Chapitre 1

Anneaux et Idéaux

Sommaire

1 Définitions . . . 2
1.1 Def et Exples . . . 2
1.2 Premiers constructeurs . . . 2
1.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$ . . . 3
1.4 Anneaux des polynômes . . . 4
1.5 Anneau des entiers de Gauss . . . 5
1.6 Petits anneaux . . . 5
2 Inversibilité et divisibilité . . . 6
2.1 Inversibilité . . . 6
2.2 Divisibilité . . . 6
3 Anneaux intègres . . . 7
4 Corps . . . 7
5 Morphismes, idéaux et anneaux quotients . . . 8
5.1 Morphismes . . . 8
5.2 Idéal . . . 9
5.3 Anneau quotient . . . 10
5.4 Propriétés des idéaux . . . 11
6 Anneaux euclidiens . . . 12
6.1 Définition et Idéaux . . . 12
6.2 Pgcd et ppcm . . . 13
6.3 Calcul des Pgcd et ppcm . . . 14
6.4 Factorisation . . . 14
7 Anneau $\mathbb{K}[X]$ . . . 15
7.1 Racines et Dérivation . . . 15
7.2 Irréductibilité . . . 18
A Petits degrés . . . 18
B Nombres complexes . . . 18
C Nombres réels . . . 18
D Nombres entiers et rationnels . . . 19
8 Théorème Chinois et Applications . . . 21

1 Définitions

1.1 Def et Exples

Définition I.1: Anneau

Soit A un ensemble muni de deux lois internes $+$ et $*$: $(A, +, *)$ est un *anneau* si $(A, +)$ est un groupe abélien (neutre noté 0), $*$ est commutative, associative, distributive par rapport à $+$ et possède un neutre (noté 1).

Remarque. Dans certains ouvrages, on ne demande pas que $*$ soit commutative. Dans ce cas, ce que nous appelons anneau s'appelle anneau commutatif.

Exemples 1. Les ensembles suivants sont des annneaux.

(i) L'ensemble $(\mathbb{Z}, +, \times)$ des entiers relatifs.
Ceci est l'exemple principal qu'il faut toujours garder en tête.

(ii) Les ensembles $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
Ces exemples ont une propriété supplémenntaires : tous les éléments de A sauf 0 ont un inverse pour $\times$.

(iii) L'espace des polynômes $\mathbb{R}[X]$.
Ceci est le deuxième exemple à garder en tête.

(iv) Plus compliqué : $\mathbb{R}[X, Y]$ l'anneau des polynômes à 2 variables et coefficients réels.

Les ensembles suivants ne sont pas des annneaux. *Trouver un argument expliquant que ces esembles ne sont pas annneaux.*

Exemples 2. (i) L'ensemble $\mathbb{N}$ des entiers naturels.

(ii) L'ensemble $2\mathbb{Z}$ des entiers pairs.

(iii) L'espace des polynômes $\mathbb{R}_n[X]$ de degré inférieur à n.

(iv) L'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices.

A chaque fois, les opérations $+$ et $\times$ sont les classiques.

1.2 Premiers constructeurs

Comme pour les groupes, on a une notion de sous-anneau :

Définition I.2: Sous-Anneau

Soit $(A, +, *)$ un anneau, $B \in \mathcal{P}(A)$: B est un *sous-anneau* de A si $0 \in B$, $1 \in B$ et B est stable pour les lois $+$, $a \mapsto -a$ et $*$.

Exemples 3. (i) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.

(ii) $\mathbb{R}$ est un sous-anneau de $\mathbb{R}[X]$.

(iii) $\{\frac{p}{2^n} \ : \ p \in \mathbb{Z}\ n \in \mathbb{N}\}$ est un sous-anneau de $\mathbb{Q}$.

(iv) L'ensemble $\mathbb{Z}[i] := \{x + iy \ : \ x, y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Il est appelé l'anneau des entiers de Gauss.

Comme pour les groupes, on a une notion de produit :

Définition I.3: Produit d'Anneaux

Soit $(A, +, *)$ et $(B, +, *)$ deux anneaux. On munit $A \times B$ des lois et éléments suivants :

$0 := (0, 0)$ et $1 := (1, 1)$.

$(a,b)+(a',b')=(a+a',b+b')$ pour tout $a,a'\in A$ et $b,b'\in B$.

$(a,b)*(a',b')=(a*a',b*b')$ pour tout $a,a'\in A$ et $b,b'\in B$. On obtient ainsi un anneau $(A\times B,+,*)$.

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

Fixons un entier naturel $n\geqslant 2$. On définit une relation d'équivalence sur $\mathbb{Z}$ (la congruence modulo n) :

$$a\equiv b \quad\Longleftrightarrow\quad n\mid a-b.$$

La classe d'équivalence de $a\in\mathbb{Z}$ est la partie suivante

$$a+n\mathbb{Z}:=\{a+kn\ :\ k\in\mathbb{Z}\}.$$

Ces classes forment une partition de $\mathbb{Z}$ en n parties deux à deux distinctes :

$$\mathbb{Z}=n\mathbb{Z}\cup(1+n\mathbb{Z})\cup\cdots\cup(n-1+n\mathbb{Z}).$$

Par définition $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble de ces n parties de $\mathbb{Z}$. Attention, un élément de $\mathbb{Z}/n\mathbb{Z}$ est une partie de $\mathbb{Z}$. En particulier le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est n.
On définit deux opérations $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par les formules suivantes :

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}):=(a+b)+n\mathbb{Z}\in\mathbb{Z}/n\mathbb{Z}$$
$$(a+n\mathbb{Z})\times(b+n\mathbb{Z}):=(ab)+n\mathbb{Z}\in\mathbb{Z}/n\mathbb{Z}$$

pour tout $a,b\in\mathbb{Z}$.
Ces définitions posent une question. En effet, les membres de droite ne doit dépendre que $(a+n\mathbb{Z})$ et $(b+n\mathbb{Z})$. Or à priori, les membres de droite dépendent de a et b, utiles pour calculer $a+b$ et ab. Montrons que ceci n'est qu'apparence pour $+$:
Soit a' et b' dans $\mathbb{Z}$ tels que $a+n\mathbb{Z}=a'+n\mathbb{Z}$ et $b+n\mathbb{Z}=b'+n\mathbb{Z}$. Alors il existe k et l dans $\mathbb{Z}$ tels que $a'=a+nk$ et $b'=b+nl$. Mais alors,

$$a'+b'+n\mathbb{Z}=a+nk+b+nl+n\mathbb{Z}=a+b+n(k+l+\mathbb{Z})=(a+b)+n\mathbb{Z}.$$

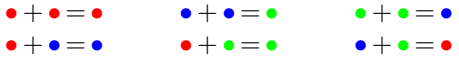
Théorème I.4. Anneau $\mathbb{Z}/n\mathbb{Z}$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de ces deux lois $+$ et $\times$ est un anneau.

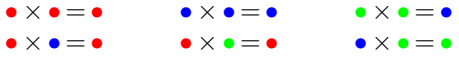
Démonstration. Chaque identité est une simple vérification laissée en exercice. □

Exemple $n=3$.

Les traits de la graduation représentent les entiers relaturels. Les rouges sont ceux de $3\mathbb{Z}$, les bleus ceux de $1+3\mathbb{Z}$ et les verts ceux de $2+3\mathbb{Z}$. Le fait que chaque trait est une couleur et une seule dit que ces parties forment une partition des entiers.
Les opérations $+$ et $\times$ sont définie sur ces parties. Si on représente une partie par sa couleur, on obtient



De même pour le produit, on obtient :



Revenons à $\mathbb{Z}/n\mathbb{Z}$. L'élément $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ est noté $\bar{k}$. En particulier le n est sous-entendu bien que très important.
Les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$ s'écrivent alors :

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Exercice 1. *Dresser de même, les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.*

1.4 Anneaux des polynômes

Soit A un anneau et X un symbole. On pose

$$A[X] := \{\sum_{n=0}^{\infty} a_n X^n \ : \ a_n \in A \quad \text{et } \exists N \quad \forall n \geqslant N a_n = 0\}.$$

La condition sur les coefficients a_n dit que tous sauf un nombre fini sont nuls. Lorsq'on écrit un polynôme, on oublie les termes de la forme $0X^n$, si bien que la somme devient finie. Il est aussi important de comprendre que la somme est formelle. Ce qui signifie que par définition $\sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} b_n X^n$ si et seulement si $a_n = b_n$ pour tout n.
On définit les deux opérations $+$ et $\times$ sur $A[X]$ par les formules suivantes :
Pour

$$P = \sum_{n=0}^{\infty} a_n X^n \qquad Q = \sum_{n=0}^{\infty} b_n X^n,$$

on a

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

et

$$PQ = \sum_{n=0}^{\infty} c_n X^n \text{ où } c_n = \sum_{k+l=n} a_k b_l.$$

La formule qui définit c_n a bien un sens car seulement un nombre fini de termes apparaissent. Combien ? Par ailleurs, PQ est bien un polynôme car les c_n sont presque tous nuls.

Proposition I.5: Anneau des polynômes

L'ensemble $(A[X], +, \times)$ est un anneau.

La preuve qui est une simple vérification est laissée en exercice.

Convention. On fait le choix d'omettre $0X^k$, X^0 et de noter $1X^k$ par X^k. Ainsi $1 + X^3 + 2X^6 \in \mathbb{R}[X]$. En effet

$$a_n = \begin{cases} 1 & \text{si } n = 0 \text{ ou } 3 \\ 2 & \text{si } n = 6 \\ 0 & \text{sinon} \end{cases}$$

Fonction associée. Soit $P \in A[X]$. Alors, on obtient une fonction

$$\tilde{P} \ : \ A \longrightarrow A,$$

dont la valeur $P(a)$ s'obtient à substituer a à X dans P.
Si $A = \mathbb{R}$, on obtient les fonctions polynômiales que vous connaissez bien. Pour d'autres anneaux, les choses peuvent être plus subtiles.

Exemple 4. Prenons $A = \mathbb{Z}/2\mathbb{Z}$ dont on note les éléments 0 et 1. Alors $P = 1 + X$, $Q = 1 + X^3$ sont deux éléments distincts de $A[X]$ car ils n'ont pas les mêmes coefficients.
On calcule $\tilde{P}(0) = 1$, $\tilde{P}(1) = 1 + 1 = 0$, $\tilde{Q}(0) = 1$ et $\tilde{Q}(1) = 1 + 1 = 0$. Donc les fonctions $\tilde{P}$ et $\tilde{Q}$ sont égales.

1.5 Anneau des entiers de Gauss

L'ensemble $\mathbb{Z}[i] := \{x + iy \ : \ x, y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Il est appelé l'anneau des entiers de Gauss.

1.6 Petits anneaux

Dans cette section, on étudie les anneaux de petits cardinaux 2,3 et 4.

Proposition I.6

Dans un anneau $(A, +, \times, 0, 1)$, on a, pour tout $a \in A$:

$$0 \times a = 0 \qquad -1 \times a = -a.$$

Ici, $-a$ signifie l'unique élément tel que $a + (-a) = 0$ (cad l'inverse de a pour la loi $+$).

Démonstration. En effet, $0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a$. Donc $0 \times a$ est l'élément neutre pour $+$, c'est-à-dire 0.
On a aussi $-1 \times a + a = -1 \times a + 1 \times a = (-1 + 1) \times a = 0 \times a = 0$. Donc $-1 \times a$ est bienl'inverse de a pour $+$. □

Exercice 2. *Justifier chacune des égalités de la preuve ci-dessus à l'aide de la définition d'un anneau.*

Cardinal 2. Soit A un anneau à deux éléments. Alors $A = \{0, 1\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Les valeurs noires s'obtiennent par définition des éléments neutres ou la proposition ci-dessus. La valeur rouge s'obtient en remarquant que 0 doit apparaître sur la ligne de 1 car 1 a un inverse pour $+$.
Ainsi $\mathbb{Z}/2\mathbb{Z}$ est le seul anneau à 2 éléments.

Cardinal 3. Soit A un anneau à trois éléments. Alors $A = \{0, 1, a\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

$\times$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Les valeurs noires s'obtiennent par définition des éléments neutres ou la proposition ci-dessus. La valeur rouge s'obtient par élimination : $1 + 1 = 1$ est impossible car $1 \neq 0$. Les valeurs vertes s'obtiennent par symétrie ($+$ est commutatif) et bijection de l'application $y \mapsto x + y$ est bijective. La valeur verte se justifie ainsi : $a = 1 + 1$; donc $a \times a = (1 + 1) \times a = a + a = 1$.
Ainsi $\mathbb{Z}/3\mathbb{Z}$ est le seul anneau à 3 éléments.

Cardinal 4. A partIr de 4 les choses se compliquent. Il y a 4 possibilités, mais cela est un peu long. Si cela vous amuse vous pouvez essayer de continuer le raisonnement ci-dessous, bien que cela puisse être long.
Réciproquement, les pages précédentes de ce chapitre permettent de voir que $\mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$. Mais il y a d'autres exemples...

Soit A un anneau à quatre éléments. Alors $A = \{0, 1, a, b\}$. Ses tables d'addition et de multiplication s'écrivent alors :

$+$	0	1	a	b
0	0	1	a	b
1	1	$x?$		
a	a			
b	b			

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

La lettre x ne peut être 1 (chaque ligne est une permutation des éléments de A). Donc, $x = 0$, a ou b. Quitte à changer les notations (entre a et b) on peut éliminer le dernier cas.

2 Inversibilité et divisibilité

2.1 Inversibilité

Un point important des anneaux est que $-x$ existe toujours alors que x^{-1} par forcément. D'où la définition suivante :

Définition I.7: Elément inversible

Soit $(A, +, \times, 0, 1)$ un anneau. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = 1$:

$$\exists b \in A \qquad ab = 1.$$

On note A^* l'ensemble des éléments inversibles.

Exemples 5. Voici quelques exemples.

(i) On a $\mathbb{Z}^* = \{\pm 1\}$ et $\mathbb{R}[X]^* = \mathbb{R}^* = \mathbb{R} - \{0\}$.

(ii) Plus difficile $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.
Pour le montrer, on part de $zz' = 1$ et on s'intéresse au module $|z|$ de z.

(iii) $(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\}$
On peut le montrer en dressant la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

On peut vérifier que $(A^*, \times, 1)$ est un groupe abélien.

2.2 Divisibilité

Bien que b^{-1} n'est pas de sens dans un anneau, il se peut que $\frac{a}{b}$ en ait un. Penser à $\frac{6}{2}$ dans $\mathbb{Z}$.
D'où la définition suivante :

Définition I.8: Elément inversible

Soit $(A, +, \times, 0, 1)$ un anneau et $a, b \in A$ avec $b \neq 0$. On dit que b *divise* a s'il existe $c \in A$ tel que $a = bc$ et on écrit $b \,|\, a$.

Dans $\mathbb{Z}$ on retrouve bien la divisibilité à laquelle nous sommes habitués. Voici un anneau dans lequel les choses sont plus compliquées.

Exemple 6. Posons $A = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$. On peut vérifier que A est un sous-anneau de $\mathbb{C}$. Comme $\mathbb{Z} \subset A$, on a $6 = 2 \times 3$ et 2 et 3 divisent 6. Mais on a aussi

$$6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

et $1 \pm i\sqrt{5}$ divisent aussi 6.
En revanche, on peut montrer que $1 + i\sqrt{5}$ et 2 n'ont pas de diviseur commun. De même, $1 + i\sqrt{5}$ et 3 n'ont pas de diviseur commun.

On pourra remarquer que si $b \in A*$ alors b divise a pour tout a. Ce sont les relations de divisibilité triviales. Un élément de A est dit irréductible si ces seuls diviseurs viennent de relations de divisibilité triviales. Plus précisément :

Définition I.9: Elément irréductible

Soit $p \in A$. L'élément p est dit *irréductible*, si p n'est pas inversible et

$$p = ab \quad \Rightarrow \quad a \text{ ou } b \text{ est inversible.}$$

Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés. De manière plus générale, dans ces questions de divisibilité un élément ou son produit avec un inversible jouent les même rôle.

3 Anneaux intègres

Vous avez appris il y a longtemps que pour qu'un produit soit nul, il faut qu'un des terme le soit. Ceci est vrai pour les nombres réels, mais pas pour les matrices (qui ne forment pas un anneau). Dans les anneaux, ça dépend. D'où la définition :

Définition I.10: Anneau intègre

L'anneau A est dit *intègre* si

$$\forall a, b \in A \qquad (ab = 0 \quad \Rightarrow \quad a = 0 \text{ ou } b = 0).$$

Exemples 7. (i) $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}[X]$, $\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{5}]$ sont intègres.

(ii) $\mathbb{Z}/3\mathbb{Z}$ est intègre (comment cela se lit-il sur sa table de multiplication ?).

(iii) $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre car $\bar{2}.\bar{2} = \bar{4}$.

(iv) $\mathbb{Z} \times \mathbb{Z}$ n'est pas intègre car $(1, 0)(0, 1) = 0$.

Définition I.11: Elément premier

Soit $p \in A$ supposé intègre. L'élément p est dit *premier*, si p n'est ni nul ni inversible et si

$$p \text{ divise } ab \quad \Rightarrow \quad p \text{ divise } a \text{ ou } b.$$

Proposition I.12: Premier vs Irréductible

Soit A un anneau intègre. Alors tout élément premier est irréductible.

Exemple 8. Trouver, dans les pages qui précèdent, un exemple montrant que la réciproque est fausse.

4 Corps

Définition I.13: Corps

Un corps $(K, +, \times)$ est un anneau dont tout élément non nul est inversible :

$$\forall a \in A^* \qquad \exists b \in A \quad ab = 1.$$

Exemples 9. (i) Les corps que vous connaissiez en sont bien : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) L'ensemble $\mathbb{R}(X)$ des fractions rationelles est un corps.

(iii) $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps.

(iv) Le sous-anneau $\mathbb{Q} + i\mathbb{Q}$ de $\mathbb{C}$ est un corps.

(v) $\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps. *Trouver un élément non nul et non inversible.*

(vi) $\mathbb{Z}$, $\mathbb{R}[X]$, $\mathbb{Z}[i]$ ne sont pas des corps.
Trouver un élément non nul et non inversible pour chacun de ces anneaux.

5 Morphismes, idéaux et anneaux quotients

5.1 Morphismes

Définition I.14: Morphisme

Soit A et B deux anneaux. Un *morphisme* f *de* A *vers* B est une application $f : A \longrightarrow B$ telle que

(i) $f(0) = 0$ et $f(1) = 1$;

(ii) $f(a + a') = f(a) + f(a')$ pour tout $a, a' \in A$;

(iii) $f(-a) = -f(a)$ pour tout $a \in A$,

(iv) $f(aa') = f(a)f(a')$ pour tout $a, a' \in A$.

Remarque. On pourra remarquer que f est en particulier un morphisme de groupes pour la loi $+$. En particulier, la définition ci-dessus est redondante car $f(a + a') = f(a) + f(a')$ implique $f(0) = 0$ et $f(-a) = -f(a)$.

Il est immédiat de vérifier que la composé de deux morphismes est un morphisme.
De même, la réciproque d'un morphisme bijectif f est un morphisme. On dit alors que f est un *isomorphisme*.

Voici quelques exemples de morphismes.

Exemples 10. (i) Pour $n \geqslant 2 \in \mathbb{N}$, l'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \bar{k} = k + n\mathbb{Z} \end{array}$$

est un morphisme.

(ii) Soit $a \in \mathbb{R}$. Alors, l'application

$$\begin{array}{rccc} \mathrm{ev}_a : & \mathbb{R}[X] & \longrightarrow & \mathbb{R} \\ & P & \longmapsto & P(a) \end{array}$$

est un morphisme.

(iii) Soit A et B deux anneaux. Alors, l'application

$$\begin{array}{ccc} A \times B & \longrightarrow & A \\ (a, b) & \longmapsto & a \end{array}$$

est un morphisme.

(iv) Soit A et B deux anneaux. Alors, l'application

$$\begin{array}{ccc} A & \longrightarrow & A \times B \\ a & \longmapsto & (a, 0) \end{array}$$

n'est pas un morphisme. Pourquoi ?

(v) L'application

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{C} \\ (x, y) & \longmapsto & x + iy \end{array}$$

n'est pas un morphisme. Pourquoi ?

(vi) Posons

$$A = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R}\}.$$

Alors $(A, 0, I_2, +, .)$ où . est le produit matriciel, I_2 la matrice identité est un anneau. De plus l'application

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & A \\ a + ib & \longmapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array}$$

est un isomorphisme d'anneaux.

Le *noyau de* $f : A \longrightarrow B$ est son noyau lorsque f est pensé comme un morphisme de groupes :

$$\mathrm{Ker} f = \{a \in A : f(a) = 0\}.$$

D'autres exemples de morphismes :

Proposition I.15: Propriété universelle de l'anneau des polynômes

Soit A et B deux anneaux, b un élément de B et $\theta : A \longrightarrow B$ un morphisme. Alors, il existe un unique morphisme d'anneaux $\tilde{\theta} : A[X] \longrightarrow B$ tel que

(i) pour tout $a \in A$, $\tilde{\theta}(a) = \theta(a)$;

(ii) $\tilde{\theta}(X) = b$.

5.2 Idéal

Définition I.16: Idéal

Soit A un anneau commutatif, $I \subset A$. Alors, I est un *idéal* ssi $(I, +)$ est un sous-groupe de $(A, +)$ et pour tout $a \in A$, pour tout $x \in I$, $ax \in I$.

Proposition I.17: Intersection d'idéaux

Toute intersection d'idéaux est un idéal.

La preuve est une simple vérification.

Définition I.18: Idéal Engendré par une Partie

Soit $P \subset A$ non vide. L'intersection de tous les idéaux de A contenant P est le plus petit idéal contenant P. On l'appelle *idéal engendré par* P, noté (P).

Théorème I.19. Idéal engendré

L'idéal engendré par P est $\{\sum_{i=1}^{r} u_i a_i \ / \ r \in \mathbb{N}, a_i \in P, u_i \in A\}$.
Remarque : Soit $a \in A$: L'idéal engendré par a est aA. On le note (a). Plus généralement, si $P = \{a_1, \ldots, a_s\}$ on note $(a_1, \ldots, a_s) = a_1 A + \cdots + a_s A$.

Démonstration. L'ensemble est bien stable par $+$, $-$ et multiplication par n'importe quel élément de A. C'est donc un idéal.
Soit I est un idéal contenant P. Comme il est stable par $+$ et multiplication par tout $a \in A$ il contient l'ensemble. □

Exemples 11. (i) L'idéal (2) engendré par 2 dans $\mathbb{Z}$ est l'ensemble des nombres pairs.

(ii) L'idéal $(6, 9)$ engendré par 6 et 9 est l'ensemble des multiples de 3.
La preuve de ce fait est laissée en exercice.

(iii) L'idéal (X) engendré par le polynôme X dans $\mathbb{R}[X]$ est l'ensemble des polynômes qui s'annulent en 0.

(iv) L'idéal $(2, X)$ engendré par les polynômes 2 et X dans $\mathbb{Z}[X]$ est l'ensemble des polynômes dont le coefficient constant est pair.
La preuve de ce fait est laissée en exercice.

(v) L'idéal engendré par deux idéaux I et J est l'ensemble

$$I + J = \{a + b \,:\, a \in I,\, b \in J\}.$$

Théorème I.20. Noyau et Idéal

Le noyau d'un morphisme d'anneaux est un idéal.

Démonstration. Soit f un tel morphisme. Comme c'est un morphisme de groupe pour $+$, son noyau est un sous-groupe. De plus, le calcul

$$f(ab) = f(a)f(b) = f(a)0 = 0$$

montre que si $b \in \mathrm{Ker} f$ alors $ab \in \mathrm{Ker} f$. □

5.3 Anneau quotient

Nous allons faire une construction qui montre la réciproque du théorème précédent : tout idéal est le noyau d'un morphisme.
Un idéal I de A est dit *strict* si $I \neq A$. Ceci équivaut à $1 \notin A$.

Théorème I.21. Anneau quotient

Soit I un idéal strict de A. On pose

$$A/I = \{a + I \,:\, a \in A\}$$

inclus dans l'ensemble des parties de A. Il existe une unique structure d'anneau sur A/I telle que l'application

$$\begin{array}{rccc} \pi : & A & \longrightarrow & A/I \\ & a & \longmapsto & a + I \end{array}$$

soit un morphisme d'anneaux.

Les lois sont données par les formules, pour tout $a, b \in A$:

$$\begin{array}{rcl} (a + I) + (b + I) & = & (a + b) + I \\ (a + I)(b + I) & = & (ab) + I \end{array}$$

La preuve est directe et nous l'avons faite dans le cas suivant : $A = \mathbb{Z}$ et $I = n\mathbb{Z} = (n)$. Nous avions obtenu l'anneau $\mathbb{Z}/n\mathbb{Z}$. Le cas général ne posant aucune difficulté supplémentaire est omise ici.
Souvent on note $a + I =: \bar{a}$, lorsque la référence à I est claire.
Application : Construction des nombres complexes.
La relation clé dans le corps des nombres complexes est bien entendu $i^2 = -1$. L'idée est donc de partir de $\mathbb{R}[X]$ est d'imposer $X^2 = -1$ c'est-à-dire $X^2 + 1 = 0$ par quotient. On obtient l'application

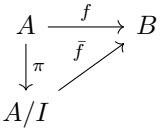
$$\begin{array}{rccc} \iota : & \mathbb{C} & \longrightarrow & \mathbb{R}[X]/(X^2 + 1) \\ & a + ib & \longmapsto & a + bX + (X^2 + 1)\mathbb{R}[X] = \overline{a + bX} \end{array}$$

qui est isomorphisme d'anneaux.

Le théorème de factorisation permet d'obtenir des isomorphismes comme ι.

Théorème I.22. Factorisation des morphismes

Soit $f : A \longrightarrow B$ un morphisme d'anneaux et I un idéal strict de A.
Si $I \subset \mathrm{Ker} f$ alors il existe un unique morphisme $\bar{f} : A/I \longrightarrow B$ tel que $\bar{f} \circ \pi = f$.



De plus, $\bar{f}$ est injectif si et seulement si $I = \mathrm{Ker} f$. Enfin, $\bar{f}$ est surjectif si et seulement si f l'est.

Application. Soit $I = (P)$ l'idéal de $\mathbb{R}[X]$ engendré par un polynôme P. La remarque est que si $P(x) = 0$, alors $Q(x) = 0$ pour tout $Q \in (P)$. Ainsi pour $P = X^2 - 1$ on obtient un morphisme

$$\begin{array}{rccc} f : & \mathbb{R}[X] & \longrightarrow & \mathbb{R} \times \mathbb{R} \\ & P & \longmapsto & (P(-1), P(1)) \end{array}$$

tel que $I \subset \mathrm{Ker} f$. On obtient donc $\bar{f} : \mathbb{R}[X]/(X^2 - 1) \longrightarrow \mathbb{R} \times \mathbb{R}$ qui est en fait un isomorphisme.

Exercice 3. *Montrer que $\mathbb{R}[X]/(X^2 - 4X)$ est isomorphe à $\mathbb{R} \times \mathbb{R}$.*
Plus difficile, montrer que $\mathbb{R}[X]/(X^2 - 2X + 1)$ est isomorphe à $\mathbb{R} \times \mathbb{R}$ muni d'une loi à définir.
Montrer que $\mathbb{R}[X]/(X^2 - 4X)$ et $\mathbb{R}[X]/(X^2 - 2X + 1)$ ne sont pas isomorphes.

Correction du cas $X^2 - 2X + 1 = (X - 1)^2$. Les multiples de ce polynômes sont ceux qui vérifient $P(1) = P'(1) = 0$. Donc l'application

$$\begin{array}{rccc} \theta : & \mathbb{R}[X]/(X^2 - 2X + 1) & \longrightarrow & \mathbb{R} \times \mathbb{R} \\ & P & \longmapsto & (P(1), P'(1)) \end{array}$$

est une bijection linéaire. En revanche θ n'est pas un morphisme d'anneau. En revanche, elle l'est pour la loi

$$(a, b) \star (a', b') := (aa', ab' + a'b).$$

5.4 Propriétés des idéaux

Définition I.23: Idéal Premier

Un idéal I d'un anneau A est dit premier si

$$\forall a, b \in A \qquad (ab \in I \ \Rightarrow a \in I \text{ ou } b \in I).$$

Cette propriété s'interprète facilement en terme de quotients.

Proposition I.24: Quotient par idéal premier

Soit I un idéal strict de A. Alors I est premier si et seulement si A/I est intègre.

Démonstration. Considérons $\pi : A \longrightarrow A/I$.
Supposons A/I est intègre. Soit a et b dans A. Alors $ab \in I$ si et seulement si $\pi(ab) = 0$ si et seulement si $\pi(a)\pi(b) = 0$. Alors, cette dernière égalité implique que $\pi(a) = 0$ ou $\pi(b) = 0$. C'est-à-dire $a \in I$ ou $b \in I$. Donc I est premier.
Supposons maintenant I premier. Soit deux éléments de A/I dont le produit fait zéro. On écrit ces deux éléments $\pi(a)$ et $\pi(b)$ avec a et b dans A. Alors $0 = \pi(a)\pi(b) = \pi(ab)$. Donc $ab \in I$. Comme I est premier cela implique que $a \in I$ ou $b \in I$. Donc $\pi(a) = 0$ ou $\pi(b) = 0$. □

Définition I.25: Idéal Maximal

Un idéal I d'un anneau A est dit maximal si $I \subset J \subset A$ implique $J = I$ ou $J = A$.
Les seuls idéaux contenant I sont I et A.

Cette propriété s'interprète facilement en terme de quotients.

Proposition I.26: Quotient par idéal maximal

Soit I un idéal strict de A. Alors I est maximal si et seulement si A/I est un corps.

Démonstration. Considérons $\pi : A \longrightarrow A/I$.
Supposons A/I est un corps. Soit J un idéal contenant strictement I. Soit $b \in J$ tel que $b \notin I$. Alors $\pi(b) \neq 0$. Donc il existe $c \in A$ tel que $\pi(c)\pi(b) = 1 = \pi(bc)$. Ceci se réécrit $1 - bc \in I \subset J$. Donc $1 = (1 - bc) + bc \in J$. Mais alors $J = A$.
Supposons maintenant I maximal. Soit $a \in A$ tel que $\pi(a) \neq 0$. Cela signifie que $a \notin A$. Considérons l'idéal $J = I + aA$ engendré par I et a. Comme I est maximal, $J = A$ et $1 \in J$. Donc il existe $b \in A$ et $i \in I$ tels que $1 = i + ab$. Mais alors $1 = \pi(ab) = \pi(a)\pi(b)$. Donc $\pi(a)$ est inversible.
On a bien montré que A/I est un corps. □

Ces derniers résultats montrent que I maximal implique I premier.

Exemples 12.
(i) L'idéal $(6) \subset \mathbb{Z}$ n 'est ni premier ni maximal. En revanche, (5) est maximal (donc premier).
(ii) $(X^2 + 1) \subset \mathbb{R}[X]$ est maximal.
(iii) $(X^2 - 1) \subset \mathbb{R}[X]$ n'est pas premier.
(iv) $(X) \subset \mathbb{Z}[X]$ est premier, non maximal.
(v) $(X^2 + Y^3) \subset \mathbb{C}[X, Y]$ est premier, non maximal.
(vi) $(3, X) \subset \mathbb{Z}[X]$ est maximal.

6 Anneaux euclidiens

6.1 Définition et Idéaux

Définition I.27: Anneau euclidien

Soit A un anneau intègre. On dit que A est euclidien s'il existe une fonction $N : A - \{0\} \longrightarrow \mathbb{N}$ telle que :

(i) $N(ab) \geqslant N(b)$, $\forall a, b \in A - \{0\}$
(ii) $\forall a, b \in A$, $b \neq 0$, $\exists (q, r) \in A$ tq. $a = bq + r$ $\quad (r = 0$ ou $N(r) < N(b)$

La fonction N est appelée **norme euclidienne**.

Exemples 13.
(i) $\mathbb{Z}$ est euclidien, avec $N(x) = |x|$. Ceci est la division euclidienne que l'on connait depuis l'école primaire.
(ii) Si $\mathbb{K}$ est un corps, $\mathbb{K}[x]$ est euclidien, avec $N(P) = deg(P)$. Ceci est la division euclidienne des polynômes.
(iii) $\mathbb{Z}[i] := \{m + in, (m, n) \in \mathbb{Z}^2\}$ est euclidien, avec $N(z = x + iy) = x^2 + y^2$.
Esquisse de démonstration. Soit $a, b \in A$, $b \neq 0$. On cherche q et r comme dans la définition. L'idée de base est que q est une approximation du quotient a/b que l'on connait dans $\mathbb{C}$. Posons donc $z = a/b \in \mathbb{C}$. Les points de $\mathbb{Z}[i]$ forme un réseau donc il existe $q \in \mathbb{Z}[i]$ tel que $|z - q| \leqslant \sqrt{2}/2$. Alors q convient.

Encore un peu de vocabulaire afin de décrire les idéaux des anneaux euclidiens. Un idéal I d'un anneau A est dit *principal* s'il est engendré par un élément. Un anneau est dit *principal* si tous ses idéaux le sont.

Théorème I.28. Euclidien et Principal

Tout anneau euclidien est principal.

Démonstration. Soit I un idéal de A. On regarde $N(I)$. Comme partie non vide de $\mathbb{N}$ elle a un minimum. Soit $b \in I$ tel que $N(b)$ soit égal à ce minimum. Montrons que

$$I = (b).$$

Il est clair que $(b) \subset I$.
Soit $a \in I$. Ecrivons $a = bq + r$ avec $r = 0$ ou $N(r) < N(b)$. Puisque $r = a - bq$ il appartient à I. Par minimalité de $N(b)$, on en déduit que $r = 0$. Mais alors, $a \in (b)$. □

On peut aussi comprendre les éléments inversibles. Regardons $\mathbb{Z}$ un élément non nul a est inversible ssi $|a| = 1$. Regardons $\mathbb{K}[X]$: un élément non nul P est inversible ssi $\deg(P) = 0$. En général, on a :

Proposition I.29: Eléments inversibles

Soit A un anneau euclidien dont on note N la norme. Soit $a \in A$ non nul. Alors a est inversible si et seulement si $N(a) = N(1)$.

Démonstration. Si $ab = 1$ alors $N(a) \leqslant N(1)$. Or $a = a \times 1$ implique que $N(1) \leqslant N(a)$. Donc si a est inversible alors $N(a) = N(1)$.
Réciproquement supposons que $N(a) = N(1)$. On fait la division euclidienne : $1 = aq + r$ avec $N(r) < N(r)$. Ce qui est impossible. Donc $r = 0$ et a est inversible. □

6.2 Pgcd et ppcm

Les pgcd et ppcm sont ceux que vous connaissez déjà sur $\mathbb{Z}$ et $\mathbb{K}[X]$. Cependant les concepts d'anneau euclidien et d'idéal permettent des définitions et démonstrations à la fois homogènes et élégantes. Soit donc A un anneau euclidien.
Une petite remarque préparatoire sous forme d'exercice.

Exercice 4. *Soit a et b non nuls dans A. Alors $(a) = (b)$ si et seulement s'il existe $c \in A$ inversible tel que $a = cb$.*

Définition I.30: pgcd

Soit $a_1, \ldots, a_s$ des éléments non tous nuls de A. Un élément $\delta \in A$ tel que $(a_1, \ldots, a_s) = (\delta)$ est appelé pgcd des éléments $a_1, \ldots, a_s$.
On note $\delta = a_1 \wedge \cdots \wedge a_s$. On peut remarquer que δ n'est défini qu'à un inversible près. Sur $\mathbb{Z}$ (resp. $\mathbb{K}[X]$), on fixe généralement cette indétermination en demandant que le pgcd soit positif (resp. unitaire).

Le nom pgcd est justifié par l'exercice suivant.

Exercice 5. *Soit q dans A non nul. Alors q divise tous les a_i si et seulement si q divise δ.*

Le lemme de Bezout est également facile à démontrer.

Exercice 6. Lemme de Bezout version 1.
Soit a et b dans A non nuls. Alors, il existe u et v dans A tels que $au + bv = a \wedge b$.

Définition I.31: éléments premiers entre eux

Soit $a_1, \dots, a_s$ des éléments non nuls de A. On dit qu'ils sont premiers entre eux si $a_1 \wedge \cdots \wedge a_s = 1$ c'est-à-dire si $(a_1, \dots, a_s) = A$.

Le lemme de Bezout est également facile à démontrer.

Exercice 7. Lemme de Bezout version 2.
Soit a et b dans A non nuls. Alors, a et b sont premiers entre eux si et seulement s'il existe u et v dans A tels que $au + bv = 1$.

Définition I.32: ppcm

Soit $a_1, \dots, a_s$ des éléments non nuls de A. Un élément $c \in A$ tel que $(a_1) \cap \cdots \cap (a_s) = (c)$ est appelé ppcm des éléments $a_1, \dots, a_s$.
On note $c = a_1 \vee \cdots \vee a_s$.

6.3 Calcul des Pgcd et ppcm

On se donne a et b non nuls dans A. On veut calculer $a \wedge b$ et $a \vee b$. Un premier résultat nous dit que la connaissance de l'un détermine l'autre.

Proposition I.33: Lien ppcm et pgcd

Il existe u inversible tel que

$$(a \wedge b)(a \vee b) = uab.$$

Démonstration. On pose $a' = a/(a \wedge b)$ et $b' = b/(a \wedge b)$. Comme $a' \wedge b' = 1$ et $a' \vee b' = (a \vee b)/(a \wedge b)$ il suffit de montrer que

$$(a' \vee b') = (a'b'),$$

sachant que $a' \wedge b' = 1$.
Autrement dit on peut supposer que $a \wedge b = 1$. Alors il existe u et v dans A tels que $au + bv = 1$.
Il est clair que $(ab) \subset (a)$. Donc $(ab) \subset (a) \cap (b) = (a \vee b)$.
Réciproquement montrons que $a \vee b \in (ab)$. Comme a divise $a \vee b$, il existe c tel que $a \vee b = ac$. Or

$$c = acu + bcv.$$

Puisque b divise bcv et $acu = u.(a \vee b)$ il divise c. Donc $c = bc'$. Ainsi $a \vee b = ac = abc'$. CQFD. □

Algorithme d'Euclide. Il s'agit d'un algorithme permettant de calculer $a \wedge b$. Il est basé sur la formule suivante. On suppose b non nul et soit $a = bq + r$ la division euclidienne alors

$$\begin{cases} a \wedge b = r \wedge b \\ 0 \wedge b = b \end{cases}$$

Pour obtenir l'algorithme, on réitère le procédé en divisant b par r pour ré-exprimer $r \wedge b$.

6.4 Factorisation

Comme nous commençons à le voir, le cadre des anneaux euclidiens (en fait principal suffit souvent) est un bon cadre où étendre les propriétés des entiers. Une propriété arithmétique fondamentale des entiers est la décomposition en produit de nombres premiers. Cela s'étend à notre cadre du jour : on dit qu'un anneau principal est factoriel.

Théorème I.34. Factoriel

Soit A un anneau euclidien et a un élément non nul de A. Alors, il existe des éléments irréductibles $p_1, \dots, p_s$ dans A, des entiers naturels non nuls $n_1, \dots, n_s$ et un élément inversible u tel que

$$a = u p_1^{n_1} \dots p_s^{n_s}.$$

De plus cette écriture est unique à l'ordre près et à multiplication des p_i et de u par des inversibles.

Un ingrédient clé pour montrer cela est le

Lemme I.35 (Lemme de Gauss)**.** *Soit a, b et c non nuls dans A. Si a divise bc et $a \wedge b = 1$ alors a divise c.*

Démonstration. On utilise encore Bezout : $au + bv = 1$. Alors $acu + bcv = c$. Donc a divise c. □

Preuve du théorème de Factorialité. Pour l'existence on fait une récurrence sur $N(a)$. Si a est irréductible, il n'y a rien à montrer. Sinon $a = bc$ avec b et c non inversibles. Alors $N(b) < N(a)$ et $N(c) < N(a)$. Par récurrence, on déduit que b et c admettent des décompositions. Donc a aussi.

Pour l'unicité supposons que

$$\prod_i p_i = u \prod_j q_j, \tag{6.1}$$

- avec p_i et q_i irréductibles et u inversible. Ici on remplace les exposant par des répétitions.
Il est clair que q_1 divisent le membre de droite. Donc il divise celui de gauche. Supposons que q_1 n'est pas conjugué à p_1. Comme ils sont irréductibles, il suit que $q_1 \wedge p_1 = 1$. Mais alors le lemme de Gauss implique que q_1 divise $\prod_{i \geqslant 2} p_i$. On recommence. On aura nécessairement à un moment q_1 divise p_i. On divise l'expression (6.1) par q_1 et on recommence (cad on fait une récurrence sur le nombre de q_i). □

Pour ceux qui auraient l'impression de ne rien avoir montré, il est intéressant de faire l'exercice suivant.

Exercice 8. *Posons $A = \{a + bi\sqrt{5} \,:\, a, b \in \mathbb{Z}\}$.*

(i) Montrer que A est un sous-anneau de $\mathbb{C}$.

(ii) Montrer que 2 et 3 sont irréductibles dans A.

(iii) Montrer que $1 \pm i\sqrt{5}$ sont irréductibles dans A.

(iv) En remarquant que $2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, montrer que A n'est pas euclidien.

7 Anneau $\mathbb{K}[X]$

Fixons un corps $\mathbb{K}$. Vous pouvez penser à $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$. Nous verrons d'autres exemples plus tard. Nous avons déjà vu que $\mathbb{K}[X]$ était un anneau euclidien : il vérifie donc Bezout, Gauss et il y a une unique décomposition en produit de polynômes irréductibles. Nous allons maintenant voir quelques techniques spécifiques à cet anneau.

7.1 Racines et Dérivation

Substitution. C'est l'opération la plus compliquée à comprendre. Soit

$$P = a_0 + a_1 X + \dots + a_d X^d$$

et Q deux polynômes. On pose alors

$$(P \circ Q)(X) = a_0 + a_1 Q(X) + \dots + a_d Q(X)^d.$$

Faisons un exemple : $P = 1 + X^3$ et $Q = 2 + X^2$:

$$\begin{aligned}(P \circ Q)(X) &= 1 + (2 + X^2)^3 \\ &= 9 + 3X^2 + 3X^4 + X^6.\end{aligned}$$

L'application $P \mapsto P \circ Q$ est linéaire mais PAS $Q \mapsto P \circ Q$.
Dérivation. L'ensemble $(1, X, X^2, \dots)$ est une base de $\mathbb{K}[X]$. On peut donc définir un endomorphisme D de $\mathbb{K}[X]$ on donnant l'image de ces monômes.

$$\begin{array}{rccll} D : & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] & \\ & X^k & \longmapsto & kX^{k-1} & \text{si } k \geqslant 1 \\ & 1 & \longmapsto & 0 & \end{array}$$

On a définit ainsi ce que l'on appelle la dérivation. Dans le cas où le corps est celui des réels cette dérivation coïncide avec la dérivation usuelle. On note souvent P' pour $D(P)$.
On a les règles de calculs usuelles de la dérivation :

Proposition I.36: Propriétés de la dérivation

Soit P et Q dans $\mathbb{K}[X]$. On a

$$D(PQ) = D(P)Q + PD(Q) \qquad (PQ)' = P'Q + QP'$$

et

$$D(P \circ Q) = D(Q).D(P) \circ Q \qquad (P \circ Q)' = Q' \times P' \circ Q.$$

Démonstration. Fixons Q. Les applications $P \mapsto D(PQ)$ et $P \mapsto D(P)Q + PD(Q)$ sont linéaires. Du coup il suffit de montrer l'égalité pour $P = X^k$.
Fixons maintenant $P = X^k$. Les applications $Q \mapsto D(PQ)$ et $Q \mapsto D(P)Q + PD(Q)$ sont linéaires. Du coup il suffit de montrer l'égalité pour $Q = X^l$.
Dans ce cas, on a

$$D(PQ) = D(X^{k+l}) = (k+l)X^{k+l-1}$$

et

$$D(P)Q + PD(Q) = D(X^k)X^l + X^k D(X^l) = kX^{k+l-1} + lX^{k+l-1} = (k+l)X^{k+l-1}.$$

Montrons maintenant la seconde égalité. Les applications $P \mapsto D(P \circ Q)$ et $P \mapsto D(Q) \times D(P) \circ Q$ sont linéaires. Du coup il suffit de montrer l'égalité pour $P = X^k$.
Dans ce cas, on a

$$D(P \circ Q) = D(Q^k) = kD(Q)Q^{k-1}$$

et

$$D(Q).D(P) \circ Q = D(Q).k.Q^{k-1}.$$

□

Evaluation – Racines.
Soit $a \in \mathbb{K}$. Alors on a une application évaluation

$$\begin{array}{rccl} \mathrm{ev}_a : & \mathbb{K}[X] & \longrightarrow & \mathbb{K} \\ & P & \longmapsto & P(a). \end{array}$$

On vérifie sans peine que ev_a est un morphisme d'anneaux. Son noyau est $\{P : P(a) = 0\}$. C'est un idéal maximal de $\mathbb{K}[X]$ car le quotient est isomorphe à $\mathbb{K}$. L'isomorphisme est donné par ev_a.

Proposition I.37: Racine et division

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de P si et seulement si $X - a$ divise P.

Démonstration. Si $P = (X - a)Q$, il est clair que $P(a) = 0$. Réciproquement supposons que $P(a) = 0$. On écrit la division euclidienne $P = Q(X - a) + R$ avec R nul ou de degré strictement inférieur à 1. Donc R est en fait un polynôme constant. Par ailleurs, $0 = P(a) = R(a)$. Donc R est nul et $X - a$ divise P. □

Définition I.38: Ordre d'une racine

Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}$. On dit que a est *racine d'odre au moins* α si $(X-a)^\alpha$ divise P.
On dit que a est *racine d'odre exactement* α si elle est racine d'ordre au moins α mais n'est pas d'odre au moins $\alpha+1$.

Proposition I.39: Ordre racine et dérivées

Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}$. Alors

(i) Si a est racine d'odre au moins α alors

$$P(a) = P'(a) = \cdots = P^{(\alpha-1)}(a) = 0.$$

(ii) Si de plus $\mathbb{K}$ est de caractéristique nulle, la réciproque de la première assertion est vrai.

Démonstration. Supposons d'abord que $(X-a)^\alpha$ divise P. Il existe alors $Q \in \mathbb{C}[X]$ tel que $P = (X-a)^\alpha Q$. On rappelle la formule le Leibnitz :

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)} g^{(k-i)}.$$

La preuve de cette formule se fait par récurrence sur k en utilisant la formule de dérivation d'un produit. On obtient pour P et $k \leqslant \alpha - 1$:

$$(P)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} ((X-a)^\alpha)^{(i)} Q^{(k-i)}. \tag{7.1}$$

On remarque alors que

$$((X-a)^\alpha)^{(i)} = (\alpha.(\alpha-1)\dots(\alpha-i+1))(X-a)^{\alpha-i} \quad \text{si } i \leqslant \alpha,$$

et

$$((X-a)^\alpha)^{(i)} = 0 \quad \text{si } i > \alpha.$$

En particulier, pour tout $i \leqslant k < \alpha$, on a

$$\Big(((X-z)^\alpha)^{(i)}\Big)(a) = 0.$$

En injectant dans la formule (7.1), on déduit que $P^{(k)}(a) = 0$.

Réciproquement, supposons que $P(a) = \cdots = P^{(\alpha-1)}(a) = 0$. Ecrivons la division euclidienne de P par $(X-a)^\alpha$:

$$P = (X-a)^\alpha Q + R,$$

avec $\deg(R) < \alpha$. L'assertion déjà démontrée implique que

$$R(a) = \cdots = R^{(\alpha-1)}(a) = 0.$$

Considérons le polynôme auxiliaire

$$S(X) = R(a+X) \quad R(X) = S(X-a).$$

La formule de dérivation d'un polynôme composé implique que

$$S^{(k)}(X) = R^{(k)}(a+X),$$

donc

$$S(0) = \cdots = S^{(\alpha-1)}(0) = 0.$$

Ecrivons $S = a_0 + a_1 X + \cdots + a_{\alpha-1} X^{\alpha-1}$. Par une récurrence immédiate, on montre que

$$S^{(k)}(0) = k! a_k \quad \forall k = 0, \ldots, \alpha - 1.$$

On en déduit que $S = 0$, puis que $R = 0$. Ainsi $(X - a)^\alpha$ divise P. □

7.2 Irréductibilité

A Petits degrés

En **petit degré**, il y a un critère simple d'irréductibilité.

Proposition I.40: Irréductibilité et racines

On a

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré supérieur à 2 n'a pas de racine.

(iii) Tout polynôme de degré 2 ou 3 qui n'a pas de racine est irréductible.

Démonstration. Soit P un polynôme. Il est irréductible, si pour tout A, B dans $\mathbb{K}[X]$ tels que $P = AB$, on a $\deg(A)$ ou $\deg(B)$ nul :

$$\forall A, B \in \mathbb{K}[X] \qquad (P = AB \Rightarrow \ (\deg(A) = 0 \text{ ou } \deg(B) = 0)).$$

Les trois énoncés de la proposition découlent facilement des deux assertions suivantes :

(i) $\deg(P) = \deg(A) + \deg(B)$;

(ii) P est divisible par un polynôme de degré un si et seulement si il a une racine.

□

En appliquant la proposition, on voit que $X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ est irréductible. Attention, il est possible qu'un polynôme sans racine ne soit pas irréductible. $(X^2 + 1)^2$ donne un exemple dans $\mathbb{R}[X]$.

B Nombres complexes

Théorème I.41. D'Alembert-Gauss

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

Ceci est bien une version du théorème de d'Alembert-Gauss qui dit que tout polynôme non constant sur $\mathbb{C}$ a une racine et donc est divisible par un polynôme de degré un.

C Nombres réels

Encore une façon de formuler le théorème de d'Alembert-Gauss.

Théorème I.42. D'Alembert-Gauss

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré 2 et de discriminant négatif.

D Nombres entiers et rationnels

On sort un peu du contexte en regardant les polynômes à coefficients entiers. Ce n'est pas un anneau euclidien.
Pour $P \in \mathbb{Z}[X]$ non nul on note $c(P)$ le pgcd des coefficients de P. Ce nombre est appelé le contenu de P.

Théorème I.43. Gauss

Soit P et Q dans $\mathbb{Z}[X]$ non nuls. Alors

$$c(PQ) = c(P)c(Q).$$

Cette formule est très simple et très utile. C'est la marque des grands...théorèmes.

Démonstration. Posons $\tilde{P} = P/c(P)$ et $\tilde{Q} = Q/c(Q)$. Ceux sont des polynômes à coefficients entiers et de contenu égal à 1. Il suffit de montrer que

$$c(\tilde{P}\tilde{Q}) = 1.$$

Soit p un nombre premier. Soit $\bar{P}$ (resp. $\bar{Q}$) le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ obtenu en considérant la classe dans $\mathbb{Z}/p\mathbb{Z}$ de chaque coefficient de $\tilde{P}$ (resp. $\tilde{Q}$). Comme $c(\tilde{P}) = 1$, $\bar{P}$ est non nul. Comme $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, on en déduit que $\bar{P}\bar{Q} \neq 0$. Donc p ne divise pas $c(\tilde{P}\tilde{Q})$. Vu l'arbitraire de p, on en déduit que $c(\tilde{P}\tilde{Q}) = 1$. □

Corollaire I.44: Irred dans $\mathbb{Z}$ et $\mathbb{Q}$

Soit $P \in \mathbb{Z}[X]$ tel que $c(P) = 1$. Alors se valent

(i) P est irréductible dans $\mathbb{Q}[X]$;

(ii) P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Un sens est évident. Réciproquement supposons que P est irréductible dans $\mathbb{Z}[X]$. Soit $P = AB$ dans $\mathbb{Q}[X]$. En chassant les dénominateurs de A et B, on obtient $d \in \mathbb{N}$, $\tilde{A}, \tilde{B} \in \mathbb{Z}[X]$ tels que

$$dP = \tilde{A}\tilde{B}. \tag{7.2}$$

En prenant le contenu, sachant que $c(P) = 1$, on obtient $d = c(\tilde{A})c(\tilde{B})$. Mais alors, en divisant l'équation (7.2) par d, on obtient

$$P = \frac{\tilde{A}}{c(\tilde{A})}\frac{\tilde{B}}{c(\tilde{A})}. \tag{7.3}$$

Cette équation vit dans $\mathbb{Z}[X]$. Donc l'irréductibilité de P dans $\mathbb{Z}[X]$ montre que $\deg(A)$ ou $\deg(B)$ est nul. CQFD. □

Ce corollaire est très puissant pour montrer qu'un polynôme de $\mathbb{Q}[X]$ est irréductible. Faisons un exemple.

Exemple 14. Soit $P = X^4 + X + 1$. Montrons que P est irréductible dans $\mathbb{Q}[X]$. Comme $P \in \mathbb{Z}[X]$ et $c(P) = 1$, il suffit de monter qu'il est irréductible dans $\mathbb{Z}[X]$. Ecrivons donc $P = AB$ avec A et B dans $\mathbb{Z}[X]$. Il s'agit de montrer que A ou B est constant. Quitte à permuter A et B, on peut supposer que $\deg(A) \leqslant \deg(B)$. Comme $\deg(A) + \deg(B) = \deg(P) = 4$, il y deux cas à considérer :

(i) $\deg(A) = 1$ et $\deg(B) = 3$.

Alors $A = aX + b$ avec $a, b \in \mathbb{Z}$. En regardant le coefficient dominant de AB, on déduit que a est inversible dans $\mathbb{Z}$. Donc $a = \pm 1$. On peut supposer que $a = -1$. Mais alors $b \in \mathbb{Z}$ est une racine de P. Avec des inégalité, on se convainc que cela est impossible.

(ii) $\deg(A) = 2$ et $\deg(B) = 2$.

Alors on a
$$X^4 + X + 1 = (aX^2 + bX + c)(a'X^2 + b'X + c')$$
dans $\mathbb{Z}$. En particulier $aa' = 1$. Donc on a $a = a' = \pm 1$. On peut supposer (quitte à multiplier les deux facteurs par -1) que $a = a' = 1$.
De plus, $cc' = 1$. Donc $c' = c = \pm 1$. Or
$$(X^2 + bX + c)(X^2 + b'X + c) = X^4 + (b' + b)X^3 + (2c + bb')X^2 + c(b + b')X + 1.$$
On obtient donc $b' = -b$ en regardant le coefficient en X^3. Donc le coefficient en X est nul. Contradiction.

Réduction modulo p. Nous venons de voir que la question de l'irréductibilité d'un polynôme de $\mathbb{Q}[X]$ se ramène à la même question dans $\mathbb{Z}[X]$. L'exemple précédent montre que cela est parfois un progrés. En revanche, nous perdons le fait l'anneau des coefficients est un corps. D'où la construction suivante.
Soit p un nombre premier. On note $a \longmapsto \bar{a}$, $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ la réduction modulo p. C'est un morphisme d'anneaux, appelé *réduction modulo p*. Celle-ci s'étend en un morphisme d'anneaux
$$\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})[X] \\ P = \sum_i a_i X^i & \longmapsto & \bar{P} = \sum_i \bar{a}_i X^i. \end{array}$$
Comme c'est un morphisme d'anneaux, une écriture $P = AB$ dans $\mathbb{Z}[X]$ induit une telle relation $\bar{P} = \bar{A}\bar{B}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Si de plus, le coefficient dominant de P n'est pas divisible par p, les degrés de P, A et B sont préservés. Cela peut permettre de démontrer des irréductibilités dans $\mathbb{Z}[X]$ comme sur l'exemple suivant ou encore dans la démonstration du théorème de Gauss ci-dessus.

Exemple 15. TODO

Un exemple d'illustration de ce principe est la proposition suivante.

Proposition I.45: Critère d'Eisenstein

Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{Z}[X]$ de degré n. Soit p un nombre premier. On suppose que

(i) p divise $a_0, \ldots, a_{n-1}$;

(ii) p ne divise pas a_n ;

(iii) p^2 ne divise pas a_0.

Alors $P \in \mathbb{Q}[X]$ est irréductible.

Preuve

Quitte à factoriser par le pgcd des coefficients, on peut supposer que les coefficients de P sont globalement premiers entre eux. Cela n'affecte pas les hypothèses. En vertu du théorème de Gauss, il s'agit alors de montrer que P est irréductible dans $\mathbb{Z}[X]$. Supposons par l'absurde, que $P = AB$ dans $\mathbb{Z}[X]$ avec A et B non inversibles. Vu la nouvelle hypothèse sur les coefficients, les degrés de A et B sont non nuls.
Considérons le morphisme $\theta : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]$. On a $\theta(P) = \theta(A)\theta(B)$.

Exemple 16. Justifier que le polynôme $3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$.

Polynômes cyclotomiques.
Les polynômes cyclotomiques sont les facteurs irréductibles des $X^n - 1$ dans $\mathbb{Q}[X]$. Dans un premier temps, on pose, pour tout $n \in \mathbb{N}^*$
$$\Phi_n = \prod_{\zeta \in \mathbb{U}_n \text{ primitif}} X - \zeta.$$

Comme chaque $\zeta \in \mathbb{U}_n$ est primitif dans un unique $\mathbb{U}_d$ pour d divisant n (d est l'ordre de ζ dans $\mathbb{U}_n$), on a :

$$X^n - 1 = \prod_{d \text{ divisant n}} \Phi_d.$$

En particulier, Φ_n est le quotient de $X^n - 1$ par

$$\prod_{\substack{d \text{ divisant n} \\ d \neq n}} \Phi_d.$$

Une récurrence montre alors que Φ_n est unitaire et appartient à $\mathbb{Z}[X]$.

Théorème I.46. Irréductibilité des polynômes cyclotomique

Pour tout $n \geqslant 1$, le polynôme Φ_n est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

La preuve de ce théorème sera faite plus tard, lorsque nous aurons étudié les corps finis.

8 Théorème Chinois et Applications

TODO

Chapitre 2

Corps

Sommaire

1 Corps, Sous-corps, Extension 24
1.1 Définition et exemples 24
1.2 Caractéristique d'un corps 24
1.3 Double extension 25
2 Corps des Fractions 25
3 Elément algébrique – Corps de décomposition 26
3.1 Polynôme minimal 26
3.2 Corps de décomposition 27
4 Corps finis 27
4.1 Premières propriétés et exemple 27
4.2 Préliminaires 28
4.3 Factorisation d'un polynôme dans $\mathbb{F}_p[X]$ 29
4.4 Existence 30
4.5 Unicité 31
4.6 Application : Irréducbilité des polynômes cyclotomiques sur $\mathbb{Q}$ 31
5 Corps des nombres constructibles à la règle et au compas 32

1 Corps, Sous-corps, Extension

1.1 Définition et exemples

Définition II.47: Corps

Un corps $(\mathbb{K}, +, \times)$ est un anneau tel que tout élément non nul est inversible pour $\times$.

Les premiers exemples sont les corps que vous manipulez depuis longtemps : $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Q}$. Autre exemple $\mathbb{Q}(i) = \mathbb{Q} + \mathbb{Q}i$.

L'anneau $\mathbb{Z}$ n'est pas un corps car 2 n'est ni nul ni inversible.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. En effet, d'après le théorème de Bezout, $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si k est premier avec n.

L'ensemble des fractions rationelles $\mathbb{K}(X)$ est un corps.

On montre facilement que $\mathbb{K}^* = \mathbb{K} - \{0\}$ est un groupe abélien. En particulier l'inverse de$x \in \mathbb{K}^*$ pour $\times$ est unique : on le note x^{-1} ou $\frac{1}{x}$.
Comme nous l'avons déjà vu des corps peuvent être inclus les uns dans les autres.

Définition II.48: Sous-Corps

Soit $(\mathbb{L}, +, \times)$ un corps. Une partie $\mathbb{K} \subset \mathbb{L}$ est un sous-corps si c'est un sous-anneau tel que

$$\forall x \in \mathbb{K} \qquad x^{-1} \in \mathbb{K}.$$

On dit aussi que $\mathbb{L}$ est une extension de $\mathbb{K}$.

Une remarque très importante est que si $\mathbb{K} \subset \mathbb{L}$ est une extension de corps alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel. La dimension de cet espace vectoriel est appelée *le degré de l'extension*. On la note $[\mathbb{L} : \mathbb{K}]$.
Par exemple $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ et $[\mathbb{C} : \mathbb{Q}] = \infty$.

1.2 Caractéristique d'un corps

Soit A un anneau. Soit n un entier naturel. On peut bien sûr le penser comme $1 + 1 + \cdots + 1$ n fois. Mais alors il prend un sens dans A. De plus, si n est négatif, $n = -(-n)$. On obtient ainsi un morphisme d'anneaux

$$\iota : \mathbb{Z} \longrightarrow A.$$

Autrement dit, $\iota(1) = 1$, $\iota(2) = 1 + 1 + 1$, $\iota(3) = 1 + 1 + 1$ etc. Et $\iota(-1) = -\iota(1)$, $\iota(-2) = -\iota(2)$, $\iota(-3) = -\iota(3)$ etc. Le noyau de ι est un idéal de A. Il s'écrit donc (n) pour un entier naturel n. L'entier n est appelé la caractéristique de A. On la note $\mathrm{car}(A)$.

Lemme II.49. *La caractéristique d'un corps est nulle ou un nombre premier p.*

Démonstration. Comme $\mathbb{Z}/n\mathbb{Z}$ s'injecte dans le corps il est intègre. Mais alors n est nul ou premier. □

Soit $\mathbb{K}$ un corps. En fait, si $\mathrm{car}(\mathbb{K}) = 0$ alors $\mathbb{K}$ contient $\mathbb{Q}$. Si $\mathrm{car}(\mathbb{K}) = p$ alors $\mathbb{K}$ contient $\mathbb{Z}/p\mathbb{Z}$.

Lemme II.50. *Le cardinal d'un corps fini est une puissance d'un nombre premier.*

Démonstration. Le morphisme ι ne peut être injectif car $\mathbb{Z}$ est infini. Il suit que le corps contient $\mathbb{Z}/p\mathbb{Z}$ avec p-premier. En particulier il est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ comme espace vectoriel (pour un certain n). Donc son cardinal est p^n. □

Nous verrons dans ce chapitre que réciproquement pour tout n, il existe un unique (à iso près) corps à p^n éléments.

1.3 Double extension

Soit $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{L}$. Combien voyez-vous d'extension ? Deux ? Et non, c'est trois.

Théorème II.51. Base télescopique

Soit $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{L}$. On suppose que $\mathbb{K}_1 \subset \mathbb{L}$ est une extension finie. Alors

$$[\mathbb{L} : \mathbb{K}_1] = [\mathbb{L} : \mathbb{K}_2] \cdot [\mathbb{K}_2 : \mathbb{K}_1].$$

Démonstration. La démonstration de ce théorème explique son nom. Soit $(e_1, \ldots, e_d)$ une base de $\mathbb{K}_2$ comme $\mathbb{K}_1$-espace vectoriel. Soit $(f_1, \ldots, f_{d'})$ une base de $\mathbb{L}$ comme $\mathbb{K}_2$-espace vectoriel.
Chaque élément y de $\mathbb{L}$ s'écrit

$$y = \sum_i x_i f_i$$

pour $x_i \in \mathbb{K}_2$. Or chaque x_i s'écrit

$$x_i = \sum_j m_{ij} e_j,$$

pour $m_{ij} \in \mathbb{K}_1$. Mais alors,

$$y = \sum_{i,j} m_{ij}(e_j f_i)$$

. Donc la famille $(e_i f_j)$ engendre $\mathbb{L}$ comme $\mathbb{K}_1$-espace vectoriel.

Supposons maintenant que

$$\sum_{i,j} m_{ij}(e_j f_i) = 0,$$

avec $m_{ij} \in \mathbb{K}_1$. Alors

$$\sum_i (\sum_j m_{ij} e_j) f_i = 0.$$

Comme $(f_1, \ldots, f_{d'})$ est libre sur $\mathbb{K}_2$, on en déduit que

$$\forall i \qquad \sum_j m_{ij} e_j = 0.$$

Comme $(e_1, \ldots, e_d)$ est libre sur $\mathbb{K}_1$, on en déduit que

$$\forall i, j \qquad m_{ij} = 0.$$

Ainsi la famille $(e_i f_j)$ est libre.

Finalement la famille $(e_i f_j)$ est une base de $\mathbb{L}$ comme $\mathbb{K}_1$-espace vectoriel. La formule du théorème en découle facilement. □

2 Corps des Fractions

Une première façon de construire des corps est de faire ce que l'on a fait pour construire $\mathbb{Q}$. Nous partions de $\mathbb{Z}$ et considérions les fractions $\frac{a}{b}$ comme un objet formel. En fait cela marche dès que l'anneau de départ est intègre. Mais au fait, vous aviez déjà vu un autre exemple : le corps des fractions rationnelles.

Soit A un anneau intègre. On considère l'ensemble quotient suivant

$$\mathrm{Frac}(A) := \{\frac{a}{b} \ : \ a \in A, b \in A - \{0\}\} / \sim$$

où la relation d'équivalence $\sim$ est définie par

$$\frac{a}{b} \sim \frac{c}{d} \quad \Leftrightarrow \quad ad - bc = 0.$$

On définit ensuite sur A les deux opérations :

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{db} \qquad \text{et} \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{db}.$$

On vérifie que ces opérations sont bien définies (c'est-à-dire passent au quotient par $\sim$) et dont de $\mathrm{Frac}(A)$ un corps. C'est un peu long mais sans difficulté.

L'anneau de départ A s'injecte dans K par l'application

$$\iota : A \longrightarrow \mathrm{Frac}(A),\ a \longmapsto \frac{a}{1}.$$

Le corps $\mathrm{Frac}(A)$ vérifie la propriété universelle suivante. Tout morphisme d'anneau injectif de A dans un corps se prolonge de manière unique à $\mathrm{Frac}(A)$. C'est une manière de dire que $\mathrm{Frac}(A)$ est le plus petit corps contenant A.

3 Elément algébrique – Corps de décomposition

3.1 Polynôme minimal

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Pensez ici à $\mathbb{Q} \subset \mathbb{C}$. Soit $\alpha \in \mathbb{L}$ et

$$\begin{array}{rccc} \varphi_\alpha : & \mathbb{K}[X] & \longrightarrow & \mathbb{L} \\ & P & \longmapsto & P(\alpha). \end{array}$$

Définition II.52: Algébrique/Transcendant

Un élément $\alpha \in \mathbb{L}$ est dit *algébrique sur* $\mathbb{K}$ s'il existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$. Sinon il est dit *transcendant*.

Dit autrement, α est transcendant si φ est injectif et algébrique sinon. Dans ce dernier cas, le générateur unitaire de $\mathrm{Ker}\varphi$ est appelé le *polynôme minimal de* α. On le note μ_α.

Proposition II.53: Corps engendré

Soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Alors le polynôme minimal de α est irréductible. De plus, l'image de φ_α est un corps, noté $\mathbb{K}[\alpha]$ et isomorphe à $\mathbb{K}[X]/(\mu_\alpha)$.

Démonstration. L'anneau quotient $\mathbb{K}[X]/(\mu_\alpha)$ s'injecte dans $\mathbb{L}$, donc il est intègre. Ce qui implique que μ_α est irréductible.
Mais alors, (μ_α) est un idéal maximal donc $\mathbb{K}[X]/(\mu_\alpha)$ est un corps. □

Par exemple, $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal est $X^2 - 2$.

Théorème II.54. Corps des nombres algébriques

L'ensemble des nombres de $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ et une extension de $\mathbb{K}$.

Démonstration. La remarque essentielle de cette démonstration est la suivante : φ_α n'est pas injective si et seulement si son image est de dimension finie si et seulement si α est algébrique.
Soit maintenant α et β dans $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$. On a déjà vu que $\alpha^{-1} \in \mathbb{K}[\alpha]$.
Considérons $\mathbb{K}[\alpha, \beta] := (\mathbb{K}[\alpha])[\beta]$. Comme β est algébrique sur $\mathbb{K}$ il l'est sur $\mathbb{K}[\alpha]$. Donc la dimension de $\mathbb{K}[\alpha, \beta]$ sur $\mathbb{K}[\alpha]$ est finie et $\mathbb{K}[\alpha, \beta]$ est un corps. D'après le théorème de la base télescopique, la dimension de $\mathbb{K}[\alpha, \beta]$ sur $\mathbb{K}$ est finie.
Or $\alpha + \beta$ appartient à $\mathbb{K}[\alpha, \beta]$ qui est un corps. Donc l'image de $\varphi_{\alpha+\beta}$ est incluse dans $\mathbb{K}[\alpha, \beta]$ et donc de dimension finie. Donc $\alpha + \beta$ est algébrique sur $\mathbb{K}$. On montre de même $\alpha\beta$ est algébrique sur $\mathbb{K}$. □

Le théorème précédent implique par exemple que le nombre complexe

$$\frac{\sqrt{5} + i}{\sqrt[3]{2} + i\sqrt[5]{3}}$$

est algébrique sur $\mathbb{Q}$. Il n'est pas facile du tout d'en trouver le polynôme minimal. On peut tout de même en mimant la preuve trouver une borne supérieure sur son degré.

3.2 Corps de décomposition

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. L'anneau quotient $\mathbb{K}[X]/(P)$ est un corps car l'idéal (P) est maximal. Notons $\bar{X}$ la classe de X dans $\mathbb{K}[X]/(P)$. Alors, par définition $P(\bar{X}) = 0$, si bien que $\mathbb{K}[X]/(P)$ est un corps, une extension de $\mathbb{K}$ et contenant une racine P. De plus, $\mathbb{K}[X]/(P)$ est engendré par $\bar{X}$ et $\mathbb{K}$ comme anneau et

$$[\mathbb{K}[X]/(P) : \mathbb{K}] = \deg(P).$$

Le corps $\mathbb{K}[X]/(P)$ est appelé *corps de rupture de* P. C'est l'unique (à isomorphisme près) extension de $\mathbb{K}$ contenant une racine de P et engendré par celle-ci.
Nous admettrons le résultat suivant.

Théorème II.55. Corps de décomposition

Soit P un polynôme non nul de $\mathbb{K}[X]$. Alors il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P est scindé sur $\mathbb{L}$ et $\mathbb{L}$ est engendré par les racines de P et $\mathbb{K}$ comme anneau.
De plus, $\mathbb{L}$ est l'unique extension de $\mathbb{K}$ vérifiant ces propriétés. $\mathbb{L}$ est appelé le *corps de décomposition de* P.

4 Corps finis

Le but de cette section est de classifier tous les corps finis. L'énoncé est le suivant :

Théorème II.56. Corps finis

(i) Soit K un corps fini. Alors il existe un nombre premier p et un entier naturel non nul n tel que $\sharp K = p^n$.

(ii) Réciproquement, soit p un nombre premier et n un entier naturel non nul. Alors, il existe un corps à p^n éléments.

(iii) De plus, deux corps finis de même cardinal sont isomorphes.

On note $\mathbb{F}_q$ l'unique corps à $q = p^n$ éléments.

4.1 Premières propriétés et exemple

Soit K un corps fini. Sa caractéristique est non nulle (car il ne peut contenir $\mathbb{Z}$), notons là p. Alors K contient $\mathbb{Z}/p\mathbb{Z}$. Posons $n = [K : \mathbb{Z}/p\mathbb{Z}]$ la dimension de K comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Alors $\sharp K = p^n$. La première assertion du théorème II.56 est démontrée.

Si $n = 1$, à la fois l'existence et l'unicité du théorème II.56 sont claires. On pose donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pensé comme un corps. Regardons le plus petit cas qui suit $p = 2$ et $n = 2$. Soit K un corps de cardinal 4. On note 0 et 1 les éléments de $\mathbb{Z}/2\mathbb{Z}$ qui est inclus dans K. Soit x dans $\mathbb{K} - \{0, 1\}$.
On peut voit que $1 + x \neq 1$ (car $x \neq 0$), $1 + x \neq 0$ (car $x \neq 1$), $1 + x \neq x$ (car $1 \neq 0$). Donc $\mathbb{K} = \{0, 1, x, 1 + x\}$. On peut dresser la table d'addition de $\mathbb{K}$:

	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

On s'intéresse à présent à x^2. On voit que $x^2 \neq 0$ (car $x \neq 0$), $x^2 \neq 1$ (car $x^2 - 1 = (x - 1)^2$), $x^2 \neq x$ (car $x^2 - x = x(x - 1)$). Donc $x^2 = 1 + x$. On peut dresser la table de multiplication de $\mathbb{K}$:

	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

4.2 Préliminaires

Avant de se lancer dans la preuve du théorème II.56, on va montrer un lemme dans $\mathbb{C}[X]$, $\mathbb{Z}[X]$ et $\mathbb{Z}$.

Lemme II.57 (**Des divisibilités**). *Soit m et n deux entiers naturels non nuls.*

(i) Dans $\mathbb{C}[X]$, $X^n - 1$ divise $X^m - 1$ si et seulement si n divise m.

(ii) De plus, $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$ si et seulement si il le divise dans $\mathbb{Z}[X]$.

(iii) Soit $a \geqslant 2$ un entier naturel. Alors $a^n - 1$ divise $a^m - 1$ si et seulement si n divise m.

Démonstration. Dans $\mathbb{C}$, on écrit

$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} X - \zeta,$$

où $\mathbb{U}_n$ désigne l'ensemble des racines n-ième de l'unité (les $e^{\frac{2ik\pi}{n}}$). Alors $X^n - 1$ divise $X^m - 1$ si et seulement si $\mathbb{U}_n$ est inclus dans $\mathbb{U}_m$ si et seulement si n divise m.

Il est clair que si $X^n - 1$ divise $X^m - 1$ dans $\mathbb{Z}[X]$ alors il le divise dans $\mathbb{C}[X]$. Réciproquement, supposons que $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$. Effectuons la division euclidienne de $X^n - 1$ par $X^m - 1$ dans $\mathbb{Q}[X]$. Comme $X^m - 1$ est unitaire, on ne divise jamais et le quotient Q et le reste R sont à coefficients entiers. Donc

$$X^n - 1 = (X^m - 1)Q + R \qquad Q, R \in \mathbb{Z}[X].$$

Effectuons la division euclidienne de $X^n - 1$ par $X^m - 1$ dans $\mathbb{C}[X]$. On fait les même calculs que lorsque nous pensions les coefficients des polynômes dans $\mathbb{Q}$. Donc les quotients et restes sont les mêmes. Mais alors comme $X^n - 1$ divise $X^m - 1$ dans $\mathbb{C}[X]$, $R = 0$. cdfd.

Si n divise m, alors $X^n - 1$ divise $X^m - 1$ dans $\mathbb{Z}[X]$. Donc en substituant a à X, $a^n - 1$ divise $a^m - 1$. Réciproquement supposons que $a^n - 1$ divise $a^m - 1$. On écrit $m = nq + r$ avec $0 \leqslant r < n$. Comme

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + 1),$$

l'entier $(a^{n-1}+a^{n-2}+\cdots+1)$ divise

$$\begin{aligned}1+\cdots+a^{m-2}+a^{m-1} = \quad & (1+\cdots+a^{n-1})\\ & +(1+\cdots+a^{n-1})a^{n}\\ & +(1+\cdots+a^{n-1})a^{2n}\\ & \vdots\\ & +(1+\cdots+a^{n-1})a^{(q-1)n}\\ & +(1+\cdots+a^{r-1})a^{qn}.\end{aligned}$$

L'entier $N := (a^{n-1}+a^{n-2}+\cdots+1)$ est de la forme $1+ab$ (un plus un multiple de a. Il est donc premier avec a (par Bezout si vous voulez). Par ailleurs, il divise la somme ci-dessus ainsi que tous ses premiers termes. Donc N divise le dernier terme de la somme, c'est-à-dire $(1+\cdots+a^{r-1})a^{qn}$. Mais alors, le lemme de Gauss implique que N divise $(1+\cdots+a^{r-1})$. Le seul moyen (inégalités) est d'avoir $r=0$. Donc n divise m. □

4.3 Factorisation d'un polynôme dans $\mathbb{F}_p[X]$

Soit d un entier naturel non nul. On note $\mathcal{I}(d,p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ unitaires irréductibles et de degré d.

Lemme II.58. *Si $\mathcal{I}(d,p)$ est non vide, alors il existe un corps à p^d éléments.*

Démonstration. En effet, $\mathbb{F}_p[X]/(P)$ convient pour $P\in\mathcal{I}(d,p)$. □

On veut donc montrer que $\mathcal{I}(d,p)$ est non vide.

Proposition II.59: Factorisation de $X^{p^n}-X$

Soit n un entier non nul. Dans $\mathbb{F}_p[X]$, on a

$$X^{p^n}-X=\prod_{d\,|\,n}\prod_{P\in\mathcal{I}(d,p)}P.$$

Démonstration. L'équation de la proposition est la décomposition de $X^{p^n}-X$ en produit de polynômes irréductibles. Il suffit donc de montrer les deux assertions suivantes, pour tout polynôme irréductible unitaire P de $\mathbb{F}_p[X]$:

(i) P^2 ne divise pas $X^{p^n}-X$;

(ii) P divise $X^{p^n}-X$ si et seulement si $\deg(P)$ divise n.

Pour la première assertion, supposons par l'absurde que $X^{p^n}-X=P^2Q$. Alors en dérivant on obtient

$$-1=P(2P'Q+PQ').$$

Donc P divise -1. Contradiction.

Supposons maintenant que $d=\deg(P)$ divise n. Soit $\mathbb{L}=\mathbb{F}_p[X]/(P)$ et $\alpha\in\mathbb{L}$ la classe de X. Alors $P(\alpha)=0$.
Si $\alpha=0$, $P=X$ et il n'y a rien à montré. Supposons donc $\alpha\neq 0$. Alors α est un élément du groupe multiplicatif $\mathbb{L}-\{0\}$ de cardinal p^d-1. Le théorème de Lagrange montre donc que $\alpha^{p^d-1}=1$. D'après le lemme II.57, on a aussi $\alpha^{p^n-1}=1$ (car p^d-1 divise p^n-1). Mais alors α est racine de $X^{p^n}-X$.
Comme P et $X^{p^n}-X$ ont une racine commune dans $\mathbb{L}$ leur pgcd n'est pas 1. Or, grâce à l'algorithme d'Euclide, le pgcd ne dépend pas du corps contenant les coefficients des polynômes. Donc, dans $\mathbb{F}_p[X]$, le pgcd de P et $X^{p^n}-X$ n'est pas 1. Mais alors, comme P est irréductible, P divise $X^{p^n}-X$.

Supposons enfin que P irréductible divise $X^{p^n}-X$. Notons encore $d=\deg(P)$, $\mathbb{L}=\mathbb{F}_p[X]/(P)$ et $\alpha\in\mathbb{L}$ la classe de X. On peut encore supposer $\alpha\neq 0$. On fait la division euclidienne : $n=ds+r$ avec $0\leqslant r<d$.

Comme P divise $X^{p^n} - X$, $\alpha^{p^n-1} = 1$ et $\alpha^{p^n} = \alpha$. Donc

$$\alpha^{p^n} = (\alpha^{p^{ds}})^{p^r} = \alpha^{p^r} = \alpha.$$

On en déduit que si β est une puissance de α alors

$$\beta^{p^r} = \beta.$$

Si par l'absurde $r \neq 0$, on a

$$(x+y)^{p^r} = x^{p^r} + y^{p^r} \qquad \forall x, y \in \mathbb{L}$$

et

$$x^{p^r} = x \qquad \forall x \in \mathbb{F}_p.$$

On en déduit que

$$x^{p^r} = x \qquad \forall x \in \mathbb{L}. \tag{4.1}$$

En particulier le polynôme $X^{p^r} - X$ de degré p^r a au moins $\sharp\mathbb{L} = p^d$ racines. Contradiction. □

Exemple 17. Dans $\mathbb{F}_2[X]$, on obtient

$$X^8 - X = X(X-1)(X^3+X+1)(X^3+X^2+1).$$

Dans $\mathbb{F}_3[X]$, on obtient

$$X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^1-X-1).$$

4.4 Existence

L'égalité des degrés dans la proposition II.59 donne

$$p^n = \sum_{d\,|\,n} \sharp\mathcal{I}(d,p)d. \tag{4.2}$$

Théorème II.60. Existence polynôme irréductible

Dans $\mathbb{F}_p[X]$ il existe des polynômes irréductibles de tout degré. En particulier, pour tout n il existe un corps à p^n éléments.

Démonstration. Il s'agit de montrer que $\mathcal{I}(d,p)$ est non vide. Or, d'après (4.2), on a

$$p^n = \sharp\mathcal{I}(n,p)n + \sum_{d\,|\,n \quad d<n} \sharp\mathcal{I}(d,p)d$$

et

$$\sharp\mathcal{I}(n,p)n \leqslant p^n.$$

Mais alors

$$p^n \leqslant \sharp\mathcal{I}(n,p)n + \sum_{d\,|\,n \quad d<n} p^d \leqslant \sharp\mathcal{I}(n,p)n + \sum_{k=0}^{n-1} p^k \leqslant \sharp\mathcal{I}(n,p)n + \frac{p^n-1}{p-1} < \sharp\mathcal{I}(n,p)n + p^n.$$

Donc $\sharp\mathcal{I}(n,p)$ est non nul.

Le lemme du début et l'existence de polynômes irréductibles impliquent l'existence de corps. □

4.5 Unicité

On peut montrer que

$$\sharp\mathcal{I}(50,2) = 22\,517\,997\,465\,744.$$

Cela fait de nombreuses manières de construire $\mathbb{F}_{2^{50}}$. Mais l'on obtient toujours la même chose!!

Démonstration. Soit $\mathbb{L}$ un corps à p^n éléments et P un polynômes irréductible unitaire de degré n dans $\mathbb{F}_p[X]$. Posons $\mathbb{K} = \mathbb{F}_p[X]/(P)$.
Tous les éléments non nuls de $\mathbb{L}$ vérifient, $\alpha^{p^n-1} = 1$, en vertu du théorème de Lagrange appliqué dans le groupe multiplicatif $\mathbb{L} - \{0\}$. Mais alors, pour tout $\alpha \in \mathbb{L}$ on a $\alpha^{p^n} = \alpha$. On en déduit que

$$X^{p^n} - X = \prod_{\alpha\in\mathbb{L}} (X - \alpha).$$

Dans $\mathbb{F}_p[X]$, on sait que P divise $X^{p^n} - X$. Donc il existe $\alpha_0 \in \mathbb{L}$ tel que $P(\alpha_0) = 0$. Comme P est irréductible sur $\mathbb{F}_p$, P est le polynôme minimal de α_0 sur $\mathbb{F}_p$. Ainsi, le morphisme

$$\mathbb{F}_p[X] \longrightarrow \mathbb{L},\ Q \longmapsto Q(\alpha_0)$$

induit un morphisme injectif

$$\mathbb{F}_p[X]/(P) \longrightarrow \mathbb{L}.$$

Par égalité des cardinaux ce morphisme injectif est en fait un isomorphisme. □

4.6 Application : Irréducbilité des polynômes cyclotomiques sur $\mathbb{Q}$

Dans ce paragraphe, on démontre le théorème I.46. Rappelons que Φ_n est le polynôme unitaire dont les racines sont les racines n-ièmes primitive de l'unité. On a déjà vu que c'est un polynôme à coefficients entiers, de degré $\phi(d)$.

Affirmation 1 : Tout diviseur de $X^n - 1$ dans $\mathbb{Q}[X]$ est à coefficients entiers et de contenu 1.

On écrit dans $\mathbb{Q}[X]$, $X^n - 1 = PQ$. Soit p et q les ppcm les dénominateurs (mis sous forme irréductibles) des coefficients de P et Q respectivment. On réécrit la relation dans $\mathbb{Z}[X]$:

$$pq(X^n - 1) = (pP)(qQ).$$

On prend le contenu

$$c(pq(X^n - 1)) = pq = c(pP)c(qQ) = 1.$$

Donc $p = q = 1$ et P et Q sont dans $\mathbb{Z}[X]$.

Soit ζ une racine primitive n-ièmes de l'unité et P_ζ son polynôme minimal dans $\mathbb{Q}[X]$. Comme P_ζ et Φ_n ont une racine en commun, ils ne sont pas premiers entre eux. Comme P_ζ est irréductible, il divise Φ_n.
Par l'affirmation 1, $P_\zeta \in \mathbb{Z}[X]$. On écrit $X^n - 1 = P_\zeta H$ avec $H \in \mathbb{Z}[X]$ (comme P_ζ est unitaire).
Soit p un nombre premier qui ne divise pas n et ξ une racine de P_ζ.

Affirmation 2 : $P_\zeta(\xi^p) = 0$.

Supposons par l'absurde que $P_\zeta(\xi^p) \neq 0$. Comme ξ^p est une racine n-ième de l'unité, $H(\xi^p) = 0$.
Par ailleurs, P_ζ est irréductible et s'annule en ξ : c'est le polynôme minimal de ξ.
Donc P_ζ divise le polynôme $H(X^p)$: $H(X^p) = P_\zeta Q$ dans $\mathbb{Z}[X]$ (comme ci-dessus).
On réduit maintenant cette égalité dans $\mathbb{F}_p[X]$:

$$\overline{H(X^p)} = (\overline{H(X)})^p = \bar{P}_\zeta \bar{Q}.$$

Soit θ un facteur irréductible de $\bar{P}_\zeta$. Alors, θ divise $\bar{H}^p$, donc il divise $\bar{H}$. Donc θ divise $\bar{P}_\zeta$ et $\bar{H}$. Donc θ^2 divise $X^n - 1$ dans $\mathbb{F}_p[X]$
Ceci est une contradiction car $X^n - 1$ est premier avec son dérivé dans $\mathbb{F}_p[X]$.

Par une récurrence immédiate, l'affirmation 2 implique que $P(\zeta^k) = 0$, pour tout $k \in \mathbb{N}$ premier avec n. Mais alors, toutes les racines primitives de n sont racines de P_ζ. Mais alors $P_\zeta = \Phi_n$ qui est irréductible.

5 Corps des nombres constructibles à la règle et au compas

Dans cette dernière section nous allons voir deux sous-corps de $\mathbb{R}$ et $\mathbb{C}$ inspirés par les mathématiques de la Grece antique. On va développer des outils permettant d'étudier des problèmes comme celui de la trisection de l'angle, la quadrature du cercle ou la construction des polyèdres réguliers.
Nous identifions le corps $\mathbb{C}$ au plan euclidien $\mathbb{R}^2$. Pour $z_1 \neq z_2$ dans $\mathbb{C}$, on note $(z_1 z_2)$ la droite passant par z_1 et z_2, et $\mathscr{C}(z_1, z_2)$ le cercle de centre z_1 et passant par z_2.
Soit S une partie de $\mathbb{C}$. On dit qu'un nombre complexe est *élémentairement constructible* à partir de S s'il existe $z_1 \neq z_2 \in S$ et $z_3 \neq z_4 \in S$ tels que l'une des affirmations suivantes est vrai :

(i) les droites $(z_1 z_2)$ et $(z_3 z_4)$ sont distinctes et sécantes en z.

(ii) les cercles $\mathscr{C}(z_1, z_2)$ et $\mathscr{C}(z_3, z_4)$ sont distincts et sécants en z.

(iii) la droite $(z_1 z_2)$ et le cercle $\mathscr{C}(z_3, z_4)$ s'intersectent en z.

On dit qu'un nombre complexe z est *constructible* s'il existe une suite $0, 1, i, z_1, \ldots, z_n = z$ telles que, pour tout $1 \leqslant i \leqslant n$, z_k est élémentairement constructible à partir de $\{0, 1, i, \ldots, z_{k-1}\}$, pour tout $k \in \{1, \ldots, n\}$. On note $\mathscr{K}$ l'ensemble des nombres complexes constructibles. Enfin, un nombre réel x est *constructible* s'il est constructible en tant que nombre complexe.

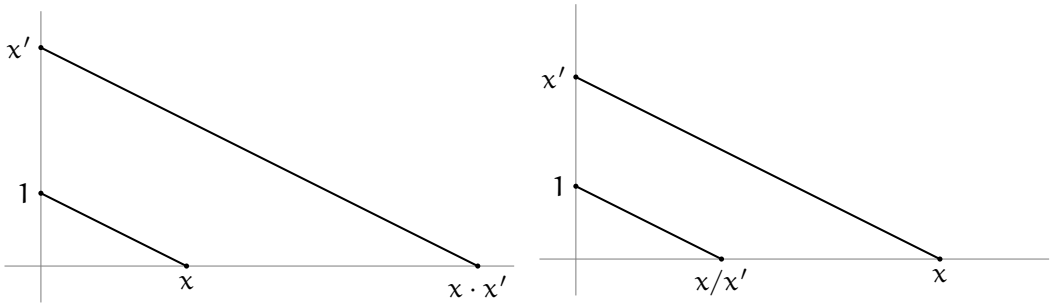
Théorème II.61. Corps des nombres constructibles

On a

(i) Les ensembles $\mathscr{K}$ et $\mathscr{K} \cap \mathbb{R}$ sont des corps.

(ii) Un élément $z \in \mathbb{C}$ appartient à $\mathscr{K}$ si et seulement si ses parties réelle et imaginaire appartiennent à $\mathscr{K} \cap \mathbb{R}$.

Démonstration. La deuxième assertion dit juste que l'on peut construire un point complexes ses coordonnées étant connues. Et que réciproquement, ses coordonnées sont constructibles à partir de z.
Comme on peut construire les paralellogrammes $\mathscr{K}$ est stable par addition. Comme on peut construire les symétries centrales $\mathscr{K}$ est stable par opposé.
On peut aussi construire la paralelle à une droite passant par un point. Mais alors en utilisant le théorème de Thalès on voit facilement que $\mathscr{K} \cap \mathbb{R}$ est stable par produit et inverse. Voir les dessins ci-dessous.



□

La théorie des corps, via le théorème suivant permet de démonter que plusieurs problèmes grecs n'ont pas de solution.

Théorème II.62. Obstruction à la constructibilité

Soit $z \in \mathscr{K}$. Alors z est algébrique sur $\mathbb{Q}$ et le degré $[\mathbb{Q}[z] : \mathbb{Q}]$ de l'extension est une puissance de 2.

Démonstration. Soit $A = x_1 + iy_1$ et $B = x_2 + iy_2$ des nombres complexes. Alors la droite (AB) a une équation de la forme :

$$\alpha x + \beta y + \gamma = 0 \tag{5.1}$$

avec α, β et γ dans $\mathbb{Q}(x_1, x_2, y_1, y_2)$. Et le cercle $\mathscr{C}(AB)$ a une équation de la forme :

$$x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \tag{5.2}$$

avec α, β et γ dans $\mathbb{Q}(x_1, x_2, y_1, y_2)$.
Soit $\mathbb{L}$ un sous-corps de $\mathbb{R}$. Montrons que si $z = x + iy$ est élémentairement constructible à partir $\mathbb{L} + i\mathbb{L}$ alors $[\mathbb{L}(x) : \mathbb{L}]$ et $[\mathbb{L}(y) : \mathbb{L}]$ valent 1 ou 2.
Si z est l'intersection de deux droites passant par des points dont les coordonnées sont dans $\mathbb{L}$, ses coordonnées s'obtiennent en résolvant un système linéaire à coefficient dans $\mathbb{L}$ donc sont dans $\mathbb{L}$. Ainsi $\mathbb{L}(x) = \mathbb{L}(y) = \mathbb{L}$.
Si z est dans l'intersection d'une droite passant par des points dont les coordonnées sont dans $\mathbb{L}$ et d'un cercle construit à partir de tels points, ses coordonnées vérifient

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \alpha', \beta, \beta', \gamma$ et γ' dans $\mathbb{L}$.
Supposons $\beta \neq 0$. Alors y s'exprime en fonction de x et $\mathbb{L} \subset \mathbb{L}(y) \subset \mathbb{L}(x)$. On tire alors y de la première équation et l'injecte dans la seconde. Le nombre x vérifie une équation de degré 2 à coefficients dans $\mathbb{L}$. Donc $[\mathbb{L}(x) : \mathbb{L}] = 1$ ou 2.
Supposons $\beta = 0$. Alors x appartient à $\mathbb{L}$. Mais alors, la deuxième équation montre que y vérifie une équation de degré 2 à coefficients dans $\mathbb{L}$. Donc $[\mathbb{L}(y) : \mathbb{L}] = 1$ ou 2.

Si z est dans l'intersection de deux cercles, ses coordonnées vérifient

$$\begin{cases} x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

avec $\alpha, \alpha', \beta, \beta', \gamma$ et γ' dans $\mathbb{L}$. En remplaçant la première équation par la différence des deux, on se ramène au cas précédent. □

Le problème de duplication du cube est le suivant. Etant donné un cube de volume V peut-on en construire un de volume $2V$. Il s'agit donc de construire $\sqrt[3]{2}$. Si cela était possible le théorème dirait que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ serait une puissance de deux.
Or $\sqrt[3]{2}$ annule $X^3 - 2$. Ce polynôme est de degré 3 et n'a pas de racine dans $\mathbb{Q}$: il est donc irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de $\sqrt[3]{2}$ et $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. Contradiction.

On peut même améliorer le théorème II.62 pour caractériser les éléments constructibles.

Théorème II.63. Wantzel(1837)

Le nombre réel a est constructible à la règle et au compas si et seulement si, il existe une suite de corps $L_0, \ldots, L_s$ tels que

(i) $L_0 = \mathbb{Q}$;
(ii) L_{i+1} est une extension quadratique de L_i, pour tout $0 \leqslant i < s$;
(iii) $a \in L_s$.

Démonstration. TODO : en fait c'est la preuve ci-dessus. □