APPENDICE A

RAPPELS D'ALGÈBRE

Cette appendice est un résumé des notions et des résultats fondamentaux d'algèbre utilisés dans le cours. Ils constituent le bagage essentiel de fin de parcours de licence.

A.1. Ensembles et relations

A.1.1. Ensembles — Dans la suite, nous supposerons le lecteur familier avec les concepts et les construction de base de la théorie des ensembles. On ne rappellera donc pas les notions d'appartenance $x \in A$, d'inclusion $A \subset B$, d'union $A \cup B$ et d'intersection $A \cap B$, ainsi que la définition de produit cartésien $A \times B$ ou d'application $f : A \to B$ et de leurs propriétés (injectivité, surjectivité,...). Les ensembles seront généralement indiqués par des lettres capitales $A, B, E, X, \ldots$ et leurs éléments par des minuscules $a, b, e, x, \ldots$. On réservera des symboles spéciaux pour des ensembles classiques tels que l'ensemble $\mathbb{N}$ des entiers naturels, l'ensemble $\mathbb{Z}$ des entiers relatifs, l'ensemble $\mathbb{Q}$ des nombres rationnels, l'ensemble $\mathbb{R}$ des nombres réels et finalement l'ensemble $\mathbb{C}$ des nombres complexes.

Le ***cardinal*** d'un ensemble fini A, noté $\mathrm{Card}(A)$, est le nombre de ses éléments. Un ensemble A est ***infini*** s'il n'est pas fini ; on écrira alors simplement $\mathrm{Card}(A) = \infty$, sans aborder des notions plus fines de cardinaux et d'ordinaux, qui n'auraient pas leur place dans ce cours.

A.1.2. Relations — Une ***relation (binaire)*** sur un ensemble X est un sous-ensemble R du produit cartésien $X \times X$. Étant donné un couple $(x, y) \in R$, on dit que x est ***en relation avec*** y et on utilise les notations xRy ou $x \sim_R y$. Parmi les différentes propriétés que peut vérifier une relation R sur X, nous retiendrons les suivantes :

- ***Reflexivité*** : quel que soit $x \in X$, on a $x \sim_R x$.
- ***Symétrie*** : quels que soient $x, y \in X$, si $x \sim_R y$ alors $y \sim_R x$.
- ***Antisymétrie*** : quels que soient $x, y \in X$, si $x \sim_R y$ et $y \sim_R x$ alors $x = y$.

- ***Transitivité*** : quels que soient $x, y, z \in X$, si $x \sim_R y$ et $y \sim_R z$ alors $x \sim_R z$.

Une relation R sur X qui est reflexive, antisymétrique et transitive est une ***relation d'ordre***; on dit aussi que R définit un ***ordre*** sur X. L'ordre est ***total*** si, étant donnés $x, y \in X$ on a $x \sim_R y$ ou $y \sim_R x$.

Exemple A.1.1 — La relation d'ordre usuelle sur $\mathbb{N}$ est un ordre total vérifiant la propriété fondamentale suivante : tout sous-ensemble non vide de $\mathbb{N}$ possède un plus petit élément. Dans ce cas, on dit que la relation d'ordre est un ***bon ordre***, ou que $\mathbb{N}$ est ***bien ordonné***. Cette propriété (de laquelle on déduit le principe de récurrence, qui lui est en fait équivalent) est à la bas de pratiquement toute construction ou démonstration concernant les entiers. On remarquera que la relation d'ordre usuelle sur $\mathbb{Z}$, qui prolonge celle de $\mathbb{N}$, n'est pas un bon ordre. Par contre, tout sous-ensemble ***minoré*** (resp. ***majoré***) de $\mathbb{Z}$ possède un plus petit (resp. plus grand) élément.

Une ***relation d'équivalence*** R sur un ensemble X est une relation reflexive, symétrique et transitive. Cette notion est fondamentale et reviendra souvent tout au long du cours. Le sous-ensemble $[x] \subset X$ des éléments qui sont en relation avec un élément fixé $x \in X$ est appelé ***classe de R-équivalence***, ou simplement ***classe d'équivalence*** de x. L'ensemble X se décompose en union disjointe de classes d'équivalence et on note X/R le sous-ensemble de $\mathcal{P}(X)$ formé par ces classes. On dit également que X/R est le ***quotient*** de X par la relation R.

A.2. Groupes abéliens

A.2.1. Définitions et premières propriétés — Un ***groupe*** est un ensemble G muni d'une loi de composition interne

$$G \times G \to G$$
$$(x, y) \mapsto x \cdot y$$

vérifiant les propriétés suivantes :

- ***Associativité :*** quels que soient $x, y, z \in G$, on a l'identité
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$
- ***Élément neutre :*** il existe $e \in G$ tel que, pour tout $x \in G$, on a les identités
$$x \cdot e = e \cdot x = x.$$
- ***Inverse :*** pour tout $x \in G$, il existe $y \in G$ tel que
$$x \cdot y = y \cdot x = e.$$

Un groupe est ***abélien*** ou ***commutatif*** si, quels que soient $x, y \in G$, on a l'identité

$$x \cdot y = y \cdot x.$$

Bien que la plupart des résultats présentés dans cet appendice soient valables dans le contexte le plus générale, tous les groupes considérés dans la suite sont abéliens.

Le groupe G est ***fini*** si c'est un ensemble fini. Dans ce cas, son cardinal, plus souvent noté $|G|$, est appelé ***ordre*** du groupe.

Exemples A.2.1 —

1. L'ensemble réduit à un seul élément e, avec pour loi de composition
$$e \cdot e = e,$$
est un groupe, appelé ***groupe trivial***.
2. L'ensemble $\mathbb{Z}$ des entiers relatifs muni de la loi de composition $(x, y) \mapsto x + y$ est un groupe commutatif, d'élément neutre 0. On l'appelle le ***groupe additif*** des entiers relatifs. En remplaçant $\mathbb{Z}$ par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on obtient respectivement le groupe additif des nombres rationnels, celui des nombres réels et celui des nombres complexes.
3. L'ensemble $\mathbb{Q}^\times$ des nombres rationnels non nuls, muni de la loi de composition $(x, y) \mapsto xy$ est un groupe commutatif, d'élément neutre 1. C'est le ***groupe multiplicatif*** des nombres rationnels non nuls. On définit de même les groupes multiplicatifs $\mathbb{R}^\times$ et $\mathbb{C}^\times$.
4. Soient $G_1, \ldots, G_n$ des groupes et considérons leur produit cartésien
$$G = G_1 \times \cdots \times G_n.$$
La loi de composition sur G définie par l'égalité
$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n),$$
munit G d'une structure de groupe. L'élément neutre est $(e_1, \ldots, e_n)$, où e_i est l'élément neutre de G_i. L'inverse d'un élément $x = (x_1, \ldots, x_n)$ est donné par la formule
$$x^{-1} = (x_1^{-1}, \ldots, x_n^{-1}).$$
Le groupe $(G, \cdot)$ est appelé ***produit direct*** des groupes $G_1, \ldots, G_n$, ou encore ***groupe produit*** de $G_1, \ldots, G_n$.

Fixons un élément x d'un groupe G. Pour tout entier naturel n, on définit l'élément x^n de manière récursive en posant $x^0 = e$ et $x^{n+1} = x \cdot x^n$. Si n est un entier négatif, on pose $x^n = y^{-n}$, où y est l'inverse de x. On vérifie alors facilement l'identité
$$x^{n+m} = x^n \cdot x^m,$$
de laquelle on déduit la seconde identité
$$(x^n)^m = x^{nm},$$
les deux étant valables pour tout choix d'entiers n et m. En particulier, l'élément x^{-1} coïncide avec l'inverse de x.

Remarque A.2.2 — La loi de composition sous-jacente à un groupe est généralement notée multiplicativement $(x, y) \mapsto xy$, ou additivement $(x, y) \mapsto x + y$. En notation multiplicative, on note généralement 1 l'élément neutre. En notation additive, on parle d'***opposé*** plutôt que d'inverse, utilisant le symbole 0 pour l'élément neutre. Pour tout entier n, on écrit alors nx au lieu de x^n. Par exemple, l'opposé de x est égal à $(-1)x$, noté simplement $-x$.

A.2.2. Sous-groupes, groupes quotient — Un sous-ensemble H d'un groupe G est un ***sous-groupe*** si les conditions suivantes sont remplies :

- L'élément neutre 1 appartient à H.
- Quels que soient $x, y \in H$, l'élément xy appartient à H.
- Pour tout $x \in H$, l'inverse x^{-1} de x appartient à H.

En d'autres termes, un H est un sous-groupe si c'est un groupe lorsque l'on le munit de la loi de composition induite par celle de G.

Exemples A.2.3 —

1. Les sous-ensembles G et $\{1\}$ sont des sous-groupes de G. Le sous-groupe $\{1\}$ s'appelle le ***sous-groupe trivial*** de G. Avec un leger abus de notation, il sera simplement noté 1 (ou 0 si l'on adopte la notation additive).
2. Le sous-ensemble de $\mathbb{R}^\times$ formé par les nombres réels strictement positifs, ainsi que le groupe $\mu_2 = \{\pm 1\}$, sont des sous-groupes de $\mathbb{R}^\times$.
3. Si n est un entier relatif, le sous-ensemble
$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$
est un sous-groupe de $\mathbb{Z}$.
4. L'intersection d'une famille (finie ou infinie) de sous-groupes d'un groupe est un sous-groupe.

La relation binaire sur G définie par $x \sim y$ si et seulement si $xy^{-1} \in H$ est une relation d'équivalence. L'ensemble quotient $G/\sim$ est noté G/H. Dans la suite, on désigne par $[g] \in G/H$, la classe d'équivalence d'un élément $g \in G$. On a alors l'identité
$$[g] = gH = \{gh \mid h \in H\}.$$

Remarque A.2.4 — Si le groupe G est noté noté additivement, la relation d'équivalence définie précédemment s'écrit alors sous la forme $x \sim_y$ si et seulement si $x - y \in H$. La classe $[g] \in G/H$ d'un élément de $g \in G$ est alors notée $g + H$.

Étant donnés $x, y \in G/H$ soient $g, h \in G$ tels que $x = [g]$ et $y = [h]$. Dans ce cas, l'élément $xy = [gh] \in G/H$ ne dépend que de x et y et pas du choix des représentants g et h choisis. En effet, si $x = [g']$ et $y = [h']$, ce qui se traduit par $g' = gu$ et $h' = hv$, avec $u, v \in H$, on obtient les identités $g'h' = ghw$, avec $w = uv \in H$ (ici,

la commutativité de G joue un rôle crucial), d'où $[g'h'] = [gh]$. On définit ainsi une loi de composition sur G/H et on vérifie sans difficulté que ce dernier est alors muni d'une structure de groupe, appelé ***quotient*** de G par (rapport à) H.

A.2.3. Parties génératrices, groupes finiment engendrés — Considérons un sous-ensemble non vide S d'un groupe G. L'ensemble H des éléments de G s'écrivant comme produit fini de puissances d'éléments de S (une telle écriture n'étant pas nécessairement unique) est un sous-groupe de G. On le note généralement $\langle S \rangle$ et on vérifie facilement qu'il coïncide avec l'intersection des sous-groupes de G contenant S. On dit alors que H est ***engendré*** par S, que S est une ***famille génératrice*** ou encore un ***système de générateurs*** de H. Tout sous-groupe H de G possède une famille génératrice. Il suffit en effet de considérer le système de générateurs formé par H lui-même.

Un groupe G (ou l'un de ses sous-groupes) est ***finiment engendré*** s'il possède un système fini de générateurs. Si G est fini, il est clairement finiment engendré. On dit que G est ***monogène*** s'il est engendré par un unique élément g, ce qui revient à affirmer que tout élément de G s'écrit de manière (pas nécessairement unique) comme g^n (ou ng, en notation additive), avec n entier. Finalement, le groupe G est ***cyclique*** lorsqu'il est fini et monogène. L'***ordre*** d'un élément $g \in G$ est par définition l'ordre du sous-groupe $\langle g \rangle$ qu'il engendre (ce dernier pouvant être infini).

Exemple A.2.5 — Le groupe $\mathbb{Z}$ est monogène, les entiers 1 et -1 étant ses uniques générateurs.

A.2.4. Le théorème de Lagrange — Soit H un sous-groupe d'un groupe (abélien) G. Si le groupe quotient G/H est fini, son ordrel, noté $(G : H)$ est l'***indice*** de H dans G. Si G est fini, il en est de même pour H et G/H. Le résultat ci-dessous est incontournable et fondamental en théorie des groupes finis.

Théorème A.2.6 **(Lagrange)** — *Pour tout sous-groupe H d'un groupe fini G, on a l'identité*

$$|G| = |H| \cdot (G : H).$$

En particulier, l'ordre de H divise celui de G.

Démonstration — Pour tout $g \in G$, les classes d'équivalence $[1] = H$ et $[g] = gH$ sont en bijection via l'application qui à h associe gh et ont donc même cardinal, égal à $|H|$. Le résultat s'en déduit aussitôt, car G est la réunion disjointe de ses classes d'équivalence modulo H. □

A.2.5. Homomorphismes — Une application $f : G \to G'$ d'un groupe G dans un groupe G' est un ***homorphisme*** si

$$f(xy) = f(x)f(y)$$

quels que soient $x, y \in G$. L'homomorphisme f est un ***isomorphisme*** s'il est bijectif, on dit alors que G et G' sont ***isomorphes***. Un ***automorphisme*** d'un groupe G est un isomorphisme $f : G \to G$.

Exemples A.2.7 —

1. Soit G un groupe. Étant donné un élément $x \in G$, l'application $f_x : \mathbb{Z} \to G$ définie par $f_x(n) = x^n$ est un homomorphisme de groupes. Son image est le sous-groupe monogène $\langle x \rangle$ de G engendré par x.
2. Pour tout sous-groupe H d'un groupe G, l'application
$$\pi : G \to G/H$$
définie par $\pi(g) = [g] = gH$ est un homomorphisme de groupes, ce qui résulte de la définition de la loi de groupe sur G/H.

Soit $f : G \to G'$ un homomorphisme de groupes. L'image $f(H)$ par f d'un sous-groupe H de G est un sous-groupe de G' et que, réciproquement, l'image réciproque $f^{-1}(H')$ de d'un sous-groupe H' de G' est un sous-groupe de G. L'***image*** de f est le sous-groupe $\mathrm{Im}(f) = f(G)$ de G'. Son ***noyau***, noté $\ker(f)$ le sous-groupe $f^{-1}(1)$ de G. On a donc
$$\ker(f) = \{x \in G \mid f(x) = 1\}.$$

Lemme A.2.8 — *Soit $f : G \to G'$ un homomorphisme de groupes. Le sous-groupe $\ker(f)$ est trivial si et seulement si f est injectif.*

Démonstration — Supposons f injectif et soit x un élément de $\ker(f)$. On a les égalités $f(x) = 1 = f(1)$, d'où $x = 1$. Le sous-groupe $\ker(f)$ est donc trivial. Réciproquement, pour $\ker(f) = 1$, soient x et y deux éléments de G tels que $f(x) = f(y)$. On a $f(x)f(y)^{-1} = 1$ i.e. $f(xy^{-1}) = 1$, d'où $xy^{-1} = 1$, puis $x = y$. □

Proposition A.2.9 — *Un homomorphisme de groupes $f : G \to G'$ induit une bijection entre les sous-groupes de $\mathrm{Im}(f)$ et les sous-groupes de G contenant $\ker(f)$.*

Démonstration — Nous avons déjà vu que si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G', clairement contenu dans $\mathrm{Im}(f)$. Réciproquement, si H' est un sous-groupe de $\mathrm{Im}(f)$, alors $f^{-1}(H')$ est un sous-groupe de G contenant $\ker(f)$ (car 1 appartient à H'). Il suffit de vérifier que ces deux applications sont inverses l'une de l'autre. De manière générale, en considérant f juste en tant qu'application, on a l'inclusion $f(f^{-1}(H')) \subset H'$ pour tout sous-ensemble H' de G' et cette inclusion est une égalité si et seulement si H' est contenu dans $\mathrm{Im}(f)$. Soit maintenant H un sous-groupe de G. On vérifie facilement que l'ensemble
$$H \ker(f) = \{hk \mid h \in H, k \in \ker(f)\}$$
est un sous-groupe de G et que l'on a l'identité
$$f^{-1}(f(H)) = H \ker(f).$$

En particulier, si H contient $\ker(f)$ on a bien l'identité $f^{-1}(f(H)) = H$. □

Remarque A.2.10 — Soit H un sous-groupe d'un groupe G. Si dans la proposition ci-dessus on considère la projection canonique $G \to G/H$, on en déduit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H, i.e. tout sous-groupe de G/H est du type K/H, où K est un sous-groupe de K contenant H.

Le résulat suivant, connu sous le nom de ***théorème d'isomorphisme (pour les groupes)***, est un outil fondamental en théorie des groupes.

Théorème A.2.11 — *Étant donné un homomorphisme de groupes $f : G \to G'$, les groupes $G/\ker(f)$ et $\mathrm{Im}(f)$ sont isomorphes.*

Démonstration — L'application $\varphi : G/\ker(f) \to \mathrm{Im}(f)$ qui associe à une classe $x = g\ker(f)$ l'élément $f(g)$ est bien définie. En effet, si h est un second élément de x, on a l'identité $h = gk$, avec $k \in \ker(f)$, d'où les relations

$$f(h) = f(gk) = f(g)f(k) = f(g).$$

Étant donnés deux éléments $x = u\ker(f)$ et $y = v\ker(f)$ de G/H, on a les identités

$$\varphi(xy) = f(uv) = f(u)f(v) = \varphi(x)\varphi(y),$$

ce qui montre que φ est un homomorphisme. Ce dernier est surjectif, car étant donné $w = f(u) \in \mathrm{Im}(f)$, on a par définition $w = \varphi(x)$, avec $x = u\ker(f)$. Il est également injectif, car pour $x = u\ker(f)$, l'identité $\varphi(x) = 1$ se traduit par la relation $f(u) = 1$, ou encore $u \in \ker(f)$, d'où les identités

$$x = u\ker(f) = \ker(f).$$

□

A.3. Anneaux

A.3.1. Anneaux et sous-anneaux — Un ***anneau*** A est un ensemble muni de deux lois de composition, une ***somme*** $(x, y) \mapsto x + y$ et un ***produit*** $(x, y) \mapsto xy$, telles que les conditions suivantes soient vérifiées :

- L'ensemble A est un groupe par rapport à la somme.
- Le produit est associatif et possède un élément neutre.
- Le produit est distributif par rapport à la somme, i.e. quels que soient $x, y, z \in A$, on a les relations

$$x(y + z) = xy + xz \quad \text{et} \quad (x + y)z = xz + yz.$$

Si la multiplication est commutative, autrement dit, si l'on a $xy = yx$ quels que soient $x, y \in A$, on dit que A est ***commutatif***. Sauf mention explicite du contraire, tous les anneaux considérés dans la suite seront supposés commutatifs.

On notera 0 l'élément neutre de A pour la somme et 1 l'élément neutre pour le produit. Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit ***nul***. Avec un léger abus de notation, on écrira alors $A = 0$.

Exemples A.3.1 —

1. En munissant $\mathbb{Z}$ des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est commutatif. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition de la multiplication usuelles (construites à partir de celles de $\mathbb{Z}$) sont également des anneaux commutatifs.
2. Soient $A_1, \ldots, A_n$ des anneaux. D'après la section précédente, on peut alors considérer le groupe (additif)
$$A = A_1 \times \cdots \times A_n,$$
produit direct des groupes (additifs) $A_1, \ldots, A_n$. L'ensemble A possède une structure naturelle d'anneau, le produit étant défini par la relation
$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$
Si tous les anneaux A_i sont commutatifs, il en est de même pour A. On dit que A est le ***produit direct*** des A_i, ou encore l'***anneau produit*** des A_i. Notons que l'élément neutre multiplicatif de A est $(1, \ldots, 1)$.

Un sous-ensemble B d'un anneau A est un ***sous-anneau*** si les conditions suivantes sont vérifiées :

- B est un sous-groupe additif de A.
- Quels que soient $x, y \in B$, leur produit xy appartient à B.
- L'élément neutre multiplicatif 1 de A appartient à B.

On vérifie que si B est un sous-anneau de A, alors B muni des deux lois de composition induites par celles de A est un anneau.

A.3.2. Idéaux et anneaux quotient — Un sous-ensemble $\mathfrak{a}$ d'un anneau A est un ***idéal*** si les deux conditions suivantes sont vérifiées :

- L'ensemble $\mathfrak{a}$ est un sous-groupe additif de A.
- Quels que soient $x \in \mathfrak{a}$ et $y \in A$, leur produit xy est un élément de $\mathfrak{a}$.

Exemples A.3.2 —

1. Tout anneau A possède deux idéaux particuliers : l'***idéal nul*** 0, formé par le seul élément neutre pour la somme et l'anneau A lui-même. Un idéal non nul et différent de A est ***propre***.
2. Dans $\mathbb{Z}$, tout sous-groupe est automatiquement un idéal.
3. Soit a un élément d'un anneau A. L'ensemble des éléments de la forme ab, où b parcourt A, est un idéal de A. On l'appelle idéal ***monogène*** engendré par a et on le note aA ou simplement (a).

Un idéal $\mathfrak{a}$ d'un anneau A étant un sous-groupe par rapport à la somme, on peut considérer le groupe quotient

$$A/\mathfrak{a} = \{a + \mathfrak{a} \mid a \in A.\}$$

On définit une nouvelle loi de composition interne sur $A/\mathfrak{a}$ (le produit) en posant

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a}.$$

On vérifie facilement qu'elle est bien définie et qu'elle munit le groupe abélien $A/\mathfrak{a}$ d'une structure d'anneau, appelé ***quotient*** de A par rapport à $\mathfrak{a}$.

A.3.3. Homomorphismes — Étant donnés deux anneaux A et B, une application $f : A \to B$ est un ***homomorphisme*** si elle vérifie les porpriétés suivantes :

- L'application f est un homomorphisme de groupes additifs.
- Quels que soient $a, b \in A$, on a l'identité $f(ab) = f(a)f(b)$.
- On a la relation $f(1) = 1$.

Exemples A.3.3 —

1. Étant donné un anneau, l'application $\iota : \mathbb{Z} \to A$ définie par

   $$\iota(n) = n \cdot 1 = 1 + \cdots (n) \cdots + 1$$

   pour $n \in \mathbb{N}$ et par $\iota(-n) = -\iota(n)$ est un homomorphisme d'anneaux. C'est d'ailleurs l'unique. En effet, un homomorphisme d'anneaux $f : \mathbb{Z} \to A$ est un homomorphisme de groupes, univoquement déterminé par l'image du générateur 1 du groupe monogène $\mathbb{Z}$, celle-ci étant imposée la condition $f(1) = 1$.
2. Pour tout idéal $\mathfrak{a}$ d'un anneau A, la projection $A \to A/\mathfrak{a}$ est un homomorphisme d'anneaux.
3. Considérons des anneaux $A_1, \ldots, A_n$ et notons $A = A_1 \times \cdots \times A_n$ leur produit. Pour tout $i \in \{1, \ldots, n\}$, l'application $\pi_i : A \to A_i$ qui associe à $(a_1, \ldots, a_n)$ l'élément a_i est un homomorphisme d'anneaux, appelé ***projection canonique***. Il est important de remarquer que l'application $f_i : A_i \to A$ définie par $f_i(a) = (0, \ldots, 0, a, 0, \ldots, 0)$ vérifie les relations $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$ quels que soient $a, b \in A_i$ mais que ce n'est néanmoins pas un homomorphisme d'anneaux car $f(1)$ n'est pas l'unité de A.

Soit $f : A \to B$ un homomorphisme d'anneaux. On vérifie facilement que l'ensemble $\mathrm{Im}(f)$, appelé ***image*** de f est un sous-anneau de B et que, pour tout idéal $\mathfrak{a}$ de A, son image $f(\mathfrak{a})$ par f est un idéal de $\mathrm{Im}(f)$ (mais généralement pas de B). De même, pour tout idéal $\mathfrak{b}$ de B, l'ensemble $f^{-1}(\mathfrak{b})$ est un idéal de A. Le ***noyau*** $\ker(f)$ d'un homomorphisme d'anneaux $f : A \to B$ est l'ensemble

$$\ker(f) = f^{-1}(0) = \{a \in A \mid f(a) = 0\}.$$

En d'autres termes, $\ker(f)$ est le noyau de l'application f, considérée en tant qu'homomorphisme de groupes additifs. Au vu de ce qui précéde, c'est un idéal.

Proposition A.3.4 — *Un homomorphisme d'anneaux $f : A \to B$ est injectif si et seulement si* $\ker(f) = 0$. *De plus, l'application f induit une bijection entre l'ensemble des idéaux de* $\mathrm{Im}(f)$ *et l'ensemble des idéaux de A contenant* $\ker(f)$.

Démonstration — On procède exactement comme pour la proposition A.2.9 et le lemme qui la précède. □

Remarque A.3.5 — Pour tout idéal $\mathfrak{a}$ de A, en considérant la projection $A \to A/\mathfrak{a}$, on obtient une bijection entre les idéaux de $A/\mathfrak{a}$ et les idéaux de A contenant $\mathfrak{a}$, i.e. tout idéal de $A/\mathfrak{a}$ s'écrit comme $\mathfrak{b}/\mathfrak{a}$, où $\mathfrak{b}$ est un idéal de A contenant $\mathfrak{a}$.

Le résultat suivant est l'analogue du théorème d'isomorphisme pour les homomorphismes de groupes. Nous en donnons une version à peine plus détaillée.

Théorème A.3.6 — *Considérons deux homomorphismes d'anneaux $f : A \to B$, et $g : A \to C$, avec f surjectif. Si* $\ker(f)$ *est contenu dans* $\ker(g)$ *alors il existe un unique homomorphisme d'anneaux $h : B \to C$ tel que $g = hf$. On dit alors que le le diagramme*

$$\begin{array}{ccc} A & \xrightarrow{\quad g \quad} & C \\ & {\scriptstyle f}\searrow \quad \nearrow{\scriptstyle h} & \\ & B & \end{array}$$

est commutatif.

Démonstration — On reprend essentiellement la même construction que pour le théorème A.2.11 : étant donné $b \in B$, soit $a \in A$ tel que $f(a) = b$. On pose alors $h(b) = g(a)$. Si $a' \in A$ vérifie $f(a') = b$, on a $a - a' \in \ker(f) \subset \ker(g)$, d'où $g(a) = g(a')$. L'application $h : B \to C$ est donc bien définie. Étant donnés $b = f(a)$ et $b' = f(a')$, on a $b + b' = f(a + a')$, ce qui donne

$$h(b + b') = g(a + a') = g(a) + g(a') = h(b) + h(b').$$

De même, l'identité $bb' = f(aa')$ amène aux relations

$$h(bb') = g(bb') = g(b)g(b') = h(b)h(b').$$

Finalement, on a $f(1) = 1$ et donc $h(1) = 1$. On a montré que h est un homomorphisme d'anneaux. Concernant son unicité, si $h' : B \to C$ est une second homomorphisme vérifiant la propriété de l'énoncé, on a $hf = h'f$. Pour $b = f(a) \in B$, on obtient alors les identités

$$h(b) = hf(a) = h'f(a) = h'(b).$$

□

Corollaire A.3.7 — *Étant donné un homomorphisme d'anneaux $f : A \to B$, les anneaux* $A/\ker(f)$ *et* $\mathrm{Im}(f)$ *sont canoniquement isomorphes.*

Démonstration — Quitte à remplacer B par $\mathrm{Im}(f)$, on peut supposer f surjectif. Considérons la projection canonique $g : A \to A/\ker(f)$. On a $\ker(f) = \ker(g)$ et le résultat précédent affirme qu'il existe un unique couple d'homomorphismes $h : A/\ker(f) \to B$ et $k : B \to A/\ker(f)$ tels que $g = kf$ et $f = hg$. Mais dans ce cas, on obtient $f = hkf$, d'où $hk = 1$, par surjectivité de f et, de même, on a l'identité $kh = 1$. □

A.3.4. Éléments réguliers, inversibles et diviseurs de zéro — Un élément a d'un anneau A est ***régulier*** si, pour tout $b \in A$, l'identité $ab = 0$ est équivalente à $b = 0$. En d'autres termes, a est régulier s'il vérifie la ***propriété d'effacement*** par rapport au produit : étant donnés $b, c \in A$, on a $ab = ac$ si et seulement si $b = c$. Un idéal $\mathfrak{a}$ de A est ***principal*** s'il est monogène et engendré par un élément régulier, ce qui revient à affirmer qu'il existe un élément $a \in \mathfrak{a}$ tel que l'homomorphisme de groupes additifs $A \to \mathfrak{a}$ qui associe à $b \in A$ l'élément ab soit bijectif. Un anneau A est ***intègre*** si tous ses éléments non nuls sont réguliers. En d'autres termes, A est intègre si et seulement si le produit de deux éléments non nuls est non nul. Dans un anneau intègre, la notion d'idéal monogène et d'idéal principal coïncident et tout sous-anneau d'un anneau intègre est intègre. Finalement, l'anneau A est ***principal*** si tous ses idéaux non nuls sont principaux (en particulier, A est intègre).

Exemple A.3.8 — L'anneau $\mathbb{C}$ est intègre. Il en est donc de même pour ses sous-anneaux $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$. Tout corps est clairement principal. D'après la classification de ses sous-groupes (qui coïncident avec ses idéaux) l'anneau $\mathbb{Z}$ est principal.

Un 'élément $a \in A$ est une ***unité***, ou un ***élément inversible*** s'il existe $b \in A$ tel que $ab = 1$ (on rappelle que l'anneau A est supposé commutatif). On dit alors que b est l'***inverse*** de a. Un élément inversible est régulier, la réciproque étant fausse en général. L'ensemble $A^\times$ des unités de A est un groupe (multiplicatif), appelé ***groupe des unités***. Un ***corps*** est un anneau non nul dans lequel tout élément non nul est inversible. Un corps est automatiquement intègre.

Exemple A.3.9 — Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps mais il n'en est pas de même pour $\mathbb{Z}$, le groupe $\mathbb{Z}^\times$ étant réduit aux éléments 1 et -1.

Remarque A.3.10 — Un élément a d'un anneau A est inversible si et seulement si $aA = A$. En effet, si a est inversible, d'inverse b, on a l'identité $1 = ab \in aA$, d'où $c = abc \in aA$ pour tout $c \in A$, ou encore $aA = A$. Réciproquement, pour $aA = A$, on a en particulier $1 \in A$, d'où l'existence d'un élément $b \in A$ tel que $ab = 1$.

Proposition A.3.11 — *Soient $A_1, \ldots, A_n$ des anneaux et notons A leur produit direct. On a alors l'identité*

$$A^\times = A_1^\times \times \cdots \times A_n^\times.$$

Démonstration — Tout d'abord, on a l'inclusion $A_1^\times \times \cdots \times A_n^\times \subset A^\times$, l'inverse de $(a_1, \ldots, a_n)$ étant donné par $(a_1^{-1}, \ldots, a_n^{-1})$. Réciproquement, si $(a_1, \ldots, a_n) \in A$ est inversible, d'inverse $(b_1, \ldots, b_n)$, on obtient les identités

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) = (1, \ldots, 1),$$

ce qui implique que pour tout entier $i \in \{1, \ldots, n\}$, l'élément $a_i \in A_i$ est inversible, d'inverse b_i, d'où l'inclusion $A^\times \subset A_1^\times \times \cdots \times A_n^\times$, qui est alors une égalité. □

Un élément $a \in A$ qui n'est pas régulier est un ***diviseur de zéro***, ce qui revient à affirmer qu'il existe un élément non nul $b \in A$ tel que $ab = 0$. On dit que a est ***nilpotent*** s'il existe un entier strictement positif n tel que $a^n = 0$. L'anneau A est ***réduit*** s'il ne possède pas de nilpotents non nuls.

A.3.5. Idéaux premiers et maximaux — Un idéal $\mathfrak{p}$ d'un anneau A est ***premier*** si $\mathfrak{p} \neq A$ et, si quels que soient $a, b \in A$, la relation $ab \in \mathfrak{p}$ implique que $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. L'idéal $\mathfrak{p}$ est ***maximal*** s'il n'est contenu dans aucun idéal propre de A. En d'autres termes, si $\mathfrak{a}$ est un idéal de A contenant $\mathfrak{p}$, on a $\mathfrak{a} = \mathfrak{p}$ ou $\mathfrak{a} = A$.

Lemme A.3.12 — *Un anneau non nul A est un corps si et seulement s'il ne possède pas d'idéaux autres que 0 et A.*

Démonstration — Si A est un corps et $\mathfrak{a}$ est un idéal non nul, en fixant un élément non nul $a \in \mathfrak{a}$, on obtient $aA = A$ (cf. la remarque A.3.10), et donc $\mathfrak{a} = A$. Récirpoquement, pour tout élément non nul $a \in A$, l'idéal aA étant non nul, il coïncide avec A et l'élément a est alors inversible. □

Ce dernier résultat implique en particulier que tout homomorphisme $f : K \to A$ d'un corps K dans un anneau A non nul est injectif. En effet, on a $\ker(f) \neq A$ (car $f(1) = 1 \neq 0$), d'où $\ker(f) = 0$.

Proposition A.3.13 — *Un idéal $\mathfrak{a}$ de A est premier (resp. maximal) si et seulement si le quotient $A/\mathfrak{a}$ est intègre (resp. un corps).*

Démonstration — Notons $\bar{a}$ l'élément $a + \mathfrak{a}$ de $A/\mathfrak{a}$. On remarquera que $\bar{a}\bar{b} = \overline{ab}$ (c'est une conséquence directe du fait que la projection $A \to A/\mathfrak{a}$ est un homomorphisme d'anneaux) et que $\bar{a} = 0$ si et seulement si $a \in \mathfrak{a}$. On en déduit immédiatement l'équivalence entre l'intégrité de $A/\mathfrak{a}$ et la primalité de $\mathfrak{a}$. Maintenant, d'après la proposition A.3.4 et la remarque qui la suit, il existe une bijection entre les idéaux de $A/\mathfrak{a}$ et les idéaux de A contenant $\mathfrak{a}$. Le lemme précédent affirme alors que $A/\mathfrak{a}$ est un corps si et seulement si $\mathfrak{a}$ est maximal. □

Corollaire A.3.14 — *Tout idéal maximal est premier.*

Démonstration — En effet, d'après le résultat précédent si $\mathfrak{p}$ est un idéal maximal d'un anneau A, le quotient $A/\mathfrak{p}$ est un corps, qui est intègre, ce qui implique que $\mathfrak{p}$ est premier. □

Le résultat élémentaire ci-dessous sera très utile dans la suite du cours.

Lemme A.3.15 — *Si un idéal premier d'un anneau contient le produit d'une famille finie d'idéaux alors il contient l'un d'entre eux.*

Démonstration — Soit $\mathfrak{p}$ un idéal premier d'un anneau A contenant le produit d'une famille finie $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ d'idéaux et supposons qu'il ne contienne aucun d'entre eux. Pour tout $i \in \{1, \ldots, n\}$, choisissons un élément $a_i \in \mathfrak{a}_i$ n'appartenant pas à $\mathfrak{p}$. Par hypothèse, le produit $a_1 \cdots a_n$ appartient à $\mathfrak{p}$ mais ce dernier ne contient aucun des facteurs, contredisant sa primalité. □

A.3.6. Algèbres sur un anneau — Dans ce cours, par ***algèbre*** sur un anneau A, ou simplement ***A-algèbre*** on entendra la donnée d'un anneau B, que l'on ne supposera généralement pas commutatif, et d'un homomorphisme d'anneaux $\iota : A \to B$, appelé ***morphisme structural*** tel que son image soit contenue dans le centre de B (le centre de B étant le sous-anneau formé par les éléments $b \in B$ tels que $bc = cb$ pour tout $c \in B$). Si l'homomorphisme ι est injectif, l'algèbre est dite ***fidèle***. Un ***homomorphisme*** de A-algèbres est un homomorphisme d'anneaux qui commute avec les morphismes structuraux.

Exemple A.3.16 — L'exemple classique d'algèbre sur un anneau provient de l'algèbre linéaire : étant donnés un corps K et un K-espace vectoriel V, l'anneau des endomorphismes $\mathrm{End}_K(V)$ est muni d'une structure canonique de K-algèbre, le corps K s'identifiant au sous-anneau des endomorphismes scalaires. Si V est de dimension finie n, ayant fixé une K-base, on obtient un isomorphisme d'anneaux entre $\mathrm{End}_K(V)$ et l'anneau $\mathrm{M}_n(K)$ des matrices carrées de taille n. On remarquera que pour tout anneau A, on peut considérer la A-algèbre $\mathrm{M}_n(A)$ des matrices carrées de taille n à coefficient dans A, la structure d'anneau étant définie exactement comme dans le cas d'un corps.

Si B est une A-algèbre commutative, toute B-algèbre possède une structure naturelle de A-algèbre, obtenue par composition des morphismes structuraux.

Remarque A.3.17 — Étant donné un sous-anneau A d'un anneau B, on a une structure naturelle de A-algèbre sur B (induite par l'inclusion). Sauf mention explicite du contraire B sera toujours automatiquement muni d'une telle structure.

A.3.7. Anneaux de polynômes — Soit A un anneau commutatif. D'un point de vue abstrait, un ***anneau de polynômes (à une indéterminée)*** sur A est la donnée d'un couple (B, X), où B est une A-algèbre et X est un élément de B, appelé ***indeterminée***, ou ***variable***, vérifiant la propriété universelle suivante : étant donnée une A-algèbre C et un élément $c \in C$, il existe un unique homomorphisme de A-algèbres

$$B \xrightarrow{\mathrm{ev}_c} C$$

tel que $\mathrm{ev}_c(X) = c$. L'homomorphisme ev_c est appelé ***homomorphisme d'évaluation*** en c. D'après cette propriété, si (C, Y) est un second anneau de poynômes sur A alors il existe un unique homomorphisme $\sigma_Y : B \to C$ tel que $\sigma_Y(X) = Y$ et on vérifie facilement que c'est un isomorphisme d'anneaux.

D'un point de vue concret, l'existence d'un anneau de polynômes découle de la construction classique suivante : considérons l'ensemble B formé par les suites $(a_n)_{n\geq 0}$ d'éléments de A qui sont nulles à partir d'un certain rang ou, ce qui revient au même, l'ensemble des applications de $a : \mathbb{N} \to A$ telles que $a(n) = 0$ pour n assez grand (on dit alors que a est à ***support fini***, c'est à dire que le sous-ensemble de $\mathbb{N}$ formé par les entiers n tels que $a_n \neq 0$ est fini). On commence par définir une structure de groupe abélien sur B en posant

$$(a_n) + (b_n) = (a_n + b_n).$$

L'élément neutre est donné par la suite $0 = (0, 0, \dots)$ de terme constant égal à 0, l'opposé de (a_n) étant la suite $(-a_n)$. Le produit de deux suites est défini par la relation

$$(a_n) \cdot (b_n) = (c_n),$$

où l'on a posé

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

On vérifie alors que l'ensemble B, muni de ces deux opérations, est un anneau. L'élément neutre pour le produit est la suite $1 = (1, 0, 0, \dots)$. Les suites du type $(a, 0, \dots)$ forment un sous-anneau de B qui s'identifie canoniquement avec A et munit B d'une structure de A-algèbre. Posons finalement $X = (0, 1, 0, \dots, 0, \dots)$. Pour tout entier $n \geq 1$, et tout élément $a = (a, 0, \dots) \in A$, on a alors l'identité $aX^n = (0, \dots, 0, a, 0, \dots)$, où le $(n+1)$-ème terme de la suite est a et où tous les autres sont nuls. En particulier, en posant $X^0 = 1$, pour toute suite $f = (a_n) \in B$, on obtient l'identité

$$f = \sum_{n\geq 0} a_n X^n,$$

la somme étant finie, car a_n est nul pour n assez grand. Par ailleurs, cette écriture est unique, car deux suites coïncident si et seulement si leurs termes sont les mêmes. La suite f sera désormais appelée ***polynôme***, les éléments a_n étant ses ***coefficients***. L'anneau B est noté $A[X]$. Étant donnés une A-algèbre C et un élément $c \in C$, l'homomorphise ev_c associe au polynôme $f = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ sa ***valeur*** en c, qui est l'élément

$$\mathrm{ev}_c(f) = a_0 + a_1 c + \cdots + a_n c^n \in C,$$

que l'on note simplement $f(c)$. L'image $A[c]$ de l'homomorphisme ev_c est la plus petite sous-A-algèbre de C contenant x. Ayant supposé A commutatif, on en déduit qu'il en est de même pour l'anneau $A[c]$.

Le ***degré*** d'un polynôme non nul $f = a_0 + a_1 X + \cdots \in A[X]$, noté $\deg(f)$, est le plus grand entier n tel que le coefficient a_n soit non nul. L'élément $a_n \in A$ est alors appelé ***coefficient dominant*** de f. Un polynôme est ***unitaire*** si son coefficient dominant est égal à 1. Le produit de deux polynômes unitaires est unitaire. Il est par ailleurs commode de poser $\deg(0) = -\infty$, avec l'accord tacite que $-\infty \leq n$ et $-\infty + n = -\infty$ pour tout entier naturel n. Avec cette convention, étant donnés deux polynômes $f, g \in A[X]$, on vérifie facilement les inégalités

$$\deg(fg) \leq \deg(f) + \deg(g) \quad \text{et} \quad \deg(f+g) \leq \max\{\deg(f), \deg(g)\},$$

la première de ces relations étant une égalité lorsque le coefficient dominant de f ou de g est régulier (tel est le cas, par exemple, si A est intègre). On en déduit en particulier que l'anneau $A[X]$ est intègre si et seulement s'il en est de même pour A. Une des deux implications étant immédiate (car tout sous-anneau d'un anneau intègre est intègre), si A est intègre, étant donnés deux polynômes non nuls f et g, on a les relations $\deg(fg) = \deg(f) + \deg(g) \geq 0$, ce qui implique que fg est non nul. Lorsque A est intègre, ces mêmes considérations sur le degré montrent que les groupes $A^\times$ et $A[X]^\times$ coïncident, ce qui est faux en général (on pourra montrer que l'inclusion $A^\times \subset A[X]^\times$ est stricte si et seulement si l'anneau A est réduit, cf. le paragraphe A.3.4).

Remarque A.3.18 — Étant donné un anneau A (pas nécessairement commutatif), il existe un unique homomorphisme d'anneaux $\mathbb{Z} \to A$. En particulier, A possède une et une unique structure de $\mathbb{Z}$-algèbre. Ayant fixé un élément $a \in A$, il existe alors un unique homomorphisme d'anneaux $\mathrm{ev}_a : \mathbb{Z}[X] \to A$ tel que $\mathrm{ev}_a(X) = a$. Son image, notée $\mathbb{Z}[a]$, est le plus petit sous-anneau de A contenant a. D'après le théorème d'isomorphisme, il s'identifie au quotient de $\mathbb{Z}[X]$ par rapport à un idéal.

La notion d'anneau de polynômes à plusieurs indeterminées est définie de manière récursive : étant donné un anneau A, l'anneau $A[X_1, \ldots, X_n]$ est l'anneau de polynômes $B[X_n]$ d'indeterminée X_n sur l'anneau $B = A[X_1, \ldots, X_{n-1}]$. Ce dernier jouit de la propriété universelle suivante, qui le caractérise à isomorphisme unique près : étant donnée une A-algèbre C et n éléments $c_1, \ldots, c_n \in C$ il existe un unique homomorphisme de A-algèbres $A[X_1, \ldots, X_n] \to C$ tel que $f(X_i) = c_i$ pour tout $i \in \{1, \ldots, n\}$.

Le résultat suivant est l'un des outils principaux dans l'étude des anneaux de polynômes.

Lemme A.3.19 — *Soit A un anneau et considérons deux polynômes $f, g \in A[X]$, avec f non nul. Si le coefficient dominant de f est inversible alors il existe un unique couple de polynômes $q, r \in A[X]$ tels que*

$$g = fq + r$$

et $\deg(r) < \deg(f)$.

Démonstration — On procède par récurrence sur l'entier $m = \deg(g)$. En posant $n = \deg(f)$, pour $m < n$, il suffit de prendre $q = 0$ et $r = g$. Supposons donc $m > n$ et que la propriété est vérifiée pour tout polynôme de degré strictement inférieur à m. Si a et b désignent respectivement les coefficients dominant de f et de g, en posant

$$q' = ba^{-1}X^{m-n},$$

le polynôme $g' = g - q'f$ est de degré strictement inférieur à m. Par hypothèse de récurrence, il existe $q'', r \in A[X]$, avec $\deg(r) < n$ tels que $g' = q''f + r$ et, en posant $q = q' + q''$, on obtient le résultat voulu. Supposons finalement que $fq + r = fq' + r'$, avec $r, r' \in A[X]$ de degré strictement inférieur à n, ce qui se traduit par l'identité $f(q - q') = r' - r$. On remarquera que l'élément a étant inversible, ce n'est pas un diviseur de 0, ce qui amène, pour tout $h \in A[X]$, aux identités

$$\deg(fh) = \deg(f) + \deg(h).$$

Si les polynômes q et q' étaient distincts, on obtiendrait l'inégalité $\deg(q - q') \geq 0$, d'où les relations

$$\begin{aligned} n = \deg(f) \leq \deg(f) + \deg(q - q') = \deg(f(q - q')) = \\ = \deg(r' - r) \leq \max\{\deg(r), \deg(r')\} < n, \end{aligned}$$

ce qui est absurde. On a donc $q = q'$ et, par conséquent, $r = r'$. □