Chapitre 3

Idéaux

3.1 Idéaux d'un anneau commutatif

Définition 3.1.1 Un *idéal* d'un anneau commutatif A est un sous-groupe I de $(A,+)$ tel que de plus :

$$\forall x \in I\ ,\ \forall a \in A\ ,\ ax \in I \quad \text{(“stabilité externe”).}$$

Il revient au même de dire que I est non vide , stable pour l'addition et qu'il vérifie la condition de“stabilité externe” $\forall x \in I\ ,\ \forall a \in A\ ,\ ax \in I$.

Voici encore une autre caractérisation : I est non vide et *stable par combinaisons linéaires* :

$$\forall x_1,\ldots,x_n \in I\ ,\ \forall a_1,\ldots,a_n \in A\ ,\ a_1x_1+\cdots+a_nx_n \in I.$$

Tout anneau non trivial a au moins deux idéaux, l'idéal *trivial* $\{0\}$ et A lui-même. Les idéaux de A distincts de A sont dits *propres*.

Tout élément x de A permet de définir un *idéal principal* :

$$(x) := Ax :=< x >:= \{ax \mid a \in A\}.$$

C'est le plus petit idéal qui contient x, on dit qu'il est *engendré par* x. Si $x = 0$, c'est l'idéal trivial. Si x est inversible (et seulement dans ce cas), $Ax = A$. On voit donc que A est un corps si, et seulement s'il a exactement deux idéaux ($\{0\}$ et lui-même).

Plus généralement, si $x_1,\ldots,x_n \in A$, le plus petit idéal contenant $x_1,\ldots,x_n$ est :

$$(x_1,\ldots,x_n) := Ax_1+\cdots+Ax_n :=< x_1,\ldots,x_n >:= \{a_1x_1+\cdots+a_nx_n \mid a_1,\ldots,a_n \in A\}$$

En effet, on vérifie immédiatement que $I := Ax_1+\cdots+Ax_n$ est non vide et stable par combinaisons linéaires, donc est un idéal ; et bien entendu, tout idéal contenant les x_i doit contenir I. On dit que I est *engendré par* $x_1,\ldots,x_n$. Nous éviterons la notation (pourtant répandue) $(x_1,\ldots,x_n)$ à cause du risque de confusion avec un n-uplet.

Exercice 3.1.2 (Cours) Supposons A intègre. On a alors les équivalences :

$$(x) \subset (y) \Longleftrightarrow x \in (y) \Longleftrightarrow y|x. \quad \text{et} \quad (x) = (y) \Longleftrightarrow x \sim y \text{ (éléments associés).}$$

(Voir l'exercice 3.6.4 pour le cas d'un anneau non intègre.)

L'exercice ci-dessus indique un lien entre l'arithmétique dans A et les relations entre ses idéaux ; en voici une confirmation.

Proposition 3.1.3 *Supposons que l'idéal $Ax_1 + \cdots + Ax_n$ est principal :*

$$Ax_1 + \cdots + Ax_n = Ad, d \in A.$$

Alors d est un pgcd de $x_1, \ldots, x_n$ dans le sens fort suivant :

$$Div(d) = Div(x_1) \cap \cdots \cap Div(x_n).$$

Autrement dit, les diviseurs communs de tous les x_i sont exactement les diviseurs de d.

Preuve. - L'hypothèse $Ax_1 + \cdots + Ax_n = Ad$ équivaut à dire d'une part que chaque x_i est dans Ad, d'autre part que $d = a_1x_1 + \cdots + a_nx_n$ avec $a_1, \ldots, a_n \in A$. Puisque $x_i \in Ax_1 + \cdots + Ax_n = Ad$, on voit que $d|x_i$, donc que d est un diviseur commun de tous les x_i, d'où l'inclusion :

$$\mathrm{Div}(d) \subset \mathrm{Div}(x_1) \cap \cdots \cap \mathrm{Div}(x_n).$$

Réciproquement, si $y \in \mathrm{Div}(x_1) \cap \cdots \cap \mathrm{Div}(x_n)$, on peut écrire $x_i = yy_i$, $y_i \in A$, donc $d = a_1x_1 + \cdots + a_nx_n = y(a_1y_1 + \cdots + a_ny_n)$, *i.e.* y divise d. On a donc prouvé l'inclusion réciproque :

$$\mathrm{Div}(x_1) \cap \cdots \cap \mathrm{Div}(x_n) \subset \mathrm{Div}(d).$$

□

Exemples 3.1.4

1. Dans $\mathbf{Z}$, tout idéal est principal, puisque tout sous-groupe est monogène. On dit que $\mathbf{Z}$ est un *anneau principal* (on y reviendra aux chapitres 4 et 5).
2. Dans $K[X]$, tout idéal est principal. Soit en effet I un idéal non trivial de $K[X]$. (Si I est trivial, la conclusion l'est aussi !) Soit $P_0 \in I$ non nul de degré minimum. Nous allons voir que $I = (P_0)$. Puisque $P_0 \in I$, il est clair que $(P_0) \subset I$. Soit réciproquement $P \in I$. On effectue la division euclidienne $P = QP_0 + R$. Alors $R = P - QP_0 \in I$. Mais comme $\deg R < \deg P_0$, le choix de P_0 (minimalité du degré) entraîne que $R = 0$, donc $P = QP_0 \in (P_0)$.
3. Dans l'anneau $\mathcal{C}(\mathbf{R}, \mathbf{R})$ des fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$, l'ensemble $I := \{f \in \mathcal{C}(\mathbf{R}, \mathbf{R}) \mid f(0) = 0\}$ est visiblement un idéal qui n'est ni trivial ni égal à l'anneau.

3.2 Opérations sur les idéaux

3.2.1 Somme, intersection, produit d'idéaux

Soient I et J deux idéaux de A. Leur intersection $I \cap J$ est évidemment un idéal. Il en est de même de leur *somme* :

$$I + J := \{x + y \mid x \in I, y \in J\}.$$

Il est clair que $I + J$ contient I et J. Réciproquement, il est immédiat que tout idéal contenant I et J contient $I + J$, qui est donc le plus petit idéal contenant I et J.

Exercice 3.2.1 (Cours) Soient $m, n \in \mathbf{N}^*$ et soit $e \in \mathbf{N}^*$ tel que $(m) \cap (n) = (e)$. Quel est le nom de e en arithmétique ? Soit $d \in \mathbf{N}^*$ tel que $(m) + (n) = (d)$. Quel est le nom de d en arithmétique ?

Plus généralement, si $I_1, \ldots, I_n$ sont des idéaux de A, il en est de même de leur intersection $I_1 \cap \cdots \cap I_n$ et de leur somme :

$$I_1 + \cdots + I_n := \{x_1 + \cdots + x_n \mid x_1 \in I_1, \ldots, x_n \in I_n\}.$$

L'idéal $I_1 + \cdots + I_n$ contient $I_1, \ldots, I_n$ et c'est le plus petit idéal qui les contient tous. Plus généralement encore, soit $(I_i)_{i \in X}$ une famille d'idéaux indexée par un ensemble arbitraire X. Alors $\bigcap_{i \in X} I_i$ est un idéal. Le plus petit idéal qui contient tous les I_i est leur *somme* :

$$\sum_{i \in X} I_i := \left\{ \sum_{i \in X} x_i \mid \forall i \in X \ , \ x_i \in I_i \text{ et presque tous les } x_i \text{ sont nuls} \right\}.$$

3.2.2 Idéal de A engendré par une partie ou une famille

L'intersection de tous les idéaux qui contiennent un sous-ensemble donné E de A est un idéal ; c'est donc le plus petit idéal contenant E : on dit qu'il est *engendré par* E. Pour le décrire, il ext plus facile de considérer les éléments de E comme les termes d'une famille, *i.e.* écrire $E = \{x_i \mid i \in X\}$. L'*idéal engendré par* E, ou *engendré par la famille* $(x_i)_{i \in X}$ est alors :

$$< E >:=< (x_i)_{i \in X} >:= \left\{ \sum_{i \in X} a_i x_i \mid \forall i \in X \ , \ a_i \in A \text{ et presque tous les } a_i \text{ sont nuls} \right\}.$$

Si E est fini, on retrouve les notations vues à la section précédente.

Remarque 3.2.2 Il faut bien distinguer les notions de sous-anneau engendré par E et d'idéal engendré par E. Dans le premier cas, on forme toutes les combinaisons linéaires $\sum_{i \in X} m_i x_i$ où $m_i \in \mathbf{Z}$ et les x_i sont des produits d'éléments de E ; dans le deuxième cas, on forme toutes les combinaisons linéaires $\sum_{i \in X} a_i x_i$ à coefficients $a_i \in A$ et où les x_i sont dans E. Par exemple, dans l'anneau $\mathbf{Q}[X]$, le sous-anneau engendré par X est $\mathbf{Z}[X]$ (polynômes à coefficients entiers) alors que l'idéal engendré par X est $X\mathbf{Q}[X]$ (polynômes à coefficients rationnels sans terme constant).

Exercice 3.2.3 (Cours) Reconnaître l'idéal engendré par $I \cup J$.

Un cas intéressant est celui de l'idéal engendré par $\{xy \mid x \in I \ , \ y \in J\}$. Cet idéal est appelé *produit* de I et J et noté IJ. Puisque $x \in I, y \in J \Rightarrow xy \in I \cap J$, il est clair que $IJ \subset I \cap J$. Naturellement, on peut définir un produit fini d'idéaux $I_1 \cdots I_n$, et même des puissances I^n (par convention, $I^0 = A$ et $I^1 = I$) ; mais on ne peut pas définir le produit d'une infinité d'idéaux.

Exemples 3.2.4

1. Dans tout anneau A, le produit des deux idéaux principaux (a) et (b) est l'idéal principal (ab). Le produit des idéaux $< a, b >$ et $< c, d >$ est $< ac, ad, bc, bd >$.
2. Dans l'anneau $K[X,Y]$, les puissances de l'idéal $I :=< X, Y >$ sont $I^2 =< X^2, XY, YX, Y^2 >=< X^2, XY, Y^2 >$, $I^3 =< X^3, X^2Y, XY^2, Y^3 >$, etc.

Exercice 3.2.5 (Cours) Quel est le produit des idéaux $< x_1, \ldots, x_n >$ et $< y_1, \ldots, y_p >$?

De manière générale, une réunion d'idéaux n'est pas un idéal. Par exemple, si I et J sont des idéaux, pour que $I \cup J$ soit un idéal, il faut, et il suffit, que $I \subset J$ ou $J \subset I$ (exercice : démontrez-le).

Cependant, le lemme sans mystère qui suit, assorti d'un principe lui très mystérieux, nous permettra à la section 3.4 de prouver un résultat important, le théorème de Krull.

Lemme 3.2.6 *Soit $(I_i)_{i\in X}$ une famille d'idéaux de A. On suppose que cette famille est "filtrante croissante" pour l'inclusion, autrement dit : $\forall i,j \in X\ ,\ \exists k \in X\ :\ I_i, I_j \subset I_k$. Alors $\bigcup_{i\in X} I_i$ est un idéal de A.*

Preuve. - La "stabilité externe" est immédiate et d'ailleurs vraie pour toute réunion d'idéaux, sans condition particulière sur l'ordre. Soient $x,y \in \bigcup_{i\in X} I_i$. Il existe des indices i,j tels que $x \in I_i$ et $y \in I_j$. La famille étant filtrante, il existe un indice k tel que $I_i, I_j \subset I_k$, donc $x,y \in I_k$, donc $x+y \in I_k$, donc $x+y \in \bigcup_{i\in X} I_i$. □

3.3 Anneaux quotients

3.3.1 Révision sur les quotients de groupes abéliens

Rappelons d'abord la définition d'un groupe quotient G/H dans le cas le plus facile, celui d'un groupe abélien G et d'un sous-groupe (nécessairement distingué !) H. On définit sur G la relation de congruence modulo H :

$$\forall x,x' \in G\ ,\ x \equiv x' \pmod{H} \underset{def}{\Longleftrightarrow} x - x' \in H.$$

C'est une relation d'équivalence compatible avec l'addition :

$$\forall x,y,x',y' \in G\ ,\ x \equiv x' \pmod{H} \text{ et } y \equiv y' \pmod{H} \Longrightarrow x+y \equiv x'+y' \pmod{H}.$$

Si l'on note $\overline{x} \in G/H$ la classe d'équivalence de $x \in G$, cette propriété se traduit ainsi :

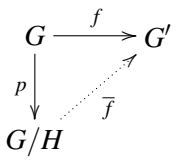
$$\forall x,y,x',y' \in G\ ,\ \overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{y'} \Longrightarrow \overline{x+y} = \overline{x'+y'}.$$

On en déduit que la définition suivante a un sens :

$$\forall x,y \in G\ ,\ \overline{x} + \overline{y} := \overline{x+y}.$$

(Réfléchissez bien : pourquoi tant de préliminaires pour donner un sens à cette définition ?)

On peut alors démontrer les faits suivants : la loi de composition interne ainsi définie sur G/H en fait un groupe commutatif ; la projection canonique $p : x \mapsto \overline{x}$ est un morphisme surjectif du groupe G sur le groupe G/H, son noyau est H ; pour tout morphisme de groupes $f : G \to G'$ tel que $H \subset \mathrm{Ker} f$, il existe un unique morphisme $\overline{f} : G/H \to G'$ défini par la formule $\overline{f}(\overline{x}) := f(x)$ (cette "définition" est elle cohérente ?), *i.e.* tel que $f = \overline{f} \circ p$. Il est classique de représenter ce "théorème de factorisation" par un *diagramme commutatif* :



La représentation de la flèche $\overline{f}$ en pointillés rappelle que ce n'est qu'une donnée déduite de p et f.

Exercice 3.3.1 Démontrer que l'application $\overline{f} \mapsto \overline{f} \circ p$ de $\mathrm{Hom}(G/H, G')$ dans $\mathrm{Hom}(G, G')$ est bijective.

Théorème 3.3.2 (Premier théorème d'isomorphisme) *Soit $f : G \to G'$ un morphisme de groupes abéliens. Le noyau $Kerf$ est un sous-groupe de G, son image Imf est un sous-groupe de G' et l'on obtient par passage au quotient un isomorphisme $\overline{f} : G/Kerf \to Imf$, d'où le diagramme commutatif*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/Kerf & \xrightarrow[\overline{f}]{} & Imf \end{array}$$

dans lequel i désigne l'inclusion de Imf dans G'.

□

Nous laissons au lecteur le soin de formuler les divers corollaires qui vont maintenant être transposés au cas des anneaux.

3.3.2 Quotient d'un anneau commutatif par un idéal

Soit I un idéal de A, donc en particulier un sous-groupe de $(A, +)$. Nous voulons définir sur le groupe quotient A/I une multiplication qui en fasse un anneau.

Lemme 3.3.3 *(i) La relation de congruence modulo I est compatible avec la multiplication :*

$$\forall x, y, x', y' \in A \ , \ x \equiv x' \pmod{I} \text{ et } y \equiv y' \pmod{I} \Longrightarrow xy \equiv x'y' \pmod{I}.$$

Preuve. - Il suffit d'écrire que, si $x - x' \in I$ et $y - y' \in I$, alors $xy - x'y' = x(y - y') + (x - x')y' \in I$. □

On traduit cette propriété comme suit :

$$\forall x, y, x', y' \in A \ , \ \overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{y'} \Longrightarrow \overline{xy} = \overline{x'y'}.$$

On en déduit que la définition suivante a un sens :

$$\forall x, y \in A \ , \ \overline{xy} := \overline{xy}.$$

Théorème 3.3.4 *(i) La multiplication ainsi définie fait de $(A/I, +, \times)$ un anneau commutatif.*
(ii) La projection canonique $p : x \mapsto \overline{x}$ est un morphisme surjectif de l'anneau A sur l'anneau A/I, son noyau est I.
(iii) Pour tout morphisme d'anneaux $f : A \to A'$ tel que $I \subset Kerf$, il existe un unique morphisme $\overline{f} : A/I \to A'$ défini par la formule $\overline{f}(\overline{x}) := f(x)$ et l'on a un diagramme commutatif :

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{f}} & \\ A/I & & \end{array}$$

Preuve. - (i) Seules les propriétés relatives à la multiplication (distributivité, associativité, élément neutre $\overline{1_A}$) doivent être vérifiées ; toutes découlent immédiatement des propriétés analogues dans A, de la surjectivité de l'application $x \mapsto \bar{x}$, et des formules $\bar{x}+\bar{y} := \overline{x+y}$ et $\overline{xy} := \overline{xy}$.
(ii) Puisque p est un morphisme de groupes, cela découle immédiatement de la formule $\overline{xy} := \overline{xy}$ et du fait que $\overline{1_A}$ est l'élément neutre de la multiplication.
(iii) Puisque $\overline{f}$ est un morphisme de groupes, il suffit de vérifier les propriétés relatives à la multiplication : on utilise encore les arguments ci-dessus (les détails sont laissés au lecteur). □

Exemples 3.3.5 1. Le quotient $\mathbf{Z}/m\mathbf{Z}$ est l'anneau bien connu des classes de congruence.

2. Notons i la classe de X dans l'anneau quotient $L := K[X]/ < X^2+1 >$, où K désigne un corps commutatif. Le morphisme $K[X] \to K[X]/ < X^2+1 >$ se restreint en un morphisme $K \to K[X]/ < X^2+1 >$ qui est nécessairement injectif puisque K est un corps. On identifiera K à son image, ce qui revient à dire que l'on identifiera $a \in K$ à $\bar{a} \in L$.
   Pour tout $P \in K[X]$, la division euclidienne $P = (X^2+1)Q+R$ admet un reste de la forme $R = a+bX$, $a,b \in K$. Puisque $P-R \in < X^2+1 >$, on a $\overline{P} = \overline{R} = \bar{a}+\overline{b}\overline{X} = a+b\mathrm{i}$, vues les identifications de $\bar{a},\overline{b}$ avec a,b. Finalement on voit que L est l'ensemble des $a+b\mathrm{i}$, $a,b \in K$, muni des lois :

   $$(a+b\mathrm{i})+(a'+b'\mathrm{i}) = (a+a')+(b+b')\mathrm{i} \text{ et } (a+b\mathrm{i})(a'+b'\mathrm{i}) = (aa'-bb')+(ab'+a'b)\mathrm{i}.$$

   Pour justifier la dernière formule, on remarque que le reste de la division euclidienne de $(a+bX)(a'+b'X)$ par X^2+1 est $(aa'-bb')+(ab'+a'b)X$ (ce que le lecteur consciencieux vérifiera !) Lorsque $K = \mathbf{R}$, on reconnaît $L = \mathbf{C}$.

3. Soit plus généralement $F(X) := X^n + p_1X^{n-1} + \cdots + p_n \in K[X]$. Dans l'anneau quotient $L := K[X]/ < F >$, notons x la classe de X. Comme ci-dessus, on voit que K s'identifie à son image dans L. Pour tout $P \in K[X]$, la division euclidienne $P = QF+R$ donne un reste de degré $\deg R \leq n-1$. On en déduit que les éléments de L sont les combinaisons linéaires $a_0+\cdots+a_{n-1}x^{n-1}$, l'addition de L étant définie de manière évidente :

   $$(a_0+\cdots+a_{n-1}x^{n-1})+(b_0+\cdots+b_{n-1}x^{n-1}) = (a_0+b_0)+\cdots+(a_{n-1}+b_{n-1})x^{n-1}.$$

   La multiplication est un tout petit peu plus compliquée :

   $$(a_0+\cdots+a_{n-1}x^{n-1})(b_0+\cdots+b_{n-1}x^{n-1}) = c_0+\cdots+c_{n-1}x^{n-1},$$

   où le reste de la division euclidienne de $(a_0+\cdots+a_{n-1}X^{n-1})(b_0+\cdots+b_{n-1}X^{n-1})$ par F est $c_0+\cdots+c_{n-1}X^{n-1}$. (Cet exemple sera repris plus rigoureusement à la section 3.4.)

4. Si par exemple $F = X^2$ et si l'on note $\varepsilon := \overline{X}$, on voit que L est l'ensemble des $a+b\varepsilon$, $a,b \in K$, avec l'addition évidente et la multiplication telle que $\varepsilon^2 = 0$ ("nombre duaux").

Théorème 3.3.6 (Premier théorème d'isomorphisme) *Soient $f : A \to A'$ un morphisme d'anneaux Le noyau $Kerf$ est un idéal de A, son image Imf est un sous-anneau de A' et l'on obtient par passage au quotient un isomorphisme $\overline{f} : A/Kerf \to Imf$, d'où le diagramme commutatif*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & A' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/Kerf & \xrightarrow[\ \overline{f}\ ]{} & Imf \end{array}$$

dans lequel i désigne l'inclusion de Imf dans A'.

Preuve. - Encore une fois, seules les propriétés relatives à la multiplication restent à démontrer. Nous prouverons simplement que Ker$f$ est un idéal de A, et Imf un sous-anneau de A', le reste étant laissé au lecteur. On sait déjà que ce sont des sous-groupes. Si $x \in \mathrm{Ker}f$ et $a \in A$, on écrit :

$$f(ax) = f(a)f(x) = f(a)0_{A'} = 0_{A'} \Longrightarrow ax \in \mathrm{Ker}f.$$

Si $y, y' \in \mathrm{Im}f$, on écrit $y = f(x)$, $y' = f(x')$, d'où :

$$yy' = f(x)f(x') = f(xx') \in \mathrm{Im}f.$$

Enfin, par définition d'un morphisme d'anneaux, $1_{A'} = f(1_A) \in \mathrm{Im}f$. □

Exemple 3.3.7 Soit $f : P \mapsto P(\mathrm{i})$ l'unique morphisme de $\mathbf{Z}[X]$ dans $\mathbf{C}$ tel que $X \mapsto \mathrm{i}$. Puisque $\mathrm{i}^{2p} = (-1)^p \in \mathbf{Z}$ et que $\mathrm{i}^{2p+1} = (-1)^p\mathrm{i} \in \mathbf{Z}\mathrm{i}$ son image est le sous-anneau

$$\mathbf{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbf{Z}\}$$

de $\mathbf{C}$: c'est l'*anneau des entiers de Gauß*. Son noyau contient le polynôme $F := X^2 + 1$, donc l'idéal $< F > \subset \mathbf{Z}[\mathrm{i}]$. En fait, ce noyau est égal à $< F >$. En effet, pour tout $P \in \mathbf{Z}[X]$, la division euclidienne $P = QF + R$ est telle que $Q, R \in \mathbf{Z}[X]$ et $\deg R < 2$. Si P est dans le noyau, c'est-à-dire si $P(\mathrm{i}) = 0$, on a $R(\mathrm{i}) = 0$, donc $R = 0$, et l'on voit que $P \in < F >$. Du premier théorème d'isomorphisme on déduit donc l'isomorphisme d'anneaux :

$$\mathbf{Z}[\mathrm{i}] \simeq \mathbf{Z}[X]/ < X^2 + 1 > .$$

Exercice 3.3.8 (Cours) Démontrer les deux affirmations non triviales de l'exemple ci-dessus : $Q, R \in \mathbf{Z}[X]$ et $R(\mathrm{i}) = 0 \Rightarrow R = 0$.

Les deux énoncés qui suivent sont essentiellement les transpositions au cas des anneaux des énoncés correspondants pour les groupes abéliens. Ils se prouvent directement en appliquant le premier théorème d'isomorphisme.

Corollaire 3.3.9 (Deuxième théorème d'isomorphisme) *(i) Les idéaux de A/I sont les J/I, où J est un idéal de A tel que $I \subset J_s ubset A$.*
(ii) Le morphisme $A/I \to A/J$ est surjectif de noyau J/I, il induit un isomorphisme :

$$(A/I)/(J/I) \simeq A/J.$$

Exemples 3.3.10

1. Les idéaux de l'anneau $\mathbf{Z}/m\mathbf{Z}$ sont les $n\mathbf{Z}/m\mathbf{Z}$ tels que $n|m$. Le quotient de l'anneau $\mathbf{Z}/m\mathbf{Z}$ par l'idéal $n\mathbf{Z}/m\mathbf{Z}$ s'identifie à l'anneau $\mathbf{Z}/n\mathbf{Z}$. En particulier, si p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps ; et réciproquement.
2. Les idéaux de l'anneau $K[X]/ < P >$ sont les $< Q > / < P >$ tels que $Q|P$. Ainsi, si P est irréductible, $K[X]/ < P >$ n'a donc pour idéaux que $\{0\}$ et lui-même, c'est donc un corps. Réciproquement, si $K[X]/ < P >$ est un corps, P est irréductible.
3. Les idéaux de l'anneau $K[X]/ < X^2 >$ des nombres duaux sont $< X^2 > / < X^2 >= \{0\}$, $< X > / < X^2 >=< \varepsilon >$ et $K[X]/ < X^2 >$.

Corollaire 3.3.11 *(i) Soient I,J deux idéaux de A. L'image de $\overline{J}$ de J dans $\overline{A} := A/I$ est égale à $(I+J)/I$. C'est un idéal de $\overline{A}$.*
(ii) Le noyau du morphisme composé $A \to \overline{A} \to \overline{A}/\overline{J}$ est $I+J$, d'où un isomorphisme :

$$A/(I+J) \simeq \overline{A}/\overline{J}.$$

Autrement dit : quotienter succesivement par I puis par (l'image de) J revient à quotienter par $I+J$.

Exemple 3.3.12 Soient $m,n \in \mathbf{N}^*$ et soit d leur pgcd. On sait (depuis quand ?) que $m\mathbf{Z}+n\mathbf{Z} = d\mathbf{Z}$. Si l'on note $\overline{m}$ l'image de m dans $\overline{\mathbf{Z}} := \mathbf{Z}/n\mathbf{Z}$, on a donc $< \overline{m} >= d\mathbf{Z}/n\mathbf{Z}$ et $\overline{\mathbf{Z}}/ < \overline{m} > \simeq \mathbf{Z}/d\mathbf{Z}$.

3.3.3 Le lemme chinois

La forme historique du lemme chinois (ou théorème des restes chinois) est la suivante. Soient $m,n \in \mathbf{N}^*$ premiers entre eux (les "modules") ; soient $a,b \in \mathbf{Z}$ arbitraires (les "restes"). Alors on peut résoudre le système de congruences suivant :

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}. \end{cases}$$

De plus, si x_0 est une solution particulière de ce système, les solutions sont exactement les $x \equiv x_0 \pmod{mn}$.

Exercice 3.3.13 (Cours) Prouver la deuxième assertion.

La forme classique du lemme chinois est la suivante. On suppose encore donnés $m,n \in \mathbf{N}^*$ premiers entre eux. Alors l'application $x \pmod{mn} \mapsto (x \pmod{m}, x \pmod{n})$ est un isomorphisme de $\mathbf{Z}/mn\mathbf{Z}$ sur l'anneau produit $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$. En voici une preuve directe.
Le morphisme $x \mapsto (x \pmod{m}, x \pmod{n})$ de $\mathbf{Z}$ dans l'anneau produit $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ a pour noyau $m\mathbf{Z} \cap n\mathbf{Z}$, c'est-à-dire l'ensemble des multiples communs à m et n. Puisque m et n sont premiers entre eux, cet ensemble est $mn\mathbf{Z}$ (*i.e.* le "ppcm" de m et n est mn : cela découle facilement du théorème de Bézout). Le premier théorème d'isomorphisme permet de conclure que l'application $x \pmod{mn} \mapsto (x \pmod{m}, x \pmod{n})$ est un morphisme injectif de $\mathbf{Z}/mn\mathbf{Z}$ dans l'anneau produit $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$. Mais ces deux anneaux ont même nombre mn d'éléments, le morphisme est donc bijectif.

Exercice 3.3.14 (Cours) Prouver que $m\mathbf{Z} \cap n\mathbf{Z} = mn\mathbf{Z}$.

Nous reviendrons à ce théorème très utile au chapitre 4, mais nous allons en donner ici une version considérablement généralisée, et qui sert non seulement en arithmétique mais également en géométrie algébrique.

Définition 3.3.15 Deux idéaux I,J de A sont dits *étrangers* (l'un à l'autre) si $I+J = A$, autrement dit, s'il existe $x \in I$ et $y \in J$ tels que $x+y = 1$.

Avant d'énoncer et de démontrer la forme généralisée du lemme chinois, collectons quelques faits utiles :

1. Si I et J sont étrangers, alors $IJ = I \cap J$. En effet, si $x \in I$ et $y \in J$ sont tels que $x+y=1$ et si $z \in I \cap J$, alors $z = zx+zy \in IJ$.
2. Si de plus I et J' sont étrangers, alors I et JJ' sont étrangers. En effet, si $x \in I$ et $y \in J$ sont tels que $x+y=1$ et si $x' \in I'$ et $y' \in J'$ sont tels que $x'+y'=1$, alors $1 = (x+y)(x'+y') = (xx'+xy'+x'y)+yy'$, or $xx'+xy'+x'y \in I$ et $yy' \in JJ'$.
3. Si I et J sont étrangers, alors I^m et J^n sont étrangers pour tous $m,n \in \mathbf{N}^*$. Cela découle par récurrence du fait précédent.

Théorème 3.3.16 (Lemme chinois) *Soient I,J deux idéaux de A étrangers entre eux. Alors l'application $x \pmod{IJ} \mapsto (x \pmod{I}, x \pmod{J})$ est un isomorphisme de A/IJ sur l'anneau produit $(A/I) \times (A/J)$.*

Preuve. - L'application $x \mapsto (x \pmod{I}, x \pmod{J})$ est un morphisme de A sur l'anneau produit $(A/I) \times (A/J)$, et son noyau est $I \cap J = IJ$. Par le premier théorème d'isomorphisme, on obtient un morphisme injectif de A/IJ dans $(A/I) \times (A/J)$.
Pour montrer la surjectivité, il suffit de vérifier le fait suivant : pour tous $a,b \in A$, il existe $c \in A$ tel que $c \equiv a \pmod{I}$ et $c \equiv b \pmod{J}$. En effet, $c \pmod{IJ}$ sera alors un antécédent de $(a \pmod{I}, b \pmod{J})$. On utilise $x \in I$, $y \in J$ tels que $x+y=1$ et l'on pose $c := bx+ay$, puis on calcule :

$$c-a = bx+ay-a = bx+a(y-1) = (b-a)x \in I,$$

et de même $c-b \in J$. □

Corollaire 3.3.17 *Soient $I_1,\dots,I_n$ des idéaux étrangers deux à deux. Alors $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ et l'on a un isomorphisme :*

$$A/(I_1 \cap \cdots \cap I_n) = A/(I_1 \cdots I_n) \simeq (A/I_1) \times \cdots \times (A/I_n).$$

Preuve. - D'après les faits précédents, I_n est étranger à $I_1 \cdots I_{n-1}$, et l'on conclut par récurrence. □

Corollaire 3.3.18 *(i) Soient K un corps commutatif et $a_1,\dots,a_n$ des éléments distincts de K. Alors tout polynôme nul en $a_1,\dots,a_n$ est divisible par $(X-a_1)\cdots(X-a_n)$.*
(ii) Un polynôme $P \in K[X]$ de degré $d \geq 0$ admet au plus d racines.

Preuve. - (i) Soit $I_i := X-a_i$. Pour $i \neq j$, l'idéal I_i+I_j contient $(X-a_i)-(X-a_j) = a_j-a_i$, qui est inversible dans $K[X]$ (constante non nulle) ; donc $I_i+I_j = K[X]$, *i.e.* les idéaux I_i sont deux à deux étrangers. On applique alors l'égalité $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.
(ii) Si $a_1,\dots,a_n$ sont racines de P, on écrit $P = (X-a_1)\cdots(X-a_n)Q$, d'où $d = n+\deg Q \geq d$ car $P,Q \neq 0$. □

Exercice 3.3.19 Résoudre le système de congruences suivant : $\begin{cases} x \equiv 3 \pmod{7}, \\ x \equiv 8 \pmod{12}, \\ x \equiv 12 \pmod{25}. \end{cases}$.

3.4 Idéaux maximaux

3.4.1 Idéaux maximaux d'un anneau commutatif

Proposition 3.4.1 *Soit $\mathfrak{M}$ un idéal de A. Les propriétés suivantes sont équivalentes :*
(i) L'anneau quotient $A/\mathfrak{M}$ est un corps.
(ii) L'idéal $\mathfrak{M}$ est maximal parmi les idéaux propres de A ; autrement dit, $\mathfrak{M}$ est propre et tout idéal qui contient $\mathfrak{M}$ est égal à $\mathfrak{M}$ ou à A.

Preuve. - La deuxième condition revient à dire que $A/\mathfrak{M}$ a exactement deux idéaux, et nous savons que cela caractérise les corps. □

Définition 3.4.2 Un idéal vérifiant ces conditions est dit *maximal* (autrement dit, il est maximal parmi les idéaux propres, mais on ne précise pas "propre").

Exemples 3.4.3
1. L'anneau A est un corps si, et seulement si, $\{0\}$ est maximal.
2. Les idéaux maximaux de $\mathbf{Z}$ sont les $p\mathbf{Z}$, où p est premier.
3. Les idéaux maximaux de $K[X]$ sont les $< P >$, où P est irréductible.
4. L'idéal $I := \{f \in \mathcal{C}(\mathbf{R},\mathbf{R}) \mid f(0) = 0\}$ de $\mathcal{C}(\mathbf{R},\mathbf{R})$ est maximal. Soit en effet un idéal J contenant strictement I et soit $g \in J \setminus I$: on a donc $g(0) \neq 0$. La fonction $g - g(0)$ est nulle en 0, donc $g - g(0) \in I$, donc $g - g(0) \in J$. La fonction constante non nulle $g(0) = g - (g - g(0))$ est donc élément de J. Comme c'est un élément inversible de $\mathcal{C}(\mathbf{R},\mathbf{R})$, on en déduit que $J = \mathcal{C}(\mathbf{R},\mathbf{R})$.

Voici un moyen commode pour démontrer qu'un idéal est maximal. Soit $\phi : A \to K$ un morphisme surjectif, K étant un corps. Alors Ker ϕ est maximal. En effet, du premier théorème d'isomorphisme on déduit que $A/\text{Ker}\,\phi$ est isomorphe à K, donc est un corps. En fait, tout idéal maximal peut s'obtenir ainsi (prendre pour ϕ la projection canonique $A \to A/\mathfrak{M}$).

Exemples 3.4.4
1. Soient $A := \mathcal{C}(\mathbf{R},\mathbf{R})$ et $\phi : f \mapsto f(0)$: on voit à nouveau que l'idéal des fonctions nulles en 0 est maximal.
2. Soient de même $A := K[X,Y]$ et $\phi : P \mapsto P(0)$. Les éléments du noyau de ϕ sont les polynômes sans terme constant, ils forment l'idéal $< X,Y >$ qui est donc maximal.

Exercice 3.4.5 Soit $(a_1,\ldots,a_n) \in K^n$. Démontrer que le noyau du morphisme $P \mapsto P(a_1,\ldots,a_n)$ de $K[X_1,\ldots,X_n]$ sur K est l'idéal $< X_1 - a_1,\ldots,X_n - a_n >$ de $K[X_1,\ldots,X_n]$, et en déduire que cet idéal est maximal.

Soient $\mathfrak{M}$ et $\mathfrak{M}'$ deux idéaux propres maximaux distincts de A. Alors ils sont étrangers. En effet, si l'idéal $\mathfrak{M} + \mathfrak{M}'$ n'était pas égal à A, par maximalité, il serait à la fois égal à $\mathfrak{M}$ et à $\mathfrak{M}'$. On peut appliquer le lemme chinois (avec puissances) :

Corollaire 3.4.6 *Soient $\mathfrak{M}_1,\ldots,\mathfrak{M}_n$ des idéaux propres maximaux distincts de A. Soient $k_1,\ldots,k_n$ des entiers naturels. On a alors un isomorphisme :*

$$A/(\mathfrak{M}_1^{k_1}\cdots\mathfrak{M}_n^{k_n}) \simeq (A/\mathfrak{M}_1^{k_1}) \times \cdots \times (A/\mathfrak{M}_n^{k_n}).$$

3.4.2 Le théorème de Krull

Le théorème de Krull dit que dans un anneau non trivial, tout idéal propre est inclus dans un idéal maximal. Ce résultat est important, mais le lecteur peut en admettre la démonstration s'il le désire.

Théorème 3.4.7 (Krull) *Soient A un anneau commutatif non trivial et I un idéal propre de A (propre signifie que l'inclusion $I \subset A$ est stricte). Il existe alors un idéal maximal contenant I.*

Preuve. - Pour démontrer ce théorème, on va faire appel à un peu de magie noire, sous la forme du *lemme de Zorn*. Celui-ci est issu de la théorie des ensembles. Il concerne un ensemble ordonné $(E, \prec)$. Ce dernier est supposé *inductif*, ce qui signifie que toute famille totalement ordonnée de E (toute *chaîne*) est majorée. La conclusion est alors que tout élément de E est majoré par un élément maximal (c'est-à-dire un élément qui n'est pas strictement majoré).
Pour appliquer le lemme de Zorn à notre situation, nous allons montrer que l'ensemble des idéaux propres de A, ordonné par inclusion, est inductif. Avec le lemme précédent c'est très facile : si $(I_i)_{i\in X}$ est une chaîne d'idéaux propres de A, c'est en particulier une famille filtrante croissante (immédiat !) donc $\bigcup_{i\in X} I_i$ est un idéal de A. De plus, cet idéal est propre : sinon, on il contiendrait 1, donc l'un des idéaux I_i contiendrait 1, contradiction puisque ces idéaux sont supposés propres. L'idéal propre $\bigcup_{i\in X} I_i$ majore donc tous les éléments de la chaîne, et l'ensemble indiqué est bien inductif.
Le lemme de Zorn affirme donc que tout idéal propre est inclus dans un idéal propre maximal, ce qui est exactement la conclusion souhaitée. □

De manière générale, il s'agit d'un théorème "platonique" car il ne donne aucune indication sur la manière de produire de tels idéaux maximaux. Dans la pratique, pour la plupart des anneaux connus, on dispose d'algorithmes permettant de construire de tels idéaux.

Exemples 3.4.8

1. Dans $\mathbf{Z}$, les idéaux propres sont les $a\mathbf{Z}$, $a \geq 2$; et les idéaux maximaux sont les $p\mathbf{Z}$, p premier. Le théorème de Krull exprime simplement le fait que tout entier $a \geq 2$ est divisible par un nombre premier.
2. Dans $\mathbf{C}[X]$, les idéaux propres sont les (P), $\deg P \geq 1$; et les idéaux maximaux sont les $(X-a)$, $a \in \mathbf{C}$. Le théorème de Krull exprime simplement le fait que tout polynôme non constant admet une racine.
3. Dans $\mathbf{C}[X,Y]$, nous démontrerons à la section 3.4 que les idéaux $< X-a, Y-b >$, $a,b \in \mathbf{C}$, sont maximaux ; et, au chapitre 6, que ce sont les seuls. On voit donc que, si I est un idéal propre de $\mathbf{C}[X,Y]$, il existe $(a,b) \in \mathbf{C}^2$ tel que $P(a,b) = 0$ pour tout $P \in I$. C'est un cas particulier du *nullstellensatz*, ou *théorème des zéros* de Hilbert, qui est très utile en géométrie algébrique (voir le cours de M1).

3.4.3 Une application à la théorie des corps

Un résultat de base de la théorie des corps est le suivant. Soit K un corps qui n'est pas algébriquement clos (par exemple $\mathbf{Q}$ ou $\mathbf{R}$) et soit $a_0 + \cdots + a_n x^n = 0$, $n \geq 1$, $a_0, \ldots, a_n \in K$, $a_n \neq 0$, une équation algébrique qui n'admet pas de racine dans K. Alors on peut "adjoindre une racine à K", ce qui signifie : construire un corps L dont K est un sous-corps et tel que l'équation ait une racine dans L. Un tel corps s'appelle "corps de rupture du polynôme $a_0 + \cdots + a_n X^n$.

La motivation la plus ancienne [1] pour une telle construction est apparemment l'usage de l'imaginaire i pour résoudre des équations réelles du troisième degré, et cela bien longtemps avant qu'on ait donné un sens et un nom aux nombres complexes. Même pour construire des racines *réelles* d'une telle équation, on est parfois obligé de passer par les nombres complexes (voir à ce sujet les "formules de Cardan" dans RW1).

La méthode est la suivante. On choisit un facteur irréductible P du polynôme $a_0 + \cdots + a_n X^n$. On pose $L := K[X]/ < P >$, qui est un corps. Le morphisme d'anneaux composé $K \to K[X] \to K[X]/ < P >= L$ est injectif (puisque sa source est un corps), ce qui permet d'identifier K à un sous-corps de L. Si l'on note x la classe de $X \in K[X]$ dans $L = K[X]/ < P >$, on voit alors que $P(x) = 0$, donc, *a fortiori*, $a_0 + \cdots + a_n x^n = 0$ *i.e.* l'équation a bien une racine dans L.

Il est facile de voir que L est engendré par K et x. On a même mieux : les éléments $1, x, \ldots, x^{d-1}$, où $d := \deg P$, forment une base du K-espace vectoriel L. En effet, le théorème de division euclidienne nous dit que le K-espace vectoriel $K[X]$ est la somme directe du sous-espace vectoriel $K[X]_{d-1}$ des polynômes de degré $\leq d-1$ (les restes R) et de l'idéal $< P >$ (les QP, Q quotient). On a donc un isomorphisme d'espaces vectoriels de $K[X]/ < P >$ sur $K[X]_{d-1}$.

On a donc une description concrète de L : ses éléments sont les expressions $a_0 + \cdots + a_{d-1} x^{d-1}$, $a_0, \ldots, a_{d-1} \in K$. L'addition se fait de façon évidente. Le produit de $a_0 + \cdots + a_{d-1} x^{d-1}$ par $b_0 + \cdots + b_{d-1} x^{d-1}$ est $c_0 + \cdots + c_{d-1} x^{d-1}$, où $c_0 + \cdots + c_{d-1} X^{d-1}$ est le reste de la division de $(a_0 + \cdots + a_{d-1} X^{d-1})(b_0 + \cdots + b_{d-1} X^{d-1})$ par P.

Exemple 3.4.9 Supposons que D n'est pas un carré dans K. Alors $P := X^2 - D$ est irréductible. Le corps $L := K[X]/ < P >$ est formé des éléments $a + bx$ avec la loi d'addition évidente et la loi de multiplication :

$$(a + bx)(a' + b'x) = (aa' + bb'D) + (ab' + ba')x.$$

En effet, la division euclidienne de $(a + bX)(a' + b'X)$ par $X^2 - D$ est la suivante :

$$aa' + bb' + (ab' + ba')X + bb'X^2 = bb'(X^2 - D) + \big((aa' + bb'D) + (ab' + ba')x\big).$$

3.5 Idéaux premiers

3.5.1 Idéaux premiers d'un anneau commutatif

Proposition 3.5.1 *Soit $\mathfrak{P}$ un idéal de A. Les conditions suivantes sont équivalentes :*
(i) L'anneau quotient $A/\mathfrak{P}$ est intègre.
(ii) L'idéal $\mathfrak{P}$ est propre et l'on a l'implication :

$$\forall x, y \in A \ , \ xy \in \mathfrak{P} \Longrightarrow (x \in \mathfrak{P} \text{ ou } y \in \mathfrak{P}).$$

Preuve. - Rappelons que, par définition, un anneau intègre est non trivial : et bien entendu, $A/\mathfrak{P}$ est non trivial si, et seulement si l'idéal $\mathfrak{P}$ est propre. L'autre condition pour l'intégrité de $A/\mathfrak{P}$ est la suivante :

$$\forall u, v \in A/\mathfrak{P} \ , \ uv = 0 \Longrightarrow (u = 0 \text{ ou } v = 0).$$

Comme tous les éléments de $A/\mathfrak{P}$ sont des classes d'éléments de A, cette condition est équivalente à la suivante :

$$\forall x, y \in A \ , \ \overline{xy} = 0 \Longrightarrow (\overline{x} = 0 \text{ ou } \overline{y} = 0).$$

1. L'impossibilité de résoudre l'équation $x^2 - 2 = 0$ dans $\mathbf{Q}$ est apparue longtemps avant, mais la résolution de cet antique problème n'a pas emprunté la même route algébrique !

Mais les conditions $\overline{xy} = 0, \overline{x} = 0$ et $\overline{y} = 0$ sont respectivement équivalentes aux conditions $xy \in \mathfrak{P}$, $x \in \mathfrak{P}$ et $y \in \mathfrak{P}$, donc (i) est bien équivalente à (ii). □

Définition 3.5.2 On dit que l'idéal $\mathfrak{P}$ est *premier* s'il vérifie les conditions de la proposition.

Corollaire 3.5.3 *(i) Tout idéal maximal est premier.*
(ii) Tout anneau non trivial admet des idéaux premiers.

Preuve. - (i) En effet, tout corps est un anneau intègre.
(ii) Cela découle du théorème de Krull. □

Exemples 3.5.4
1. L'idéal A n'est jamais premier. L'idéal $\{0\}$ l'est si, et seulement si A est intègre.
2. Soit $p \in \mathbf{Z}$. Alors (p) est un idéal premier si, et seulement si p est premier dans $\mathbf{Z}$.
3. Soit $P \in K[X]$. Alors $< P >$ est un idéal premier si, et seulement si P est irréductible.
4. Soit $P \in K[X,Y]$. Alors $< P >$ est un idéal premier si, et seulement si P est irréductible. Ce n'est pas évident, on le prouvera au chapitre 6.
5. Soit $\phi : A \to K$ un morphisme d'anneaux, K étant un corps. Alors $\mathrm{Ker}\phi$ est premier (d'après le premier théorème d'isomorphisme, le quotient est isomorphe au sous-anneau $\mathrm{Im}\phi$ de K, qui est intègre.

Exercice 3.5.5 Montrer que tout idéal premier de A peut s'obtenir comme noyau d'un morphisme d'anneaux $\phi : A \to K$, K étant un corps.

En appliquant les résultats de la section 3.3, on obtient immédiatement :

Proposition 3.5.6 *Soit I un idéal propre de A. Les idéaux premiers de A/I sont les idéaux $\mathfrak{P}/I$, où $\mathfrak{P}$ est un idéal premier de A tel que $\mathfrak{P} \supset I$.*

□

Remarque 3.5.7 On peut également caractériser les idéaux premiers d'un anneau de fractions. Soit S une partie multiplicative d'un anneau intègre commutatif A. On suppose que S ne rencontre pas A^*, de sorte que l'anneau $S^{-1}A$ est non trivial. On vérifie alors les faits suivants :

1. Pour tout idéal premier $\mathfrak{P}$ de A qui ne rencontre pas S, l'ensemble $S^{-1}\mathfrak{P} := \{p/s \mid p \in \mathfrak{P}\ ,\ s \in S\}$ est un idéal premier de $S^{-1}A$.
2. Pour tout idéal premier $\mathfrak{Q}$ de $S^{-1}A$, l'intersection $\mathfrak{Q} \cap A$ est un idéal premier de A qui ne rencontre pas S.
3. Les applications $\mathfrak{P} \mapsto S^{-1}\mathfrak{P}$ et $\mathfrak{Q} \mapsto \mathfrak{Q} \cap A$ sont des bijections réciproques l'une de l'autre entre l'ensemble des idéaux premiers de A qui ne rencontrent pas S et l'ensemble de tous les idéaux premiers de $S^{-1}A$.

3.5.2 Éléments premiers, éléments irréductibles

Le cas particulier d'un anneau intègre A et d'un idéal principal (a) est important. On voit que (a) est premier si, et seulement si a n'est pas inversible et :

$$\forall x, y \in A \ , \ a|xy \Longrightarrow (a|x \text{ ou } a|y).$$

On dit alors que l'élément a est *premier*. Cela entraîne que a est *irréductible*, c'est-à-dire qu'il est non inversible et que :

$$\forall x, y \in A \ , \ a = xy \Longrightarrow \Big(\big((a \sim x) \text{ et } (y \in A^*) \big) \text{ ou } \big((a \sim y) \text{ et } (x \in A^*) \big) \Big).$$

Exercice 3.5.8 (Cours) Vérifier que, dans un anneau intègre, tout élément premier est irréductible.

Cependant, la réciproque est fausse : dans certains anneaux, il y a des éléments irréductibles non premiers, et nous en verrons des exemples. Le chapitre 5 de ce cours est consacré à des anneaux ou ce genre d'anomalie ne se produit pas.

3.5.3 Le nilradical

Définition 3.5.9 L'ensemble de tous les éléments nilpotents de A est appelée *nilradical* de A.

Si x est nilpotent, il est clair que ax l'est pour tout a. On a vu en TD que la somme de deux nilpotents en est un. (Ces deux propriétés ne sont vraies que parce que A est implicitement supposé commutatif.) Comme 0 est évidemment nilpotent, mais pas 1 (l'anneau étant implicitement supposé non trivial), on conclut que le nilradical est un idéal propre de A.

Proposition 3.5.10 *Le nilradical de A est égal à l'intersection des idéaux premiers de A.*

Preuve. - Soient $x \in A$ un élément nilpotent et $\mathfrak{P} \subset A$ un idéal premier. L'image $\overline{x} \in A/\mathfrak{P}$ est un élément nilpotent, donc nul puisque cet anneau est intègre, *i.e.* $x \in \mathfrak{P}$. Puisque c'est vrai de tout nilpotent et de tout idéal premier, on conclut que le nilradical est inclus dans l'intersection des idéaux premiers.
On prouve la réciproque par contraposée : soit donc x non nilpotent, on va trouver un idéal premier qui ne le contient pas. On pose $S := \{x^n \mid n \in \mathbf{N}\}$. C'est une partie multiplicative qui ne contient pas 0. L'ensemble des idéaux de A qui ne rencontrent pas S est non vide car $\{0\}$ est un tel idéal. Cet ensemble est également inductif : en effet, si $(I_i)_{i \in X}$ est une chaîne de tels idéaux, $\bigcup I_i$ est un tel idéal. D'après le lemme de Zorn, il y a donc un élément maximal $\mathfrak{P}$ dans cet ensemble. On va montrer que $\mathfrak{P}$ est un idéal premier, ce qui achèvera la démonstration.
On le prouve encore par contraposée. Supposons donc que $a, b \in A$ sont tels que $a, b \notin \mathfrak{P}$. Alors les idéaux $\mathfrak{P} + (a)$ et $\mathfrak{P} + (b)$ contiennent strictement $\mathfrak{P}$. Par la propriété de maximalité de celui-ci, ces deux idéaux rencontrent S : il existe $k, l \in \mathbf{N}$ tels que $x^k \in \mathfrak{P} + (a)$ et $x^l \in \mathfrak{P} + (b)$. On en déduit que $x^{k+l} \in (\mathfrak{P} + (a))(\mathfrak{P} + (b))$. Mais un petit calcul montre que $(\mathfrak{P} + (a))(\mathfrak{P} + (b)) = \mathfrak{P} + (ab)$. Comme ce dernier idéal rencontre S, il n'est pas égal à $\mathfrak{P}$, donc $ab \notin \mathfrak{P}$. □

En appliquant cette proposition à l'anneau quotient A/I, et en prenant les images réciroques par la projection canonique $p : A \to A/I$, on peut en déduire que le radical de I, défini comme suit :

$$\sqrt{I} := \{x \in A \mid \exists n \in \mathbf{N} \ : \ x^n \in I\}$$

est égal à l'intersection des idéaux premiers qui contiennent I.

Exercice 3.5.11 Le démontrer.

3.6 Exercices sur le chapitre 3

Exercice 3.6.1 (Cours) Soient $f : A \to B$ un morphisme d'anneaux et I un idéal de A et J un idéal de B.
1) Le sous-groupe $f(I)$ de B est-il nécessairement un idéal ? Que dire si f est supposé surjectif ?
2) On suppose que $f(I) \subset J$. Montrer que f passe au quotient en un morphisme $\overline{f} : A/I \to B/J$.
3) Montrer que $f^{-1}(J)$ est un idéal de A et que $A/f^{-1}(J)$ est isomorphe à un sous-anneau de B/J.

Exercice 3.6.2 (Cours) 1) Décrire les éléments inversibles de $\mathbf{Z}/m\mathbf{Z}$, $m \in \mathbf{Z}$. Donner une condition nécessaire et suffisante portant sur m pour que $\mathbf{Z}/m\mathbf{Z}$ soit intègre, resp. un corps.
2) Mêmes questions concernant $K[X]/(P)$.

Exercice 3.6.3 1) On note ici A l'anneau $\mathbf{Z}[\mathrm{i}] := \{a+b\mathrm{i} \mid a,b \in \mathbf{Z}\}$ des entiers de Gauß. Montrer que son corps des fractions est le sous-corps $K := \mathbf{Q}[\mathrm{i}] := \{a+b\mathrm{i} \mid a,b \in \mathbf{Q}\}$ de $\mathbf{C}$.
2) Montrer que, pour tout $w \in K$, il existe $z \in A$ tel que $|z-w| < 1$.
3) Pour tout $z = a+b\mathrm{i} \in A$, on note $N(z) := a^2+b^2$. Montrer que, quels que soient $z, z' \in A$, $z \neq 0$, il existe $q, r \in A$ tels que $z' = qz+r$ et $N(r) < N(z)$. Y a-t-il unicité de cette "division euclidienne" ?
4) Soit I un idéal non trivial de A. Montrer qu'il existe un élément x de I tel que $N(x)$ soit minimum non nul. Déduire de la question 3 que x engendre I.
On a donc montré que l'anneau $\mathbf{Z}[\mathrm{i}]$ des entiers de Gauß est *principal*, autrement dit, que tout idéal de $\mathbf{Z}[\mathrm{i}]$ est principal.

Exercice 3.6.4 Dans l'anneau $K[X,Y]/ < X(1-YX) >$, on note x la classe de X et y la classe de Y. Montrer que chacun des éléments x et yx divise l'autre mais qu'ils ne sont pas associés.

Exercice 3.6.5 On dit qu'un idéal I d'un anneau commutatif A est *de type fini* s'il existe $x_1, \ldots, x_n \in A$ tels que $I = < x_1, \ldots, x_n >$. Montrer que la somme et le produit de deux idéaux de type fini sont des idéaux de type fini.

Exercice 3.6.6 Soit (I_k) une suite croissante d'idéaux. On suppose que l'idéal $\bigcup I_k$ est de type fini. Montrer que la suite est stationnaire.

Exercice 3.6.7 1) Soient $f_1, \ldots, f_n \in \mathcal{C}(\mathbf{R}, \mathbf{R})$. Montrer que tout élément g de $< f_1, \ldots, f_n >$ vérifie $g = O(|f_1| + \cdots + |f_n|)$ au voisinage de 0. En déduire que l'idéal $I := \{f \in \mathcal{C}(\mathbf{R}, \mathbf{R}) \mid f(0) = 0\}$ n'est pas de type fini. (Si $f_1, \ldots, f_n \in I$, la fonction $f := \sqrt{|f_1| + \cdots + |f_n|}$ appartient à I mais pas à $< f_1, \ldots, f_n >$.)
2) Dans l'anneau $\mathcal{C}(\mathbf{R}, \mathbf{R})$, l'idéal I des fonctions nulles en 0 Montrer que $I^2 = I$. (Toute fonction $f \in I$ s'écrit $f = gh$ où $g := \sqrt{|f|}$ et $h := \mathrm{sgn}(f)g$.)

Exercice 3.6.8 On dit qu'un anneau est *local* s'il admet un unique idéal maximal. Montrer que cette condition est équivalente à la suivante : la somme de deux éléments non inversibles est un élément non inversible. Dans ce cas, l'idéal maximal est l'ensemble de tous les éléments non inversibles.

Exercice 3.6.9 Montrer que les idéaux de $\mathbf{Z}_{(p)} := S^{-1}\mathbf{Z}$, où $S := \mathbf{Z} \setminus p\mathbf{Z}$, sont 0 et les (p^n), $n \in \mathbf{N}$. Montrer que cet anneau est principal et local.

Exercice 3.6.10 1) Soit X un espace topologique compact. Montrer que les seuls idéaux maximaux de $\mathcal{C}(X,\mathbf{R})$ (resp. de $\mathcal{C}(X,\mathbf{C})$) sont les idéaux de la forme $\{f \mid f(a)=0\}$, où $a \in X$.
2) Montrer que ce n'est pas vrai dans $\mathcal{C}(\mathbf{R},\mathbf{R})$ (resp. $\mathcal{C}(\mathbf{R},\mathbf{C})$).

Exercice 3.6.11 1) Démontrer que tout idéal premier contient un idéal premier minimal.
2) En déduire que le radical est l'intersection des idéaux premiers minimaux.

Exercice 3.6.12 1) On note $\mathrm{Spec}(A)$ (*spectre* de A) l'ensemble des idéaux premiers de A. A quelle condition $\mathrm{Spec}(A)$ est-il vide ?
2) Pour tout idéal I de A, on note $V(I) := \{\mathfrak{P} \in \mathrm{Spec}(A) \mid I \subset \mathfrak{P}\}$. A quelle condition a-t-on $V(I)=\emptyset$, resp. $V(I)=\mathrm{Spec}(A)$?
3) Montrer que $V(IJ)=V(I\cap J)=V(I)\cup V(J)$ et que $V(\sum I_i)=\bigcap V(I_i)$. En déduire que les $V(I)$ sont les fermés d'une topologie sur $\mathrm{Spec}(A)$.
4) Quels sont les points fermés de $\mathrm{Spec}(A)$? La topologie est-elle séparée ?
5) Montrer que, si A est intègre, l'élément (0) de $\mathrm{Spec}(A)$ est dense (il appartient à tous les ouverts non vides).
6) Montrer que, si $x,y \in \mathrm{Spec}(A)$ sont distincts, il existe un ouvert contenant l'un et pas l'autre.
7) Montrer que l'adhérence de $X \subset \mathrm{Spec}(A)$ est le fermé $V(I)$ où $I = \bigcap\limits_{\mathfrak{P}\in X} \mathfrak{P}$.
8) Soit $f : A \to B$ un morphisme d'anneaux. Montrer que l'application $f^* : \mathfrak{Q} \mapsto f^{-1}(\mathfrak{Q})$ de $\mathrm{Spec}(B)$ dans $\mathrm{Spec}(A)$ est continue.
9) Dans le cas où $B=A/I$ et où f est le morphisme canonique, montrer que f^* est un homéomorphisme de $\mathrm{Spec}(B)$ sur le fermé $V(I)$.
10) Dans le cas où $B=S^{-1}A$, avec $S=\{a^n \mid n \in \mathbf{N}\}$ pour un certain $a \in A$, et où f est le morphisme canonique, montrer que f^* est un homéomorphisme de $\mathrm{Spec}(B)$ sur l'ouvert $\mathrm{Spec}(A)\setminus V(Aa)$.

Exercice 3.6.13 Un *idéal à gauche* de l'anneau A (non nécessairement commutatif) est un sous-groupe I de $(A,+)$ tel que :

$$\forall a \in A\ ,\ \forall x \in I\ ,\ ax \in I.$$

Montrer que, pour tout $x \in A$, l'ensemble $Ax := \{ax \mid a \in A\}$ est un idéal à gauche. A quelle condition est-il trivial ? A quelle condition est-il égal à A ?

Exercice 3.6.14 1) Soit $f : A \to B$ un morphisme d'anneaux (non nécessairement commutatifs). Montrer que le noyau de f est un *idéal bilatère* de A, autrement dit, un sous-groupe de $(A,+)$ tel que :

$$\forall a \in A\ ,\ \forall x \in I\ ,\ ax \in I \text{ et } xa \in I.$$

2) Montrer que les seuls idéaux bilatères de l'anneau $M_n(K)$ des matrices carrées de taille n sur le corps commutatif K sont l'idéal trivial et l'anneau tout entier. Donner des exemples d'idéaux à gauche de $M_2(\mathbf{R})$ qui ne soient ni triviaux ni égaux à l'anneau tout entier.

Exercice 3.6.15 On dit que la relation d'équivalence $a \sim b$ dans l'anneau A (non nécessairement commutatif) est *compatible avec les lois de l'anneau* si :

$$\forall a,b,a',b' \in A\ ,\ (a \sim a' \text{ et } b \sim b') \Longrightarrow (a+b \sim a'+b' \text{ et } ab \sim a'b').$$

1) Montrer qu'alors $I := \{x \in A \mid a \sim 0\}$ est un idéal bilatère de A et que $a \sim a' \Leftrightarrow a'-a \in I$.
2) Montrer qu'il existe une unique multiplication sur le groupe quotient A/I qui en fasse un anneau et telle que le morphisme de groupes canonique $A \to A/I$ soit un morphisme d'anneaux.