ALGÈBRE

(COURS DE L3, PREMIER SEMESTRE 2012/2013)

J. Sauloy [1]

19 novembre 2012

1. Institut mathématique de Toulouse et U.F.R. M.I.G., Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse CEDEX 4

Introduction

Contenu du cours

Le cours d'algèbre du premier semestre de L3 porte sur les anneaux, et ceux-ci sont presque toujours commutatifs et unitaires (sauf dans quelques exercices). Outre la théorie (élémentaire !), on propose de nombreuses applications arithmétiques (y compris de l'étude des anneaux de polynômes). Des applications géométriques seront données dans les cours d'algèbre du premier et du second semestre de M1. Comme la structure d'anneau a pris de l'importance dans les mathématiques du XXème siècle (en géométrie et en analyse, les anneaux de fonctions sur un espace sont un moyen efficace d'étude de cet espace), l'étudiant trouvera dans ses cours de L3, M1 et M2 de nombreuses autres applications (par exemple l'anneau $\mathbf{C}(\{z\})$ des séries entières, dans le cours d'analyse complexe du second semestre de L3).

On a ajouté à l'étude des anneaux quelques connaissances d'algèbre générale, voire de théorie des ensembles, qui semblent devoir faire partie d'un "socle de licence" mais ne sont pas enseignées (ou suffisamment détaillées) ailleurs : propriété de clôture algébrique de $\mathbf{C}$, nombres algébriques, résultant, dénombrabilité et puissance du continu, familles indexées par un ensemble arbitraire ...

Enfin, pour préparer ceux des étudiants qui iront en M1 MFA l'an prochain (et donc pour qui le "socle de licence" n'est pas suffisant), certains points plus délicats (comme les anneaux de fractions) sont abordés, mais leur connaissance ne sera pas exigée aux examens. En règle générale, les passages correspondants sont imprimés en petits caractères (comme ceux-ci).

Exercices et TD

Le rôle essentiel des exercices dans l'enseignement des mathématiques devrait à ce stade être évident pour tous. Rappelons qu'un exercice dont on écoute ou dont on lit la solution avant de l'avoir cherché est perdu pour toujours. Les séances TD ne sont qu'un cadre mis en place pour faciliter le travail, mais l'essentiel de ce travail a lieu en dehors du temps de présence en cours ou en TD : c'est la lecture du cours avec un papier et un crayon, pour vérifier tous les calculs et les raisonnements ; et la recherche personnelle des solutions des exercices (seul ou à plusieurs). D'ailleurs tous les exercices ne seront pas traités en séance de TD.

Certains exercices (ils sont alors signalés par la mention **Cours**) visent à démontrer des résultats qui font partie du cours : la connaissance de ces résultats pourra donc être exigée aux examens, ainsi que la compréhension de leurs démonstrations.

Bibliographie

Les principaux ouvrages généraux recommandés sont les suivants :

1. Le livre “Algebra” de Serge Lang, champion toutes catégories.
2. Le “Tout-en-un pour la licence” niveau L1, de Ramis-Warusfel, que l’on citera RW1 : chapitres II.1, II.2 et II.6.
3. Le “Tout-en-un pour la licence” niveau L2, de Ramis-Warusfel, que l’on citera RW2 : chapitres II.1 et II.7.

Signalons aussi parmi les références recommandables : “Algebra” de Michael Artin et “Cours d’algèbre” de Roger Godement.

Pour le lecteur qui souhaite aller au delà (par exemple l’étudiant qui vise un M1, voire l’agrégation ou un M2R), la suite naturelle de ce cours est l’algèbre commutative. On peut suggérer, à un niveau encore élémentaire :

1. Le livre “Basic Algebra” de Nathan Jacobson.
2. Les chapitres 4 et 7 du livre “Algèbre” de Bourbaki.
3. Le “Cours de mathématiques pures et appliquées” de Ramis-Warusfel, que l’on citera RW3 : niveau L3-M, chapitres 4,5,6.

Conventions générales et notations

Conventions générales

La notation $A := B$ signifiera que le terme A est défini par la formule B. Les expressions nouvelles sont écrites en *italiques* au moment de la définition. Noter qu'une définition peut apparaitre au cours d'un théorème, d'un exemple, d'un exercice, etc.

Exemple 0.0.1 L'espace vectoriel $E^* := \mathrm{Hom}_K(E,K)$ est appelé *dual* de E.

La fin d'un démonstration ou son absence est indiquée par le signe $\square$

Notations

$(x), Ax, < x >, (x_1,\ldots,x_n), Ax_1+\cdots+Ax_n, < x_1,\ldots,x_n >$
$\mathrm{Div}(x)$
$x \wedge y$
$\mathbf{F}_p, \mathbf{F}_q$
sgn
$\lfloor - \rfloor$
$K[X]_d$

Chapitre 1

Rappels sur l'arithmétique de Z et de $K[X]$

Dans tout ce chapitre, K désigne un corps commutatif quelconque ; mais le lecteur peut supposer qu'il s'agit de **Q**, de **R**, ou de **C**. Outre une "remise en route" des capacités techniques et théoriques, ce chapitre est l'occasion de mettre en place deux exemples fondamentaux et d'illustrer leur similitude (qui va d'ailleurs bien plus loin que ce que l'on en verra ici).

Remarque 1.0.2 On a choisi de faire ressortir l'aspect algorithmique de ces notions avec les véritables notations de l'algorithmique (variables, affectations, structures de contrôle ...) et pas seulement avec les constructions de suites par récurrence qui en tiennent souvent lieu dans les textes mathématiques. Pour approfondir cet aspect, on peut consulter RW1, chapitre II.8.

1.1 Division euclidienne

Nous admettrons le théorème suivant :

Théorème 1.1.1 *Soient $a, b \in \mathbf{Z}$ avec $b > 0$. Il existe alors un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{Z}$ tel que* $\begin{cases} a = qb + r, \\ 0 \leq r < b. \end{cases}$

□

Pour simplifier l'écriture des algorithmes, nous noterons $\text{diveucl}(a, b) := (q, r)$ ce couple ; q et r sont *le quotient et le reste de la division euclidienne de a par b*.

Exercice 1.1.2 Et si $b \leq 0$?

Théorème 1.1.3 *Soient $A, B \in K[X]$ avec $B \neq 0$. Il existe alors un unique couple $(Q, R) \in K[X] \times K[X]$ tel que* $\begin{cases} A = QB + R, \\ \deg R < \deg B. \end{cases}$

Nous noterons $\text{diveucl}(A, B) := (Q, R)$ ce couple ; Q et R sont *le quotient et le reste de la division euclidienne de A par B*.

Preuve. - Rappelons que, par convention $\deg 0 = -\infty$: la conclusion permet donc le cas $R = 0$. En général, si $B = b_0 + \cdots + b_n X^n$ avec $n \geq 0$ et $b_n \neq 0$, on a $\deg B = n$ et l'on notera $\mathrm{td}(B) := b_n X^n$ (terme dominant) et $\mathrm{cd}(B) = b_n$ (coefficient dominant). On suppose ici connues les règles de calcul usuelles (voir RW1, chap. II.6).

Unicité. Si $A = Q_1 B + R_1 = Q_2 B + R_2$ avec $\deg R_1, \deg R_2 < \deg B$, alors $R_2 - R_1 = B(Q_1 - Q_2)$. Comme $\deg(R_2 - R_1) \leq \max(\deg R_2, \deg R_1) < \deg B$, cela n'est possible que si $R_2 - R_1 = 0$; comme $B \neq 0$, cela implique $Q_1 - Q_2 = 0$.

Existence. La remarque de base est que, si $\deg A \geq \deg B$, alors $A_1 := A - \dfrac{\mathrm{cd}(A)}{\mathrm{cd}(B)} X^{\deg A - \deg B} B$ est tel que $\deg A_1 < \deg A$ (les termes dominants se sont éliminés). On définit donc une suite $A_0, A_1, \ldots, A_{r+1}$ et une suite $Q_0, Q_1, \ldots, Q_r$ en prenant $A_0 := A$, puis, tant que $\deg A_i \geq \deg B$:

$$\begin{cases} Q_i := \dfrac{\mathrm{cd}(A_i)}{\mathrm{cd}(B)} X^{\deg A_i - \deg B} = \dfrac{\mathrm{td}(A_i)}{\mathrm{td}(B)}, \\ A_{i+1} := A_i - Q_i B. \end{cases}$$

Puisque les $\deg A_i$ décroissent strictement, il existe r tel que $\deg A_r \geq \deg B > \deg A_{r+1}$. On vérifie (c'est une consigne !) par récurrence que $A = (Q_0 + \cdots + Q_i)B + A_{i+1}$ pour tout $i = 0, \ldots, r$. Ainsi, en prenant $Q := Q_0 + \cdots + Q_r$ et $R := A_{r+1}$, on obtient le résultat souhaité.
Pour traduire cet "algorithme" en véritable langage algorithmique, on va introduire deux variables : Q qui prendra successivement les valeurs $Q_0 + \cdots + Q_{i-1}$ et R qui prendra successivement les valeurs A_i, tout cela pour $i = 0, \ldots, r+1$. Voici l'algorithme :

```
Q := 0:
R := A;
tant que deg R >= deg B
   q := td(R)/td(B);
   R := R - q B;
   Q := Q + q;
rendre(Q,R);;
```

La "preuve de correction" de cet algorithme est la suivante. D'abord $\deg R$ diminue à chaque étape, donc l'algorithme finit par s'arrêter avec $\deg R < \deg B$ (condition de sortie de la boucle "tant que").
D'autre part, on a à chaque étape $A = QB + R$. En effet, c'est vrai au début (vues les initialisations des variables Q, R). Pour vérifier que chaque étape conserve cette propriété, on introduit les notations suivantes : on note temporairement Q, R les valeurs *avant* l'exécution des trois instructions et Q', R' les valeurs *après*. On a donc $R' = R - qB$ et $Q' = Q + q$, où $q := \dfrac{\mathrm{td}(R)}{\mathrm{td}(B)}$; il s'ensuit immédiatement que $Q'B + R' = QB + R$, et donc que si $A = QB + R$ alors $A = Q'B + R'$.
Enfin, la propriété $A = QB + R$ étant vérifiée à tout moment, elle l'est à la fin, et l'on a de plus $\deg B < \deg R$ (sortie de boucle "tant que"). □

Exercice 1.1.4 (Cours) Le reste de la division de P par $(X - a)$ est $P(a)$. Pour que a soit racine de P, il faut, et il suffit, que $(X - a)$ divise P.

Exemple 1.1.5 On prend $A := X^7 + X + 1$ et $B := X^3 + X + 1$, donc $\mathrm{td}(B) = X^3$. Voici les valeurs successives de Q, R, q :

Q	0	X^4	$X^4 - X^2$	$X^4 - X^2 - X$	$X^4 - X^2 - X + 1$
R	$X^7 + X + 1$	$-X^5 - X^4 + X + 1$	$-X^4 + X^3 + X^2 + X + 1$	$X^3 + 2X^2 + 2X + 1$	$2X^2 + X$
q	X^4	$-X^2$	$-X$	1	-

On retiendra la structure d'une preuve de correction d'algorithme :

1. Il y a un *compteur* (ici $\deg R$) qui décroît à chaque étape et garantit la terminaison.
2. Il y a un *invariant de boucle* (ici, l'égalité $A = QB + R$), propriété vérifiée par les variables au début par initialisation ; conservée à chaque étape ; et donc encore vérifiée à la fin.
3. La *condition de sortie* (négation de la condition posée dans la clause "tant que") (ici, l'inégalité stricte $\deg R < \deg B$), jointe à l'invariant de boucle, doit permettre de prouver la propriété que l'on souhaite garantir pour le résultat de l'algorithme (ici, la définition du quotient et du reste d'une division euclidienne).

1.2 Algorithme d'Euclide et théorème de Bézout

Pour tout $a \in \mathbf{Z}$, notons $\mathrm{Div}(a) \subset \mathbf{Z}$ l'ensemble des diviseurs de a :

$$\mathrm{Div}(a) := \{b \in \mathbf{Z} \mid \exists c \in \mathbf{Z} \ : \ bc = a\}.$$

De même, pour tout $A \in K[X]$, notons $\mathrm{Div}(A) \subset K[X]$ l'ensemble des diviseurs de A :

$$\mathrm{Div}(A) := \{B \in K[X] \mid \exists C \in K[X] \ : \ BC = A\}.$$

Théorème 1.2.1 (Théorème de Bézout) *Soient $a, b \in \mathbf{Z}$. Il existe alors un unique $x = ua + vb$, $u, v \in \mathbf{Z}$, tel que $\mathrm{Div}(x) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$ et $x \geq 0$. On dit que x est* le pgcd (plus grand commun diviseur) *de a et de b, et on le note $\mathrm{pgcd}(a, b)$ ou encore $a \wedge b$. On dit également que x et $-x$ sont* les pgcd de a et de b.

Preuve. - On va trouver $u, v \in \mathbf{Z}$ tels que $x := ua + vb$ divise à la fois a et b. Tout le reste est facile est laissé en exercice au lecteur.
Puisque $ua = (-u)(-a)$ et $vb = (-v)(-b)$, on peut supposer $a, b \in \mathbf{N}$. Le principe de l'*algorithme d'Euclide* repose sur les faits suivants :

- Si $b = 0$ (et $a \geq 0$), alors $\mathrm{pgcd}(a, b) = a$.
- Si $a = qb + r$, alors $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b) \cap \mathrm{Div}(r)$ (en effet, si d divise a et b, il divise également $r = a - qb$; et si réciproquement d divise b et r, il divise également $a = qb + r$). Par conséquent, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.
- Pour calculer $\mathrm{pgcd}(a, b)$, il suffit donc de calculer $\mathrm{pgcd}(b, r)$, où $(q, r) := \mathrm{diveucl}(a, b)$; et c'est peut-être plus facile (voir ci-dessous).

La version mathématique [1] de l'algorithme est la suivante : on pose $x_0 := a$ et $y_0 := b$. Tant que $y_i > 0$, on calcule $(q_i, r_i) := \mathrm{diveucl}(x_i, y_i)$, puis on pose $x_{i+1} := y_i$, $y_{i+1} := r_i$. On a donc à tout moment $\mathrm{pgcd}(x_i, y_i) = \mathrm{pgcd}(a, b)$. D'autre part, $0 \leq y_{i+1} = r_i < y_i$, la suite ne peut donc être infinie.

1. Une version un peu différente ne faisant intervenir qu'une suite est proposée en TD.

Il existe donc r tel que $y_r = 0$ et l'on a alors $x_r = \text{pgcd}(x_r, y_r) = \text{pgcd}(a,b)$.
Cette version de l'algorithme ne fournit que le pgcd x et non les *coefficients de Bézout* u, v tels que $x = ua + vb$. Pour obtenir ces derniers, on introduit des suites u_i, v_i, s_i, t_i d'entiers tels que $x_i = u_i a + v_i b$ et $y_i = s_i a + t_i b$. Il suffit de prendre $(u_0, v_0) := (1,0)$ et $(s_0, t_0) := (0,1)$; puis de poser les relations de récurrence :

$$\begin{cases} (u_{i+1}, v_{i+1}) := (s_i, t_i), \\ (s_{i+1}, t_{i+1}) := (u_i - q_i s_i, v_i - q_i t_i). \end{cases}$$

Nous laissons au lecteur le soin d'effectuer les vérifications nécessaires.
Pour écrire l'algorithme, on introduit les variables x, y, u, v, s, t qui prendront les valeurs successives $x_i, y_i, u_i, v_i, s_i, t_i$. Voici le "code" :

```
x := a; y := b; u := 1; v := 0; s := 0; t := 1;
tant que y > 0
   (q,r) := diveucl(x,y);
   x := y; q := r;
   (u,v,s,t) := (s,t,u-qs,v-qt);
rendre(x,u,v);;
```

Le compteur qui garantit la terminaison est ici évidemment r. L'invariant de boucle est l'assertion suivante :

$$\text{pgcd}(x,y) = \text{pgcd}(a,b) \text{ et } x = ua + vb \text{ et } y = sa + tb \text{ et } y \geq 0.$$

La condition de sortie de boucle est $y \leq 0$, qui jointe à l'invariant de boucle entraîne $y = 0$, $x = \text{pgcd}(a,b)$ et bien entendu $x = ua + vb$. Le lecteur prendra soin de vérifier toutes ces affirmations. □

Le théorème de Bézout et l'algorithme d'Euclide s'adaptent pour les polynômes avec quelques petites précautions dûes à la différence suivante entre $\mathbf{Z}$ et $K[X]$:

- pour tout $x \in \mathbf{Z}$, on a $\text{Div}(y) = \text{Div}(x) \Leftrightarrow y = \pm x$ et un choix "canonique" dans la classe d'équivalence $\{+x, -x\}$ est toujours possible, celui de $|x|$;
- pour tout $\Delta \in K[X]$, on a $\text{Div}(\Delta') = \text{Div}(\Delta) \Leftrightarrow \Delta' = c\Delta, c \in K^*$ et un choix "canonique" dans la classe d'équivalence $K^*\Delta$ est encore possible : si $\Delta = 0$, c'est évidemment 0, sinon c'est l'unique polynôme unitaire de cette classe, qui est $\dfrac{1}{\text{cd}(\Delta)}\Delta$.

Théorème 1.2.2 (Théorème de Bézout pour les polynômes) *Soient $A, B \in K[X]$ non tous deux nuls. Il existe alors $\Delta = FA + GB$, $F, G \in K[X]$, tel que $Div(\Delta) = Div(A) \cap Div(B)$. On dit que Δ est* un pgcd de A et de B. *On peut choisir Δ unitaire, il est alors unique et on le note $pgcd(A,B)$ ou encore $A \wedge B$. On dit alors que Δ est* le pgcd de A et de B.

Preuve. - On va trouver $F, G \in K[X]$ tels que

$$\Delta := FA + GB$$

divise à la fois A et B. Tout le reste est facile est laissé en exercice au lecteur. L'algorithme d'Euclide pour les polynômes est similaire à celui que nous avons vu ; nous en donnons directement la version vraiment algorithmique :

```
Delta := A; Delta1 := B; F := 1; G := 0; F1 := 0; G1 := 1;
tant que D1 <> 0
   (Q,R) := diveucl(Delta,Delta1);
   Delta := Delta1; Delta1 := R;
   (F,G,F1,G1) := (F1,G1,F-QF1,G-QG1);
rendre(Delta,F,G);;
```

Le compteur qui garantit la terminaison est ici $\deg R$. L'invariant de boucle est l'assertion suivante :

$$\text{pgcd}(\Delta,\Delta_1) = \text{pgcd}(A,B) \text{ et } \Delta = FA+GB \text{ et } \Delta_1 = F_1A+G_1B.$$

La condition de sortie de boucle est $\Delta_1 = 0$. Le lecteur prendra soin de tout vérifier. (ATTENTION ! Le résultat n'est pas ici *le* pgcd mais *un* pgcd.) □

Exemple 1.2.3 On prend $A := X^2-1$ et $B := X^3-1$. Voici les valeurs successives de $\Delta, \Delta_1, F, G, F_1, G_1$:

Δ	X^2-1	X^3-1	X^2-1	$X-1$
Δ_1	X^3-1	X^2-1	$X-1$	0
(F,G)	$(1,0)$	$(0,1)$	$(1,0)$	$(-X,1)$
(F_1,G_1)	$(0,1)$	$(1,0)$	$(-X,1)$	$(X^2+X+1,-X-1)$

La valeur finale de Δ, c'est-à-dire $X-1$, est donc un pgcd ; et les valeurs finales de F et G, c'est-à-dire $-X$ et 1, des coefficients de Bézout. On voit bien que $X-1$ divise A et B et que l'on a la relation de Bézout :

$$-X.A+1.B = -X(X^2-1)+(X^3-1) = X-1.$$

On a même ici trouvé Δ unitaire, c'est donc *le* pgcd : mais c'est un hasard.

1.3 Divisibilité dans Z et dans $K[X]$

Rappelons que les éléments inversibles de $\mathbf{Z}$ sont $+1$ et -1 et que ceux de $K[X]$ sont les polynômes constants non nuls $\lambda \in K^*$. Par ailleurs on notera $|$ la relation "divise" :

$$\forall a,b \in \mathbf{Z}\ ,\ b|a \Longleftrightarrow \exists c \in \mathbf{Z}\ :\ a = bc,$$
$$\forall A,B \in K[X]\ ,\ B|A \Longleftrightarrow \exists C \in K[X]\ :\ A = BC.$$

Exercice 1.3.1 (Cours) Quels éléments de $\mathbf{Z}$, resp. de $K[X]$, divisent tous les autres ? Quels éléments sont divisibles par tous les autres ? À quelle condition deux éléments se divisent-ils mutuellement ? Traduire ces propriétés à l'aide de la notation $\text{Div}(a)$, resp. $\text{Div}(A)$.

Définition 1.3.2 Les entiers $a,b \in \mathbf{Z}$ sont dits *premiers entre eux* s'ils n'ont aucun diviseur commun non trivial (c'est-à-dire ici non inversible).

Corollaire 1.3.3 (du théorème de Bézout) *Les entiers $a,b \in \mathbf{Z}$ sont premiers entre eux si, et seulement s'il existe $u,v \in \mathbf{Z}$ tels que $ua+vb = 1$.*

□

Définition 1.3.4 Les polynômes $A, B \in K[X]$ sont dits *premiers entre eux* s'ils n'ont aucun diviseur commun non trivial (c'est-à-dire ici non inversible).

Corollaire 1.3.5 (du théorème de Bézout pour les polynômes) *Les polynômes $A, B \in K[X]$ sont premiers entre eux si, et seulement s'il existe $F, G \in K[X]$ tels que $FA + GB = 1$.*

□

Définition 1.3.6 (i) L'entier $a \in \mathbf{Z}$ est dit *irréductible* s'il n'est pas inversible et si $a = bc$, $b, c \in \mathbf{Z}$, entraîne que b ou c est inversible.
(ii) L'entier $a \in \mathbf{Z}$ est dit *premier* s'il n'est pas inversible et si $a|bc$, $b, c \in \mathbf{Z}$, entraîne que $a|b$ ou $a|c$.

Théorème 1.3.7 (Euclide) *Pour qu'un élément de $\mathbf{Z}$ soit irréductible, il faut, et il suffit, qu'il soit premier.*

Preuve. - Il est facile de voir (c'est une consigne !) que tout élément premier est irréductible. La réciproque découle immédiatement du théorème suivant (en dépit de la chronologie !). □

Théorème 1.3.8 (Gauß) *Soient $a, b \in \mathbf{Z}$ premiers entre eux et soit $c \in \mathbf{Z}$ tel que $a|bc$. Alors $a|c$.*

Preuve. - On invoque le théorème de Bézout sous la forme de son corollaire ci-dessus : il existe $u, v \in \mathbf{Z}$ tels que $ua + vb = 1$. Alors $c = uac + vbc$, le premier terme est trivialement multiple de a, le second l'est parce que bc l'est par hypothèse, donc c est multiple de a. □

Exercice 1.3.9 (Cours) Déduire le théorème d'Euclide du théorème de Gauß.

Définition 1.3.10 (i) Le polynôme $A \in K[X]$ est dit *irréductible* s'il n'est pas inversible et si $A = BC$, $B, C \in K[X]$, entraîne que B ou C est inversible.
(ii) Le polynôme $A \in K[X]$ est dit *premier* s'il n'est pas inversible et si $A|BC$, $B, C \in K[X]$, entraîne que $A|B$ ou $A|C$.

Les deux théorèmes qui suivent se démontrent exactement comme les deux précédents.

Théorème 1.3.11 (Euclide pour les polynômes) *Pour qu'un élément de $K[X]$ soit irréductible, il faut, et il suffit, qu'il soit premier.*

□

Théorème 1.3.12 (Gauß pour les polynômes) *Soient $A, B \in \mathbf{Z}$ premiers entre eux et soit $C \in \mathbf{Z}$ tel que $A|BC$. Alors $A|C$.*

□

Exercice 1.3.13 Soient $a, b \in \mathbf{Z}$ tels que pour tout $c \in \mathbf{Z}$, on ait l'implication : $a|bc \Rightarrow a|c$. Peut-on en déduire que a et b sont premiers entre eux ? Même question dans $K[X]$.

Dorénavant, dans le cas de $\mathbf{Z}$ et de $K[X]$, on confondra les termes "irréductible" et "premier" (il n'en sera pas toujours ainsi, voir la section 2.5). Noter cependant qu'il est d'usage de parler de *polynômes irréductibles* et de *nombres premiers* (mais, dans ce dernier cas, l'expression est en principe réservée aux premiers positifs).

Exercice 1.3.14 Le polynôme X^2+1 est-il irréductible ?

Notons que $-5 \in \mathbf{Z}$ et $2X-2 \in \mathbf{R}[X]$ sont irréductibles mais pas aussi simples que possible : 5 et $X-1$ sont plus simples et leur sont respectivement "équivalents".

Définition 1.3.15 Les entiers $a, b \in \mathbf{Z}$ sont dits *associés* si chacun divise l'autre, *i.e.* $\mathrm{Div}(a) = \mathrm{Div}(b)$. On notera : $a \sim b$.

Cela équivaut évidemment à $b = \pm a$. Tout entier non nul est donc associé à un unique entier strictement positif et tout irréductible de $\mathbf{Z}$ est associé à un unique *nombre premier*, *i.e.* un élément de l'ensemble $P := \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,\ldots\}$. (On sait depuis Euclide que P est infini ; savez-vous le démontrer ?)

Définition 1.3.16 Les polynômes $A, B \in K[X]$ sont dits *associés* si chacun divise l'autre, *i.e.* $\mathrm{Div}(A) = \mathrm{Div}(B)$. On notera : $A \sim B$.

Cela équivaut évidemment à $B = cA$, $c \in K^*$. Tout polynôme non nul est donc associé à un unique polynôme irréductible unitaire

Exercice 1.3.17 (Cours) Soient $a, b, a', b' \in \mathbf{Z}$ tels que $a \sim a'$ et $b \sim b'$. Que peut-on conclure si a est irréductible ? si $a|b$? si a et b sont premiers entre eux ? Mêmes questions dans $K[X]$.

1.4 Les théorèmes fondamentaux

Notons $p_1 := 2, p_2 := 3, p_3 := 5, \ldots$ les *nombres premiers*, *i.e.* les éléments irréductibles positifs de $\mathbf{Z}$ rangés par ordre croissant. (On rappelle qu'il y en a une infinité dénombrable !)

Théorème 1.4.1 (Théorème Fondamental de l'Arithmétique) *Pour tout $a \in \mathbf{Z}$ non nul, il existe un unique $\varepsilon = \pm 1$ et une unique suite $(r_1, r_2, r_3, \ldots)$ d'entiers naturels presque tous nuls tels que :*

$$a = \varepsilon \prod_{i \geq 1} p_i^{r_i}.$$

Preuve. -

Existence. Notons d'abord que, puisque les exposants r_i sont presque tous nuls (c'est-à-dire que tous sauf un nombre fini d'entre eux sont nuls), les facteurs $p_i^{r_i}$ sont presque tous égaux à 1 et qu'on a donc en réalité un produit fini. (Les produits infinis présupposent un passage à la limite et n'ont donc de sens qu'en présence d'une topologie !)
Puisque $a = \varepsilon|a|$ avec $\varepsilon = \pm 1$ et $|a| \in \mathbf{N}^*$, il suffit de décomposer $|a|$, autrement dit, on peut supposer d'emblée que $a > 0$. On veut alors montrer que a est produit de nombres premiers (qu'il

suffira de regrouper pour obtenir l'expression voulue). On va procéder pour cela par "descente infinie", méthode inventée par Fermat, et qui est une variante de la démonstration par récurrence forte. Supposons donné $a \in \mathbf{N}^*$ qui n'est pas produit de facteurs premiers. Il n'est donc ni égal à 1 (produit vide) ni premier ; il est donc réductible : $a = bc$, avec $b, c \neq \pm 1$. Quitte à remplacer b, c par leurs valeurs absolues, on a donc $b, c \geq 2$, donc $b = a/c < a$ et $c = a/b < a$. Si b et c étaient tous deux produits de facteurs premiers, a le serait ; donc par exemple b n'est pas produit de facteurs premiers. Ainsi, à tout nombre a de $\mathbf{N}^*$ qui n'est pas produit de facteurs premiers, on peut associer un nombre $b < a$ dans $\mathbf{N}^*$ qui a la même propriété ; or, une telle "descente infinie" est impossible dans $\mathbf{N}$, contradiction.

Unicité. Supposons que $a = \varepsilon \prod p_i^{r_i} = \varepsilon' \prod p_i^{r'_i}$. En comparant les signes, on voit que $\varepsilon = \varepsilon'$, d'où l'égalité $\prod p_i^{r_i} = \prod p_i^{r'_i}$. Posons $s_i := r_i - \min(r_i, r'_i)$ et $s'_i := r'_i - \min(r_i, r'_i)$. En divisant les deux membres par $\prod p_i^{\min(r_i, r'_i)}$, on obtient l'égalité $\prod p_i^{s_i} = \prod p_i^{s'_i}$, dans laquelle, pour tout i, soit $s_i = 0$ soit $s'_i = 0$. On va démontrer que les deux sont vrais, donc que $r_i = r'_i$ comme désiré.
Si l'on avait par exemple $s_j \geq 1$, alors p_j diviserait $\prod p_i^{s_i} = \prod p_i^{s'_i}$, donc l'un des $p_i^{s'_i}$ (puisque p_j est premier), qui ne pourrait être que $p_j^{s'_j}$ (puisque p_j ne divise aucun autre p_i), et l'on en tirerait $s'_j \geq 1$, contradiction. □

Notons maintenant $(P_i)_{i \in I}$ la famille de tous les polynômes irréductibles unitaires de $K[X]$.

Théorème 1.4.2 (Théorème Fondamental de l'Arithmétique pour les polynômes) *Pour tout $A \in K[X]$ non nul, il existe un unique $c \in K^*$ et une unique famille $(r_i)_{i \in I}$ d'entiers naturels presque tous nuls tels que :*

$$A = c \prod_{i \in I} P_i^{r_i}.$$

Preuve. - Le principe de la preuve est le même, la descente infinie étant remplacée par une récurrence sur le degré. □

Remarque 1.4.3 Il faut prendre garde qu'en général les polynômes irréductibles unitaires de $K[X]$ ne forment pas un ensemble dénombrable, donc ne peuvent être écrits comme une suite (voir plus loin le cas de $\mathbf{C}[X]$) : c'est pourquoi nous sommes contraints de recourir à la notation en *famille* d'ensemble d'indices I non précisé. (Nous reparlerons de dénombrabilité et de familles à la section 2.4 du chapitre 2.)
Par ailleurs, le produit $\prod_{i \in I}$ ne pose pas de problème parce qu'il s'agit en réalité d'un produit fini (presque tous les exposants sont nuls, donc presque tous les facteurs sont égaux à 1) et que la multiplication des polynômes est commutative et associative (l'ordre des facteurs et l'ordre des opérations n'ont donc pas d'importance).

Exercice 1.4.4 1) Montrer que, quel que soit le corps K, l'ensemble E des polynômes irréductibles unitaires de $K[X]$ est infini.
2) Si K est fini ou dénombrable, E est dénombrable.
3) Si K n'est pas dénombrable, E ne l'est pas non plus.

1.5 Le cas de $\mathbf{C}[X]$ et de $\mathbf{R}[X]$

1.5.1 Le cas de $\mathbf{C}[X]$

Théorème 1.5.1 (D'Alembert-Gauß) *Le corps* $\mathbf{C}$ *est* algébriquement clos, *autrement dit, tout polynôme* $P \in \mathbf{C}[X]$ *non constant admet au moins une racine.*

Preuve. - On écrit $P(z) = a_0 + \cdots + a_n z^n$, où $n \geq 1$ et où $a_0, \ldots, a_n \in \mathbf{C}$, $a_n \neq 0$. (Donc $\deg P = n$.) On va utiliser de la topologie (rudimentaire) de $\mathbf{C}$. Tout d'abord, $\lim_{|z|\to+\infty} |P(z)| = +\infty$, ce qui signifie de manière précise : $\forall M > 0\ ,\ \exists R > 0\ :\ |z| > R \Longrightarrow |P(z)| > M$. En effet, on voit immédiatement que si $|z| > R > 0$, on a :

$$|P(z)| \geq \left(|a_n| R^n\right) \left(1 - \left|\frac{a_{n-1}}{a_n}\right| \frac{1}{R} - \cdots - \left|\frac{a_0}{a_n}\right| \frac{1}{R^n}\right),$$

et, pour R assez grand, le premier facteur est strictement supérieur à $2M$ et le second à $1/2$.
On en déduit que la fonction $|P(z)|$ a un minimum atteint sur $\mathbf{C}$. Prenant en effet $M := |P(0)|$ dans la condition ci-dessus, on voit qu'il suffit de chercher le minimum de la fonction continue $|P(z)|$ sur le disque fermé $\overline{\mathrm{D}}(0,R)$: or toute fonction continue sur une partie compacte (*i.e.* fermée bornée) non vide de $\mathbf{C}$ y admet un minimum atteint.
Soit donc $z_0 \in \mathbf{C}$ un point où la fonction $|P(z)|$ atteint son minimum. On va montrer par l'absurde que $P(z_0) = 0$. Supposons donc que $P(z_0) \neq 0$. Au voisinage de z_0, un tout petit calcul donne le développement limité suivant :

$$P(z_0 + h) = a + bh^k + \text{ des termes de degré supérieur en } k = a + bh^k + \varepsilon(h)h^k, \quad \lim_{h\to 0} \varepsilon(h) = 0,$$

où $a := P(z_0) \neq 0$ (par hypothèse) et où $b \neq 0$ et $k \geq 1$ (car on a supposé P non constant). On choisit $h_0 \in \mathbf{C}$ tel que $h_0^k = -a/b$ (il y a k possibilités). On en tire, pour tout $t > 0$:

$$\left|\frac{1}{a} P(z_0 + t h_0)\right| = \left|1 + b t^k h_0^k / a + \varepsilon'(t) t^k\right| = \left|1 - t^k + \varepsilon'(t) t^k\right| \leq \left|1 - t^k\right| + \varepsilon''(t) t^k, \lim_{t\to 0} \varepsilon'(t) = \lim_{t\to 0} \varepsilon''(t) = 0.$$

Il suffit de choisir $t > 0$ tel que $|\varepsilon''(t)| < 1/2$ pour avoir $\left|1 - t^k\right| + \varepsilon''(t) t^k < 1$, donc $|P(z_0 + t h_0)| < |a| = |P(z_0)|$, contredisant la minimalité en z_0. □

Corollaire 1.5.2 *Tout polynôme* $P \in \mathbf{C}[X]$ *est produit de facteurs du premier degré.*

Preuve. - Si $\deg P \geq 1$, il existe $z_0 \in \mathbf{C}$ tel que $P(z_0) = 0$ donc $P = (X - z_0)Q$ (exercice 1.1.4). On conclut par récurrence sur le degré. □

Corollaire 1.5.3 *Les polynômes irréductibles de* $\mathbf{C}[X]$ *sont les polynômes de degré* 1.

Corollaire 1.5.4 *Tout polynôme* $P \in \mathbf{C}[X]$ *admet une unique écriture* $P = C \prod_{a\in C} (X - a)^{m_a}, C \in \mathbf{C}^*$ *dans laquelle les* m_a *(famille non dénombrable !) sont presque tous nuls.*

Exercice 1.5.5 (Cours) (i) L'entier m_a ci-dessus est le plus grand entier m tel que $(X - a)^m | P$.
(ii) C'est également le plus grand entier m tel que $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ (*multiplicité* de la racine a de P ou *ordre* du zéro de P en a).

1.5.2 Le cas de $\mathbf{R}[X]$

On voit *a priori* que tous les polynômes du premier degré de $\mathbf{R}[X]$ sont irréductibles (c'est vrai sur n'importe quel corps). Un polynôme du second degré est irréductible si, et seulement s'il n'admet pas de racines (c'est encore vrai pour n'importe quel corps ; démontrez-le), donc, dans le cas de $\mathbf{R}[X]$, si son discriminant est strictement négatif.

Corollaire 1.5.6 *Les polynômes unitaires irréductibles de* $\mathbf{R}[X]$ *sont les* $(X-a)$, $a \in \mathbf{R}$ *et les* X^2+pX+q, $p,q \in \mathbf{R}$, $p^2-4q<0$.

Preuve. - Il suffit de voir que tout polynôme irréductible de $\mathbf{R}[X]$ est de degré 1 ou 2 ; et, pour cela, de voir que tout polynôme non constant de $\mathbf{R}[X]$ est divisible par un polynôme de degré 1 ou 2. Soit donc $P \in \mathbf{R}[X]$ un polynôme non constant. En tant que polynôme non constant de $\mathbf{C}[X]$, il admet au moins une racine $a \in \mathbf{C}$. Si $a \in \mathbf{R}$, le meme raisonnement que plus haut (division euclidienne par $(X-a)$) permet de conclure que P est divisible par $(X-a)$. Si $a \notin \mathbf{R}$, du calcul $0 = \overline{P(a)} = P(\overline{a})$ (puisque P est à coefficients réels), on déduit que $(X-\overline{a})$ divise P. Puisque P est divisible par les polynômes irréductibles non associés $(X-a)$ et $(X-\overline{a})$, il est divisible par leur produit $(X-a)(X-\overline{a}) = X^2+pX+q$ où $p := a+\overline{a} \in \mathbf{R}$ et $q := a\overline{a} \in \mathbf{R}$. On peut d'ailleurs remarquer que $p^2-4q = (a-\overline{a})^2 < 0$. □

Exercice 1.5.7 (Cours) Énoncer de manière explicite le théorème fondamental dans $\mathbf{R}[X]$.

1.5.3 Application à la décomposition en éléments simples

Soit $F := A/B \in \mathbf{C}(X)$, $A,B \in \mathbf{C}[X]$, $B \neq 0$, une fraction rationnelle à coefficients complexes. De la division euclidienne de A par B, on tire $F = Q + R/B$ où $\deg R < \deg B$. Le polynôme Q est appelé *partie entière* de F. L'entier $\deg A - \deg B$, qui ne dépend pas de l'écriture de F (vérifiez-le !) est appelé *degré* de F et noté $\deg F$. Ainsi la partie entière de F est l'unique polynôme Q tel que $\deg(F-Q) < 0$. Supposons maintenant et A,B premiers entre eux et B unitaire (écriture irréductible). On décompose $B = \prod_{i=1}^{k} (X-a_i)^{m_i}$ (les racines a_i étant deux à deux distinctes et les multiplicités m_i étant non nulles). D'après l'exercice 1.6.6, on peut écrire :

$$F = \sum_{i=1}^{k} \frac{A_i}{(X-a_i)^{m_i}},$$

les A_i étant des polynômes. Quitte à remplacer chaque A_i par son reste dans la division euclidienne par $(X-a_i)^{m_i}$, on peut supposer que $\deg A_i < m_i$ et le membre de gauche de l'égalité par $F-Q$, où Q est la somme des quotients : c'est évidemment la partie entière de F. On écrit maintenant $A_i(X+a_i) = A_{i,0} + \cdots + A_{i,m-1}X^{m_i-1}$ avec $A_{i,j} \in \mathbf{C}$, d'où finalement :

$$F = Q + \sum_{i=1}^{k} \sum_{j=0}^{m_i-1} \frac{A_{i,j}}{(X-a_i)^{m_i-j}}.$$

C'est la version complexe de la *décomposition en éléments simples* de F. On trouvera dans RW1 (chapitre sur les polynômes) les méthodes pratiques de calcul de la décomposition en éléments simples d'une fraction rationnelle, aussi bien dans le cas complexe que dans le cas réel. Ces méthodes sont utiles entre autres pour calculer des intégrales.

1.6 Exercices sur le chapitre 1

Exercice 1.6.1 (Cours) 1) Soient $a, b \in \mathbf{Z}$ premiers entre eux. Il existe donc $u_0, v_0 \in \mathbf{Z}$ tels que $u_0 a + v_0 b = 1$. Déterminer tous les couples $(u, v) \in \mathbf{Z} \times \mathbf{Z}$ tels que $ua + vb = 1$.
2) On suppose $b > 0$. Montrer qu'il existe un unique couple $(u, v) \in \mathbf{Z} \times \mathbf{Z}$ tel que $ua + vb = 1$ et $0 \leq u \leq b - 1$.
3) Comment s'étendent ces résultats lorsque le pgcd de a et b est un entier $d > 0$ arbitraire ?
4) Résoudre, pour $c \in \mathbf{Z}$ quelconque, l'équation $ax + by = c$ avec $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

Exercice 1.6.2 (Cours) 1) Soient $A, B \in K[X]$ non tous deux constants et premiers entre eux. Montrer que, pour tout couple $(F, G) \in K[X] \times K[X]$ tel que $FA + GB = 1$, les conditions et $\deg F < \deg B$ et $\deg G < \deg A$ sont équivalentes ; et qu'il existe un unique couple les vérifiant.
2) Comment s'étend ce résultat lorsque le pgcd de A et B est un polynôme arbitraire ?

Exercice 1.6.3 (Cours) 1) Soient $a_1, \ldots, a_n \in \mathbf{Z}$. Montrer qu'il existe un unique $d \in \mathbf{N}$ tel que :

$$\mathrm{Div}(d) = \mathrm{Div}(a_1) \cap \cdots \cap \mathrm{Div}(a_n).$$

C'est donc le pgcd de $a_1, \ldots, a_n$.
2) Montrer qu'il existe $x_1, \ldots, x_n \in \mathbf{Z}$ tels que $d = a_1 x_1 + \cdots + a_n x_n$.
3) Enoncer et prouver les assertions correspondantes pour $K[X]$.

Exercice 1.6.4 (Cours) 1) Soient $a = \varepsilon \prod p_i^{r_i}$ et $a' = \varepsilon' \prod p_i^{r'_i}$ (décompositions en facteurs premiers). Montrer que a' divise a si, et seulement si, $\forall i$, $r'_i \leq r_i$. En déduire le nombre de diviseurs de a.
2) Montrer qu'en général $a \wedge a' = \prod p_i^{\min(r_i, r'_i)}$.
3) Donner une condition nécessaire et suffisante pour que a soit un carré.
4) On suppose a et a' premiers entre eux et tels que aa' soit un carré. Montrer que soit a et a' sont des carrés, soit $-a$ et $-a'$ sont des carrés.
5) Montrer que 2 n'est pas le carré d'un nombre rationnel.

Exercice 1.6.5 (Cours) 1) Soit p un nombre premier. Montrer que les coefficients binomiaux $\binom{p}{k}$ sont multiples de p pour $k = 1, \ldots, p-1$.
2) En déduire, pour $x, y \in \mathbf{Z}$ arbitraires, la congruence $(x+y)^p \equiv x^p + y^p \pmod{p}$.
3) Démontrer le petit théorème de Fermat : $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbf{Z}$.
4) Démontrer que $a^{561} \equiv a \pmod{561}$ pour tout $a \in \mathbf{Z}$.

Exercice 1.6.6 (Cours) 1) Soient $a_1, \ldots, a_n \in \mathbf{Z}$ strictement positifs et premiers entre eux deux à deux. Montrer que les entiers $b_i := \prod_{\substack{1 \leq j \leq n \\ j \neq i}} a_j$ sont premiers entre eux dans leur ensemble, et en déduire, pour tout $b \in \mathbf{Z}$, l'existence de $x_1, \ldots, x_n, y \in \mathbf{Z}$ tels que :

$$\frac{b}{a_1 \cdots a_n} = y + \frac{x_1}{a_1} + \cdots + \frac{x_n}{a_n}.$$

Montrer que l'on peut imposer $0 \leq x_i \leq a_i - 1$ pour $i = 1, \ldots, n$ et que l'écriture est alors unique.
2) Enoncer et prouver les assertions correspondantes pour $K[X]$. Détailler en particulier le cas du corps $K = \mathbf{C}$. (On aura reconnu la *décomposition en éléments simples* des fractions rationnelles.)

Exercice 1.6.7 (Cours) Quels sont les irréductibles de $\mathbf{R}[X]$? de $\mathbf{C}[X]$? Quels sont les irréductibles de degré 2 de $\mathbf{Q}[X]$? Quel lien y a-t-il en général entre l'existence de racines de $P(X)$ dans K et son irréductibilité dans $K[X]$? Que peut-on dire de mieux pour les degrés 2 et 3 ?

Exercice 1.6.8 1) Soient $x,y,z \in \mathbf{Z}$ tels que $x^2+y^2=z^2$. On suppose tout d'abord x,y,z premiers entre eux dans leur ensemble, autrement dit, que leur pgcd est 1. Montrer : qu'ils sont premiers entre eux deux à deux ; que x ou y est impair, mais pas les deux ; que z est impair.
2) On suppose que c'est x qui est impair. Montrer que $z-x$ et $z+x$ ont pour pgcd 2, puis que $(z-x)/2$ et $(z+x)/2$ sont des carrés. En déduire qu'il existe $u,v \in \mathbf{Z}$ tels que $x=u^2-v^2$, $y=2uv$ et $z=u^2+v^2$.
3) Décrire toutes les solutions entières de l'équation $x^2+y^2=z^2$ sans hypothèse sur x,y,z.
4) Montrer que l'équation $x^4+y^4=z^4$ n'admet pas de solutions entières non évidentes, *i.e.* telles que $xy \neq 0$.

Exercice 1.6.9 1) Montrer que le reste de la division euclidienne de X^a-1 par X^b-1 est X^r-1, où r est le reste de la division euclidienne de a par b.
2) Montrer que le pgcd de X^n-1 et de X^p-1 est X^q-1, où q est le pgcd de n et p.

Exercice 1.6.10 1) On pose $P_n(X) := \dfrac{1}{n!}\prod_{i=0}^{n-1}(X-i)$. (Donc, par la convention usuelle sur les produits vides, $P_0=1$.) Montrer que tout polynôme de $\mathbf{C}[X]$ de degré $\leq n$ admet une unique décomposition $P=a_0P_0+\cdots+a_nP_n$ avec $a_0,\ldots,a_n \in \mathbf{C}$.
2) Montrer que $P(\mathbf{Z}) \subset \mathbf{Z}$ si, et seulement si, $a_0,\ldots,a_n \in \mathbf{Z}$.

Exercice 1.6.11 1) Soient $a,b \in \mathbf{Z}$ avec $a>b>0$. On définit une suite (x_n) d'entiers par $x_0 := a$, $x_1 := b$; et, pour tout $n \geq 2$ tel que x_n est non nul, x_{n+1} est le reste de la division euclidienne de x_{n-1} par x_n. Montrer que la suite (x_n) décroît strictement et qu'il existe p tel que $x_p \neq 0$ et $x_{p+1}=0$. (La suite est donc finie.) Vérifier que $d := x_p$ est le pgcd de a et b.
2) On note q_n le quotient de la division euclidienne de x_{n-1} par x_n. Démontrer la formule :

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} d \\ 0 \end{pmatrix}, \text{ où } M := \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_p & 1 \\ 1 & 0 \end{pmatrix}.$$

3) Montrer que M^{-1} est à coefficients entiers et permet de calculer les coefficients de Bézout.

Exercice 1.6.12 1) Soient $A,B \in K[X]$ tous deux non nuls et tels que $\deg A > \deg B$. On définit une suite (A_n) de polynômes par $A_0 := A$, $A_1 := B$; et, pour tout $n \geq 2$ tel que A_n est non nul : A_{n+1} est le reste de la division euclidienne de A_{n-1} par A_n. Montrer que la suite $(\deg A_n)$ décroît strictement et qu'il existe p tel que $A_p \neq 0$ et $A_{p+1}=0$. Vérifier que $\Delta := A_p$ est un pgcd de A et B.
2) On note Q_n le quotient de la division euclidienne de A_{n-1} par A_n. On pose $F_0 := 1$, $G_0 := 0$, $F_1 := 0$, $G_1 := 1$, puis, pour $n=1,\ldots,p$:

$$F_{n+1} := F_{n-1} - Q_nF_n \text{ et } G_{n+1} := G_{n-1} - Q_nG_n.$$

3) Montrer que $A_n = F_nA + G_nB$ pour $n=0,\ldots,p+1$. Vérifier, pour $n=1,\ldots,p$, les relations :

$$\deg Q_n = \deg A_{n-1} - \deg A_n \text{ et } \deg G_n = \deg Q_1 + \cdots + \deg Q_{n-1}.$$

4) En déduire que F_p, G_p sont, à un facteur constant près, les coefficients obtenus à l'exercice 1.6.2.

Chapitre 2

Anneaux commutatifs

Plusieurs conventions existent quant à la définition d'un anneau ; nous choisirons celle qui suppose l'existence d'un élément unité (neutre pour la multiplication). De plus, nous ne considérerons dans ce cours que des anneaux commutatifs (sauf dans quelques rares exemples et exercices).

2.1 Définition et exemples de base

Définition 2.1.1 Un *anneau* est un ensemble A muni de deux lois de composition interne $+$ (addition) et $\times$ (multiplication) soumises aux axiomes suivants :

1. $(A,+)$ est un groupe commutatif. On emploiera les notations usuelles pour les groupes additifs : 0 pour l'élément neutre (ou bien 0_A s'il y a un risque d'ambiguïté), $-a$ pour l'opposé de a, etc.
2. La multiplication est associative et admet un élément neutre. On emploiera les notations usuelles pour les lois multiplicatives : 1 pour l'élément neutre (ou bien 1_A s'il y a un risque d'ambiguïté), ab pour $a \times b$, etc.
3. La multiplication est distributive à gauche et à droite par rapport à l'addition.

Notons que la commutativité de l'addition est conséquence des autres axiomes en vertu du calcul suivant :

$$\begin{aligned}(1+1)(a+b) &= 1.(a+b)+1.(a+b) = a+b+a+b,\\ &= (1+1).a+(1+1).b = a+a+b+b,\end{aligned}$$

d'où l'on tire $a+b+a+b = a+a+b+b \Rightarrow b+a = a+b$ (simplification dans le groupe $(A,+)$).

Premières propriétés.

- 0 est absorbant pour la multiplication, *i.e.* $0.a = a.0 = 0$ pour tout $a \in A$. Cela découle du calcul suivant :
$$0.a = (0+0).a = 0.a+0.a \Longrightarrow 0.a = 0$$
(par simplification dans le groupe $(A,+)$) et similairement pour $a.0$.
- Si $0 = 1$ alors $A = \{0\}$, car $a = a.1 = a.0 = 0$ pour tout $a \in A$. On dit que l'anneau est *trivial*. Nous exclurons presque toujours ce cas sans nécessairement le préciser.

– Comme dans tout groupe abélien, on définit $ma \in A$ pour tout $m \in \mathbf{Z}$ et $a \in A$, de telle sorte que $m \mapsto ma$ soit l'unique morphisme de groupe $\mathbf{Z} \to A$ tel que $1 \mapsto a$. On a alors les propriétés usuelles $(m+n)a = ma + na$, $m(a+b) = ma + mb$, $m(na) = (mn)a$, etc. Concrètement, si $m \geq 0$, on pose $ma := a + \cdots + a$ (m termes) et si $m < 0$, on définit ma comme l'opposé de $|m|\,a$.
– On définit les puissances $a^m \in A$, $m \in \mathbf{N}$ de $a \in A$ par $a^0 = 1$ et $a^{m+1} := a^m.a$. De l'associativité, on déduit alors par récurrence que $a^{m+n} = a^m.a^n$ et que $a^{mn} = (a^m)^n$.

Définition 2.1.2 On dit que l'anneau $(A, +, \times)$ est *commutatif* si la multiplication est commutative.

Dans ce cours, nous n'étudierons que les anneaux commutatifs. Cependant nous montrerons parfois des exemples d'anneaux non commutatifs pour voir où cette propriété intervient.

Proposition 2.1.3 *Dans un anneau commutatif, on a les deux propriétés suivantes :*

$$\forall x, y \in A\ ,\ \forall n \in \mathbf{N}\ ,\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$
$$(xy)^n = x^n y^n.$$

Preuve. - La deuxième propriété est évidente. La première (formule du binôme) est un cas particulier de la formule du multinôme, donnée en exercice dans le TD. □

Exemples 2.1.4

1. $(\mathbf{Z}, +, \times)$ est un anneau commutatif.
2. $(K[X], +, \times)$ est un anneau commutatif (comme d'habitude, K désigne un corps commutatif).
3. $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ (classes de congruence modulo n) est un anneau commutatif. Rappelons que, si l'on note $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ la classe de congruence de $a \in \mathbf{Z}$, les opérations dans $\mathbf{Z}/n\mathbf{Z}$ sont définies par les formules $\overline{a} + \overline{b} := \overline{a+b}$ et $\overline{a}\overline{b} := \overline{ab}$.
4. Pour tout espace topologique X, les ensembles de fonctions continues $\mathcal{C}(X, \mathbf{R})$ et $\mathcal{C}(X, \mathbf{C})$ sont des anneaux commutatifs.
5. Soit A un anneau commutatif. Une expression de la forme [1] $\sum_{n \geq 0} a_n X^n$, où les $a_n \in A$, est appelée *série formelle en l'indéterminée X à coefficients dans A*. Noter qu'une telle expression comporte une infinité de termes ; on ne la considère pas comme une fonction et l'on ne cherchera pas à "l'évaluer" ou à "donner une valeur à X". On définit sur l'ensemble $A[[X]]$ des séries formelles deux lois de composition interne :

$$\sum_{n \geq 0} a_n X^n + \sum_{n \geq 0} b_n X^n := \sum_{n \geq 0} (a_n + b_n) X^n,$$
$$\left(\sum_{n \geq 0} a_n X^n \right) \times \left(\sum_{n \geq 0} b_n X^n \right) = \sum_{n \geq 0} c_n X^n \text{ où } c_n := \sum_{i+j=n} a_i b_j.$$

On peut vérifier que $(A[[X]], +, \times)$ est ainsi muni d'une structure d'anneau commutatif.

1. Ce qui suit n'est pas une définition rigoureuse ; voir RW1 et RW2 sur ce sujet.

6. Une série formelle $\sum_{n\geq 0} a_n X^n$ dans laquelle presque tous les coefficients (c'est-à-dire tous sauf un nombre fini d'entre eux) sont nuls est un *polynôme en l'indéterminée X à coefficients dans A*. L'ensemble de ces polynômes est noté $A[X]$. La somme et le produit de polynômes sont définis par les mêmes formules que pour les séries formelles ; on obtient bien ainsi des polynômes, comme le vérifiera le courageux lecteur. On munit ainsi $(A[X],+,\times)$ d'une structure d'anneau commutatif (en fait, un "sous-anneau" de $A[[X]]$ au sens de la section 2.3). Les anneaux de polynômes à coefficients dans un anneau seront étudiés au chapitre 6 ; mais nous y ferons appel dès à présent à titre d'exemples non triviaux.
7. Par exemple $(\mathbf{Z}[X],+,\times)$ (polynômes à une indéterminée à coefficients entiers) est un anneau commutatif, en fait un "sous-anneau" de $\mathbf{Q}[X]$ au sens de la section 2.3.
8. Pour tout $m \in \mathbf{N}^*$, on peut aussi définir l'anneau $(\mathbf{Z}/m\mathbf{Z})[X]$ des polynômes en X à coefficients dans $\mathbf{Z}/m\mathbf{Z}$.
9. $(K[X,Y],+,\times)$ (polynômes à deux indéterminées sur le corps commutatif K) est un anneau commutatif, que l'on peut identifier aux choix à l'anneau $(K[X])[Y]$ ou à l'anneau $(K[Y])[X]$.
10. $(\mathrm{Mat}_n(K),+,\times)$ (matrices carrées d'ordre n) est un anneau non commutatif, sauf dans le cas particulier où $n = 1$.

Un petit calcul. Il s'agit d'illustrer l'utilité de la commutativité dans la proposition vue plus haut. Soit $A := \mathrm{Mat}_2(\mathbf{R})$ et soient $M := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $N := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Alors :

$$MN = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = NM,$$
$$M^2N^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = (MN)^2,$$
$$M^2 + 2MN + N^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (M+N)^2.$$

2.2 Éléments particuliers dans un anneau

Inversibles. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = ba = 1$ (on dit parfois aussi que a est une *unité* de A). S'il existe, l'inverse b est unique et on le note a^{-1}. On note A^* l'ensemble des inversibles de A. Il est stable pour la multiplication (en fait, $(ab)^{-1} = b^{-1}a^{-1}$) et $(A^*,\times)$ est un groupe. (Pourquoi ?)

Exemples 2.2.1
1. Les inversibles de $(\mathbf{Z},+,\times)$ sont ± 1.
2. Les inversibles de $(K[X],+,\times)$ sont les constantes non nulles.
3. Les inversibles de $(\mathbf{Z}/n\mathbf{Z},+,\times)$ sont les $a = \overline{p}$ tels qu'il existe $b = \overline{q}$ tel que $ab = 1$, *i.e.* $pq \equiv 1 \pmod{n}$. D'après le théorème de Bézout, ce sont donc les $\overline{p}$ tels que $p \wedge n = 1$.
4. Les inversibles de $\mathcal{C}(X,\mathbf{R})$ et $\mathcal{C}(X,\mathbf{C})$ sont les fonctions qui ne s'annulent pas.
5. Les inversibles de $(\mathbf{Z}[X],+,\times)$ sont ± 1.
6. Les inversibles de $(K[X,Y],+,\times)$ sont les constantes non nulles.

7. L'élément $1+\dot{2}X$ est inversible dans $(\mathbf{Z}/4\mathbf{Z})[X]$ (il est égal à son propre inverse).
8. Les inversibles de $(\mathrm{Mat}_n(K),+,\times)$ font l'objet de la discussion qui suit.

Exercice 2.2.2 Démontrer que $\sum a_n X^n \in A[[X]]$ est inversible si, et seulement si a_0 est inversible dans A.

Remarque 2.2.3 On démontre en algèbre linéaire que si $M,N \in \mathrm{Mat}_n(K)$ sont tels que $MN = I_n$, alors $NM = I_n$: ces éléments sont donc inversibles et inverses l'un de l'autre. Mais cela ne se produit pas dans tout anneau non commutatif. Par exemple, si $A = \mathcal{L}_K(E)$ est l'anneau des endomorphismes d'un K-espace vectoriel de dimension infinie (vérifier qu'un tel anneau existe !) et si $f \in \mathcal{L}_K(E)$ est une application linéaire injective et non surjective (vérifier qu'il en existe !), alors f est inversible à gauche (il existe $g \in A$ telle que $gf = \mathrm{Id}_E$) mais pas à droite (il n'existe pas $h \in A$ telle que $fh = \mathrm{Id}_E$). Symétriquement, si f est une application linéaire surjective et non injective (vérifier qu'il en existe !), alors f est inversible à droite mais pas à gauche.

Exercice 2.2.4 Démontrer tout cela.

Définition 2.2.5 Un *corps* est un anneau non trivial dans lequel tout élément non nul est inversible.

Exercice 2.2.6 Quels sont les corps parmi les exemples donnés plus haut ?

Diviseurs de 0. Un élément $a \in A$ est un *diviseur de* 0 s'il existe $b \in A$ non nul tel que $ab = ba = 0$. Naturellement, 0 est un diviseur de 0 (car $0.1 = 1.0 = 0$ et $1 \neq 0$ puisque nous ne considérons que des anneaux non triviaux). Dans l'exemple de $\mathrm{Mat}_n(K)$, $ab = 0$ n'entraîne pas $ba = 0$, mais, s'il existe $b \neq 0$ tel que $ab = 0$ alors il existe $c \neq 0$ tel que $ca = 0$. En revanche, même cela n'est plus vrai dans le cas de l'anneau $\mathcal{L}_K(E)$, où E est de dimension infinie : prendre les mêmes exemples ! Cette notion est donc très délicate dans le cas d'un anneau non commutatif.

Définition 2.2.7 L'anneau (commutatif non trivial) A est dit *intègre* si son seul diviseur de 0 est 0 ; autrement dit, si $ab = 0$ implique $a = 0$ ou $b = 0$.

Un élément inversible n'est jamais un diviseur de 0. En conséquence, tout corps est un anneau intègre (la réciproque est évidemment fausse).

Exemples 2.2.8
1. Si n est réductible, $\mathbf{Z}/n\mathbf{Z}$ n'est pas intègre : si $n = pq$ avec $p,q \geq 2$, $a := \overline{p}$ et $b := \overline{q}$ sont non nuls mais $ab = 0$. Si n est irréductible, $\mathbf{Z}/n\mathbf{Z}$ est intègre : si $a := \overline{p}$ et $b := \overline{q}$ sont tels que $ab = 0$, alors $n|pq$, donc $n|p$ ou $n|q$ (puisque n est premier), donc $a = 0$ ou $b = 0$.
2. Si X est réduit à un point, les anneaux $\mathcal{C}(X,\mathbf{R})$ et $\mathcal{C}(X,\mathbf{C})$ s'identifient respectivement à $\mathbf{R}$ et $\mathbf{C}$ (il n'y a que des fonctions constantes !) donc ils sont intègres. Si par exemple $X = \mathbf{R}$, les fonctions $x \mapsto x + |x|$ et $x \mapsto x - |x|$ sont continues et non nulles, mais leur produit est nul : donc les anneaux $\mathcal{C}(\mathbf{R},\mathbf{R})$ et $\mathcal{C}(\mathbf{R},\mathbf{C})$ ne sont pas intègres.
3. Les anneaux $A[[X]]$ et $A[X]$ sont intègres si, et seulement si, A est intègre.
4. Tous les autres exemples d'anneaux commutatifs cités sont intègres (le vérifier !).

Exercice 2.2.9 (Cours) Vérifier que, si $\mathbf{Z}/p\mathbf{Z}$, $p > 0$, est intègre, c'est un corps. (On reviendra sur cet exemple au chapitre 4.)

Remarque 2.2.10 Lorsque p est un nombre premier, il est d'usage de noter $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. Plus généralement, on démontre que, pour chaque entier $n \geq 1$, il y a (à isomorphisme près) un unique corps à $q := p^n$ éléments (Galois), que l'on note $\mathbf{F}_q$. On démontre aussi que $\mathbf{F}_q$ est commutatif (Wedderburn). Il ne faut pas confondre $\mathbf{F}_q$ avec $\mathbf{Z}/q\mathbf{Z}$: si $n \geq 2$, ce dernier anneau n'est même pas intègre, puisque $\dot{p}$ est nilpotent (pourquoi ?). D'ailleurs, le groupe additif obtenu en oubliant la multiplication de $\mathbf{F}_q$ n'est pas isomorphe à $\mathbf{Z}/q\mathbf{Z}$ (il n'est pas cyclique), mais à $(\mathbf{Z}/p\mathbf{Z})^n$ (voir le cours d'algèbre du premier semestre de M1, et, en attendant, le chapitre 4).

Nilpotents et idempotents. Un élément $a \in A$ est dit *nilpotent* s'il existe $n \geq 1$ tel que $a^n = 0$; et *idempotent* si $a^2 = a$. (Ces notions gardent un sens pour un anneau non commutatif.) Dans tout anneau, 0 est nilpotent, et 0 et 1 sont idempotents. Dans un anneau intègre, les réciproques sont vraies : 0 est le seul nilpotent, et 0 et 1 sont les seuls idempotents.

Exemples 2.2.11
1. Dans $\mathbf{Z}/4\mathbf{Z}$, le seul nilpotent non trivial (*i.e.* non nul) est $\overline{2}$ et il n'y a pas d'idempotents non triviaux (*i.e.* autres que 0 et 1).
2. Dans $\mathbf{Z}/6\mathbf{Z}$, le seul idempotent non trivial est $\overline{3}$ et il n'y a pas de nilpotents non triviaux.
3. Dans $\mathcal{C}(X,\mathbf{R})$ et $\mathcal{C}(X,\mathbf{C})$, il n'y a pas de nilpotents non triviaux. Un idempotent est une fonction à valeurs dans $\{0,1\}$; si X est connexe, il n'y a donc pas d'idempotents non triviaux.

2.3 Sous-anneaux

Définition 2.3.1 Un *sous-anneau* de l'anneau $(A,+,\times)$ est un sous-ensemble $A' \subset A$ tel que :
1. $(A',+)$ est un sous-groupe de $(A,+)$,
2. $1 \in A'$ et A' est stable pour la multiplication, *i.e.* si $a,b \in A'$ alors $ab \in A'$.

Il s'ensuit que $(A',+,\times)$ est un anneau ; on considèrera toujours un sous-anneau comme muni de cette *structure d'anneau induite*.

Remarque 2.3.2 Il découle de cette définition que $1_{A'} = 1_A$. Il peut arriver qu'un anneau A' soit inclus dans un anneau et que les lois de A' soient induites par celles de A sans pour autant que A' soit un sous-anneau de A. Par exemple, dans l'anneau $\mathbf{Z}/6\mathbf{Z}$, le sous-ensemble $3\mathbf{Z}/6\mathbf{Z}$ est un sous-groupe pour l'addition, il est stable pour la multiplication et c'est un anneau d'élément unité $\dot{3}$ (classe de 3 modulo $6\mathbf{Z}$) : ce n'est pourtant pas un sous-anneau, car il ne contient pas $\dot{1}$.

Exercice 2.3.3 (i) Soit e un idempotent d'un anneau commutatif A. Montrer que le sous-ensemble $A' := Ae = \{ae \mid a \in A\}$ est un sous-groupe pour l'addition, qu'il est stable pour la multiplication et que c'est un anneau d'élément unité e ; mais que ce n'est pas un sous-anneau si $e \neq 1$.
(ii) Prouver réciproquement que tout sous-groupe A' de A qui est stable pour la multiplication et admet un élément unité pour la multiplication est de cette forme.
(iii) Vérifier que l'exemple de la remarque ci-dessus est de ce type.

Sous-anneau de A engendré par une partie $E \subset A$. Il est clair que l'intersection d'une famille de sous-anneaux de A est un sous-anneau de A (c'en est un sous-groupe qui contient 1 et qui est stable pour la multiplication). Pour toute partie $E \subset A$, l'intersection de tous les sous-anneaux de

A qui contiennent E est donc le plus petit sous-anneau de A contenant E : on dit que c'est *le sous-anneau de A engendré par E*.
Ce sous-anneau contient évidemment tous les produits d'éléments de E (y compris le "produit vide" qui, par convention générale [2] vaut 1_A). Ce sous-anneau contient également toutes les expressions $\sum m_i x_i$ où les x_i sont des produits d'éléments de E et où les m_i sont des éléments de $\mathbf{Z}$. On vérifie sans peine (autrement dit : faites-le !) que ces expressions $\sum m_i x_i$ forment un sous-anneau de A, qui est donc le sous-anneau engendré par E.

Exemple 2.3.4 (Sous-anneau premier de A) Prenons $E := \emptyset$. Le sous-anneau engendré par E est alors le plus petit de tous les sous-anneaux de A, appelé *le sous-anneau premier de A*. Ses éléments sont les $m.1_A$. Notons A_0 le sous-anneau premier. C'est donc l'image du morphisme de groupes $\phi : \mathbf{Z} \to A$, $m \mapsto m.1_A$, $m \in \mathbf{Z}$. La règle $(m.a)(n.b) = (mn).ab$ implique en particulier que $\phi(mn) = \phi(m)\phi(n)$. Nous verrons plus loin (section 2.6) que ϕ est un "morphisme d'anneaux". Il y a lieu de distinguer deux cas :

1. Le noyau de ϕ est le sous-groupe $\{0\}$ de $\mathbf{Z}$. On a donc un isomorphisme de groupes $\phi : \mathbf{Z} \to A_0$. C'est même, en un sens intuitivement évident, un "isomorphisme d'anneaux". On peut donc identifier $m \in \mathbf{Z}$ avec $m.1_A \in A_0$ et l'anneau $\mathbf{Z}$ avec l'anneau A_0, ce que nous ferons. On dit dans ce cas que A *est de caractéristique nulle*.
2. Le noyau de ϕ est le sous-groupe $p\mathbf{Z}$ de $\mathbf{Z}$, $p > 0$. On en déduit donc un isomorphisme de groupes $\psi : \mathbf{Z}/p\mathbf{Z} \to A_0$. C'est même, en un sens intuitivement évident, un "isomorphisme d'anneaux". On peut donc identifier $\overline{m} \in \mathbf{Z}/p\mathbf{Z}$ avec $m.1_A \in A_0$ et l'anneau $\mathbf{Z}/pZ$ avec l'anneau A_0, ce que nous ferons. On dit dans ce cas que A *est de caractéristique* p.

Comme tout sous-anneau d'un anneau intègre est visiblement intègre, et comme $\mathbf{Z}/p\mathbf{Z}$, $p > 0$, n'est intègre que si p est premier, on voit que *la caractéristique d'un anneau intègre (en particulier d'un corps) est nulle, ou un nombre premier*. Dans le premier cas, le sous-anneau premier est $\mathbf{Z}$; dans le second cas, c'est le corps [3] $\mathbf{Z}/p\mathbf{Z}$. Ce corps est généralement noté $\mathbf{F}_p$.

Exercice 2.3.5 (Cours) 1) Soit K un corps commutatif de caractéristique nulle. Montrer que son plus petit sous-corps (*i.e.* sous-anneau qui est un corps) peut être identifié à $\mathbf{Q}$.
2) Soit K un corps commutatif de caractéristique $p > 0$. Quel est son plus petit sous-corps ?
(Dans les deux cas, ce plus-petit sous-corps s'appelle *sous-corps premier de K*.)

Remarque 2.3.6 Tous sous-anneau de A contient le sous-anneau premier A_0. Le sous-anneau de A engendré par E est donc le même que celui engendré par $A_0 \cup E$. On le note parfois $A_0[E]$, mais il ne faut pas confondre cette notation avec celle des anneaux de polynômes.

Exemple 2.3.7 (Sous-anneau engendré par un élément) Prenons $E := \{x\}$ où $x \in A$. Le sous-anneau engendré est formé des expressions $a_0.1_A + a_1.x + \cdots + a_m.x^m$, où $m \in \mathbf{N}$ et $a_i \in \mathbf{Z}$ pour $i = 0, \ldots, m$. On le note parfois $A_0[x]$. Selon la terminologie qui sera introsuite plus loin dans le cours, $A_0[x]$ est l'image de l'unique morphisme $A_0[X] \to A$ tel que $X \mapsto x$.

2. Pour toute loi interne sur un ensemble A, associative et admettant un élément neutre 1, et pour toute suite finie (x_i) d'éléments de A, on peut définir $\prod x_i$. Lorsque la suite est vide (de longueur 0) on convient que $\prod x_i = 1$. Cette convention est compatible avec la plupart des règles simples, et elle justifie par exemple les égalités connues $a^0 = 1$ et $0! = 1$.

3. Rappelons pourquoi c'est bien un corps : tout $x \in \mathbf{Z}/p\mathbf{Z}$ non nul est la classe d'un $a \in \mathbf{Z}$ qui n'est pas multiple de p, donc qui est premier avec p (puisque p est supposé premier). D'après le théorème de Bézout, on a $ua + vp = 1$ avec $u, v \in \mathbf{Z}$, et la classe de u dans $\mathbf{Z}/p\mathbf{Z}$ est l'inverse de x. Nous y reviendrons au chapitre 4.

Exemple 2.3.8 (Anneaux quadratiques) Si $d \in \mathbf{Z}$, on note $\sqrt{d}$ la racine carrée "usuelle" de d si $d \geq 0$, et $\sqrt{d} := \mathrm{i}\sqrt{-d}$ si $d < 0$. Le sous-anneau de $\mathbf{C}$ engendré par $\sqrt{d}$ est l'anneau :

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}.$$

En effet, tout anneau contenant $\sqrt{d}$ contient évidemment cet ensemble ; et celui-ci est un sous-anneau, parce que c'est un sous-groupe qui contient évidemment 1 et qui est stable par multiplication en vertu de l'égalité :

$$(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + ba')\sqrt{d}.$$

De même, soit $j := e^{2\mathrm{i}\pi/3} = \dfrac{-1+\sqrt{-3}}{2}$, de sorte que $j^2 + j + 1 = 0$. Le sous-anneau de $\mathbf{C}$ engendré par j est l'anneau :

$$\mathbf{Z}[j] = \{a + bj \mid a, b \in \mathbf{Z}\}.$$

En effet, tout anneau contenant j contient évidemment cet ensemble ; et celui-ci est un sous-anneau, parce que c'est un sous-groupe qui contient évidemment 1 et qui est stable par multiplication en vertu de l'égalité :

$$(a + bj)(a' + b'j) = (aa' - bb') + (ab' + ba' - bb')j.$$

Exercice 2.3.9 Si $x \in \mathbf{C}$ est tel que $x^n + p_1 x^{n-1} + \cdots + p_n = 0$, avec $p_1, \ldots, p_n \in \mathbf{Z}$, montrer que $\mathbf{Z}[x] = \{a_0 + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbf{Z}\}$ et (après avoir lu la section 2.4) que son corps des fractions est $\mathbf{Q}[x] = \{a_0 + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbf{Q}\}$.

Remarque 2.3.10 Un tel x est appelé *entier algébrique*. Les *anneaux quadratiques* comme $\mathbf{Z}[\sqrt{d}]$ sont des cas particuliers d'anneaux d'entiers algébriques ; ces derniers seront étudiés en M1.

2.4 Nombres algébriques et nombres transcendants

2.4.1 Nombres algébriques

Ce qui va suivre sera raconté dans le cadre de l'extension de corps $\mathbf{Q} \subset \mathbf{C}$, mais il existe une théorie analogue pour toute extension de corps $K \subset L$ (voir le cours d'algèbre de M1).

Soit x un nombre complexe et soit $\mathbf{Q}[x]$ le sous-anneau de $\mathbf{C}$ engendré par $\mathbf{Q}$ et x :

$$\mathbf{Q}[x] = \{a_0 + \cdots + a_n x^n \mid n \in \mathbf{N} \text{ et } a_0, \ldots, a_n \in \mathbf{Q}\}.$$

On voit donc que $\mathbf{Q}[x]$ est le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{C}$ engendré par la famille (infinie) des x^n, $n \in \mathbf{N}$. On distingue alors deux cas principaux.

Cas où la famille des x^n, $n \in \mathbf{N}$, est $\mathbf{Q}$-liée. Il existe donc une relation linéaire non triviale à coefficients rationnels entre les x^n, $n \in \mathbf{N}$:

$$a_0 + \cdots + a_n x^n + \cdots = 0,$$

les $a_n \in \mathbf{Q}$ non tous nuls. Remarquons que, par définition d'une relation linéaire, presque tous les a_n sont nuls : en effet, en algèbre, seules ont un sens les sommes finies (sinon, il faut faire intervenir de la topologie). On peut donc arrêter l'écriture de la relation linéaire ci-dessus au plus grand entier n tel que $a_n \neq 0$. Autrement dit, x est solution d'une équation algébrique non triviale $a_0 + \cdots + a_n x^n = 0$ à coefficients rationnels $a_0, \ldots, a_n \in \mathbf{Q}$, $n \geq 0$, $a_n \neq 0$. Il y a donc un polynôme $P \in \mathbf{Q}[X]$ non nul tel que $P(x) = 0$ (ici, P est de degré n).

Cas où la famille des x^n, $n \in \mathbf{N}$, est Q-libre. Cela revient à dire que l'application $P \mapsto P(x)$ de $\mathbf{Q}[X]$ dans $\mathbf{C}$ est injective, autrement dit, que x n'est solution d'aucune équation algébrique (non triviale) $a_0 + \cdots + a_n x^n = 0$ à coefficients rationnels $a_i \in \mathbf{Q}$ (non tous nuls). Il y a donc une bijection $P \mapsto P(x)$ de $\mathbf{Q}[X]$ sur $\mathbf{Q}[x]$ et les lois habituelles concernant l'évaluation : $(P+Q)(x) = P(x) + Q(x)$, $(PQ)(x) = P(x)Q(x)$, nous disent que le sous-anneau $\mathbf{Q}[x]$ de $\mathbf{C}$ est isomorphe à l'anneau $\mathbf{Q}[X]$ des polynômes. (Le mot "isomorphisme" ne sera défini qu'à la section 2.6 mais sa signification est évidente.) Par exemple, on en conclut que l'anneau $\mathbf{Q}[x]$ est loin d'être un corps ! (Ses seuls inversibles sont les éléments de $\mathbf{Q}^*$.)

Définition 2.4.1 On dit que x est un *nombre algébrique* s'il existe un polynôme $P \in \mathbf{Q}[X]$ non nul tel que $P(x) = 0$; dans le cas contraire, on dit que x est un *nombre transcendant*.

Exemples 2.4.2

1. Le nombre $\sqrt{2} + \sqrt{3}$ est algébrique.
2. Toutes les racines de l'unité $e^{2ki\pi/n}$, $k \in \mathbf{Z}$, $n \in \mathbf{N}^*$, sont des nombres algébriques.
3. On peut démontrer (Liouville) que $\sum_{n \geq 0} 10^{-n!}$ est un nombre transcendant ; en fait, ce n'est pas très difficile (voir RW1).
4. On peut aussi démontrer que e est transcendant (Hermite) ainsi que π (Lindeman), mais c'est beaucoup plus difficile !

Théorème 2.4.3 *Soit x un nombre algébrique et soit n le plus petit degré d'un polynôme $P \in \mathbf{Q}[X]$ non nul tel que $P(x) = 0$. Alors :*
(i) Le $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[x]$ est de dimension n, et $(1, x, \ldots, x^{n-1})$ en est une base.
(ii) L'anneau $\mathbf{Q}[x]$ est un corps.

Preuve. - (i) Les éléments $1, x, \ldots, x^{n-1}$ sont linéairement indépendants sur $\mathbf{Q}$, sinon il existerait un polynôme de $\mathbf{Q}[X]$ non nul et de degré $< n$ dont x soit racine.
Par hypothèse, x est solution d'une équation algébrique non triviale $a_0 + \cdots + a_n x^n = 0$ à coefficients rationnels $a_0, \ldots, a_n \in \mathbf{Q}$, $n \geq 0$, $a_n \neq 0$. On en déduit :

$$x^n = \alpha_0 + \cdots + \alpha_{n-1} x^{n-1}, \text{ où } \alpha_i := -a_i/a_n \in \mathbf{Q}.$$

Donc $x^n \in \mathrm{Vect}_{\mathbf{Q}}(1, x, \ldots, x^{n-1})$. Mais on a également $x^{n+p} = \alpha_0 x^p + \cdots + \alpha_{n-1} x^{n-1+p}$, d'où $x^{n+p} \in \mathrm{Vect}_{\mathbf{Q}}(x^p, x^{1+p}, \ldots, x^{n-1+p})$, d'où, par récurrence, $x^{n+p} \in \mathrm{Vect}_{\mathbf{Q}}(1, x, \ldots, x^{n-1})$. La suite $(1, x, \ldots, x^{n-1})$ est donc bien une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[x]$, qui est donc bien de dimension n.
(ii) Soit $y \in \mathbf{Q}[x]$ non nul. L'application $z \mapsto zy$ envoie $\mathbf{Q}[x]$ dans lui-même (stabilité de l'anneau $\mathbf{Q}[x]$ par multiplication) ; elle est $\mathbf{Q}$-linéaire (vérification immédiate, laissée au lecteur) ; elle est injective ($yz = 0 \Rightarrow z = 0$ puisque $y \neq 0$). C'est donc un endomorphisme injectif d'un espace vectoriel de dimension finie, donc un automorphisme. Puisque $1 \in \mathbf{Q}[x]$, il existe donc $z \in \mathbf{Q}[x]$ tel que $yz = 1$, autrement dit, tout élément non nul de l'anneau $\mathbf{Q}[x]$ est inversible, autrement dit, cet anneau est un corps. □

Nous démontrerons au chapitre 6 que la somme et le produit de deux nombres algébriques sont des nombres algébriques. À l'aide de la deuxième assertion du théorème ci-dessus (pour pouvoir inverser), on en déduit facilement que *l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est un sous-corps de* $\mathbf{C}$. On peut également démontrer que $\overline{\mathbf{Q}}$ est algébriquement clos, mais c'est plus compliqué (voir le cours de M1).

2.4.2 Presque tous les nombres complexes sont transcendants

Rappelons qu'un ensemble est dit *dénombrable* s'il peut être mis en bijection avec $\mathbf{N}$. Nous allons voir, sans théorie compliquée, que l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est dénombrable. Pour cela, pour tout $N \in \mathbf{N}^*$, nous noterons E_N l'ensemble des nombres complexes x qui sont solution d'une équation de la forme $a_0 + \cdots + a_n x^n = 0$, où $n \geq N$ et où les a_i sont des rationnels non tous nuls et de la forme p/q avec $p, q \in \mathbf{Z}$ et $|p|, |q| \leq N$. Le lecteur vérifiera (avec un petit peu de travail) les trois faits suivants : chaque E_N est un ensemble fini, notons n_N son cardinal ; ces ensembles forment une suite croissante $E_1 \subset E_2 \subset \cdots$; leur réunion est $\overline{\mathbf{Q}}$. On indexe donc successivement les éléments de $\bigcup E_N$ comme suit : les éléments de E_1 sont notés $x_1, \ldots, x_{n_1}$ (ordre arbitraire) ; ceux de $E_2 \setminus E_1$ sont notés $x_{n_1+1}, \ldots, x_{n_2}$; etc. Finalement, on voit que $(x_1, x_2, \ldots)$ est une *énumération* de $\overline{\mathbf{Q}}$, qui est donc bien dénombrable.

D'autre part, on sait par le cours de topologie que $\mathbf{R}$ n'est pas dénombrable, donc $\mathbf{C}$ non plus : ils ont la "puissance du continu" (c'est ainsi que l'on appelle le cardinal de $\mathbf{R}$). On en conclut que l'ensemble $\mathbf{C} \setminus \overline{\mathbf{Q}}$ n'est pas dénombrable, et même qu'il a la puissance du continu : il est "beaucoup plus gros" que $\overline{\mathbf{Q}}$. Autrement dit, dans leur écrasante majorité, les nombres complexes sont transcendants. En fait, on verra en cours d'intégration que tout ensemble dénombrable est "de mesure nulle". Cela peut s'interpréter géométriquement comme suit : le sous-ensemble $\overline{\mathbf{Q}}$ du plan a une aire nulle ! Et, probabilistement : si l'on tire au hasard un point dans un carré du plan, la probabilité qu'il corresponde à un nombre algébrique est nulle.

2.4.3 Suites et familles

On indexe souvent les éléments d'un ensemble de manière à les considérer comme élements d'une suite (finie ou non). Par exemple, si un sous-ensemble d'un espace vectoriel E est générateur et linéairement indépendant, il est commode de le noter $\{e_1, \ldots, e_n\}$ et de considérer la *famille* $(e_1, \ldots, e_n)$. Dans ce cas, c'est une *suite finie*, c'est-à-dire une application de $\{1, \ldots, n\}$ dans E.

On manipule également de cette manière des ensembles infinis ; par exemple, au lieu de considérer l'ensemble P des nombres premiers, il est commode d'en faire une suite $(p_1, p_2, \ldots)$, c'est-à-dire une application $i \mapsto p_i$ de $\mathbf{N}^*$ dans $\mathbf{Z}$ qui réalise une bijection avec P. On bénéficie alors de notations abrégées [4] comme $\prod_{i=1}^{+\infty} p_i^{r_i}$.

Si l'on veut indexer un ensemble non dénombrable, on ne peut le faire avec une suite. Par exemple, il n'y a pas de suite de polynômes $P_i \in \mathbf{C}[X]$, $i \in \mathbf{N}^*$, telle que tous les polynômes irréductibles unitaires soient représentés (ce sont les $X - a$, $a \in \mathbf{C}$, leur ensemble a la puissance du continu). La solution mathématique de ce dilemne est de remplacer l'application $i \mapsto P_i$ de $\mathbf{N}$ dans $\mathbf{C}[X]$ par une application d'un ensemble I dans $\mathbf{C}[X]$, que l'on notera encore $i \mapsto P_i$. En général, on ne précise pas l'ensemble I (qui est certainement très gros !) mais cela n'a pas d'importance, la plupart des calculs se déroulant de la même manière. On parle alors de *famille* $(P_i)_{i \in I}$ *indexée par l'ensemble* I.

4. Rappelons cependant qu'en algèbre un tel produit infini n'a de sens que si presque tous les facteurs, *i.e.* tous sauf un nombre fini d'entre eux, valent 1. De même, une combinaison linéaire $\sum_{i=1}^{+\infty} \alpha_i x_i$ dans un espace vectoriel n'a de sens que si presque tous les coefficients sont nuls.

2.5 Divisibilité

Dans toute cette section, l'anneau commutatif A est supposé intègre.

Soient $a, b \in A$. On dit que b *divise* a, ce que l'on note $b|a$, ou que a *est multiple de* b s'il existe $c \in A$ tel que $a = bc$. La relation "divise" est réflexive et transitive. On note $\mathrm{Div}(a)$ l'ensemble des diviseurs de a. L'ensemble des multiples de b est noté Ab ou bA. On dit que a et b sont *associés*, ce que l'on note $a \sim b$, si $a|b$ et $b|a$. C'est une relation d'équivalence. Les propriétés suivantes sont immédiates :

$$b|a \Longleftrightarrow b \in \mathrm{Div}(A) \Longleftrightarrow \mathrm{Div}(b) \subset \mathrm{Div}(a),$$

$$a \sim b \Longleftrightarrow \mathrm{Div}(a) = \mathrm{Div}(b) \Longleftrightarrow \exists u \in A^* \ : \ b = au,$$

$$\mathrm{Div}(0) = A, \quad \mathrm{Div}(1) = A^*, \quad \forall a \in A \ , \ A^* \subset \mathrm{Div}(A).$$

Exercice 2.5.1 (Cours) Pour quels $a \in A$ a-t'on $\mathrm{Div}(a) = A$? $\mathrm{Div}(a) = A^*$?

Définition 2.5.2 (i) L'élément non nul et non inversible $a \in A$ est dit *irréductible* si tous ses diviseurs sont inversibles ou lui sont associés, autrement dit, si $a = bc$ entraine $b \in A^*$ (et donc $c \sim a$) ou $c \in A^*$ (et donc $b \sim a$).
(ii) L'élément non nul et non inversible $a \in A$ est dit *premier* si $a|bc$ entraine $a|b$ ou $a|c$.

Proposition 2.5.3 *Tout élément premier de a est irréductible.*

Preuve. - Soit a premier et supposons que $a = bc$. Alors a divise b ou c (puisqu'il est premier), par exemple $a|b$: écrivons $b = ad$. On a donc $a = adc$, donc $dc = 1$ (puisque A intègre et $a \neq 0$) donc c est inversible. □

En général, la réciproque est fausse. Nous étudierons au chapitre 5 des anneaux dans lesquels elle est vraie. D'après le chapitre 1 section 1.3, $\mathbf{Z}$ et $K[X]$ sont des exemples de tels bons anneaux. En voici un mauvais.

Exemple 2.5.4 Soit $A := \mathbf{Z}[\sqrt{-3}] = \{p + q\sqrt{-3} \mid p, q \in \mathbf{Z}\}$ (*cf.* exemple 2.3.8 page 22). Nous allons montrer que 2 est irréductible mais non premier dans A. L'outil essentiel est l'application $z \mapsto N(z) := z\overline{z} = |z|^2$. Elle envoie A dans $\mathbf{N}$ puisque $N(p + q\sqrt{-3}) = p^2 + 3q^2$; et elle vérifie la propriété $N(ab) = N(a)N(b)$ (car l'application de conjugaison $z \mapsto \overline{z}$ la vérifie). On en déduit d'abord :

$$a \in A^* \Longleftrightarrow a \in A \text{ et } N(a) = 1.$$

En effet, si $a \in A$ est tel que $N(a) = a\overline{a} = 1$, alors clairement, $\overline{a} \in A$ est l'inverse de A. Réciproquement, si $a \in A^*$, soit $b \in A$ tel que $ab = 1$. Alors $N(a)N(b) = N(ab) = N(1) = 1$, donc $N(a) = 1$ puisque $N(a), N(b) \in \mathbf{N}$. Par ailleurs $N(p + q\sqrt{-3}) = p^2 + 3q^2 = 1$ avec $p, q \in \mathbf{Z}$ n'est possible que si $p = \pm 1$ et $q = 0$. Finalement, $A^* = \{+1, -1\}$.
Supposons maintenant $2 = ab$, $a, b \in A$. Alors $4 = N(2) = N(a)N(b)$. Or, $N(a), N(b) \in \mathbf{N}$. L'égalité $N(p + q\sqrt{-3}) = p^2 + 3q^2 = 2$ avec $p, q \in \mathbf{Z}$ est clairement impossible, on a donc $N(a) = 1$ et $N(b) = 4$ ou $N(a) = 4$ et $N(b) = 1$; donc a ou b est inversible, donc 2 est bien irréductible.
Montrons maintenant que 2 n'est pas premier dans A. Soient $a := 1 + \sqrt{-3}$ et $b := \overline{a} = 1 - \sqrt{-3}$. Alors $ab = 4 = 2 \times 2$, donc $2|ab$. Mais ni $a/2$ ni $b/2$ ne sont éléments de A, donc 2 ne divise ni a ni b, donc il n'est pas premier.

Exercice 2.5.5 Quels éléments $p \in \mathbf{Z}$ sont irréductibles dans $\mathbf{Z}[\sqrt{-3}]$?

Définition 2.5.6 (i) Les éléments $a, b \in A$ sont dits *premiers entre eux* si tous leurs diviseurs communs sont inversibles, *i.e.* $\mathrm{Div}(a) \cap \mathrm{Div}(b) = A^*$.
(ii) Les éléments $a, b \in A$ sont dits *étrangers* s'il existe $u, v \in A$ tels que $ua + vb = 1$. (Selon la terminologie du chapitre 3, cela signifie que la somme des idéaux Aa et Ab est $Aa + Ab = A$.)

Proposition 2.5.7 *Deux éléments étrangers sont premiers entre eux.*

Preuve. - Supposons que $ua + vb = 1$. Alors tout diviseur commun à a et b divise également $ua + vb = 1$, donc est inversible. □

En général, la réciproque est fausse. Nous étudierons au chapitre 5 des anneaux dans lesquels elle est vraie. D'après le théorème de Bézout (chapitre 1), $\mathbf{Z}$ et $K[X]$ sont des exemples de tels bons anneaux. En voici deux mauvais.

Exemples 2.5.8 (i) Dans $\mathbf{Z}[X]$, les éléments 2 et X sont premiers entre eux mais pas étrangers.
(ii) Dans $K[X, Y]$, les éléments X et Y sont premiers entre eux mais pas étrangers.

2.6 Morphismes

Définition 2.6.1 Un *morphisme* ou *homomorphisme* de l'anneau A dans l'anneau B est une application $f : A \to B$ qui est un morphisme de groupes de $(A, +)$ dans $(B, +)$ tel que $f(1_A) = 1_B$ et qui conserve la multiplication, *i.e.* $f(aa') = f(a)f(a')$ quels que soient $a, a' \in A$.

Notons que la condition $f(1_A) = 1_B$ ne découle pas de la troisième, comme le montre l'exemple de l'application constante 0_B. En revanche, on peut déduire de ces axiomes la propriété suivante : si $x \in A$ est inversible, alors $f(x)$ l'est aussi, et $f(x^{-1}) = f(x)^{-1}$; en effet, $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_A) = 1_B$ et $f(x^{-1})f(x) = f(x^{-1}x) = f(1_A) = 1_B$. On voit également que f induit un morphisme de groupes de A^* dans B^*.

Exercice 2.6.2 (Cours) Si A est un corps, montrer que tout morphisme d'anneau de A dans un anneau arbitraire B est injectif. (Si $x \neq 0$ considérer $f(xx^{-1})$.)

On retrouve tout le vocabulaire classique : *endomorphisme* (morphisme de A dans lui-même), *isomorphisme* (morphisme bijectif), *automorphisme* (endomorphisme bijectif) etc. De plus, le composé de deux morphismes d'anneaux est un morphisme d'anneaux et l'identité de l'anneau A en est un automorphisme. On notera $\mathrm{Hom}(A, B)$ l'ensemble des morphismes d'anneaux de A dans B et $\mathrm{End}(A) := \mathrm{Hom}(A, A)$. La définition du terme "isomorphisme" est justifiée par le fait évident que, si f est un morphisme bijectif, l'application réciproque est un morphisme. (En effet, le véritable sens du mot "isomorphisme" est "morphisme inversible pour la composition".) Dire que deux anneaux sont isomorphes, c'est dire qu'on ne peut les distinguer du point de vue algébrique, comme l'illustre l'exercice suivant.

Exercice 2.6.3 (Cours) Soit $f : A \to B$ un isomorphisme d'anneaux. Montrer que A est commutatif, resp. intègre, resp. un corps, si, et seulement si, B l'est. Montrer que $a \in A$ est inversible, resp. diviseur de zéro, resp. nilpotent, resp. idempotent, si, et seulement si, B l'est. Montrer que f induit un isomorphisme de groupes de A^* dans B^*.

Exemples 2.6.4

1. Pour tout anneau A, il y a un unique morphisme d'anneaux de $\mathbf{Z}$ dans A : il est défini par $m \mapsto m.1_A$. En effet, on doit avoir $1 \mapsto 1_A$, puis $m \mapsto m.1_A$, et l'on retrouve le morphisme déjà étudié dans la définition du sous-anneau premier.
2. Soit $\mathbf{Z}[X_1,\dots,X_n]$ le sous-anneau de $\mathbf{Q}[X_1,\dots,X_n]$ formé des polynômes à n indéterminées dont tous les coefficients sont entiers. (On vérifiera que c'est bien un sous-anneau !) Soient A un anneau commutatif et $a_1,\dots,a_n$ des éléments quelconques de A. Il y a alors un unique morphisme $f : \mathbf{Z}[X_1,\dots,X_n] \to A$ tel que $f(X_i) = a_i$ pour $i = 1,\dots,n$. En effet, on a alors nécessairement :

$$f\left(\sum_{i_1,\dots,i_n\geq 0} m_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}\right) = \sum_{i_1,\dots,i_n\geq 0} m_{i_1,\dots,i_n} a_1^{i_1}\cdots a_n^{i_n},$$

et, réciproquement, en définissant f par cette formule, on vérifie (Qui ? Mais vous, courageux lecteur !) que l'on obtient bien un morphisme.

Le deuxième exemple ci-dessus, pour formel qu'il soit, est à l'origine de la méthode de "transport des identités algébriques" aux conséquences étonnantes.

Une application du "transport des identités algébriques". Soit K un corps commutatif ; il découle du cours d'algèbre linéaire que l'on a $M\tilde{M} = \tilde{M}M = I_n$, où $M \in \mathrm{Mat}_n(K)$ et où l'on note $\tilde{M}$ la transposée de la matrice des cofacteurs de M ("formules de Cramer"). Ces formules reposent sur le théorie des espaces vectoriels, donc sur le fait que K est un corps. Nous allons les "transporter" dans un anneau commutatif arbitraire A.

Pour cela on pend pour K le corps $\mathbf{Q}(X_{1,1},\dots,X_{n,n})$ des fractions rationnelles en les n^2 indéterminées $X_{i,j}$, $1 \leq i,j \leq n$, et à coefficients dans $\mathbf{Q}$. Nous n'utiliserons que des propriétés évidentes de ce corps (essentiellement le fait qu'il contient l'anneau $\mathbf{Z}[X_{1,1},\dots,X_{n,n}]$).

Nous appliquons les formules de Cramer à la matrice $M \in \mathrm{Mat}_n(K)$ dont les composantes sont les $X_{i,j}$. Ces composantes appartiennent au sous-anneau $\mathbf{Z}[X_{1,1},\dots,X_{n,n}]$ de K engendré par les $X_{i,j}$, et il en est donc de même de $\det M$ et des composantes de $\tilde{M}$, puisque leur calcul ne fait intervenir aucune division. Ainsi, l'égalité $M\tilde{M} = I_n$ (par exemple) est-elle équivalente à la conjonction de n^2 égalités $P_{i,j}(X_{1,1},\dots,X_{n,n}) = 0$ dans l'anneau $\mathbf{Z}[X_{1,1},\dots,X_{n,n}]$.

Soit maintenant A un anneau commutatif quelconque et soit $N \in \mathrm{Mat}_n(A)$ une matrice carrée à coefficients dans A. Notons $a_{i,j} \in A$ ses n^2 composantes. Soit $f : \mathbf{Z}[X_{1,1},\dots,X_{n,n}] \to A$ l'unique morphisme d'anneaux tel que $f(X_{i,j}) = a_{i,j}$ pour $1 \leq i,j \leq n$. Puisque c'est un morphisme d'anneaux, on a :

$$f\left(P_{i,j}(X_{1,1},\dots,X_{n,n})\right) = P_{i,j}(f(X_{1,1}),\dots,f(X_{n,n})) = P_{i,j}(a_{1,1},\dots,a_{n,n});$$

on a utilisé pour cela le fait que chaque $P_{i,j}$ est un polynôme à coefficients entiers. On en déduit que $P_{i,j}(a_{1,1},\dots,a_{n,n}) = 0$ pour $1 \leq i,j \leq n$. Mais ces n^2 égalités signifient exactement que $N\tilde{N} = I_n$, ce que nous voulions démontrer. La relation $\tilde{N}N = I_n$ se démontre de la même manière.

Exercice 2.6.5 Comment caractériser les morphismes de $A[X]$ dans B ?

Anneau produit. Soit I un ensemble d'indices, et, pour tout $i \in I$, soit A_i un anneau. L'ensemble produit $A := \prod_{i\in I} A_i$ est formé des familles $(a_i)_{i\in I}$ indexées par I et telles que chaque a_i soit élément de A_i. Par exemple si $I = \{1,\dots,n\}$ on trouve le produit cartésien $A = A_1 \times \cdots \times A_n$.
On munit d'abord A de l'addition définie composante par composante :

$$(a_i)_{i\in I} + (b_i)_{i\in I} := (a_i + b_i)_{i\in I}.$$

On voit que $(A,+)$ est le produit des groupes $(A_i,+)$.

On munit ensuite A de la multiplication définie composante par composante :

$$(a_i)_{i\in I}(b_i)_{i\in I} := (a_i b_i)_{i\in I}.$$

On voit que la loi de composition obtenue est associative, distributive par rapport à l'addition et qu'elle possède un élément neutre $1_A := (1_{A_i})_{i\in I}$. Ainsi, on a fait de $(A,+,\times)$ un anneau appelé l'*anneau produit des A_i*.
Pour chaque indice particulier $i_0 \in I$, l'application f_{i_0} de A dans A_{i_0} qui associe à l'élément $(a_i)_{i\in I}$ sa composante d'indice i_0 :

$$f_{i_0}\left((a_i)_{i\in I}\right) := a_{i_0},$$

est un morphisme d'anneaux.
Soit maintenant B un anneau quelconque. En associant à tout morphisme $f \in \mathrm{Hom}(B,A)$ la famille des composés $f_i \circ f \in \mathrm{Hom}(B,A_i)$, on définit une application :

$$\mathrm{Hom}(B,A) \to \prod_{i\in I} \mathrm{Hom}(B,A_i).$$

Cette application est une bijection ; cette propriété (que l'on admettra) est la *propriété universelle du produit d'anneaux*.

Produit de deux anneaux. Le cas particulier le plus important est évidemment celui où $I := \{1,2\}$, *i.e.* celui de deux anneaux A_1 et A_2, que nous noterons plutôt A et B. Le produit cartésien $A \times B$ est muni des opérations définies par :

$$(a,b)+(a',b') := (a+a',b+b') \text{ et } (a,b).(a',b') := (aa',bb').$$

L'opposé de (a,b) est $(-a,-b)$, le neutre de l'addition est $(0,0)$, le neutre de la multiplication est $(1,1)$. L'élément (a,b) est inversible si, et seulement si, a et b le sont : $(A\times B)^* = A^* \times B^*$. Les deux projections $p : (a,b) \mapsto a$ et $q : (a,b) \mapsto b$ sont des morphismes d'anneaux.

Pour tout morphisme d'anneaux $f : C \to A \times B$, on en déduit des morphismes $p \circ f : C \to A$ et $q \circ f : C \to B$, d'où une application $f \mapsto (p\circ f, q\circ f)$:

$$\mathrm{Hom}(C,A\times B) \to \mathrm{Hom}(C,A) \times \mathrm{Hom}(C,B).$$

Réciproquement, si l'on a des morphismes $g : C \to A$ et $h : C \to B$, en posant $f(c) := (g(c),h(c))$, on définit un morphisme d'anneaux $f : C \to A \times B$ tel que $g = p \circ f$ et $h = q \circ f$. Autrement dit, l'application ci-dessus de $\mathrm{Hom}(C,A\times B)$ dans $\mathrm{Hom}(C,A) \times \mathrm{Hom}(C,B)$ est bijective.

Exercice 2.6.6 (Cours) Le sous-ensemble $A \times \{0\}$ de $A \times A$ en est-il un sous-anneau ? L'application $a \mapsto (a,0)$ de A dans $A \times A$ est-elle un morphisme d'anneaux ?

Anneau A^I. Un autre cas particulier est celui où tous les anneaux sont égaux : $A_i = A$. L'anneau produit est noté A^I, ses éléments sont toutes les familles (a_i) d'éléments de A indexées par I. Si au lieu de considérer une telle famille on considère l'application $i \mapsto a_i$ de I dans A, on voit que A^I s'identifie à l'anneau $\mathcal{F}(I,A)$ des applications de I dans A. Les opérations sont les suivantes : si $f,g \in \mathcal{F}(I,A)$, on définit $f+g$ comme l'application $i \mapsto f(i)+g(i)$ et fg comme l'application $i \mapsto f(i)g(i)$. L'élément neutre de l'addition est l'application constante 0, celui de la multiplication est l'application constante 1, etc.

2.7 Corps des fractions d'un anneau intègre commutatif

On a déjà vu que tout sous-anneau d'un corps est intègre. Le théorème suivant contient une réciproque de ce fait.

Théorème 2.7.1 *1) Pour tout anneau commutatif*[5] *intègre A, il existe un corps commutatif K contenant A et tel que tous les éléments de K sont de la forme a/b avec $a,b \in A$, $b \neq 0$.*
2) Le corps K est unique dans le sens suivant : si K' est un corps possédant les mêmes propriétés, il existe un unique isomorphisme d'anneaux de K sur K' dont la restriction à A soit l'identité.

Preuve. - 1) Notons que, dans un corps commutatif, la notation a/b est bien définie comme $ab^{-1} = b^{-1}a$. Elle possède de plus les propriétés suivantes :

$$\begin{aligned} &a/b = c/d \Longleftrightarrow ad = bc,\\ &a/b + c/d = (ad+bc)/(bd),\\ &a/b \times c/d = (ac)/(bd). \end{aligned}$$

Cela justifie la méthode qui va suivre pour la construction de K. Soit $E := A \times (A \setminus \{0\})$. On va définir sur l'ensemble E une relation binaire et deux lois de compositions internes :

$$\begin{aligned} &(a,b) \sim (c,d) \underset{def}{\Longleftrightarrow} ad = bc,\\ &(a,b) \oplus (c,d) := (ad+bc, bd),\\ &(a,b) \otimes (c,d) := (ac, bd). \end{aligned}$$

On vérifie alors sans peine (mais avec un peu de temps : au travail !) les faits suivants :

1. La relation $\sim$ est une relation d'équivalence sur E.
2. La relation $\sim$ est compatible avec les lois $\oplus$ et $\otimes$, autrement dit :

$$\forall x,x',y,y' \in E \ , \ x \sim x' \text{ et } y \sim y' \Longrightarrow x \oplus y \sim x' \oplus y' \text{ et } x \otimes y \sim x' \otimes y'.$$

On en conclut que l'ensemble quotient $K := E/\sim$ est muni de deux lois de composition internes $+$ et $\times$ telles que, si l'on note a/b la classe d'équivalence de (a,b), on ait $a/b + c/d = (ad+bc)/(bd)$ et $a/b \times c/d = (ac)/(bd)$ quels que soient $a,b,c,d \in A$, $b,d \neq 0$. On démontre alors (c'est fastidieux mais mécanique) que $(K,+,\times)$ est un anneau commutatif ; l'élément neutre de l'addition est $0_K := (0,1)$ et celui de la multiplication est $1_K := (1,1)$, etc. De plus, si $a/b \neq 0_K$, ce qui équivaut à $a \neq 0$, l'élément a/b est inversible d'inverse b/a. L'anneau K est donc un corps commutatif. Enfin, l'application $a \mapsto a/1$ est un morphisme injectif de l'anneau A dans l'anneau K, ce qui permet d'identifier A à un sous-anneau de K et chaque $a \in A$ à $a/1 \in K$. On voit alors que $a/b = ab^{-1}$.
2) Soit maintenant K' un corps commutatif contenant A et tel que tout élément de K' soit de la forme ab^{-1} avec $a,b \in A$ et $b \neq 0$. L'application $a/b \mapsto ab^{-1}$ de K dans K' est bien définie car si $a/b = c/d$ (égalité dans K mettant en jeu des éléments de A) alors $ab^{-1} = cd^{-1}$ (égalité dans K' mettant en jeu des éléments de A) : en effet, les deux égalités équivalent à $ad = bc$ (égalité dans A). L'application $a/b \mapsto ab^{-1}$ est visiblement un isomorphisme d'anneaux de K sur K' dont la restriction à A est l'identité, et c'est clairement le seul possible. □

5. Il existe des anneaux non commutatifs intègres qui ne sont contenus dans aucun corps (*cf.* le livre de Jacobson).

Définition 2.7.2 Le corps K est appelé *corps des fractions* de l'anneau commutatif intègre A.

L'unicité de K est en fait un cas particulier de la propriété universelle suivante qui dit qu'en un certain sens K est "le plus petit corps contenant l'anneau A" :

Proposition 2.7.3 *Soient K' un corps et $f : A \to K'$ un morphisme d'anneaux injectif. Il existe alors un unique morphisme d'anneaux $g : K \to K'$ dont la restriction à K soit f.*

Preuve. - On a nécessairement $g(a/b) = f(a)(f(b))^{-1}$, d'où l'unicité. Réciproquement, si l'on pose $g(a/b) := f(a)(f(b))^{-1}$, on voit que g est bien définie, *i.e.* si $a/b = c/d$ alors $f(a)(f(b))^{-1} = f(c)(f(d))^{-1}$. On vérifie ensuite que g est bien un morphisme d'anneaux de K dans K' dont la restriction à A est f. □

Exercice 2.7.4 (Cours) Soit f l'application de K dans K définie par $f(a/b) = (a+1)/(b+1)$. Calculer l'image de $0_K = 0/b$, $b \neq 0$, et conclure.

Exemples 2.7.5

1. Lorsque $A = \mathbf{Z}$, la construction du corps des fractions indiquée ci-dessus est la construction usuelle du corps $\mathbf{Q}$ des nombres rationnels.
   Tout nombre rationnel a/b admet une *écriture réduite* a_0/b_0 où $a_0, b_0 \in \mathbf{Z}$ sont premiers entre eux : il suffit en effet de poser $\delta := \text{pgcd}(a,b)$ puis $a_0 := a/\delta$, $b_0 := b/\delta$. De plus :
   - Deux écritures réduites a_0/b_0 et a'_0/b'_0 d'un même nombre rationnel sont telles que $a'_0 = \varepsilon a_0$, $b'_0 = \varepsilon b_0$, où $\varepsilon \in \mathbf{Z}^*$, *i.e.* $\varepsilon = \pm 1$. En particulier, tout nombre rationnel admet une unique écriture réduite à dénominateur positif, et c'est cette dernière que l'on choisira par défaut.
   - L'écriture réduite a_0/b_0 étant fixée, toutes les écritures du nombre rationnel correspondant sont de la forme $(ka_0)/(kb_0)$, où $k \in \mathbf{Z} \setminus \{0\}$. En effet :

     $$a/b = a_0/b_0 \Rightarrow ab_0 = a_0 b \Rightarrow b_0 | a_0 b \Rightarrow b_0 | b \text{ (en vertu du lemme de Gauß)},$$

     on peut donc poser $b = kb_0$ et le reste s'ensuit.
2. Lorsque $A = K[X]$, anneau des polynômes sur le corps commutatif K, on obtient le corps $K(X)$ des fractions rationnelles sur K. Toute fraction rationnelle A/B admet une *écriture réduite* A_0/B_0 où $A_0, B_0 \in K[X]$ sont premiers entre eux : il suffit en effet de poser $\Delta := \text{pgcd}(A,B)$ puis $A_0 := A/\Delta$, $B_0 := B/\Delta$. De plus :
   - Deux écritures réduites A_0/B_0 et A'_0/B'_0 d'une même fraction rationnelle sont telles que $A'_0 = cA_0$, $B'_0 = cB_0$, où $c \in K[X]^*$, *i.e.* $c \in K^*$. En particulier, toute fraction rationnelle admet une unique écriture réduite à dénominateur unitaire, et c'est cette dernière que l'on choisira par défaut.
   - L'écriture réduite A_0/B_0 étant fixée, toutes les écritures de la fraction rationnelle correspondante sont de la forme $(CA_0)/(CB_0)$, où $C \in K[X] \setminus \{0\}$. En effet :

     $$A/B = A_0/B_0 \Rightarrow AB_0 = A_0 B \Rightarrow B_0 | A_0 B \Rightarrow B_0 | B \text{ (en vertu du lemme de Gauß pour les polynômes)},$$

     on peut donc poser $B = CB_0$ et le reste s'ensuit.

Lorsque l'on part d'un anneau A qui est un sous-anneau d'un corps commutatif L connu, le corps des fractions est immédiatement donné comme sous-corps de L :

$$K = \{ab^{-1} \mid a, b \in A, b \neq 0\} \subset L,$$

où le calcul de ab^{-1} s'effectue dans L. En effet, le corps K ainsi défini vérifie les propriétés énoncées dans le théorème, c'est donc bien le corps des fractions.

Exemple 2.7.6 L'anneau $A := \mathbf{Z}[\sqrt{d}]$ (*cf.* exemple 2.3.8 page 22) est un sous-anneau de $\mathbf{C}$, son corps des fractions K est donc l'ensemble des nombres complexes de la forme $\dfrac{a'+b'\sqrt{d}}{a+b\sqrt{d}}$, $a,b,a',b' \in \mathbf{Z}$, a,b non tous deux nuls. En fait, ce corps des fractions est $K = \mathbf{Q}[\sqrt{d}] := \{x+y\sqrt{d} \mid x,y \in \mathbf{Q}\}$. En effet, tout quotient de deux éléments de A est dans $\mathbf{Q}[\sqrt{d}]$ en vertu du calcul suivant :

$$\frac{a'+b'\sqrt{d}}{a+b\sqrt{d}} = \frac{(a'+b'\sqrt{d})(a-b\sqrt{d})}{(a+b\sqrt{d})(a-b\sqrt{d})} = x+y\sqrt{d}, \text{ où } \begin{cases} x = \dfrac{a'a-db'b}{a^2-db^2}, \\ y = \dfrac{b'a-a'b}{a^2-db^2}. \end{cases}$$

Réciproquement, tout élément de $\mathbf{Q}[\sqrt{d}]$ est quotient de deux éléments de A en vertu du calcul suivant :

$$\frac{s}{t} + \frac{u}{v}\sqrt{d} = \frac{sv+ut\sqrt{d}}{tv+0.\sqrt{d}}.$$

Anneaux de fractions. Une partie S de l'anneau commutatif A est dite *multiplicative* si $1 \in S$, si S est stable pour la multiplication et si $0 \notin S$. Comme dans toute cette section, nous allons supposer que A est intègre. Soit K son corps des fractions. Notons S^{-1} l'ensemble des inverses s^{-1} des $s \in S$.

Proposition 2.7.7 *Le sous-anneau $A[S^{-1}]$ de K engendré par $A \cup S^{-1}$ est égal à l'*anneau de fractions *:*

$$S^{-1}A := \{a/s \mid a \in A, s \in S\}.$$

Preuve. - Il est évident d'une part que A et S^{-1} sont inclus dans $S^{-1}A$; d'autre part que tout élément de $S^{-1}A$ est le produit d'un élément de A et d'un élément de S^{-1}, et donc que $S^{-1}A \subset A[S^{-1}]$. Il suffit donc de vérifier que $S^{-1}A$ est un sous-anneau de K. Cela résulte immédiatement du fait que $0,1 \in S^{-1}A$ (évident) et des formules $a/s \pm b/t = (at \pm bs)/(st)$ et $(a/s)(b/t) = (ab)/(st)$, jointes au fait que $s,t \in S \Rightarrow st \in S$. □

Exemples 2.7.8

1. Soit $p \in \mathbf{N}^*$. Prenons $A := \mathbf{Z}$ et $S := \{p^n \mid n \in \mathbf{N}\}$. L'anneau de fractions $S^{-1}A$ est alors noté $\mathbf{Z}[1/p]$. C'est l'ensemble des nombre rationnels de la forme a/p^n.
2. Soit $p \in \mathbf{N}^*$ un nombre premier. Prenons $A := \mathbf{Z}$ et pour S l'ensemble des entiers relatifs qui ne sont pas multiples de p : comme p est premier, c'est bien une partie multiplicative. L'anneau de fractions $S^{-1}A$ est alors noté $\mathbf{Z}_{(p)}$. C'est l'ensemble des nombre rationnels de la forme a/b, où b n'est pas multiple de p.
3. Soit $a \in \mathbf{C}$. Prenons $A := \mathbf{C}[X]$ et $S := \{P \in \mathbf{C}[X] \mid P(a) \neq 0\}$. L'anneau de fractions $S^{-1}A$ est formé des fractions rationnelles R telles que l'évaluation $R(a)$ a un sens.

Exercice 2.7.9 Voyez-vous une similarité entre les deux derniers exemples ?

2.8 Exercices sur le chapitre 2

Exercice 2.8.1 (Cours) Dans un anneau commutatif A, démontrer la *formule du multinôme* :

$$\forall p \in \mathbf{N}^* \ , \ \forall a_1, \ldots, a_p \in A \ , \ \forall n \in \mathbf{N} \ , \ (a_1 + \cdots + a_p)^n = \sum_{\substack{k_1, \ldots, k_p \geq 0 \\ k_1 + \cdots + k_p = n}} \frac{n!}{k_1! \cdots k_p!} a_1^{k_1} \cdots a_p^{k_p}.$$

Exercice 2.8.2 (Cours) On appelle *ordre de nilpotence* de $a \in A$ (anneau commutatif) :

$$\nu(a) := \inf\{n \in \mathbf{N} \mid a^n = 0\}.$$

Par convention, c'est donc $+\infty$ si a n'est pas nilpotent. Montrer que $\nu(a+b) \leq \nu(a) + \nu(b) - 1$.

Exercice 2.8.3 1) Soient a et b deux idempotents de l'anneau commutatif A tels que $ab = 0$ (on dit alors qu'ils sont *orthogonaux*). Montrer que $a+b$ est idempotent. Vérifier que le produit de deux idempotents quelconques est idempotent.
2) Soient a et b deux idempotents quelconques. Montrer que $a(1-b)$ et $b(1-a)$ sont des idempotents orthogonaux et que $a \star b := a + b - 2ab$ est idempotent.
3) Montrer que l'ensemble des idempotents muni des lois $\star$ et . (multiplication de A) est un anneau.

Exercice 2.8.4 1) Soit A un anneau intègre fini. Montrer que c'est un corps.
2) Peut-on appliquer ce résultat à $\mathbf{Z}/m\mathbf{Z}$?

Exercice 2.8.5 (Cours) Soient A un anneau commutatif, B un sous-anneau et E une partie quelconque. Décrire le sous-anneau $B[E]$ de A engendré par $B \cup E$.

Exercice 2.8.6 1) Soit A un anneau non nécessairement commutatif. Montrer que son *centre* $Z(A) := \{a \in A \mid \forall x \in A \ , \ ax = xa\}$ en est un sous-anneau.
2) Déterminer le centre de tous les anneaux donnés en exemple dans le cours.
3) Étendre l'exercice précédent au cas d'un anneau A non commutatif, mais tel que $B \subset Z(A)$ ("sous-anneau central").

Exercice 2.8.7 Montrer que dans l'anneau $\mathcal{C}(\mathbf{R}, \mathbf{R})$, il n'y a aucun élément irréductible.

Exercice 2.8.8 1) Soit d un entier non carré. Si $d < 0$, on posera $\sqrt{d} := \mathrm{i}\sqrt{-d}$. Vérifier que l'application $(a,b) \mapsto a + b\sqrt{d}$ est injective de $\mathbf{Z}^2$ dans $\mathbf{C}$ et que son image est le sous-anneau $A := \mathbf{Z}[\sqrt{d}]$ de $\mathbf{C}$ engendré par $\sqrt{d}$.
2) Pour $z := a + b\sqrt{d} \in A$, on pose $\overline{z} := a - b\sqrt{d}$ et $N(z) := z\overline{z}$. (Attention : l'application $z \mapsto \overline{z}$ ne coïncide avec la conjugaison de $\mathbf{C}$ que si $d < 0$.) Vérifier que $z \mapsto \overline{z}$ est un automorphisme de l'anneau $(A, +)$.
3) Vérifier que l'application N envoie A dans $\mathbf{Z}$ et que $N(zz') = N(z)N(z')$.
4) Montrer que $z \in A$ est inversible si, et seulement si, $N(z) = \pm 1$.
5) Montrer que $p \in \mathbf{Z}$ est un élément irréductible de A si, et seulement si, p est premier dans $\mathbf{Z}$ et que ni p ni $-p$ ne sont de la forme $a^2 - db^2$ avec $a, b \in \mathbf{Z}$.
6) On prend $d := -6$. Trouver dans A un élément irréductible non premier.

Exercice 2.8.9 1) Soit d un entier non carré tel que $d \equiv 1 \pmod 4$. On pose :

$$x := \frac{1+\sqrt{d}}{2} \text{ et } \overline{x} := \frac{1-\sqrt{d}}{2}\cdot$$

Vérifier que l'application $(a,b) \mapsto a+bx$ est injective de $\mathbf{Z}^2$ dans $\mathbf{C}$ et que son image est le sous-anneau $A := \mathbf{Z}[x]$ de $\mathbf{C}$ engendré par x.
2) Pour $z := a+bx \in A$, on pose $\overline{z} := a+b\overline{x}$ et $N(z) := z\overline{z}$. Reprendre les questions de l'exercice précédent.
3) Application : $d := -3$.

Exercice 2.8.10 (Cours) Déterminer tous les automorphismes de $\mathbf{Z}$, de $\mathbf{Z}/m\mathbf{Z}$.

Exercice 2.8.11 1) Dans le produit d'anneaux commutatifs $\prod A_i$, déterminer les inversibles, les nilpotents, les idempotents et les diviseurs de zéro.
2) Donner une condition nécessaire et suffisante d'intégrité de ce produit.

Exercice 2.8.12 1) Soit $\mathcal{P}(E)$ l'ensemble des parties de E. On le munit de la loi définie par :

$$A \oplus B := (A \setminus B) \cup (B \setminus A).$$

Vérifier que l'on obtient ainsi un groupe commutatif dans lequel chaque élément est son propre opposé.
2) On munit également $\mathcal{P}(E)$ de la loi définie par :

$$A.B := A \cap B.$$

Vérifier que l'on obtient ainsi un anneau commutatif. Déterminer les inversibles, les diviseurs de 0, les idempotents et les nilpotents de cet anneau et en caractériser la relation de divisibilité.
3) Pour tout $A \subset E$ on définit la fonction caractéristique χ_A de E dans $\mathbf{Z}/2\mathbf{Z}$ par $\chi_A(x) = \dot{1}$ si $x \in A$, et 0 autrement. Vérifier que l'application qui associe à un élément $A \in \mathcal{P}(E)$ l'élément $\chi_A \in (\mathbf{Z}/2\mathbf{Z})^E$ est un isomorphisme d'anneaux.

Exercice 2.8.13 1) Soit $e \neq 0,1$ un idempotent non trivial de l'anneau commutatif A. On a vu (exercice 2.3.3) que les opérations de A induisent une structure d'anneau sur le sous-ensemble $Ae := \{ae \mid a \in A\}$, mais que ce n'est pas un sous-anneau. Montrer que $a \mapsto ae$ est un morphisme surjectif d'anneaux de A sur Ae. Quel est son noyau ?
2) Soit $f := 1-e$. Vérifier que c'est un idempotent et que l'application $a \mapsto (ae, af)$ est un isomorphisme d'anneaux de A sur l'anneau produit $Ae \times Af$.

Exercice 2.8.14 On appelle *saturé* d'une partie multiplicative S de l'anneau commutatif intègre A l'ensemble $\overline{S}$ des diviseurs des éléments de S. Montrer que c'est une partie multiplicative de A, que $(S^{-1}A)^*$ est égal à $\overline{S}$ et que $\overline{S}^{-1}A = S^{-1}A$.

Exercice 2.8.15 Soit $\overline{S}$ le saturé de la partie multiplicative S de l'anneau commutatif A. Vérifier que le morphisme canonique de $S^{-1}A$ dans $\overline{S}^{-1}A$ est un isomorphisme.

Exercice 2.8.16 1) Soient A, B deux anneaux commutatifs, $S \subset A$ et $T \subset B$ des parties multiplicatives et $f : A \to B$ un morphisme tel que $f(S) \subset T$. Définir un morphisme $S^{-1}A \to T^{-1}B$ et énoncer sa propriété caractéristique.
2) Appliquer au cas de deux anneaux intègres et de leurs corps des fractions.

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 :

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

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

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

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

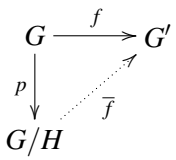
$$\forall x,y,x',y' \in G \text{ , } \overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{y'} \Longrightarrow \overline{x+y} = \overline{x'+y'}.$$

On en déduit que la définition suivante a un sens :

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

(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.

Chapitre 4

Compléments d'arithmétique de Z

4.1 L'anneau $\mathbf{Z}/m\mathbf{Z}$

Soit $m \in \mathbf{N}$, $m \geq 2$. L'anneau $\mathbf{Z}/m\mathbf{Z}$ est le quotient de l'anneau $\mathbf{Z}$ par l'idéal principal $m\mathbf{Z}$. Il n'est pas trivial. Ses éléments sont les classes de congruence $\overline{0}$, ..., $\overline{m-1}$, où l'on note $\overline{a} := a \pmod{m}$, classe d'équivalence pour la relation :

$$\forall a, b \in \mathbf{Z}\ ,\ a \equiv b \pmod{m} \underset{def}{\Longleftrightarrow} m|a-b.$$

Cette relation d'équivalence est compatible avec l'addition et la multiplication de $\mathbf{Z}$, ce qui donne un sens aux définitions suivantes :

$$\forall a, b \in \mathbf{Z}\ ,\ \overline{a}+\overline{b} := \overline{a+b} \text{ et } \overline{a}\overline{b} := \overline{ab}.$$

On obtient ainsi un anneau commutatif $(\mathbf{Z}/m\mathbf{Z}, +, \times)$ et un morphisme surjectif $a \mapsto \overline{a}$, $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$.

Lemme 4.1.1 *(i) Pour que $\overline{a} \in \mathbf{Z}/m\mathbf{Z}$ soit inversible, il faut, et il suffit, que $a \in \mathbf{Z}$ soit premier avec m.*
(ii) Les éléments inversibles de $\mathbf{Z}/m\mathbf{Z}$ sont les $\overline{a}$ pour $a \wedge m = 1$ et $1 \leq a \leq m-1$.

Preuve. - (i) D'après le théorème de Bézout, a est premier avec m si, et seulement si, il existe $u, v \in \mathbf{Z}$ tels que $ua + vm = 1$. Cette condition équivaut à : il existe $u \in \mathbf{Z}$ tel que $au \equiv 1 \pmod{m}$, ou encore à : il existe $x \in \mathbf{Z}/m\mathbf{Z}$ tel que $\overline{a}x = \overline{1}$, *i.e.* à l'inversibilité de $\overline{a}$ (la dernière équivalance utilise implicitement que tout $x \in \mathbf{Z}/m\mathbf{Z}$ est de la forme $\overline{u}$, $u \in \mathbf{Z}$).
(ii) Puisque tout élément de $\mathbf{Z}/m\mathbf{Z}$ est de la forme $\overline{a}$, $0 \leq a \leq m-1$ et puisque $\overline{0}$ n'est pas inversible, la deuxième assertion découle directement de la première. □

Théorème 4.1.2 *Les propriétés suivantes sont équivalentes :*
(i) L'entier m est irréductible.
(ii) L'entier m est premier.
(iii) L'anneau $\mathbf{Z}/m\mathbf{Z}$ est intègre.
(iv) L'anneau $\mathbf{Z}/m\mathbf{Z}$ est un corps.

Preuve. - Les relations logiques $(iv) \Rightarrow (iii)$, $(iii) \Leftrightarrow (ii)$ et $(ii) \Rightarrow (i)$ sont évidemment valables dans tout anneau intègre. On va donc prouver que $(i) \Rightarrow (iv)$. Supposons donc m irréductible. Pour tout $a \in \mathbf{Z}$, $a \wedge m$ divise m, donc est égal à 1 ou à m (irréductibilité). Dans le premier cas, $\overline{a}$ est inversible d'après le lemme. Dans le second cas, $m|a$, donc $\overline{a} = \overline{0}$. Ainsi, tout élément de $\mathbf{Z}/m\mathbf{Z}$ est nul ou inversible : c'est bien un corps. □

Dans le cas général, par application directe du chapitre 3 (section 3.3), on voit que les idéaux de $\mathbf{Z}/m\mathbf{Z}$ sont les $n\mathbf{Z}/m\mathbf{Z}$ pour $n \in \mathrm{Div}(m)$, que ses idéaux premiers ou maximaux sont les mêmes et que ce sont les $n\mathbf{Z}/m\mathbf{Z}$ pour $n \in \mathrm{Div}(m)$, n premier.

On écrit dorénavant $m = p_1^{r_1} \cdots p_k^{r_k}$ la décomposition de m en facteurs premiers. Par convention, pour toute écriture de ce type, les p_i sont des nombres premiers deux à deux distincts et les r_i sont non nuls [1]. Puisque $m > 1$, nous avons ici de plus $k \geq 1$.

Il est facile de voir (et laissé en exercice amusant) que $a \in \mathbf{Z}$ admet une puissance multiple de m si, et seulement si, a est multiple de $p_1 \cdots p_k$. Les nilpotents de $\mathbf{Z}/m\mathbf{Z}$ forment donc l'idéal $p_1 \cdots p_k \mathbf{Z}/m\mathbf{Z}$: c'est le nilradical de $\mathbf{Z}/m\mathbf{Z}$. En particulier, pour que l'anneau $\mathbf{Z}/m\mathbf{Z}$ soit *réduit* (c'est-à-dire sans nilpotents non triviaux), il faut, et il suffit, que $r_1 = \cdots = r_k = 1$. Un tel entier est dit *sans facteurs carrés* ou *quadratfrei*.

Théorème 4.1.3 (Lemme chinois) *L'application* $x \pmod m \mapsto (x \pmod{p_1^{r_1}}, \cdots, x \pmod{p_k^{r_k}})$ *est un isomorphisme de* $\mathbf{Z}/m\mathbf{Z}$ *sur* $\prod_{i=1} \mathbf{Z}/p_i^{r_i}\mathbf{Z}$.

Preuve. - C'est une application directe du lemme chinois général (théorème 3.3.16 du chapitre 3, section 3.3), mais nous allons donner une preuve plus "constructive" de la surjectivité (l'injectivité est facile). Il s'agit, $a_1, \ldots, a_k \in \mathbf{Z}$ étant donnés, de résoudre le système de congruences : $a \equiv a_i \pmod{p_i^{r_i}}$, $i = 1, \ldots, k$.
On commence par appliquer le théorème de Bézout (et donc l'algorithme d'Euclide) pour trouver $u_i, v_i \in \mathbf{Z}$ tels que :

$$u_i p_i^{r_i} + v_i P_i' = 1, \text{ où l'on a posé } P_i' := \prod_{\substack{1 \leq j \leq k \\ j \neq i}} p_j^{r_j}.$$

On pose alors $x_i := v_i P_i'$, de sorte que $x_i \equiv 1 \pmod{p_i^{r_i}}$ et $x_i \equiv 0 \pmod{p_j^{r_j}}$ pour $j \neq i$. Il est alors immédiat que $a := a_1 x_1 + \cdots + a_k x_k$ est solution du système de congruences.
En termes de bijectivité : l'unique antécédent de $(a_1 \pmod{p_1^{r_1}}, \cdots, a_k \pmod{p_k^{r_k}}) \in \prod_{i=1} \mathbf{Z}/p_i^{r_i}\mathbf{Z}$ est $a \pmod m \in \mathbf{Z}/m\mathbf{Z}$. □

Exercice 4.1.4 (Cours) Démontrer l'injectivité.

Remarque 4.1.5 La méthode ci-dessus n'est pas réellement praticable. Il y en a une meilleure dans le volume II de "The Art of Computer Programming" de Donald Knuth.

1. Cette dernière convention sera modifiée à la section 4.3.

4.2 Le groupe $(\mathbf{Z}/m\mathbf{Z})^*$ et l'indicatrice d'Euler

Définition 4.2.1 Pour tout $m \geq 2$, on note $\phi(m)$ le nombre des entiers de $\{1,\ldots,m-1\}$ qui sont premiers avec m. On pose de plus $\phi(1) := 1$. La fonction ϕ est appelée *indicatrice d'Euler*.

Corollaire 4.2.2 *Le groupe $(\mathbf{Z}/m\mathbf{Z})^*$ des éléments inversibles de $\mathbf{Z}/m\mathbf{Z}$ a $\phi(m)$ éléments.*

Preuve. - Si $m \geq 2$, cela découle de la description des inversibles à la section précédente (lemme 4.1.1). Pour $m = 1$, l'anneau $\mathbf{Z}/m\mathbf{Z}$ est trivial et le groupe $(\mathbf{Z}/m\mathbf{Z})^*$ aussi. (Dans ce cas, 0 est inversible !) □

Lemme 4.2.3 *Si $m = p^r$, p premier, $r \geq 1$ (un tel nombre est dit* primaire*), alors :*

$$\phi(m) = p^r - p^{r-1} = m(1-1/p).$$

Preuve. - Les entiers qui ne sont pas premiers avec p^r sont les multiples de p, les éléments non inversibles de $\mathbf{Z}/m\mathbf{Z}$ sont donc les p^{r-1} classes $\overline{a}$, où $a = pb$, $0 \leq b < p^{r-1}$; les inversibles sont les $(p^r - p^{r-1})$ autres classes. □

Dans ce cas, les non-inversibles forment un idéal (l'idéal $p\mathbf{Z}/m\mathbf{Z}$), l'anneau est "local" (*cf.*l'exercice 3.6.8 du chapitre 3).

Lemme 4.2.4 *Si m et n sont premiers entre eux, $\phi(mn) = \phi(m)\phi(n)$. (On dit que la fonction ϕ est* multiplicative.*)*

Preuve. - Du lemme chinois, on déduit un isomorphisme d'anneaux $\mathbf{Z}/mn\mathbf{Z} \simeq (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$. D'après l'exercice 2.8.11 du chapitre 2, pour deux anneaux commutatifs quelconques on a une égalité :

$$(A \times B)^* = A^* \times B^*$$

On a donc ici $(\mathbf{Z}/mn\mathbf{Z})^* \simeq (\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$ et la conclusion vient en prenant les cardinaux. □

Théorème 4.2.5 *Soit $m = p_1^{r_1} \cdots p_k^{r_k}$ la décomposition de m en facteurs premiers. Alors :*

$$\phi(m) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}) = m(1-1/p_1) \cdots (1-1/p_k).$$

Preuve. - C'est immédiat à l'aide des deux lemmes. □

Théorème 4.2.6 (Euler) *Soit $a \in \mathbf{Z}$ tel que $a \wedge m = 1$. Alors $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Preuve. - En effet, d'après le théorème de Lagrange, l'élément $x := \overline{a}$ du groupe $(\mathbf{Z}/m\mathbf{Z})^*$ vérifie $x^{\phi(m)} = 1$. □

Théorème 4.2.7 (Petit théorème de Fermat) *Si p est premier et $a \in \mathbf{Z}$, alors $a^p \equiv a \pmod{p}$.*

Preuve. - Si a est multiple de p, c'est clair. Sinon, $a \wedge p = 1$ et comme $\phi(p) = p-1$, le théorème d'Euler ci-dessus donne $a^{p-1} \equiv 1 \pmod{p}$, d'où la conclusion en multipliant par a. □

Remarque 4.2.8 La réciproque est fausse. Soit en effet $m := 561 = 3 \times 11 \times 17$. Pour tout $a \in \mathbf{Z}$, on a $a^{561} \equiv a \pmod{561}$: on dit que 561 est un *nombre de Carmichael*. Pour prouver la congruence ci-dessus, il suffit de prouver que $a^{561} - a$ est (séparément) multiple de 3, de 11 et de 17. Voyons l'exemple de la congruence modulo 3. Si a est multiple de 3, elle est évidente. Sinon, d'après le deuxième cas du petit théorème de Fermat, $a^2 \equiv 1 \pmod{3}$, donc, en élevant à la puissance 280, $a^{560} \equiv 1 \pmod{3}$, donc, en multipliant par a, $a^{561} \equiv a \pmod{3}$. On en conclut que le petit théorème de Fermat fournit une condition *nécessaire* mais *pas suffisante* de primalité.

Exercice 4.2.9 Traiter de même les congruences modulo 11 et modulo 17.

Théorème 4.2.10 (Wilson) [2] *L'entier naturel p est premier si, et seulement si, on a la congruence* $(p-1)! \equiv -1 \pmod{p}$.

Preuve. - Si p vérifie cette congruence, tout diviseur strict de p divise $(p-1)!+1$, et comme il divise évidemment $(p-1)!$, il divise 1.
Supposons réciproquement que p soit premier. On regroupe alors les éléments $\overline{1}, \ldots, \overline{p-1}$ du groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^* = (\mathbf{Z}/p\mathbf{Z}) \setminus \{0\}$ par paires d'inverses. Le produit de tous ces éléments, *i.e.* la classe de $(p-1)!$, est donc égal au produit des éléments qui sont leur propre inverse, c'est-à-dire tels que $x^2 = 1$. Puisque nous sommes dans un corps, ces éléments sont $+1$ et -1, dont le produit est bien -1. □

Exercice 4.2.11 Dans la dernière étape de la démonstration, que se passe-t-il si $1 = -1$?

Remarque 4.2.12 Le théorème de Wilson fournit une condition nécessaire et suffisante de primalité. Cependant, les calculs impliqués le rendent impraticable pour un nombre p un peu grand (ce qui est le cas dans les applications pratiques à la cryptographie, à la génération de nombres aléatoires, etc). Pour des tests de primalité plus efficaces, voir le "Cours d'algèbre" de Demazure et le cours optionnel d'algorithmique au second semestre de L3.
Pour des applications basées sur l'étude du groupe $(\mathbf{Z}/m\mathbf{Z})^*$ (cryptographie, générateurs pseudo-aléatoires ...), voir les mêmes références ainsi que le cours optionnel "Mathématiques-Informatique" du premier semestre de L1.

4.3 Valuations

Nous notons maintenant $p_1, p_2, \ldots$ la suite croissante de tous les nombres premiers, *i.e.* $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Tout entier relatif non nul $m \in \mathbf{Z} \setminus \{0\}$ s'écrit donc de manière unique :

$$m = \varepsilon p_1^{r_1} p_2^{r_2} \cdots \text{ où } \varepsilon \in \mathbf{Z}^* = \{+1, -1\} \text{ et } r_1, r_2, \ldots \in \mathbf{N} \text{ sont presque tous nuls.}$$

La dernière condition signifie que tous les r_i sont nuls, sauf un nombre fini d'entre eux, ou encore qu'ils sont tous nuls à partir d'un certain rang. Elle entraîne que presque tous les facteurs primaires

2. Selon Demazure, ce critère est du à Ibn al Haytam, au Xème siècle !

$p_i^{r_i}$ sont égaux à 1, donc que ce produit infini n'en est pas vraiment un.

Dans l'écriture ci-dessus, il est visible que p_i^r divise m si, et seulement si, $r \leq r_i$. Cela justifie la définition suivante.

Définition 4.3.1 Pour tout $m \in \mathbf{Z}$ et pour tout nombre premier $p \in P := \{p_1, p_2, \ldots\}$, on note $v_p(m)$ la borne supérieure des entiers r tels que p^r divise m :

$$v_p(m) := \sup\{r \in \mathbf{N} \mid p^r | m\}.$$

La fonction v_p est appelée *valuation p-adique*.

Si $m = 0$, $v_p(m) = +\infty$ pour tout $p \in P$. Si $m \neq 0$, $v_p(m) \in \mathbf{N}$ pour tout $p \in P$ et $v_p(m)$ est nul pour presque tout $p \in P$. De plus :

$$\prod_{p \in P} p^{v_p(m)} = |m|.$$

Les deux propriétés suivantes sont évidentes et fondamentales ; pour $a, b \in \mathbf{Z}$:

$$v_p(a+b) \geq \min(v_p(a), v_p(b)),$$
$$v_p(ab) = v_p(a) + v_p(b).$$

(Ce sont ces deux propriétés qu'exprime le mot "valuation".) De plus :

$$a|b \Longleftrightarrow \forall p \in P\ ,\ v_p(a) \leq v_p(b).$$

Grâce à la propriété $v_p(ab) = v_p(a) + v_p(b)$, on peut étendre la définition de $v_p(x)$ à des rationnels $x \in \mathbf{Q}$: il suffit de poser $v_p(a/b) := v_p(a) - v_p(b)$. En effet, si $a/b = a'/b'$, on a $ab' = a'b$ d'où $v_p(a) + v_p(b') = v_p(a') + v_p(b)$ d'où $v_p(a) - v_p(b) = v_p(a') - v_p(b')$ (les soustractions sont possibles parce que $v_p(b), v_p(b')$ ne sont pas infinis) et donc le calcul de $v_p(x)$ ne dépend pas d'une écriture particulière $x = a/b$. Si $x \neq 0$, l'entier $r := v_p(x)$ est caractérisé par le fait que $x = p^r u/v$ où $u, v \in \mathbf{Z} \setminus p\mathbf{Z}$.

Les propriétés précédentes se généralisent directement. Si $x \in \mathbf{Q}^*$, presque tous les $v_p(x)$ sont nuls et l'on a :

$$\prod_{p \in P} p^{v_p(x)} = |x|.$$

Les deux propriétés suivantes sont encore vérifiées pour $x, y \in \mathbf{Q}$:

$$v_p(x+y) \geq \min(v_p(x), v_p(y)),$$
$$v_p(xy) = v_p(x) + v_p(y).$$

De plus :

$$x \in \mathbf{Z} \Longleftrightarrow \forall p \in P\ ,\ v_p(x) \geq 0.$$

Exemple 4.3.2 Voici une application à un problème célèbre : prouver que $\sqrt{2}$ est irrationnel. Si $x \in \mathbf{Q}$ était tel que $x^2 = 2$, on aurait $1 = v_2(2) = 2v_2(x)$, ce qui est impossible puisque $v_2(x) \in \mathbf{Z}$. Plus généralement, on voit que $y \in \mathbf{Q}^*$ est le carré d'un rationnel si, et seulement s'il est positif et tous les $v_p(x)$ sont pairs.

Voici une généralisation de la propriété précédente.

Théorème 4.3.3 *L'anneau* $\mathbf{Z}$ *est* intégralement clos *(voir explication avec la preuve).*

Preuve. - La propriété signifie que tout élément du corps des fractions de $\mathbf{Z}$ qui est un entier algébrique sur $\mathbf{Z}$ est dans $\mathbf{Z}$. Soit donc $x \in \mathbf{Q}$ tel que $x^n + p_1 x^{n-1} + \cdots + p_n = 0$, avec $p_1, \ldots, p_n \in \mathbf{Z}$. Pour tout $p \in P$, on a $nv_p(x) = v_p(-x^n) = v_p(p_1 x^{n-1} + \cdots + p_n)$, d'où :

$$nv_p(x) \geq \min\big(v_p(p_1 x^{n-1}), \ldots, v_p(p_n)\big) \geq \min\big(v_p(x^{n-1}), \ldots, 0\big) \geq \min\big((n-1)v_p(x), \ldots, 0\big),$$

ce qui n'est possible que si $v_p(x) \geq 0$. □

Exemple 4.3.4 Montrons que $\sqrt{2}+\sqrt{3}$ est irrationnel. C'est un entier algébrique, car racine de l'équation $x^4 - 10x + 1 = 0$. S'il était rationnel, il serait entier en vertu du théorème. Mais, par petit calcul direct, $1,4 < \sqrt{2} < 1,5$ et $1,7 < \sqrt{3} < 1,8$, d'où $3,1 < \sqrt{2}+\sqrt{3} < 3,3$.

4.4 L'anneau Z[i] des entiers de Gauß

Une question fondamentale en théorie des nombres est la suivante : si p est un nombre premier naturel, donc un élément irréductible et premier de l'anneau $\mathbf{Z}$, reste-t-il premier, resp. irréductible dans un anneau d'entiers algébriques ? À titre de justification partielle de l'interêt de cette question, nous allons étudier le cas de $\mathbf{Z}[\mathrm{i}]$ et (au chapitre 5) l'appliquer à la détermination des sommes de deux carrés dans $\mathbf{N}$ (résultat dû à Fermat).

Soit p un nombre premier. On le considère comme un élément de $\mathbf{Z}[\mathrm{i}]$.

Théorème 4.4.1
- *si* -1 *est un carré dans* $\mathbf{F}_p$, p *n'est pas premier dans* $\mathbf{Z}[i]$;
- *si* -1 *n'est pas un carré dans* $\mathbf{F}_p$, p *est premier dans* $\mathbf{Z}[i]$ *(et l'idéal* $< p >$ *de* $\mathbf{Z}[i]$ *est même maximal).*

Preuve. - Nous avons vu à la sous-section 3.3.2 que le morphisme $P \mapsto P(\mathrm{i})$ de $\mathbf{Z}[X]$ dans $\mathbf{C}$ induit un isomorphisme $\mathbf{Z}[X]/ < X^2+1 > \simeq \mathbf{Z}[\mathrm{i}]$. L'anneau quotient $\mathbf{Z}[\mathrm{i}]/ < p >$ est donc isomorphe au quotient de $\overline{A} = A/I = \mathbf{Z}[X]/ < X^2+1 >$ par l'idéal $\overline{J}$ de $\overline{A}$ engendré par p. L'idéal $\overline{J}$ est l'image de l'idéal J de $A = \mathbf{Z}[X]$ engendré par p. D'après le corollaire 3.3.11 de la sous-section 3.3.2, on a donc :

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

Par ailleurs, en appliquant le même corollaire dans l'autre sens, on voit que $\mathbf{Z}[X]/ < X^2+1, p >$ s'obtient en quotient $\mathbf{Z}[X]$ par $< p >$, puis le quotient par l'image de $< X^2+1 >$. Rappelons que, p étant premier, $\mathbf{Z}/p\mathbf{Z}$ est le corps $\mathbf{F}_p$. Il est facile de voir que $\mathbf{Z}[X]/ < p >$ s'identifie à $\mathbf{F}_p[X]$. On obtient donc l'isomorphisme :

$$\mathbf{Z}[X]/ < X^2+1, p > \simeq \mathbf{F}_p[X] < X^2+1 > .$$

D'après la sous-section 3.4.3, c'est un corps si, et seulement si, X^2+1 est irréductible dans $\mathbf{F}_p[X]$; pour un polynôme de degré 2, cela équivaut à ne pas avoir de racine. Dans le cas contraire, X^2+1 est réductible dans $\mathbf{F}_p[X]$ et l'anneau n'est même pas intègre. □

Définition 4.4.2 Soit $m \in \mathbf{N}^*$ un entier naturel non nul. On dit que $a \in \mathbf{Z}$ est *résidu quadratique modulo m* s'il est congru modulo m à un carré.

Il revient au même de dire que $\overline{a}$ est un carré dans $\mathbf{Z}/m\mathbf{Z}$.

Exercice 4.4.3 Quels sont les résidus quadratiques modulo m pour $m = 1, 2, 3$?

Corollaire 4.4.4 *Pour que p soit premier dans $\mathbf{Z}[i]$, il faut, et il suffit, que -1 ne soit pas résidu quadratique modulo p.*

Exercice 4.4.5 Quels sont les nombres premiers $p \leq 100$ tels que -1 soit résidu quadratique modulo p ?

Il est clair que -1 est résidu quadratique modulo 2. Voici un critère pour les nombres premiers impairs.

Théorème 4.4.6 *Soit p un nombre premier impair.*
(i) Pour tout $x \in {\mathbf{F}_p}^*$ soit un carré, on a $x^{(p-1)/2} = \pm 1$.
(ii) Pour que $x \in {\mathbf{F}_p}^*$ soit un carré, il faut, et il suffit, que $x^{(p-1)/2} = 1$.

Preuve. - (i) D'après le théorème de Lagrange, tout élément du groupe à $(p-1)$ éléments ${\mathbf{F}_p}^*$ vérifie $x^{p-1} = 1$. Comme $p-1$ est pair, cette égalité s'écrit $(x^{(p-1)/2})^2 = 1$, d'où $(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = 0$, d'où ($\mathbf{F}_p$ étant intègre) $x^{(p-1)/2} = \pm 1$.
(ii) Si x est un carré, $x = y^2$, on a $x^{(p-1)/2} = y^{p-1} = 1$. C'est la réciproque qui est plus difficile à démontrer.
On considère le morphisme de groupes $y \mapsto y^2$ de ${\mathbf{F}_p}^*$ dans lui-même. Son noyau est $\{1, -1\}$ (on vient de voir que ce sont les seuls éléments dont le carré est 1). De plus, $1 \neq -1$ puisque $p \neq 2$. Le noyau a donc 2 élements. D'après le premier théorème d'isomorphisme pour les groupes, l'image est isomorphe à ${\mathbf{F}_p}^*$ quotienté par le noyau, donc elle a exactement $(p-1)/2$ éléments. Il y a donc exactement $N := (p-1)/2$ carrés dans ${\mathbf{F}_p}^*$. Notons les $x_1, \ldots, x_N$.
Chacun de ces $(p-1)/2$ carrés vérifie $x^{(p-1)/2} = 1$, donc est racine du polynôme $P := X^{(p-1)/2} - 1$. Par comparaison des degrés et coefficients dominants, on voit que P est le produit des $X - x_i$, donc n'admet pas d'autre racine que les x_i. On en déduit que tout élément tel que $x^{(p-1)/2} = 1$ est un carré. □

Corollaire 4.4.7 *Pour que -1 soit résidu quadratique modulo p, il faut, et il suffit, que $p = 2$ ou $p \equiv 1 \pmod 4$.*

Preuve. - Le cas où $p = 2$ a été vu plus haut. Dans le cas où p est impair, on applique le théorème, en remarquant que $(-1)^{(p-1)/2} = 1$ si $p \equiv 1 \pmod 4$ et -1 sinon. Or on ne peut avoir $-1 \equiv 1 \pmod p$. □

Corollaire 4.4.8 *Le nombre premier p reste premier dans $\mathbf{Z}[i]$ si, et seulement si, $p \equiv -1 \pmod 4$.*

Exemple 4.4.9 L'anneau $\mathbf{Z}[\mathrm{i}]/ < 3 >$ est un corps isomorphe à $\mathbf{F}_9 := \mathbf{F}_3[X]/ < X^2 + 1 >$. Si l'on note (abusivement ?) i la classe de X dans ce corps, on voit que les éléments de $\mathbf{F}_9$ sont les $a + b\mathrm{i}$, $a, b \in \mathbf{F}_3$: c'est donc un corps à 9 éléments. On verra en M1 que c'est le seul (à un isomorphisme près).

4.5 Exercices sur le chapitre 4

Exercice 4.5.1 Pour tous $a, b \in \mathbf{Z}$, démontrer que $ab(a^{60} - b^{60})$ est multiple de 56786730.

Exercice 4.5.2 1) Soient p un nombre premier et $r \geq 1$. Montrer que les seuls idempotents de $\mathbf{Z}/p^r\mathbf{Z}$ sont $\dot{0}$ et $\dot{1}$.
2) En quoi peut-on en déduire que le lemme chinois est "optimal" ?
3) Relier la première question à la propriété d'être un anneau local.

Exercice 4.5.3 1) Soit p un nombre premier impair. Démontrer que, pour tout $k \geq 0$, on a $(1+p)^{p^k} = 1 + p^{k+1}x$ avec x entier non multiple de p.
2) En déduire que l'élément $1 + p \pmod{p^m}$ du groupe $(\mathbf{Z}/p^m\mathbf{Z})^*$ est d'ordre p^{m-1}.

Exercice 4.5.4 Soit $m \in \mathbf{N}^*$ et soit $d \in \mathbf{N}^*$ un diviseur de m. Dénombrer les entiers a de $\{1, \ldots, m\}$ tels que $a \wedge m = d$ et en déduire la formule :

$$\sum_{d|m} \phi(d) = m.$$

Exercice 4.5.5 1) Soit p premier. Montrer que pour tout diviseur d de $p-1$, il y a, dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$, au plus d éléments dont l'ordre divise d.
2) A l'aide de l'exercice précédent, en déduire que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.
3) Démontrer de même que, si K est un corps commutatif, tout sous-groupe fini de K^* est cyclique.

Exercice 4.5.6 1) Soit p premier. On note x un générateur du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^*$ (voir l'exercice précédent). Soit $m \geq 1$, et soit $y \in \mathbf{Z}/p^m\mathbf{Z}$ un antécédent de x par le morphisme canonique $\mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. Montrer que $y \in (\mathbf{Z}/p^m\mathbf{Z})^*$ et que son ordre est de la forme $(p-1)q$. Quel est l'ordre de l'élément $z := y^q$?
2) On suppose p impair. Montrer que $(\mathbf{Z}/p^m\mathbf{Z})^*$ est cyclique.

Exercice 4.5.7 1) On note $\lfloor x \rfloor$ la partie entière du réel x. Montrer que le nombre de $a \in \{1, \ldots, m\}$ tels que $v_p(a) \geq r$ est égal à $\lfloor m/p^r \rfloor$. En déduire la formule :

$$v_p(m!) = \sum_{r \geq 1} \lfloor m/p^r \rfloor.$$

2) Utiliser cette formule pour démontrer que, si $0 \leq n \leq m$, alors $\dfrac{m!}{n!(m-n)!}$ est un entier.

Exercice 4.5.8 Calculer $v_p(a \wedge b)$ et $v_p(a \vee b)$ (on note $a \vee b$ le ppcm de a et b). En déduire une égalité remarquable au sujet de $(a \wedge b)(a \vee b)$.

Exercice 4.5.9 Pour tout $x \in \mathbf{Q}$, on pose :

$$|x|_p := p^{-v_p(x)}.$$

Montrer que $d_p(x,y) := |x-y|_p$ définit une distance *ultramétrique* sur $\mathbf{Q}$; autrement dit, l'inégalité du triangle est remplacée par l'inégalité plus forte :

$$d_p(x,z) \leq \max\big(d_p(x,y), d_p(y,z)\big).$$

Exercice 4.5.10 Dénombrer les solutions de $x^2 = 1$ dans $\mathbf{Z}/n\mathbf{Z}$. (Cette formule sert en cryptographie, *cf.* le théorème de Rabin dans le livre de Demazure.)

Chapitre 5

Anneaux factoriels

Dans tout ce chapitre, tous les anneaux sont supposés commutatifs (et unitaires).

5.1 Définition des anneaux factoriels

Ce sont les anneaux dans lesquels il y a une "bonne" théorie de la divisibilité et de la factorisation, *i.e.* ceux dans lequel le "théorème fondamental de l'arithmétique" est valable. Nous allons donc nous intéresser à la possibilité de décomposer tout élément (non nul et non inversible) d'un anneau intègre A en produit d'irréductibles, et à l'éventuelle unicité d'une telle décomposition.

Une telle unicité ne peut être prise au sens littéral, comme le montre l'exemple de $\mathbf{Z}$ où l'on a $6 = 2 \times 3 = (-2) \times (-3)$: il est impératif de prendre en compte la présence d'éléments inversibles. Rappelons que, dans tout anneau intègre, p et q sont dits associés, ce que l'on note $p \sim q$, si $\mathrm{Div}(p) = \mathrm{Div}(q)$; de manière équivalente : $Ap = Aq$; de manière encore équivalente : il existe $\varepsilon \in A^*$ tel que $q = \varepsilon p$. Rappelons aussi que, si $p \sim q$, alors p est irréductible (resp. premier) si, et seulement si, q l'est.

Nous dirons donc qu'il y a unicité de la décomposition (éventuelle) en produit d'irréductibles si l'on a la propriété suivante : quels que soient les irréductibles $p_1, \ldots, p_r, q_1, \ldots, q_s$ de A,

$$p_1 \cdots p_r = q_1 \cdots q_s \Longrightarrow \big(r = s \text{ et } \exists \sigma \in \mathcal{S}_n \ , \ q_1 \sim p_{\sigma(1)}, \ldots, q_r \sim p_{\sigma(r)}\big)$$

Sous cette forme, la propriété n'est pas très maniable. Pour l'améliorer un peu, nous ferons le choix d'un ensemble de représentants [1] des éléments irréductibles pour la relation d'association $\sim$; nous noterons P cet ensemble. Autrement dit, $P \subset A$ est formé d'irréductibles et :

$$\forall q \text{ irréductible de } A \ , \ \exists ! p \in P \ : \ q \sim p.$$

De plus, nous écrirons P comme l'ensemble des éléments d'une famille :

$$P = \{p_i \mid i \in I\}.$$

1. La notion d'ensemble de représentants est bien définie pour toute relation d'équivalence sur un ensemble. L'existence d'un ensemble de représentants est conséquence d'un principe mystérieux de la théorie des ensembles, l'*Axiome du Choix*. Cependant, dans tous les exemples que nous rencontrerons (en L3 mais aussi en M1), il sera possible de construire explicitement un tel ensemble P sans faire appel à l'Axiome du Choix.

Alors tout produit d'irréductibles dans A peut s'écrire sous la forme $\varepsilon \prod_{i\in I} p_i^{r_i}$, où $\varepsilon \in A^*$ et où les r_i sont des entiers naturels presque tous nuls ; sous forme plus concise : $(r_i)_{i\in I} \in \mathbf{N}^{(I)}$. Avec ces notations, on voit qu'il y a unicité de la décomposition (éventuelle) en produit d'irréductibles si l'on a la propriété suivante :

$$\forall \varepsilon, \eta \in A^* \ , \ \forall (r_i)_{i\in I}, (s_i)_{i\in I} \in \mathbf{N}^{(I)} \ , \ \varepsilon \prod_{i\in I} p_i^{r_i} = \eta \prod_{i\in I} p_i^{s_i} \Longrightarrow \varepsilon = \eta \text{ et } \forall i \in I \ , \ r_i = s_i.$$

Théorème 5.1.1 *Soit A un anneau intègre. On suppose que tout élément non nul et non inversible de A est produit d'éléments irréductibles. Pour qu'il y ait dans A unicité de la décomposition en produit d'irréductibles, il faut, et il suffit, que tout irréductible de A soit premier.*

Preuve. - Supposons que tout irréductible de A soit premier. Supposons que $\varepsilon \prod_{i\in I} p_i^{r_i} = \eta \prod_{i\in I} p_i^{s_i}$ (avec les notations ci-dessus). Posons $r_i' := r_i - \min(r_i, s_i)$ et $s_i' := s_i - \min(r_i, s_i)$. Pour tout i, on a donc $r_i' = 0$ ou $s_i' = 0$. On va montrer que tous les r_i', s_i' sont nuls, ce qui impliquera $r_i = s_i$ et $\varepsilon = \eta$. Pour cela, on divise l'égalité ci-dessus par $\prod_{i\in I} p_i^{\min(r_i,s_i)}$, ce qui donne $\varepsilon \prod_{i\in I} p_i^{r_i'} = \eta \prod_{i\in I} p_i^{s_i'}$. Si par exemple $r_i' \neq 0$, alors p_i divise le membre de gauche, donc le membre de droite, donc l'un des $p_j^{s_j'}$ puisqu'il est premier par hypothèse. Mais c'est impossible pour $j \neq i$, et aussi pour $j = i$ car $s_i' = 0$. (Notons que, pour démontrer cette implication, nous n'avons pas eu besoin d'invoquer l'*existence* de la décomposition en produit d'irréductibles de tout élément de A.)
Supposons réciproquement qu'il y ait dans A unicité de la décomposition en produit d'irréductibles. Soit p un irréductible et soient $a, b, c \in A$ tels que $pc = ab$. Si a (resp. b) est inversible, alors p divise b (resp. a). Si ni a ni b ne sont inversibles, ils sont par hypothèse produits d'irréductibles : $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$. De la décomposition de c en produit d'irréductibles, de l'égalité $n := pc = p_1 \cdots p_r q_1 \cdots q_s$ et de l'unicité de la décomposition de n, on déduit que p est associé à l'un des p_i ou à l'un des q_j, donc qu'il divise a ou b. □

Définition 5.1.2 Un anneau A est dit *factoriel* si tout élément non nul et non inversible de A est produit d'irréductibles et si la décomposition en produits d'irréductibles est unique.

Corollaire 5.1.3 *Soit A un anneau factoriel et soit P un ensemble de représentants de ses éléments irréductibles. Alors tout élément non nul de A admet une unique écriture $\varepsilon \prod_{i\in I} p_i^{r_i}$, où $\varepsilon \in A^*$ et où $(r_i)_{i\in I} \in \mathbf{N}^{(I)}$.*

Remarque 5.1.4 Un cas limite de la définition ci-dessus est celui où il n'y a aucun élément irréductible : l'anneau est alors un corps. (Il est d'ailleurs également euclidien et principal, voir plus loin).

5.2 Les deux implications : euclidien, principal, factoriel

5.2.1 Euclidien implique principal

Dans le programme de L3, les principaux exemples d'anneaux factoriels sont les anneaux principaux ; et la manière la plus fréquente de prouver qu'un anneau est principal est de prouver qu'il est euclidien. On rencontre des définitions variées de ce dernier terme, celle qui suit est raisonnablement standard.

Définition 5.2.1 L'anneau (commutatif, unitaire) A est dit *euclidien* s'il est intègre et s'il possède un *stathme euclidien*, c'est-à-dire une application $g : A \setminus \{0\} \to \mathbf{N}$ telle que :

$$\forall x,x' \in A, x,x' \neq 0 \ , \ g(x) \leq g(xx'),$$
$$\forall x,y \in A, x \neq 0 \ , \ \exists q,r \in A \ : \ y = qx + r \text{ et } \big(r = 0 \text{ ou } g(r) < g(x)\big).$$

Remarquons que la fonction g n'est pas définie en 0, d'où une description par cas un peu lourde de la *division euclidienne* $x = qy + r$.

Exemples 5.2.2
1. L'anneau $\mathbf{Z}$ muni du stathme $g(x) := |x|$ $(x \neq 0)$ est euclidien.
2. L'anneau $K[X]$ muni du stathme $g(P) := \deg P$ $(P \neq 0)$ est euclidien.
3. L'anneau $\mathbf{Z}[\mathrm{i}]$ muni du stathme $g(z) := |z|$ $(z \neq 0)$ est euclidien (exercice 3.6.3).

Exercice 5.2.3 Montrer que le cas d'un stathme g identiquement nul correspond à un corps.

Théorème 5.2.4 *Tout anneau euclidien est principal.*

Preuve. - Soit I un idéal non trivial de l'anneau euclidien A (muni du stathme g). Soit $x \in I$ un élément non nul tel que l'entier $g(x)$ soit minimum. Il est *a priori* évident que $Ax \subset I$, nous allons montrer l'inclusion réciproque, ce qui permettra de conclure.
Soit donc $y \in I$ et soit $y = qx + r$ la division euclidienne : alors $r = y - qx \in I$. Si r était non nul, on aurait $g(r) < g(x)$, en contradiction avec la propriété de minimalité qui définit x ; on a donc $r = 0$, donc $y = qx$, donc $y \in Ax$. □

Remarque 5.2.5 Comme on va le voir (proposition 5.2.9), dans tout anneau principal, deux éléments a et b quelconques admettent un pgcd et des coefficients de Bézout. Dans le cas d'un anneau euclidien, on peut les calculer grâce à l'algorithme d'Euclide :

```
x := a; y := b; u := 1; v := 0; s := 0; t := 1;
tant que y > 0
   (q,r) := diveucl(x,y);
   x := y; q := r;
   (u,v,s,t) := (s,t,u-qs,v-qt);
rendre(x,u,v);;
```

La justification est la même que dans le cas de $\mathbf{Z}$: ici c'est l'entier $g(y)$ qui diminue strictement à chaque étape, assurant la terminaison ; et l'invariant de boucle $\mathrm{Div}(x) \cap \mathrm{Div}(y) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$, que l'on déduit de la formule (facile à prouver) $\mathrm{Div}(qy + r) \cap \mathrm{Div}(y) = \mathrm{Div}(y) \cap \mathrm{Div}(r)$, nous garantit qu'à la fin on a bien $\mathrm{Div}(x) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$. Le lecteur complètera cet argument pour prendre en compte la relation de Bézout.

5.2.2 Principal implique factoriel

Lemme 5.2.6 *Dans tout ensemble ordonné $(E, \prec)$, il y a équivalence entre les deux propriétés suivantes :*
(i) toute suite croissante de E est stationnaire ;
(ii) toute partie non vide de E admet un élément maximal.

Preuve. - Supposons (ii) vérifiée et soit $x_0 \prec x_1 \prec \cdots$ une suite croissante. Soit $F := \{x_n \mid n \in \mathbf{N}\}$, donc une partie non vide de E : par hypothèse, elle admet un élément maximal x_m. Alors, pour $n \geq m$, l'inégalité large $x_m \prec x_n$ ne peut être stricte (puisque x_m est maximal), donc $x_m = x_n$ et la suite stationne au rang m.
Pour établir la réciproque, nous démontrerons sa contraposée. Nous supposons donc que la partie non vide F de E n'admet pas d'élément maximal, et nous construisons par récurrence une suite strictement croissante $(x_n)_{n\in\mathbf{N}}$. L'élément x_0 est arbitraire dans F (qui est supposée non vide). Le terme $x_n \in F$ étant construit, on prend pour x_{n+1} un majorant strict de x_n dans F (c'est possible puisque x_n n'est pas maximal par hypothèse sur F). Il est clair que la suite construite est strictement croissante. □

Lemme 5.2.7 *Soit $I_0 \subset I_1 \subset \cdots$ une suite croissante d'idéaux d'un anneau commutatif A. Alors $I := \bigcup I_n$ est un idéal de A.*

Preuve. - Naturellement $0 \in I$. Si $x, y \in I$, alors il existe p, q tels que $x \in I_p$, $y \in I_q$ et donc $x + y \in I_{\max(p,q)} \subset I$. Enfin, si $a \in A$ et $x \in I$, il existe p tel que $x \in I_p$, donc $ax \in I_p \subset I$. □

Lemme 5.2.8 *Dans un anneau principal, toute suite croissante d'idéaux est stationnaire. Toute famille non vide d'idéaux admet un élément maximal (*i.e. *qui n'est strictement inclus dans aucun autre élément de la famille).*

Preuve. - Nous allons démontrer la première propriété, la seconde en découlera d'après le lemme 5.2.6. Soit donc $I_0 \subset I_1 \subset \cdots$ une suite croissante d'idéaux de l'anneau principal A. d'après le lemme 5.2.7, $I := \bigcup I_n$ est un idéal de A. C'est donc un idéal principal : $I = Aa$ pour un certain $a \in I$. Il existe p tel que $a \in I_p$, donc $I \subset I_p$, d'où $I = I_n$ pour tout $n \geq p$. (Selon une terminologie qui sera introduite en M1, on dit que tout anneau principal est "noetherien".) □

Proposition 5.2.9 *Dans un anneau principal, le "théorème de Bézout" est vérifié,* i.e. *deux éléments a, b quelconques ont un pgcd d qui de la forme $d = ua + vb$, $u, v \in A$ (et bien entendu tout pgcd est de cette forme).*

Preuve. - L'idéal $Aa + Ab$ est principal : $Aa + Ab = Ad$. On applique alors la proposition 3.1.3 du chapitre 3. L'assertion entre parenthèses vient de ce que tous les pgcd sont associés entre eux. □

Remarque 5.2.10 On n'a pas pleinement utilisé la principalité de A, seulement le fait que tout idéal engendré par deux éléments est principal. Un anneau intègre vérifiant cette propriété est appelé "anneau de Bézout".

Proposition 5.2.11 *Dans un anneau principal, le "lemme d'Euclide" est vérifié,* i.e. *tout irréductible est premier.*

Preuve. - Soit p un irréductible de l'anneau principal A. Pour démontrer que p est premier, nous supposons que p divise ab et que p ne divise pas a. Puisque p est irréductible, un pgcd de p et a est inversible ou associé à p (puisqu'il divise p qui est irréductible) ; dans le deuxième cas, p diviserait a, contredisant l'hypothèse. De la proposition 5.2.9, on tire alors une "relation de Bézout" $up + va = 1$, $u, v \in A$. On en déduit $b = upb + vab$, qui est bien multiple de p puisque ab l'est. □

Théorème 5.2.12 *Tout anneau principal est factoriel.*

Preuve. - Soit A un anneau principal. Supposons qu'il y ait des éléments non nuls et non inversibles qui ne soient pas produits d'irréductibles et soit F l'ensemble (par hypothèse non vide) des idéaux principaux Ax engendrés par de tels éléments x. Soit Aa un élément maximal de F (lemme 5.2.8) : a n'est donc ni nul ni inversible, et il n'est pas non plus irréductible (sinon il serait produit d'irréductibles et Aa ne serait pas élément de F). On a donc $a = bc$ avec b, c ni nuls ni inversibles. les idéaux Ab et Ac contiennent Aa (puisque b et c divisent a) et cette inclusion est stricte (si l'on avait par exemple $Ab = Aa$, c serait inversible). Les idéaux Ab et Ac ne sont donc pas éléments de F (par maximalité de Aa dans F) donc b et c sont produits d'irréductibles [2] donc $a = bc$ aussi, contradiction. On a donc démontré que tout élément non nul et non inversible de A est produit d'irréductibles.
Soit maintenant p un irréductible de A ; nous voulons démontrer que p est premier : mais cela découle de la proposition 5.2.11. □

5.3 Propriétés des anneaux factoriels

On fixe un anneau factoriel A et un ensemble P de représentants de ses éléments irréductibles, que l'on écrira aussi bien sous la forme d'une famille $(p_i)_{i\in I}$. Tout élément non nul de A admet donc une unique écriture $a = \varepsilon \prod p_i^{r_i}$, $\varepsilon \in A^*$, $(r_i)_{i\in I} \in \mathbf{N}^{(I)}$.

5.3.1 Divisibilité

Si $a = \varepsilon \prod p_i^{r_i}$, $b = \eta \prod p_i^{s_i}$, alors l'écriture correspondante du produit est $ab = (\varepsilon\eta) \prod p_i^{r_i+s_i}$. On en déduit immédiatement que, pour que $a' = \varepsilon' \prod p_i^{r'_i}$ divise a, il faut, et il suffit, que $\forall i \in I$, $r'_i \leq r_i$.

On en déduit ensuite que deux éléments non nuls quelconques a et b écrits comme ci-dessus admettent un pgcd :

$$a \wedge b = \prod p_i^{\min(r_i,s_i)},$$

et un ppcm :

$$a \vee b = \prod p_i^{\max(r_i,s_i)}.$$

On conviendra que $a \wedge b$ est *le* pgcd et $a \vee b$ *le* ppcm de a et b.

Proposition 5.3.1 (Lemme d'Euclide) *Tout irréductible p de A est premier*, i.e. $p|ab \Rightarrow p|a$ *ou* $p|b$.

Preuve. - Cela découle du théorème 5.1.1 et de la définition 5.1.2. □

Proposition 5.3.2 (Lemme de Gauß) *Si a et b sont premiers entre eux et si $a|bc$ alors $a|c$.*

Preuve. - On écrit $a = \varepsilon \prod p_i^{r_i}$, $b = \eta \prod p_i^{s_i}$ et $c = \phi \prod p_i^{t_i}$ (conventions habituelles). Les hypothèses se traduisent par : $\forall i \in I$, $r_i = 0$ ou $s_i = 0$; et $\forall i \in I$, $r_i \leq s_i + t_i$. Il faut en déduire que $\forall i \in I$, $r_i \leq t_i$: mais c'est évident dans chacun des deux cas possibles $r_i = 0$ ou $s_i = 0$. □

2. Il y a ici une toute petite subtilité : comme $Ab \notin F$, on sait que Ab admet un générateur b' qui n'est pas produit d'irréductibles ; mais $b \sim b'$, c'est donc encore vrai de b. Même chose pour c.

5.3.2 Valuations

Pour tout $a \in A$ non nul et pour tout $p \in P$, notons $v_p(a)$ le plus grand entier $r \in \mathbf{N}$ tel que $p^r | a$. Dans l'écriture $a = \varepsilon \prod p_i^{r_i}$, si $p = p_i$ alors $v_p(a) = r_i$. On a donc :

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)}.$$

Des calculs précédents, on tire :

$$\begin{aligned} v_p(ab) &= v_p(a) + v_p(b), \\ v_p(a \wedge b) &= \min(v_p(a), v_p(b)), \\ v_p(a \vee b) &= \max(v_p(a), v_p(b)), \\ a|b &\iff \forall p \in P\ ,\ v_p(a) \leq v_p(b), \\ a \sim b &\iff \forall p \in P\ ,\ v_p(a) = v_p(b). \end{aligned}$$

On étend v_p en une application définie sur A tout entier en posant $v_p(0) := +\infty$. Avec les règles habituelles de calcul sur dans $\mathbf{N} \cup \{+\infty\}$, toutes les relations ci-dessus restent valables pour $a, b \in A$. De plus, du fait que la somme de deux multiples de p^r est un multiple de p^r, *i.e.* que $v_p(a), v_p(b) \geq r \Rightarrow v_p(a+b) \geq r$, on tire la règle suivante :

$$v_p(a+b) \geq \min(v_p(a), v_p(b)).$$

Soient $a, b, a', b' \in A$, $b, b' \neq 0$ et supposons que $ab' = a'b$. Alors :

$$v_p(ab') = v_p(a'b) \Longrightarrow v_p(a) + v_p(b') = v_p(a') + v_p(b) \Longrightarrow v_p(a) - v_p(b) = v_p(a') - v_p(b'),$$

la dernière égalité se déduisant de la précédente en soustrayant $v_p(b) + v_p(b')$, ce qui est licite car c'est un élément de $\mathbf{N}$ et non $+\infty$. Il est donc légitime de poser $v_p(a/b) := v_p(a) - v_p(b)$ pour tout $a/b \in K$, le corps des fractions de A. On a encore les règles :

$$\begin{aligned} v_p(ab) &= v_p(a) + v_p(b), \\ v_p(a+b) &\geq \min(v_p(a), v_p(b)), \end{aligned}$$

pour $a, b \in K$. On dit que l'application $v_p : K \to \mathbf{Z} \cup \{+\infty\}$ est une *valuation*. Cette valuation particulière est appelée *valuation p-adique*. De la règle antérieure $a|b \Leftrightarrow \forall p \in P\ ,\ v_p(a) \leq v_p(b)$ on déduit, pour tout $x \in K$:

$$x \in A \iff \forall p \in P\ ,\ v_p(x) \geq 0.$$

On va en déduire une généralisation du théorème selon lequel $\mathbf{Z}$ est intégralement clos (théorème 4.3.3 du chapitre 4).

Théorème 5.3.3 *Tout anneau factoriel est intégralement clos.*

Preuve. - Soient A un anneau factoriel et K son corps des fractions. Soit $x \in K$ un élément entier sur A, autrement dit solution d'une équation algébrique $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, $a_1, \ldots, a_n \in A$. Il s'agit de montrer que $x \in A$. Nous allons pour cela invoquer le tout dernier critère. Soit donc $p \in P$ un irréductible choisi dans l'ensemble de représentants P. On a $-x^n = a_1 x^{n-1} + \cdots + a_n$, d'où :

$$n v_p(x) = v_p(a_1 x^{n-1} + \cdots + a_n) \geq \min\big(v_p(a_1 x^{n-1}), \ldots, v_p(a_{n-1} x), v_p(a_n)\big) \geq \min\big((n-1)v_p(x), \ldots, v_p(x), 0\big),$$

ce qui n'est possible que si $v_p(x) \geq 0$. □

5.4 Application arithmétique

Théorème 5.4.1 *L'anneau $\mathbf{Z}[i]$ des entiers de Gauß est euclidien, principal et factoriel.*

Preuve. - On pose $g(z) := z\bar{z} = a^2 + b^2$ si $z = a + b\mathrm{i}$, $a, b \in \mathbf{Z}$. Il est clair que $g(z) \in \mathbf{N}$ si $z \in \mathbf{Z}[\mathrm{i}]$ n'est pas nul (c'est encore vrai si $z = 0$ mais cela ne fait pas partie de la définition d'un stathme). De même, si $z, z' \in \mathbf{Z}[\mathrm{i}]$, $z, z' \neq 0$, l'inégalité $g(z) \leq g(zz')$ découle du fait que $g(zz') = g(z)g(z')$ (propriété de la conjugaison dans $\mathbf{C}$) et du fait que $g(z), g(z') \geq 1$. Supposons enfin que $z, z' \in \mathbf{Z}[\mathrm{i}]$ et $z \neq 0$. Alors $w := z'/z \in \mathbf{Q}[\mathrm{i}]$: on l'écrit $w = x + y\mathrm{i}$ avec $x, y \in \mathbf{Q}$. Il existe $a, b \in \mathbf{Z}$ tels que $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$ (prendre pour a soit $\lfloor x \rfloor$ soit $\lfloor x \rfloor + 1$ et de même pour b). Soit $q := a + b\mathrm{i}$: alors $q \in \mathbf{Z}[\mathrm{i}]$ et $|w - q|^2 \leq 1/4 + 1/4 = 1/2$, d'où $|z' - qz|^2 < |z|^2$. En posant $r := z' - qz$, on a bien $q, r \in \mathbf{Z}[\mathrm{i}]$, $z' = qz + r$ et $r = 0$ ou $g(r) < g(z)$.
La principalité et la factorialité découlent alors des théorèmes 5.2.4 et 5.2.12. □

Corollaire 5.4.2 (Fermat,Euler) *Tout entier de la forme $p = 4n + 1$ est somme de deux carrés.*

Preuve. - D'après le corollaire 4.4.8 (section 4.4 du chapitre 4), p n'est pas premier dans $\mathbf{Z}[\mathrm{i}]$. Cet anneau étant factoriel, p n'y est donc pas non plus irréductible ! Comme il n'est ni nul ni inversible (pourquoi ?), il est réductible, *i.e.* $p = uv$ avec $u = a + b\mathrm{i}, v = c + d\mathrm{i} \in \mathbf{Z}[\mathrm{i}]$ non inversibles. Alors $p^2 = (a^2 + b^2)(c^2 + d^2)$ avec $a^2 + b^2, c^2 + d^2 > 1$, d'où $p = a^2 + b^2 = c^2 + d^2$. □

Avant de déterminer exactement les sommes de deux carrés dans $\mathbf{N}$, nous avons encore besoin d'un lemme :

Lemme 5.4.3 *Soit q un nombre premier de la forme $4m - 1$ et soit $n = a^2 + b^2$, $a, b \in \mathbf{Z}$. Alors $v_q(n)$ est pair.*

Preuve. - Si q ne divise pas n, on a $v_q(n) = 0$, qui est pair. Sinon, notant x, y les classes de a, b modulo q, on voit que $x^2 + y^2 = 0$ dans $\mathbf{F}_q$. Si l'on avait par exemple $x \neq 0$, l'élément $z := y/x \in \mathbf{F}_q$ vérifierait $z^2 = -1$, ce qui est impossible d'après le corollaire 4.4.7 (section 4.4 du chapitre 4). Donc $x = y = 0$, *i.e.* q divise a et b : $a = qa_1$, $b = qb_1$ et l'on a $n = q^2 n_1$ où $n_1 = a_1^2 + b_1^2$; on recommence alors le raisonnement avec n_1. □

Le résultat suivant a été énoncé et très probablement démontré par Fermat, mais sa première démonstration publiée est due à Euler ; c'est même ses efforts pour la trouver qui convertirent Euler à la théorie des nombres.

Théorème 5.4.4 (Fermat, Euler) *Soit $n = 2^r p_1^{s_1} \cdots p_k^{s_k} q_1^{t_1} \cdots q_l^{t_l}$, où la décomposition en facteurs premiers de $n \in \mathbf{N} \setminus \{0\}$ est écrite de telle sorte que $p_1, \ldots, p_k$ sont des premiers distincts, $p_i \equiv +1 \pmod 4$ et $q_1, \ldots, q_l$ sont des premiers distincts, $q_j \equiv -1 \pmod 4$. Alors, pour que n soit somme de deux carrés, il faut, et il suffit, que tous les exposants t_j soient pairs.*

Preuve. - Supposons que n soit somme de deux carrés : $n = a^2 + b^2$. D'après le lemme ci-dessus, chaque $t_j = v_{q_j}(n)$ est pair.
Supposons réciproquement que tous les exposants t_j sont pairs. Puisque $2 = 1^2 + 1^2$, chaque p_i (d'après le corollaire 5.4.2) et bien entendu chaque $q_j^{t_j} = \left(q_j^{t_j/2}\right)^2$ est une somme de deux carrés, il suffit de vérifier que le produit de deux sommes de deux carrés est une somme de deux carrés. C'est immédiat d'après la formule $(a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2$. □

5.5 Exercices sur le chapitre 5

Exercice 5.5.1 On dit qu'un anneau est *noetherien* si tout idéal est de type fini. Montrer que dans un tel anneau, toute suite croissante d'idéaux est stationnaire. (Généraliser l'argument du lemme 5.2.8.) Prouver la réciproque. (Si I n'est pas de type fini, choisir $x_0 \in I$ puis $x_1 \in I \setminus Ax_0$, etc.)

Exercice 5.5.2 1) On dit que A est *de Bézout* si, quels que soient $x, y \in A$, l'idéal $Ax + Ay$ est principal. Montrer que cette propriété équivaut à la suivante : tout idéal de type fini est principal.
2) Montrer que, dans un anneau noetherien de Bézout, tout idéal est principal, et réciproquement.
3) Donner un exemple d'anneau noetherien de Bézout non principal.

Exercice 5.5.3 1) Soit A l'anneau des fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$. Montrer que $f, g \in A$ sont premiers entre eux (autrement dit, $\mathrm{Div}(f) \cap \mathrm{Div}(g) = A^*$) si, et seulement s'ils n'ont pas de zéro commun. Montrer que, dans ce cas, $Af + Ag = A$.
2) Montrer que l'anneau A ne contient aucun élément irréductible et aucun élément premier.
3) Montrer que l'ensemble des fonctions $f \in A$ telles que $f(0) = 0$ est un idéal non principal de A.

Exercice 5.5.4 Dans un anneau factoriel, les idéaux premiers non nuls minimaux sont principaux.

Exercice 5.5.5 Soit g un stathme euclidien sur l'anneau A. Montrer les équivalences suivantes :

$$g(x) \text{ minimum } \iff x \text{ inversible}, \qquad \big(g(x) = g(y) \text{ et } x|y\big) \iff x \sim y.$$

Exercice 5.5.6 Soit $A := \mathbf{Z}[j]$ avec $j := \dfrac{-1+\sqrt{-3}}{2}$. Montrer que A est euclidien et effectuer la division euclidienne de 5 par $1+\sqrt{-3}$.

Exercice 5.5.7 Montrer à l'aide de la "norme" $N(z) := z\bar{z}$ que, dans $\mathbf{Z}[\sqrt{-6}]$, tout élement non nul et non inversible est produit d'irréductibles mais que cet anneau n'est pas factoriel.

Exercice 5.5.8 1) Soit $d \in \mathbf{Q}$ un rationnel non carré. Si $d < 0$, on convient que $\sqrt{d} := \mathrm{i}\sqrt{|d|}$. Montrer que $K := \{a + b\sqrt{d} \mid a, b \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{C}$, et que c'est un $\mathbf{Q}$-espace vectoriel de base $(1, \sqrt{d})$. On le notera $\mathbf{Q}(\sqrt{d})$.
2) Montrer qu'il existe un unique $d' \in \mathbf{Z} \setminus \{1\}$ quadratfrei (c'est à dire sans facteur carré > 1) tel que $K = \mathbf{Q}(\sqrt{d'})$. Dorénavant, on supposera $d \in \mathbf{Z} \setminus \{1\}$ et quadratfrei.
3) Montrer que l'application $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ est un automorphisme du corps K.
4) Pour tout $u \in K$, vérifier que l'application $x \mapsto ux$ est un endomorphisme du $\mathbf{Q}$-espace vectoriel K et calculer sa trace et son déterminant. La trace sera notée $\mathrm{Tr}(u)$ et appelée *trace de* u ; le déterminant sera noté $N(u)$ et appelé *norme de* u. Vérifier que $\mathrm{Tr}(u) = u + \sigma(u)$ et $N(u) = u\sigma(u)$.
5) On dit que $x \in K$ est *entier sur* $\mathbf{Z}$, ou encore que c'est un *entier algébrique*, si $\mathrm{Tr}(x) \in \mathbf{Z}$ et $N(x) \in \mathbf{Z}$. Montrer que l'ensemble A des entiers algébriques de K est égal à :

$$A = \{a + b\delta \mid a, b \in \mathbf{Z}\}, \quad \text{avec } \delta := \begin{cases} \sqrt{d} \text{ si } d \equiv 2 \text{ ou } 3 \pmod 4, \\ \dfrac{-1+\sqrt{d}}{2} \text{ si } d \equiv 1 \pmod 4. \end{cases}$$

et que c'est un sous-anneau de K dont K est le corps des fractions.
6) Montrer que $A^* = \{u \in A \mid N(u) = \pm 1\}$.
7) Montrer que, si $d \in \{-1, 2, -2, 3, -3 - 7, -11\}$, alors N est un stathme euclidien sur A.

Chapitre 6

Polynômes

6.1 Polynômes à une indéterminée sur un anneau commutatif

Si A est un anneau intègre de corps des fractions K, l'ensemble des éléments de $K[X]$ dont tous les coefficients appartiennent à A en forme un sous-anneau que nous avons noté $A[X]$. (C'est un exercice facile laissé au lecteur ; d'ailleurs, il se déduit de l'un des résultats qui vont suivre : lequel ?) Plus généralement, on a introduit [1] dans les exemples de la section 2.1 l'anneau $A[X]$ des polynômes à coefficients dans n'importe quel anneau commutatif A. L'application principale en L3 concerne le cas où A est factoriel, que nous étudierons à la section suivante.

6.1.1 Propriétés générales

Rappelons qu'un élément de $A[X]$ est une expression de la forme $\sum_{i\geq 0} a_i X^i$, où les a_i sont nuls à partir d'un certain rang, autrement dit $(a_i)_{i\geq 0} \in A^{(\mathbf{N})}$. On convient que l'égalité : $\sum_{i\geq 0} a_i X^i = \sum_{i\geq 0} b_i X^i$ équivaut à la suite d'égalités : $\forall i \in \mathbf{N}$, $a_i = b_i$. De plus, si $a_i = 0$ pour tout $i > n$, on abrège la notation ci-dessus en posant $\sum_{i\geq 0} a_i X^i =: \sum_{i=0}^{n} a_i X^i = a_0 + \cdots + a_n X^n$.

La structure algébrique de $A[X]$ provient des deux lois de composition interne suivantes (addition et multiplication) :

$$\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i := \sum_{i\geq 0} (a_i + b_i) X^i,$$

$$\left(\sum_{i\geq 0} a_i X^i\right) \times \left(\sum_{i\geq 0} b_i X^i\right) := \sum_{i\geq 0} \left(\sum_{j+k=i} a_j b_k\right) X^i.$$

Théorème 6.1.1 *(i) On obtient ainsi un anneau commutatif $(A[X], +, \times)$. L'élément neutre de l'addition est $0 := \sum_{i\geq 0} 0X^i$. L'opposé de $\sum_{i\geq 0} a_i X^i$ est $\sum_{i\geq 0} (-a_i) X^i$. L'élément neutre de la multiplication est (avec la notation de Kronecker) $1 := \sum_{i\geq 0} \delta_{i,0} X^i$.*

(ii) L'application $a \mapsto \sum_{i\geq 0} (a\delta_{i,0}) X^i$ est un isomorphisme de A sur le sous-anneau de $A[X]$ formé des

1. Comme déjà remarqué, on ne peut parler d'une véritable *définition* dans la formulation de ces exemples : voir pour cela RW1 et RW2.

polynômes $\sum_{i\geq 0} a_i X^i$ *tels que* $a_i = 0$ *pour* $i > 0$. *On identifie* A *à ce sous-anneau, dont les éléments sont appelés polynômes constants.*
(iii) Soit A' *un sous-anneau de* A. *Le sous-ensemble* $A'[X]$ *de* $A[X]$ *en est un sous-anneau.*

Preuve. - La démonstration est entièrement mécanique et laissée au lecteur. □

La dernière assertion permet de retrouver le cas d'un anneau intègre A de corps des fractions K : on voit que $A[X]$ est bien un sous-anneau de $K[X]$. Dans les deux énoncés qui suivent, nous notons, pour tout idéal I de A :

$$IA[X] := \left\{ \sum_{i\geq 0} a_i X^i \in A[X] \mid \forall i \in \mathbf{N}\ ,\ a_i \in I \right\}.$$

Proposition 6.1.2 *Soit* $f : A \to B$ *un morphisme d'anneaux. Alors l'application* $\sum_{i\geq 0} a_i X^i \mapsto \sum_{i\geq 0} f(a_i) X^i$ *est un morphisme d'anneaux de* $A[X]$ *dans* $B[X]$. *Son image est* $B'[X]$, *où* $B' := Imf$. *Son noyau est* $JA[X]$, *où* $J := Kerf$.

Preuve. - La démonstration est entièrement mécanique et laissée au lecteur. □

Corollaire 6.1.3 *Soit* I *un idéal quelconque de l'anneau* A. *Le morphisme* $A[X] \to (A/I)[X]$ *déduit du morphisme canonique* $A \to A/I$ *est surjectif de noyau* $IA[X]$. *En particulier,* $IA[X]$ *est un idéal de* $A[X]$ *et* $A[X]/IA[X] \simeq (A/I)[X]$.

Preuve. - Appliquer la proposition à $B := A/I$. □

Notations de base. Si $P := \sum_{i\geq 0} a_i X^i$ n'est pas nul et si $n \in \mathbf{N}$ est le plus grand indice tel que $a_n \neq 0$, on pose :

$$\begin{aligned} \deg P &:= n && \text{(degré de } P\text{)},\\ \mathrm{td}P &:= a_n X^n && \text{(terme dominant de } P\text{)},\\ \mathrm{cd}P &:= a_n && \text{(coefficient dominant de } P\text{)}. \end{aligned}$$

On posera de plus $\deg 0 := -\infty$; mais les expressions $\mathrm{td}(0)$ et $\mathrm{cd}(0)$ ne sont pas définies. Ces notations servent surtout si A est un anneau intègre :

Proposition 6.1.4 *Soit* A *un anneau intègre et soient* $P, Q \in A$. *Alors :*

$$\begin{aligned} \deg(P+Q) &\leq \max(\deg P, \deg Q),\\ \deg(PQ) &= \deg P + \deg Q,\\ td(PQ) &= (tdP)(tdQ),\\ cd(PQ) &= (cdP)(cdQ). \end{aligned}$$

De plus, si $\deg P \neq \deg Q$, *la première inégalité devient une égalité. Plus généralement, le seul cas où ce n'est pas une égalité est celui où* $td(P) = -td(Q)$.

Preuve. - La démonstration est entièrement mécanique et laissée au lecteur. □

Corollaire 6.1.5 *Les inversibles de $A[X]$ sont les éléments de A^* (l'anneau A étant toujours supposé intègre).*

Preuve. - En effet, si $PQ = 1$ alors $\deg(P) + \deg(Q) = 0$, donc $\deg(P) = \deg(Q) = 0$, *i.e.* P et Q sont constants : la conclusion vient facilement. □

Les exemples suivants montrent que l'hypothèse d'intégrité n'est pas superflue.

Exemples 6.1.6
1. Prenons $A = \mathbf{Z}/6\mathbf{Z}$, $P := 1 + \dot{2}X$ et $Q := 1 + \dot{3}X$. Alors $PQ = 1 + \dot{5}X$, donc $\deg PQ = \deg P + \deg Q - 1$.
2. Prenons $A = \mathbf{Z}/4\mathbf{Z}$ et $P := 1 + \dot{2}X$. Alors $P^2 = 1$, donc P est inversible.

Exercice 6.1.7 (Cours) Montrer que quatre formules restent vraies sur un anneau quelconque (non supposé intègre), à condition, pour les trois dernières, que l'on suppose que $\mathrm{cd}(P)$ ou $\mathrm{cd}(Q)$ n'est pas diviseur de zéro.

6.1.2 Division euclidienne dans $A[X]$

Proposition 6.1.8 *Soit A un anneau commutatif. (On ne suppose pas A intègre !)*
(i) Soit $P \in A[X]$ non nul, de terme dominant $\mathrm{td}(P) = aX^n$. Pour tout $F \in A[X]$, il existe $k \in \mathbf{N}$ et $Q, R \in A[X]$ tels que :

$$\begin{cases} a^k F = PQ + R, \\ \deg R < \deg P. \end{cases}$$

On peut prendre $k := \max(0, 1 + \deg F - \deg P)$.
(ii) Si $a = cd(P)$ est inversible, on peut prendre $k = 0$; et Q, R sont alors uniques.

Preuve. - (i) Si $\deg F < \deg P$, on prend $k = 0$, $Q = 0$ et $R = F$.
Si $\deg F \geq \deg P$, on élimine le terme dominant en posant $F_1 := aF - \mathrm{cd}(F)X^{\deg F - \deg P}P$, qui est de degré $\deg F_1 < \deg F$. Par récurrence, on peut donc supposer que $a^{k_1}F_1 = PQ_1 + R$, $\deg R < \deg P$, avec $k_1 := \max(0, 1 + \deg F_1 - \deg P)$. On en tire $a^k F = PQ + R$ avec $k = k_1 + 1$ et $Q = Q_1 + a^{k_1}\mathrm{cd}(F)X^{\deg F - \deg P}$.
(ii) Si a est inversible, on déduit de l'égalité précédente $F = P(a^{-k}Q) + a^{-k}R$, avec $\deg a^{-k}R = \deg R < \deg P$. Pour prouver l'unicité, on suppose $PQ + R = PQ_1 + R_1$ avec $\deg R, \deg R_1 < \deg P$. On a alors $\deg P(Q - Q_1) < \deg P$, ce qui n'est possible que si $Q - Q_1 = 0$: en effet, le coefficient dominant $a = \mathrm{cd}(P)$ ne peut vérifier $a \times \mathrm{cd}(Q - Q_1) = 0$. □

Exemples 6.1.9
1. On prend $A = \mathbf{Z}[X]$, $P = 2X + 1$ et $F = X^3 + X^2 + X + 1$. Alors $8F = P(4X^2 + 2X + 3) + 5$.
2. On prend $A = K[X, Y]$, $P = XY + 1$ et $F = X^3 + X^2 + X + 1$. Le calcul se mène ainsi :
$$YF = X^2P + F_1, \text{ où } F_1 = (Y-1)X^2 + YX + Y,$$
$$YF_1 = (Y-1)XP + F_2, \text{ où } F_2 = (Y^2 - Y + 1)X + Y^2,$$
$$YF_2 = (Y^2 - Y + 1)P + F_2, \text{ où } F_2 = Y^3 - Y^2 + Y - 1,$$
$$Y^3F = Y^2(YF - F_1) + Y(YF_1 - F_2) + YF_2 = P(Y^2X^2 + Y(Y-1)X + (Y^2 - Y + 1)) + (Y^3 - Y^2 + Y - 1).$$
3. Si $P \in \mathbf{Z}[X]$ est tel que $P(\mathrm{i}) = 0$ alors $P \in (X^2 + 1)\mathbf{Z}[X]$.

Exercice 6.1.10 Comment déduire rigoureusement le premier exemple du second ?

6.2 Polynômes sur un anneau factoriel

Dans toute cette section, l'anneau A est supposé factoriel. On suppose de plus choisi un ensemble P de représentants des irréductibles de A pour la relation d'association (voir les sections 5.1 et 5.3 du chapitre 5). On notera P^+ l'ensemble des produits d'éléments de P :

$$P^+ := \{p_1 \cdots p_k \mid k \in \mathbf{N} \text{ et } p_1, \ldots, p_k \in P\}. = \left\{ \prod_{p \in P} p^{r_p} \mid (r_p) \in \mathbf{N}^{(P)} \right\}.$$

Ainsi, pour une famille quelconque (a_i) d'éléments de A, *le* pgcd des a_i est bien défini et c'est un élément de P^+ ; et les a_i sont premiers entre eux dans leur ensemble si, et seulement si, leur pgcd est égal à 1.

Exercice 6.2.1 (Cours) Démontrer ces affirmations concernant K.

Définition 6.2.2 (i) On appelle *contenu* d'un polynôme non nul de $A[X]$ le pgcd de ses coefficients. On notera $c(F)$ le contenu du polynôme F.
(ii) Le polynôme non nul de $A[X]$ est dit *primitif* si ses coefficients sont premiers entre eux dans leur ensemble. Le polynôme F est donc primitif si $c(F) = 1$.

Lemme 6.2.3 *Tout polynôme non nul $F \in A[X]$ s'écrit de manière unique $F = c\tilde{F}$, où $c \in P^+$ et où $\tilde{F}$ est primitif ; le facteur c est égal au contenu $c(F)$.*

Preuve. - L'égalité $\sum a_i X^i = c \sum \tilde{a}_i X^i$ avec $c \in P^+$ et les $\tilde{a}_i$ premiers entre eux dans leur ensemble équivaut à $\forall i$, $a_i = c\tilde{a}_i$, donc c doit être le pgcd des a_i. □

Théorème 6.2.4 (Gauß) *(i) Le produit de deux polynômes primitifs est un polynôme primitif.*
(ii) Soient $F, G \in A[X]$ deux polynômes non nuls. Alors $c(FG) = c(F)c(G)$ et $\widetilde{FG} = \tilde{F}\tilde{G}$.

Preuve. - (i) Supposons $F, G \in A[X]$ primitifs. On va démontrer par l'absurde que les coefficients de FG sont premiers entre eux dans leur ensemble. Sinon, il existerait $p \in P$ qui divise tous les coefficients de FG. Notant B l'anneau intègre $A/(p)$, cela revient à dire que l'image $\overline{FG}$ de FG par le morphisme $A[X] \to B[X]$ est nulle. Mais cette image est égale à $\overline{F} \times \overline{G}$, donc $\overline{F}$ ou $\overline{G}$ est nul, *i.e.* p divise $c(F)$ ou $c(G)$, contradiction. (On peut aussi raisonner plus directement : si a_i, resp. b_j sont les coefficients de F, resp. G non multiples de p de plus grands indices, alors le coefficient de FG d'indice $i+j$ n'est pas multiple de p.)
(ii) On écrit en vertu le lemme ci-dessus $F = c(F)\tilde{F}$ et $G = c(G)\tilde{G}$, d'où $FG = c(F)C(G)\tilde{F}\tilde{G} = c(FG)\widetilde{FG}$, d'où, puisque $\tilde{F}\tilde{G}$ est primitif, les égalités voulues (toujours en vertu du lemme). □

Extension au corps des fractions. Soit K le corps des fractions de A. On notera P^* le sous-groupe de K^* engendré par P :

$$P^* = \left\{ \prod_{p \in P} p^{r_p} \mid (r_p) \in \mathbf{Z}^{(P)} \right\}.$$

Tout élément $a \in K^*$ admet alors une unique écriture $a = \varepsilon a'$ avec $\varepsilon \in A^*$ et $a' \in P^*$. D'autre part, toute famille (a_i) d'éléments non tous nuls de K admet un unique "pgcd" $c \in P^*$ tel que les $b_i := c^{-1} a_i$ sont des éléments de A premiers entre eux dans leur ensemble.

Corollaire 6.2.5 *(i) Tout polynôme non nul $F \in K[X]$ admet une unique écriture $F = c\tilde{F}$, où $c \in P^*$ et où $\tilde{F} \in A[X]$ est primitif.*
(ii) On a encore les formules $c(FG) = c(F)c(G)$ et $\widetilde{FG} = \tilde{F}\tilde{G}$.

□

La constante $c(F) \in P^*$ est encore appelée *contenu de F*.

Corollaire 6.2.6 *Soit $F \in K[X]$. Alors $F \in A[X] \Leftrightarrow c(F) \in A$.*

Corollaire 6.2.7 *Soit $F \in K[X]$. Alors $FK[X] \cap A[X] = \tilde{F}A[X]$.*

Lemme 6.2.8 *(i) Les éléments irréductibles de A sont premiers dans $A[X]$.*
(ii) Les polynômes $F \in A[X]$ qui sont primitifs dans $A[X]$ et irréductibles dans $K[X]$ sont premiers dans $A[X]$.

Preuve. - (i) Soit $p \in P$ (il suffit évidemment de considérer ce cas). Si $p|FG$, $F, G \in A[X]$ alors on peut écrire $FG = pH$, $H \in A[X]$, donc, en prenant les contenus : $pc(H) = c(F)c(G)$, donc $p|c(F)c(G)$ dans A, donc $p|c(F)$ ou $p|c(G)$ dans A (car p est premier dans A) donc $p|F$ ou $p|G$ dans $A[X]$ (clair).
(ii) Soit $H \in A[X]$ primitif dans $A[X]$ et irréductible dans $K[X]$ et supposons que $H|FG$, $F, G \in A[X]$. Alors $H|FG$ dans $K[X]$; comme H est irréductible, donc premier, dans $K[X]$, on en déduit par exemple que $H|F$ dans $K[X]$ (le cas où $H|G$ se traitant de la même manière). On écrit donc $F = HL$, $HL \in K[X]$. En prenant les contenus, on trouve que $c(F) = c(H)c(L) = c(L)$, puisque H est primitif. Donc $c(L) \in A$, donc $L \in A[X]$, donc $H|F$ dans $A[X]$. □

Théorème 6.2.9 *L'anneau $A[X]$ des polynômes sur l'anneau factoriel A est factoriel. Ses irréductibles sont d'une part les éléments irréductibles de A, d'autre part les polynômes primitifs dans $A[X]$ qui sont irréductibles dans $K[X]$.*

Preuve. - Tout d'abord, il est clair que tout élément irréductible de $A[X]$ est de l'une des formes indiquées. D'après le lemme, on voit donc que tout élément irréductible de $A[X]$ est premier.
Soit maintenant $F \in A[X]$ non nul et non inversible. Si $\deg F = 0$, c'est un élément de l'anneau factoriel A, donc un produit d'irréductibles de A, donc de $A[X]$. Si $\deg F \geq 1$, c'est un produit d'irréductibles de $K[X]$: $F = G_1 \cdots G_k$. On en déduit que $\tilde{F} = \tilde{G}_1 \cdots \tilde{G}_k$; or chaque $\tilde{G}_i$ est irréductible dans $K[X]$ (car associé à G_i) et primitif (par définition) donc $\tilde{F}$ est un produit d'irréductibles de $A[X]$. Il en est de même de $c(F)$ (premier cas, ou cas spécial $c(F) = 1$), donc de $F = c(F)\tilde{F}$. □

Corollaire 6.2.10 *Les anneaux $\mathbf{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$ sont factoriels.*

Exercice 6.2.11 Vérifier que tout élément irréductible de $A[X]$ est de l'une des formes indiquées.

Choix d'un ensemble de représentants des irréductibles de $A[X]$. Il suffit de prendre les éléments de P d'une part, et d'autre part les polynômes primitifs dans $A[X]$ qui sont irréductibles dans $K[X]$ en imposant de plus que leur coefficient dominant soit dans P^+.

6.3 Idéaux premiers de $\mathbf{C}[X,Y]$

On va décrire, en vue d'applications à la géométrie, tous les idéaux premiers de $\mathbf{C}[X,Y]$. Le résultat demeure d'ailleurs valable si l'on remplace $\mathbf{C}$ par n'importe quel corps algébriquement clos. Notons que $\mathbf{C}[X,Y]$ est factoriel d'après la section précédente.

Lemme 6.3.1 *Soit S une partie multiplicative d'un anneau intègre A ne contenant pas 0 et soit $B := S^{-1}A$ (qui n'est donc pas trivial).*
(i) Pour tout idéal premier $\mathfrak{P}$ de A tel que $S\cap\mathfrak{P}=\emptyset$, l'idéal $\mathfrak{Q} := S^{-1}\mathfrak{P}$ de B est premier.
(ii) Pour tout idéal premier $\mathfrak{Q}$ de B, l'idéal $\mathfrak{P} := \mathfrak{Q}\cap A$ de A est premier et $S\cap\mathfrak{P}=\emptyset$.
(iii) 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 $B = S^{-1}A$.

Preuve. - La démonstration des assertions (i) et (ii) est entièrement mécanique et laissée au lecteur, ainsi que la preuve que, si $\mathfrak{Q}$ est un idéal premier de $S^{-1}A$, alors $\mathfrak{Q} = S^{-1}(\mathfrak{Q}\cap A)$.
Il reste à vérifier que, si $\mathfrak{P}$ est un idéal premier de A qui ne rencontre pas S, on a $\mathfrak{P} = (S^{-1}\mathfrak{P})\cap A$. Il est évident que $\mathfrak{P}\subset(S^{-1}\mathfrak{P})\cap A$. Soit réciproquement $x\in(S^{-1}\mathfrak{P})\cap A$. Donc $x = p/s\in A$ avec $p\in\mathfrak{P}$ et $s\in S$. Puisque $sx = p\in\mathfrak{P}$ et $s\notin\mathfrak{P}$, on a $x\in\mathfrak{P}$ (c'est un idéal premier), ce qu'il fallait démontrer. □

Soit maintenant $\mathfrak{P}$ un idéal premier de $\mathbf{C}[X,Y] = A[X]$, où A désigne l'anneau principal $\mathbf{C}[Y]$. L'idéal $\mathfrak{P}\cap A$ de A est premier (c'est le noyau du morphisme composé $A\to A[X]\to A[X]/\mathfrak{P}$, ce qui fait de $A/(\mathfrak{P}\cap A)$ un sous-anneau de l'anneau intègre $A[X]/\mathfrak{P}$). Il est donc soit trivial, soit maximal et de la forme $< f >$ où $f\in A$ est premier.

Premier cas : $\mathfrak{P}\cap A =< f >$. Ici, $f(Y)$ est un polynôme irréductible, donc du premier degré (puisque $\mathbf{C}$ est algébriquement clos) et l'on peut prendre $f = Y-b$, $b\in\mathbf{C}$. On a donc $Y-b\in\mathfrak{P}$, donc $(Y-b)A[X]\subset\mathfrak{P}$. L'idéal premier $\mathfrak{P}$ est donc l'image réciproque d'un idéal premier de l'anneau :

$$A[X]/(Y-b)A[X] = \big(A/ < Y-b >\big)[X] = \mathbf{C}[X],$$

i.e. l'idéal trivial ou bien un $< X-a >$, $a\in\mathbf{C}$.
En conclusion, dans ce cas, $\mathfrak{P} =< X-a, Y-b >$ ou $\mathfrak{P} =< Y-b >$.

Deuxième cas : $\mathfrak{P}\cap A = \{0\}$. Notons $S := A\setminus\{0\}$ et K le corps des fractions de A. D'après le lemme, $\mathfrak{P} = \mathfrak{Q}\cap A[X]$ où $\mathfrak{Q}$ est un idéal premier de $K[X]$, qui est principal. Si $\mathfrak{Q}$ est trivial, alors $\mathfrak{P}$ l'est également. Sinon, $\mathfrak{Q}$ est engendré par un polynôme irréductible $F(X)$ de $K[X]$. Appliquant les résultats de la section précédente, on voit que $\mathfrak{P}$ est engendré par $\tilde{F}$, *i.e.* par un polynôme irréductible de $\mathbf{C}[X,Y]$.

Théorème 6.3.2 *les idéaux premiers de $\mathbf{C}[X,Y]$ sont l'idéal trivial $\{0\}$, les idéaux principaux $< F >$, où $F(X,Y)$ est irréductible et les idéaux $< X-a, Y-b >$, $a,b\in\mathbf{C}$.*

□

Corollaire 6.3.3 *Les idéaux maximaux de de $\mathbf{C}[X,Y]$ sont les idéaux $< X-a, Y-b >$, $a,b\in\mathbf{C}$.*

Corollaire 6.3.4 (Nullstellensatz de Hilbert, ici en dimension deux) *Soit I un idéal propre de $\mathbf{C}[X,Y]$. Il existe alors $(a,b)\in\mathbf{C}^2$ tel que $\forall F\in I$, $F(a,b)=0$.*

Preuve. - En effet, I est inclus dans un idéal maximal $< X-a, Y-b >$. □

6.4 Exercices sur le chapitre 6

Exercice 6.4.1 Soient A un anneau intègre et S une partie multiplicative de A. Montrer que $(S^{-1}A)[X]$ et $S^{-1}(A[X])$ sont isomorphes. On donnera un sens précis à la deuxième notation.

Exercice 6.4.2 1) Quels sont les facteurs irréductibles de X^4-1, de X^4+1, de X^4+X^2+1 dans $\mathbf{Z}[X]$, dans $\mathbf{Q}[X]$, dans $\mathbf{R}[X]$, dans $\mathbf{C}[X]$?
2) Soit $a \in \mathbf{Z} \setminus \{0\}$. Montrer que X^4+aX^2-1 est irréductible dans $\mathbf{Z}[X]$.

Exercice 6.4.3 Montrer que le polynôme $1+aX$ est inversible dans $A[X]$ si, et seulement si, a est nilpotent. Si $1+aX$ n'est pas inversible et si $\mathfrak{M}$ un idéal maximal qui ne le contient pas (pourquoi en existe-t'il ?), montrer que $\mathfrak{P} := A \cap \mathfrak{M}$ est un idéal premier de A qui ne contient pas a. En déduire une nouvelle preuve du fait que le nilradical est l'intersection des idéaux premiers.

Exercice 6.4.4 Soit $x \in \mathbf{Q}$. Quel est le noyau du morphisme $P \mapsto P(x)$ de $\mathbf{Z}[X]$ dans $\mathbf{Q}$?

Exercice 6.4.5 Pour que l'anneau $A[X]$ soit principal, il faut, et il suffit, que A soit un corps. À quelle condition $A[X]$ est-il un corps ?

Exercice 6.4.6 Soit A un anneau factoriel et soit $a \in A$. L'anneau $A[X]/ < X^2-a >$ est-il intègre ? Intégralement clos ? Factoriel ?

Exercice 6.4.7 1) Soient A un anneau factoriel et $p \in A$ un irréductible. Soit $P = a_0X^n + \cdots + a_n \in A[X]$ tel que $p \not| a_0$, $p|a_1, \ldots, p|a_n$ et $p^2 \not| a_n$. Démontrer que P est irréductible (critère d'Eisenstein).
2) Soit $p \in \mathbf{N}$ un nombre premier. Démontrer que le polynôme $P := X^{p-1} + \cdots + 1$ est irréductible. (Appliquer le critère d'Eisenstein au polynôme $P(X+1)$.)

Exercice 6.4.8 Soient A un anneau factoriel de corps des fractions K et $F, G \in K[X]$ unitaires tels que $FG \in A[X]$. Démontrer que $F, G \in A[X]$.

Exercice 6.4.9 1) Soit v une valuation discrète sur le corps commutatif K, autrement dit, une application de K dans $\mathbf{Z} \cup \{+\infty\}$ telle que : $v^{-1}(+\infty) = \{0\}$; $v(a+b) \geq \min(v(a), v(b))$; et $v(ab) = v(a) + v(b)$. Montrer que $v^{-1}(\mathbf{N} \cup \{+\infty\})$ est un anneau de valuation discrète, autrement dit un anneau local (*cf.* l'exercice 3.6.8 du chapitre 3) principal qui n'est pas un corps.
2) Soient A un anneau de valuation discrète et p un générateur de son idéal principal. On note : $v_p(a) := \sup\{m \in \mathbf{N} \mid p^m | a\}$. Montrer que v_p s'étend en une valuation discrète sur le corps des fractions de A, telle que $A = v^{-1}(\mathbf{N} \cup \{+\infty\})$. Vérifier que cette construction est la réciproque de la construction précédente. Montrer que tout idéal non nul I de A est engendré par p^m, où $m := \min v_p(I)$.

Exercice 6.4.10 1) Dans l'anneau $A := \mathbf{Z}[X]/ < 2(X^2-1) >$, on note $\dot{2}$ la classe de 2 et x la classe de X. Vérifier que les éléments $\dot{2}$ et $y := \dot{2}x$ engendrent le même idéal. Vérifier que, si $y = \dot{2}x'$, alors $x' = x + (x^2-1)u$ pour un certain $u \in A$.
2) Notons $U(X) \in \mathbf{Z}[X]$ un antécédent de u et $X' = X + (X^2-1)U(X)$, qui est donc un antécédent de x' dans $\mathbf{Z}[X]$. Montrer que l'image de X' par la surjection canonique $\mathbf{Z}[X] \to \mathbf{F}_2[X]$ est égale à l'image de x' par la surjection canonique $A \to \mathbf{Z}[X]/ < 2 >$, modulo l'identification naturelle de $\mathbf{Z}[X]/ < 2 >$ avec $\mathbf{F}_2[X]$. En déduire que, si x' est inversible dans A, alors l'image $X + (X^2-1)\overline{U}$ de X' dans $\mathbf{F}_2[X]$ est inversible. Vérifier que c'est impossible.
3) Les éléments $\dot{2}$ et y sont-ils associés ?

Table des matières