q = 4X^2 = 0$, donc $\deg(P \cdot Q) = -\infty$. Cependant, si A est un anneau intègre, alors $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ et l'anneau $A[X]$ est lui aussi intègre.

4.2 Polynômes à plusieurs indéterminées

Soit $n \in \mathbb{N}^*$. On définit l'anneau des polynômes à n indéterminées, noté $A[X_1, X_2, \ldots, X_n]$, par récurrence sur n :

- Pour $n = 1$, c'est l'anneau $A[X_1]$ défini à la section 1.
- Pour $n \geq 2$, on pose : $A[X_1, \ldots, X_{n-1}, X_n] = \big(A[X_1, \ldots, X_{n-1}]\big)[X_n]$

Un polynôme à n indéterminées est donc simplement un polynôme en l'indéterminée X_n dont les coefficients sont eux-mêmes des polynômes à $n-1$ indéterminées $X_1, \ldots, X_{n-1}$.

Écriture canonique : Pour manipuler symétriquement les variables, on utilise les éléments de $\mathbb{N}^n$. Un multi-indice est un uplet $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$. Pour $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$, on note X^α le monôme défini par :

$$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$$

Tout polynôme $P \in A[X_1,\dots,X_n]$ s'écrit de manière unique sous la forme d'une somme finie :

$$P = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha = \sum_{(\alpha_1,\dots,\alpha_n)} a_{\alpha_1,\dots,\alpha_n} X_1^{\alpha_1}\dots X_n^{\alpha_n}$$

où les coefficients a_α appartiennent à A et sont presque tous nuls. Autrement dit $P = \sum_{\alpha\in S} a_\alpha X^\alpha$, où $S \subseteq \mathbb{N}^n$ est une partie finie.

Notions de Degrés : Contrairement au cas à une variable, il existe plusieurs façons de définir le degré d'un polynôme à plusieurs variables.

- **Degré partiel :** Le degré partiel de P par rapport à la variable X_i, noté $\deg_{X_i}(P)$, est le degré de P vu comme un polynôme en la seule variable X_i à coefficients dans $A[X_1,\dots,X_{i-1},X_{i+1},\dots,X_n]$.
- **Degré total :** Soit un monôme non nul $a_\alpha X^\alpha$. On appelle longueur ou degré du multi-indice la quantité $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Le degré total de P (souvent appelé simplement "le degré") est défini par : $\deg(P) = \max\{|\alpha| \in \mathbb{N} \mid a_\alpha \neq 0\}$

4.3 Polynômes homogènes

Définition 3.1.

Un polynôme $P \in A[X_1,\dots,X_n]$ est dit homogène de degré d si tous ses monômes constitutifs ont un degré total exactement égal à d. C'est-à-dire : $P = \sum_{|\alpha|=d} a_\alpha X^\alpha$.

Exemple : .....

Théorème 3.2.

Tout polynôme P de degré d s'écrit de manière unique comme une somme finie de polynômes homogènes :$P = P_0 + P_1 + \cdots + P_d$ où chaque P_k est soit nul, soit homogène de degré k.

Démonstration : .....

On définit la dérivée partielle formelle par rapport à X_i par ;

- $\frac{\partial}{\partial X_i}(X_1^{\alpha_1}\dots X_i^{\alpha_i}\dots X_n^{\alpha_n}) = \alpha_i X_1^{\alpha_1}\dots X_i^{\alpha_i-1}\dots X_n^{\alpha_n}$
- Si $P = \sum_{\alpha\in S} a_\alpha X^\alpha$, par définition $\frac{\partial}{\partial X_i}(P) = \sum_{\alpha\in S} a_\alpha \frac{\partial}{\partial X_i}(X^\alpha)$.

Exemples : .....

Théorème 3.3. (Formule d'Euler)

Soit $P \in A[X_1,\dots,X_n]$ un polynôme homogène de degré d. Alors on a l'identité suivante :

$$\sum_{i=1}^{n} X_i \frac{\partial P}{\partial X_i} = d \cdot P$$

4.4 Formule de Taylor

Pour tout multi-indice $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}^n$, on définit :

- La factorielle de multi-indice : $\alpha! = \alpha_1! \times \alpha_2! \times \cdots \times \alpha_n!$.
- L'opérateur différentiel d'ordre supérieur : $\partial^\alpha = \frac{\partial^{|\alpha|}}{\partial X_1^{\alpha_1} \dots \partial X_n^{\alpha_n}}$.

Exemple : $P(X,Y) = X^3Y^2 + Y^5$, $\alpha = (2,1)$, ...

Théorème 4.1.

oit $\mathbb{K}$ un corps de caractéristique nulle. Soit $P \in A[X_1,\dots,X_n]$ un polynôme de degré total inférieur ou égal à d et $a = (a_1,\dots,a_n) \in A^n$, alors :

$$P(X_1,\dots,X_n) = \sum_{|\alpha| \le d} \frac{\partial^\alpha P(a_1,\dots,a_n)}{\alpha!} (X-a)^\alpha$$

où $(X-a)^\alpha = (X_1-a_1)^{\alpha_1} \dots (X_n-a_n)^{\alpha_n}$.

4.5 Exercices

Exercice 4.1

Soit A un anneau intègre. Déterminer les éléments inversibles de l'anneau $A[X_1,\dots,X_n]$.

Exercice 4.2

Soit A un anneau. Soit $(x_1,\dots,x_n)\in A^n$. On considère l'application $\phi : A[X_1,\dots,X_n]\to A$ définie par $\phi(P)=P(x_1,\dots,x_n)$.

1. *Montrer que ϕ est un morphisme d'anneaux.*
2. *Caractériser son noyau dans le cas $n=2$ pour $x_1=0, x_2=0$.*

Exercice 4.3

Soient P et Q deux polynômes non nuls de $A[X_1,\dots,X_n]$, homogènes de degrés respectifs d et m. Montrer que PQ est homogène de degré $d+m$.

Exercice 4.4

Soit $\mathbb{K}$ un corps infini ($\mathbb{R}$, $\mathbb{C}$...). Soit $P\in\mathbb{K}[X_1,\dots,X_n]$. Montrer que P est homogène de degré d si et seulement si pour tout $t\in\mathbb{K}$, $P(tX_1,\dots,tX_n)=t^dP(X_1,\dots,X_n)$.

Exercice 4.5

Soit $P\in\mathbb{R}[X,Y]$ un polynôme vérifiant l'identité $X\frac{\partial P}{\partial X}+Y\frac{\partial P}{\partial Y}=d\cdot P$ pour un certain entier $d\in\mathbb{N}$. Montrer que P est homogène de degré d.

Exercice 4.6

Soit $A=(\mathbb{Z}/3\mathbb{Z})[X,Y]$. Soit $P(X,Y)=X^3+Y$.

1. *Calculer $X\frac{\partial P}{\partial X}+Y\frac{\partial P}{\partial Y}$.*
2. *Montrer que P vérifie l'identité d'Euler pour un certain degré d alors qu'il n'est pas homogène.*

Exercice 4.7

Soit $\mathbb{K}$ un corps et $I=\{P\in\mathbb{K}[X_1,\dots,X_n]\mid P(0,\dots,0)=0\}$.

1. *Montrer que I est l'idéal engendré par la famille $\{X_1,\dots,X_n\}$.*

2. *Montrer que l'anneau quotient $\mathbb{K}[X_1,\dots,X_n]/I$ est isomorphe à $\mathbb{K}$. Qu'en déduit-on pour I ?*

Exercice 4.8

Soit $I=(X,Y)$ dans l'anneau $\mathbb{K}[X,Y]$. Montrer que I n'est pas principal.

Exercice 4.9

Soit $\mathbb{K}$ un corps infini. Soit $P\in\mathbb{K}[X_1,\dots,X_n]$. On suppose que pour tout $(x_1,\dots,x_n)\in\mathbb{K}^n$, $P(x_1,\dots,x_n)=0$. Montrer par récurrence sur n que P est le polynôme nul.

Exercice 4.10

Soit $P(X,Y)=X^3-2XY+Y^2+1\in\mathbb{R}[X,Y]$. Écrire le développement de Taylor exact de P au point $a=(1,2)$.

Exercice 4.11

Soit $P\in\mathbb{R}[X_1,\dots,X_n]$ un polynôme de degré $\leq d$. Montrer à l'aide de la formule de Taylor que si toutes les dérivées partielles de P de tout ordre (y compris l'ordre 0) s'annulent à l'origine $(0,\dots,0)$, alors P est le polynôme nul.

Exercice 4.12

Soit A un anneau commutatif unitaire. Soit $I=\langle X_1,\dots,X_k\rangle$ l'idéal de $A[X_1,\dots,X_n]$ engendré par les k premières indéterminées (avec $1\leq k\leq n$).

1. *Montrer que l'anneau quotient $A[X_1,\dots,X_n]/I$ est isomorphe à $A[X_{k+1},\dots,X_n]$.*
2. *À quelle condition sur A, l'idéal I est-il premier ? maximal ?*