

Licence de Mathématiques
ALGÈBRE

GROUPES, ANNEAUX, CORPS
(Résumé de cours)

Jean-Luc Chabert

1998/1999

Chapter 1

Groupes

1.1 Relations d'équivalence et ensembles quotients

Définition. Se donner une *relation binaire* dans un ensemble E , c'est se donner une partie $\mathcal{R}$ de l'ensemble produit $E \times E = \{(x, y) \mid x, y \in E\}$. On écrit $x\mathcal{R}y$ au lieu de $(x, y) \in \mathcal{R}$. La relation $\mathcal{R}$ est dite :

- *réflexive* si, pour tout $x \in E$, $x\mathcal{R}x$,
- *symétrique* si, pour tous $x, y \in E$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$,
- *transitive* si, pour tous $x, y, z \in E$, $[x\mathcal{R}y \text{ et } y\mathcal{R}z] \Rightarrow x\mathcal{R}z$.

Définition. Une *relation d'équivalence* dans un ensemble E est une relation binaire dans E qui est à la fois réflexive, symétrique et transitive.

Exemples. a) Les congruences dans $\mathbb{Z}$.

b) Si $g : E \rightarrow F$, alors $g(x) = g(y)$ définit une relation d'équivalence dans E que l'on notera $\mathcal{R}_g$ [$x\mathcal{R}_g y := g(x) = g(y)$].

Définitions. Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E .

1. Deux éléments $x, y \in E$ sont dits *équivalents* si $x\mathcal{R}y$.
2. Pour tout $x \in E$, l'ensemble $\{y \in E \mid x\mathcal{R}y\}$ est appelé *classe d'équivalence* de x suivant la relation $\mathcal{R}$ (on la notera souvent $\bar{x}$).
3. Tout élément de $\bar{x}$ est appelé un *représentant* de la classe $\bar{x}$.

Proposition 1.1.1 *Soit E un ensemble.*

1. *Si $\mathcal{R}$ est une relation d'équivalence dans E , alors les classes d'équivalence suivant $\mathcal{R}$ forment une partition de l'ensemble E .*
2. *A toute partition de E correspond une relation d'équivalence $\mathcal{R}$ dont les classes sont les éléments de cette partition.*

Définition. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. L'ensemble des classes d'équivalence est appelé *ensemble quotient* de E par $\mathcal{R}$, on le note $E/\mathcal{R}$. L'application $p : x \in E \mapsto \bar{x} \in E/\mathcal{R}$ est appelée *surjection canonique* de E sur $E/\mathcal{R}$.

Proposition 1.1.2 [Décomposition canonique d'une application].

Soit $g : E \rightarrow F$ une application. Soient $\mathcal{R}_g$ la relation d'équivalence dans E associée, $p : E \rightarrow E/\mathcal{R}_g$ la surjection canonique et $j : f(E) \rightarrow F$ l'injection-inclusion de $f(E)$ dans F . Alors il existe une application et une seule (en fait une bijection) $\bar{g} : E/\mathcal{R}_g \rightarrow g(E)$ telle que g soit l'application composée :

$$g : E \xrightarrow{p} E/\mathcal{R}_g \xrightarrow{\bar{g}} f(E) \xrightarrow{j} F.$$

1.2 Lois de composition et quotients

Définition. Une *loi de composition* (interne) sur un ensemble E est une application de $E \times E$ dans $E : (x, y) \mapsto x * y$. On dit que cette loi :

- est *associative* si, pour tous $x, y, z \in E$, on a $(x * y) * z = x * (y * z)$,
- est *commutative* si pour tous $x, y \in E$, on a $x * y = y * x$,
- possède un *élément neutre* s'il existe un élément e de E tel que, pour tout $x \in E$, on a : $x * e = e * x = x$.

Si une loi possède un élément neutre, alors celui-ci est nécessairement unique.

Définition. Considérons une loi de composition $*$ sur E possédant un élément neutre e . On dit qu'un élément x de E possède :

- un *inverse à gauche* s'il existe x' dans E tel que $x' * x = e$,
- un *inverse à droite* s'il existe x'' dans E tel que $x * x'' = e$,
- un *inverse* s'il existe x' dans E tel que $x' * x = e = x * x'$ (on dit alors que x est *invertible*).

Si la loi $*$ est associative et possède un élément neutre et si l'élément x possède un inverse, alors celui-ci est nécessairement unique.

Exemple. Dans l'ensemble E^E des applications de E dans E , la composition des applications est associative et admet l'application identique 1_E pour élément neutre. Une application f admet un inverse à gauche g [$g \circ f = 1_E$] si et seulement si elle est injective et un inverse à droite h [$f \circ h = 1_E$] si et seulement si elle est surjective.

Définition. Soit E un ensemble muni d'une loi $*$. Une partie A de E est dite *stable* pour la loi $*$ si, quels que soient x et $y \in A$, $x * y \in A$.

Exemples. 1. $\mathbb{N}$ est une partie de $\mathbb{R}$ stable pour les lois $+$ et $\times$.
 2. Dans l'ensemble E^E muni de la composition, le sous-ensemble formé des applications injectives (resp. surjectives, resp. bijectives) est stable.

Les parties $\emptyset$ et E sont toujours stables.

Proposition 1.2.1 *Soit E un ensemble muni d'une loi $*$.*

1. *Une intersection de parties de E stables pour la loi $*$ est encore une partie stable.*
2. *Toute partie non vide A_0 de E est contenue dans une plus petite partie stable (à savoir, l'intersection des parties stables contenant A_0).*

Exemple. La plus petite partie de $\mathbb{R}$ stable pour la différence et contenant $\mathbb{N}$ est $\mathbb{Z}$.

Toute partie stable A de E peut être munie de la loi induite sur A par la loi $*$ de E .

Définition. Soit E un ensemble muni à la fois d'une loi $*$ et d'une relation d'équivalence $\mathcal{R}$. La relation $\mathcal{R}$ est dite *compatible* avec la loi $*$ si

$$\forall x, x', y, y' \in E \quad [x\mathcal{R}x' \text{ et } y\mathcal{R}y'] \Rightarrow (x * y)\mathcal{R}(x' * y').$$

Proposition 1.2.2 *Soit E un ensemble muni d'une loi $*$ et d'une relation d'équivalence $\mathcal{R}$. Si la relation $\mathcal{R}$ est compatible avec la loi $*$, alors il existe sur l'ensemble quotient $E/\mathcal{R}$ une loi et une seule (que l'on notera encore $*$) vérifiant :*

$$\forall x, y \in E \quad \overline{x} * \overline{y} = \overline{x * y}.$$

On l'appelle loi quotient de la loi de E par la relation $\mathcal{R}$.

Proposition 1.2.3 *Soit E un ensemble muni d'une loi $*$ et d'une relation d'équivalence compatible avec la loi.*

1. *Si la loi de E est associative (resp. commutative), la loi quotient est associative (resp. commutative).*
2. *Si e est élément neutre pour la loi de E , alors $\bar{e}$ est élément neutre pour la loi quotient.*
3. *Si $x \in E$ est inversible d'inverse x' , alors $\bar{x}$ est inversible d'inverse $\overline{x'}$.*

1.3 Groupes et sous-groupes

Définition. Un *groupe* est un ensemble G muni d'une loi (de composition interne)

- a) associative,
- b) possédant un élément neutre,
- c) telle que tout élément soit inversible,

autrement dit, on a :

- a) $\forall x, y, z \in G [(x * y) * z = (x * y) * z]$,
- b) $\exists e \in G$ tel que $\forall x \in G [x * e = e * x = x]$,
- c) $\forall x \in G \exists x' \in G$ tel que $[x * x' = x' * x = e]$.

Le plus souvent, on note multiplicativement la loi du groupe et on note x^{-1} l'inverse de x . Lorsque le groupe G est *commutatif* ou *abélien*, c'est-à-dire lorsque sa loi est commutative, on la note parfois additivement, et l'inverse de x est alors appelé l'*opposé* de x et est noté $-x$.

Définition. On appelle *ordre* d'un groupe G le nombre (fini ou infini) de ses éléments ; on le note souvent $|G|$.

Exemples. a) Soit E un ensemble non vide. Le sous-ensemble de E^E formé des applications bijectives est stable pour la composition des applications. Muni de la loi induite, c'est un groupe que l'on l'appelle *groupe des permutations* de E et que l'on le note Σ_E . Lorsque $E = \{1, 2, \dots, n\}$, on l'appelle *groupe symétrique* de degré n et on le note Σ_n (ou S_n). Son ordre est $|\Sigma_n| = n!$.

b) Soient E un ensemble et G un groupe (abélien). L'ensemble G^E des applications de E dans G est muni d'une façon naturelle d'une loi de groupe (abélien) : pour f et $g \in G^E$, $f + g$ est définie par $(f + g)(x) = f(x) + g(x)$ pour tout $x \in E$.

Définition. Un *sous-groupe* d'un groupe G est une partie H de G stable pour la loi du groupe et qui, munie de la loi induite, est un groupe.

Proposition 1.3.1 *Soit G un groupe. Pour qu'une partie non vide H de G soit un sous-groupe il faut et il suffit que H soit stable à la fois pour la loi du groupe ($x, y \in H \Rightarrow xy \in H$) et pour le passage à l'inverse ($x \in H \Rightarrow x^{-1} \in H$); ou encore, il faut et il suffit que H soit stable pour la loi $(x, y) \mapsto xy^{-1}$.*

Exemples. 1. G et $\{e\}$ sont toujours des sous-groupes de G (où e désigne l'élément neutre).

2. Les sous-groupes de $\mathbb{Z}$ sont exactement les ensembles $k\mathbb{Z} = \{kn \mid n \in \mathbb{N}\}$ où $k \in \mathbb{N}$.

3. Si H est un sous-groupe de G , alors, pour tout $x \in G$, l'ensemble $x^{-1}Hx = \{x^{-1}yx \mid y \in H\}$ est un sous-groupe de G , dit *conjugué* de H .

4. $Z(G) = \{x \in G \mid xy = yx \ \forall y \in G\}$ est un sous-groupe de G appelé *centre* de G .

Proposition 1.3.2 Soit G un groupe.

1. Toute intersection de sous-groupes de G est un sous-groupe de G .
2. Pour toute partie non vide A de G , il existe un plus petit sous-groupe de G contenant A (l'intersection des sous-groupes de G contenant A).

Définitions. Soit G un groupe.

1. Soit A une partie non vide de G . On appelle *sous-groupe engendré* par A le plus petit sous-groupe de G contenant A ; on le note $\langle A \rangle$.
2. Un *système de générateurs* de G est un ensemble B d'éléments de G tel que $G = \langle B \rangle$.

Exemples. 1. Le sous-groupe de $\mathbb{R}$ engendré par $\{2\}$ relativement à l'addition est l'ensemble $2\mathbb{Z}$.

2. Le groupe Σ_n admet l'ensemble des transpositions pour système de générateurs.

Proposition 1.3.3 Soient G un groupe et A une partie non vide de G . Le sous-groupe engendré par A est l'ensemble :

$$\langle A \rangle = \{x_1 \cdots x_n \mid n \in \mathbb{N}, x_i \in A \text{ ou } x_i^{-1} \in A\}.$$

1.4 Groupes quotients

Proposition 1.4.1 Soient G un groupe et H un sous-groupe de G . Considérons la relation suivante dans G : $x\mathcal{R}y := x^{-1}y \in H$.

1. $\mathcal{R}$ est une relation d'équivalence.
2. Le sous-groupe H est la classe de l'élément neutre.
3. Les classes sont de la forme $\bar{x} = xH = \{xh \mid h \in H\}$ et elles sont en bijection avec H .

Ces classes d'équivalence sont appelées *classes à gauche modulo H* . En considérant la relation $x\mathcal{R}y := yx^{-1} \in H$, on obtiendrait les sous-ensembles Hx , appelés *classes à droite modulo H* . Lorsque G est commutatif, pour tout $x \in G$, $xH = Hx$; on parle de *classes modulo H* .

Définition. Soit G un groupe et H un sous-groupe de G . On appelle *indice* de H dans G le nombre de classes à gauche (ou à droite) suivant H et on le note $[G : H]$.

Proposition 1.4.2 [Théorème de Lagrange]

Si l'ordre du groupe G est fini, l'ordre de tout sous-groupe H de G divise l'ordre de G et on a $|G| = [G : H]|H|$.

Corollaire 1.4.3 . Si l'ordre du groupe G est un nombre premier, G n'a pas de sous-groupes propres (c.-à-d. autres que $\{e\}$ et G).

Proposition 1.4.4 Soient G un groupe et H un sous-groupe de G . Pour que la relation d'équivalence $x\mathcal{R}y := x^{-1}y \in H$ soit compatible avec la loi du groupe, il faut et il suffit que :

$$\text{pour tout } x \in G, xHx^{-1} \subset H.$$

Cette condition revient encore à :

$$\text{pour tout } x \in G, xHx^{-1} = H,$$

ou encore à :

$$\text{pour tout } x \in G, xH = Hx.$$

Définition. On dit que le sous-groupe H de G est *distingué* si, pour tout $x \in G$, on a $xH = Hx$. On dit aussi que H est un sous-groupe *invariant* ou un sous-groupe *normal* de G . On écrit alors $H \triangleleft G$.

Exemples. a) $\{e\} \triangleleft G$, b) $G \triangleleft G$, c) $Z(G) \triangleleft G$.

Si G est commutatif, tout sous-groupe de G est distingué.

Proposition 1.4.5 Pour qu'une relation d'équivalence $\mathcal{R}$ dans un groupe G soit compatible avec la loi du groupe il faut et il suffit qu'elle soit de la forme $x\mathcal{R}y := x^{-1}y \in H$ où $H \triangleleft G$.

Proposition 1.4.6 Soient G un groupe et H un sous-groupe distingué de G . Si $\mathcal{R}$ désigne la relation d'équivalence associée à H , alors l'ensemble quotient $G/\mathcal{R}$ muni de la loi quotient est un groupe.

Définition. Soient G un groupe et H un sous-groupe distingué de G . Le groupe défini dans la proposition précédente est appelé *groupe quotient* de G par H et est noté G/H .

Si l'ordre de G est fini, on a la formule :

$$|G| = |G/H| \times |H|.$$

Si G est commutatif, G/H est commutatif.

1.5 Homomorphismes de groupes

Homomorphismes

Définition. Soient G et G' deux groupes (notés multiplicativement). Un *homomorphisme* de G dans G' est une application $f : G \rightarrow G'$ telle que, quels que soient $x, y \in G$, $f(xy) = f(x)f(y)$.

Si H est un sous-groupe de G , alors l'injection $j : H \rightarrow G$ est un homomorphisme. Si $H \triangleleft G$, alors la surjection $p : G \rightarrow G/H$ est un homomorphisme.

Proposition 1.5.1 *Si $f : G \rightarrow G'$ est un homomorphisme de groupes, alors*

$$f(x^n) = f(x)^n \quad \forall x \in G \quad \text{et} \quad \forall n \in \mathbb{Z}.$$

Par convention, $x^0 = e$ élément neutre. En notation additive, on aurait $f(x+y) = f(x)+f(y) \quad \forall x, y \in G$, et donc, $f(nx) = nf(x) \quad \forall x \in G, n \in \mathbb{N}$.

Proposition 1.5.2 *Soit $f : G \rightarrow G'$ un homomorphisme de groupes.*

1. *Pour tout sous-groupe H de G , $f(H) = \{f(x) \mid x \in H\}$ est un sous-groupe de G' .*
2. *Pour tout sous-groupe H' de G' , $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ est un sous-groupe de G . De plus, si $H' \triangleleft G'$, alors $f^{-1}(H') \triangleleft G$.*

Définition. Soit $f : G \rightarrow G'$ un homomorphisme de groupes. On appelle :
— *image* de f le sous-groupe $f(G)$ de G' ,
— *noyau* de f le sous-groupe distingué $f^{-1}(e') = \{x \in G \mid f(x) = e'\}$ où e' désigne l'élément neutre de G' ; on le note souvent $\text{Ker}(f)$.

Si $f : G \rightarrow G'$ est un homomorphisme, la relation d'équivalence $\mathcal{R}_f$ dans G associée à l'application f [$f(x) = f(y)$] est aussi la relation d'équivalence dans G associée au sous-groupe distingué $\text{Ker}(f)$ [$x^{-1}y \in \text{Ker}(f)$]. En particulier :

Proposition 1.5.3 *Un homomorphisme de groupes est injectif si et seulement si son noyau est réduit à $\{e\}$.*

Le composé de deux homomorphismes de groupes est un homomorphisme.

Isomorphismes

Définition. Un *isomorphisme* de groupes est un homomorphisme de groupes qui est bijectif.

L'application réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

S'il existe un isomorphisme entre les groupes G et G' , on dit que les groupes G et G' sont *isomorphes* et on écrit $G \simeq G'$.

Exemple. $\Sigma_E \simeq \Sigma_n \Leftrightarrow |E| = n$.

Proposition 1.5.4 [Isomorphisme associé à un homomorphisme]

Soit $f : G \rightarrow G'$ un homomorphisme de groupes. Alors le groupe quotient $G/\text{Ker}(f)$ est isomorphe au sous-groupe image $f(G)$, [$G/\text{Ker}(f) \simeq f(G)$]. Plus précisément, (si j désigne l'injection de $f(G)$ dans G') il existe un isomorphisme et un seul $\bar{f} : G/\text{Ker}(f) \rightarrow f(G)$ tel que

$$f : G \xrightarrow{p} G/\text{Ker}(f) \xrightarrow{\bar{f}} f(G) \xrightarrow{j} G'.$$

Corollaire 1.5.5 *Si $f : G \rightarrow G'$ est un homomorphisme surjectif de groupes, alors tout sous-groupe H' de G' est l'image par f d'un sous-groupe H de G et l'on a l'isomorphisme $H' \simeq H/\text{Ker}(f)$.*

Groupes cycliques

Définition. On appelle *ordre d'un élément x* d'un groupe G l'ordre du sous-groupe qu'il engendre.

Le sous-groupe engendré par x , (c.-à-d. par la partie $\{x\}$) est l'ensemble $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Proposition 1.5.6 *Soit x un élément d'un groupe G .*

1. *Si l'ordre de x est infini, alors $\langle x \rangle \simeq \mathbb{Z}$.*
2. *Si l'ordre de x est fini égal à k , alors $\langle x \rangle \simeq \mathbb{Z}/k\mathbb{Z}$ et*

$$x^n = x^{n'} \Leftrightarrow n \equiv n' \pmod{k}.$$

Un groupe engendré par un élément est dit *monogène* ou *cyclique*. (On réserve parfois l'appellation cyclique pour les groupes monogènes finis.)

Corollaire 1.5.7 *Soit G un groupe d'ordre fini n .*

1. *Pour tout $x \in G$, $x^n = e$ (l'ordre d'un élément divise l'ordre du groupe).*
2. *Si n est un nombre premier p , alors $G \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proposition 1.5.8 *Un groupe cyclique est commutatif et tout sous-groupe d'un groupe cyclique est cyclique.*

De plus, un sous-groupe d'un groupe cyclique d'ordre infini, qui n'est pas réduit à l'élément neutre, est nécessairement d'ordre infini.

Endomorphismes et automorphismes

Définitions.

1. Un homomorphisme d'un groupe G dans lui-même est appelée un *endomorphisme* de G .
2. Un isomorphisme d'un groupe G sur lui-même est appelé un *automorphisme* de G .

L'ensemble des endomorphismes d'un groupe ablien G est muni de façon naturelle d'un loi de groupe (cf. § 1.3), on le note $\text{End}(G)$.

Exemple. $\mathbb{Z} \simeq \text{End}(\mathbb{Z})$: $k \in \mathbb{Z} \mapsto (\alpha_k : n \mapsto kn) \in \text{End}(\mathbb{Z})$ (la loi dans $\text{End}(\mathbb{Z})$ est notée $+$).

L'ensemble des automorphismes de G est un sous-groupe du groupe Σ_G des permutations de G , on l'appelle *groupe des automorphismes* de G et on le note $\text{Aut}(G)$.

Exemple. $\text{Aut}(\mathbb{Z}) \simeq \{\pm 1\}$ (la loi dans $\text{Aut}(\mathbb{Z})$ est notée $\circ$).

Définition. Pour tout $x \in G$, l'application $\alpha_x : y \in G \mapsto xyx^{-1} \in G$ est un automorphisme de G , appelé *automorphisme intérieur* de G .

Proposition 1.5.9 *L'application $x \in G \mapsto \alpha_x \in \text{Aut}(G)$ est un homomorphisme de noyau le centre $Z(G)$ de G et d'image le groupe $\text{Int}(G) = \{\alpha_x \mid x \in G\}$, groupe des automorphismes intérieurs de G . Par suite, $G/Z(G) \simeq \text{Int}(G)$. De plus, $\text{Int}(G) \triangleleft \text{Aut}(G)$.*

$$G \text{ commutatif} \Leftrightarrow Z(G) = G \Leftrightarrow \text{Int}(G) = \{id_G\}.$$

1.6 Exemples

Groupes commutatifs

loi notée additivement :

$$\mathbb{Z}, k\mathbb{Z} (k \in \mathbb{N}), \mathbb{Z}/2\mathbb{Z} = \{0, 1\}, \mathbb{Z}/k\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

loi notée multiplicativement

$$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}, (\mathbb{Z}/3\mathbb{Z})^* = \{\pm 1\}$$

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\}, U = \{z \in \mathbb{C} \mid |z| = 1\}$$

quelques homomorphismes et les isomorphismes associés :

$$\boxed{\{0, 1\} \rightarrow \{+1, -1\} \parallel \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/3\mathbb{Z})^*}$$

$x \in \mathbb{R}^*$	$\mapsto$	$ x \in \mathbb{R}^*$	$\mathbb{R}^*/\{\pm 1\} \simeq \mathbb{R}_+^*$
$z \in \mathbb{C}^*$	$\mapsto$	$ z \in \mathbb{R}^*$	$\mathbb{C}^*/U \simeq \mathbb{R}_+^*$
$x \in \mathbb{R}^*$	$\mapsto$	$\ln x \in \mathbb{R}$	$\mathbb{R}^*/\{\pm 1\} \simeq \mathbb{R}$
$x \in \mathbb{R}$	$\mapsto$	$e^x \in \mathbb{R}^*$	$\mathbb{R} \simeq \mathbb{R}_+^*$
$x \in \mathbb{R}$	$\mapsto$	$e^{2i\pi x} \in \mathbb{C}^*$	$\mathbb{R}/\mathbb{Z} \simeq U$
$z \in \mathbb{C}$	$\mapsto$	$e^z \in \mathbb{C}^*$	$\mathbb{C}/2i\pi\mathbb{Z} \simeq \mathbb{C}^*$

Groupes non commutatifs (a priori)

$GL_n(K)$ *groupe linéaire général* (groupe des matrices carrés inversibles d'ordre n à coefficients dans le corps K)

$SL_n(K)$ *groupe linéaire spécial* (sous-groupe de $GL_n(K)$ formé des matrices de déterminant 1)

L'application $\det : M \in GL_n(K) \mapsto \det(M) \in K^*$ est un homomorphisme

$\text{Ker}(\det) = SL_n(K)$, $SL_n(K) \triangleleft GL_n(K)$, $GL_n(K)/SL_n(K) \simeq K^*$

$O_n(\mathbb{R})$ *groupe orthogonal* (groupe des matrices carrées orthogonales, c.-à-d. des matrices M telles que ${}^t M \cdot M = I_n$)

$SO_n(\mathbb{R})$ *groupe orthogonal spécial* ou *groupe des rotations* (sous-groupe de $O_n(\mathbb{R})$ formé des matrices de déterminant $+1$ ou sous-groupe de $SL_n(\mathbb{R})$ formé des matrices orthogonales)

$O_n(\mathbb{R})/SO_n(\mathbb{R}) \simeq \{\pm 1\}$

$U_n(\mathbb{C})$ *groupe unitaire* (groupe des matrices carrées unitaires, c.-à-d. des matrices M telles que ${}^t \bar{M} \cdot M = I_n$)

Le groupe symétrique de degré n

La *signature* d'une permutation $\sigma \in \Sigma_n$ est le nombre

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Il vaut ± 1 et mesure la parité du nombre d'*inversions* de σ , c.-à-d. de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$. La permutation σ est dite *paire* ou *impaire* selon que $\varepsilon(\sigma) = +1$ ou -1 .

L'application $\varepsilon : \sigma \in \Sigma_n \mapsto \varepsilon(\sigma) \in \{\pm 1\}$ est un homomorphisme de groupes. Son noyau $\mathcal{A}_n$, ensemble des permutations paires, est appelé *groupe alterné* de degré n . On a donc :

$$\mathcal{A}_n \triangleleft \Sigma_n, \Sigma_n/\mathcal{A}_n \simeq \{\pm 1\} \text{ et } |\mathcal{A}_n| = n!/2.$$

La signature d'une transposition étant -1 , la signature d'une permutation σ mesure aussi la parité du nombre de transpositions dans une décomposition de σ en produit de transpositions.

Groupes produits

Définition. Etant donnés deux groupes G_1 et G_2 , l'ensemble produit $G = G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}$ muni de la loi de composition $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$ est un groupe appelé *groupe produit* des groupes G_1 et G_2 et est encore noté $G_1 \times G_2$.

On définit de façon analogue le produit $G_1 \times \cdots \times G_n$ de n groupes $G_1, \dots, G_n$.

Exemple. Le *groupe de Klein* $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ est un groupe abélien d'ordre 4 non cyclique, donc non isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Considérons les sous-groupes de $G_1 \times G_2$:

$$G'_1 = \{(x_1, e_2) \mid x_1 \in G_1\} \text{ et } G'_2 = \{(e_1, x_2) \mid x_2 \in G_2\}.$$

On a :

$$G_1 \simeq G'_1, G_2 \simeq G'_2, G'_1 \triangleleft G, G'_2 \triangleleft G, G/G'_1 \simeq G_2, G/G'_2 \simeq G_1, \\ G'_1 \cap G'_2 = \{(e_1, e_2)\} \text{ et } G'_1 G'_2 = G.$$

Si K_1 est un sous-groupe de G_1 et K_2 un sous-groupe de G_2 , alors $K_1 \times K_2$ s'identifie à un sous-groupe de $G_1 \times G_2$. Si $K_1 \triangleleft G_1$ et $K_2 \triangleleft G_2$, alors :

$$K_1 \times K_2 \triangleleft G_1 \times G_2 \text{ et } (G_1 \times G_2)/(K_1 \times K_2) \simeq (G_1/K_1) \times (G_2/K_2).$$

Proposition 1.6.1 *Si $H \triangleleft G$, $K \triangleleft G$, $H \cap K = \{e\}$ et $HK = G$ où $HK = \{hk \mid h \in H, k \in K\}$, alors $G \simeq H \times K$.*

Exemple. $z \mapsto (|z|, z/|z|)$ fournit l'isomorphisme $\mathbb{C}^* \simeq \mathbb{R}_+^* \times U$.

Le groupe diédral

Définition. Le *groupe diédral de degré n* est le groupe D_n des isométries du plan qui conservent un polygone régulier à n côtés.

Si a désigne la rotation d'angle $2\pi/n$ et b l'une des symétries axiales, alors a est d'ordre n et b est d'ordre 2. De plus, ab , qui est une symétrie axiale, est d'ordre 2 et $\{a, b\}$ engendrent D_n . Inversement :

Proposition 1.6.2 *Tout groupe engendré par deux éléments a et b tels que a soit d'ordre n et b et ab soient d'ordre 2 est isomorphe au groupe diédral D_n .*

Le groupe D_n a $2n$ éléments : $e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$. D_2 est le groupe de Klein et, pour $n \geq 3$, D_n n'est pas commutatif.

1.7 Groupe opérant sur un ensemble

Orbites

Définition. Soient E un ensemble et G un groupe (d'élément neutre e). On dit que G *opère (à gauche) sur E* si on a une application

$$(g, x) \in G \times E \mapsto g.x \in E$$

telle que :

- a) $\forall g, h \in G, \forall x \in E, \quad g.(h.x) = (gh).x,$
- b) $\forall x \in E, \quad e.x = x.$

De façon équivalente, G opère sur E si on a un homomorphisme de groupes $\varphi : G \rightarrow \Sigma_E$. L'opération sur G est alors donnée par la formule $g.x = \varphi(g)(x)$.

Définition. Soient E un ensemble et G un groupe opérant sur E . Pour tout élément x de E , on appelle *orbite* de x sous G l'ensemble $\Omega_x = \{g.x \mid g \in G\}$. [La notation Ω_x n'est pas universelle.]

La relation $x\mathcal{R}y$ dans E définie par “il existe $g \in G$ tel que $g.x = y$ ” étant une relation d’équivalence, les orbites sous G en sont les classes d’équivalence et celles-ci forment donc une partition de E .

Exemples. (a) Σ_E opère sur E et E n’a qu’une orbite.

(b) Le groupe des isométries du plan (et tout sous-groupe) opère sur l’ensemble des points du plan. Si G est le sous-groupe des rotations de centre O fixé, les orbites sous G sont les cercles de centre O .

(c) Le groupe $GL_n(\mathbb{R})$ des matrices carrées d’ordre n , inversibles, à coefficients dans $\mathbb{R}$ opère sur l’espace vectoriel $\mathbb{R}^n$.

Décomposition d’une permutation en un produit de cycles disjoints

Définition. On dit que $\sigma \in \Sigma_n$ est une *permutation circulaire* ou un *cycle* de *longueur* k si les éléments de $\{1, \dots, n\}$ peuvent être ordonnés sous la forme $\{x_1, \dots, x_k\} \cup \{y_1, \dots, y_{n-k}\}$ de sorte que $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_{k-1}) = x_k, \sigma(x_k) = x_1$ et $\sigma(y_i) = y_i$ pour $1 \leq i \leq n - k$. On la note alors $(x_1, x_2, \dots, x_k)$.

Deux permutations σ et τ sont *disjointes* si, pour tout $i \in \{1, 2, \dots, n\}$, $\sigma(i) \neq i$ implique $\tau(i) = i$. Elles sont alors permutables (c.-à-d. $\sigma\tau = \tau\sigma$).

Proposition 1.7.1 *Toute permutation est décomposable en un produit de cycles disjoints et cette décomposition est unique à l’ordre près des facteurs.*

En effet, soit $\sigma \in \Sigma_n$. Puisque Σ_n opère sur $\{1, 2, \dots, n\}$, le groupe $\langle \sigma \rangle$ opère aussi sur $\{1, 2, \dots, n\}$. Soient $\Omega_1, \dots, \Omega_s$ les orbites de $\{1, 2, \dots, n\}$ sous $\langle \sigma \rangle$. Définissons $\sigma_1, \dots, \sigma_s$ par $\sigma_i(x) = \sigma(x)$ si $x \in \Omega_i$ et $\sigma_i(x) = x$ si $x \notin \Omega_i$. Les permutations σ_i sont des cycles de longueur $|\Omega_i|$ (noter que, si $|\Omega_j| = 1$, alors $\sigma_j = id$) et on a la décomposition $\sigma = \sigma_1 \cdots \sigma_s$. On notera que les cycles σ_i sont disjoints. L’unicité se vérifie aisément.

Corollaire 1.7.2 *Toute permutation est décomposable en un nombre fini de transpositions (mais de façon non unique).*

Formule des classes

Définition. Soit G un groupe opérant sur un ensemble E et soit x un élément de E . L’ensemble $H_x = \{g \in G \mid g.x = x\}$ est un sous-groupe de G appelé *stabilisateur* de x . [La notation H_x n’est pas universelle.]

Les stabilisateurs H_x et H_y de deux éléments x et y appartenant à la même orbite sont conjugués.

Le stabilisateur de n dans Σ_n est isomorphe à Σ_{n-1} .

L'élément x étant fixé, considérons l'application $g \in G \mapsto g.x \in \Omega_x$. On a $g.x = h.x \Leftrightarrow h^{-1}g \in H_x$; autrement dit, les classes relatives à la relation d'équivalence dans G associée à cette application ne sont autres que les classes à gauche dans G modulo H_x . Ainsi, selon la proposition 1.1.2, il y a une bijection entre l'ensemble quotient correspondant et Ω_x . En particulier :

Proposition 1.7.3 *Soit G un groupe opérant sur un ensemble E .*

1. *Si G est fini, alors $|G| = |H_x| |\Omega_x|$ pour tout $x \in E$.*
2. *Si E est fini et si E_0 désigne une partie de E contenant un représentant et un seul de chaque orbite, alors on a la formule des classes :*

$$|E| = \sum_{x \in E_0} |\Omega_x| = \sum_{x \in E_0} [G : H_x].$$

Définition. Soit G un groupe opérant sur un ensemble E .

1. G opère *transitivement* sur E si : $\forall x, y \in E \exists g \in G$ tel que $g.x = y$, autrement dit, s'il n'y a qu'une orbite sous G .
2. G opère *fidèlement* sur E si : $\forall g \in G \{[\forall x \in E (g.x = x)] \Rightarrow [g = e]\}$, autrement dit, si $\varphi : G \rightarrow \Sigma_E$ est injectif.

Par exemple, G opère transitivement sur chaque orbite.

Le groupe Σ_E opère transitivement et fidèlement sur E .

Translations à gauche

Un groupe G opère sur lui-même par *translation à gauche* :

$$\forall g, x \in G, g.x = gx.$$

Il opère transitivement : $\forall x, y \in G \exists g \in G$ tel que $gx = y$ (en fait, g est unique) et fidèlement (en fait, pour tout $x \in G$, $H_x = \{e\}$).

L'homomorphisme correspondant $\varphi : g \in G \mapsto \varphi(g) \in \Sigma_G$ est injectif. [Noter que, pour g fixé, $x \mapsto gx$ est une permutation, mais non un automorphisme de G .]

Proposition 1.7.4 [Théorème de Cayley]

Si $|G| = n$, alors G peut être identifié à un sous-groupe de Σ_n .

Exemple. Soient G un groupe, H un sous-groupe de G et E l'ensemble des classes à gauche de G modulo H . Alors, G opère transitivement sur E par translation à gauche : $g.xH = gxH$. Le stabilisateur de xH est

le sous-groupe xHx^{-1} . L'homomorphisme $g \in G \mapsto \varphi(g) \in \Sigma_E$ n'est pas injectif en général [$\text{Ker}(\varphi) = \cap_{x \in G} xHx^{-1}$].

Conjugaison

Un groupe G opère sur lui-même par automorphismes intérieurs :

$$\forall g, x \in G, g.x = gxg^{-1}.$$

Deux éléments dans la même orbite sont dits *conjugués*, les orbites sont appelées les *classes de conjugaison*.

Le stabilisateur H_x de x est appelé *centralisateur* de x , on a :

$$H_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Exemples. 1. Les conjugués d'un cycle $\sigma = (x_1, \dots, x_k)$ de longueur k sont les cycles de longueur k : pour tout $\tau \in \Sigma_n$, $\tau\sigma\tau^{-1} = (\tau(x_1), \dots, \tau(x_k))$.

2. Les conjugués d'une matrice dans $GL_n(K)$ sont les matrices qui lui sont semblables.

Proposition 1.7.5 [Conséquence de la formule des classes]

Si $|G| = p^k$ où p est un nombre premier et $k \geq 1$, alors $Z(G) \neq \{e\}$.

Chapter 2

Anneaux

2.1 Anneaux

Anneaux

Définition. On appelle *anneau* un ensemble A muni de deux lois de composition, l'une notée additivement et appelée *addition*, l'autre notée multiplicativement et appelée *multiplication*, telles que :

- a) l'addition soit une loi de groupe commutatif,
- b) la multiplication soit associative et possède un élément neutre,
- c) la multiplication soit *distributive* par rapport à l'addition.

L'élément neutre pour l'addition est appelé *zéro* et noté généralement 0 , tandis que l'élément neutre pour la multiplication est appelé *élément unité* et est noté généralement e ou 1 .

[On supposera en général $1 \neq 0$, autrement dit on écartera le cas peu intéressant de l'anneau réduit à l'élément 0 .]

Dire que l'ensemble A est un anneau revient à dire qu'il est muni de deux opérations qui, notées $+$ et $\cdot$, vérifient :

- a) $\forall x, y, z \in A \quad x + (y + z) = (x + y) + z,$
 $\exists 0 \in A$ tel que : $x + 0 = 0 + x = x \quad \forall x \in A,$
 $\forall x \in A \exists (-x) \in A$ tel que $(-x) + x = x + (-x) = 0,$
 $\forall x, y \in A \quad x + y = y + x.$
- b) $\forall x, y, z \in A, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z,$
 $\exists e \in A$ tel que : $x \cdot e = e \cdot x = x \quad \forall x \in A,$
- c) $\forall x, y, z \in A, \quad x \cdot (y + z) = x \cdot y + x \cdot z$ et $(y + z) \cdot x = y \cdot x + z \cdot x.$

Exemples.

- a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/k\mathbb{Z}$ où $k \geq 2$.
 b) Si G est un groupe abélien, l'ensemble $\text{End}(G)$ des endomorphismes de G muni de l'addition définie "point par point" et de la multiplication-composition est un anneau.
 c) Si E est un ensemble et A est un anneau, l'ensemble A^E muni de l'addition et de la multiplication définies "point par point" est un anneau.
 d) Si K est un corps (ou un anneau), l'ensemble $\mathcal{M}_n(K)$ des matrices carrées d'ordre n à coefficients dans K est un anneau dont l'élément zéro est la matrice 0 et l'élément unité est la matrice identité I_n .
 e) $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ anneau des *entiers de Gauss*.
 f) L'ensemble des *quaternions* $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ est muni d'une addition, en considérant $\mathbb{H}$ comme un espace vectoriel sur $\mathbb{R}$ admettant pour base $(1, i, j, k)$, et d'une multiplication, admettant 1 pour élément neutre, définie par bilinéarité (distributivité par rapport à l'addition) avec les formules $i^2 = j^2 = k^2 = -1$, $jk = -kj = i$, $ki = -ik = j$ et $ij = -ji = k$. Muni de ces deux lois, $\mathbb{H}$ est un anneau non commutatif dans lequel tout élément non nul est inversible : on dit que $\mathbb{H}$ est un *corps non commutatif*.

Quelques règles de calcul

$$\begin{aligned}
 x.(y - z) &= x.y - x.z, & (y - z).x &= y.x - z.x, & x.0 &= 0.x = 0 \\
 x.(-y) &= -(x.y) = (-x).y, & (-x).(-z) &= x.z \\
 (-x)^n &= x^n \text{ si } n \text{ pair et } = -x^n \text{ si } n \text{ est impair} \\
 (a + b)^2 &= a^2 + a.b + b.a + b^2
 \end{aligned}$$

$$\left(\sum_{i=1}^p a_i\right) \cdot \left(\sum_{j=1}^q b_j\right) = \sum_{i=1}^p \left(\sum_{j=1}^q a_i \cdot b_j\right) = \sum_{j=1}^q \left(\sum_{i=1}^p a_i \cdot b_j\right) = \sum_{1 \leq i \leq p, 1 \leq j \leq q} a_i \cdot b_j.$$

Lorsque la multiplication est commutative, on dit qu'il s'agit d'un *anneau commutatif*. On a alors la formule du binôme :

$$(a + b)^n = \sum_{i=0}^n C_n^i a^i \cdot b^{n-i}.$$

Le groupe des unités

Les éléments *inversibles* dans un anneau A (c.-à-d. inversibles pour la multiplication) sont aussi appelés *unités* de A . Leur ensemble $U(A)$ est un groupe (pour la multiplication), on l'appelle le *groupe des unités* de A , et souvent on le note encore $A^\times$.

Exemples.

$U(\mathbb{Z}) = \{\pm 1\}$, $U(\mathbb{C}) = \mathbb{C}^*$, $U(\mathbb{Z}/4\mathbb{Z}) = \{\bar{1}, \bar{3}\}$, $U(\mathcal{M}_n(K)) = GL_n(K)$,
 $U(\text{End}(G)) = \text{Aut}(G)$, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

Un élément a d'un anneau A est dit *régulier* s'il est simplifiable pour la multiplication, c.-à-d. : $\forall x, y \in A \ [ax = ay \Rightarrow x = y]$. Tout élément inversible est régulier, l'inverse n'est pas toujours vrai.

Proposition 2.1.1 Soit $k \geq 2$. Dans $\mathbb{Z}/k\mathbb{Z}$, on a les équivalences :

1. $\bar{n}$ est inversible (pour la multiplication),
2. $\bar{n}$ est simplifiable (pour la multiplication),
3. $\bar{n}$ engendre $\mathbb{Z}/k\mathbb{Z}$ (en tant que groupe additif),
4. n et k sont premiers entre eux.

Corollaire 2.1.2 Soit $k \geq 2$.

1. Soit $\varphi(k)$ le nombre d'entiers n premiers à k et tels que $1 \leq n \leq k$. Alors

$$|(\mathbb{Z}/k\mathbb{Z})^\times| = \varphi(k).$$

2. Soit $\text{Aut}(\mathbb{Z}/k\mathbb{Z})$ le groupe des automorphismes du groupe additif $\mathbb{Z}/k\mathbb{Z}$. Alors

$$\text{Aut}(\mathbb{Z}/k\mathbb{Z}) \simeq (\mathbb{Z}/k\mathbb{Z})^\times.$$

Corollaire 2.1.3 Soit p un nombre premier. Pour tout entier m , on a

$$m^p \equiv m \pmod{p}.$$

Sous-anneaux

Définition. Un *sous-anneau* d'un anneau A est une partie B de A qui est un sous-groupe pour l'addition, est stable pour la multiplication et contient l'élément unité e de A .

Autrement dit, un sous-anneau de A est une partie B telle que $e \in B$ et $\forall x, y \in A \ [(x, y \in B) \Rightarrow (x - y \in B \text{ et } xy \in B)]$. Muni des lois induites, un sous-anneau est en particulier un anneau.

Les sous-ensembles $\mathbb{N}$ et $k\mathbb{Z}$ ($k \geq 2$) de $\mathbb{Z}$ sont stables pour l'addition et la multiplication, mais ne sont pas des sous-anneaux de $\mathbb{Z}$.

2.2 Idéaux et anneaux quotients

Les anneaux seront désormais supposés commutatifs

Anneaux quotients

Définition. On appelle *idéal* d'un anneau A toute partie I de A qui est un sous-groupe pour l'addition et qui est stable pour la multiplication par n'importe quel élément de l'anneau $[\forall x \in A \forall y \in I (xy \in I)]$.

Exemple. Les idéaux de $\mathbb{Z}$ sont les ensembles $k\mathbb{Z}$ où $k \in \mathbb{N}$.

Proposition 2.2.1 Une relation d'équivalence dans un anneau A est compatible avec les deux opérations de A si et seulement si elle est associée à un idéal I de A , c.-à-d. est de la forme $x - y \in I$ où I est un idéal de A .

Définition. Soient A un anneau et I un idéal de A . L'ensemble quotient pour la relation d'équivalence dans A associée à l'idéal I $[x - y \in I]$ muni des lois quotients $[\bar{x} + \bar{y} = \overline{x + y}, \bar{x} \cdot \bar{y} = \overline{x \cdot y}]$ est un anneau appelé *anneau quotient* de A par I et noté A/I .

Exemple. $A = \mathbb{Z}, I = k\mathbb{Z} (k \geq 2), \mathbb{Z}/k\mathbb{Z}$ anneau des entiers modulo k .

Idéaux engendrés

Une intersection d'idéaux d'un anneau A est un idéal de A .

Définition. Etant donnée une partie non vide M d'un anneau A , l'intersection des idéaux contenant M est le plus petit idéal de A contenant M , on l'appelle *idéal engendré* par M .

Définition. On appelle idéal *principal* tout idéal engendré par un élément.

L'idéal engendré par x est l'ensemble $xA = \{xa \mid a \in A\}$, noté aussi (x) . L'élément x est inversible si et seulement si $xA = A$.

Exemples.

- Dans un anneau $\{0\}$ et A sont toujours des idéaux. Soit I un idéal de A , $A/I \neq \{0\}$ équivaut à $I \neq A$. On appelle *idéal propre* de A un idéal distinct de A .
- L'idéal de A engendré par $\{x, y\}$ est l'ensemble $\{ax + by \mid a, b \in A\}$.
- Si $\mathcal{A}$ et $\mathcal{B}$ sont des idéaux, alors $\mathcal{A} + \mathcal{B} = \{a + b \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ est un idéal, on l'appelle *idéal somme* des idéaux $\mathcal{A}$ et $\mathcal{B}$.
- En revanche, si $\mathcal{A}$ et $\mathcal{B}$ sont des idéaux, $\mathcal{AB} = \{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ n'est pas un idéal en général. L'idéal engendré par la partie $\mathcal{AB}$ est l'ensemble des sommes finies $\sum_{p=0}^k a_p b_p$ où $a_p \in \mathcal{A}$ et $b_p \in \mathcal{B}$, on l'appelle *idéal produit* des idéaux $\mathcal{A}$ et $\mathcal{B}$ et on le note $\mathcal{A} \cdot \mathcal{B}$. On a alors $\mathcal{A} \cdot \mathcal{B} \subset \mathcal{A} \cap \mathcal{B}$.
- Les idéaux de $\mathbb{Z}$, étant de la forme $k\mathbb{Z}$, sont principaux. Dans ce cas particulier, on a $\mathcal{AB} = \mathcal{A} \cdot \mathcal{B}$.

Idéaux étrangers

Définition. Deux idéaux $\mathcal{A}$ et $\mathcal{B}$ d'un anneau A sont dits *étrangers* lorsque $\mathcal{A} + \mathcal{B} = A$.

Les idéaux $a\mathbb{Z}$ et $b\mathbb{Z}$ de $\mathbb{Z}$ sont étrangers si et seulement si a et b sont premiers entre eux.

Proposition 2.2.2 Soient $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ des idéaux d'un anneau A .

1. $\mathcal{A}$ et $\mathcal{B}$ sont étrangers si, et seulement si, il existe $a \in \mathcal{A}$ et $b \in \mathcal{B}$ tels que $a + b = 1$.
2. Si $\mathcal{A}$ et $\mathcal{B}$ sont étrangers, alors $\mathcal{A} \cdot \mathcal{B} = \mathcal{A} \cap \mathcal{B}$.
3. Si $\mathcal{A}$ est étranger à $\mathcal{B}$ et $\mathcal{C}$, alors $\mathcal{A}$ est étranger à $\mathcal{B} \cdot \mathcal{C}$.

Plus généralement, si $\mathcal{A}$ est étranger à chaque idéal $\mathcal{I}_1, \dots, \mathcal{I}_r$, alors $\mathcal{A}$ est étranger à l'idéal $\mathcal{I}_1 \cdots \mathcal{I}_r$. Si les idéaux $\mathcal{I}_1, \dots, \mathcal{I}_r$ sont étrangers deux à deux, alors $\mathcal{I}_1 \cdots \mathcal{I}_r = \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_r$.

Idéaux maximaux

Définition. Un idéal M d'un anneau A est dit *maximal* s'il est maximal parmi les idéaux propres de A .

C'est-à-dire, pour tout idéal $\mathcal{I}$ de A $[(M \subset \mathcal{I}) \Rightarrow (\mathcal{I} = M \text{ ou } \mathcal{I} = A)]$; ou encore, $\forall x \in A \setminus M$, l'idéal engendré par M et x est A .

Deux idéaux maximaux distincts sont toujours étrangers.

Les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$ où p est un nombre premier.

Proposition 2.2.3 Tout idéal propre d'un anneau A est contenu dans au moins un idéal maximal M de A .

Dire que deux idéaux sont étrangers revient à dire qu'ils ne sont pas contenus tous deux dans un même idéal maximal.

Un élément est inversible si, et seulement si, il n'est contenu dans aucun idéal maximal, autrement dit :

$$A \setminus A^\times = \bigcup_{\text{id. max. } M} M.$$

2.3 Homomorphismes d'anneaux

Homomorphismes et isomorphismes

Définition. Soient A et A' deux anneaux. On dit que $f : A \rightarrow A'$ est un *homomorphisme d'anneaux* lorsque l'on a :

1. quels que soient x et $y \in A$, $f(x + y) = f(x) + f(y)$,
2. quels que soient x et $y \in A$, $f(xy) = f(x)f(y)$.
3. $f(1_A) = 1_{A'}$

Proposition 2.3.1 *Soit $f : A \rightarrow A'$ un homomorphisme d'anneaux. Alors :*

1. $\forall x \in A, \forall n \in \mathbb{Z}, f(nx) = nf(x)$ (en particulier, $f(0) = 0$),
2. $f(A)$ est un sous-anneau de A' ,
3. pour tout idéal $\mathcal{J}$ de A' , $f^{-1}(\mathcal{J})$ est un idéal de A .

En particulier, $f^{-1}(0)$ est un idéal de A appelé *noyau* de f . Pour que f soit injectif, il faut et il suffit que son noyau soit réduit à $\{0\}$.

Proposition 2.3.2 *Soient A un anneau et $\mathcal{I}$ un idéal propre de A . La surjection $p : A \rightarrow A/\mathcal{I}$ est un homomorphisme d'anneaux. L'application $\mathcal{I} \mapsto p(\mathcal{I})$ est une bijection de l'ensemble des idéaux (resp. idéaux maximaux) de A contenant $\mathcal{I}$ sur l'ensemble des idéaux (resp. idéaux maximaux) de $A/\mathcal{I}$.*

Le composé de deux homomorphismes d'anneaux est un homomorphisme d'anneaux. Un homomorphisme d'anneaux qui est bijectif est appelé un *isomorphisme*. L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux. S'il existe un isomorphisme entre les anneaux A et A' , on dit qu'il s'agit d'*anneaux isomorphes* et on écrit $A \simeq A'$.

Proposition 2.3.3 [Isomorphisme associé à un homomorphisme]

Soit $f : A \rightarrow A'$ un homomorphisme d'anneaux. Il existe un homomorphisme injectif et un seul

$$\bar{f} : A/\text{Ker}(f) \rightarrow A'$$

tel que $f = \bar{f} \circ p$ [$\bar{f}$ est défini par $\bar{f}(\bar{a}) = f(a)$]. En particulier,

$$A/\text{Ker}(f) \simeq f(A).$$

Un homomorphisme d'un anneau A dans lui-même est appelé un *endomorphisme* de A . Une isomorphisme d'un anneau A sur lui-même est appelé un *automorphisme* de A . Le seul endomorphisme de l'anneau $\mathbb{Z}$ est l'identité.

Produit d'anneaux

Définition. Soient A et B deux anneaux. L'*anneau produit* des anneaux A et B est l'ensemble produit $A \times B$ muni de l'addition et de la multiplication définies par $(a, b) + (a', b') = (a + a', b + b')$ et $(a, b)(a', b') = (aa', bb')$.

On a $(A \times B)^\times = A^\times \times B^\times$.

On définit de façon analogue le produit $A_1 \times \cdots \times A_n$ de n anneaux $A_1, \dots, A_n$.

Soient $\mathcal{A}$ et $\mathcal{B}$ deux idéaux de A . L'homomorphisme

$$f : a \in A \mapsto (a_1, a_2) \in A/\mathcal{A} \times A/\mathcal{B},$$

où a_1 et a_2 désignent respectivement les classes de a dans $A/\mathcal{A}$ et $A/\mathcal{B}$, a pour noyau $\mathcal{A} \cap \mathcal{B}$; d'où un homomorphisme injectif

$$\bar{f} : A/(\mathcal{A} \cap \mathcal{B}) \rightarrow A/\mathcal{A} \times A/\mathcal{B}.$$

Cet homomorphisme est surjectif si et seulement si $\mathcal{A}$ et $\mathcal{B}$ sont étrangers. Plus généralement :

Proposition 2.3.4 [Théorème chinois]

Si $\mathcal{I}_1, \dots, \mathcal{I}_n$ sont des idéaux d'un anneau A étrangers deux à deux, alors

$$A/(\cap_{k=1}^n \mathcal{I}_k) \simeq A/\mathcal{I}_1 \times \cdots \times A/\mathcal{I}_n.$$

Corollaire 2.3.5 Si $k_1, \dots, k_n$ sont des entiers premiers entre eux deux à deux, alors :

1. $\mathbb{Z}/k_1 \cdots k_n \mathbb{Z} \simeq \mathbb{Z}/k_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/k_n \mathbb{Z}$,
2. quels que soient $a_1, \dots, a_n \in \mathbb{Z}$, il existe $x \in \mathbb{Z}$ (unique modulo $k_1 \cdots k_n$) tel que, pour $i = 1, \dots, n$, $x \equiv a_i \pmod{k_i}$,
3. $(\mathbb{Z}/k_1 \cdots k_n \mathbb{Z})^\times \simeq (\mathbb{Z}/k_1 \mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/k_n \mathbb{Z})^\times$,
4. $\varphi(k_1 \cdots k_n) = \varphi(k_1) \cdots \varphi(k_n)$.

L'indicateur d'Euler φ vérifie :

- si p est premier, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$,
- si a et b sont premiers entre eux, $\varphi(ab) = \varphi(a)\varphi(b)$.

Par suite :

- si $k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (les p_i désignant des nombres premiers distincts),

$$\varphi(k) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_r - 1)p_r^{\alpha_r - 1} = k(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

Algèbres

Définition. Soit A un anneau. Une A -algèbre est un anneau B muni d'un homomorphisme d'anneaux $\varphi : A \rightarrow B$ [non nécessairement injectif].

Tout anneau A est une $\mathbb{Z}$ -algèbre où $\varphi : n \in \mathbb{Z} \mapsto n.e \in A$.

L'anneau A_0 engendré par e est le plus petit sous-anneau contenu dans A , on l'appelle le *sous-anneau premier* de A .

Si φ est injectif, $A_0 \simeq \mathbb{Z}$. Sinon $\text{Ker}(\varphi) = k\mathbb{Z}$ où $k \geq 2$, $A_0 \simeq \mathbb{Z}/k\mathbb{Z}$ et, pour tout $x \in A$, $kx = (ke)x = 0$.

Définition. Si $ne = 0$ équivaut $n = 0$, on dit que A est de *caractéristique* 0. Si $ne = 0$ équivaut $k|n$, on dit que A est de *caractéristique* k .

Définition. Soit A un anneau. Une *série formelle* en l'indéterminée X à coefficients dans A est une expression de la forme $\sum_{n=0}^{\infty} a_n X^n$ où les *coefficients* a_n appartiennent à A . Leur ensemble, noté $A[[X]]$, est muni d'une addition définie par

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) + \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

et d'une multiplication définie par

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} c_n X^n$$

où

$$c_n = \sum_{p+q=n} a_p b_q = \sum_{p=0}^n a_p b_{n-p}.$$

Muni de ces deux lois, l'ensemble $A[[X]]$ est un anneau.

[On pourrait aussi identifier une série formelle à la suite $(a_n)_{n \in \mathbb{N}}$ de ses coefficients, c.-à-d. à une application de $\mathbb{N}$ dans A , et munir l'ensemble $A^{\mathbb{N}}$ d'une addition et d'une multiplication.]

Dans la pratique, on omet les termes $a_n X^n$ pour lesquels $a_n = 0$. Posant $X^0 = 1$, on identifie l'anneau A à un sous-anneau de $A[[X]]$ (un élément $a \in A$ est identifié à la série $\sum_{n=0}^{\infty} a_n X^n$ où $a_0 = a$ et $a_n = 0$ pour $n > 0$). En particulier, $A[[X]]$ est une A -algèbre. De plus, posant $X^1 = X$ (c.-à-d. X représente la série $\sum_{n=0}^{\infty} a_n X^n$ où $a_1 = 1$ et $a_n = 0$ pour $n \neq 1$), on vérifie que X^n correspond bien dans $A[[X]]$ au produit de n termes X .

Définition. Un *polynôme* en l'indéterminée X à coefficients dans A est une série formelle qui n'a au plus qu'un nombre fini de coefficients non nuls. Leur ensemble est noté $A[X]$.

$A[X]$ est le plus petit sous-anneau de $A[[X]]$ contenant A et X .

Définitions.

1. Le *degré* d'un polynôme non nul $P = \sum a_n X^n$ est le plus grand entier n tel que $a_n \neq 0$, on le note $\deg(P)$.
2. L'*ordre* d'une série formelle non nulle $\alpha = \sum a_n X^n$ est le plus petit entier n tel que $a_n \neq 0$, on le note $\text{ord}(\alpha)$.

Proposition 2.3.6 *Si $\mathcal{I}$ est un idéal de A , alors l'ensemble $\mathcal{I}[X]$ (resp. $\mathcal{I}[[X]]$) des polynômes (resp. séries formelles) dont tous les coefficients sont dans $\mathcal{I}$ est un idéal de $A[X]$ (resp. $A[[X]]$) et on a les isomorphismes :*

$$A[X]/[\mathcal{I}] \simeq (A/\mathcal{I})[X] \quad A[[X]]/\mathcal{I}[[X]] \simeq (A/\mathcal{I})[[X]].$$

2.4 Anneaux intègres

Anneaux intègres

Définition. Un élément non nul a d'un anneau A est un *diviseur de zéro* dans A s'il existe un élément non nul b de A tel que $ab = 0$.

Un élément non nul est régulier ou simplifiable pour la multiplication dans A si, et seulement si, il n'est pas un diviseur de 0 dans A .

Définition. Un *anneau intègre* est un anneau sans diviseurs de zéro.

Dans un anneau intègre : $xy = 0 \Leftrightarrow x = 0$ ou $y = 0$.

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

Proposition 2.4.1 *La caractéristique d'un anneau intègre est soit 0, soit un nombre premier p .*

Si un anneau A est de caractéristique p , alors, quels que soient x et $y \in A$:

$$(x + y)^p = x^p + y^p.$$

Proposition 2.4.2 *Si A est un anneau intègre, alors les anneaux $A[X]$ et $A[[X]]$ sont intègres. De plus, si P et $Q \in A[X]^*$, alors $\deg(PQ) = \deg(P) + \deg(Q)$, et, si α et $\beta \in A[[X]]^*$, alors $\text{ord}(\alpha\beta) = \text{ord}(\alpha) + \text{ord}(\beta)$.*

Idéaux premiers

L'anneau $\mathbb{Z}$ est intègre, mais $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre ($\bar{2}$ est un diviseur de zéro). Donc un quotient d'un anneau intègre n'est pas toujours intègre.

Définition. Un *idéal premier* d'un anneau A est un idéal propre de A tel que, quels que soient x et $y \in A$, $[xy \in \mathcal{P} \Rightarrow x \in \mathcal{P} \text{ ou } y \in \mathcal{P}]$.

Les idéaux premiers de $\mathbb{Z}$ sont (0) et $p\mathbb{Z}$ où p est un nombre premier.

Proposition 2.4.3 *Tout idéal maximal est premier.*

Proposition 2.4.4 *Soient A un anneau et $\mathcal{I}$ un idéal de A . L'anneau quotient $A/\mathcal{I}$ est intègre si et seulement si l'idéal $\mathcal{I}$ est premier.*

En particulier, l'anneau A est intègre si et seulement si l'idéal (0) est premier.

Proposition 2.4.5 *Soit $f : A \rightarrow B$ un homomorphisme d'anneaux. Pour tout idéal premier $\mathcal{Q}$ de B , l'idéal $f^{-1}(\mathcal{Q})$ est un idéal premier de A .*

Si $\mathcal{P}$ est un idéal premier de l'anneau A , alors $\mathcal{P}[X]$ (resp. $\mathcal{P}[[X]]$) est un idéal premier de l'anneau $A[X]$ (resp. $A[[X]]$).

Divisibilité dans un anneau intègre

Etant donnés deux éléments a et b d'un anneau A , on dit que b *divise* a dans A , et on écrit $b|a$, s'il existe $c \in A$ tel que $a = bc$. On a les équivalences :

$$b|a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subset (b).$$

Définitions. Soit A un anneau intègre.

1. Deux éléments a et b sont dits *associés* si $(a) = (b)$, c.-à-d. si $b = au$ où $u \in A^\times$.
2. Deux éléments a et b sont dits *premiers entre eux* s'ils n'ont pas de diviseurs communs autres que les éléments inversibles.
3. Un élément non nul et non inversible π est dit *irréductible* s'il n'est divisible que par des éléments associés ou inversibles.

Exemples.

- a) $\mathbb{Z}^\times = \{\pm 1\}$, donc a et b sont associés dans $\mathbb{Z}$ si et seulement si $a = \pm b$.
- b) $A[X]^\times = A^\times$, donc P et Q sont associés dans $A[X]$, si et seulement si $P = \lambda Q$ où $\lambda \in A^\times$.
- c) $\mathbb{Z}[[X]]^\times = \{\sum_n a_n X^n \mid a_0 = \pm 1\}$
- d) Les éléments irréductibles de $\mathbb{Z}$ sont de la forme $\pm p$ où p est un nombre premier.
- e) Si l'idéal πA est premier et non nul, alors l'élément π est irréductible. La réciproque est vraie dans $\mathbb{Z}$, mais fausse en général.
- f) Si les idéaux (a) et (b) sont étrangers, alors les éléments a et b sont premiers entre eux. La réciproque est vraie dans $\mathbb{Z}$, mais fausse en général.
- g) Dans $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$, $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ et 3 sont irréductibles et, pourtant, $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

Définitions. Soient a et b deux éléments d'un anneau intègre A .

1. Un élément d de A est un *plus grand commun diviseur* (ou p.g.c.d.) de a et b lorsque :

$$d|a, d|b \text{ et} \\ \text{pour tout } c \in A, c|a \text{ et } c|b \text{ implique } c|d.$$

2. Un élément m de A est un *plus petit commun multiple* (ou p.p.c.m.) de a et b lorsque :

$$a|m, b|m \text{ et} \\ \text{pour tout } n \in A, a|n \text{ et } b|n \text{ implique } m|n.$$

Il n'existe pas toujours un p.g.c.d. ou un p.p.c.m. Mais si d est un p.g.c.d. de a et b , alors d_1 est un p.g.c.d. de a et b si et seulement si d_1 est associé à d . De même, si m est un p.p.c.m. de a et b , alors m_1 est un p.p.c.m. de a et b si et seulement si m_1 est associé à m .

Dire que a et b sont premiers entre eux revient à dire qu'ils admettent 1 pour p.g.c.d. Si d est un p.g.c.d. de a et b , alors a/d et b/d sont premiers entre eux. Si m est un p.p.c.m. de a et b , alors m/a et m/b sont premiers entre eux.

2.5 Corps

Corps et idéaux maximaux

Définition. On appelle *corps* un ensemble K muni d'une addition et d'une multiplication telles que :

1. K soit un anneau commutatif,
2. $K^\times = K^*$ (où $K^* = K \setminus \{0\}$).

Ou encore telles que :

- (1) K muni de l'addition soit un groupe commutatif,
- (2) K^* muni de la multiplication soit un groupe commutatif,
- (3) la multiplication soit distributive par rapport à l'addition.

Attention : ici, un corps est supposé a priori commutatif. Par suite :

- dans ce contexte, l'énoncé “tout corps fini est commutatif” n'est pas un théorème, mais une tautologie,
- lorsque l'on parle du *corps* $\mathbb{H}$ des *quaternions*, il s'agit d'une variante de la notion de corps où la multiplication n'est pas nécessairement commutative.

Notation. Soit K un corps. Si $a, b \in K$ avec $b \neq 0$, au lieu de ab^{-1} ou $b^{-1}a$ on écrit $\frac{a}{b}$. Soient $a, b, c, d \in K$ avec $bd \neq 0$, on vérifie :

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc, \quad \frac{a}{b} = \frac{ad}{bd}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Proposition 2.5.1 Soient A un anneau et $\mathcal{I}$ un idéal de A . L'anneau quotient $A/\mathcal{I}$ est un corps si et seulement si l'idéal $\mathcal{I}$ est maximal.

Corollaire 2.5.2 Soit $k \geq 2$. Les assertions suivantes sont équivalentes :

1. k est un nombre premier,
2. $\mathbb{Z}/k\mathbb{Z}$ est un anneau intègre,
3. $\mathbb{Z}/k\mathbb{Z}$ est un corps.

Si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$, souvent noté $\mathbb{F}_p$, est de caractéristique p . Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0.

Exemple. $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$

Homomorphismes de corps

Définition. Une partie F d'un corps K est un *sous-corps* de K si elle est stable pour les deux lois de K et si, munie des deux lois induites, F est un corps. On dit aussi que K est un *sur-corps* de F ou encore que K est une *extension* de F .

Ainsi, $\mathbb{R}$ est un sur-corps de $\mathbb{Q}$ et un sous-corps de $\mathbb{C}$.

Un corps a pour seul idéal propre l'idéal (0) ; celui-ci est donc maximal !

Proposition 2.5.3 Tout homomorphisme de corps $f : K \rightarrow K'$ (c.-à-d. tout homomorphisme d'anneaux où K et K' sont des corps) est injectif.

Par suite, $f(K)$ est un sous-corps de K' isomorphe à K et K' peut être identifié à une extension de K .

Une intersection de sous-corps d'un corps K est un sous-corps de K . Etant donnée une partie M de K , l'intersection des sous-corps de K contenant M est le plus petit sous-corps de K contenant M , on l'appelle le *sous-corps de K engendré par M* . Le plus petit sous-corps d'un corps K est appelé le *sous-corps premier* de K . La caractéristique d'un corps étant 0 ou un nombre premier p , le sous-corps premier d'un corps est soit $\mathbb{Q}$, soit un corps $\mathbb{F}_p$.

Proposition 2.5.4 Tout anneau intègre fini est un corps.

Corps des fractions d'un anneau intègre

Définition. Soit A un anneau intègre. On appelle corps des fractions de A tout corps K contenant A dont tout élément peut s'écrire sous la forme $\frac{a}{b}$ où $a \in A$ et $b \in A^*$.

Construction d'un corps des fractions : $K = A \times A^* / \mathcal{R}$ où $A \times A^*$ est muni des opérations $(a, b) + (c, d) = (ad + bc, bd)$ et $(a, b)(c, d) = (ac, bd)$ et $\mathcal{R}$ est la relation d'équivalence $(a, b)\mathcal{R}(c, d) := ad = bc$.

Proposition 2.5.5 *Tout anneau intègre A admet un corps des fractions K ; celui-ci est unique à isomorphisme près. Si A est un anneau intègre de corps des fractions K , si L est un corps et si $f : A \rightarrow L$ est un homomorphisme injectif d'anneaux, alors il existe un homomorphisme de corps et un seul $\bar{f} : K \rightarrow L$ prolongeant f .*

Exemples.

- $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.
- Si A désigne un anneau intègre de corps des fractions K , alors le corps des fractions de l'anneau de polynômes $A[X]$ est le corps des fractions rationnelles $K(X)$.

Anneaux de fractions d'un anneau intègre

Définition. Une *partie multiplicative* d'un anneau A est une partie S de A stable pour la multiplication, contenant 1 et ne contenant pas 0.

Exemples. Si A est intègre, les parties suivantes sont multiplicatives :

- $A \setminus \{0\}$,
- $\{s^n \mid n \in \mathbb{N}\}$ où $s \in A \setminus \{0\}$,
- $A \setminus \mathcal{P}$ où $\mathcal{P}$ désigne un idéal premier de A ,

Définition. Soit A un anneau intègre de corps des fractions K et soit S une partie multiplicative de A . L'ensemble $\{\frac{a}{s} \in K \mid a \in A, s \in S\}$ est un sous-anneau de K contenant A , noté $S^{-1}A$ et appelé *anneau des fractions de A à dénominateurs dans S* .

Exemples.

- Si $S = \{1\}$ ou $S = A^\times$, alors $S^{-1}A = A$.
- Si $S = A \setminus \{0\}$, alors $S^{-1}A$ est le corps des fractions K de A .
- Si $S = \{10^n \mid n \in \mathbb{N}\}$, alors $S^{-1}\mathbb{Z}$ est l'anneau des nombres décimaux.
- Si $S = \mathbb{Z} \setminus p\mathbb{Z}$ où p est premier, $S^{-1}\mathbb{Z} = \{\frac{a}{s} \in \mathbb{Q} \mid a \in \mathbb{Z}, s \in \mathbb{Z}, p \nmid s\}$.

Ainsi, étant donné un anneau intègre A , on obtient d'autres anneaux intègres en considérant des sous-anneaux de A , des anneaux localisés de A , des anneaux de polynômes ou de séries formelles à coefficients dans A ou encore en passant au quotient par des idéaux premiers.

Proposition 2.5.6 *Si S est une partie multiplicative de A , l'application $\mathcal{I} \mapsto S^{-1}\mathcal{I} = \{\frac{i}{s} \mid i \in \mathcal{I}, s \in S\}$ est une surjection de l'ensemble des idéaux de A sur l'ensemble des idéaux de $S^{-1}A$. De plus,*

$$S^{-1}\mathcal{I} \neq S^{-1}A \Leftrightarrow \mathcal{I} \cap S = \emptyset.$$

Corollaire 2.5.7 *L'application $\mathcal{P} \mapsto S^{-1}\mathcal{P}$ est une bijection de l'ensemble des idéaux premiers de A ne rencontrant pas S sur l'ensemble des idéaux premiers de $S^{-1}A$. La bijection inverse est donnée par : $\mathcal{Q} \mapsto \mathcal{Q} \cap A$.*

Lorsque $S = A \setminus \mathcal{P}$ où $\mathcal{P}$ est un idéal premier, l'anneau $S^{-1}A$ a un seul idéal maximal, à savoir $S^{-1}\mathcal{P}$.

Exercice. Soit A un anneau. Les assertions suivantes sont équivalentes :

1. A n'a qu'un idéal maximal.
2. L'ensemble des éléments non inversibles de A est un idéal.

Racines de l'unité

Définition. Soit K un corps et soit $n \in \mathbb{N}^*$. On appelle

1. *racine n -ième de l'unité* du corps K tout élément x de K tel que $x^n = 1$.
2. *racine primitive n -ième de l'unité* du corps K tout élément ζ de K tel que $\zeta^n = 1$ et, pour $1 \leq m < n$, $\zeta^m \neq 1$.

On notera $\mu_n(K)$ le groupe multiplicatif formé par les racines n -ièmes de l'unité de K .

Exemple. Dans $\mathbb{C}$, les racines n -ièmes de l'unité sont de la forme $e^{\frac{2ik\pi}{n}}$ où $0 \leq k < n - 1$ et les racines primitives n -ièmes correspondent aux entiers k premiers à n . Si ζ est une racine primitive n -ième de $\mathbb{C}$, on a un isomorphisme

$$k \in \mathbb{Z}/n\mathbb{Z} \mapsto \zeta^k \in \mu_n(\mathbb{C})$$

du groupe additif $\mathbb{Z}/n\mathbb{Z}$ sur le groupe multiplicatif $\mu_n(\mathbb{C})$.

Proposition 2.5.8 *Soit K un corps. Tout sous-groupe fini de K^* est cyclique.*

Lemme 2.5.9 *Soient G un groupe commutatif et $x_1, \dots, x_r \in G$ d'ordres respectifs $m_1, \dots, m_r$.*

1. *Si $m_1, \dots, m_r$ sont premiers entre eux deux à deux, alors $x = x_1 \cdots x_r$ est d'ordre $m_1 \cdots m_r$.*
2. *Si $m = p.p.c.m.\{m_1, \dots, m_r\}$, alors il existe $y \in G$ d'ordre m .*

Corollaire 2.5.10 *Soit K un corps.*

1. *$\mu_n(K)$ est un sous-groupe cyclique de K^* dont l'ordre divise n .*
2. *Si K est fini, alors le groupe K^* est cyclique.*

Si le corps K a q éléments, alors a) $q = p^s$ où p est un nombre premier ;
b) pour tout $x \in K^*$, on a $x^{q-1} = 1$; c) pour tout $x \in K$, on a $x^q = x$.

2.6 Anneaux ordonnés

Ensembles ordonnés

Soient E un ensemble et $\mathcal{R}$ une relation binaire dans E . La relation $\mathcal{R}$ est dite *antisymétrique* si, pour tous $x, y \in E$, $[x\mathcal{R}y \text{ et } y\mathcal{R}x] \Rightarrow [x = y]$.

Définition. Une relation binaire $\mathcal{R}$ dans un ensemble E est appelée une *relation d'ordre* si elle est réflexive, antisymétrique et transitive.

Exemples. Les relations binaires suivantes sont des relations d'ordre :

- dans $\mathbb{N}$, $a|b$,
- dans $\mathcal{P}(E)$, $A \subset B$,
- dans $\mathbb{R}^2$, $(x, y) \leq (x', y') := [x \leq x' \text{ et } y \leq y']$,
- dans $\mathbb{R}^2$, $(x, y) \leq (x', y') := [x < x' \text{ ou } (x = x' \text{ et } y \leq y')]$ (*ordre lexicographique*)

Définition. Soit E un ensemble.

- 1) E est dit *ordonné* s'il est muni d'une relation d'ordre $(\preceq)$.
- 2) E est dit *totalelement ordonné* si E est ordonné et si :
quels que soient $x, y \in E$, on a $x \preceq y$ ou $y \preceq x$.

Définition. Soit F une partie non vide d'un ensemble ordonné E .

1. x est un *majorant* (resp. *minorant*) de F :
 $\forall a \in F \quad a \preceq x$ (resp. $x \preceq a$),
2. F est *majoré* (resp. *minoré, borné*) :
 F possède un majorant (resp. un minorant, un majorant et un minorant),
3. x est un *plus grand élément* (resp. *plus petit élément*) de F :
 $x \in F$ est un majorant (resp. minorant) de F ,
4. x est une *borne supérieure* (resp. *inférieure*) de F :
 x est le plus petit des majorants (resp. minorants), s'il existe on le note :
 $\sup F$ ou $\sup_{a \in F} a$ (resp. $\inf F$ ou $\inf_{a \in F} a$).

Groupes ordonnés

Définition. Un groupe commutatif G est un *groupe ordonné* s'il est muni d'une relation d'ordre $\preceq$ compatible avec la loi du groupe, c.-à-d. :

$$\forall x, y, z \in G \quad [(x \preceq y) \Rightarrow (x + z \preceq y + z)].$$

Proposition 2.6.1 *Soit G un groupe commutatif.*

1. Si G est un groupe ordonné, alors l'ensemble $P = \{x \in G \mid 0 \preceq x\}$ vérifie $P \cap (-P) = \{0\}$ et $P + P \subset P$ où $-P = \{-x \mid x \in P\}$.
2. Si P est une partie de G telle que $P \cap (-P) = \{0\}$ et $P + P \subset P$, alors la relation $x \preceq y$ définie par $y - x \in P$ fait de G un groupe ordonné.

G est totalement ordonné si et seulement si $P \cup (-P) = G$.
 Un groupe d'ordre fini $n > 1$ ne peut être totalement ordonné.

Anneaux ordonnés

Définition. Un anneau A est un *anneau ordonné* s'il est muni d'une relation d'ordre $\preceq$ telle que :

$$\begin{aligned} \forall x, y, z \in A \quad & [(x \preceq y) \Rightarrow (x + z) \preceq (y + z)], \\ \forall x, y, z \in A \quad & [(x \preceq y \text{ et } 0 \preceq z) \Rightarrow (xz \preceq yz)]. \end{aligned}$$

Proposition 2.6.2 Soit A un anneau.

1. Si A est un anneau ordonné, alors l'ensemble $P = \{x \in A \mid 0 \preceq x\}$ vérifie $P \cap (-P) = \{0\}$, $P + P \subset P$ et $PP \subset P$,
2. Si P est une partie de A telle que $P \cap (-P) = \{0\}$, $P + P \subset P$ et $PP \subset P$, alors la relation $x \preceq y$ définie par $y - x \in P$ fait de A un anneau ordonné.

Règle. $[(0 \preceq x \preceq y) \text{ et } (0 \preceq z \preceq t)] \Rightarrow [xz \preceq yt]$.

Dans un anneau totalement ordonné, tout carré est positif.

Corps ordonnés

Définition. Un corps K est un *corps ordonné* s'il est un anneau totalement ordonné.

Règles. $[x \succ 0 \iff \frac{1}{x} \succ 0]$ et $[x \succ 1 \iff 0 \prec \frac{1}{x} \prec 1]$.

Un corps ordonné est nécessairement de caractéristique 0.

$\mathbb{Q}$ et $\mathbb{R}$ munis de $\leq$ sont des corps ordonnés.

$\mathbb{F}_p$ et $\mathbb{C}$ ne peuvent être des corps ordonnés.

Chapter 3

Anneaux particuliers

3.1 Anneaux principaux

Anneaux principaux

Définition. Un *anneau principal* est un anneau intègre dont tous les idéaux sont principaux.

Exercice. Un localisé d'un anneau principal est un anneau principal.

Exemples.

- (i) Les anneaux $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}_{(p)}$ sont principaux.
- (ii) Les anneaux $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[X]$ et $\mathbb{C}[X, Y]$ ne sont pas principaux.
- (iii) L'anneau $A[X]$ est principal si et seulement si A est un corps.

Proposition 3.1.1 *Les idéaux premiers d'un anneau principal A sont l'idéal (0) et, pour tout élément irréductible π de A , les idéaux maximaux πA .*

Corollaire 3.1.2 (1) *Dans un anneau principal, si π est irréductible et $\pi|ab$, alors $\pi|a$ ou $\pi|b$ (Euclide).*

(2) *Si K est un corps et $P \in K[X]$ irréductible, alors $K[X]/(P)$ est un corps.*

L'identité de Bezout

Proposition 3.1.3 *Soit A un anneau principal. Deux éléments a et b de A possèdent toujours un pgcd et un ppcm. De plus :*

- (1) *d est un pgcd de a et b si et seulement si $(d) = (a, b)$,*
- (2) *m est un ppcm de a et b si et seulement si $(m) = (a) \cap (b)$.*

Remarque. (1) Dans un anneau intègre quelconque, l'existence d'un ppcm pour a et b équivaut au fait que l'idéal $(a) \cap (b)$ soit principal.

(2) Par contre, dans un anneau intègre quelconque, l'existence d'un pgcd pour a et b ne suffit pas pour affirmer que l'idéal (a, b) est principal [considérer l'idéal (X, Y) de $\mathbb{C}[X, Y]$.]

Corollaire 3.1.4 (L'identité de Bezout) Soit A un anneau principal.

(1) Si d désigne un pgcd de a et b , alors il existe $u, v \in A$ tels que

$$au + bv = d.$$

(2) Les éléments a et b sont premiers entre eux si et seulement s'il existe u et $v \in A$ tels que

$$au + bv = 1.$$

Corollaire 3.1.5 (Gauss) Soit A un anneau principal. Si $a|bc$ et a et b sont premiers entre eux, alors $a|c$.

Corollaire 3.1.6 Soit A un anneau principal. Si $a_1, \dots, a_m$ sont premiers entre eux deux à deux, alors les idéaux $(a_1), \dots, (a_m)$ sont étrangers entre eux deux à deux et donc, par le théorème chinois :

$$A/(a_1 \cdots a_m) \simeq A/(a_1) \times \cdots \times A/(a_m).$$

Proposition 3.1.7 (Critère d'Eisenstein) Soient A un anneau principal, K son corps des fractions et $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polynôme unitaire de $A[X]$. S'il existe un élément irréductible π de A tel que π divise $a_0, a_1, \dots, a_{n-1}$, mais π^2 ne divise pas a_0 , alors $P(X)$ est irréductible dans $K[X]$ (et aussi dans $A[X]$).

Anneaux euclidiens

Définition. Un anneau intègre A est dit *euclidien* s'il est muni d'une *division euclidienne*, c'est-à-dire s'il existe une application (appelée *stathme euclidien*) $\varphi : A^* \rightarrow \mathbb{N}$ telle que, $\forall(a, b) \in A \times A^*, \exists(q, r) \in A^2$ tel que

$$a = bq + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(b).$$

Exemples. Les anneaux suivants sont euclidiens.

(i) $\mathbb{Z}$ avec $\varphi(k) = |k|$.

(ii) $\mathbb{Z}[i]$ avec $\varphi(z) = z.\bar{z}$.

(iii) Pour tout corps K , $K[X]$ avec $\varphi(P) = \deg P$.

Proposition 3.1.8 Un anneau euclidien est principal.

Remarque. A partir de la division euclidienne dans $\mathbb{Z}$, on a montré que $\mathbb{Z}$ est un anneau principal. Cette section sur les anneaux principaux prouve l'identité de Bezout dans $\mathbb{Z}$, ce qui justifie a posteriori –sans cercle vicieux– son utilisation antérieure dans les exemples relatifs à $\mathbb{Z}$.

Exercice. L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal, mais n'est pas euclidien.

Algorithme d'Euclide de détermination d'un pgcd

Soient A un anneau euclidien et $a, b \in A^*$. On construit une suite a_n par récurrence de la façon suivante. On pose :

$$a_0 = a \text{ et } a_1 = b$$

et, tant que $a_n \neq 0$, on choisit a_{n+1} de façon que :

$$a_{n-1} = a_n q_n + a_{n+1} \text{ où } a_{n+1} = 0 \text{ ou } \varphi(a_{n+1}) < \varphi(a_n).$$

Si a_k est le dernier terme non nul ainsi obtenu, alors a_k est le pgcd de a et b puisque :

$$\text{pgcd}(a, b) = \text{pgcd}(a_0, a_1) = \text{pgcd}(a_1, a_2) = \dots = \text{pgcd}(a_k, 0) = a_k.$$

Cet algorithme permet aussi d'obtenir u et $v \in A$ tels que $au + bv = \text{pgcd}(a, b)$. On utilise pour cela les relations successives en commençant par la dernière :

$$\begin{aligned} a_k &= a_{k-2} - a_{k-1}q_{k-1} = a_{k-2} - (a_{k-3} - a_{k-2}q_{k-2})q_{k-1} \\ &= a_{k-2}(1 + q_{k-2}q_{k-1}) - a_{k-3}q_{k-1} = \dots = a_1(\dots) + a_0(\dots). \end{aligned}$$

3.2 L'anneau $K[X]$

Dans cette section, K désigne un corps et on s'intéresse à l'anneau principal $K[X]$.

A propos de l'identité de Bezout

Proposition 3.2.1 *Si les polynômes non constants P et $Q \in K[X]$ sont premiers entre eux, alors il existe des polynômes U_0 et $V_0 \in K[X]$ uniques tels que*

$$U_0P + V_0Q = 1, \deg(U_0) < \deg(Q) \text{ et } \deg(V_0) < \deg(P).$$

Corollaire 3.2.2 *Si les polynômes non constants P et $Q \in K[X]$ admettent D pour pgcd, alors il existe des polynômes U et V uniques tels que*

$$UP + VQ = D,$$

avec

$$\deg(U) < \deg(Q) - \deg(D) \text{ et } \deg(V) < \deg(P) - \deg(D).$$

Exercice. De façon analogue : si a et b sont des entiers ≥ 2 premiers entre eux, alors il existe des entiers u_0 et v_0 uniques tels que

$$u_0 a - v_0 b = 1, \quad 0 < u_0 < b \text{ et } 0 < v_0 < a.$$

Résultant de deux polynômes

Soient

$$P(T) = a_0 + a_1 T + \cdots + a_p T^p \in K[X] \text{ avec } a_p \neq 0$$

et

$$Q(T) = b_0 + b_1 T + \cdots + b_q T^q \in K[X] \text{ avec } b_q \neq 0.$$

Notons $K_i[T]$ le K -espace vectoriel de dimension $i+1$ formé par les polynômes de degré $\leq i$ et considérons l'application linéaire :

$$\Phi : (U, V) \in K_{q-1}[T] \times K_{p-1}[T] \mapsto UP + VQ \in K_{p+q-1}[T].$$

Le rang de Φ est $p + q - d$ où d désigne le degré d'un pgcd D de P et Q . L'application Φ est bijective si et seulement si P et Q sont premiers entre eux [et alors, avec les notations ci-dessus, $\Phi(U_0, V_0) = 1$.]

Proposition 3.2.3 *Les polynômes P et Q ne sont pas premiers entre eux si, et seulement si, il existe $U, V \in K[X]$ non nuls tels que :*

$$UP + VQ = 0, \quad \deg(U) < \deg(Q) \text{ et } \deg(V) < \deg(P).$$

La matrice de Φ , relativement aux bases

$$\{(1, 0), (T, 0), \dots, (T^{q-1}, 0), (0, 1), (0, T), \dots, (0, T^{p-1})\}$$

et

$$\{1, T, \dots, T^{p+q-1}\},$$

est appelée *matrice résultant* des polynômes P et Q .

C'est la matrice carrée d'ordre $p + q$ suivante :

$$\begin{pmatrix} a_0 & 0 & . & . & 0 & b_0 & 0 & . & . & 0 \\ a_1 & a_0 & . & . & 0 & b_1 & b_0 & . & . & 0 \\ a_2 & a_1 & . & . & 0 & b_2 & b_1 & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ a_{q-1} & a_{q-2} & . & . & a_0 & b_{q-1} & b_{q-2} & . & . & 0 \\ a_q & a_{q-1} & . & . & a_1 & b_q & b_{q-1} & . & . & 0 \\ . & . & . & . & . & 0 & b_q & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ a_{p-1} & a_{p-2} & . & . & a_{p-q} & 0 & 0 & . & . & b_0 \\ a_p & a_{p-1} & . & . & . & 0 & 0 & . & . & b_1 \\ 0 & a_p & . & . & . & 0 & 0 & . & . & b_2 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & a_p & 0 & 0 & . & . & b_q \end{pmatrix}$$

Définition. Le *résultant* $Res(P, Q)$ des polynômes P et Q est le déterminant de la matrice résultant de P et Q .

Proposition 3.2.4 Les polynômes non constants $P = a_0 + a_1T + \dots + a_pT^p$ et $Q = b_0 + b_1T + \dots + b_qT^q \in K[X]$, où $\deg(P) = p > 0$ et $\deg(Q) = q > 0$, sont premiers entre eux si et seulement si $Res(P, Q) \neq 0$.

Complément. Si l'on n'est pas assuré du degré de P et de Q , c.-à-d., de ce que $a_p \neq 0$ et $b_q \neq 0$, alors $Res(P, Q) = 0$ signifie ou bien P et Q ne sont pas premiers entre eux, ou bien $a_p = b_q = 0$.

Remarque. On peut retrouver l'identité de Bezout à l'aide du résultant : on ajoute à la 1ère ligne la 2ème multipliée par T , la 3ème multipliée par T^2 , ..., la k ème par T^{k-1} , ... et on développe par rapport à cette 1ère ligne.

Définition. On appelle *discriminant* d'un polynôme P de degré $p \geq 2$, et on note $\Delta(P)$, la quantité $(-1)^{\frac{p(p-1)}{2}} Res(P, P')$ où P' désigne le polynôme dérivé de P .

Exemples.

$$\Delta(aX^2 + bX + c) = a(b^2 - 4ac) \quad \Delta(X^3 + pX + q) = -(4p^3 + 27q^2)$$

Proposition 3.2.5 Si $P(T) \in \mathbb{C}[T]$, alors le discriminant de P est nul si et seulement si P admet au moins une racine multiple dans $\mathbb{C}$.

Remarque. Dans $\mathbb{R}[X]$, $P = (X^2 + 1)^2$ et $P' = 4X(X^2 + 1)$ ne sont pas premiers entre eux, mais ils n'ont pas de racine commune dans $\mathbb{R}$.

3.3 Anneaux noethériens

Dans cette section, les anneaux considérés ne sont pas intègres a priori.

Définition. Un *idéal de type fini* est un idéal engendré par un nombre fini d'éléments.

L'idéal $\mathfrak{J}$ de l'anneau A engendré par $x_1, \dots, x_n$, c.-à-d. le plus petit idéal de A contenant $\{x_1, \dots, x_n\}$, est égal à $\mathfrak{J} = \{a_1x_1 + \dots + a_nx_n \mid a_1, \dots, a_n \in A\}$. On écrit $\mathfrak{J} = (x_1, \dots, x_n)$.

Définition. Un *anneau noethérien* A est un anneau dont tous les idéaux sont de type fini.

Les anneaux considérés seront le plus souvent noethériens, mais pas toujours.

Exemple. L'anneau $\mathbb{Z}^{\mathbb{N}}$ n'est pas noethérien : l'idéal $\mathfrak{J} = \{f : \mathbb{N} \rightarrow \mathbb{Z} \mid f(n) = 0 \text{ sauf pour au plus un nombre fini de } n\}$ n'est pas de type fini.

Proposition 3.3.1 Soit A un anneau. Les assertions suivantes sont équivalentes.

- (1) A est noethérien.
- (2) Toute suite croissante d'idéaux de A est stationnaire.
- (3) Tout ensemble non vide d'idéaux de A possède un élément maximal.

L'assertion (ii) signifie que, quelle que soit la suite $(\mathfrak{J}_n)_{n \in \mathbb{N}}$ d'idéaux de A telle que $\mathfrak{J}_n \subset \mathfrak{J}_{n+1}$, il existe n_0 tel que, pour $n \geq n_0$, $\mathfrak{J}_n = \mathfrak{J}_{n_0}$. L'assertion (iii) permet de retrouver l'existence d'idéaux maximaux contenant les idéaux propres.

Proposition 3.3.2 Soit A un anneau noethérien. Pour tout idéal propre $\mathfrak{J}$ de A , l'anneau quotient $A/\mathfrak{J}$ est noethérien.

Proposition 3.3.3 (Théorème de Hilbert) Si l'anneau A est noethérien, alors l'anneau $A[X]$ est noethérien.

Exemple. L'anneau $\mathbb{Z}[i\sqrt{5}] \simeq \mathbb{Z}[X]/(X^2 + 5)$ est noethérien.

Exercice. Soit A un anneau intègre noethérien. Pour toute partie multiplicative S de A , l'anneau localisé $S^{-1}A$ est noethérien.

Proposition 3.3.4 Soit A un anneau intègre noethérien. Tout élément non nul et non inversible de A peut s'écrire sous la forme

$$u\pi_1^{k_1} \dots \pi_r^{k_r}$$

où $u \in A^\times$, $\pi_1, \dots, \pi_r$ sont irréductibles et $r, k_1, \dots, k_r \in \mathbb{N}^*$.

Remarque. Cette écriture n'est pas nécessairement unique ; par exemple, dans l'anneau $\mathbb{Z}[i\sqrt{5}]$ on a : $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 3 \times 3$. En revanche :

Proposition 3.3.5 *Si l'anneau A est principal et si*

$$u\pi_1^{k_1} \cdots \pi_r^{k_r} = v\tau_1^{h_1} \cdots \tau_s^{h_s}$$

où $u, v \in A^\times$ et $\pi_1, \dots, \pi_r, \tau_1, \dots, \tau_s$ sont irréductibles, alors $s = r$ et, quitte à changer l'ordre des τ_i , pour $i = 1, \dots, r$, π_i et τ_i sont associés et $h_i = k_i$.

3.4 Polynômes à plusieurs variables

Dans cette section, les anneaux considérés ne sont pas intègres a priori.

On peut définir la A -algèbre $A[X, Y]$ des polynômes à 2 indéterminées à coefficients dans A de la façon suivante :

– les éléments de $A[X, Y]$ sont les *sommes finies* de la forme

$$\sum_{k,h} a_{k,h} X^k Y^h \text{ où } k, h \in \mathbb{N} \text{ et } a_{k,h} \in A,$$

– les règles d'addition et de multiplication s'écrivent

$$\sum_{k,h} a_{k,h} X^k Y^h + \sum_{k,h} b_{k,h} X^k Y^h = \sum_{k,h} (a_{k,h} + b_{k,h}) X^k Y^h$$

$$\sum_{k,h} a_{k,h} X^k Y^h \times \sum_{k,h} b_{k,h} X^k Y^h = \sum_{k,h} c_{k,h} X^k Y^h$$

où

$$c_{k,h} = \sum_{p+q=k, m+n=h} a_{p,m} b_{q,n}.$$

En fait, il y a un isomorphisme d'anneaux : $A[X, Y] \simeq A[X][Y]$ défini par :

$$\sum_{k,h} a_{k,h} X^k Y^h \in A[X, Y] \mapsto \sum_h b_h(X) Y^h \in A[X][Y] \text{ où } b_h = \sum_k a_{k,h} X^k.$$

Plus généralement, quel que soit $n \in \mathbb{N}^*$, on définit la A -algèbre $A[X_1, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans A de façon tout à fait analogue, les éléments de $A[X_1, \dots, X_n]$ étant les *sommes finies*

$$\sum_{k_1, \dots, k_n} a_{k_1, \dots, k_n} X_1^{k_1} \cdots X_n^{k_n} \text{ où } k_1, \dots, k_n \in \mathbb{N} \text{ et } a_{k_1, \dots, k_n} \in A.$$

En fait, l'anneau $A[X_1, \dots, X_n]$ peut aussi être défini par récurrence à l'aide de l'isomorphisme d'anneaux :

$$A[X_1, \dots, X_n] \simeq A[X_1, \dots, X_{n-1}][X_n].$$

Proposition 3.4.1 *Soit A un anneau et $n \in \mathbb{N}^*$.*

- (1) *Si A est intègre, alors $A[X_1, \dots, X_n]$ est intègre.*
- (2) *Si A est noethérien, alors $A[X_1, \dots, X_n]$ est noethérien.*

Corollaire 3.4.2 *Soient A un anneau noethérien, $n \in \mathbb{N}^*$ et $\mathfrak{J}$ un idéal de l'anneau $A[X_1, \dots, X_n]$. Alors l'anneau $A[X_1, \dots, X_n]/\mathfrak{J}$ est noethérien.*

Contre-exemple. L'anneau $A[X_1, \dots, X_n, \dots] = \bigcup_{n \in \mathbb{N}^*} A[X_1, \dots, X_n]$ n'est pas noethérien.

Degrés

Définition. On appelle *degré* du polynôme P par rapport à l'indéterminée X_k et on note $\deg_{X_k} P$ le degré de P considéré comme un polynôme en X_k à coefficients dans l'anneau $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n]$.

Par convention, $\deg(0) = -\infty$. On a alors :

$$\deg_{X_k}(P + Q) \leq \sup(\deg_{X_k} P, \deg_{X_k} Q),$$

$$\deg_{X_k}(PQ) \leq \deg_{X_k} P + \deg_{X_k} Q,$$

et, si A est intègre :

$$\deg_{X_k}(PQ) = \deg_{X_k} P + \deg_{X_k} Q.$$

Définition. On appelle *degré total* de $P = \sum a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n}$ et on note $\deg P$ la quantité :

$$\sup\{k_1 + \dots + k_n \mid a_{k_1, \dots, k_n} \neq 0\} \text{ avec } \deg(0) = -\infty.$$

Polynômes homogènes

Définition. On appelle *polynôme homogène de degré k* un polynôme dont les monômes sont tous de degré total k .

On pourra convenir que le polynôme 0 est homogène pour n'importe quel degré.

Si P est homogène de degré k et Q est homogène de degré l , alors PQ est homogène de degré $k + l$.

Proposition 3.4.3 . Soit $P \in A[X_1, \dots, X_n]^*$

(1) P est homogène de degré k si et seulement si, dans l'anneau $A[X_1, \dots, X_n, T]$, on a :

$$P(TX_1, \dots, TX_n) = T^k P(X_1, \dots, X_n).$$

(2) Si P est homogène de degré k , alors P vérifie la formule d'Euler :

$$X_1 \frac{\partial P}{\partial X_1} + \dots + X_n \frac{\partial P}{\partial X_n} = kP.$$

La réciproque est vraie en caractéristique 0.

3.5 L'anneau des polynômes symétriques

Soit K un corps et soit $n \in \mathbb{N}^*$. Le groupe Σ_n opère sur $K[X_1, \dots, X_n]$ par $(\sigma, P) \mapsto P_\sigma$ où

$$P_\sigma(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Pour $\sigma \in \Sigma_n$ fixé, $P \mapsto P_\sigma$ est un automorphisme de $K[X_1, \dots, X_n]$, c.-à-d., pour tous P, Q , $(P + Q)_\sigma = P_\sigma + Q_\sigma$, $(PQ)_\sigma = P_\sigma Q_\sigma$ (et $1_\sigma = 1$).

Attention, avec le choix précédent, pour $\sigma, \tau \in \Sigma_n$, on a : $(P_\sigma)_\tau = P_{\tau\sigma}$.

Définition. Soit G un sous-groupe de Σ_n . On dit qu'un polynôme P de $K[X_1, \dots, X_n]$ est invariant par G si, pour tout $\sigma \in G$, $P_\sigma = P$.

Pour que P soit invariant par G il faut et il suffit que $P_\sigma = P$ pour tous les σ décrivant un système de générateurs de G .

On note $K[X_1, \dots, X_n]^G$ le sous-anneau de $K[X_1, \dots, X_n]$ formé des polynômes invariants par G .

Définitions. 1) Un polynôme est dit *symétrique* s'il est invariant par le groupe symétrique Σ_n .

2) Un polynôme est dit *alterné* s'il est invariant par le groupe alterné $\mathcal{A}_n$.

L'anneau $K[X_1, \dots, X_n]^{\Sigma_n}$ se note aussi $K[X_1, \dots, X_n]^{sym}$.

Exemples. 1) Le polynôme $\prod_{1 \leq i < j \leq n} (X_j - X_i)$ est alterné.

2) Pour tout $k \geq 1$, le polynôme $S_k = X_1^k + X_2^k + \dots + X_n^k$ est symétrique.

3) Pour tout $k \in \{1, \dots, n\}$, $\Sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$ est appelé *polynôme symétrique élémentaire*. Ainsi pour $n = 3$ on a :

$$\Sigma_1 = X + Y + Z, \Sigma_2 = XY + YZ + ZX, \Sigma_3 = XYZ.$$

[Ne pas confondre le polynôme Σ_n et le groupe Σ_n .]

Proposition 3.5.1 Si $F = F_0 + F_1 + \dots + F_d$ où chaque F_i est homogène de degré i , alors F est symétrique si et seulement si chaque F_i est symétrique.

Proposition 3.5.2 (1) Si $P \in K[X_1, \dots, X_n]^{sym}$, alors $Q(X_1, \dots, X_{n-1}) = P(X_1, \dots, X_{n-1}, 0) \in K[X_1, \dots, X_{n-1}]^{sym}$.
 (2) Si $P \in K[X_1, \dots, X_n]^{sym}$ et $P(X_1, \dots, X_{n-1}, 0) = 0$, alors Σ_n divise P dans l'anneau $K[X_1, \dots, X_n]^{sym}$.

Théorème 3.5.3 Tout polynôme symétrique peut s'exprimer à l'aide des polynômes symétriques élémentaires. Plus précisément :
 pour tout $F \in K[X_1, \dots, X_n]^{sym}$, il existe $G \in K[\Sigma_1, \dots, \Sigma_n]$ tel que

$$F(X_1, \dots, X_n) = G(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n)).$$

Complément. Si F est homogène de degré total d , alors G est de poids d , c.-à-d. les monômes de G sont de la forme

$$a \Sigma_1^{\alpha_1} \Sigma_2^{\alpha_2} \dots \Sigma_n^{\alpha_n} \text{ avec } \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = d.$$

Par exemple, pour $n \geq 2$, $S_2 = X_1^2 + \dots + X_n^2$

$$= (X_1 + \dots + X_n)^2 - 2(X_1X_2 + \dots + X_{n-1}X_n) = \Sigma_1^2 - 2\Sigma_2.$$

Algorithme pour déterminer G . Soit F un polynôme symétrique et homogène de degré d . On munit $\mathbb{N}^n$ de l'ordre lexicographique et on considère le degré de F pour l'ordre lexicographique, c.-à-d., le plus grand n -uplet $(\beta_1, \dots, \beta_n)$ tel que F possède un monôme de la forme $aX_1^{\beta_1} \dots X_n^{\beta_n}$. Alors, le polynôme

$$F - a \Sigma_1^{\beta_1 - \beta_2} \Sigma_2^{\beta_2 - \beta_3} \dots \Sigma_{n-1}^{\beta_{n-1} - \beta_n} \Sigma_n^{\beta_n}$$

est un polynôme symétrique et homogène de degré d , mais de degré lexicographique strictement inférieur à celui de F . En itérant l'opération, on arrive au bout d'un nombre fini d'étapes l'expression du polynôme G .

Exemple. $F = \sum_{1 \leq i < j \leq 3} X_i^2 X_j^2$, $(\beta_1, \beta_2, \beta_3) = (2, 2, 0)$,
 $F - \Sigma_2^2 = -2(X_1^2 X_2 X_3 + X_1 X_2^2 X_3 + X_1 X_2 X_3^2) = -2\Sigma_1 \Sigma_3$. D'où : $G = \Sigma_2^2 - 2\Sigma_1 \Sigma_3$.

Relations. Dans $K[X_1, \dots, X_n][U, V]$, on a :

$$\prod_{k=1}^n (U + V X_k) = \sum_{k=0}^n \Sigma_k U^{n-k} V^k.$$

En particulier, dans $K[X_1, \dots, X_n][T]$, on a :

$$\prod_{k=1}^n (1 + T X_k) = \sum_{k=0}^n \Sigma_k T^k \quad \text{et} \quad \prod_{k=1}^n (T - X_k) = \sum_{k=0}^n (-1)^{n-k} \Sigma_{n-k} T^k.$$

Proposition 3.5.4 (Relations de Newton) .

1) Pour $k \geq n$, on a :

$$S_k - \Sigma_1 S_{k-1} + \cdots + (-1)^p \Sigma_p S_{k-p} + \cdots + (-1)^n \Sigma_n S_{k-n} = 0.$$

2) Pour $1 \leq k \leq n$, on a :

$$S_k - \Sigma_1 S_{k-1} + \cdots + (-1)^p \Sigma_p S_{k-p} + \cdots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k k \Sigma_k = 0.$$

Application. Pour $n \geq 3$, $S_3 = \Sigma_1^3 - 3\Sigma_1 \Sigma_2 + 3\Sigma_3$.

Proposition 3.5.5 Soient $n \in \mathbb{N}^*$, $P(X) = a_n X^n + \cdots + a_0 \in K[X]$ avec $a_n \neq 0$ et $(\alpha_1, \dots, \alpha_n) \in K^n$. Pour $1 \leq k \leq n$, posons $\Sigma_k(\alpha_1, \dots, \alpha_n) = \sigma_k$. Les assertions suivantes sont équivalentes :

$$1. P(X) = a_n (X - \alpha_1) \cdots (X - \alpha_n),$$

$$2. \sigma_k = (-1)^k \frac{a_{n-k}}{a_n} \text{ pour } 1 \leq k \leq n.$$

Application. Calcul de

$$s_7 = x_1^7 + x_2^7 + x_3^7$$

où x_1, x_2, x_3 désignent les racines de l'équation

$$X^3 + pX + q = 0.$$

En divisant X^7 par $X^3 + pX + q$ on obtient le reste

$$R(X) = 2pqX^2 + (q^2 - p^3)X - p^2q.$$

Donc, $x_i^7 = R(x_i)$ pour $i = 1, 2, 3$. Par suite, $s_7 = R(x_1) + R(x_2) + R(x_3) = 2pq s_2 + (q^2 - p^3) s_1 - 3p^2 q$. Or, $s_1 = \sigma_1 = 0$ et $s_2 = \sigma_1^2 - 2\sigma_2 = -2p$. D'où

$$s_7 = -7p^2 q.$$

Proposition 3.5.6 Soient

$$P(T) = a_0 + a_1 T + \cdots + a_p T^p$$

et

$$Q(T) = b_0 + b_1 T + \cdots + b_q T^q \in \mathbb{C}[X].$$

Notons $\alpha_1, \dots, \alpha_p$ les racines de P et $\beta_1, \dots, \beta_q$ les racines de Q (répétées selon leur multiplicité). Alors :

$$\begin{aligned} \text{Res}(P, Q) &= a_p^q b_q^p \prod_{1 \leq i \leq p, 1 \leq j \leq q} (\alpha_i - \beta_j) = a_p^q \prod_{i=1}^p Q(\alpha_i) \\ &= (-1)^{pq} b_q^p \prod_{j=1}^q P(\beta_j) = (-1)^{pq} \text{Res}(Q, P). \end{aligned}$$

Corollaire 3.5.7 *Si $P(T) = a_0 + a_1T + \dots + a_pT^p \in \mathbb{C}[X]$ a pour racines $\alpha_1, \dots, \alpha_p$, alors P a pour discriminant :*

$$\Delta(P) = a_p^{2p-1} \prod_{1 \leq i < j \leq p} (\alpha_i - \alpha_j)^2.$$

Chapter 4

Extensions algébriques

4.1 Éléments algébriques

Sous-corps engendrés

On sait que tout homomorphisme de corps est injectif. Ainsi, si $f : K \rightarrow L$ est un homomorphisme de corps, K peut être identifié à un *sous-corps* de L ; on dit aussi que L est un *sur-corps* de K ou encore une *extension* de K . (Bien sûr, les corps K et L ont alors la même caractéristique.)

On sait aussi qu'une intersection de sous-anneaux (resp. sous-corps) est un sous-anneau (resp. sous-corps). On peut donc parler de sous-anneau et de sous-corps engendrés : si A est une partie de L , le sous-anneau (resp. sous-corps) de L engendré par A est le plus petit sous-anneau (resp. sous-corps) de L contenant A .

Soit $K \subset L$ une extension de corps. Pour tout élément x de L , on note $K[x]$ le sous-anneau de L engendré par K et x . On a alors :

$K[x] = \{P(x) \mid P \in K[X]\}$ (ensemble des *expressions polynomiales* en x).

Pour tout élément x de L , on note $K(x)$ le sous-corps de L engendré par K et x . On a alors :

$K(x) = \left\{ \frac{P(x)}{Q(x)} \mid P, Q \in K[X], Q(x) \neq 0 \right\}$ (ensemble des *expressions rationnelles* en x).

Le corps $K(x)$ est le corps des fractions de l'anneau intègre $K[x]$.

Plus généralement, pour $x_1, \dots, x_n \in L$,

$$K[x_1, \dots, x_n] = K[x_1, \dots, x_{n-1}][x_n] = \{P(x_1, \dots, x_n) \mid P \in K[X_1, \dots, X_n]\}$$

$$K(x_1, \dots, x_n) = K(x_1, \dots, x_{n-1})(x_n) =$$

$$\left\{ \frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)} \mid P, Q \in K[X_1, \dots, X_n], Q(x_1, \dots, x_n) \neq 0 \right\}.$$

Définition. Soit $K \subset L$ une extension de corps.

1. On dit que l'extension est *monogène* s'il existe un élément $x \in L$ tel que $L = K(x)$.
2. On dit que l'extension est *de type fini* s'il existe un nombre fini d'éléments $x_1, \dots, x_n \in L$ tels que $L = K(x_1, \dots, x_n)$.

Eléments algébriques

Définition. Soit $K \subset L$ une extension de corps. On appelle *degré* de l'extension et on note $[L : K]$, la dimension, finie ou non, du K -espace vectoriel L . Si ce degré est fini, on dit qu'il s'agit d'une *extension finie*.

Par exemple, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{F}_3(T) : \mathbb{F}_3] = \infty$.

Définition. Soit $K \subset L$ une extension de corps et soit x un élément de L .

1. x est dit *algébrique* sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$.
2. x est dit *transcendant* sur K s'il n'est pas algébrique sur K .

Par exemple, $\sqrt{3}$ et i sont algébriques sur $\mathbb{Q}$, tandis que e et π sont transcendants sur $\mathbb{Q}$.

Proposition 4.1.1 Soit $K \subset L$ une extension de corps et soit x un élément de L . Les assertions suivantes sont équivalentes :

1. x est algébrique sur K ,
2. $[K(x) : K]$ est fini,
3. $K[x]$ est un corps.

Ainsi, lorsque x est algébrique sur K , $K(x) = K[x]$.

Corollaire 4.1.2 Soient $K \subset L$ une extension de corps et x un élément de L . L'homomorphisme d'anneaux $P \in K[X] \mapsto P(x) \in L$ a pour image $K[x]$ et pour noyau un idéal premier de $K[X]$.

1. Si x est transcendant sur K , le noyau est l'idéal (0) , $K[x] \simeq K[X]$, $K(x) \simeq K(X)$ et $[K(x) : K] = \infty$.
2. Si x est algébrique sur K , le noyau est engendré par un polynôme P irréductible sur K et $K[x] \simeq K[X]/(P)$. De plus, si $\deg(P) = n$, alors $\{1, x, \dots, x^{n-1}\}$ est une base de $K[x]$ sur K et $[K[x] : K] = n$.

Ainsi, $\mathbb{Q}[2 + i\sqrt{5}] \simeq \mathbb{Q}[X]/(X^2 + 9)$ tandis que $\mathbb{Q}[\pi] \simeq \mathbb{Q}[X]$.

Définition. Pour tout élément non nul $x \in L$ algébrique sur K , on appelle *polynôme minimal* de x sur K le polynôme unitaire $P \in K[X]$ de plus petit degré tel que $P(x) = 0$.

Le polynôme minimal de x sur K est l'unique polynôme unitaire irréductible sur K tel que $P(x) = 0$.

Proposition 4.1.3 Soient $K \subset L \subset M$ des extensions finies de corps. Si $(x_i)_{1 \leq i \leq n}$ est une base du K -espace vectoriel L et si $(y_j)_{1 \leq j \leq m}$ est une base du L -espace vectoriel M , alors $(x_i y_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une base du K -espace vectoriel M . En particulier

$$[M : K] = [M : L][L : K].$$

Exercice. Si $[L : K]$ est un nombre premier, alors il n'y a pas de corps strictement compris entre K et L (noter que $[L : K] = 1$ équivaut à $L = K$).

Corollaire 4.1.4 Soit $K \subset L$ une extension finie.

1. Tout élément $x \in L$ est algébrique sur K et le degré du polynôme minimal de x divise $[L : K]$.
2. Pour toute extension M de L , un élément $x \in M$ est algébrique sur K si et seulement si il est algébrique sur L .

Définition. L'extension $K \subset L$ est dite *algébrique* si tout élément de L est algébrique sur K .

Si L est une extension algébrique de K , alors, pour tous $x_1, \dots, x_n \in L$, on a $K(x_1, \dots, x_n) = K[x_1, \dots, x_n]$ et $[K(x_1, \dots, x_n) : K]$ est fini.

Par exemple, pour tout $n \in \mathbb{N}^*$, $[\mathbb{Q}[e^{\frac{i\pi}{2^n}}] : \mathbb{Q}] = 2^n$, et $\bigcup_{n \in \mathbb{N}} \mathbb{Q}[e^{\frac{i\pi}{2^n}}]$ est une extension de $\mathbb{Q}$ qui est algébrique mais non de type fini.

4.2 Norme et trace

Soit $K \subset L$ une extension algébrique de degré n . Pour x fixé dans L , considérons l'application K -linéaire $m_x : y \in L \mapsto xy \in L$. Si x est non nul, m_x est un K -automorphisme du K -espace vectoriel L . On se souvient du polynôme caractéristique de m_x :

$$\det(m_x - X \text{id}_L) = (-1)^n X^n + (-1)^{n-1} \text{Tr}(m_x) X^{n-1} + \dots + \det(m_x).$$

Définition. Soit $K \subset L$ une extension algébrique de degré fini et soit $x \in L$.

1. On appelle *trace* de x sur K , et on note $\text{Tr}_{L/K}(x)$, la trace de l'application K -linéaire m_x .
2. On appelle *norme* de x sur K , et on note $N_{L/K}(x)$, le déterminant de l'application K -linéaire m_x .

Ces deux définitions dépendent du sur-corps L contenant x .

Exemple. Si $[L : K] = n$ et $a \in K$, alors $\text{Tr}_{L/K}(a) = na$ et $N_{L/K}(a) = a^n$.

Proposition 4.2.1 Soit $K \subset L$ une extension algébrique de degré fini.

1. L'application trace, $\text{Tr}_{L/K} : x \in L \mapsto \text{Tr}_{L/K}(x) \in K$, est une forme linéaire sur le K -espace vectoriel L .
2. L'application norme, $N_{L/K} : x \in L \mapsto N_{L/K}(x) \in K$, induit un homomorphisme de groupes multiplicatifs de L^* sur K^* .

En d'autres termes, pour tous $x, y \in L$ et $a \in K$, on a :

$$\begin{aligned} \text{Tr}_{L/K}(x + y) &= \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y), & \text{Tr}_{L/K}(ax) &= a \text{Tr}_{L/K}(x), \\ N_{L/K}(xy) &= N_{L/K}(x) N_{L/K}(y), & \text{et on a aussi, } N_{L/K}(ax) &= a^n N_{L/K}(x). \end{aligned}$$

Proposition 4.2.2 Supposons $L = K[x]$.

Soit $n = [L : K]$ et soit $F(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ le polynôme minimal de x sur K . Alors :

1. Le polynôme caractéristique de m_x est égal $(-1)^n F(X)$,
2. $\text{Tr}_{K[x]/K}(x) = -a_{n-1}$,
3. $N_{K[x]/K}(x) = (-1)^n a_0$.

Corollaire 4.2.3 *Supposons $K \subset \mathbb{C}$.*

Soit $x \in \mathbb{C}$ algébrique sur K . Si $x_1 = x, x_2, \dots, x_n$ désignent les racines du polynôme minimal de x sur K , alors :

1. $Tr_{K[x]/K}(x) = x_1 + x_2 + \dots + x_n,$
2. $N_{K[x]/K}(x) = x_1 x_2 \dots x_n.$

Les racines $x_1 = x, x_2, \dots, x_n$ sont appelées les *conjugués* de x sur K .

Exemple. 1) $K = \mathbb{Q}, L = \mathbb{Q}[\sqrt{2}], x = a + b\sqrt{2}, F(X) = X^2 - 2aX + a^2 - 2b^2, Tr_{\mathbb{Q}[\sqrt{2}]/\mathbb{Q}}(a + b\sqrt{2}) = 2a, N_{\mathbb{Q}[\sqrt{2}]/\mathbb{Q}} = a^2 - 2b^2 [= (a + b\sqrt{2})(a - b\sqrt{2})].$

2) $K = \mathbb{Q}, L = \mathbb{Q}[i\sqrt{5}], x = a + ib\sqrt{5}, F(X) = X^2 - 2aX + a^2 + 5b^2, Tr_{\mathbb{Q}[i\sqrt{5}]/\mathbb{Q}}(a + ib\sqrt{5}) = 2a, N_{\mathbb{Q}[i\sqrt{5}]/\mathbb{Q}} = a^2 + 5b^2 [= (a + ib\sqrt{5})(a - ib\sqrt{5})].$

Application. Soit $x = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] : x \in \mathbb{Z}[i\sqrt{5}]^\times \Leftrightarrow N_{\mathbb{Q}[i\sqrt{5}]/\mathbb{Q}}(x) = \pm 1.$

Exercice. Soit p un nombre premier ≥ 3 et soit $\zeta_p = e^{2i\pi/p}$. Alors :

$$Tr_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(\zeta_p) = -1 \quad \text{et} \quad N_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(\zeta_p) = 1.$$

Proposition 4.2.4 *Soient $K \subset L \subset M$ des extensions algébriques de degrés finis. Posons $[L : K] = n$ et $[M : L] = m$. Pour tout $x \in L$, on a :*

$$Tr_{M/K}(x) = m Tr_{L/K}(x) \quad \text{et} \quad N_{M/K}(x) = (N_{L/K}(x))^m.$$

Corollaire 4.2.5 *Supposons $K \subset L \subset \mathbb{C}$ et $[L : K] = n$.*

Soit $x \in L$ et soient $x_1 = x, x_2, \dots, x_r$ les conjugués de x sur K . Alors,

$$[K(x) : K] = r, \quad n = rs \quad \text{où} \quad s = [L : K(x)]$$

$$Tr_{L/K}(x) = s(x_1 + \dots + x_r) \quad \text{et} \quad N_{L/K}(x) = (x_1 \dots x_r)^s.$$

4.3 Corps de rupture et corps de décomposition

Corps de rupture

Définition. Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K . On appelle *corps de rupture* du polynôme P toute extension L de K contenant un élément x tel que :

1. $P(x) = 0,$
2. $L = K[x].$

Dans ce cas, le degré de l'extension $[K[x] : K]$ est égal au degré de P . De plus, si P est unitaire, alors P est le polynôme minimal de x .

Par exemple, $\mathbb{Q}[i]$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{Q}$.

Proposition 4.3.1 *Soit $P \in K[X]$ un polynôme irréductible sur K . Le corps $K[X]/(P)$ est une extension de K . Muni de l'élément $\bar{X}$, image de X dans le quotient, c'est un corps de rupture du polynôme P , appelé corps de rupture canonique de P .*

Exemple. $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$ où $\bar{X}$ est classiquement noté i .

Définition. On dit que deux extensions L et M du corps K sont K -isomorphes s'il existe un isomorphisme de corps de L sur M qui laisse fixes les éléments de K .

Par exemple, $z \in \mathbb{C} \mapsto \bar{z} \in \mathbb{C}$ est un $\mathbb{R}$ -automorphisme de $\mathbb{C}$.

Proposition 4.3.2 *Soit $P \in K[X]$ un polynôme irréductible et soit L une extension de K . Si L contient une racine de P , alors, pour toute racine y de P dans L , on a : $K[y] \simeq K[X]/(P)$. Deux corps de rupture de P sont toujours K -isomorphes.*

Exemple. Le polynôme $X^3 - 2$ irréductible sur $\mathbb{Q}$ admet dans $\mathbb{C}$ les trois racines : $\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2$. On a :

$$\mathbb{Q}[X]/(X^3 - 2) \simeq \mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\sqrt[3]{2}j] \simeq \mathbb{Q}[\sqrt[3]{2}j^2].$$

Exercice. Si P est un polynôme irréductible sur K dont le degré est premier avec $[L : K]$, alors P est encore irréductible sur L .

Corps de décomposition

Définition. Soit $P = a_0 + a_1X + \dots + a_nX^n \in K[X]$ où $a_n \neq 0$. On appelle *corps de décomposition* de P toute extension L de K contenant des éléments $x_1, \dots, x_n$ (non nécessairement distincts) tels que :

1. P s'écrit sous la forme $a_n \prod_{1 \leq i \leq n} (X - x_i)$,
2. $L = K[x_1, \dots, x_n]$.

Exemple. $\mathbb{Q}[\sqrt[3]{2}, j] = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2]$ est un corps de décomposition de $X^3 - 2$. On a

$$\left[\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q} \right] = \left[\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q}[\sqrt[3]{2}] \right] \times \left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q} \right] = 6.$$

Proposition 4.3.3 *Pour tout polynôme $P \in K[X]$, il existe une extension L de K qui est un corps de décomposition de P . Deux corps de décomposition de P sont K -isomorphes.*

4.4 Clôture algébrique

Proposition 4.4.1 *Soit $K \subset L$ une extension de corps.*

1. *L'ensemble $\overline{K}_L = \{x \in L \mid x \text{ algébrique sur } K\}$ est un sous-corps de L .*
2. *Tout élément de L algébrique sur $\overline{K}_L$ est dans $\overline{K}_L$.*

Le sous-corps $\overline{K}_L$ est appelé la *fermeture algébrique* de K dans L .

Définition. Un corps Ω est dit *algébriquement clos* si, pour tout sur-corps L de Ω , tout élément de L algébrique sur Ω appartient en fait à Ω .

Ω est algébriquement clos équivaut aux assertions équivalentes suivantes :

- tout polynôme irréductible $P \in \Omega[X]$ est de degré 1,
- tout polynôme non constant $P \in \Omega[X]$ se décompose en un produit de facteurs du premier degré à coefficients dans Ω (P est dit *scindé* dans Ω),
- tout polynôme non constant $P \in \Omega[X]$ a au moins une racine dans Ω .

Théorème de d'Alembert.

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

Un corps algébriquement clos est infini.

Un corps algébriquement clos ne peut être ordonné.

Définition. Une *clôture algébrique* d'un corps K est une extension Ω de K telle que

1. Ω soit algébrique sur K ,
2. Ω soit algébriquement clos.

Par exemple, $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 4.4.2 (admis) *Tout corps K possède une clôture algébrique. Deux clôtures algébriques de K sont K -isomorphes.*

Exemple. La fermeture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}$. C'est un corps dénombrable appelé *corps des nombres algébriques*.

Remarque. Si Ω est une clôture algébrique de K , alors, pour tout polynôme $P \in K[X]$, Ω contient un corps de décomposition et un seul de P (c'est le corps engendré sur K par les racines de P dans Ω).

4.5 Racines de l'unité

Soit K un corps et soit $n \in \mathbb{N}^*$. On rappelle qu'une *racine n -ième de l'unité* du corps K est un élément x de K tel que $x^n = 1$ et que l'ensemble $\mu_n(K) = \{x \in K \mid x^n = 1\}$ est un sous-groupe cyclique de K^* dont l'ordre divise n .

Proposition 4.5.1 *Soit K_n un corps de décomposition du polynôme $X^n - 1$ de $K[X]$. Si la caractéristique de K ne divise pas n , alors $\mu_n(K_n)$ est cyclique d'ordre n , donc est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

On rappelle qu'une *racine primitive n -ième de l'unité* dans K est un élément $\zeta \in K$ tel que $\zeta^n = 1$ et, pour $1 \leq m < n$, $\zeta^m \neq 1$.

Si la caractéristique de K ne divise pas n , tout générateur ζ de $\mu_n(K_n)$ est une racine primitive n -ième de l'unité et il y a en a $\varphi(n)$.

$[k \in \mathbb{Z}/n\mathbb{Z} \mapsto \zeta^k \in \mu_n(K_n)]$ est un isomorphisme de groupes et les générateurs k du groupe additif $\mathbb{Z}/n\mathbb{Z}$ correspondent aux générateurs ζ^k du groupe multiplicatif $\mu_n(K_n)$.

Exemple. $\mu_n(\mathbb{C}) = \{e^{\frac{2ik\pi}{n}} \mid 0 \leq k \leq n-1\}$. Les racines primitives correspondent aux entiers k premiers avec n .

Définition. On appelle *n -ième polynôme cyclotomique* le polynôme :

$$\Phi_n(X) = \prod_{0 \leq k \leq n-1, (k,n)=1} (X - e^{\frac{2ik\pi}{n}}).$$

Proposition 4.5.2 *Soit $n \in \mathbb{N}^*$. On a :*

1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. $n = \sum_{d|n} \varphi(d)$.

3. $\Phi_n(X) \in \mathbb{Z}[X]$.
4. $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ [assertion admise].

Proposition 4.5.3 *Tout anneau intègre fini est un corps.*

Proposition 4.5.4 1. *Le cardinal q d'un corps fini est toujours une puissance d'un nombre premier.*

2. *Toute puissance q d'un nombre premier est le cardinal d'un corps fini.*
3. *Deux corps de même cardinal fini q sont isomorphes.*

Proposition 4.5.5 *Soit p un nombre premier et soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$.*

1. *Pour tout sous-corps fini K de $\overline{\mathbb{F}}_p$, on a $|K| = p^f$ où $f \in \mathbb{N}^*$.*
2. *Pour tout $f \in \mathbb{N}^*$, il existe un unique sous-corps $\mathbb{F}_q$ de $\overline{\mathbb{F}}_p$ tel que $|\mathbb{F}_q| = p^f = q$.*
3. *Soit $f \in \mathbb{N}^*$, soit $q = p^f$ et soit ζ une racine primitive $(q - 1)$ -ième de l'unité dans $\overline{\mathbb{F}}_p$. Alors $\mathbb{F}_q = \mathbb{F}_p[\zeta]$.*
4. $\overline{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}^*} \mu_n(\overline{\mathbb{F}}_p)$.

Contents

1	Groupes	1
1.1	Relations d'équivalence et ensembles quotients	1
1.2	Lois de composition et quotients	2
1.3	Groupes et sous-groupes	3
1.4	Groupes quotients	5
1.5	Homomorphismes de groupes	6
1.6	Exemples	9
1.7	Groupe opérant sur un ensemble	11
2	Anneaux	15
2.1	Anneaux	15
2.2	Idéaux et anneaux quotients	17
2.3	Homomorphismes	19
2.4	Anneaux intègres	23
2.5	Corps	25
2.6	Anneaux ordonnés	29
3	Anneaux particuliers	31
3.1	Anneaux principaux	31
3.2	L'anneau $K[X]$	33
3.3	Anneaux noethériens	36
3.4	Polynômes à plusieurs variables	37
3.5	L'anneau des polynômes symétriques	39
4	Extensions algébriques	43
4.1	Eléments algébriques	43
4.2	Norme et trace	46
4.3	Corps de rupture et corps de décomposition	47
4.4	Clôture algébrique	49
4.5	Racines de l'unité	50