Licence 2 : Structures Algébriques

Lucas Gaebele

23 novembre 2024

Basé sur le cours de Charles Walter

Table des matières

Chapitre 0

Disclaimer

L'unique objectif de ce document est de donner une idée de ce qui a été fait en amphi. Je le partage à la demande de certains mais il n'a évidement pas à vocation de remplacer votre cours. Il contient probablement de nombreuses erreurs mathématiques et typographiques, celles-ci me sont entièrement imputables, merci de me les signaler par les voies usuelles.

Pour des références plus fiables, on pourra par exemple consulter [1] ou [2] (disponible en pdf sur le site de la BU) ou encore [3]. Pour ceux qui voudraient aller (beaucoup) plus loin, on peut citer [4] ou le légendaire [5].

Chapitre 1

Groupes

1.1 Définition et notations

Definition 1.1.1 (Loi de composition interne (l.c.i))

Rappel : Si E est un ensemble, une loi de composition interne (l.c.i) sur E est une application $\star : E \times E \to E$. En général, on n'utilise pas la notation fonctionnelle $\star(x, y)$ mais la notation infixe $x \star y$.

Definition 1.1.2 (Groupe)

Un groupe est la donnée d'un ensemble G et d'une loi de composition interne $\star$ sur G vérifiant les propriétés suivantes :

i (Associativité) $x \star (y \star z) = (x \star y) \star z$ pour tout $x, y, z \in G$.

ii (Neutre) Il existe $e \in G$ tel que pour tout $x \in G$, $x \star e = e \star x = x$.

iii (Symétrique) Pour tout $x \in G$, il existe $y \in G$ tel que $x \star y = y \star x = e$.

Definition 1.1.3 (Groupe abélien)

Un groupe $(G, \star)$ est dit commutatif ou abélien si sa loi est commutative :
$x \star y = y \star x$ pour tout $x, y \in G$.

Remarque 1.1.4 (Notations)

Dans ce qui suit, G est un groupe de neutre e et x, y, z, t sont des éléments de G.

- Pour alléger la notation, on utilisera souvent la notation multiplicative pour la loi $(x, y) \mapsto x \cdot t$ voir $(x, y) \mapsto xy$ (sans symbole).
- Si (et seulement si !) le groupe est commutatif on utilise souvent la notation additive $(x, y) \mapsto x + y$.
- L'élément neutre est souvent noté 1_G (ou 1 si aucune confusion n'est possible) pour la notation multiplicative et 0_G ou 0 pour la notation additive.
- L'associativité correspond intuitivement (on peut le démontrer par récurrence) au fait que l'on peut changer le parenthésage sans affecter le résultat $(xyzt = (xy)zt = (xy)(zt) = x(yz)t = \ldots)$,par contre l'ordre des éléments est en général important.
- Un neutre d'une loi, s'il existe est unique, on peut donc parler DU neutre d'un groupe. De même l'inverse est unique. En effet, si $e' \in G$ est un neutre, on a $e = ee' = e'$, et si y et z sont inverses de x on a $y = ye = y(xz) = (yx)z = ez = z$.
- En notation multiplicative, on note x^{-1} le symétrique de x et on parle alors d'inverse. En notation additive, on le note $(-x)$ et on parle d'opposé.
- Pour $n \in Z$ et x on pose $x^n = xx \cdots x$ (n fois) si $n \geq 1$, $x^n = (x^{-1})^{-n}$ si $n \leq -1$ et on adopte la convention $x^n = 1$ pour $n = 0$ (En notation additive, on note cela $nx, (-n)x, 0x = 0$).
- Par abus de notation, la loi du groupe ne sera pas toujours précisée si elle est claire. Par exemple on parlera du groupe $\mathbb{Z}$ au lieu de $(\mathbb{Z}, +)$ car $+$ est la seule loi 'usuelle' qui munit $\mathbb{Z}$ d'une structure de groupe (voir exemples plus loin).

1.2 Exemples et non-exemples de groupes

Exemple 1.2.1 ($(\mathbb{Z},+)$, $(\mathbb{Q},+)$,$(\mathbb{R},+)$,$(\mathbb{C},+)$)

Un premier exemple de groupe est $\mathbb{Z}$ muni de l'addition usuelle, en effet on vérifie facilement que les axiomes d'un groupe sont vérifiés :

- La somme de deux entiers relatifs est un entier relatif.
- La somme est associative.
- Il existe un neutre : 0.
- Chaque entier a admet un symétrique : $-a$.

Comme en plus l'addition est commutative, $\mathbb{Z}$ est un groupe abélien. On vérifie de la même manière que $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des groupes abéliens.

Contre-exemple 1.2.2 ($(\mathbb{N},+)$,$(\mathbb{Z},-)$)

En revanche, $\mathbb{N}$ muni de l'addition usuelle n'est pas un groupe car à part 0, les éléments n'ont pas d'inverse. De même, $\mathbb{Z}$ muni de la soustraction usuelle n'est pas un groupe car la loi n'est pas associative et n'a pas de neutre.

Exemple 1.2.3 (Groupe symétrique)

Soit E un ensemble, l'ensemble des bijections de E dans E, muni de la loi $\circ$ de composition des applications forme un groupe appelé groupe symétrique de E. On le note en général S_E ou $\mathfrak{S}_E$, son élément neutre est noté id ou id_X, l'inverse d'une bijection σ est noté σ^{-1}. Dans le cas où $E = \{1, 2, \ldots, n\}$ avec $n \geq 1$ entier, on le note S_n ou $\mathfrak{S}_n$. Pour $n \geq 3$, S_n n'est pas commutatif.

Exemple 1.2.4 (Groupe linéaire)

Soit E un k-espace vectoriel, l'ensemble des automorphismes (applications k-linéaires bijectives) de E noté $\mathrm{Aut}(E)$ muni de la loi $\circ$ de composition des applications forme un groupe appelé groupe linéaire de E et noté $\mathrm{GL}(E)$

Proposition 1.2.5 (Règles de calculs dans un groupe)

Soit G un groupe et x, y, z des éléments de G. On a les propriétés suivantes :

1. Formule des puissances : $x^{n+m} = x^n x^m$ pour tout $n, m \in \mathbb{Z}$.
2. Inverse d'un produit : $(xy)^{-1} = y^{-1}x^{-1}$
3. Régularité : $xy = xz \implies y = z$ et $xy = zy \implies x = z$

Démonstration. Immédiates

1. Récurrence + associativité.
2. Calculer $(xy)(y^{-1}x^{-1})$.
3. Multiplier par l'inverse.

□

1.3 Sous-groupes,groupe produit

Definition 1.3.1 (Sous-groupe)

Une partie H d'un groupe G est un sous-groupe si la restriction de la loi de G à H munit H d'une structure de groupe.

Exemple 1.3.2 (Sous-groupes triviaux, sous-groupes propres)

Pour tout groupe G, $\{0\}$ et G sont des sous-groupes de G, on les appelle sous-groupes triviaux ou impropres, les sous-groupes non triviaux sont appelés sous-groupes propres.

Exemple 1.3.3 ($\mathbb{U}$)

L'ensemble $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ des complexes de module 1 est un sous-groupe (multiplicatif) de $\mathbb{C}^*$.

Exemple 1.3.4 ($n\mathbb{Z}$)

Pour n entier, l'ensemble $n\mathbb{Z} = \{nz | z \in \mathbb{Z}\}$ des multiples entiers de n est un sous-groupe de $\mathbb{Z}$.

Proposition 1.3.5 (Caractérisation des sous-groupes)

Une partie H d'un groupe G est un sous-groupe si et seulement si on a :

1. $1 \in H$.
2. $x^{-1} \in H$ pour tout $x \in H$.
3. $xy \in H$ pour tout $x, y \in H$.
   (on peut aussi faire 2 et 3 en une fois en vérifiant que $xy^{-1} \in H$ pour tout $x, y \in H$.)

Démonstration. Il suffit de vérifier les axiomes des groupes, la réciproque est évidente. □

Exemple 1.3.6 (Sous-groupes de $\mathbb{Z}$)

On cherche à caractériser les sous-groupes de $\mathbb{Z}$.
On sait déjà que pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, montrons que tout sous-groupe de $\mathbb{Z}$ est de cette forme.
Soit G un sous-groupe de $\mathbb{Z}$.

— Si G est trivial, on a $G = 0\mathbb{Z}$.

— Sinon, il existe $g \in G$ avec $g \neq 0$ et comme G est un groupe, $-g \in G$ ainsi, G possède des éléments strictement positifs. Notons n le plus petit d'entre eux ($G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ donc elle admet un plus petit élément) et montrons par double inclusion que $G = n\mathbb{Z}$. Comme $n \in G$ et G est un groupe, on a $nk \in G$ pour tout $k \in \mathbb{Z}$ donc $n\mathbb{Z} \subset G$. Réciproquement, soit $g \in G$, il faut montrer que n divise g. Notons $g = nq+r, 0 \leq r < n$ la division euclidienne de g par n, comme G est un groupe et $n, g \in G$, on a $g - nq = r \in G$ et donc $r = 0$ car sinon r serait un élément strictement positif de G inférieur à n ce qui est exclu. Ainsi, n divise g et on a bien $G \subset n\mathbb{Z}$ et donc $G = n\mathbb{Z}$.

Proposition 1.3.7 (Intersection de sous-groupes)

Une intersection quelconque de sous-groupes d'un même groupe G est encore un sous-groupe de G.

Démonstration. Soit G un groupe, I un ensemble non vide et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Montrons que $H = \bigcap_{i\in I} H_i$ est un sous-groupe de G. Déjà, il est clair que $H \subset G$, ensuite, pour tout $i \in I$, comme H_i est un sous-groupe de G, on a $1 \in H_i$ et donc $1 \in H$. Enfin, soit $h, h' \in H$, pour tout $i \in I$, on a $h, h' \in H_i$ donc comme H_i est un sous-groupe de G, on a $hh'^{-1} \in H_i$ et donc $hh'^{-1} \in H$ ce qui fait bien de H un sous-groupe de G. □

Definition 1.3.8 (Sous-groupe engendré)

Soit G un groupe et E une partie de G. On appelle sous-groupe engendré par E, et on note $< E >$ l'intersection de tous les sous-groupes de G contenant E. C'est le plus petit (pour l'inclusion) des groupes qui contient E. Si $E = \{g\}$, on note $< g >$ le sous-groupe engendré par $\{g\}$. Si $< E >= G$, on dit que E engendre G ou que E est une partie génératrice de G. Si G est engendré par un seul élément g ($G =< g >$), on dit que G est monogène et que g est un générateur de G.

Proposition 1.3.9 (Sous-groupe engendré)

Soit G un groupe et E une partie de G. Les éléments du sous-groupe engendré par E sont exactement les produits d'éléments ou d'inverses d'éléments de E.

Démonstration. Notons F l'ensembles des produits d'éléments ou produits d'éléments ou d'inverses de E. Il est clair que F est un sous-groupe de G qui contient E et donc par définition $< E >\subset F$. Réciproquement, pour que $< E >$ soit un groupe, il doit nécessairement contenir tout élément de F et donc $< E >= F$. □

Definition 1.3.10 (Produit direct)

Soient $(G, \star)$ et $(H, *)$ deux groupes. On munit le produit cartésien $G \times H$ de la loi de composition $\diamond$ composante par composante : $(g_1, h_1) \diamond (g_2, h_2) = (g_1 \star g_2, h_1 * h_2)$. On vérifie aisément que $(G \times H, \diamond)$ est un groupe dit produit direct (ou produit cartésien) de G et H.
On peut généraliser le procédé à une famille finie de groupes.

1.4 Morphismes de groupe

Definition 1.4.1 (Morphisme de groupe)

Soient G et G' deux groupes et $\varphi : G \to G'$ une application. On dit que φ est un morphisme (ou homomorphisme) de groupes si $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $x, y \in G$.
L'ensemble des morphismes de groupes de G dans G' se note $\mathrm{Hom}_{Gr}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte est clair).

Proposition 1.4.2

Soient G et G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. On a :

1. $\varphi(e_G) = e_{G'}$.
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$ pour tout $x \in G$.

Démonstration.

1. On a $e_G e_G = e_G$ donc $\varphi(e_G)\varphi(e_G) = \varphi(e_G)$, en multipliant à gauche par $\varphi(e_G)^{-1}$, on obtient $\varphi(e_G) = e_{G'}$.
2. Soit $x \in G$, on a $e_G = xx^{-1}$ donc $e_H = \varphi(x)\varphi(x^{-1})$. Similairement, $e_G = x^{-1}x$ donc $e_{G'} = \varphi(x^{-1})\varphi(x)$. Ainsi, par unicité de l'inverse, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

□

Definition 1.4.3 (Isomorphismes, endomorphismes, automorphismes)

Soient G et G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes.

1. Si φ est bijective, on dit que φ est un isomorphisme de groupes.
2. Si $G' = G$, on dit que φ est un endomorphisme de groupes.
3. Si $G' = G$ et que φ est bijective, on dit que c'est un automorphisme de groupes.

L'ensemble des isomorphismes de groupes G dans G' est noté $\mathrm{Isom}_{Gr}(G, G')$ (ou simplement $\mathrm{Isom}(G, G')$), l'ensemble des endomorphismes $\mathrm{End}(G)$ et l'ensemble des automorphismes $\mathrm{Aut}(G)$.

Remarque 1.4.4

Si φ est un isomorphisme de G dans G', alors φ^{-1} est un isomorphisme (donc en particulier un morphisme) de G' dans G.

Definition 1.4.5 (Noyau et image d'un morphisme)

Soient G et G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. Le noyau de φ, noté $\ker\varphi$ est l'ensemble des éléments de G qui ont $e_{G'}$ pour image par φ : $\ker\varphi = \{x \in G, \varphi(x) = e_{G'}\} = \varphi^{-1}(\{e_{G'}\})$. L'image de φ, noté $\mathrm{im}\varphi$ ou $\varphi(G)$ est l'ensemble des éléments de G' qui sont images par φ d'éléments de G. $\mathrm{im}\varphi = \{\varphi(x), x \in G\}$.

Remarque 1.4.6

Si E et F sont des espaces vectoriels sur un même corps, et que $L : E \to F$ est linéaire, alors L est un morphisme de groupes entre $(E, +)$ et $(F, +)$ et $\ker L$ est le même ensemble que le noyau vu en algèbre linéaire.

Proposition 1.4.7 (Le noyau et l'image sont des sous-groupes)

Soient G et G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes, alors :

1. $\ker\varphi$ est un sous-groupe de G.
2. $\mathrm{im}\varphi$ est un sous-groupe de G'.

Démonstration.

1. Soient $x, x' \in \ker\varphi$, on a $\varphi(x') = e_{G'}$ donc $\varphi(x'^{-1}) = \varphi(x')^{-1} = e_{G'}^{-1} = e_{G'}$ donc $x^{-1} \in \ker\varphi$ et $\varphi(xx') = \varphi(x)\varphi(x') = e_{G'}e_{G'} = e_{G'}$ donc $xx' \in \ker\varphi$. De plus, il est clair que $e_G \in \ker\varphi$ donc $\ker\varphi$ est un sous-groupe de G.
2. Soient $y, y' \in \mathrm{im}\varphi$, il existe des éléments $x, x' \in G$ tels que $y = \varphi(x)$ et $y' = \varphi(x')$ donc $yy'^{-1} = \varphi(x)\varphi(x')^{-1} = \varphi(x)\varphi(x'^{-1}) = \varphi(xx'^{-1})$ donc $yy'^{-1} \in \mathrm{im}\varphi$ et comme précédemment, il est clair que $e_{G'} \in \mathrm{im}\varphi$ donc $\mathrm{im}\varphi$ est un sous-groupe de G'.

□

Théorème 1.4.8 (Morphisme injectif et noyau trivial)

Un morphisme de groupes est injectif si et seulement si son noyau est trivial.

Démonstration. Soient G et G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. Supposons φ injectif, soit $x \in \ker\varphi$, comme $e_G \in \ker\varphi$, on a $\varphi(e_G) = \varphi(x)$ donc par injectivité, $e_G = x$ et donc $\ker\varphi = \{e_G\}$.
Réciproquement, supposons le noyau trivial et soient $x, x' \in G$ tels que $\varphi(x) = \varphi(x')$. En multipliant par l'inverse à gauche, on obtient $\varphi(x)^{-1}\varphi(x) = \varphi(x)^{-1}\varphi(x')$ donc $e_{G'} = \varphi(x)^{-1}\varphi(x') = \varphi(x^{-1}x')$ c'est à dire $e_G = x^{-1}x'$ comme le noyau est trivial. Ainsi, en multipliant par x à gauche, on obtient $x = x'$ et donc φ est injectif. □

1.5 Congruences

1.5.1 Cadre général (HP)

Definition 1.5.1 (Congruence modulo un sous-groupe)

Soit G un groupe et H un sous-groupe de G, on définit sur $G \times G$ la relation $\sim_H$: $x \sim_H y \iff x^{-1}y \in H$ qui est clairement d'équivalence. La relation $\sim_H$ est appelé relation de congruence (à gauche) modulo H. L'ensemble des classes d'équivalences est noté G/H. Le cardinal de G/H est appelé l'indice de H dans G et est noté $[G : H]$.

Proposition 1.5.2 (Classes)

Soit G un groupe et H un sous-groupe de G. Les classes de congruences (à gauche) d'un élément $x \in G$ sont égales à $xH = \{xh, h \in H\}$.

Démonstration. Soit $y \in G$ un élément de la classe de congruence de x modulo H, on a $x \sim_H y$ donc $x^{-1}y \in H$ et $y \in xH$. Réciproquement, si $y \in xH$, $x^{-1}y \in H$ et donc y est dans la classe de x. □

Definition 1.5.3 (Sous-groupe distingué)

Soit H un sous-groupe d'un groupe G. On dit que H est un sous-groupe distingué (ou normal) de G (pour faire plus court, on dit aussi que H est distingué dans G) et on note $H \lhd G$ si pour tout $g \in G, h \in H$, on a $ghg^{-1} \in H$.

Théorème 1.5.4 (Groupe quotient)

Soit G un groupe et H distingué dans G et soit $\pi : G \to G/H, x \mapsto xH$ la projection canonique. Il existe sur G/H une unique structure de groupe telle que π soit un morphisme de groupes.

Démonstration. On définit la multiplication sur les classes par $(g_1H)(g_2H) = (g_1g_2)H$ et on vérifie que cela fonctionne (voir cours de structures II). □

1.5.2 Exemple fondamental : Congruences dans $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$, on prend $(\mathbb{Z}, +)$ comme groupe de base et $(n\mathbb{Z}, +)$ comme sous-groupe et on considère le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Pour résumer, on défini la relation d'équivalence $\sim$ sur $\mathbb{Z}$ par $x \sim y$ si et seulement si n divise $y - x$, on dit alors que x est congru à y modulo n et on note $x \equiv y \pmod{n}$.

La classe d'équivalence $\overline{x}$ (on note aussi $\mathring{x}, \tilde{x}, \cdots$ si on a besoin de plusieurs symboles) d'un entier x est l'ensemble des entiers de la forme $nk + x$ avec $k \in \mathbb{Z}$. Dans la suite, on prendra comme représentant de la classe de x le reste de la division euclidienne de x par n.
Ainsi, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. La loi du groupe est l'addition des classes : pour tout $x, y \in \mathbb{Z}, \overline{x+y} = \overline{x} + \overline{y}$.

Théorème 1.5.5 (Définition de l'addition)

L'addition des classes définie plus haut est bien définie, c'est à dire indépendante du représentant de la classe. C'est à dire que pour $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes et bien un groupe (qui est clairement abélien)

Démonstration. $x, y \in \mathbb{Z}$ et soit x' un représentant de $\overline{x}$ et y' un représentant de $\overline{y}$. On doit montrer que $\overline{x+y} = \overline{x'+y'}$. Par hypothèse, il existe des entiers k et k' tels que $x' = nk + x$ et $y' = nk + y$ et donc $x' + y' = n(k+k') + x + y$ d'où le résultat.

□

Proposition 1.5.6 (Compatibilité avec la multiplication)

Soit $n \in \mathbb{N}$, la relation de congruence de $\mathbb{Z}/n\mathbb{Z}$ est compatible avec la multiplication. On a donc pour $x, y \in Z$, $\overline{xy} = \overline{xy}$.

Démonstration. $x, y \in \mathbb{Z}$ et soit x' un représentant de $\overline{x}$ et y' un représentant de $\overline{y}$. On doit montrer que $\overline{xy} = \overline{x'y'}$. Par hypothèse, il existe des entiers k et k' tels que $x' = nk + x$ et $y' = nk + y$ et donc $x'y' = (nk + x)(nk' + y) = n^2kk' + nky + xnk' + xy = n(nkk' + ky + k'x) + xy$ d'où le résultat car $(nkk' + ky + k'x) \in \mathbb{Z}$.

□

Remarque 1.5.7

Attention, $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ muni de la multiplication des classes n'est en général pas un groupe.

1.6 Ordre d'un élément

Definition 1.6.1 (Ordre d'un élément)

Soit G un groupe. L'ordre d'un élément x de G est, s'il existe, le plus petit entier $n \geq 1$ tel que $x^n = 1$ (en notation additive cela donne $nx = 0$). Si un tel entier n'existe pas, on dit que l'ordre de x est infini. On le note $\text{ord}(x)$ ou $o(x)$ ou $|x|$.

Remarque 1.6.2

Le neutre d'un groupe est toujours d'ordre 1 et c'est le seul élément d'ordre 1.

Proposition 1.6.3 (Suite des puissances/multiples)

Soit x un élément d'un groupe G tel que $|x| = n$. Les éléments de toute suite de n puissances consécutives de x sont distincts. C'est à dire $x^k \neq x^{k+1} \neq \ldots \neq x^{k+n-1}$ pour tout entier k.

Démonstration. Soit k un entier. Distinguons selon que l'ordre de x soit fini ou non.

— Supposons n fini et supposons qu'il existe un entier $0 < l < n$ tel que $x^k = x^{k+l}$, alors en multipliant l'égalité par x^{-k}, on obtient $1 = x^l$ avec $0 < l < n$ ce qui contredit la définition de $|x|$.

— On procède de la même manière, on aboutit à $x^l = 1$ avec l fini ce qui est exclu.

□

Proposition 1.6.4

Soit G un groupe et soit $x \in G$ d'ordre fini n. Alors, pour tout entier k, $x^k = 1$ si et seulement si $n \mid k$.

Démonstration. Soit k un entier tel que $x^k = 1$, on note $k = nq + r, 0 \; ler < n$ la division euclidienne de k par n, on a $x^k = x^{nq+r} = (x^n)^q x^r = x^r = 1$ mais alors si $r > 0$, on a un entier strictement positif strictement inférieur à n tel que $x^r = 1$ ce qui est exclu donc $r = 0$ et k divise n.
Réciproquement, si $n \mid k$, il existe un entier q tel que $k = nq$ et $x^k = x^{nq} = (x^n)^q = 1^q = 1$. D'où le résultat. □

Méthode 1.6.5 (Vérifier l'ordre d'un élément)

Cadre : On cherche l'ordre d'un élément x d'un groupe G et on suppose qu'on a trouvé un entier k tel que $x^k = 1$. Pour vérifier que $|x| = k$, il faudrait, d'après la définition vérifier que $x^l \neq 1$ pour tout $0 < l < k$ mais d'après ce qui précède il suffit de vérifier que $x^d \neq 1$ pour tout diviseur d de k. En fait, on peut faire encore mieux en remarquant que si $k = p_1^{a_1} \dots p_n^{a_n}$ est la décomposition en facteurs premiers de k et si $n < k$ est l'ordre de x, alors n divise un (au moins) des $\frac{k}{p_i}$.
Exemple : Supposons qu'on a trouvé $x^{120} = 1$, on a $120 = 2^3 \times 3 \times 5$, 120 est l'ordre de x si et seulement si $x^{2^2 \times 3 \times 5} = x^{60} \neq 1$ et $x^{2^3 \times 5} = x^{40} \neq 1$ et $x^{2^3 \times 3} = x^{24} \neq 1$.

Proposition 1.6.6 (Ordre d'une puissance)

Soit G un groupe, x un élément de G et k un entier non nul.

1. Si l'ordre de x est infini, alors l'ordre de x^k est infini.
2. Sinon, on a $|x^k| = \frac{|x|}{|x| \wedge k}$.

Démonstration. 1. Le premier point est évident (sinon l'ordre de x serait fini).

2. Déjà, il est clair que $|x^k|$ est fini car $|x|$ est fini. Notons $n = |x^k|$ et $m = |x|$. On a $(x^k)^n = x^{kn} = 1$ donc $m \mid kn$ ainsi, $\frac{m}{m\wedge k} \mid \frac{kn}{m\wedge k}$ mais $\frac{m}{m\wedge k}$ et $\frac{k}{m\wedge k}$ sont premiers entre-eux donc d'après le lemme de Gauss, $\frac{m}{m\wedge k} \mid n$. Réciproquement, on a $(x^k)^{\frac{m}{m\wedge k}} = (x^m)^{\frac{k}{m\wedge k}} = 1$ car $\frac{k}{m\wedge k}$ est entier donc $n \mid \frac{m}{m\wedge k}$ et finalement $n = \frac{m}{m\wedge k}$.

□

Corollaire 1.6.7 (Conséquences)

1. Soit n un entier naturel non nul et k un entier. L'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{n\wedge k}$.
2. Soient G et H deux groupes, $x \in G, y \in H$ deux éléments d'ordres finis. Alors l'ordre de (x, y) dans $G \times H$ est $|x| \vee |y|$.

Démonstration. 1. Conséquence immédiate du théorème précédent en remarquant que $\overline{k} = k\overline{1}$ et que l'ordre de $\overline{1}$ est n.

2. On a $(x, y)^k = (x^k, y^k)$ donc $(x, y)^k = 1$ si et seulement si $|x| \mid k$ et $|y| \mid k$ et par définition, le plus petit $k \geq 1$ ayant cette propriété est $|x| \vee |y|$.

□

Remarque 1.6.8 (Ordre d'un produit)

Attention, il n'y a pas de formule générale reliant l'ordre du produit de deux éléments en fonction de l'ordre des éléments, il se peut même que les ordres des deux soient finis alors que l'ordre du produit est infini ou vice-versa.

Théorème 1.6.9 (Théorème de Lagrange)

Soit G un groupe et H un sous-groupe de G. L'ordre de H divise l'ordre de G.

Démonstration. On a vu que l'ensemble G/H des classes modulo H partitionnent G en $[G : H]$ ensembles de même cardinal $|H|$. D'après le lemme des bergers, on a donc $|G| = |H|[G : H]$ et en particulier, $|H| \mid |G|$. □

Corollaire 1.6.10

Soit G un groupe fini et $x \in G$. On a $|x| \mid |G|$.

Démonstration. On sait que$< x >$ est un sous-groupe de cardinal $|x|$ donc le théorème de Lagrange donne le résultat. □

1.7 Groupes cycliques

Definition 1.7.1 (Groupe cyclique)

Un groupe G est dit cyclique (ou monogène) si il est engendré par une seul élément, c'est à dire, il existe $g \in G$ tel que $G =< g >$, un tel élément est appelé un générateur du groupe.

Proposition 1.7.2

Tout groupe cyclique est abélien.

Démonstration. Soit G un groupe cyclique, g un générateur et $x, y \in G$. Par hypothèse, il existe des entiers $k$et l tels que $x = g^k$ et $y = g^l$ donc $xy = g^k g^l = g^{k+l} = g^{l+k} = g^l g^k = yx$. □

Proposition 1.7.3 (Caractérisation des groupes cycliques finis)

Un groupe fini d'ordre n est cyclique si et seulement si il contient un élément d'ordre n, un tel élément est alors un générateur du groupe.

Démonstration. Soit G un groupe fini. Si G est cyclique, un générateur est par définition d'ordre n, réciproquement, si un g élément est d'ordre n, on a vu que n puissances successives sont distinctes et donc $< g >$ est un sous-groupe de G d'ordre n, c'est à dire $< g >= G$. □

1.8 Groupes isomorphes

Definition 1.8.1 (Groupes isomorphes)

S'il existe un isomorphisme de groupes entre deux groupes G et H, on dit qu'ils sont isomorphes et on note $G \simeq H$.

Exemple 1.8.2

Les groupes $\mathbb{Z}/2\mathbb{Z}$ et $\{-1, 1\} \subset \mathbb{R}^*$ sont isomorphes (vérifier que LE morphisme est bijectif). Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ sont isomorphes($\exp : \mathbb{R} \mapsto \mathbb{R}_+^*$).

Proposition 1.8.3

On peut dire que deux groupes isomorphes sont 'les mêmes' à un ré-étiquetage près. près, en particulier :
Soit $\varphi : G \xrightarrow{\sim} H$.

i $|G| = |H|$.

ii F est un sous-groupe de G si et seulement si $\varphi(F)$ est un sous-groupe de H.

iii pour $x \in G$, $o_G(x) = o_H(\varphi(x))$.

iv G est cyclique si et seulement si H est cyclique et alors g est un générateur de g si et seulement si $\varphi(g)$ est un générateur de H.

v G est abélien si et seulement si H est abélien.

Démonstration. Toutes ces propriétés se montrent de la même façon, on utilise en particulier que la bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupes. Détaillons par exemple le dernier point : Supposons G abélien et soit $y_1, y_2 \in H$. Comme φ est une bijection, il existe d'uniques $x_1, x_2 \in G$ tels que $y_1 = \varphi(x_1), y_2 = \varphi(x_2)$ et par propriété des morphismes de groupes, on a $y_1 y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1 x_2)$ donc comme G est abélien, $\varphi(x_1 x_2) = \varphi(x_2 x_1) = \varphi(x_2)\varphi(x_1) = y_2 y_1$. On montre la réciproque exactement de la même manière en échangeant les rôles de G et H et en considérant φ^{-1}.

□

Théorème 1.8.4 (Caractérisation des groupes cycliques)

Soit G un groupe cyclique, on a l'alternative suivante selon le cardinal de G :

i Si G est fini d'ordre n, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

ii Si G est infini, alors $G \simeq \mathbb{Z}$.

Autrement dit, à isomorphisme près, $\mathbb{Z}$ et les $\mathbb{Z}/n\mathbb{Z} (n \in \mathbb{N}^*)$ sont les seuls groupes cycliques.

Démonstration.

i On vérifie facilement que $\varphi : \mathbb{Z}/n\mathbb{Z} \to G, \overline{k} \mapsto g^k$ est un isomorphisme de groupes.

ii De même avec $\varphi : \mathbb{Z} \mapsto G : k \mapsto g^k$.

□

1.9 Groupe symétrique

Definition 1.9.1 (Groupe symétrique : cas général)

Soit E un ensemble, l'ensemble des bijections de E dans lui-même muni de la loi de composition des applications forme un groupe appelé groupe symétrique, on le note S_E ou $\mathfrak{S}_E$.

Definition 1.9.2 (Groupe symétrique : cas particulier)

En particulier, pour n un entier non nul et pour $E = \{1, 2, \dots, n\}$ on note S_n le groupe symétrique d'indice n, c'est l'ensemble des permutations de $\{1, 2, \dots, n\}$, et on a $|S_n| = n!$. Pour $\sigma \in S_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Dans la suite de cette section, (sauf mention contraire) n est un entier naturel non nul et on considère le groupe symétrique S_n.

Definition 1.9.3 (Transposition)

Soit deux entiers $1 \leq i, j \leq n$ distincts, on appelle transposition sur i, j la permutation notée $\tau_{i,j}$ qui permute i et j et fixe tous les autres éléments.
$\tau_{i,j} = \begin{pmatrix} 1 & \dots i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots n \\ 1 & \dots i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots n \end{pmatrix}$.
Remarquons que $\tau_{i,j}\tau_{i,j} = id$ et que $\tau_{i,j} = \tau_{j,i}$.

Definition 1.9.4 (Cycle)

Soit $l \geq 2$, une permutation σ contient un cycle de longueur l (ou l-cycle) s'il existe des entiers $a_1, a_2, \dots a_l \in \{1, \dots, n\}$ tous distincts tels que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_l) = a_1$. On note alors ce cycle $(a_1 a_2 a_3 \dots a_l)$.
L'ensemble $\{a_1, a_2, \dots, a_l\}$ est appelé le support du cycle. (de manière plus générale, le support d'une permutation est l'ensemble des éléments qui ne sont pas fixés par la permutation). Deux cycles sans éléments en commun sont dit à supports disjoints.
Remarque : une transposition est un cycle de longueur 2.

Théorème 1.9.5 (Décomposition en transpositions)

Tout permutation se décompose en produit de transpositions.

Méthode 1.9.6 (Décomposition d'une permutation en produit de transpositions/idée de la preuve)

Considérons dans S_5 la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$, on souhaite décomposer σ en produits de transpositions. On commence par "bien placer" le 1, il faut ici le permuter avec 4. On obtient $(14)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$. Ensuite on passe à 2 qu'il faut permuter avec le 3 ce qui donne $(23)(14)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$. Puis à 3 donc $(34)(23)(14)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$. Le 4 et le 5 sont bien placés on a obtenu l'identité $(34)(23)(14)\sigma = id$, comme une transposition est égale à son inverse, il suffit de retourner l'ordre pour obtenir $\sigma = (14)(23)(34)$.

Démonstration. On procède par récurrence, l'initialisation est claire pour S_1 et S_2, on fixe $n \geq 3$ et on suppose que toute permutation de S_{n-1} est décomposable. Soit $\sigma \in S_n$, si $\sigma(n) = n$, on peut voir σ comme un élément de S_{n-1} et appliquer l'hypothèse de récurrence, sinon soit $k \in \{1, \ldots, n-1\}$ l'entier tel que $\sigma(k) = n$, on a $(\tau_{k,n}\sigma)(n) = n$ donc par ce qui précède on peut la décomposer en produit de transpositions, il suffit alors de composer par $\tau_{k,n}$ pour obtenir une décomposition de σ. □

Remarque 1.9.7 (Non-unicité de la décomposition)

Il est évident que la décomposition précédente n'est pas unique (par exemple on aurait pu placer les éléments dans un autre ordre ou rajouter des transpositions). Par contre on verra que la parité du nombre de transpositions de la décomposition l'est (voir signature dans la suite).

Théorème 1.9.8 (Décomposition en cycles à supports disjoints)

Toute permutation non-triviale, se décompose en produit de cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre des facteurs prêt.

Méthode 1.9.9 (Décomposition d'une permutation en produit de cycles à support disjoints/idée de la preuve)

Comme pour les transpositions, la méthode est très simple. Considérons dans S_8 la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 6 & 8 & 2 & 5 & 7 \end{pmatrix}$.
On commence par chercher le 1 et ses images successives jusqu'à retomber sur 1, ici $1 \to 3 \to 4 \to 6 \to 2 \to 1$ donc un premier cycle est (13462). Ensuite on prend le premier entier de $\{2, 3 \dots, n\}$ qui n'est pas dans notre cycle, ici $2, 3, 4$ sont dans le cycle donc on prend 5, $5 \to 8 \to 7 \to 5$ ce qui donne (587) On recommence le procédé jusqu'à avoir examiné tous les entiers de $\{1, \dots, n\}$ (dans cet exemple on a déja terminé !). La permutation est le produit des cycles obtenus. Dans cet exemple, on a $\sigma = (13462)(587)$.

Proposition 1.9.10

Deux cycles à support disjoints commutent.

Démonstration. Soient u, v deux cycles à support disjoints et $i \in \{1, \dots, n\}$.

Si i n'est dans aucun des deux supports, clairement $(uv)(i) = (vu)(i)$. Sinon, i est dans seulement un des deux supports, par exemple dans celui de u, mais alors par définition, $u(i)$ est dans le support de u et donc pas dans celui de v et donc $(uv)(i) = u(i)$ et $(vu)(i) = v(u(i)) = u(i)$.

□

Definition 1.9.11 (Signature d'une permutation (HP))

La signature dune permutation σ, noté $\varepsilon(\sigma)$ est le produit $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Proposition 1.9.12 (Quelques propriétés de la signature (HP))

i Pour $\sigma, \mu \in S_n$, $\varepsilon(\sigma\mu) = \varepsilon(\sigma)\varepsilon(\mu)$.

ii Une transposition est de signature -1

iii Un cycle de longueur l est de signature $(-1)^{l-1}$

iv Pour $\sigma \in S_n$, $\varepsilon(\sigma) \in \{-1, 1\}$. Les permutations de signature 1 sont dites paires, celles de signature -1 impaires.

v L'application $\varepsilon : S_n \to \{-1, 1\}$ est un morphisme de groupe.

vi L'ensemble des permutations paires de S_n forment un sous groupe de S_n appelé groupe alterné d'indice n et noté A_n. On a $|A_n| = \frac{n!}{2}$.

Démonstration. i Soient $\sigma, \mu \in S_n$, calculons gaiement :On a $\varepsilon(\sigma\mu) = \prod_{1\leq i<j\leq n} \frac{(\sigma\mu)(j)-(\sigma\mu)(i)}{j-i}$, en multipliant par "1", on obtient $\varepsilon(\sigma\mu) = \prod_{1\leq i<j\leq n} \frac{(\sigma\mu)(j)-(\sigma\mu)(i)}{\mu(j)-\mu(i)} \prod_{1\leq i<j\leq n} \frac{\mu(i)-\mu(j)}{j-i}$. Le second produit est clairement $\varepsilon\mu$ et comme μ est une permutation (et donc une bijection), on peut réindexer le premier produit en posant $(k, l) = (\mu(i), \mu(j))$ ce qui donne $\prod_{1\leq i<j\leq n} \frac{(\sigma\mu)(j)-(\sigma\mu)(i)}{\mu(j)-\mu(i)} = \prod_{1\leq k<l\leq n} \frac{\sigma(l)-\sigma(k)}{l-k} = \varepsilon(\sigma)$ d'où le résultat.

ii Calcul immédiat.

iii On a vu que l'on peut décomposer une cycle de longueur l en $l-1$ transpositions donc par i et ii on a le résultat.

iv Découle immédiatement de la décomposition d'une permutation en produit de transpositions et de ii

v Découle de iv et i et de la définition d'un morphisme.

vi $A_n = \ker \epsilon$ et le noyau d'un morphisme est un sous-groupe. Pour le cardinal, on montre que l'indice de A_n dans S_n est 2.

□

Chapitre 2

Anneaux

2.1 Généralités

Definition 2.1.1 (Anneau)

Un anneau est la donnée d'un ensemble A et de deux lois de composition interne sur A, généralement notées l'une additivement, l'autre multiplicativement, vérifiant les propriétés suivantes.

i $(A, +)$ est un groupe abélien (rappel : associativité,neutre (0),symétrie,commutativité)

ii La multiplication est associative : $x(yz) = (xy)z$ pour tout $x, y, z \in A$.

iii La multiplication est distributive à droite et à gauche par rapport à l'addition : $(x+y)z = xz+yz$ et $x(y+z) = xy+xz$ pour tout $x, y, z \in A$.

Si en plus, la multiplication possède un neutre (1), on dit que l'anneau est unitaire. Dans la suite, sauf mention contraire, tous les anneaux de ce cours seront unitaire, on dira donc simplement anneau pour anneau unitaire.
Si en plus, la multiplication est commutative, on dit que l'anneau est commutatif (attention, l'addition est toujours commutative dans un anneau !).

Remarque 2.1.2

Comme avec les groupes, on omet souvent de préciser les lois de l'anneau si celles-ci sont 'évidentes'.

Exemple 2.1.3

Parmi les exemples d'anneaux que nous détaillerons dans la suite, on trouve $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{K}[X]$ qui sont commutatifs, ou $\mathcal{M}_n(\mathbb{R})$ qui n'est pas commutatif.
Un exemple théorique important est l'anneau nul réduit à un élément $\{0\}$.

Proposition 2.1.4 (Règles de calculs dans un anneau)

oit A un anneau, on a :

1. Pour tout $x \in A$, $0x = x0 = 0$.
2. Pour tout $x, y \in A$, $(-x)y = x(-y) = -xy$.
3. Pour tout $x, y \in A$ et $n \in \mathbb{Z}$, $(nx)y = n(xy) = x(ny)$
4. Pour tout $x \in A$, $l, m \in \mathbb{N}^*$, $x^{l+m} = x^l x^m = x^m x^l$ et $(x^n)^m = x^{nm}$
   Comme dans les groupes, on pose $x^0 = 1$ pour tout x.

Démonstration. Soient $x, y \in A$, $n \in \mathbb{Z}$, $l, m \in \mathbb{N}^*$.

1. On a $0 = 0 + 0$ donc $x0 = x(0 + 0) = x0 + x0$ donc $x0 = 0$ on montre de même que $0x = 0$.
2. Par 1., $0 = (x - x)y = xy + (-x)y$ donc $(-x)y = -xy$ de même, $0 = x(y - y) = xy + x(-y)$ donc $x(-y) = -xy$.
3. Si $n = 0$, on a le résultat par 1., si $n > 0$, par distributivité, $(nx)y = (x+x+\cdots+x)y = xy+xy+\cdots xy = n(xy)$, si $n < 0$, on pose $n' = -n$, on a $n' > 0$ donc par ce qui précède, $(nx)y = ((-n')x)y = (-n')(xy) = n(xy)$. On obtient l'autre égalité de manière similaire.
4. Conséquence directe de l'associativité de la multiplication.

□

Proposition 2.1.5

Soit A un anneau (unitaire). On a $0_A = 1_A$ si et seulement si A est l'anneau nul.

Démonstration. Supposons $0_A = 1_A$, soit $x \in A$, on a $1_A x = x$ mais $1_A = 0_A$ donc $0_A x = x = 0_A$ donc A est nul. Réciproquement, si A est nul on a forcément $0_A = 1_A$ car il n'y a qu'un seul élément. □

Definition 2.1.6 (Inverse, inversibles)

Soit A un anneau et $x \in A$. On dit que x admet un inverse à gauche s'il existe $y \in A$ tel que $yx = 1$. Similairement, x admet un inverse à droite s'il existe $z \in A$ tel que $xz = 1$. Si x est inversible à gauche et à droite on a $y = z$ (car $y(xz) = y = (yx)z = z$), on dit alors que x est inversible et l'élément $y = z$ est l'inverse de x et est noté x^{-1}.

Théorème 2.1.7 (Groupe des inversibles)

Soit A un anneau, l'ensemble des éléments inversibles de A, noté A^* ou $A^\times$ forme un groupe pour la multiplication.

Démonstration. — L'associativité découle de celle de A,

— Si $x, y \in A$ sont inversibles, par associativité $(xy) = 1 = (y^{-1}x^{-1})(xy)$.

— Clairement 1 est inversible.

— Si x est inversible, x^{-1} est inversible d'inverse x.

□

Exemple 2.1.8

On a $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ (ouf !), $\mathcal{M}_n(\mathbb{R})^* = \mathrm{GL}_n(\mathbb{R})$, $\mathbb{Z}^* = \{1; -1\}$. On verra dans la suite que si K est un corps, $\mathbb{K}[X]^* = \mathbb{K}^*$ et que

$$(\mathbb{Z}/n\mathbb{Z} = \{\overline{k} \mid (k \wedge n) = 1\}$$

.

Definition 2.1.9 (Corps)

Si A est un anneau commutatif non nul dans lequel tout élément non nul est inversible, on dit que A est un corps.

Exemple 2.1.10 (Exemples de corps)

On vérifie aisément que $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps (commutatifs), par contre $\mathbb{Z}$ ou $\mathbb{K}[X]$ ne sont pas des corps, on verra dans la suite que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Remarque 2.1.11 (Corps gauche, anneau à division)

Dans certains ouvrages, la commutativité n'est pas demandée dans la définition d'un corps. On parles alors de corps commutatif ... Dans ce cours, on considère que les corps sont commutatifs et on les appelles simplement corps. Une structure non commutative vérifiant les propriétés des corps sera appelé un corps gauche ou un anneau à division.

Exemple 2.1.12 (Exemple de corps gauche)

Un exemple important de corps gauche est celui des quaternions

$$\mathbb{H} = \{\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C}\}$$

.
On vérifie que tous les axiomes d'un corps sont vérifiés sauf la commutativité.
On a

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{ad} - \overline{b}c & \overline{ac} - \overline{b}d \end{pmatrix}$$

Mais

$$\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \begin{pmatrix} ac - \overline{b}d & \overline{a}d + bc \\ -a\overline{d} - \overline{bc} & \overline{ac} - b\overline{d} \end{pmatrix}$$

Definition 2.1.13 (Diviseur de zéro, Anneau intègre, Domaine d'intégrité)

Soit A un anneau, un élément non nul $x \in A$ est un diviseur de zéro à gauche s'il existe $y \in A$ non nul tel que $xy = 0$, on définit de même la notation de diviseur de zéro à droite. Si A est commutatif, les deux notions coincident et on parle seulement de diviseur de zéro.
Un anneau est dit intègre s'il est non nul et sans diviseur de zéro. Un anneau intègre commutatif est appelé un domaine d'intégrité (integral domain (ID) dans la langue de Shakespeare). Dans certains ouvrages (et dans la suite de ce cours), la définition d'anneau intègre comprend la commutativité et les deux notions sont synonymes.

Proposition 2.1.14

Tout corps est un anneau intègre.

Démonstration. Soit F un corps et $x, y \in F$ tels que $xy = 0$. Supposons $x \neq 0$, alors $x^{-1}xy = y = 0$. □

Definition 2.1.15 (Sous-anneau)

Soit A un anneau, $B \subset A$ est un sous-anneau de A si :

1. B est un sous-groupe additif de A.
2. B est stable pour la multiplication.
3. Le neutre multiplicatif de A appartient à B.

Exemple 2.1.16 (Exemples et contre-exemples de sous-anneaux)

On vérifie aisément que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, ou que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est un sous-anneau de $\mathbb{C}$, par contre $\mathbb{N}$ ou $2\mathbb{Z}$ ne sont pas des sous-anneaux de $\mathbb{Z}$ ($\mathbb{N}$ n'est pas un sous-groupe de $\mathbb{Z}$, et $1 \notin 2\mathbb{Z}$).

Proposition 2.1.17 (Caractérisation des sous-anneaux)

Soit A un anneau, B est un sous-anneau de A si et seulement si :

— $1 \in B$.

— Pour tout $x, y \in B$, $x + y \in B$

— Pour tout $x, y \in B$, $xy \in B$

Démonstration. Immédiate. □

Proposition 2.1.18

Un sous-anneau d'un anneau intègre est un anneau intègre.

Démonstration. Immédiate. □

Definition 2.1.19 (Idéal)

Soit A un anneau et I un sous-ensemble de A. On dit que I est un idéal à gauche si :

1. $(I, +)$ est un sous-groupe de A.
2. Pour tout $x \in I, a \in A$ on a $ax \in I$.

Similairement, on dit que I est un idéal à droite si :

1. $(I, +)$ est un sous-groupe de A.
2. Pour tout $x \in I, a \in A$ on a $xa \in I$.

On dit que I est un idéal bilatère (ou simplement idéal si aucune confusion n'est possible) si I est à la fois un idéal à gauche et un idéal à droite de A.
Il est clair que si A est commutatif, toutes ces définitions coincident.

Exemple 2.1.20 (Idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$)

On vérifie que les idéaux de $\mathbb{Z}$ sont les $m\mathbb{Z}$, $m \in \mathbb{Z}$.
Les idéaux de $\mathbb{K}[X]$ sont de la forme $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

Démonstration. La démonstration suit de près celle des sous-groupes de $\mathbb{Z}$. Déjà on vérifie aisément que pour $P \in \mathbb{K}[X]$, l'ensemble des multiples de P forme un idéal de $\mathbb{K}[X]$. Réciproquement, soit I un idéal de $\mathbb{K}[X]$. Si $I = \{0\}$, il suffit de prendre $P = 0$. Supposons que I n'est pas réduit au polynôme nul, notons E l'ensemble des degrés des éléments de I. Comme I n'est pas réduit au polynôme nul, E est une partie non vide de $\mathbb{N}$ donc elle contient un plus petit élément n_0 et il existe $P_0 \in I$ de degré n_0. Soit $P \in I$, on note $P = P_0Q + R$, $R = 0$ ou $\deg(R) < \deg(P_0)$ la division euclidienne (voir plus bas) de P par P_0. Comme I est un idéal, $R = P - P_0Q \in I$ et donc $R = 0$ car sinon R est un polynôme non nul de I de degré strictement inférieur à n_0 ce qui est exclu. □

Definition 2.1.21 (Idéal engendré par une partie)

Soit A un anneau et E une partie de A. L'idéal engendré par E, noté (E) ou $< E >$ est le plus petit idéal de A contenant E. C'est l'intersection de tous les idéaux de A contenant E.
On peut le décrire comme

$$< E >= \{\sum_{i=1}^{n} a_i x_i b_i \mid n \in \mathbb{N}, a_i, b_i \in A, x_i \in E\}$$

.

Definition 2.1.22 (Idéal principal, anneau principal)

Un idéal I d'un anneau A est principal s'il existe $x \in A$ tel que $I =< x >$. Si tous les idéaux de A sont principaux et si A est commutatif, on dit que A est un anneau principal.

Exemple 2.1.23 (Exemples d'anneaux principaux)

D'après ce qui précède, $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux. Par contre $\mathbb{Z}[X]$ n'est pas principal (vérifier que $(2, X)$ n'est pas principal).

Definition 2.1.24 (Morphisme d'anneaux, noyau)

Soient A, B des anneaux, et $\varphi : A \to B$ une application. On dit que φ est un morphisme d'anneaux si les conditions suivantes sont vérifiées :

- $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$ pour tout $x, y \in A$.
- $\varphi(x \times_A y) = \varphi(x) \times_B \varphi(y)$ pour tout $x, y \in A$.
- $\varphi(1_A) = 1_B$.

On définit, comme dans le cas des groupe, le noyau d'un morphisme d'anneaux $\varphi : A \to B$ par $\ker \varphi = \{x \in A \mid \varphi(x) = 0_B\}$.

Proposition 2.1.25

Soit A, B des anneaux et $\varphi : A \to B$ un morphisme d'anneaux, alors :

1. $\ker \varphi$ est un idéal de A.
2. φ est injectif si et seulement si $\ker \varphi = \{0\}$.

Démonstration. 1. D'après la partie sur les groupes, on sait déjà que $\ker \varphi$ est un sous-groupe additif. Soit $a \in A, x \in \ker \varphi$, on a $\varphi(ax) =$

$\varphi(a)\varphi(x) = \varphi(a) \times 0 = 0$ donc $ax \in \ker\varphi$. Donc $\ker\varphi$ est un idéal de A.

2. Même démonstration que dans le cas des groupes.

□

Exemple 2.1.26 (Premiers exemples de morphismes)

On vérifie aisément que pour $n > 0$ entier, l'application $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto \overline{x}$ est un morphisme d'anneaux surjectif de noyau $\ker\pi_n = n\mathbb{Z}$. De même, si $\mathbb{K}$ est un corps, l'application $\pi : \mathbb{K} \to \mathbb{K}[X], a \mapsto a$ est un morphisme d'anneaux injectif.

Proposition 2.1.27

Soient $m, n \in \mathbb{N}^*$, l'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}, \overline{a} \mapsto \mathring{a}$ définit un morphisme d'anneaux surjectif.

Démonstration. Vérifions que φ est bien définie. Soient $\overline{a}, \overline{b} \in \mathbb{Z}/mn\mathbb{Z}$ tels qe $\overline{a} = \overline{b}$, il faut vérifier que $\varphi(\mathring{\overline{a}}) = \varphi(\mathring{\overline{b}})$. Comme $\overline{a} = \overline{b}$, il existe $k \in \mathbb{Z}$ tel que $a = b + (mn)k$ mais alors $a = b + n(mk)$ donc $\mathring{a} = \mathring{b}$ et φ est bien définie. Le fait que ce soit un morphisme d'anneaux est une simple vérification et le caractère surjectif est évident. □

2.2 Arithmétique dans $\mathbb{K}[X]$

Dans la suite, sauf mention contraire $\mathbb{K}$ est un corps quelconque.

Proposition 2.2.1 ($\mathbb{K}[X]^* = \mathbb{K}^*$)

Les inversibles de $\mathbb{K}[X]$ sont les inversibles de $\mathbb{K}$.

Démonstration. Il est clair que les inversibles de $\mathbb{K}$ (vus comme polynômes constant) sont inversibles. Réciproquement, soit $P \in \mathbb{K}[X]$ inversible, on a $\deg(PP^{-1}) = \deg(1) = 0 = \deg(P) + \deg(P^{-1})$ donc $\deg(P) = \deg(Q) = 0$. □

Definition 2.2.2 (Multiple, diviseur)

Soit $P, Q \in \mathbb{K}[X]$ S'il existe $R \in \mathbb{K}[X]$ tel que $P = QR$, on dit que Q divise P et que P est un multiple de Q.

Théorème 2.2.3 (Division euclidienne)

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $R = 0$ ou $\deg(R) < \deg(B)$.

Démonstration. — Unicité : Soit (Q', R') un autre couple, on a $A = BQ + R = BQ' + R'$ donc $B(Q - Q') = R' - R$ or $\deg(R' - R) \leq \deg(R') < \deg(B)$ donc le degré de $B(Q - Q')$ est strictement inférieur au degré de B ce qui n'est possible que si $(Q - Q') = 0$ et donc $Q = Q'$. En remplaçant dans les équations, on obtient $R = R'$.

— Existence : On note m le degré de A et n celui de B. Raisonnons par récurrence sur m. Si $m < n$ ou si $A = 0$, il suffit de prendre $Q = 0$ et $B = R$. Soit $k \geq n$ supposons la propriété établie pour $m < k$ et montrons la pour $m = k$. On note $A = \sum_{i=0}^{m} a_i X^i$ et $B = \sum_{i=0}^{n} b_i X^i$. Soit $C = A - \frac{a_m}{b_n} X^{m-n} B$, on a $\deg(C) < n$ donc par hypothèse de récurrence, il existe un couple (Q_C, R_C) avec $C = BQ_C + R_C, \deg(R_C) < n$ ou $R_C = 0$. En posant $Q = \frac{a_m}{b_n} X^{m-n} + Q_C$ et $R = R_C$ et en remplaçant, on obtient $A = BQ + R$, $\deg(R) < n$ ou $R = 0$ d'où le résultat.

□

Lemme 2.2.4

Soient $A, B \in \mathbb{K}[X]$, on a :

1. $(A) \subset (B)$ si et seulement si $B \mid A$.
2. Il existe $D \in \mathbb{K}[X]$ tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.
3. Il existe $M \in \mathbb{K}[X]$ tel que $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$.

Démonstration. 1. $(A) \subset (B) \iff B \in (A) \iff B|A$.

2. Comme tous les idéaux sont principaux, il suffit de montrer que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ est un idéal ce qui est clair.
3. De même.

□

Proposition 2.2.5 (pgcd, ppcm)

Soient $P_1, P_2 \in \mathbb{K}[X]$, il existe des polynômes $D, M \in \mathbb{K}[X]$ tels que :

I D divise P_1 et D divise P_2.

II Tout polynôme divisant P_1 et P_2 divise D.

1. M est un multiple de P_1 et de P_2.
2. Tout polynôme multiple de P_1 et P_2 est un multiple de M.

D s'appelle un pgcd de P_1 et P_2 et M s'appelle un pgcd de P_1 et P_2.
Si en plus, on suppose D et M unitaires, alors ils sont uniques.
Si le pgcd (unitaire) et P_1 et P_2 est 1, on dit que A et B sont premiers entre eux.

Démonstration. I D'après le lemme, il existe un polynôme $D \in \mathbb{K}[X]$ tel que $D\mathbb{K}[X] = P_1\mathbb{K}[X] + P_2\mathbb{K}[X]$, en particulier, $(P_1) \subset (D)$ et donc $D|P_1$ et de même, $D|P_2$.

II Soit $D' \in \mathbb{K}[X]$ un diviseur commun P_1 et P_2, on a $P_1\mathbb{K}[X] \subset D'\mathbb{K}[X]$ et $P_2\mathbb{K}[X] \subset D'KX$ donc $P_1\mathbb{K}[X] + ¶_2KX = D\mathbb{K}[X] = D'\mathbb{K}[X]$ et donc $D'|D$.

On montre l'existence du ppcm de la même manière.

□

Proposition 2.2.6 (Théorème de Bézout)

Soient $A, B \in \mathbb{K}[X]$. Les polynômes A et B sont premiers entre eux si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BC = 1$.

Démonstration. L'implication découle directement du lemme. Réciproquement, si $AU + BV = 1$, si D divise A et B, il divise $AU + BV = 1$ donc D est constant. □

Proposition 2.2.7 (Lemme de Gauss)

Soient $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et A et B sont premiers entre eux, alors $A \mid C$.

Démonstration. (La même que dans $\mathbb{Z}$). D'après le théorème de Bézout, il existe des polynômes U, V tels que $AU+BV = 1$ et donc $ACU+BCV = C$ et comme $A \mid BC$, il existe un polynôme Q tel que $AQ = BC$. En remplaçant, on obtient $A(CU + QV) = C$ et donc $A \mid C$. □

2.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème 2.3.1

Soit $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Démonstration. Par le chapitre précédent, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$. Le résultat en découle immédiatement.

□

Théorème 2.3.2 (Petit théorème de Fermat)

Soit p un entier premier et a un entier. On a les deux énoncés équivalents suivants :

1. Si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$.
2. $a^p \equiv a \pmod{p}$.

Démonstration.

1. Par ce qui précède, $\mathbb{Z}/p\mathbb{Z}$ est un corps et donc le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p-1$. Le théorème de Lagrange donne $\overline{a}^{p-1} = \overline{1}$ et donc en termes de congruences, $a^{p-1} \equiv 1 \pmod{p}$.
2. Si a n'est pas divisible par p, il suffit de multiplier 1. par a. Sinon, l'équation devient $0 \equiv 0 \pmod{p}$ qui est vérifiée.

□

Théorème 2.3.3 (Théorème des restes chinois)

Soit $m, n \geq 1$ des entiers premiers entre eux, l'application

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \overline{a} \mapsto (\mathring{a}, \tilde{a})$$

est bien définie et est un isomorphisme d'anneaux.

Démonstration. Le fait que l'application est bien définie découle de 2.1.27. On vérifie facilement que c'est un morphisme injectif. La bijectivité découle de l'injectivité car les cardinaux de la source et du but sont les mêmes. □

Definition 2.3.4 (Indicatrice d'Euler)

Soit $n \geq 1$ entier, on défini la fonction indicatrice d'Euler $\varphi(n)$ comme le nombre d'entiers entre 1 et n premiers avec n.

$$\varphi(n) = \text{Card}\{1 \leq k \leq n \mid k \wedge n = 1\}$$

.
De manière équivalente, c'est l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Dans toute la suite, sauf mention contraire, φ désignera la fonction indicatrice d'Euler.

Théorème 2.3.5 (Theorème d'Euler)

Soit n un entier strictement positif et a un entier premier avec n, on a : $a^{\varphi}(n) \equiv 1 \pmod{n}$.

Démonstration. Comme $a \wedge n = 1$, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ qui est d'ordre $\varphi(n)$ donc d'après le théorème de Lagrange, $\overline{a}^{\varphi(n)} = \overline{1}$ d'où le résultat. □

Proposition 2.3.6 (Propriété de l'indicatrice 1)

1. Pour $m, n \geq 1$ entiers premiers entre eux, on a $\varphi(mn) = \varphi(m)\varphi(n)$.
2. Pour p premier, $\varphi(p) = p - 1$.
3. Pour p et q premiers distincts, on a $\varphi(pq) = (p-1)(q-1)$.

Démonstration.

1. En considérant l'isomorphisme du théorème des restes chinois, les inversibles de $\mathbb{Z}/mn\mathbb{Z}$ correspondent aux couples formés par un inversible de $\mathbb{Z}/n\mathbb{Z}$ et un inversible de $\mathbb{Z}/m\mathbb{Z}$ donc on a le résultat.
2. Evident.
3. Parmi les pq premiers entiers, tous sont premiers avec pq sauf les q mutiples de p et les p multiples de q. Par inclusion exclusion, on a compté pq deux fois car c'est un multiple de p et q. Au final, $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

□

2.3.1 RSA

RSA...

Fin du cours de structures algébriques 1.
Début du cours de structures algébriques 2.

Proposition 2.3.7 (Propriétés de l'indicatrice 2)

On a les propriétés suivantes :

1. $\varphi(1) = 1$
2. Si p est premier et n entier naturel,
$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(1 - \frac{1}{p})$$
3. Si $N \geq 1$ est un entier dont la décomposition en facteurs premiers est $N = \prod_{i \in I} p_i^{\alpha_i}$ alors
$$\varphi(N) = \prod_{i \in I}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = N \prod_{i \in I}(1 - \frac{1}{p_i})$$
.

Démonstration. 1. Evident.

2. Les seuls entiers entre 1 et p^n non premiers avec p^n sont les multiples de p, il y en a p^{n-1}. Les autres égalités s'en déduisent.
3. Les $p_i^{\alpha_i}$ sont premiers entre-eux, en combinant avec les autres formules on a le résultat.

□

2.4 Polynomes vs fonctions polynomiales

Definition 2.4.1 (Fonction polynomiale)

Soit $P \in \mathbb{K}[X]$ la fonction $p : \mathbb{K} \to \mathbb{K}, x \mapsto P(x)$ est appelée fonction polynomiale associée à P.

Théorème 2.4.2

Pour $P \in \mathbb{K}[X]$, on note p la fonction polynomiale associée à P. On considère l'application $\Phi : \mathbb{K}[X] \to \mathcal{F}(\mathbb{K}, \mathbb{K}), P \mapsto p$, on :

1. L'application Φ est un morphisme d'anneaux
2. Si $\mathbb{K}$ est fini, alors Φ n'est pas injective (mais surjective)
3. Si $\mathbb{K}$ est infini, alors Φ est injective (mais pas surjective).

Démonstration. 1. Simple vérification.

2. Comme $\mathbb{K}$ est fini, $\mathcal{F}(\mathbb{K}, \mathbb{K})$ aussi, alors que $\mathbb{K}[X]$ est infini, donc Φ n'est pas injective. L'aspect surjectif ne nous intéresse pas dans ce cours mais on peut par exemple utiliser l'interpolation de Lagrange
3. Le noyau de Φ est trivial car si $P \in \ker \Phi$, P admet une infinité de racines (car $\mathbb{K}$ est infini) et donc P est le polynôme nul. Le fait que Φ n'est pas surjective ne nous intéresse pas non plus dans ce cours mais par exemple la fonction exponentielle n'est pas polynomiale.

□

Remarque 2.4.3

On déduit du théorème précédent que si $\mathbb{K}$ est infini, on peut identifier polynôme et fonction polynomiale.

2.5 Factorisation en irréductibles

Dans la suite, R est un anneau intègre et $A = \mathbb{Z}$ ou $\mathbb{K}[X]$.

Definition 2.5.1 (Elements associés, irréductibles, premiers)

Soit $p, q \in R$,

1. p et q sont associés s'il existe $c \in R$ inversible tel que $p = cq$.
2. p est irréductible s'il est non nul, non inversible et ses seuls diviseurs sont les inversibles et les éléments associés à p. (Une autre définition équivalente :p est irréductible s'il est non nul, non inversible et si on écrit $p = ab$ avec $a, b \in R$ alors a ou b est inversible)
3. p est premier si pour tout $a, b \in R$ tels que p divise ab, p divise a ou p divise b.

Exemple 2.5.2 (Elements associés de $\mathbb{Z}$, de $\mathbb{K}[X]$, irréductibles de $\mathbb{Z}$)

— Comme les inversibles de $\mathbb{Z}$ donc ± 1, les éléments associés à $n \in \mathbb{Z}$ donc $\pm n$.

— Comme les inversibles de $\mathbb{K}[X]$ sont les éléments de $\mathbb{K}^*$, les éléments associés à $P \in \mathbb{K}[X]$ sont les aP avec $a \in \mathbb{K}^*$.

— Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p premier.

Lemme 2.5.3 (Quelques lemmes/résultats dans $\mathbb{K}[X]$)

1. Les polynômes de degré 1 sont irréductibles.
2. Soit $P, Q \in \mathbb{K}[X]$ irréductibles. Si $P \mid Q$ alors P et Q sont associés.
3. Lemme d'Euclide : Soit $P, A, B \in \mathbb{K}[X]$ avec P irréductible et divisant AB, alors $P|A$ ou $P|B$.

Démonstration. 1. Evident.

2. Evident.
3. Conséquence directe du lemme de Gauss.

□

Théorème 2.5.4 (Décomposition en produits d'irréductibles)

Tout $m \in A$ non nul, non inversible peut se décomposer en un produit fini d'irréductibles. Cette décomposition est "unique" à ordre et à inversible près.

Démonstration. 1. Pour $m \in A = \mathbb{Z}$, si $m > 0$, on retrouve le théorème fondamental de l'Arithmétique, si $m < 0$, on décompose $-m > 0$ et on multiplie par -1 qui est inversible.

2. Existence : Soit $P \in A = \mathbb{K}[X]$ non nul, non inversible. On raisonne par récurrence forte sur le degré de P. Si $\deg P = 1$ le résultat est clair, sinon, soit P est irréductible et il n'y a rien à faire, soit il existe A, B de degrés au moins un tels que $P = AB$ et comme $\deg A < \deg P$ et $\deg B < \deg P$, on peut appliquer l'hypothèse de récurrence.
Unicité : Supposons que $\mathbb{K}[X] \ni P = A_1 \dots A_r = B_1 \dots B_s$ avec $A_1, \dots A_r, B_1, \dots, B_s$ irréductibles. On raisonne par récurrence sur r.

Si $r = 1$, le résultat est évident. Sinon, d'après le lemme d'Euclide, A_1 divise un des B_i pour $i \in \{1, \dots, s\}$, quitte à changer l'ordre, on peut supposer que A_1 divise B_1, donc A_1 et B_1 sont associés donc il existe $c \in \mathbb{K}^*$ tel que $A_2 \dots A_r = cB_2 \dots B_s$. On applique alors l'hypothèse de récurrence.

□

Remarque 2.5.5 (Anneau factoriel)

Un anneau dans lequel tout élément non nul, non inversible peut se décomposer de manière "unique" est appelé un anneau factoriel.

Exemple 2.5.6 (Anneau sans unicité de la factorisation)

L'anneau $\mathbb{Z}/8\mathbb{Z}$ n'est pas factoriel car par exemple on a $X^2 - \overline{1} = (X - \overline{1})(X + \overline{1}) = (X - \overline{3})(X + \overline{3})$.

2.6 Irréductibles de $\mathbb{K}[X]$

Théorème 2.6.1 (Théorèmes du reste et du facteur)

Soit $P \in R[X]$ et $a \in R$.

1. Théorème du reste : Le reste de la division de P par $(X - a)$ est $P(a)$.
2. Théorème du facteur : $X - a$ divise P si et seulement si $P(a) = 0$.

Démonstration. 1. Soit $P(X) = Q(X)(X - a) + R(x)$ avec $R = 0$ ou $\deg(R) < 1$ la division euclidienne de P par $X - a$, en évaluant en $X = a$, on obtient $P(a) = Q(a)(a - a) = R(a)$ d'où le résultat.

2. Immédiat.

□

Théorème 2.6.2 (Nombre maximal de racines)

Un polynôme de $\mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$.

Démonstration. Conséquence immédiate de la décomposition en produit d'irréductibles. □

Definition 2.6.3 (Corps algébriquement clos)

Un corps K est algébriquement clos si tout polynôme non constant de $K[X]$ admet une racine dans K.

Théorème 2.6.4 (Théorème fondamental de l'algèbre (théorème de d'Alembert-Gauss))

Le corps $\mathbb{C}$ est algébriquement clos.

Démonstration. De nombreuses preuves existent, toutes celles que j'ai vues dépassent le cadre de de ce cours, celle-ci est cependant relativement simple à suivre. □

Corollaire 2.6.5 (Irréductibles de $\mathbb{C}[X]$)

Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration. Conséquence immédiate du théorème et du fait que les polynômes de degré 1 sont toujours irréductibles. □

Definition 2.6.6 (Polynome scindé)

Un polynôme de $\mathbb{K}[X]$ est scindé (sur $\mathbb{K}$) s'il est décomposable en facteurs de degré 1 sur $\mathbb{K}$.

Corollaire 2.6.7

Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Démonstration. Récurrence immédiate. □

Théorème 2.6.8 (Quelques critères d'irréductibilité dans $\mathbb{K}[X]$)

Soit $P \in \mathbb{K}[X]$.

- Si $\deg P \geq 2$ et P a une racine dans $\mathbb{K}$, alors P est réductible dans $\mathbb{K}[X]$.
- Si $\deg P \in \{2, 3\}$, alors P est irréductible si et seulement si il n'a pas de racine dans $\mathbb{K}$.

Démonstration. — Théorème du facteur

— Pour le degré 3, P est réductible si et seulement si il existe des polynômes non constants tels que $P = QR$ mais alors $\deg P = 1$ ou $\deg Q = 1$ et donc P admet une racine. Pour le degré 2 idem mais les deux sont de degré 1.

□

Exemple 2.6.9 (Réductibles sans racines)

Le polynôme $P(X) = X^4 + 1$ n'a clairement pas de racine dans $\mathbb{R}$ mais il est de degré 4 et donc réductible dans $\mathbb{R}$ $P(X) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ par contre, il est irréductible comme polynôme de $\mathbb{Q}[X]$. On peut aussi montrer qu'il est réductible dans tout $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Théorème 2.6.10 (Irréductibles de $\mathbb{R}[X]$)

Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles.

Démonstration. D'après ce qui précède, on sait déjà que les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles sont irréductibles. Soit $P \in \mathbb{R}[X]$ de degré supérieur ou égal à 3, si P admet une racine réelle, il est réductible, sinon, P admet une racine $z \in \mathbb{C}$
$\mathbb{R}$ et on vérifie que $\overline{z}$ est aussi racine de P donc P est divisible par $(X - z)(X - \overline{z}) = X^2 - 2\Re(z) + |z|^2 \in \mathbb{R}[X]$ et est donc réductible. □

2.7 Dérivée formelle et racines

Definition 2.7.1 (Polynôme dérivé, Dérivée formelle)

Soit $\mathbb{K}[X] \ni P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme.
On appelle polynôme dérivé de P et on note P' ou DP le polynôme $P'(X) = DP(X) = \sum_{k=1}^{n} k a_k X^{k-1}$ (Si $P = 0$, on pose $P' = 0$.)
L'application $D : \mathbb{K}[X] \to \mathbb{K}[X], P \mapsto P'$ est appelée dérivation formelle.

Théorème 2.7.2 (Propriétés de la dérivée formelle)

L'application $D : \mathbb{K}[X] \to \mathbb{K}[X], P \mapsto P'$ est K-linéaire et vérifie $D(PQ) = D(P)Q + PD(Q)$ pour tout $P, Q \in \mathbb{K}[X]$.

Démonstration. La linéarité est évidente, pour la formule du produit, il suffit, par linéarité de montrer le résultat pour les monômes. Si $P = X^m, Q = X^n$, on a $D(PQ) = D(X^{m+n}) = (m+n)X^{m+n-1}$ et $D(P)Q + PD(Q) = mX^{m-1}X^n + X^m nX^{n-1} = (m+n)X^{m+n-1}$ d'où le résultat. □

Corollaire 2.7.3 (Dérivée d'une puissance)

Pour $m > 0$ entier et $P \in \mathbb{K}[X]$, on a $(P^m)' = mP'P^{m-1}$.

Démonstration. Par récurrence sur m, le résultat est évident pour $m = 1$. Supposons le vérifié pour $m-1$, on a alors $(P^m)' = (P^{m-1}P)' = (P^{m-1})'P + P'(P^{m-1}) = (m-1)P^{m-2}P'P + P'(P^{m-1}) = P^{m-1}P'(m-1+1) = mP'P^{m-1}$. □

Théorème 2.7.4 (Formule de Taylor)

Ici, K est supposé de caractéristique nulle. Soit $P(X) \in \mathbb{K}[X]$ de degré n et $a \in K$. On a $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)(X-a)^k}{k!}$.

Démonstration. On note $P(X) = a_0 + a_1X + \cdots a_nX^n$, il est clair qu'il existe des éléments $b_0, \cdots, b_n \in \mathbb{K}$ tels que $P(X) = b_0 + b_1(X-a) + \cdots b_n(X-a)^n$, en effet on prend $b_n = a_n$ puis on prend b_{n-1} pour avoir le bon coefficient de X^{n-1} etc de proche en proche. Pour exprimer les coefficients en fonction des dérivées, il suffit d'évaluer celles-ci en $X = a$. On trouve immédiatement $b_0 = P(a)$ puis on calcule $P'(x) = nb_n(X-a)^{n-1} + \cdots + 2b_2(X-a) + b_1$ ce qui donne après évaluation $b_1 = P'(a)$, on trouve ensuite $P''(a) = 2b_2$ et plus généralement $k!b_i = P^{(i)}(a)$ d'où la formule annoncée. □

Corollaire 2.7.5 (Multiplicité et dérivée)

Ici encore, K est supposé de caractéristique nulle. Soit $m > 0$ entier,$P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

1. $(X-a)^m$ divise $P(X)$ si et seulement si
$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$$
.
2. a est une racine de multiplicité m si et seulement si
$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \text{ et } P^{(m)} \neq 0$$
.

Démonstration.
1. En prenant la formule de Taylor, $(X-a)^m | P(x)$ si et seulement si les m premiers coefficients sont nuls, c'est à dire $P(a) = \cdots = P^{(m-1)}(a) = 0$
2. Conséquence immédiate du point précédent.

□

Proposition 2.7.6

Soit $a \in K$ et $P \in \mathbb{K}[X]$. Si a est une racine multiple de P, alors $P \wedge P' \neq 1$.

Démonstration. Comme a est racine au moins double, il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^2 Q(X)$ et $P'(X) = 2(X-a)Q(X) + (X-a)^2 Q'(X) = (X-a)(2Q(X) + (X-a)Q'(X))$ donc $(X-a)$ divise P et P' d'où le résultat. □

Théorème 2.7.7 (Racines multiples dans une extension de corps)

Soit $L \supset K$ un corps (on dit que L est une extension de K) et $P \in \mathbb{K}[X]$ scindé sur L.
Alors P n'a pas de racine multiple dans L si et seulement si $P \wedge P' = 1$ dans $\mathbb{K}[X]$.

Démonstration. On commence par montrer le résultat pour $L = K$. Supposons donc P scindé simple sur K et que $P \wedge P' \neq 1$, il existe donc a racine commune à P et P', donc il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)Q(x)$ et donc $P'(X) = Q(X) + (X-a)Q'(X)$ mais en évaluant en $X = a$, on obtient

$0 = P'(a) = Q(a)$ donc a est racine de Q et donc $(X-a)^2 | P(X)$ ce qui est exclu. La réciproque est la contraposée de la proposition précédente. Le fait que le résultat reste valable pour $L \supset K$ est du au fait que le pgcd dans $\mathbb{K}[X]$ est aussi celui dans $L[X]$. □

Exemple 2.7.8

— Pour $n > 0$ entier, $X^n - 1$ n'a pas de racine multiple dans $\mathbb{C}[X]$ car $\text{pgcd}(X^n - 1, nX^{n-1}) = 1$.

— Pour p premier, $X^p - X$ n'a pas de racine multiple car $(X^p - X)' = pX^{p-1} - 1 \equiv \overline{-1} \pmod{p}$ donc $\text{pgcd}(X^p - X, pX^{p-1} - 1) = 1$

2.8 Racines rationnelles d'un polynôme à coefficients entiers

Théorème 2.8.1 (Théorème de la racine rationnelle)

Soit $P = a_0 + \cdots + a_n X^n$ un polynôme à coefficients entiers, r, s deux entiers premiers entre-eux avec $s \neq 0$. Si $\frac{r}{s}$ est racine de P dans $\mathbb{Q}[X]$, alors $s \mid a_n$ et $r \mid a_0$.

Démonstration. On a $0 = s^n \times 0 = s^n P(\frac{r}{s}) = a_0 s^n + \cdots + a_{n-1} r^{n-1} s + a_n r^n$ donc $s(a_0 s^{n-1} + \cdots + a_{n-1}) = -a_n r^n$ donc $s \mid a_n r^n$ or $s \wedge r^n = 1$ donc d'après le lemme de Gauss, $s | a_n$. De la même manière, $0 = s^n \times 0 = s^n P(\frac{r}{s}) = a_0 s^n + \cdots + a_{n-1} r^{n-1} s + a_n r^n$ donc $r(a_1 s^{n-1} + \cdots a_n r^{n-1}) = -a_0 s^n$ or $r \wedge s^n 1$ donc $r \mid a_0$. □

Corollaire 2.8.2

Soit $P = a_0 + a_1 X + \cdots + X^n$ un polynôme unitaire à coefficients entiers, alors toute racine de P est entière et divise a_0.

Démonstration. Conséquence immédiate du théorème précédent. □

Exemple 2.8.3

On cherche à factoriser $X^3 + X - 10$ dans $\mathbb{Q}[X]$, d'après ce qui précède, il suffit de vérifier si $\{\pm 1, \pm 2, \pm 5, \pm 10\}$ sont racines. On trouve que 2 est la seule racine et que $X^3 + X - 10 = (X-2)(X^2 + 2X + 5)$.

Chapitre 3

Groupes 2 : Le retour

3.1 Groupes cycliques

Lemme 3.1.1

Soit H un groupe cyclique d'ordre n, alors H contient :

1. n éléments x tels que $x^n = e$.
2. $\varphi(n)$ générateurs (éléments d'ordre n).

Démonstration. 1. Immédiat d'après le théorème de Lagrange.

2. H est cyclique fini donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et l'ordre d'un élément $y \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{y \wedge n}$ donc il y a exactement $\varphi(n)$ éléments d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$.

□

Théorème 3.1.2

Soit H un groupe cyclique d'ordre n et d un diviseur de n alors H contient :

1. d éléments x tels que $x^d = e$.
2. $\varphi(d)$ éléments d'ordre d.

Démonstration. Soit $x \in H$ d'ordre d, par définition, $< x >$ est cyclique d'ordre d, il suffit donc d'appliquer le lemme précédent. □

Corollaire 3.1.3 (Une jolie formule)

Soit $n > 1$ un entier naturel, on a :

$$\sum_{d|n} \varphi(d) = n$$

.

Démonstration. Les ordres forment une partition du groupe $\mathbb{Z}/n\mathbb{Z}$ donc le théorème précédent donne le résultat. □

Démonstration. Autre preuve : si $n = p^k$ avec p premier, $\sum_{d|n} \varphi(d) = \sum_{l=0}^{k} \varphi(p^l) = 1 + \sum_{l=1}^{k} (p^l - p^{l-1}) = p^k = n$ et comme φ est multiplicative, on obtient le résultat pour n quelconque en considérant sa factorisation en produit de facteurs premiers. □

Dans la suite, on note $\lambda_d(G)$ le nombre d'éléments d'ordre d dans G avec G un groupe fini d'ordre n et d un diviseur de n.

Proposition 3.1.4

Soit G un groupe fini d'ordre n, on a :

$$\sum_{d|n} \lambda_d(G) = n$$

.

Démonstration. La preuve est la même que le corollaire précédent. □

Remarque 3.1.5

Si G n'est pas cyclique, $\lambda_n(G) = 0$ et donc il existe un diviseur d_0 de n tel que $\lambda_{d_0}(G) > \varphi(d_0)$ ce qui amène au résultat suivant.

Lemme 3.1.6

Soit G un groupe fini non cyclique d'ordre n, il existe un diviseur d_0 de n tel que :

1. G contient plus de $\varphi(d_0)$ éléments d'ordre d_0.
2. G contient plus de d_0 éléments x tels que $x^{d_0} = e$.

Démonstration.

1. On a $\sum_{d|n} \varphi(d) = \sum_{d|n} \lambda_d(G) = n$ et $\lambda_{d_0}(G) > \varphi(d_0)$ et comme les deux sommes sont sur les diviseurs de n, on a le résultat.
2. Comme $\lambda_{d_0}(G) > \varphi(d_0) > 0$,il existe $y \in G$ d'ordre d_0 mais alors $< y >= \{e, y, y^2, \ldots, y^{d_0-1}\}$ est un sous groupe de G d'ordre d_0 donc tous ses éléments x vérifient x^{d_0} mais comme $\lambda_{d_0}(G) > \varphi(d_0)$ il existe encore au moins un autre élément $u \notin < y >$ tel que $u^{d_0} = e$ d'ù le résultat.

□

Théorème 3.1.7 (Les sous-groupes fini du groupe multiplicatif d'un corps sont cycliques)

Soit $\mathbb{K}$ un corps. Tout sous-groupe fini de $\mathbb{K}^*$ est cyclique.

Démonstration. Soit G un sous-groupe fini de $\mathbb{K}^*$ d'ordre n. Supposons G non cyclique, par ce qui précède, il existe $d_0|n$ tel que G contient plus de d_0 éléments x tels que $x^{d_0} = 1$ et donc le polynôme $x^{d_0} - 1 \in K[X]$ admet plus de d_0 racines et donc est nul, ce qui est absurde. □

Corollaire 3.1.8

Soit p premier, le groupe (multiplicatif) $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique et isomorphe au groupe (additif) $\mathbb{Z}/(p-1)\mathbb{Z}$.

Démonstration. Conséquence immédiate du théorème précédent comme $(\mathbb{Z}/p\mathbb{Z})^*$ est un corps d'ordre $p-1$. □

Exemple 3.1.9

Pour $n \geq 1$ entier, le groupe des racines n-èmes (complexes) de l'unité est cyclique (de générateur $e^{i\frac{2k\pi}{n}}$ avec $k \wedge n = 1$).

3.2 Actions de groupes

Definition 3.2.1 (Action de groupe)

Soit G un groupe et E un ensemble, une action (à gauche) de G sur E est une application $G \times E \to E : (g, x) \mapsto gx$ vérifiant les deux propriétés suivantes :

1. Pour tout $x \in E$, $ex = x$.
2. Pour tout $g, g' \in G$ et $x \in E$, $g(g'(x)) = (gg')x$.

On dit aussi que G agit (ou opère) sur l'ensemble E.

Attention aux notations, ici on note de la même manière (c'est à dire sans rien !) l'action et l'opération du groupe.

Exemple 3.2.2 (Exemples d'actions)

— $\mathrm{GL}_n(K)$ agit sur $\mathbb{K}^n$ par l'action $(A, v) \mapsto Av$.

— Plus généralement, $\mathrm{GL}_n(K)$ agit sur $\mathcal{M}_{n,m}$ par l'action (sur les lignes) $(A, M) \mapsto AM$.

— On peut voir les translations, rotations, symétries comme des actions sur le plan.

— Le groupe S_n agit naturellement sur $\{1, 2, \ldots, n\}$.

— Un groupe G opère sur lui-même par translation à gauche : $(g, x) \mapsto gx$, et par conjugaison $(g, x) \mapsto gxg^{-1}$.

Théorème 3.2.3

Soit G un groupe et E un ensemble. Supposons que G agisse sur E, alors l'application l'application $\phi : E \to E, x \mapsto gx$ est un morphisme de groupe de E dans S_E. Réciproquement, un tel morphisme ϕ définit une action de G sur E en prenant $gx = \phi(g)(x)$..

Démonstration. On a $ex = x$ pour tout $x \in E$ donc $\phi(e) = Id_E$, et on a $g(g^{-1}x) = (gg^{-1})x = x = (g^{-1}g)x = g^{-1}(gx)$ donc $\phi(g)\phi(g^{-1}) = \phi(g^{-1})\phi(g) = Id_E$ donc ϕ est bijective et enfin, pour tout $g, g' \in G, x \in E$, on a $g(g'x) = (gg')x$ donc $\phi(gg') = \phi(g)\phi(g')$. La réciproque se montre de manière analogue. □

3.3 Signature d'une permutation

Théorème 3.3.1 (Signature d'une permutation)

Soit $n \geq 2$, il existe un unique morphisme de groupe non trivial $\varepsilon : S_n \to (\pm 1, \times)$ tel que $\varepsilon((ij)) = -1$ pour toute transposition (ij).

Si γ est un cycle de longueur l, alors $\varepsilon(\gamma) = (-1)^{l-1}$.

Démonstration. L'unicité est assez claire car les transpositions engendrent S_n et que toutes sont conjuguées.

La propriété sur les cycles évidente car on a vu qu'on peut décomposer un cycle de longueur l en $l-1$ transpositions.

La preuve de l'existence va demander plus de travail. □

Definition 3.3.2 (Polynôme symétrique)

Soit $P \in K[X_1, X_2, \ldots, X_n]$, on dit que P est symétrique s'il est invariant par permutation de ses indices, c'est à dire si pour toute permutation $\sigma \in S_n$, $P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

Definition 3.3.3 (Inversion pour une permutation)

Soit σ une permutation. Une inversion pour $\sigma \in S_n$ est un couple d'entiers (i, j) dans $\{1, \ldots, n\}$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Démonstration. Preuve de l'existence de la permutation :
Pour $\sigma \in S_n$, on note $I(\sigma)$ le nombre d'inversions de σ et on pose $\epsilon(\sigma) = (-1)^{I(\sigma)}$, il est clair que ϵ est une application surjective de S_n dans $\{\pm 1\}$ qui vaut -1 pour toute transposition. Montrons que c'est bien un morphisme de groupes. On va utiliser l'action de S_n sur l'ensemble des polynômes à n indéterminées $\mathbb{C}[X_1, \ldots, X_n]$,$(\sigma, P(X_1, \ldots, X_n) \mapsto P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Considérons le polynôme (de Vandermonde) $V(X_1, \ldots X_n) = \prod_{i<j}(X_j - X_i)$ et calculons $\sigma V(X_1, \ldots X_n) = \prod_{i<j}(X_{\sigma(j)} - X_{\sigma(i)})$.

Pour un couple (i, j) avec $i < j$, il y a deux cas possibles, soit (i, j) est une inversion et on pose $i' = \sigma(j), j' = \sigma(i)$, soit (i, j) n'est pas une inversion et on pose $i' = \sigma(i), j' = \sigma(j)$ de sorte que $i' < j'$. On a donc $(X_\sigma(j) - X_\sigma(i)) = \pm(X_{j'} - X_{i'})$ et , en considérant tous les couples, $\sigma V(X_1, \ldots, X_n) = \epsilon(\sigma) \prod_{i'<j'}(X_{j'} - X_{i'})$ et comme on a une action de groupe, pour $\sigma, \tau \in S_n$, $\epsilon(\sigma\tau)V = (\sigma\tau)V = \sigma(\tau V) = \sigma(\epsilon(\tau)V) = \epsilon(\tau)\sigma V = \epsilon(\tau)\epsilon(\sigma)V$ et on a bien $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$ donc ϵ est bien un morphisme de groupes. □

Definition 3.3.4 (Déterminant à partir de la signature)

Soit $A = (a_{ij})$ una matrice carrée d'ordre n. On a la formule suivante (de Leibniz) :

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}$$

.

Remarque 3.3.5

Cette formule possède évidement (la somme contient $n!$ termes !) un intérêt calculatoire limité mais elle a un intérêt théorique.

Definition 3.3.6 (Groupe alterné)

Comme la signature est un morphisme de groupes, son noyau est un groupe, appelé groupe alterné et noté A_n.

Exemple 3.3.7 (A_3)

On vérifie par exemple que $A_3 = \{id, (123), (132)\}$.

Bibliographie

[1] Calais Josette 1931-2022. *Eléments de théorie des groupes.* Mathématiques. [3e édition]. edition, 1998.

[2] Jean-Pierre Ramis 1943-... *Mathématiques : tout-en-un pour la Licence 1.* 4e édition. edition, 2022.

[3] Berhuy Grégory 1973-... *Algèbre : le grand combat.* Mathématiques en devenir 121. 2018.

[4] Chenevier Gaetan. Algèbre 1. `http://gaetan.chenevier.perso.math.cnrs.fr/AlgebreI.html`. [Accessed 02-10-2024].

[5] Jean-Pierre Serre. Groupes finis. `https://arxiv.org/abs/math/0503154`. [Accessed 02-10-2024].