Anneaux & Corps

Zsolt Patakfalvi

(Basé sur des notes du cours de Jérôme Scherer donné durant l'année académique 2018-2019, ce qui était mise en page par Émir Nairi.)

25 mai 2022

Table des matières

Chapitre 1

Codes couleurs

On utilise les couleurs différentes dans ces notes, ce qui indique la suivante :

Révision

Partie descriptive du texte, où les mathématiques ne sont pas 100% précise. Autrement dit, une partie ce qui ne contient pas les définitions, théorèmes, propositions, lemmes et exemples numérotés.

Matériel optionnel

Partie optionnelle du matériel, pour ceux qui s'intéressent à l'algèbre. Si vous voulez prendre les cours du track "Geometry and algebra" dans l'avenir, alors c'est fortement suggéré de lire cette partie. Cependant, cette partie ne serait pas donc demandée à l'examen.

Chapitre 2

Généralités sur les Anneaux

Révision

2.1 Définitions de base et exemples connus

Nous donnons la définition d'anneau, et énumérons quelques exemples bien connus sur lesquels nous nous appuierons pour construire par la suite de nouveaux exemples. Ces notions sont considérées comme étant acquises avant le début du cours et constituent donc des prérequis.

2.1.1 La notion d'anneau

Nous commençons par la définition d'un anneau.

Définition 2.1.1. Un *anneau* est un triplet $(A, +, \cdot)$ où A est un ensemble, où $+$ et $\cdot$ sont deux lois de composition internes appelées *addition* et *multiplication* telles que :

(1) $(A, +)$ est un groupe abélien ;
(2) $(A, \cdot)$ est un monoïde, ce qui veut dire que :
   (i) la multiplication est associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pour tout $a, b, c \in A$;
   (ii) Il existe un élément $1 = 1_A$ appelé *unité* ou élément neutre pour la multiplication, tel que $1_A \cdot a = a = a \cdot 1_A$ pour tout $a \in A$.
(3) la multiplication est distributive (à gauche et à droite) par rapport à l'addition :
   (i) $a \cdot (b + c) = a \cdot b + a \cdot c$ pour tous $a, b, c \in A$,
   (ii) $(b + c) \cdot a = b \cdot a + c \cdot a$ pour tous $a, b, c \in A$;

Remarque 2.1.2. Tous les anneaux que nous considérerons sont donc *unitaires*.

Exemple 2.1.3. On donne les exemples suivants d'anneaux :

(1) les entiers relatifs $\mathbb{Z}$,
(2) les nombres rationnels $\mathbb{Q}$,
(3) les nombres réels $\mathbb{R}$,
(4) les nombres complexes $\mathbb{C}$, munis de l'addition et de la multiplication usuelles,
(5) pour tout anneau A et tout entier $n \geq 1$, l'ensemble, $M_n(A)$ des matrices carrées de taille $n \times n$ pour la somme et la multiplication matricielles,
(6) et finalement l'anneau nul $\{0\}$ est le seul anneau dans lequel $0 = 1$.

Remarque 2.1.4. Il existe des définitions plus souples, on pourrait par exemple parler d'anneau sans unité (par exemple les fonctions réelles à support compact ou encore $2\mathbb{Z}$), mais nous ne le ferons pas dans ce cours. Une raison simple pour cela est que nous allons souvent considérer des ensembles de multiples d'un élément a donné, $(a) = \{x \cdot a \mid x \in A\}$, de manière analogue à ce que nous faisons dans $\mathbb{Z}$ où (n) désigne l'ensemble des multiples de n. Sans unité dans notre anneau a n'appartiendrait pas à (a)...

Voici une liste de propriétés qui sont vraies dans tout anneau, et dont les preuves figurent dans le cours d'algèbre linéaire de première année.

Lemme 2.1.5. *Soit A un anneau. Pour tout $a, b \in A$ on a :*

(1) L'élément neutre pour $+$ est absorbant *: $0 \cdot a = 0 = a \cdot 0$.*
(2) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$. En particulier $(-1) \cdot a = -a$.
(3) L'unité est unique : Si $e \in A$ est tel que $e \cdot a = a$ pour tout $a \in A$, alors $e = 1$.

Définition 2.1.6. Un anneau est dit *commutatif* si la multiplication est commutative.

Les anneaux de matrices, même lorsque les coefficients vivent dans un anneau commutatif (non nul), ne sont pas des anneaux commutatifs dès que $n \geq 2$ puisque

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

2.1.2 Homomorphismes d'anneaux et sous-anneaux

Comme souvent en mathématiques il n'est pas très utile de définir de nouveaux objets si on ne sait pas comment les comparer entre eux. La notion qui permet de le faire pour les anneaux est celle d'homomorphisme d'anneaux (de la même manière qu'on a de comparer deux groupes en considérant des homomorphismes de groupes, deux espaces vectoriels avec des applications linéaires, des espaces topologiques avec des applications continues, etc.). Sans surprise, un homomorphisme d'anneaux est une application qui est un homomorphisme de groupes (additifs) et qui est également compatible avec la structure multiplicative. Les mathématiciens étant paresseux, la définition impose les conditions minimales qui assurent ces conditions.

Définition 2.1.7. Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux. Un *homomorphisme d'anneaux* $f \colon A \to B$ est une application telle que :

(1) f est un homomorphisme de groupes additifs, ce qui veut dire que pour tout $a, b \in A$: $f(a + b) = f(a) + f(b)$;
(2) f est un homomorphisme des monoïdes multiplicatifs, ce qui veut dire que pour tout $a, b \in A$:
   (i) $f(a \cdot b) = f(a) \cdot f(b)$;
   (ii) $f(1_A) = 1_B$.

Remarque 2.1.8. En utilisant que f est un homomorphisme additif on obtient que $f(0_A) = 0_B$ et que $f(-a) = -f(a)$.

Définition 2.1.9. Un homomorphisme d'anneaux est un *isomorphisme* s'il est bijectif.

Remarque 2.1.10. En réalité, un isomorphisme d'anneaux est un homomorphisme qui admet un inverse. La bijectivité permet de considérer l'application inverse, qui est aussi un homomorphisme d'anneaux.

Si B est un anneau, un sous-ensemble $A \subseteq B$ est un sous-anneau si l'addition et la multiplication de B définissent des lois de composition sur A qui en font un anneau. Autrement dit, l'application d'inclusion $i : A \mapsto B$ est un homomorphisme d'anneaux.

Définition 2.1.11. Soit B un anneau. Un sous-ensemble A de B est un *sous-anneau* de B si

(1) $(A, +)$ est un sous-groupe de $(B, +)$
(2) $(A, \cdot)$ est un sous-monoïde de $(B, \cdot)$, ce qui veut dire que
   (i) l'unité 1_B de B est contenue dans A,
   (ii) A est stable pour la multiplication, avec les formules :

$$a, b \in A \implies a \cdot b \in A$$

Les inclusions $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sont toutes des inclusions de sous-anneaux.

Exemple 2.1.12. Le sous-ensemble C de $M_2(\mathbb{R})$ formé des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ où $a, b \in \mathbb{R}$, est un sous anneau. En effet, il s'agit clairement d'un sous-groupe (pour l'addition), la matrice $I_2 \in C$ définit l'unité, et on vérifie à la main que le produit de deux matrices de C est encore dans C.

L'application $f : \mathbb{C} \to C$ qui envoie le nombre complexe $a + bi$ sur la matrice $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ est un isomorphisme d'anneaux.

On termine avec une proposition basique mais importante :

Proposition 2.1.13. *Si $f : A \to B$ est un homomorphisme d'anneaux, alors l'image $\operatorname{im} f = f(A) \subseteq B$ est un sous-anneau.*

Remarque 2.1.14. Si $f : A \to B$ est un homomorphisme d'anneaux tel que $B \neq 0$, alors $\ker f \subseteq A$ n'est pas un sous-anneau. Effectivement, on a

$$\underset{\boxed{\text{par la Définition 2.1.7}}}{f(1)} = \underset{\uparrow}{1} \neq \underset{\boxed{B \neq 0}}{0}$$

Cela implique que $1_A \notin \ker f$, et donc $\ker f \subseteq A$ n'est pas un sous-anneau par Définition 2.1.11.

On verra cependant dans la Section 2.4 que $\ker f$ admet lui aussi une structure particulière.

2.2 Exemples d'anneaux

2.2.1 Anneaux des polynômes et des séries formelles

Soit A un anneau commutatif. Dans cette sous-section on définit les anneaux suivants :

- $A[\![t]\!]$: l'anneau des séries formelles (d'un variable)
- $A[t]$: l'anneau des polynômes d'un variable
- $A[x_1, \ldots, x_n]$: l'anneau des polynômes des plusieurs variables.

Une *série formelle* sur A est une expression formelle de forme

$$f = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots = \sum_{i=0}^{\infty} a_i t^i$$

où $a_i \in A$, et les a_i sont appelés des *coefficients* de f. On dénote par $A[\![t]\!]$ l'ensemble des séries formelles sur A (deux séries formelles sont différentes si il existe un i tel que l'i-ième coefficients sont différents). On munit $A[\![t]\!]$ d'une structure d'anneau dans la manière suivant : si a_i, b_i, c_i et d_i sont les coefficients de f, g, $f+g$ et $f \cdot g$, alors on met

$$c_i = a_i + b_i, \text{ et } d_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

On laisse en exercice de la vérification que $A[\![t]\!]$ est en effet un anneau.

Un *polynôme* sur A est une série formelle sur A avec un nombre fini de non-zéro coefficients. La convention de la notation est que tous coefficients non-écrit d'un polynôme sont zéros.

Exemple 2.2.1. $f = 1 + t$ et $g = 1 + t + 0 \cdot t^2$ sont les même polynômes. En effet, ils sont juste différentes notations de la même série formelle :

$$1 + 1 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 + 0 \cdot t^4 + \ldots$$

On laisse en exercice de la vérification que les polynômes sur A forme un sous-anneau de $A[\![t]\!]$. On dénote cet anneau par $A[t]$.

Il est important de noter que on ne regarde pas les polynômes et les séries formelles en tant que des fonctionnes. Ils sont simplement des expressions formelles. La raison pour cette distinction est expliqué dans l'exemple suivant :

Exemple 2.2.2. Il existe des anneaux A et polynômes $f, g \in A[t]$ tels que f et g sont distincts en tant que polynômes, mais ils sont les mêmes en tant que des fonctionnes. Par exemple, les choix suivantes donnent tels polynômes : $A = \mathbb{F}_p$, $f = t$ et $g = t^p$.

En effet, $\left|\mathbb{F}_p^\times\right| = p - 1$. En appliquant le théorème de Lagrange à $\left(\mathbb{F}_p^\times, \times\right)$, on obtient que $t^{p-1} - 1$ est satisfait pour chaque élément de $\mathbb{F}_p^\times$. Si on multiple $t^{p-1} - 1$ par t, on obtient $t^p - t$, ce qui est satisfait pour chaque élément de $\mathbb{F}_p$. Autrement dit, les fonctionnes données par f et g sont les mêmes.

On peut, de manière analogue, itérer la construction des anneaux des polynômes. De cette façon, on obtient $A[x_1][x_2]$, $A[x_1][x_2][x_3]$, etc. Notons que ces anneaux se transforment par un isomorphisme canonique si on permute les variables. Par exemple, $A[x_1][x_2] \cong A[x_2][x_1]$ par l'application

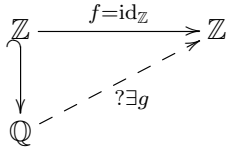
$$\sum_{j=0}^{m} \left(\sum_{i=0}^{m} a_{ji} x_1^i \right) x_1^j \mapsto \sum_{i=0}^{m} \left(\sum_{j=0}^{m} a_{ji} x_2^j \right) x_1^i$$

Par conséquent, on utilise les notations $A[x_1, x_2] = A[x_1][x_2]$, $A[x_1, x_2, x_3] \cong A[x_1][x_2][x_3]$, etc.

2.2.2 Évaluation des polynômes

Les homomorphismes usuels ne s'étendent pas à des sous-anneaux. Par exemple, regardons l'homomorphisme $f = \mathrm{id}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$, et essayons l'étendre à $\mathbb{Q}$. La situation est visualisé dans le

diagramme suivant :



(2.2.a)

En réalité, g n'existe pas. Pour qu'il existe, il faudrait par exemple avoir

$$g\left(\frac{1}{2}\right)2 = g\left(\frac{1}{2}\right)g(2) = g\left(\frac{1}{2}\cdot 2\right) = g(1) = 1$$

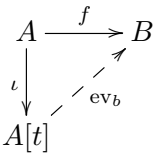
Autrement dit, il faudrait qu'il existe un $x \in \mathbb{Z}$ tel que $2x = 1$, qui, concrètement, n'existe pas.

Cependant, il existe une situation similaire à (2.2.a) où l'on peut étendre f. La proposition suivante présente cette situation :

Proposition 2.2.3. *Soit $f : A \to B$, un homomorphisme d'anneaux commutatifs et fixons $b \in B$. Alors il existe un unique homomorphisme d'anneaux $\mathrm{ev}_b : A[t] \to B$ tel que*

(1) $\mathrm{ev}_b(t) = b$, et

(2) $\mathrm{ev}_b \circ \iota = f$, où ι désigne l'inclusion $\iota\colon A \hookrightarrow A[t]$. En d'autres termes, le diagramme commute :



De plus, ev_b est donné par la formule

$$\mathrm{ev}_b\left(\sum_{j=0}^{m} a_j t^j\right) = \sum_{j=0}^{m} f(a_j) b^j. \tag{2.2.b}$$

Démonstration. Si ev_b existe, il doit satisfaire

$$\mathrm{ev}_b\left(\sum_{j=0}^{m} a_j t^j\right) \underset{\uparrow}{=} \sum_{j=0}^{m} \mathrm{ev}_b(a_j)\,\mathrm{ev}_b(t)^j \underset{\uparrow}{=} \sum_{j=0}^{m} \mathrm{ev}_b(\iota(a_j))\,\mathrm{ev}_b(t)^j \underset{\uparrow}{=} \sum_{j=0}^{m} f(a_j) b^j,$$

ev_b est un homomorphisme ; $\forall a \in A\colon \iota(a) = a$; $\mathrm{ev}_b \circ \iota = f$ et $\mathrm{ev}_b(t) = b$

donc la définition donnée par (2.2.b) est la seule option pour définir ev_b. Il faut juste vérifier que cela nous donne bien un homomorphisme. Premièrement, on vérifie que $\mathrm{ev}_b(1) = 1$:

$$\mathrm{ev}_b(1) \underset{\uparrow}{=} f(1) \underset{\uparrow}{=} 1$$

définition de ev_b ; point (2|(ii)) de la Définition 2.1.7

Deuxièmement, on vérifie que ev_b est additif (on peut supposer que la somme sur les deux éléments termine à m) :

$$\mathrm{ev}_b\left(\sum_{j=0}^{m} a_j t^j\right) + \mathrm{ev}_b\left(\sum_{j=0}^{m} c_j t^j\right) \underset{\uparrow}{=} \sum_{j=0}^{m} f(a_j) b^j + \sum_{j=0}^{m} f(c_j) b^j \underset{\uparrow}{=} \sum_{j=0}^{m} \big(f(a_j) + f(c_j)\big) b^j$$

définition de ev_b ; distributivité, plus précisément point (3) de la Définition 2.1.1

Finalement, on vérifie que ev_b préserve la multiplication :

$$\mathrm{ev}_b\left(\sum_{j=0}^{m} a_j t^j\right)\cdot \mathrm{ev}_b\left(\sum_{j=0}^{m} c_j t^j\right) \underset{\text{définition de } \mathrm{ev}_b}{=} \left(\sum_{j=0}^{m} f(a_j)b^j\right)\cdot\left(\sum_{j=0}^{m} f(c_j)b^j\right) \underset{\substack{\text{distributivité, plus précisément point (3) de la Définition 2.1.1,} \\ \text{et le fait que } a_i = c_i = 0 \text{ pour } i > m}}{=} \sum_{j=0}^{2m}\left(\sum_{i=0}^{j} f(a_i)b^i f(c_{j-i})b^{j-i}\right)$$

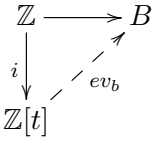
$$\underset{B \text{ est commutatif}}{=} \sum_{j=0}^{2m}\left(\sum_{i=0}^{j} f(a_i)f(c_{j-i})b^j\right) \underset{f \text{ est un homomorphisme}}{=} \sum_{j=0}^{2m}\left(\sum_{i=0}^{j} f(a_i c_{j-i})b^j\right) \underset{\text{par la définition de } \mathrm{ev}_b}{=} \mathrm{ev}_b\left(\sum_{j=0}^{2m}\left(\sum_{i=0}^{j} a_i c_{j-i} t^j\right)\right)$$

$$\underset{\text{par la définition de la multiplication dans } A[t]}{=} \mathrm{ev}_b\left(\left(\sum_{j=0}^{m} a_j t^j\right)\cdot\left(\sum_{j=0}^{m} c_j t^j\right)\right)$$

□

Remarque 2.2.4. On appelle l'application ev_b de la Proposition 2.2.3 l'homomorphisme d'évaluation puisque si $A = A$ et $f = \mathrm{id}_A$, $\mathrm{ev}_b(p(t))$ est dans ce cas simplement la valeur $p(b)$ du polynôme $p(t)$ en $b \in A$.

Exemple 2.2.5. Le cas de $\mathbb{Z}$ est particulier. Soit B un anneau commutatif. Les propriétés du morphisme impliquent (par une petite récurrence), qu'il existe un unique homomorphisme d'anneaux $f : \mathbb{Z} \hookrightarrow B$. On dit que $\mathbb{Z}$ est un objet initial dans la catégorie des anneaux commutatifs (et aussi dans la catégorie des anneaux non-commutatifs, mais on peut seulement appliquer la Proposition 2.2.3 pour les anneaux commutatifs). On obtient que, pour chaque $b \in B$, il existe un unique homomorphisme ev_b comme indiqué dans le diagramme suivant :

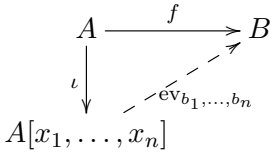


En itérant la Proposition 2.2.3 on obtient le résultat suivant :

Corollaire 2.2.6. *Soit $f : A \to B$, un homomorphisme d'anneaux commutatifs et fixons $b_1, \ldots, b_n \in B$. Il existe un unique homomorphisme d'anneaux $\mathrm{ev}_{b_1,\ldots,b_n} : A[x_1, \ldots, x_n] \to B$ tel que*

(1) $\mathrm{ev}_{b_1,\ldots,b_n}(t_i) = b_i$ pour chaque $1 \le i \le n$, et

(2) $\mathrm{ev}_{b_1,\ldots,b_n} \circ \iota = f$, où ι désigne l'inclusion $\iota\colon A \hookrightarrow A[x_1, \ldots, x_n]$. En d'autres termes le diagramme commute :



Définition 2.2.7. Si A est un sous anneau d'un anneau commutatif B, et $b_1, \ldots, b_n \in B$, alors le *sous-anneau de B engendré par A et $b_1, \ldots, b_n$* est l'image de $\mathrm{ev}_{b_1,\ldots,b_n}$, et on le note $A[b_1, \ldots, b_n]$.

On dit que B est *une A-algèbre finiment engendrée* s'il existe $b_1, \ldots, b_n \in B$ tels que $A[b_1, \ldots, b_n] = B$.

Remarque 2.2.8. Il faut être prudent avec la possible confusion entre la notation de l'anneau des polynômes et celle du sous-anneau engendré par une collection des éléments. Cela veut dire quand lorsqu'on voit $A[t_1, \dots, t_n]$, il faut toujours vérifier si les t_i sont variables ou des éléments d'un anneau qui contient A.

Exemple 2.2.9. En appliquant Définition 2.2.7 avec $A = \mathbb{Z}$, $B = \mathbb{C}$ et $b = i$ on obtient les sous-anneaux suivants de $\mathbb{C}$:

$$\mathbb{Z}[i] \underset{\uparrow}{=} \left\{ p(i) \;\middle|\; p(t) \in \mathbb{Z}[t] \right\} \underset{\uparrow}{=} \left\{ a + bi \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

par Définition 2.2.7 — $\forall k \in \mathbb{N}$: $i^{2k} = (-1)^k$ et $i^{2k+1} = i(-1)^k$

On appelle cet anneau l'anneau des entiers de Gauss. Ainsi, on peut voir que $\mathbb{Z}[i] \ncong \mathbb{Z}[t]$. En effet, il existe, dans le premier, un élément a (i lui-même), tel que $a^2 = -1$. Cependant, dans le dernier, on ne peut pas trouver de tel élément (le coefficient du terme de degré plus grand de a^2 est le carré du coefficient du terme de degré plus grand de $a \in \mathbb{Z}[t]$, et par conséquence c'est une racine de -1, et telle racine de -1 n'existe pas dans $\mathbb{Z}$).

2.2.3 Anneaux de groupes

Soit G un groupe, A un anneau. L'anneau $A[G]$, appelé *l'anneau du groupe* G, est constitué de l'ensemble des combinaisons linéaires *finies* formelles d'éléments de G, avec pour coefficients des éléments de A. Avec formules :

$$\left\{ \sum_{k=1}^{m} a_k g_k \;\middle|\; m \in \mathbb{N},\ a_k \in A,\ g_k \in G \right\}$$

La somme de ces éléments est définie terme à terme, et la multiplication induite par celle de G :

$$\left(\sum_{i=1}^{m} a_i g_i \right) \left(\sum_{j=1}^{n} b_j h_j \right) = \sum_{i,j} \underbrace{a_i b_j}_{\text{loi de } A} \overbrace{(g_i h_j)}^{\text{loi de } G} \tag{2.2.c}$$

L'unité de cet anneau est $1_A \cdot 1_G$. On laisse comme exercice la vérification que $A[G]$ est bien un anneau.

Exemple 2.2.10. $\mathbb{Z}[S_3]$ est, comme *groupe abélien*, isomorphe à $\mathbb{Z}^6$. Toutefois, cet anneau n'est pas commutatif, car

$$1(12) \cdot 1(23) = 1(123) \neq 1(132) = 1(23) \cdot 1(12)$$

Ceci constitue un exemple de deux ensembles isomorphes en tant que groupes mais *pas* en tant qu'anneaux.

Un autre exemple de calcul dans $\mathbb{Z}[S_3]$ est

$$(1 + (12))^2 = (1 + (12))(1 + (12)) \overset{\overbrace{\text{distributivité}}}{=} 1 + 1(12) + (12)1 + \underbrace{(12)(12)}_{=1} = 2 + 2(12)$$

2.2.4 Les entiers modulaires

On note $\mathbb{Z}/n\mathbb{Z}$ le groupe abélien des classes de congruences modulo n. On note $\bar{k}$ la classe de k.

Définition 2.2.11. On définit $\bar{k} \cdot \bar{l} = \bar{kl}$.

Proposition 2.2.12. *Muni de la multiplication "$\cdot$" définie précédemment,* $\left(\mathbb{Z}/n\mathbb{Z}, \cdot, +\right)$ *est un anneau.*

La Proposition 2.2.12 est un cas particulier de la la Proposition 2.4.11, alors on reporte la preuve jusque l'introduction de cette proposition.

2.3 Anneaux intègres et corps

2.3.1 Quelques définitions

Définition 2.3.1. Soit A un anneau. Un élément $0 \neq a \in A$ est un *diviseur de zéro*, si il existe $0 \neq b \in A$ tel que $ba = 0$ ou $ab = 0$.

Un élément $a \in A$ est dit *inversible* s'il existe un élément $b \in A$ tel que $ac = 1 = ca$.

Si a est inversible il n'est pas un diviseur de zéro ($ab = 0 \implies b = cab = c \cdot 0 = 0$ et $ba = 0 \implies b = bac = 0 \cdot c = 0$). Par conséquent, si un élément c comme ci-dessus existe, alors il est unique (si c' est un autre tel élément, alors $a(c - c') = 0$, et alors $0 = c - c'$). Alors, on dénote c par a^{-1}. On note de plus $A^\times$ l'ensemble des éléments inversibles de A.

La fin du 1. cours, le 21.02.2021.

Remarque 2.3.2. On doit demander que l'inverse b soit un inverse à gauche et à droite si l'anneau n'est pas commutatif (en général). Le phénomène agréable étudié en algèbre linéaire qui fait qu'une matrice carrée est un inverse à gauche si et seulement si c'est un inverse à droite est basé sur le fait qu'un endomorphisme de K^n est injectif si et seulement s'il est surjectif. Cette particularité n'est pas vraie dans un anneau quelconque. Nous verrons un exemple dans la série 2.

Remarque 2.3.3. Si $f : A \to B$ est un homomorphisme d'anneaux, l'image d'un élément a inversible est inversible et alors $f(a^{-1}) = (f(a))^{-1}$. En particulier, la dernière équation découle du développement suivant :

$$f(a^{-1})f(a) \underset{\uparrow}{=} f(a^{-1}a) = f(1) \underset{\uparrow}{=} 1$$

Définition 2.1.7 Définition 2.1.7

Exemple 2.3.4. On prétend que $F[t]^\times = F$ où F et un corps. Pour cela rappelons que le degré $\deg p(t)$ d'un polynôme $p(t) \in F[t]$ est le plus grand entier naturel n tel que le coefficient devant t^n de $p(t)$ est différent de zéro (ce coefficient s'appelle le *coefficient dominant*). On a clairement, pour $p(t)$ et $q(t) \in F[t]$, que

$$\deg\big(p(t) \cdot q(t)\big) = \big(\deg p(t)\big) + \big(\deg q(t)\big) \tag{2.3.a}$$

et

$$p(t) \in F \iff \deg p(t) = 0$$

Pour démontrer $F[t]^\times = F$, on commence par remarquer que $F \subseteq F[t]^\times$. Pour l'autre inclusion, prenons $p(t) \in F[t]^\times$. Par la définition d'être inversible, il existe $q(t) \in F[t]$ tel que $q(t)p(t) = 1$. En utilisant l'équation (2.3.a) on obtient que $\big(\deg p(t)\big) + \big(\deg q(t)\big) = 0$, et la seule possibilité est alors $\deg p(t) = 0$, ce qui signifie que $p(t) \in F$.

Définition 2.3.5. Un anneau non nul A est un *corps* s'il est commutatif et que $A^\times = A \setminus \{0\}$.

On parle parfois de *corps gauche* lorsque l'hypothèse de commutativité n'est pas demandée, mais dans ce cours les corps seront commutatifs par définition.

Exemple 2.3.6. On a appris en Algèbre Linéaire I que $\mathbb{Z}/p\mathbb{Z}$ est un corps pour chaque premier $p \in \mathbb{N}$. Dans ce cas, on le note $\mathbb{F}_p$.

Définition 2.3.7. Un anneau A est *intègre* s'il est non nul, commutatif et s'il n'a pas de diviseur de zéro.

Proposition 2.3.8. *Tout anneau fini et intègre est un corps.*

La preuve est en exercice dans la série 2. Elle est basée sur l'analyse de l'application $\varphi_a \colon A \to A$ définie par $\varphi_a(b) = ab$ pour tout $b \in A$.

Exemple 2.3.9.
- $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$
- Si A est un sous anneau d'un corps K, alors il est intègre.

2.3.2 Le corps des fractions

Dans cette section, on généralise la construction de $\mathbb{Q}$. On pense à $\mathbb{Q}$ comme un corps qui contient $\mathbb{Z}$ comme sous-anneau, et dont tous les éléments sont des fractions d'éléments de $\mathbb{Z}$. On fait la même construction pour un anneau intègre quelconque A. En réalité, la construction et les preuves seront les mêmes que dans le cas de $\mathbb{Q}$. Notre but principal est donc de vérifier qu'ils restent mathématiquement corrects et cohérents en remplaçant $\mathbb{Z}$ par A.

Définition 2.3.10. Un *corps des fractions* d'un anneau intègre A est un corps K qui contient A tel que tout élément non nul $x \in K$ s'écrit comme fraction $x = \frac{a}{b}$, où $a \in A$ et $b \in A \setminus \{0\}$.

Notation 2.3.11. Si K est un corps des fractions d'un anneau intègre A, alors on note l'injection structurelle $\iota : A \to K$. Par définition, c'est un homomorphisme injectif.

Remarque 2.3.12. Il y a deux aspects de la Définition 2.3.10 qui ne sont pas clairs à ce point :

(1) Il n'est pas clair qu'un tel corps existe. Nous allons le démontrer.
(2) Il n'est pas clair qu'un tel corps est unique dans un quelconque sens.

Construction du corps des fractions

On définit une relation sur $A \times \big(A \setminus \{0\}\big)$ par

$$(a, b) \sim (a', b') \Leftrightarrow\ ab' = a'b$$

Affirmation 2.3.13. *Cette relation définit une relation d'équivalence.*

Démonstration. (1) la symétrie et la réflexivité sont évidentes.

(2) Pour la transitivité, supposons que $(a, b) \sim (a', b')$ et que $(a', b') \sim (\tilde{a}, \tilde{b})$. Alors on a les égalités

$$ab' = a'b \qquad \text{et} \qquad a'\tilde{b} = b'\tilde{a}$$

Notre but est de montrer que $a\tilde{b} = \tilde{a}b$. On calcule d'abord

$$a\tilde{b}b' = ab'\tilde{b} = a'b\tilde{b} = a'\tilde{b}b = b'\tilde{a}b$$

Ce qui nous donne

$$(a\tilde{b} - b\tilde{a})b' = 0.$$

Par intégrité et puisque $b' \neq 0$, on a $\tilde{a}b = a\tilde{b}$.

□

Remarque 2.3.14. Dans la dernière partie de la preuve ci-dessus, on a simplifié par un élément non nul : cette pratique est toujours valable dans un anneau intègre.

Lemme 2.3.15 (Lemme et notation)**.** *$\frac{a}{b}$ désigne la classe (a, b), et on définit K comme l'ensemble des classes d'équivalence de $A \times \big(A \setminus \{0\}\big)$ par $\sim$.*

Soient $a, a', c \in A$, et $b, b', d \in A \setminus \{0\}$. On munit K de deux opérations :

(1) Somme : $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}$
(2) Produit : $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Ces opérations sont bien définies (i.e, ne dépendent pas du choix du représentant d'une classe).

Démonstration. si $\frac{a}{b} = \frac{a'}{b'}$ et que $\frac{c}{d} = \frac{c'}{d'}$, alors on a les relations

$$ab' = a'b \qquad \text{et} \qquad cd' = c'd \tag{2.3.b}$$

On voudrait montrer que

$$\begin{gathered}\frac{ad+bc}{bd} = \frac{a'd'+c'd'}{b'd'} \\ \Updownarrow \\ (ad+bc)b'd' = (a'd'+c'b')bd \\ \Updownarrow \\ adb'd'+bcb'd' = a'd'bd+c'b'bd \\ \Updownarrow \\ ab'dd'+cd'bb' = a'bd'd+c'db'b\end{gathered}$$

En particulier, la dernière ligne est vraie grace à l'équation (2.3.b).

Le produit se montre de façon similaire. □

Proposition 2.3.16. *K définit précédemment est un corps qui contient A sous la forme d'un sous-anneau via l'homomorphisme d'inclusion*

$$\forall a \in A\colon \iota(a) = \frac{a}{1},$$

En particulier, $\frac{0}{1}$ et $\frac{1}{1}$ sont le zéro et l'unité de K, et, de plus, K est un corps des fractions de A.

Démonstration.

K est un corps :

(1) $(K,+)$ est un groupe abélien.

(i) $\frac{0}{1}$ est l'élément neutre, puisque pour tout $a, b \in A$, on a l'identité suivante dans K :

$$\frac{0}{1} + \frac{a}{b} \underset{\uparrow}{=} \frac{0\cdot b + 1\cdot a}{1\cdot b} \underset{\uparrow}{=} \frac{a}{b}$$

définition de l'addition dans K | identités des opérations dans A

(ii) pour tout $a, b \in A$, $-\frac{a}{b} = \frac{-a}{b}$ dans K :

$$\frac{a}{b} + \frac{-a}{b} \underset{\uparrow}{=} \frac{a+(-a)}{b} \underset{\uparrow}{=} \frac{0}{b} \underset{\uparrow}{=} \frac{0}{1}$$

définition de l'addition dans K | identités des opérations dans A | par la définition de $\sim$, parce que $0\cdot 1 = 0\cdot b$ dans A

(iii) $+$ est associative dans K, ce qui veut dire que pour tout $a, b, a', b', \overline{a}, \mathrm{Ob} \in A$, le résultat final du calcul suivant est invariant par permutation des trois paires (a,b), (a',b') et $(\overline{a}, \mathrm{Ob})$, en utilisant le fait que A est commutatif :

$$\left(\frac{a}{b} + \frac{a'}{b'}\right) + \frac{\overline{a}}{\mathrm{Ob}} = \frac{ab'+a'b}{bb'} + \frac{\overline{a}}{\mathrm{Ob}} = \frac{(ab'+a'b)\,\mathrm{Ob} + bb'\overline{a}}{bb'\,\mathrm{Ob}} = \frac{ab'\,\mathrm{Ob} + a'b\,\mathrm{Ob} + \overline{a}bb'}{bb'\,\mathrm{Ob}}$$

(2) $(K,\cdot)$ est un monoïde avec $\frac{1}{1}$ comme l'élément neutre, et les deux opérations dans K sont distributives : cela est similaire à la preuve que $(K,+)$ est un groupe abélien. On les laisse en exercice.

ι est un homomorphisme : pour tout $a, b \in A$, on a

(1)
$$\iota(a+b) = \frac{a+b}{1} = \frac{a\cdot 1 + b\cdot 1}{1\cdot 1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$$

(2)
$$\iota(a\cdot b) = \frac{a\cdot b}{1} = \frac{a\cdot b}{1\cdot 1} = \frac{a}{1}\cdot\frac{b}{1} = \iota(a)\cdot\iota(b)$$

(3) $\iota(1) = \frac{1}{1}$ est l'unité de K

ι est injectif : on a

$$\iota(a) = \iota(b) \iff \underset{\boxed{\text{en } K}}{\frac{a}{1} = \frac{b}{1}} \iff \underset{\boxed{\text{en } A}}{b\cdot 1 = a\cdot 1} \iff \underset{\boxed{\text{en } A}}{b = a}$$

K est un corps des fractions de A : Chaque élément peut s'écrire comme produit d'un élément de A et de l'inverse d'un élément de $A^\times$, puisque $\frac{a}{b} = \frac{a}{1}\frac{1}{b} = \frac{\iota(a)}{\iota(b)}$. □

Corollaire 2.3.17. *Soit A un anneau. Alors :*

$$A \text{ est intègre} \Leftrightarrow A \text{ est un sous-anneau d'un corps.}$$

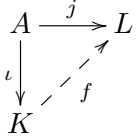
Exemple 2.3.18.

(1) $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.
(2) Si A est déjà un corps, le corps des fractions de A est A.
(3) Le corps des fractions de $K[t]$ est le corps des fractions rationnelles $K(t)$ dont les éléments sont des quotients de polynômes :

$$K(t) = \left\{ \frac{p(t)}{q(t)} \;\middle|\; p(t) \in K[t],\ q(t) \in K[t] \setminus \{0\} \right\}$$

Propriété universelle du corps des fractions

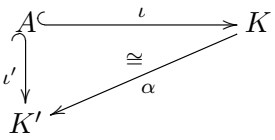
Proposition 2.3.19. PROPRIÉTÉ UNIVERSELLE DU CORPS DES FRACTIONS. *Soit $\iota\colon A \hookrightarrow K$ un corps des fractions de A. Pour tout homomorphisme* injectif *$j : A \hookrightarrow L$, où L est un corps, il existe un unique homomorphisme de corps $K \overset{f}{\hookrightarrow} L$ tel que $f \circ \iota = j$. En d'autres termes le diagramme suivant commute :*



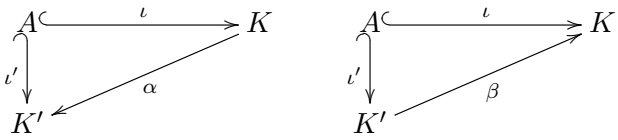
Démonstration. La commutativité du diagramme nous force à avoir $f(\frac{a}{b}) = j(a)j(b)^{-1}$. Il faut alors montrer que cette définition nous donne un homomorphisme, ce qui sera une exercice de la série de cette semaine. □

On est prêt à démontrer en quel sens les corps des fractions de A sont uniques (par conséquent, on écrira *le* corps des fractions).

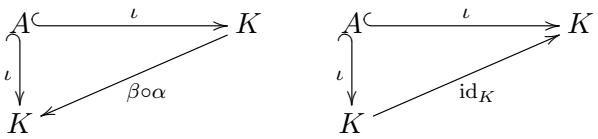
Corollaire 2.3.20. *Le corps des fractions est unique modulo un unique isomorphisme. Cela veut dire que si $\iota\colon A \to K$ et $\iota'\colon A \to K'$ sont deux corps des fractions distincts, il existe un unique isomorphisme $\alpha : K \to K'$ tel que le diagramme suivant commute :*



Démonstration. La preuve est simplement l'utilisation itérée de la Proposition 2.3.19. En utuilisant une première fois la Proposition 2.3.19 pour $j = \iota$ et ensuite pour $j = \iota'$ on obtient deux uniques homomorphismes $\alpha : K \to K'$ et $\beta : K' \to K$ tels que les diagrammes suivants commutent :



Cependant, à ce point, on ne sait pas si α ou β sont des isomorphismes. Cela se démontre avec l'argument suivant, très répandu en algèbre abstraite : considérons $\beta \circ \alpha$ et notons qu'il satifait, aisi que id_K, le même type de diagramme commutatif :



En utilisant l'unicité énoncée dans la Proposition 2.3.19, on obtient que $\beta \circ \alpha = \mathrm{id}_K$. D'une façon similaire, on obtient que $\alpha \circ \beta = \mathrm{id}_{K'}$. Ces deux égalités d'homomorphismes nous disent précisemment que α et β sont des isomorphismes. □

2.4 IDÉAUX ET ANNEAUX QUOTIENTS

Dans cette section, les anneaux ne sont pas nécessairement intègres ou commutatifs, sauf si l'une des ces conditions est demandée explicitement.

Considérons un anneau A et un sous groupe additif I de $(A, +)$. Puisque $(A, +)$ est commutatif, I est un sous-groupe normal de A. On obtient que le quotient A/I, avec la structure additive, est un groupe abélien. On aimerait trouver des conditions sur I qui nous donnent une structure d'anneau sur A/I. En parallèle, on voudrait reconstruire les propositions apprisent pour des groupes dans la catégorie des anneaux. Cela veut dire qu'on souhaiterait que I soit le noyau de l'homomorphisme naturel $A \to A/I$ donné par $a \mapsto a + I$.

Avant de commencer à exécuter le plan ci-dessus, rappelons qu'il existe deux manières de penser à A/I :

(1) C'est l'ensemble des classes à gauche de I, ou, avec des formules

$$A/I = \{\ a + I \mid a \in A\ \}$$

Dans ce cas, on définit l'addition par $(a + I) + (b + I) = (a + b) + I$, l'élément neutre est $0 + I$ et l'inverse est $-(a + I) = -a + I$.

(2) C'est le quotient A/R par la relation d'équivalence $a \sim b \iff b - a \in I$. Dans ce cas, on définit les opérations à l'aide des représentants. Cela veut dire que, pour chaque élément a, $[a]$ dénote la classe d'équivalence qui contient a, et on définit $[a] + [b] = [a + b]$. L'élément neutre est $[0]$ et l'inverse est $-[a] = [-a]$.

Il y a un théorème de théorie de groupes qui montre que les classes d'équivalence de R sont précisemment les classes à gauche.

2.4.1 Idéaux : définitions

On commence en devinant les propriétés de I qui nous garantissent que A/I est un anneau tel que l'application $\xi : A \to A/I$ est un homomorphisme. Dans ce cas, $I = \ker \xi$, et on peut trouver un indice pour notre devinette en réfléchissant sur les propriétés des noyaux. Quelles sont les propriétés particulières du noyau $\ker \phi$ d'un homomorphisme ϕ d'anneau ? Par exemple, on a :

$$a \in \ker \phi, b \in A \implies \phi(ba) \underset{\uparrow}{=} \phi(b)\phi(a) \underset{\uparrow}{=} 0 \cdot \phi(a) = 0 \implies ba \in \ker \phi \tag{2.4.a}$$

ϕ est un homomorphisme — $a \ker \phi$

Cela est la motivation de la définition suivante :

Définition 2.4.1. Un sous ensemble I de A est un *idéal à gauche* (resp. à droite) si $(I, +)$ est un sous-groupe abélien de $(A, +)$ et si

$$\forall a \in A, \forall x \in I \ : \ ax \in I \qquad (\text{resp. } xa \in I). \tag{2.4.b}$$

Si I est un idéal à gauche et à droite, on dit que I est un idéal *bilatère*.

La notation $I \trianglelefteq A$ dénote que I est un idéal bilatère de A.

Lemme 2.4.2. *Un sous-ensemble I d'un anneau A est un idéal à gauche si et seulement si les deux propriétés suivantes sont satisfaites :*

(1) $\forall x, y \in I \ : \ x + y \in I$, *et*

(2) $\forall x \in I, a \in A \ : \ ax \in I$

Démonstration. La seule différence entre cette proposition et la Définition 2.4.1 est que, si on utilise la Définition 2.4.1 pour vérifier que $(I, +)$ est un sous-groupe de $(A, +)$, alors il faut aussi vérifier que

$$\forall x \in I \ : \ -x \in I \tag{2.4.c}$$

En particulier, il faut juste montrer qu'en supposant les deux propriétés listées dans le lemme actuel, on obtient (2.4.c) automatiquement. En effet, on retrouve cela par le calcul suivant, où $x \in I$ quelconque :

$$-x = (-1) \cdot x \underset{\uparrow}{\in} I$$

en utilisant la condition (2) du lemme actuel pour $a = -1$

□

Remarque 2.4.3. Si A est commutatif, tout idéal est bilatère, et on dit simplement que I est un idéal.

Exemple 2.4.4. Dans un anneau A quelconque, $\{0\}$ et A sont des idéaux bilatères. On les appelle les *idéaux (bilatères) triviaux*.

Définition 2.4.5. Soit A un anneau. Pour $a \in A$, *l'idéal à gauche* (a) *engendré par* a est le plus petit idéal de A qui contient a. On peut vérifier que

$$(a) = Aa = \{\ ba \mid b \in A\ \}.$$

(En réalité, les éléments ba doivent être contenus dans (a), et il suffit ensuite de vérifier que Aa est stable pour l'addition et la multiplication à gauche). On appelle un idéal de la forme (a) un *idéal principal*.

Pour $a_1, \dots a_m \in A$ *l'idéal à gauche* $(a_1, \dots, a_m)$ *engendré par* $a_1, \dots a_m$ est le plus petit idéal de A qui contient tous les a_i. Dans manière similaire, on peut vérifier que

$$(a_1, \dots, a_n) = \sum_{i=1}^{m} Aa_i = \left\{ \sum_{i=1}^{m} b_i a_i \;\middle|\; b_i \in A \right\}$$

La fin du 2. cours, le 23.02.2021.

Exemple 2.4.6. Considérons $A = \mathbb{Z}$, et un idéal $I \trianglelefteq A$ non-trivial. En particulier, I contient au moins un élément, et par conséquent on peut prendre le plus grand entier positif $\operatorname{pgdc}(I)$ qui divise tous les élément de I. On peut voir qu'en réalité il s'agit du plus grand commun diviseur d'un nombre fini d'éléments $a_1, \ldots, a_m \in I$. En utilisant l'algorithme d'Euclide (et peut-être l'induction), on obtient qu'il existe des entiers $b_1, \ldots, b_m \in \mathbb{Z}$, tels que

$$\operatorname{pgdc}(I) = \sum_{i=1}^{m} b_i a_i.$$

Par conséquent $\operatorname{pgdc}(I) \in I$. De plus, par la définition de $\operatorname{pgdc}(I)$ chaque élément de I est de la forme $b \cdot \operatorname{pgdc}(I)$ pour un entier b adéquat. On obtient que $I = \big(\operatorname{pgdc}(I)\big)$.

En somme, on conclut que tous les idéaux de $\mathbb{Z}$ sont principaux.

Proposition 2.4.7. *Soit K un anneau commutatif. Alors :*

$$K \text{ est un corps} \iff \text{les seuls idéaux de } K \text{ sont } \{0\} \text{ et } K$$

Démonstration.

$\boxed{\Longrightarrow :}$ Si I est un idéal non nul de K, on montre qu'il s'agit de K. Soit $x \in I$ non nul. Puisque K est un corps, et par définition d'un idéal, $1_K = x^{-1}x \in I$. Ceci nous permet de déduire que $K = I$.

$\boxed{\Longleftarrow :}$ Considérer, pour un élément x non nul de K, l'idéal monogène (x). Il est égal à K par hypothèse, et donc $1_K \in (x)$. C'est équivalent à dire que $x^{-1} \in K$. □

Remarque 2.4.8. La Proposition 2.4.7 est fausse sans l'hypothèse K commutatif.

Proposition 2.4.9. *Soit $f\colon A \to B$ un homomorphisme d'anneaux. Alors le noyau $\ker(f)$ de f est un idéal bilatère de A.*

Démonstration. On sait de théorie de groupes que $\ker(f)$ est un sous-groupe de $(A, +)$. Ainsi, il suffit de démontrer la propriété (2.4.b). Or cela est démontré en (2.4.a). □

Exemple 2.4.10.

(1) Considérons $ev_a : A[t] \mapsto A$ pour un anneau commutatif A et un élément $f \in A$ quelconque. On affirme que $\ker(ev_a) = (t - a)$.

$\boxed{(t-a) \subseteq \ker(\mathrm{ev}_a) :}$ soit $p(t) \in A[t]$ arbitraire. Le calcul suivant montre cette inclusion :

$$\mathrm{ev}_a\big(p(t)(t-a)\big) \underset{\uparrow}{=} \mathrm{ev}_a\big(p(t)\big)\,\mathrm{ev}_a(t-a) \underset{\uparrow}{=} \mathrm{ev}_a\big(p(t)\big) \cdot 0 = 0$$

$\boxed{\mathrm{ev}_a \text{ est un homomorphisme}}$ $\qquad$ $\boxed{\mathrm{ev}_a(t-f) = 0 \text{ par définition de } \mathrm{ev}_a.}$

$\boxed{(t-a) \supseteq \ker(\mathrm{ev}_a) :}$ Prenons $p(t) \in \ker(\mathrm{ev}_a)$. On démontre que $p(t) \in (t-a)$ par récurrence sur $\deg p(t)$.

Si $\underline{\deg p(t) = 0}$, alors $p(t)$ contient seulement un terme constant, disons $c \in A$. Dans ce cas, $\mathrm{ev}_a(p(t)) = c$, et par conséquent, c et $p(t)$ doivent être égaux à 0.

Si $\underline{\deg p(t) > 0}$, alors notons $m = \deg p(t)$ et

$$p(t) = \sum_{i=0}^{m} a_i t^i.$$

Par conséquent, on a $a_m \neq 0$. De la même façon que ci-dessus, il s'ensuit que $a_m t^{m-1}(t-a) \in \ker \mathrm{ev}_a$. Cela implique que

$$\ker \mathrm{ev}_a \ \ni \ p(t) - a_m t^{m-1}(t-a) = \underbrace{(a_{m-1} - a\cdot a_m)t^{m-1} + \sum_{i=1}^{m-2} a_i t^i}_{\uparrow \text{ le degré et au plus } m-1}.$$

En utilisant l'hypothèse de récurrence, on obtient que $p(t) - a_m t^{m-1}(t-a) \in (t-a)$, qui implique que

$$p(t) = \Big(\underbrace{p(t) - a_m t^{m-1}(t-a) \in (t-a)}_{\uparrow \in (t-a)}\Big) + \underbrace{a_m t^{m-1}(t-a)}_{\uparrow \in (t-a)} \quad \in \ (t-a).$$

(2) Pour regarder des exemples spécifiques on peut prendre $A = \mathbb{Q}$ et $a = 2$. Dans ce cas, $\ker \mathrm{ev}_2$ est l'ensemble des polynômes rationnels de variable t qui s'annulent en 2. L'affirmation que $\ker \mathrm{ev}_2 = (t-2)$ nous dit qu'un polynôme s'annule en 2 si et seulement ce polynôme est un multiple de $t-2$.

(3) En particulier, le point précédent fonctionne pour un corps K quelconque. Cela veut dire que, pour $a \in K$, un polynôme $f \in K[t]$ s'annule en a si et seulement si f est un multiple de $t-a$.

(4) Pour regarder un exemple plus pathologique, on peut prendre un anneau commutatif non-intègre, comme $A = {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$. Pour de tels anneaux, la proposition ci-dessus est vraie. En effet, on n'a supposé là-bas que la commutativité de A. Cependant, $(t-a)$ peut avoir des éléments auxquels nous ne sommes pas habitués : par exemple si $a = [2] \in {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$, alors $[3]t \in (t-[2])$ puisque $[3](t-[2]) = [3]t$.

2.4.2 Anneau quotient et sa propriété universelle

Dans cette section, on présente la construction de l'anneau quotient promise au début de la Section 2.4.

Proposition 2.4.11. CONSTRUCTION DE L'ANNEAU QUOTIENT. *Si I est un idéal* bilatère *d'un anneau A, alors le quotient A/I du groupe abélien $(A,+)$ possède une structure d'anneau, dont les lois d'addition et de multiplication sont induites par celles de A, i.e*

$$(a+I)+(b+I) = (a+b)+I$$

$$(a+I)\cdot(b+I) = (a\cdot b)+I \tag{2.4.d}$$

et l'unité est $1+I \in {}^{A}\!/_{I}$.

Démonstration. On sait déjà (cf cours de Théorie des groupes) que ${}^{A}\!/_{I}$ possède une structure de groupe additif.

Premièrement, on vérifie que la multiplication est bien définie. Prenons $a, b, a', b' \in A$ tels que, dans ${}^{A}\!/_{I}$, on ait les égalités :

$$a+I = a'+I \iff a-a' \in I \qquad \text{et} \qquad b+I = b'+I \iff b-b' \in I.$$

On obtient alors que la multiplication est bien définie par le calcul suivant :

$$ab - a'b' = \underbrace{(a-a')}_{\uparrow \in I} b + a' \underbrace{(b-b')}_{\uparrow \in I} \in I \quad \uparrow \ I \text{ est un idéal bilatère}$$

Deuxièmement, il faut vérifier que la multiplication de A/I nous donne une structure de monoïde et que l'addition et la multiplication, conjointes, sont distributives. Ces vérifications découlent également des règles satisfaites par l'addition et la multiplication dans A. Par exemple, on démontre l'associativité de la multiplication, et on laisse les autres propriétés en exercice. Pour $a, b, c \in A$, on a :

$$\big((a+I)\cdot(b+I)\big)\cdot(c+I) \underset{\uparrow}{=} \big((a\cdot b)+I\big)+(c+I) \underset{\uparrow}{=} (a\cdot b)\cdot c + I \underset{\uparrow}{=} a\cdot(b\cdot c)+I$$

(2.4.d) (2.4.d) multiplication dans A est associative

$$= (a+I)\cdot\big((b\cdot c)+I\big) \underset{\uparrow}{=} (a+I)\cdot\big((b+I)\cdot(c+I)\big)$$

(2.4.d) (2.4.d)

□

Définition 2.4.12. On appelle l'anneau $\left(A/I, +, \cdot\right)$ construit dans la Proposition 2.4.11 *l'anneau quotient* de A par l'idéal bilatère I.

Exemple 2.4.13. Définition 2.4.12 ouvre la porte à beaucoup d'exemples importants de la forme

$$F[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$$

où F est un corps et $f_i \in F[x_1, \ldots, x_n]$ sont polynômes. Par exemple :

(1) $F[t]/(t^2)$ est notre premier exemple d'un anneau commutatif avec un élément $a \neq 0$ tel que $a^2 = 0$ (il faut choisir $a = [t]$, dans quel cas on a $[t]^2 = [t^2] = 0 \in F[t]/(t^2)$). On appelle de tels éléments des éléments nilpotents, et on en apprendra plus durant le semestre.

(2) On apprendra plus tard dans le semestre que $\mathbb{F}_2[t]/(1+t+t^2)$ est un corps.

Proposition 2.4.14. *Soit I un idéal bilatère d'un anneau A. L'application*

$$\begin{aligned} \xi : A &\to A/I \\ a &\mapsto [a] = a + I \end{aligned}$$

est un homomorphisme d'anneau appelé homomorphisme quotient.

Démonstration. On a appris en théorie de groupes que ξ est un homomorphisme de groupe. De plus, le calcul suivant vérifie les autres propriétés qui définissent un homomorphisme :

$$\xi(1) = \underbrace{1+I}_{\uparrow}$$

l'unité en A/I

et pour chaque $a, b \in A$ on a :

$$\xi(ab) = ab + I \underset{\uparrow}{=} (a+I)\cdot(b+I) = \xi(a)\cdot\xi(b)$$

(2.4.d)

□

Corollaire 2.4.15. *Tout idéal bilatère d'un anneau est noyau d'un homomorphisme.*

La prochaine étape est de comprendre les homomorphismes avec source A/I. Pour chaque homomorphisme $\phi : A/I \to B$ d'anneaux, on peut regarder la composition de ϕ avec l'homomorphisme quotient $\xi : A \to A/I$, et on peut essayer de comprendre ϕ à partir de $\phi \circ \xi$. Il y a deux questions auxquelles il faut répondre :

(1) Quels homomorphismes $\rho : A \to B$ sont de la forme $\phi \circ \xi$? Puisque $\ker \xi = I$, on obtient que $I \subseteq \ker(\phi \circ \xi)$. Par conséquent, le meilleur qu'on puisse espérer est que chaque ρ tel que $I \subseteq \ker \rho$ soit de la forme $\phi \circ \xi$.
(2) Pour chaque homomorphisme $\rho : A \to B$, combien de ϕ existe-t-il tels que $\phi \circ \xi = \rho$? Ici le meilleur qu'on puisse espérer est que lorsque ϕ existe, alors il n'en existe qu'un unique.

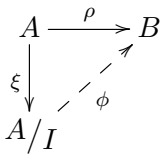
En fait, toutes les spéculations ci-dessus sont vraies, ce qui est exactement le sujet de la proposition suivante.

Proposition 2.4.16. PROPRIÉTÉ UNIVERSELLE DES QUOTIENTS *Soit $\rho : A \to B$ un morphisme d'anneaux tel que I, un idéal bilatère de A, soit inclus dans $\ker(\rho)$. Dénotons par $\xi : A \to A/I$ l'homomorphisme quotient.*

(1) Alors, il existe un unique homomorphisme d'anneaux $\phi : A/I \to B$ tel que

$$\phi \circ \xi = \rho$$

En d'autres termes, le diagramme suivant commute.



(2) Si $I = \ker \rho$, alors le ϕ du point précédent nous donne un isomorphism $A/I \cong \operatorname{im} \rho$.

Démonstration. (1) L'existence de ϕ comme homomorphisme additif ainsi que l'unicité de ϕ est une conséquence des propositions correspondantes en théorie de groupes. On note que ϕ est défini par $\phi(a + I) = \xi(a)$.

Il nous reste à vérifier que ϕ est un homomorphisme d'anneaux. La conservation de l'inversibles découle du fait que ϕ et ξ sont des homomorphismes :

$$\phi\left(1_{A/I}\right) \underset{\uparrow}{=} \phi\big(\xi(1_A)\big) \underset{\uparrow}{=} \rho(1_A) \underset{\uparrow}{=} 1_B$$

$\boxed{\xi \text{ est un homomorphisme}}$ $\boxed{\rho = \phi \circ \xi}$ $\boxed{\rho \text{ est un homomorphisme}}$

La conservation de la multiplication est similaire ; il faut juste argumenter plus longuement. Pour $a, b \in A$ on a :

$$\phi\big((a+I)(b+I)\big) \underset{\uparrow}{=} \phi(ab+I) \underset{\uparrow}{=} \phi(\xi(ab)) \underset{\uparrow}{=} \rho(ab) \underset{\uparrow}{=} \rho(a)\rho(b) \underset{\uparrow}{=} \phi(\xi(a))\phi(\xi(b)) \underset{\uparrow}{=} \phi(a+I)\phi(b+I)$$

$\boxed{\text{multiplication en } A/I}$ $\boxed{\text{la définition de } \xi}$ $\boxed{\phi \circ \xi = \rho}$ $\boxed{\rho \text{ est un homomorphisme}}$ $\boxed{\phi \circ \xi = \rho}$ $\boxed{\text{la définition de } \xi}$

(2) Dans ce cas ϕ est injectif : l'argument suivant démontre que $\ker \phi = \{0 + I\}$, où $a \in A$:

$$\phi(a + I) = 0 \;\Rightarrow\; \rho(a) = 0 \underset{\uparrow}{\Rightarrow} a \in I.$$

$\boxed{I = \ker \rho}$

Par conséquent, ϕ nous donne un isomorphisme ${}^{A}/_{I} \to \operatorname{im}\phi$. Par la surjectivité de ξ, on a aussi $\operatorname{im}\phi = \operatorname{im}\rho$. Ceci conclut la démonstration.

□

Corollaire 2.4.17. THÉORÈME D'ISOMORPHISME. *Soit $\rho : A \to B$ un homomorphisme d'anneaux. Alors on a ${}^{A}/_{\ker\rho} \cong \operatorname{im}\rho$. En particulier, si ρ est surjectif, ${}^{A}/_{\ker\rho} \cong B$.*

Démonstration. C'est un cas particulier du point (2) de la Proposition 2.4.16. □

Exemple 2.4.18. Considérons $\mathrm{ev}_i : \mathbb{Z}[t] \mapsto \mathbb{C}$. On prétend que $\ker \mathrm{ev}_i = (t^2+1)$. L'argument est similaire au point (1) de l'Exemple 2.4.10. Comme dans cette démonstration, on obtient premièrement que $(t^2+1) \subseteq \ker \mathrm{ev}_i$, et dans un second temps on démontre que $f \in \ker \mathrm{ev}_i$ est aussi contenu dans (t^2+1). La deuxième partie est démontrée par récurrence sur $\deg f$:

$\deg f \leq 1$: Dans ce cas $f = at + b$ pour $a, b \in \mathbb{Z}$. En utilisant que $at + b \in \ker ev_i$ on obtient que $ai + b = 0$ comme éléments de $\mathbb{C}$. Cela implique par définition de $\mathbb{C}$ que $a = b = 0$.

$\deg f > 1$: Ce cas est pratiquement identique au point (1) de l'Exemple 2.4.10, on ne présente donc pas les détails. La condition cruciale qui permet d'utiliser le même argument est que le coefficient dominant de t^2+1 (le coefficient non-zéro de plus grand degré) est 1 et donc l'inverse existe.

On obtient que, effectivement, $\ker \mathrm{ev}_i = (t^2+1)$. On a déjà vu aussi dans l'Exemple 2.2.9 que $\operatorname{im}(ev_i) = \mathbb{Z}[i]$. En mettant ensemble ces deux faits, et en utilisant la Corollaire 2.4.17, on obtient que

$$\mathbb{Z}[t]\Big/(t^2+1) \cong \mathbb{Z}[i]$$

C'est notre première application du Corollaire 2.4.17.

Exemple 2.4.19. Le Corollaire 2.4.17 est un cas spécifique de la Proposition 2.4.16, qui possède beaucoup d'applications. On donne ici un exemple.

En général la Proposition 2.4.16 peut être utilisé pour comprendre les homomorphismes de quotients. Par exemple, pour un anneau quelconque B, les homomorphismes $\mathbb{F}_p \to B$ correspondent aux homomorphismes $\rho : \mathbb{Z} \to B$ tels que $p\mathbb{Z} \subseteq \ker\rho$.

Exemple 2.4.20. Considérons $I = (1+3i) \subseteq \mathbb{Z}[i] = A$. On cherche à étudier le quotient $B = {}^{A}/_{I}$. Considérons l'homomorphisme universel $\rho\colon \mathbb{Z} \to B$ de l'Exemple 2.2.5. On comprendra B en utilisant ρ. Plus précisément, si on démontre que ρ est surjectif, alors il suffit de trouver son noyau pour avoir une bonne description, grâce au Corollaire 2.4.17.

ρ est surjectif : Considérons $a + bi \in \mathbb{Z}[i]$. On dénote par $[a+bi]$ la classe à gauche de $(a+bi)+I \in B$. En utilisant cette notation, le calcul suivant conclut la surjectivité de ρ :

$$[a+bi] = [a] + [bi] \underset{\uparrow}{=} [a] + [b3] = \rho(a+3b).$$

$$\boxed{1+3i \in I \implies i(1+3i) = i-3 \in I \implies [bi] = [b3]}$$

$\ker\rho = (10)$: pour un entier $a \in \mathbb{Z}$, on a $\rho(a) = 0$ si et seulement si

$$\exists c, d \in \mathbb{Z} \ : \ a = (1+3i)(c+di) = (c-3d)+(3c+d)i \iff d = -3c \text{ et } a = c-3d \underset{\uparrow}{=} c+9c = 10c.$$

$$\boxed{d = -3c}$$

On obtient que $\rho(a) = 0$ si et seulement si $a \in (10)$.

Utilisons le Corollaire 2.4.17 : On obtient que $B \cong {}^{\mathbb{Z}}/_{10\mathbb{Z}}$. En particulier, B n'est pas intègre. On verra à la Section 2.5 que cela signifie que $(1+3i) \subseteq \mathbb{Z}[i]$ n'est pas un idéal premier.

La fin du 3. cours, le 02.03.2021.

2.4.3 La caractéristique d'un anneau

Soit A un anneau et $f\colon \mathbb{Z} \to A$ l'unique homomorphisme d'anneaux de source $\mathbb{Z}$, introduit dans l'Exemple 2.2.5. On observe que $f(1) = 1_A$, et comme $n = 1 + \cdots + 1$ pour tout entier naturel n, alors par induction

$$f(n) = \underbrace{1_A + \cdots + 1_A}_{\boxed{n\text{-fois}}}$$

Le noyau de f est un idéal de $\mathbb{Z}$, il est donc de la forme (n) pour un entier $n \in \mathbb{N}$, en utilisant Exemple 2.4.6.

Définition 2.4.21. La *caractéristique* de l'anneau A est le seul entier naturel $\operatorname{car} A = n$ tel que $\ker(f) = (n)$ où $f : \mathbb{Z} \to A$ est l'unique homomorphisme de source $\mathbb{Z}$.

Exemple 2.4.22. (1) $\operatorname{car} \mathbb{Z} = 0 = \operatorname{car} \mathbb{Q} = \operatorname{car} \mathbb{R}$

(2) $\operatorname{car}\left(\mathbb{Z}/n\mathbb{Z}\right) = n = \operatorname{car}\left(M_n(\mathbb{Z}/n\mathbb{Z})\right) = \operatorname{car}\left((\mathbb{Z}/n\mathbb{Z})[t]\right)$.

En général, pour un anneau quelconque A, il y a trois possibilités pour $\operatorname{car} A$:

(1) $\boxed{\operatorname{car} A = 1 :}$ dans ce cas, par définition $1 = 0$, et on obtient $A = 0$.

(2) $\boxed{\operatorname{car} A = 0 :}$ ce cas se passe si et seulement si $f\colon \mathbb{Z} \to A$ est injectif.

(3) $\boxed{\operatorname{car} A = n \geq 2 :}$ ce cas se passe si et seulement s'il y un homomorphisme injectif $\mathbb{Z}/n\mathbb{Z} \hookrightarrow A$ (c'est découle directement de la Corollaire 2.4.17).

On note que, dans ce dernier cas, si A est intègre, alors n est un nombre premier. En effet, on pourrait autrement écrire $n = ab$ pour des entiers $a, b > 1$, et alors on aurait $A \ni [n] = 0 = [a][b]$. Ici, $[a] \neq 0$ et $[b] \neq 0$, parce que $a, b < n$. Ainsi, $0 = [a][b]$ nous donnerait des diviseurs de zéro, ce qui est une contradiction.

Pour les corps, on peut même en dire plus. Pour un corps K on a deux possibilité :

(1) $\boxed{\operatorname{car} K = 0 :}$ Dans ce cas on a un homomorphisme injectif $\mathbb{Q} \hookrightarrow K$ en utilisant la Proposition 2.3.19.

(2) $\boxed{\operatorname{car} K = p > 0 \text{ pou un nombre premier } p :}$ Dans ce cas, on a déjà démontré au dessus qu'on obtient un homomorphisme injectif $\mathbb{F}_p \hookrightarrow K$.

Définition 2.4.23. Le sous-corps dans les deux cas au-dessous sont les plus petits sous-corps de K, et on les appelle les *corps premiers* de K.

Remarque 2.4.24. On peut trouver une définition équivalente pour la caractéristique de A : c'est l'ordre de 1_A pour le groupe $(A, +)$.

Exemple 2.4.25. Attention ! Si $\operatorname{car}(A) = p$, A n'est pas nécessairement intègre. Prenons par exemple $\mathbb{F}_p[t]\big/(t^2)$.

2.4.4 Opérations sur les idéaux

Ici on discute des constructions qui permettent d'obtenir de nouveaux idéaux à gauche à partir d'autres idéaux à gauche. Nous ne traiterons pas explicitement le cas des idéaux à droite, semblable en tout point à ce que nous présentons ici pour les idéaux à gauche.

Étant donné deux idéaux à gauche I et J d'un anneaux A, on peut se demander quels sont les idéaux les plus petits contenus dans I et J (resp. plus grands qui contiennent I et J).

(1) **Intersection.** L'*intersection* $I \cap J$ de I et J est le plus grand des minorants de I et J. C'est même le plus grand sous-ensemble contenu dans I et J, il suffit donc juste de vérifier que c'est bien un idéal à gauche. Pour cela, il faut montrer qu'il contient $0 \in A$, et qu'il

est stable pour l'addition et pour la multiplication par un élément de A à gauche. C'est une conséquence directe du fait que les mêmes conditions sont satisfaites pour I et pour J aussi.

(2) **Somme.** La *somme* de I et J est

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

et c'est le plus petit des majorants de I et J. On peut vérifier que c'est un idéal à gauche en utilisant la distributivité ainsi que le fait que $+$ est commutative. On laisse les détails en exercice.

(3) **Produit.** Le *produit* de I et J, est

$$I \cdot J = \left\{ \sum_{k=1}^{n} x_k \cdot y_k \;\middle|\; k \in \mathbb{N}, x_k \in I, y_k \in J \right\}.$$

On laisse en exercice la vérification que $I \cdot J$ est un idéal à gauche de A.

Matériel optionnel

Remarque 2.4.26. Il est important dans la définition d'un produit d'idéaux de prendre des sommes finies de produits d'éléments, et pas seulement des produits d'éléments.

Par exemple, si F est un corps, pour $A = F[x_1, x_2, x_3, x_4]$, $I = (x_1, x_2)$ et pour $J = (x_3, x_4)$, l'ensemble

$$(I \cdot J)_{\text{faux}} = \left\{ x \cdot y \;\middle|\; x \in I, y \in J \right\}.$$

n'est pas stable pour l'addition. En effet, on a x_1x_3 et $x_2x_4 \in (I \cdot J)_{\text{faux}}$, mais $x_1x_3 + x_2x_4 \notin (I \cdot J)_{\text{faux}}$. Pour le montrer précisément, supposons que $x_1x_3 + x_2x_4 = fg$ pour $f \in I$ et $g \in J$. Notons que tous les éléments non-zéros de I et J ont degré au moins 1. On note que dans un anneau de polynômes de plusieurs variables, le degré est défini de façon similaire au cas d'anneau de polynômes d'une variable. Cela veut dire que pour $h \in F[x_1, x_2, x_3, x_4]$, le degré $\deg h$ de h est défini comme le plus grand degré $d_1 + d_2 + d_3 + d_4$ des monômes $x_1^{d_1}x_2^{d_2}x_3^{d_3}x_4^{d_4}$ qui apparaissent dans h avec des coefficients non-zéros. On note aussi qu'on retient la multiplicativité du degré des anneaux de polynômes d'une variable. Cela veut dire que pour $h_1, h_2 \in F[x_1, x_2, x_3, x_4]$, on a $\deg(h_1h_2) = (\deg h_1) + (\deg h_2)$. En effet, cette égalité découle directement de la règle de multiplication pour les monômes. Cela implique qu'on a $\deg(h_1h_2) \leq (\deg h_1) + (\deg h_2)$ pour h_i arbitraire. Pour démontrer $\deg(h_1h_2) \geq (\deg h_1) + (\deg h_2)$, il faut trouver un monôme de h_1h_2 de degré $(\deg h_1) + (\deg h_2)$. Le problème est qu'en évaluant h_1h_2, il peut y avoir beaucoup de termes qui s'annulent entre eux, et dans ce cas, le coefficient du produit de certains monômes non-zéros de h_1 et de h_2 peuvent être 0 en h_1h_2. Ce problème est résolvable, ce qui veut dire que l'on peut trouver un monôme de h_1h_2 de degré $(\deg h_1) + (\deg h_2)$ avec coefficient non-zéro en ordonnant par exemple les monômes de plus grand degré de h_1 et de h_2 par ordre lexicographique. Si c_1 et c_2 sont les coefficients des monômes m_1 et m_2 plus hauts dans cet ordre, alors on obtient que le coefficient du monôme m_1m_2 de h_1h_2 est c_1c_2. Le point crucial ici est que parce que m_1 et m_2 sont plus hauts dans l'ordre lexicographique, il n'y pas d'autre monôme qui contribue à m_1m_2.

De toute façon, puisque $fg = x_1x_3 + x_2x_4$, on obtient que $\deg f = \deg g = 1$.

Cependant, les éléments de degré 1 de I et J sont de la forme $a_1x_1 + a_2x_2$ et de la forme $a_3x_3 + a_4x_4$ respectivement, pour $a_i \in F$ (pour le démontrer considérons les homomorphismes $\mathrm{ev}^1 : k[x_1, x_2, x_3, x_4] \to k[x_1, x_2]$ et $\mathrm{ev}^2 : k[x_1, x_2, x_3, x_4] \to k[x_3, x_4]$ donnés par la composition des homomorphismes d'évaluation qui envoient x_i à 0. Notons que les polynômes linéaires dans $\ker \mathrm{ev}^1$ et dans $\ker \mathrm{ev}^2$ sont de la forme $a_3x_3 + a_4x_4$ et $a_1x_1 + a_2x_2$ respectivement). Par conséquence, on a

$$x_1x_3+x_2x_4 = (a_1x_1+a_2x_2)\cdot(a_3x_3+a_4x_4) = a_1a_3x_1x_3+a_1a_4x_1x_4+a_2a_3x_2x_3+a_2a_4x_2x_4$$

$$\Downarrow$$

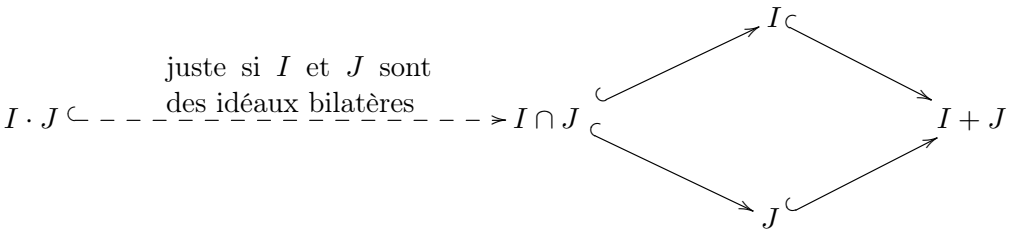
$$a_1a_3 = 1, \qquad a_2a_4 = 1, \qquad a_1a_4 = 0, \qquad a_2a_3 = 0$$

C'est une contradiction, parce que les a_i sont à la fois inversibles et diviseurs de zéro. (Si $ab = 0$, et b est inversible, alors $a = abb^{-1} = 0b^{-1} = 0$.)

Remarque 2.4.27. La réunion $I \cup J$ n'est pas un idéal en général, plus précisément ce n'est même pas un sous-groupe additif en général. C'est la raison pour laquelle cela ne peut pas être le plus petit idéal qui contient I et J.

Pour un exemple spécifique, regardons, pour un corps F, l'anneau $A = \mathbb{Z}$ et les anneaux $I = (2)$ et $J = (3)$. Alors, $2 + 3 = 5 \notin I \cup J$, parce que $2 \nmid 5$ et $3 \nmid 5$.

Remarque 2.4.28. On peut visualiser les inclusions entre idéaux définis au-dessus par



Un exemple où $I \cdot J \not\subseteq I \cap J$ pour I et J des idéaux à gauche est le suivant : prenons un corps F et l'anneau des matrices $\mathrm{Mat}(F, 3)$ de dimension 3×3 et les idéaux

$$I = \left\{ \begin{pmatrix} a & 0 & 0 \\ d & 0 & 0 \\ g & 0 & 0 \end{pmatrix} \;\middle|\; a, d, g \in F \right\} \qquad J = \left\{ \begin{pmatrix} a & b & 0 \\ d & e & 0 \\ g & h & 0 \end{pmatrix} \;\middle|\; a, b, d, e, g, h \in F \right\}$$

Dans ce cas $I \cap J = I$ mais

$$I \cdot J = \left\{ \begin{pmatrix} a & b & 0 \\ d & e & 0 \\ g & h & 0 \end{pmatrix} \;\middle|\; a, b \in F \right\}$$

Remarque 2.4.29. La somme et le produit des idéaux (à gauche) peut être calculée aisément si les idéaux (à gauche) sont donnés par générateurs. Par exemple : si $I = (f_1, \ldots, f_m)$ et $J = (g_1, \ldots, g_n)$ sont idéaux à gauche dans un anneau A, alors par définition on a

$$I + J = \left(f_1, \ldots, f_m, g_1, \ldots, g_n \right).$$

et quand A est commutatif on a aussi

$$I \cdot J = \left(f_i \cdot g_j \;\middle|\; 1 \leq i \leq m, 1 \leq j \leq n \right)$$

D'un autre côté, l'intersection d'idéaux ne peut pas être calculée explicitement dans un anneau général. Cependant, dans des anneaux spécifiques , même l'intersection peut être calculée . On peut de plus donner de meilleures formules pour le produit et la somme dans des anneaux spécifiques, voyons l'Exemple 2.4.30.

Exemple 2.4.30. Dans $\mathbb{Z}$, on peut calculer très efficacement les opérations ci-dessus pour les idéaux. Premièrement, si I et J sont des idéaux de $\mathbb{Z}$, alors de l'Exemple 2.4.6, on sait que $I = (a)$ et $J = (b)$ pour des entiers $a, b \in \mathbb{Z}$. Dans ce cas, il y a les expressions suivantes pour l'intersection et la somme, qui seront démontrées dans un exercice :

$$I \cap J = \text{ppmc}\{a, b\} \qquad \text{et} \qquad I + J = \text{pgdc}\{a, b\}$$

En utilisant ces expressions et aussi la Remarque 2.4.29 pour le produit, on obtient que si $I = (12)$ et $J = (18)$, alors

- $I \cdot J = (216)$,
- $I \cap J = (36)$ car 36 est le ppmc de 12 et 18, et
- $I + J = (6)$ car 6 est leur pgdc.

Lemme 2.4.31. *Soit $f : A \to B$ un homomorphisme d'anneaux, $J \subseteq B$ un idéal à gauche (resp. à droite). Alors $f^{-1}(J)$ est un idéal de A à gauche (resp. à droite).*

Démonstration. Le cas à droite se traite de façon identique :

(1) On connait par la théorie de groupes que $f^{-1}(J)$ est un sous groupe de $(A, +)$.
(2) Pour la stabilité par rapport à la multiplication par un élément $a \in A$ à gauche :

$$x \in f^{-1}(J) \implies \exists y \in J \colon f(x) = y \implies f(ax) = f(a)f(x) = f(a)y \in J \implies ax \in f^{-1}(J)$$

□

Exemple 2.4.32. Considérons la composition $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{Q}[t]$. En utilisant Proposition 2.2.3, on obtient $\iota : \mathbb{Z}[t] \hookrightarrow \mathbb{Q}[t]$ qui envoie un polynôme avec coefficients dans $\mathbb{Z}$ au même polynôme mais considéré comme un polynôme avec coefficients dans $\mathbb{Q}$. On peut obtenir beaucoup d'idéaux de $\mathbb{Z}[t]$ de la forme $\iota^{-1}J$, en utilisant le Lemme 2.4.31.

Par exemple, soit $J = \left(1 + \frac{1}{2}t\right)$. On a

$$\iota^{-1}J = \left\{ \left(\sum_{i=0}^{m} a_i t^i\right)\left(1 + \frac{1}{2}t\right) \in \mathbb{Z}[t] \;\middle|\; a_i \in \mathbb{Q} \right\} = \left\{ \frac{a_m}{2}t^{m+1} + a_0 t + \sum_{i=1}^{m} \left(a_i + a_{i-1}\frac{1}{2}\right) t^i \in \mathbb{Z}[t] \;\middle|\; a_i \in \mathbb{Q} \right\}$$

$$= \left\{ \frac{a_m}{2}t^{m+1} + a_0 t + \sum_{i=1}^{m} \left(a_i + a_{i-1}\frac{1}{2}\right) t^i \;\middle|\; a_i \in \mathbb{Z},\ 2|i \right\} = \left\{ f(t)\left(1 + \frac{1}{2}t\right) \in \mathbb{Q}[t] \;\middle|\; f(t) \in 2\mathbb{Z}[t] \right\} = (2+t)_{\mathbb{Z}[t]}$$

(la flèche ↑ sous le premier $=$ pointe vers le cadre ci-dessous)

on démontre par récurrence décroissante sur i que $2|a_i$:
(1) pour $i = m$ on a $\frac{a_m}{2} \in \mathbb{Z}$, et
(2) pour $i < m$ on que $a_{i+1} - a_i\frac{1}{2} \in \mathbb{Z}$, où on sait déjà que $a_{i+1} \in 2\mathbb{Z}$.

Remarque 2.4.33. En général, il n'est pas facile de calculer les générateurs de l'idéal $f^{-1}J$, parce que, comme le montre l'Exemple 2.4.32,les générateurs de $f^{-1}J$ peuvent changer par rapport aux ceux de J.

Lemme 2.4.34. *Si $f \colon A \to B$ est un homomorphisme d'anneau surjectif, l'image d'un idéal $I \subseteq A$ à gauche (resp. à droite) est un idéal à gauche (resp. à droite).*

Démonstration. On traite le cas à gauche uniquement.

(1) On sait par le cours de théorie de groupes que $f(I)$ est un sous groupe de $(B, +)$.

(2) Pour la stabilité par rapport à la multiplication par un élément $b \in A$ à gauche, notons que : puisque f est surjective, $\exists a \in A\colon f(a) = b$. Soit $y \in f(I)$. Alors $\exists x \in I\colon f(x) = y$. On obtient :

$$by = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I).$$

□

Remarque 2.4.35. Par définition, on a $f\big((a_1, \ldots, a_m)\big) = \big(f(a_1), \ldots, f(a_m)\big)$.

Exemple 2.4.36. Considérons l'homomorphisme quotient $\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$. De la même façon que dans l'Exemple 2.4.32 on obtient $\xi_p : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ qui envoie un polynôme aux coefficients dans $\mathbb{Z}$ au polynôme obtenu par réduction de tous les coefficients mod p.

Ainsi, beaucoup d'idéaux sont envoyés sur le même idéal. Par exemple, fixons $p = 2$. En utilisant la Remarque 2.4.35, on obtient que :

(1) $\xi_p\big((t+1)\big) = (t+1)$, et
(2) $\xi_p\big((3t+1)\big) = (t+1)$ (notons que $3t+1$ n'est pas un multiple de $t+1$ en $\mathbb{Z}[t]$, et vice-versa, alors $(t+1) \neq (3t+1)$).

Mais aussi que

(3) $\xi_p\big((t+1, 2)\big) = (t+1)$ est vrai ($(t+1, 2)$ n'est pas égal aux deux idéaux au-dessus, parce qu'il contient $2 \in \mathbb{Z}$).

Remarque 2.4.37. La surjectivité dans le Lemme 2.4.34 est indispensable. En effet, considérons par exemple $f : F[x_1] \hookrightarrow F[x_1, x_2]$ et $I = (x_1)$. Dans ce cas, $f(I)$ n'est pas un idéal parce qu'il contient x_1 mais il ne contient pas x_1x_2.

2.4.5 Théorèmes de correspondance

Nous ne traiterons pas explicitement le cas des idéaux à droite dans cette section, semblable en tout point à ce que nous présentons ici pour les idéaux à gauche.

Le théorème de correspondance pour les groupes se généralise aux anneaux de la façon suivante :

Proposition 2.4.38. THÉORÈME DE CORRESPONDANCE. *Soit I un idéal bilatère d'un anneau A, et soit $\xi : A \to {}^{A}\!/_{I}$ l'homomorphisme quotient. Dans ce cas, les applications suivantes donne une bijection :*

$$\begin{array}{ccc} \left\{ J \subseteq A \;\middle|\; J \text{ est un idéal à gauche de } A,\ I \subseteq J \right\} & \longleftrightarrow & \left\{ J' \subseteq {}^{A}\!/_{I} \;\middle|\; J' \text{ est un idéal à gauche de } {}^{A}\!/_{I} \right\} \\ \cup & & \cup \\ J & \longmapsto & \xi(J) \\ \xi^{-1}(J') & \longmapsfrom & J' \end{array}$$

Démonstration. On connait la proposition pour les sous-groupes de $(A, +)$ est de $\big({}^{A}\!/_{I}, +\big) = {}^{(A,+)}\!/_{(I,+)}$. Il suffit de noter que les applications données envoient les idéaux sur des idéaux, ce qui est montré dans le Lemme 2.4.34 et le Lemme 2.4.31. □

Exemple 2.4.39. Les idéaux de ${}^{\mathbb{Z}}\!/_{12\mathbb{Z}}$ correspondent aux idéaux de $\mathbb{Z}$ contenant (12). Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ (Exemple 2.4.6). Pour un tel idéal, on a $12 \in (n) \iff n|12$. Ainsi, à la liste des diviseurs de 12, on attribue les idéaux de $\mathbb{Z}/(12)$, qui sont $([0]), ([1]), ([2]), ([3]), ([4]), ([6])$.

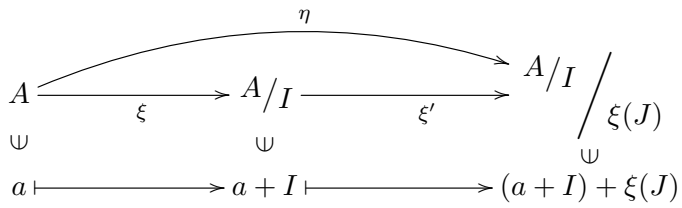
Exemple 2.4.40. Considérons l'homomorphisme $\xi_p\colon \mathbb{Z}[t] \to \mathbb{F}_p[t]$ construit dans l'Exemple 2.4.36. La Proposition 2.4.38 nous donne une correspondance bijective :

$$\begin{array}{ccc} \left\{ (p, f) \subseteq \mathbb{Z}[t] \;\middle|\; f = \sum_{i=0}^{m} a_i t^i,\ a_i \in \mathbb{Z} \right\} & \longleftrightarrow & \left\{ (g) \subseteq \mathbb{F}_p[t] \;\middle|\; g = \sum_{i=0}^{m} b_i t^i,\ b_i \in \mathbb{F}_p \right\} \\ \cup & & \cup \\ a_i & \longmapsto & b_i = a_i + p\mathbb{Z} \end{array}$$

Proposition 2.4.41. QUOTIENT EN DEUX TEMPS. *Soient $I \subseteq J$ deux idéaux bilatères d'un anneau A, et soit $\xi\colon A \to {}^{A}\!/_{I}$ l'homomorphisme quotient. Alors on a un isomorphisme*

$$A/J \cong \left.{}^{A}\!/_{I}\right/_{\xi(J)}$$

Démonstration. Considérons la composition d'homomorphismes quotients par I et par $\xi(J)$:



Notons que

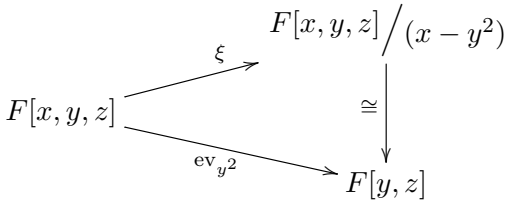
$$a \in \ker\eta \iff (a+I)+\xi(J) = \xi(J) \iff (a+I) \in \xi(J) \iff a \in J$$

On a obtenu que $\ker\eta = J$. En utilisant le Corollaire 2.4.17 pour η on obtient que

$$A/J \cong \left.{}^{A}\!/_{I}\right/_{\ker\eta} \cong \left.{}^{A}\!/_{I}\right/_{\xi(J)}$$

□

Exemple 2.4.42. Soit F un corps. Essayons de comprendre $\left.F[x,y,z]\right/(x-y^2, y^3+z^4)$. On a vu dans l'Exemple 2.4.10 que $(x-y^2) = \ker \mathrm{ev}_{y^2}$, où $\mathrm{ev}_{y^2}\colon k[x,y,z] = \big(k[y,z]\big)[x] \to k[y,z]$ est l'homomorphisme d'évaluation de la Proposition 2.2.3. Par conséquent, par la Proposition 2.4.16, on a l'identification suivante avec un isomorphisme vertical unique :



Ainsi, on peut identifier ξ avec ev_{y^2} et on peut utiliser la Proposition 2.4.41 pour $A = F[x,y,z]$, $I = (x-y^2)$ et $J = (x-y^2, y^3+z^4)$ pour obtenir :

$$\underbrace{\left.F[x,y,z]\right/(x-y^2,y^3+z^4)}_{\uparrow\ = \boxed{A/J}} \cong \underbrace{\left.\left.F[x,y,z]\right/(x-y^2)\right/\left(\mathrm{ev}_{y^2}\left(y^3+z^4\right)\right)}_{\uparrow\ = \boxed{\left.A/I\right/\xi(J)}} \cong \left.F[y,z]\right/(y^3+z^4)$$

$\uparrow$ $\left.F[x,y,z]\right/(x-y^2) \cong F[y,z]$ en utilisant Corollaire 2.4.17 pour ev_{y^2}

La représentation $\left.F[y,z]\right/(y^3+z^4)$ est la forme la plus optimale que l'on puisse trouver pour A. C'est un anneau qui ne peut pas être écrit comme un quotient d'un anneau polynôme d'une variable. Cela peut être démontré en utilisant plus de théorie d'algèbre commutatif et de géométrie algébrique.

Exemple 2.4.43. Considérons les anneaux

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a, b, d \in \mathbb{Z} \right\} \quad , \quad B = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in \mathbb{Z} \right\}$$

et les idéaux suivants de A (on laisse comme exercice la vérification que ce sont en effet des idéaux) :

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \;\middle|\; b \in \mathbb{Z} \right\} \quad , \quad J = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in 2\mathbb{Z},\ b \in \mathbb{Z} \right\}$$

Notons que $I \subseteq J$. On cherche à étudier A/J. Pour cela, on considère l'application naturelle $\xi \colon A \to B$ (qui envoie la coordonnée b sur 0). On a $\ker \xi = I$, et par le Corollaire 2.4.17, on obtient que $B \cong A/I$. Alors, pour comprendre A/J, il suffit de comprendre $\xi(J)$, en utilisant la Proposition 2.4.41. En effet, on a $\xi(J) = 2B$. Ainsi, on obtient que

$$A/J \cong B/2B \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in \mathbb{Z}/2\mathbb{Z} \right\}$$

en utilisant Corollaire 2.4.17 et que $2B = \ker\left(\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in \mathbb{Z} \right\} \to \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in \mathbb{Z}/2\mathbb{Z} \right\} \right)$

2.4.6 Produit d'anneaux

Définition 2.4.44. Soient A et B deux anneaux. L'*anneau produit* $A \times B$ est l'anneau sur l'ensemble $A \times B$ donné par les opérations suivantes, où $a, a' \in A$ et $b, b' \in B$:

(1) $(a, b) + (a', b') = (a + a', b + b')$,
(2) $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$, et
(3) l'unité de $A \times B$ est $(1, 1) \in A \times B$.

On laisse comme devoir de vérifier que $A \times B$ est en effet un anneau, et que les projections $\mathrm{pr}_A \colon A \times B \to A$ et $\mathrm{pr}_B \colon A \times B \to B$ sont des homomorphismes d'anneau.

Remarque 2.4.45. C'est important de remarquer que, dans le contexte de la Définition 2.4.44, $I = A \times \{0\} \subseteq A \times B$ et $J = \{0\} \times \subseteq A \times B$ ne sont pas des sous-anneaux, parce que l'unité $(1, 1)$ de $A \times B$ n'est contenue ni dans I, ni dans J. C'est une grande différence par rapport à la théorie des groupes.

Cependant, *I et J sont des idéaux bilatéraux*. De plus, si l'on regarde I et J comme objets individuels, ce sont bien des anneaux. En somme :

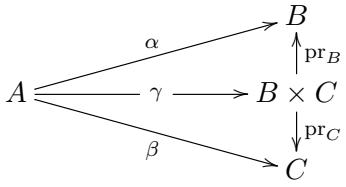
	sous-anneaux	idéaux bilatères	anneaux
I et J sont	×	✓	✓

Proposition 2.4.46. PROPRIÉTÉ UNIVERSELLE DES PRODUITS. *Soient A, B, C des anneaux. Étant donné des homomorphismes d'anneaux $\alpha : A \to B$ et $\beta : A \to C$, il existe un unique homomorphisme d'anneau $\gamma : A \to B \times C$ tel que $\mathrm{pr}_B \circ \gamma = \alpha$ et $\mathrm{pr}_C \circ \gamma = \beta$.*

On note aussi que γ est donné par la formule

$$\gamma(a) = \big(\alpha(a), \beta(a)\big) \tag{2.4.e}$$

et la situation peut être visualisée dans le diagramme commutatif suivant :



Démonstration. Le seul option de définir γ est avec la formule (2.4.e). On laisse la vérification que γ est un homomorphisme d'anneau comme devoir.

□

La fin du 4. cours, le 09.03.2021.

2.4.7 Le théorème des restes chinois

Définition 2.4.47. Deux idéaux bilatéraux I et J d'un anneau A sont *premiers entre eux* si $I + J = A$.

Remarque 2.4.48. On remarque que I et J sont premiers entre eux si et seulement s'il existe $x \in I$ et $y \in J$ tels que $x + y = 1_A$.

Exemple 2.4.49. Sous les hypothèses de la Définition 2.4.47, soit :

(1) $A = \mathbb{Z}$: dans ce cas $I = (n)$ et $J = (m)$ par l'Exemple 2.4.6. En utilisant l'Exemple 2.4.30, on voit que I et J sont premiers entre eux si et seulement si $\operatorname{pgdc}(n, m) = 1$. C'est la motivation d'utiliser le nom "premier entre eux" dans la Définition 2.4.47.

(2) $A = \mathbb{R}[t]$, $I = (t + 1)$ et $J = (t - 1)$: dans ce cas I et J sont premiers entre eux en utilisant la Remarque 2.4.48 et que $\frac{1}{2}(t + 1) + \frac{1}{2}(t - 1) = 1$.

Théorème 2.4.50. THÉORÈME DES RESTES CHINOIS. *Si I et J sont deux idéaux bilatéraux premiers entre eux d'un anneau A, et si*

$$\alpha \colon A \to {}^{A}\!/_{I} \qquad \text{et} \qquad \beta \colon A \to {}^{A}\!/_{J}$$

sont les homomorphisme quotients, alors l'homomorphisme

$$\begin{array}{ccc} A & \xrightarrow{\quad\gamma\quad} & {}^{A}\!/_{I} \times {}^{A}\!/_{J} \\ \cup & & \cup \\ a & \longmapsto & (a + I, a + J) \end{array}$$

donné par la propriété universelle du produit (Proposition 2.4.46) induit un isomorphisme

$${}^{A}\!/_{I \cap J} \cong {}^{A}\!/_{I} \times {}^{A}\!/_{J}$$

en utilisant le Corollaire 2.4.17.

Démonstration. Considérons γ définit dans la proposition. Pour un $a \in A$, on a

$$\gamma(a) = 0 \iff a + I = 0 + I, \text{ et } a + J = 0 + J \iff a \in I, \text{ et } a \in J \iff a \in I \cap J$$

Autrement dit, $\ker \gamma = I \cap J$, et alors il suffit de démontrer que γ et surjectif.

Pour cela, prenons $(a + I, b + J) \in {}^{A}\!/_{I} \times {}^{A}\!/_{J}$. Soit $x, y \in A$ les éléments donnés par la Remarque 2.4.48. Autrement dit, on a $x + y = 1$, $x \in I$ et $y \in J$. On postule que $\gamma(ay + bx) = (a + I, b + J)$. Pour ceci, il faut démontrer que $ay + bx - a \in I$ et $ay + bx - b \in J$. Ces deux propositions sont symétriques, ainsi il suffit seulement de démontrer la première :

$$ay + bx - a = a(y - 1) + bx \underset{\uparrow}{=} -ax + bx = (b - a)x \underset{\uparrow}{\in} I$$

$x + y = 1$; $x \in I$, et I et un idéal bilatére

□

Lemme 2.4.51. *Soient I et J deux idéaux premiers entre eux d'un anneau* commutatif *A, alors $I \cdot J = I \cap J$.*

Démonstration. On a $I \cdot J \subseteq I \cap J$ pour A commutatif (Remarque 2.4.28). Ainsi, il suffit de démontrer l'autre direction d'inclusion. Soit $z \in I \cap J$, et x et y les éléments donnés par Remarque 2.4.48. Cela signifie que $x \in I$, $y \in J$ et $x + y = 1$. Le calcul suivant nous montre que $I \cdot J = I \cap J$:

$$z = z \cdot 1 = z \cdot (x + y) = \underbrace{z}_{\in J}\underbrace{x}_{\in I} + \underbrace{y}_{\in J}\underbrace{z}_{\in I} \in IJ$$

□

Exemple 2.4.52. CONGRUENCES.

(1) On cherche à trouver $n \in \mathbb{N}$ tel que

$$n \equiv 2 \mod 7 \qquad \text{et} \qquad n \equiv 3 \mod 5$$

Pour cela, on remarque que $3 \cdot 5 - 2 \cdot 7 = 1$ et que, par le théorème du reste chinois (Théorème 2.4.50),

$$\mathbb{Z}/35\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

On cherche donc la pré-image de $([3], [2])$ par notre isomorphisme. Par la preuve du théorème des restes chinois (Théorème 2.4.50), cet élément est la classe à gauche d'entiers suivante en

$$3 \cdot (-2 \cdot 7) + 2(3 \cdot 5) = -6 \cdot 7 + 6 \cdot 5 = -12 \equiv 23 \mod 35$$

Une solution modulo 35 de notre équation est donc 23.

(2)

$$\mathbb{R}[t]\Big/(t^2 - 1) \cong \mathbb{R}[t]\Big/(t - 1) \times \mathbb{R}[t]\Big/(t + 1) \underset{\uparrow}{\cong} \mathbb{R} \times \mathbb{R}$$

point (1) de l'Exemple 2.4.10 et la Corollaire 2.4.17

Notre prochain objectif est de mieux comprendre quand est ce qu'un anneau est un produit. La notion essentielle pour ce faire est la notion d'idempotence.

Définition 2.4.53. Soient A, B des anneaux.

(1) Un élément $a \in A$ est *idempotent* si $a^2 = a$.
(2) Deux idempotents $a, b \in A$ sont *orthogonaux* si $ab = 0$ et $ba = 0$. (Notons que, si $a \in A$ est un idempotent, alors $b = 1 - a$ est aussi un idempotent orthogonal à a : $(1 - a)^2 = 1 - 2a + a^2 = 1 - a$ et $(1 - a)a = a - a^2 = 0 = a(1 - a)$.)
(3) Le *centre* de A
$$Z(A) = \left\{ a \in A \;\middle|\; \forall b \in A \colon ba = ab \right\}$$
(4) Un élément $a \in A$ est un *idempotent central* si a est idempotent et si $a \in Z(A)$. (Notons que $a = (1, 0)$ et $b = (0, 1) \in A \times B$ sont idempotents centraux orthogonaux tels que $a + b = 1$.)

Lemme 2.4.54. *Si $a \in A$ est un élément idempotent central dans un anneau, alors*

(1) aA est un anneau avec l'addition et la multiplication de A et avec l'élément a pour unité (mais ce n'est pas un sous-anneau de A !), et
(2) l'application $\phi : A \to aA$ donnée par $b \mapsto ab$ est un homomorphisme.

Démonstration. (1) On laisse la démonstration en exercice. La clé est que $a \cdot (ac) = a^2c = ac$, mais il faut vérifier aussi les autres points de la Définition 2.1.1.

(2) Soient $b, c \in A$. Alors la vérification que ϕ est un homomorphisme est donnée par les calculs suivants :

$$\phi(1) = c = 1_{aA},$$

$$\phi(b+c) = a(b+c) = ab + ac = \phi(b) + \phi(c),$$

$$\phi(bc) = abc \underset{\uparrow}{=} a^2bc \underset{\uparrow}{=} abac = \phi(b)\phi(c).$$

a est idempotent — $a \in Z(A)$

□

Proposition 2.4.55. *Si, $a, b \in C$ sont idempotents orthogonaux centraux non-zéros tels que $a + b = 1$, alors l'application suivante est un isomorphisme :*

$$\begin{array}{ccc} C & \xleftrightarrow{\cong} & Ca \times Cb \\ \cup & & \cup \\ c & \longmapsto & (ca, cb) \end{array}$$

Démonstration. Soit $I = Ca$ et $J = cB$. Notons que

- $I \cap J = \{0\}$: en fait si $ca = c'b$ pour éléments $c, c' \in C$, alors $ca \underset{\uparrow}{=} ca^2 = c'ba \underset{\uparrow}{=} c'0 = 0$.

  a est idempotent — a et b sont orthogonaux
- $I + J$ sont premiers entre eux parce que $a + b = 1$.

En utilisant le Théorème 2.4.50, on obtient l'isomorphisme

$$\begin{array}{ccc} C & \xleftrightarrow{\cong} & C/Cb \times C/Ca \\ \cup & & \cup \\ c & \longmapsto & (c + Cb, c + Ca) \end{array}$$

Ainsi, il suffit de démontrer que $C/Cb \cong Ca$ par l'application $c + Cb \mapsto ca$, et aussi la paire de cette proposition obtenu en échangeant a et b. Par symétrie, il suffit en fait uniquement de montrer le premier isomorphisme. Par le Corollaire 2.4.17, il suffit de démontrer que Cb est le noyau de $\phi : C \to Ca$ donné par $\phi(c) = ca$, qui est un homomorphisme par le Lemme 2.4.54. Il y a deux inclusions à montrer ici :

- Prenons $c \in \ker \phi$, qui signifie que $ca = 0$. Alors, $c \in Cb$, parce que $c = c(b+a) = cb+ca = cb$.
- Pour $cb \in Cb$ on a $cb \in \ker \phi$, parce que $(cb)a = c(ba) = 0$.

□

Remarque 2.4.56. La Proposition 2.4.55 peut être reformulée comme une proposition de forme "si et seulement si", en disant que C est un produit si et seulement s'il possède des idempotents de la forme de ceux de la proposition.

Exemple 2.4.57. Soit F un corps et G un groupe fini tel que $|G| > 1$ et pgdc $\big(|G|, \operatorname{car} F\big) = 1$. Alors

$$a = \frac{1}{|G|} \sum_{g \in G} g \ \in \ F[G]$$

est un idempotent :

$$\left(\frac{1}{|G|}\sum_{g\in G} g\right)\left(\frac{1}{|G|}\sum_{g\in G} g\right) = \left(\frac{1}{|G|}\sum_{h\in G} h\right)\left(\frac{1}{|G|}\sum_{f\in G} f\right) = \frac{1}{|G|^2}\sum_{h,f\in G} hf$$

$\uparrow$ renommer les variables

$$= \frac{1}{|G|^2}\sum_{g\in G}\left(\sum_{h,f\in G, hf=g} hf\right) = \frac{1}{|G|^2}\sum_{g\in G}\left(\sum_{h\in G} h(h^{-1}g)\right) = \frac{1}{|G|}\sum_{g\in G} g$$

$\uparrow$ repartitionner la sommme par rapport à la valeur de $g = hf$

Les éléments a et $b = 1 - a$ de $F[G]$ sont des idempotents de la forme décrite dans la Proposition 2.4.55. On obtient que $F[G] = F[G]a \oplus F[G]b$. En particulier, $F[G]$ contient les diviseurs des zéros.

En effet l'hypothèse $\operatorname{pgdc}\big(|G|, \operatorname{car} F\big) = 1$ ci-dessus est indispensable. Il y aura un exercice dans une des séries décrivant un exemple qui montre que $F[G]$ peut être indécomposable lorsque $\operatorname{car} F$ divise $|G|$.

Exemple 2.4.58. L'hypothèse que a et b soient centraux est nécessaire en Proposition 2.4.55. En fait dans $A = \operatorname{Mat}(2, \mathbb{C})$ les éléments

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

satisfont toutes les hypothèses sur a et b sauf qu'ils ne sont pas centraux. De ce fait ils ne donnent pas une décomposition en un produit parce que Aa n'est pas même un anneau. Pour démontrer cette affirmation, considérons le calcul :

$$\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} \tag{2.4.f}$$

$\uparrow$ $\in Aa$

L'équation (2.4.f) nous montre que la seule solution à

$$D\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

est $D = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Cependant $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ n'est pas une unité de Aa par le même calcul (2.4.f). Alors, on obtient que Aa ne possède pas d'unité.

2.5 Idéaux premiers, maximaux

Dans cette section tous les anneaux sont commutatifs.

2.5.1 Idéaux premiers

On aimerait étudier les cas où le quotient d'un anneau par un idéal est intègre (voire, est un corps).

Définition 2.5.1. Un idéal I d'un anneau commutatif est *premier* si I est un idéal propre (i.e $I \subsetneq A$) et si

$$ab \in I \implies a \in I \ \text{ ou } \ b \in I. \tag{2.5.a}$$

Proposition 2.5.2. *Soit I un idéal d'un anneau commutatif A. Alors*

$$A/I \text{ est intègre} \iff I \text{ est un idéal premier.}$$

Démonstration. C'est une conséquence directe de la définition d'anneau quotient. En utilisant que

$$ab \in I \iff ab + I = 0 + I \iff (a + I)(b + I) = 0 + I$$

on obtient que (2.5.a) est équivalent à dire que

$$(a + I)(b + I) = 0 + I \implies a + I = 0 + I \quad \text{ou} \quad b + I = 0 + I.$$

Cela veut dire que A/I ne contient pas de diviseurs de zéro. □

Exemple 2.5.3. Dans $\mathbb{Z}$, en utilisant que

$$a \in (n) \iff n|a$$

on obtient que $(n) \neq (0)$ est premier si et seulement si

$$n|ab \implies n|a \quad \text{ou } n|b$$

On obtient que (n) est premier si et seulement si n est premier.

2.5.2 Idéaux maximaux

Définition 2.5.4. Un idéal I d'un anneau commutatif A est *maximal* s'il est propre et s'il est maximal pour la relation d'inclusion, c'est-à-dire que les seuls idéaux qui contiennent I sont A et I lui-même.

Proposition 2.5.5. *Soit I un idéal d'un anneau commutatif A. Alors*

$$A/I \text{ est un corps} \iff I \text{ est maximal}$$

Démonstration. C'est une conséquence direct du théorème de correspondance (Proposition 2.4.38). □

Corollaire 2.5.6. *Si $I \subsetneq A$ est un idéal maximal d'un anneau commutatif A, alors I est premier.*

Démonstration. Il suit de la Proposition 2.5.5. □

Remarque 2.5.7. Premier n'implique pas maximal en général. Prenons par exemple l'idéal (t) dans $\mathbb{Z}[t]$. En utilisant le Corollaire 2.4.17 pour $\mathrm{ev}_0 : \mathbb{Z}[t] \to \mathbb{Z}$ on obtient que $\mathbb{Z}/(t) \cong \mathbb{Z}$, qui est un anneau intègre mais n'est pas un corps.

Exemple 2.5.8. On a vu dans la Remarque 2.5.7 que premier n'implique pas maximal en général. Cependant pour certains anneaux spécifiques cette implication peut tenir. Par exemple, dans l'Exemple 2.5.3 on a vu que les idéaux premiers non-nuls de $\mathbb{Z}$ sont de forme (p) pour un entier $p \in \mathbb{Z}$. Puisque $\mathbb{Z}/(p) = \mathbb{F}_p$ est un corps on obtient que ces idéaux sont aussi maximaux. Autrement dit, dans $\mathbb{Z}$, un idéal est maximal si et seulement s'il est premier et non-nul. Les tels anneaux sont les anneaux de Krull-dimension 1. D'étude de la notion de dimension de Krull est le sujet de la grande partie du cours qui suit celui-ci et qui s'appelle "Rings and modules".

En fait, la dimension de Krull de $\mathbb{Z}[t]$ est 2, c'est-à-dire l'exemple de la Remarque 2.5.7 est minimal pour la propriété qu'il contient des idéaux premiers non-zéro non-maximaux.

La fin du 5. cours, le 16.03.2021.

Proposition 2.5.9. *Si $f : A \to B$ est un homomorphisme d'anneaux commutatifs, et $J \subseteq B$ est un idéal premier, alors $f^{-1}(J)$ est un idéal premier de A.*

Démonstration. Premièrement on vérifie que $f^{-1}J \neq A$:

$$J \text{ est premier} \implies J \neq B \implies 1 \notin J \underset{\uparrow}{\implies} 1 \notin f^{-1}J \implies f^{-1}J \neq A$$

$f(1) = 1$ par la Définition 2.1.7

Deuxièmement on vérifie l'équation (2.5.a) pour J :

$$ab \in f^{-1}J \iff f(ab) \in J \underset{\uparrow}{\iff} f(a)f(b) \in J \underset{\uparrow}{\implies} f(a) \in J \quad \text{ou} \quad f(b) \in J \iff a \in J \quad \text{ou} \quad b \in J$$

f est un homomorphisme — J est premier

□

On se base sur l'*axiome du choix* sous la forme du *lemme de Zorn* pour prouver le résultat suivant :

Théorème 2.5.10. Théorème de Krull *Soit A un anneau commutatif et $I \subsetneq A$ un idéal propre de A. Alors il existe un idéal maximal m de A tel que $I \subseteq m$.*

En fait on démontre une proposition un peu plus générale que Théorème 2.5.10. C'est une forme qui implique Théorème 2.5.10, mais qu'on aura besoin aussi dans la Section 2.5.3.

Proposition 2.5.11. *Soit A un anneau commutatif, $I \subsetneq A$ un idéal propre de A et $a \in A$ un élément tel que pour tous entiers $i > 0$ on a $a^i \notin I$. Alors il existe un idéal m de A maximal pour les propriétés $I \subseteq m$ et $a \notin m$.*

Rappelons d'abord le Lemme de Zorn, qui utilise les définitions suivantes dans un ensemble partiellement ordonné $(\mathcal{X}, \preceq)$:

- une chaîne dans $\mathcal{X}$ est un sous-ensemble totalement ordonné,
- $x \in X$ est maximal si $x \preceq y \implies x = y$.

Lemme 2.5.12. Lemme de Zorn *Soit $(\mathcal{X}, \preceq)$ un ensemble partiellement ordonné. Si chaque chaîne de $\mathcal{X}$ admet un majorant, alors $\mathcal{X}$ admet un élément maximal.*

L'idée pour la suite sera d'utiliser comme ensemble $\mathcal{X}$ l'ensemble des idéaux propres de A contenant I, et de choisir la relation d'inclusion comme relation d'ordre partiel.

Démonstration de la Proposition 2.5.11. Soit

$$\mathcal{X} = \left\{ I \subseteq J \subseteq A \;\middle|\; J \text{ est un idéal de } A;\ \forall i > 0 \colon a^i \notin J \right\}$$

Remarquons que $I \in \mathcal{X}$ et donc que $\mathcal{X}$ est non vide. Cet ensemble, muni de la relation d'inclusion, est partiellement ordonné. Si on montre que $\mathcal{X}$ possède un élément maximal, alors on aura montré le théorème. Ainsi, il suffit de démontrer l'hypothèse du Lemme 2.5.12.

Pour cela, prenons une chaine $\emptyset \neq \mathcal{Y} \subseteq \mathcal{X}$ de $\mathcal{X}$. Il faut démontrer que $\mathcal{Y}$ possède un majorant en $\mathcal{X}$. Posons $K = \bigcup_{J \in \mathcal{Y}} J$. Il suffit de démontrer que $K \in \mathcal{X}$:

- Puisque $a^i \notin J$ pour chaque J dans la définition de K et pour chaque entier $i > 0$, on obtient que $a^i \notin K$.
- On démontre que K est un idéal.
  - Soit $x, y \in K$. Par la définition de K il existe $J_1, J_2 \in \mathcal{Y}$ tels que $x \in J_1$ et $y \in J_2$. Puisque $\mathcal{Y}$ est une chaîne, on peut supposer sans perte de généralité que $J_1 \subseteq J_2$ (sinon on échange les indices). L'ensemble J_2 étant un idéal, on a $x + y \in J_2 \subseteq K$.

- Soit $x \in K$ et $b \in A$. Par la définition de K il existe $J \in \mathcal{Y}$ tel que $x \in J$. Ainsi par la définition d'un idéal : $bx \in J \subseteq K$

□

Démonstration du Théorème 2.5.10. C'est le cas spécial $a = 1$ de la Proposition 2.5.11. □

Corollaire 2.5.13. *Tout anneau commutatif A contient un idéal maximal.*

Démonstration. Appliquer le théorème précédent à l'idéal nul $(0) \subseteq A$. □

2.5.3 Le nilradical

Pour un anneau commutatif A, on a une manière très efficace pour étudier A si il est aussi intègre : on peut plonger A dans son corps des fractions K. On peut se demander si cette méthode pourrait être adaptée à un anneau commutatif général. L'outil crucial qui nous permet de réaliser cette stratégie est le nilradical (dans ce cours on ne pourra pas parcourir toute la longueur de cette stratégie, on pourra la finir dans le cours "Rings and modules") :

Définition 2.5.14. Soit A un anneau commutatif. Un élément $x \in A$ est *nilpotent* s'il existe un entier $n > 0$ tel que $x^n = 0$. Le *nilradical* $\mathrm{nil}(A)$ de A est

$$\left\{ x \in A \;\middle|\; x \text{ est nilpotent} \right\}$$

Par Proposition 2.5.15, $\mathrm{nil}(A)$ est un idéal de A.

Proposition 2.5.15. *Si A est un anneau commutatif, alors* $\mathrm{nil}(A)$ *est un idéal de A.*

Matériel optionnel

Démonstration. Premièrement on démontre que $\mathrm{nil}(A)$ est stable pour l'addition. Soit $x, y \in \mathrm{nil}(A)$. Par la définition de $\mathrm{nil}(A)$ il existe $n, m \in \mathbb{N}$ tels que $x^m = y^n = 0$. Par la loi binomiale on obtient que

$$(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^i y^{n+m-1-i}$$

Par conséquent pour montrer la stabilité par rapport à l'addition, il suffit de démontrer que pour chaque entier $0 \leq i \leq n+m+1$ on a $x^i y^{n+m-1-i} = 0$. En fait c'est vrai parce que :

- si $i \geq m$ alors $x^i = 0$, et
- si $i < m$, alors $n + m - -1 - i \geq n$ et $y^{n+m-1-i} = 0$.

Deuxièmement on démontre que $\mathrm{nil}(A)$ est stable aussi pour la multiplication. Si $a \in A$ et $x \in \mathrm{nil}(A)$, alors on a $(ax)^m = a^m x^m = 0$ et donc $ax \in \mathrm{nil}(A)$. □

Remarque 2.5.16. On remarque que l'anneau ${}^{A}/_{\mathrm{nil}(A)}$ ne possède pas d'élément nilpotent. En fait, si $a + \mathrm{nil}(A) \in {}^{A}/_{\mathrm{nil}(A)}$ était nilpotent, ceci signifierait que pour un entier $n > 0$ on aurait

$$a^n + \mathrm{nil}(A) = 0 + \mathrm{nil}(A) \iff a^n \in \mathrm{nil}(A) \implies a \in \mathrm{nil}(A) \iff a + \mathrm{nil}(A) = 0 + \mathrm{nil}(A).$$

En effet on voit que $\mathrm{nil}(A)$ est le plus petit idéal de A tel que ${}^{A}/_{\mathrm{nil}(A)}$ ne possède pas d'élément nilpotent. On voit aussi que $\mathrm{nil}(A)$ est le plus grand idéal qui contient uniquement des éléments nilpotents.

Par conséquent une manière de démontrer qu'un idéal I de A est égal à $\mathrm{nil}(A)$ est de démontrer que tous les éléments de I sont nilpotents, et que A/I ne contient pas d'éléments nilpotents. Pour la première partie il suffit de démontrer que les générateurs de I sont nilpotents par la preuve de Proposition 2.5.15. Par exemple pour $A = F[x,y]$ et pour $I = (x^2, y^3)$,

$$\mathrm{nil}\left(A/I\right) = (x+I, y+I),$$

parce que les générateurs $x+I$ et $y+I$ sont nilpotents en A/I, et parce qu'en utilisant Proposition 2.4.41 on obtient que

$$A/I \Big/ (x+I, y+I) \cong F[x,y]/(x,y) \cong F$$

(la flèche $\cong$: en appliquant le Corollaire 2.4.17 à la composition des homomorphismes d'évaluation $\mathrm{ev}_0 \colon F[x,y] \to F[y]$ et $\mathrm{ev}_0 : F[y] \to F$; c'est expliqué dans un exercice de la série que le noyau de cette composition est exactement (x,y))

Théorème 2.5.17. *Le nilradical d'un anneau commutatif A est égal à l'intersection de tous les idéaux premiers de A :*

$$\mathrm{nil}(A) = \bigcap_{\substack{p \text{ idéal} \\ \text{premier} \\ \text{de } A}} p$$

Matériel optionnel

Démonstration. Pour l'inclusion de $\mathrm{nil}(A)$ dans tous les idéaux premiers, considérons $x \in \mathrm{nil}(A)$ et un idéal premier p de A. Par définition de $\mathrm{nil}(A)$ il existe un entier $i > 0$ tel que $x^i = 0 \in p$. Par (2.5.a) on obtient que $x \in p$.

On prouve l'autre inclusion par contraposée. Soit $a \in A$ non nilpotent. Par la Proposition 2.5.11 on peut trouver un idéal p de A qui est maximal pour les propriétés que $\mathrm{nil}\, A \subseteq p$ et $a \notin p$. Il suffit de démontrer que p est premier.

On argumente par contradiction. Supposons que i p n'est pas premier, ça veut dire par définition qu'il existe $b, c \in A \setminus p$ tels que $bc \in p$. Les idéaux $p + (b)$ et $p + (c)$ contiennent p, et par la maximalité de p il existe $k, l \in \mathbb{N}$ tels que $a^k \in p + (b)$ et $a^l \in p + (c)$. On obtient :

$$a^{k+l} \in \big(p+(b)\big)\cdot\big(p+(c)\big) = p\cdot p + p\cdot(c) + (b)\cdot p + (b)\cdot(c) \subseteq p + (b)\cdot(c) = p + (bc) = p$$

(les égalités et inclusions sont dans cet ordre)

- $=$: les opérations sur les idéaux sont distributives dans le sens que pour idéaux I, J et $K \subseteq A$ on a $(I+J)\cdot K = I\cdot K + J\cdot K$ et $K\cdot(I+J) = K\cdot I + K\cdot J$; cela découle de la définition de ces opérations, et on laisse la démonstration comme devoir
- $\subseteq$: pour deux idéaux I et J de A on a $I \cdot J \subseteq I$ par la définition d'idéal et du produit $I \cdot J$
- $=$: Remarque 2.4.29
- $=$: $bc \in p \implies (bc) \subseteq p$

C'est une contradiction avec la définition de p, et par conséquent p est en effet premier. □

Le nilradical est en fait un cas particulier du radical d'un idéal, le nilradical de $(0) \subseteq A$.

Définition 2.5.18. Soit A un anneau commutatif, et I un idéal. On définit le radical de l'idéal I, noté $\sqrt{I}$ l'ensemble

$$\sqrt{I} = \{\ x \in A \mid \exists n > 0\ :\ x^n \in I\ \}$$

On peut montrer toutes les propriétés basiques de $\sqrt{I}$ avec les propriétés correspondantes de ${}^{A}/_{I}$:

Proposition 2.5.19. *Soit A un anneau commutatif, I un idéal de A et $\xi : A \to {}^{A}/_{I}$ l'application quotient. On a*

(1) $\sqrt{I} = \xi^{-1}\big(\mathrm{nil}(A)\big)$

(2) $\sqrt{I} \subseteq A$ *est un idéal*

(3)

$$\sqrt{I} = \bigcap_{\substack{p \text{ est un idéal premier de } A \text{ tel que} \\ I \subseteq p}} p$$

Démonstration. (1) Pour $x \in A$ et pour un entier $n > 1$ on a

$$0 + I = (x+I)^n \iff 0 + I = x^n + I \iff x^n \in I$$

$\uparrow$

$(x+I)^n = x^n + I$ par la définition de la multiplication en ${}^{A}/_{I}$

On obtient que x est nilpotent si et seulement si $\xi(x) = x + I$ est nilpotent.

(2) C'est un conséquence directe du point (1).

(3) C'est un conséquence directe du point (1) et de la Proposition 2.5.9.

□

2.6 La fonction φ d'Euler et le théorème de Fermat (lisez comme devoir)

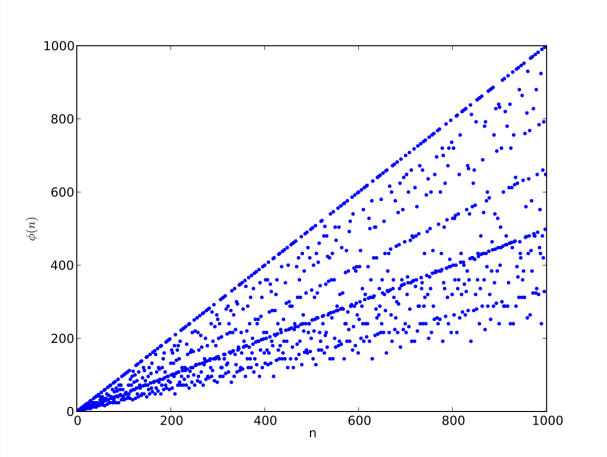
Nous connaissons bien l'anneau $\mathbb{Z}/n$, ses idéaux, ceux qui sont premiers, ceux qui sont maximaux. Nous savons aussi comment le Théorème chinois permet d'identifier l'anneau $\mathbb{Z}/mn$ lorsque m et n sont premiers entre eux. Nous allons encore étudier les éléments inversibles de $\mathbb{Z}/n$.

Définition 2.6.1. La *fonction φ d'Euler* est définie pour tout entier naturel $n \geq 1$ par $\varphi(n) = \mathrm{Card}\{1 \leq k \leq n \mid (k,n) = 1\}$.

Exemple 2.6.2. (a) Pour p un nombre premier on a $\varphi(p) = p - 1$.

(b) On a $\varphi(6) = 2$ car parmi $\{1,2,3,4,5,6\}$ seuls 1 et 5 sont premiers à 6.

Voici les 1000 premières valeurs de la fonction φ (source : Wikipédia).



La fonction d'Euler compte le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n$.

Proposition 2.6.3. *Pour tout $n \geq 1$ on a $\varphi(n) = \mathrm{Card}((\mathbb{Z}/n)^\times)$.*

Démonstration. Comme $\mathbb{Z}/n = \{\bar{1}, \ldots, \bar{n}\}$ nous allons montrer que $\bar{k}$ est inversible si et seulement si $(k, n) = 1$. Par Bézout $(k, n) = 1$ si et seulement s'il existe $a, b \in \mathbb{Z}$ tels que $ak + bn = 1$, autrement dit si et seulement s'il existe $a \in \mathbb{Z}$ tel que $ak - 1 \in (n)$. Cette dernière affirmation est équivalente à dire que $\bar{a} \cdot \bar{k} = \bar{1}$ dans $\mathbb{Z}/n$, i.e. $\bar{k}$ est inversible. □

Exemple 2.6.4. On calcule $\varphi(8) = 4$ car les éléments $\bar{0}, \bar{2}, \bar{4}$ et $\bar{6}$ sont pairs, donc diviseurs de zéro et non inversibles dans $\mathbb{Z}/8$, alors que $\bar{1}, \bar{3}, \bar{5}$ et $\bar{7}$ sont inversibles.

Lemme 2.6.5. *Soit p un nombre premier. Alors $\varphi(p^k) = p^{k-1}(p-1)$.*

Démonstration. Le cas $k = 1$ a été vu dans le premier exemple ci-dessus. En général l'argument utilisé pour calculer $\varphi(8)$ fonctionne pour évaluer $\varphi(p^k)$. En effet les multiples de $\bar{p}$ dans $\mathbb{Z}/p^k$ sont au nombre de p^{k-1}, il s'agit explicitement de $\bar{p}, 2\bar{p}, \ldots, (p^{k-1} - 1)\bar{p}, p^{k-1}\bar{p} = \overline{p^k} = \bar{0}$. Les autres éléments sont premiers à p et sont au nombre de $p^{k-1}(p-1)$. □

On poursuit l'étude de la fonction φ.

Proposition 2.6.6. *Si $(m, n) = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Démonstration. Nous avons établi que $\varphi(mn) = \#(\mathbb{Z}/mn)^\times$. Par le théorème chinois, on a $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$. Or les unités d'un anneau produit sont les produits des unités de chaque anneau : on en a donc $\varphi(m)\varphi(n)$. □

Théorème 2.6.7. *Si $n = p_1^{r_1} \ldots p_k^{r_k}$ avec $k \in \mathbb{N}^*, r_i \in \mathbb{N}^*, i \in [k]$ et les p_i distincts et premiers. Alors*

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)$$

Démonstration. Suit de la proposition précédente et du fait que

$$\varphi(p_i^{r_i}) = p_i^{r_i - 1}(p_i - 1).$$

□

Exemple 2.6.8. $288 = 2^5 \cdot 3^2$. $\varphi(288) = 2^4 \cdot (2-1) \cdot 3^1 \cdot (3-1) = 2^5 \cdot 3$.

Proposition 2.6.9. *Soit $(\mathcal{C}_n, \cdot)$ un groupe cyclique d'ordre n. Alors $\#\{g \in \mathcal{C}_n | \ < g >= \mathcal{C}_n\} = \varphi(n)$.*

Démonstration. Ce groupe est isomorphe à $(\mathbb{Z}/n, +)$. □

Théorème 2.6.10 (Théorème d'Euler)**.** *Si $(k, n) = 1$, alors $k^{\varphi(n)} \equiv 1[n]$*

Démonstration. Les unités de $\mathbb{Z}/n$ forment un groupe fini à $\varphi(n)$ éléments. Par le théorème de Lagrange (vu en théorie des groupes), on a que si $x \in (\mathbb{Z}/n)^\times$ alors $x^{\varphi(n)} \equiv 1[n]$. Or $k \in (\mathbb{Z}/n)^\times \iff (k, n) = 1$. □

Théorème 2.6.11 (Théorème de Fermat)**.** *Soit p un nombre premier. Alors*

(1) $k^{p-1} \equiv 1[p]$, si $p \not| \, k$

(2) $k^p \equiv k[p]$, $\forall k \in \mathbb{Z}$

Démonstration. Le premier point est une conséquence du théorème de Euler, car $\varphi(p) = p - 1$ et que $(k, p) = 1$, p étant premier et ne divisant pas k.
Le second point est une conséquence du premier, en le combinant avec le fait que si $p|k$ alors $k^p \equiv 0[p]$. Sinon on multiplie par k de chaque coté de la congruence. □

Chapitre 3

Arithmétique dans les anneaux

Dans cette chapitre tous anneau est commutatif, sauf dans la Section 3.6. Dans la plupart, tous anneau est même intègre sauf quelques endroits spécifiques :

- la Section 3.6,
- quelques propositions dans la première moitié de la Section 3.2 :
  - le Lemme 3.2.1,
  - le Proposition 3.2.3
  - la Proposition 3.2.4 et
- le Corollaire 3.3.5, à la fin de la Section 3.3.

3.1 Introduction

Le but principal de ce chapitre est de comprendre quand le théorème fondamental de l'arithmétique tient dans un anneau intègre A. En particulier :

- On introduit des notions des éléments *irréductibles* et *premiers* dans les anneaux dans la Section 3.4. On souvient du cours "Structures algébriques" que ces sont des notions cruciales pour la preuve du théorème fondamental de l'arithmétique dans $\mathbb{Z}$.
- Dans la Section 3.5, on définie précisément ce que veut dire que le théorème fondamental de l'arithmétique tient dans un anneau. Tels anneaux s'appellent des *anneaux factoriel*s.
- Dans le Théorème 3.7.1 de la Section 3.7, on démontre notre caractérisation des anneaux factoriels.
- Dans la Section 3.2, on introduit une classe d'anneau pour laquelle on démontrera plus tard dans le chapitre que les anneaux dans cette classe sont factoriels. Ces anneaux s'appellent les *anneaux euclidiens*. On utilise Théorème 3.7.1 pour conclure que en effet les anneaux euclidiens sont factoriels.
- Dans la Section 3.8, on démontre que si A est factoriel, alors $A[t]$ est aussi factoriel.
- On obtient la plupart des nos exemples des anneaux factoriels de la combinaison des 2 points précédents.

3.2 Anneaux euclidiens

Soit A un anneau commutatif. On rappelle que le degré du polynôme nul vaut $-\infty$, une convention qui permet d'écrire le résultat suivant en toute généralité, si on admet que $-\infty+n = -\infty$ pour tout entier naturel n.

Lemme 3.2.1. *Soit A un anneau commutatif. Si $f, g \in A[t]$, et*

(1) soit A est intègre,

(2) soit le coefficient dominant de f est inversible,

alors $\deg(fg) = \deg f + \deg g$.

Démonstration. La proposition est claire si f ou g est le polynôme nul. Sinon, on écrit $f(t) = a_n t^n + \cdots + a_1 t + a_0$, un polynôme de degré n et $g(t) = b_m t^m + \cdots + b_1 t + b_0$, un polynôme de degré m. Alors, le coefficient dominant de fg est $a_n b_m$ qui est non zéro par les arguments suivants dans les cas respectifs :

(1) si A est intègre, alors il ne contient pas des diviseurs de zéro,
(2) si a_n est inversible, alors $a_n b_m \neq 0$ parce que $a_n^{-1} a_n b_m = b_m \neq 0$.

Cela conclut la démonstration du lemme. □

Remarque 3.2.2. Si A n'est pas intègre, le degré du produit peut être moins que la somme des degrés des facteurs. En effet, dans $\left(\mathbb{Z}/6\mathbb{Z}\right)[t]$ on calcule par exemple

$$3 = 1 + 2 = \deg(3t) + \deg(2t^2 + 1) \neq \deg\left((3t)(2t^2 + 1)\right) = \deg(3t) = 1$$

Le Lemme 3.2.1 permet de conclure aussi que $A[t]$ est intègre, en restreignant notre attention sur le coefficient dominant d'un produit de polynômes non nuls.

Proposition 3.2.3. *Si A est un anneau commutatif, alors A est intègre si et seulement si $A[t]$ est intègre.*

Proposition 3.2.4. *Soient A un anneau commutatif, et $f, g \in A[t]$. On suppose que le coefficient dominant de g est inversible dans A. Alors il existe d'uniques $q, r \in A[t]$ avec $\deg(r) < \deg(g)$, tels que $f = qg + r$.*

Démonstration.

Unicité : Supposons d'abord que q et r existent. On démontre qu'ils sont uniques. Supposons que q, r, q' and r' soient des entiers non-négatifs tels que $\deg r, \deg r' < g$, $f = qg + r$ et $f = q'g + r'$. Alors,

$$qg + r = a'g + r' \implies \underbrace{r - r'}_{\uparrow} = \underbrace{g(q' - q)}_{\uparrow} \implies q - q' = 0 \implies r - r' = 0 \implies q = q' \text{ et } r = r'$$

$\deg r, \deg r' < \deg g \implies \deg r - r' < \deg g$

si $q' - q \neq 0$, alors $\deg g(q' - q) \geq \deg g$ en utilisant Lemme 3.2.1

Ceci démontre que b et r sont uniques, s'ils existent.

Existence : Pour conclure la preuve, il faut encore démontrer que q et r existent. On le démontre par induction sur $\deg f$.

Si $\deg f < \deg g$ on peut choisir $q = 0$ et $r = f$.

Il nous reste donc à démontrer le pas d'induction. Supposons démontrée l'existence si l'on remplace f par un quelconque polynôme de plus petit degré. Soit a_n et b_m les coefficients dominants de f et g respectivement. Notons que :

- $b_m \in A^\times$,
- $n \geq m$ (parce que on a fait déjà le cas $\deg f < \deg g$), et
- pour $h = f - \frac{a_n}{b_m} t^{n-m} g$ on a $\deg h < \deg f$.

En appliquant l'hypothèse d'induction à h on obtient que $h = q_0 g + r_0$ où $\deg r_0 < \deg g$. Si on met cette equation ensemble avec la définition de h on obtient que

$$f = \frac{a_n}{b_m} t^{n-m} g + h = \left(q_0 + \frac{a_n}{b_m} t^{n-m}\right) g + r_0.$$

Ceci conclut notre preuve.

□

Exemple 3.2.5. Dans $\mathbb{Z}[t]$ le quotient de la division de t^4-2 par t^2-1 est t^2+1 et le reste vaut -1. On peut effectuer la division en colonnes pour vérifier que $(t^2+1)(t^2-1)-1=t^4-2$.

On introduit une division euclidienne plus générale que celle déjà connue :

Définition 3.2.6. Un anneau intègre A est *euclidien* s'il existe une fonction euclidienne $\sigma : A \to \mathbb{N}\cup\{-\infty\}$ telle que

(1) $\sigma(a)\in\mathbb{N}$ pour chaque $a\neq 0$, et
(2) pour chaque $a\in A\setminus\{0\}$ et $b\in A$ il existe $q,r\in A$ tel que :

$$b=qa+r \qquad \text{et} \qquad \sigma(r)<\sigma(a) \tag{3.2.a}$$

Exemple 3.2.7.

(1) $\mathbb{Z}$ est euclidien, avec $\sigma=|\cdot|$
(2) En utilisant Proposition 3.2.4, on voit que pour chaque corps F l'anneau $F[t]$ est euclidien, où une fonction euclidean est donnée par deg: $F[t]\to\mathbb{N}\cup\{-\infty\}$.
(3) On postule que $\mathbb{Z}[i]$ est euclidien avec $\sigma=|\cdot|^2$. Il faut vérifier les deux propriétés dans Définition 3.2.6 :

Propriété (1) : Prenons $c+di\in\mathbb{Z}[i]\setminus\{0\}$. On a $|c+di|^2=c^2+d^2\in\mathbb{N}$.

Propriété (2) : Fixons $a\in\mathbb{Z}[i]\setminus\{0\}$ et $b\in\mathbb{Z}[i]$. Il faut trouver $r,q\in\mathbb{Z}[i]$ avec les propriété donné dans l'équation (3.2.a). Par division avec $a\neq 0$ c'est équivalent à démontrer que :

$$\exists r,q\in\mathbb{Z}[i] \text{ tel que } |r|<|a| \text{ , et } \frac{b}{a}=q+\frac{r}{a}.$$

$$\boxed{s=\tfrac{r}{a}\in \mathrm{Frac}\,(\mathbb{Z}[i])} \to \Updownarrow \leftarrow \boxed{r=a\left(\tfrac{b}{a}-q\right)=b-qa\in\mathbb{Z}[i]}$$

$$\exists q\in\mathbb{Z}[i], s\in\mathrm{Frac}\,(\mathbb{Z}[i]) \text{ tel que } |s|<1 \text{ , et } \frac{b}{a}=q+s.$$

$$\Updownarrow \leftarrow \boxed{s \text{ est déterminé uniquement par } q \text{ et par } \tfrac{b}{a}=q+s}$$

$$\exists q\in\mathbb{Z}[i] \text{ tel que } \left|\frac{b}{a}-q\right|<1 \tag{3.2.b}$$

S'il y a un $q\in\mathbb{Z}[i]$ qui satisfait (3.2.b), alors l'entier de Gauss avec les coordonnées les plus proches à $\frac{b}{a}$ la satisfait aussi. Alors, choisissons $q\in\mathbb{Z}[i]$ d'être cet entier de Gauss. Autrement dit avec ce choix on aura que

$$\left|\mathcal{R}e\left(\frac{b}{a}-q\right)\right|\leq\frac{1}{2} \qquad \text{et} \qquad \left|\mathcal{I}m\left(\frac{b}{a}-q\right)\right|\leq\frac{1}{2}$$

Ceci implique que

$$\left|\frac{b}{a}-q\right|\leq\sqrt{\frac{1}{2^2}+\frac{1}{2^2}}=\sqrt{\frac{1}{2}}$$

On obtient que le choix en-dessus de q satisfait (3.2.b), qui conclut la démonstration que $\mathbb{Z}[i]$ est euclidien.

(4) Pour un nombre premier p, l'anneau suivant est euclidien (cet anneau est noté par $\mathbb{Z}_{(p)}$) :

$$A=\left\{\ \frac{c}{d}\in\mathbb{Q}\ \middle|\ p\nmid d\ \right\}$$

Pour donner la fonction euclidienne notons qu'on peut écrire chaque $\frac{c}{d}\in A$ dans la forme de $\frac{p^j e}{f}=\frac{c}{d}$ où $p\nmid e,f$, et de plus j est le même pour chaque choix de e et f. Autrement

dit, on peut écrire chaque $a \in A \setminus \{0\}$ dans la forme $p^j u$ où $u \in A^\times$ et j est uniquement déterminé. En particulier, on peut définir $\sigma(a) = j$, qui est bien défini par l'unicité de j. On mets $\sigma(0) = -\infty$.

On démontre la propriété (2) de la Définition 3.2.6 : fixons $a, b \in A$ tel que $a \neq 0$. Pour $b = 0$ on peut choisir $q = r = 0$, alors on suppose aussi que $b \neq 0$. Cela veut dire que l'on peut écrire $a = p^{\sigma(a)}u$ et $b = p^{\sigma(b)}v$ où $u, v \in A^\times$. On a deux cas :

(i) Si $\sigma(a) > \sigma(b)$, on peut mettre $q = 0$ et $r = b$.

(ii) Si $\sigma(a) \leq \sigma(b)$, la décomposition est donné dans le calcul suivant

$$b = p^{\sigma(b)}v = \underbrace{\left(p^{\sigma(b)-\sigma(a)}\frac{v}{u}\right)}_{\boxed{=q}}\underbrace{\left(p^{\sigma(a)}u\right)}_{\boxed{=a}} + \underbrace{0}_{\boxed{=r}}.$$

Finalement on note que A est un exemple d'un anneau de valuation discrète, qui sont des anneaux particulièrement importants dans la théorie de nombre et dans la géométrie algébrique et dans la théorie des nombres algébrique. Vous pouvez apprendre plus sur ces anneaux dans les cours "Algebraic curves" et "Modern algebraic geometry".

En effet, tous les exemples d'anneaux euclidiens en-dessus sont liés aux valeurs absolues de $\mathbb{Q}$, sauf exemple (2). Dans les cas des points (1) et (3) on utilise la valeur absolue archimédienne sur $\mathbb{Q}$, qui est simplement la restriction de la valeur absolue habituelle sur $\mathbb{C}$. Cependant, dans le point (4) on utilise la valeur absolue p-adique de $\mathbb{Q}$. Celle-ci est donné par la valuation p-adique. Vous pourriez apprendre plus sur les valuations en prenant les cours du traque "Algebra and geometry".

On mentionne que ce n'est pas une coïncidence que l'on donne des exemples qu'en utilisant les valeurs absolues archimédienne et p-adiques. Il y a en effet un théorème célèbre de Ostrowski qui affirme que ces sont les seuls valeurs absolues modulo équivalence.

3.3 Anneaux principaux

Définition 3.3.1. Soit A un anneau intègre. On dit que A est *principal* si tout idéal de A est principal. Cela veut dire en utilisant la Définition 2.4.5 que tout idéal es engendré par un élément.

On remarque que le nom anglais de la notion de l'anneau principal est PID (principal ideal domain).

Exemple 3.3.2. (1) $\mathbb{Z}$ est principal par Exemple 2.4.6.

(2) N'importe quel corps K est principal, par Proposition 2.4.7.

(3) $\mathbb{Z}[t]$ est non principal, parce que si on regarde $\xi_p : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ défini dans l'Exemple 2.4.36, alors dans exercice 2 de la série 3 il était démontré que $\xi_p^{-1}(I)$ n'est pas principal pour un idéal propre, non-zéro I de $\mathbb{F}_p[t]$. On peut prendre $I = (t)$, est alors on obtient que (p, t) n'est pas principal.

Les anneaux principaux sont plus généraux que les anneaux euclidiens :

Proposition 3.3.3. *Si A est un anneau euclidien, alors A est principal.*

Démonstration. Soit I un idéal de A. Si $I = 0$, alors I est principal. Si $I \neq (0)$, en désignant σ une fonction euclidienne sur A, on choisit dans I un élément $x \neq 0$ tel que $\sigma(x)$ est minimal. On démontre que $(x) = I$.

$\boxed{(x) \subseteq I :}$ Puisque $x \in I$, l'idéal (x) engendré par x est contenu dans I.

$\boxed{I \subseteq (x) :}$ Choisissons $y \in I$. Alors on peut écrire $y = ax + b$ avec $\sigma(b) < \sigma(x)$. Par conséquent $y - ax = b \in I$. Par la minimalité de $\sigma(x)$ entre les éléments de $I \setminus \{0\}$ on obtient que $b = 0$. Autrement dit, on a $y = ax$ qui est équivalent à dire que $y \in (x)$. Ceci conclut là démonstration que $I \subseteq (x)$.

□

Exemple 3.3.4. Les anneaux de l'Exemple 3.2.7 sont principaux.

Matériel optionnel

Corollaire 3.3.5. *Soit A un anneau intègre. Alors*

$$A \text{ est un corps} \iff A[t] \text{ est principal.}$$

Démonstration. $\boxed{\Longrightarrow :}$ Conséquence du point (2) de l'Exemple 3.2.7.

$\boxed{\Longleftarrow :}$ Dans cette preuve, on parle de idéaux dans A et aussi dans $A[t]$ engendré par certains éléments. Pour éviter des confusions, on dénote dans sous-indice de quel on parle.

Soit $a \in A \setminus \{0\}$. I faut démontrer que a est inversible dans A. Considérons l'idéal $(t, a)_{A[t]}$. Par hypothèse cet idéal est principal : il existe $f \in A[t]$ tel que $(t, a)_{A[t]} = (f)_{A[t]}$. Puisque $a \in (f)_{A[t]}$, il existe un $h \in A[t]$ tel que $fh = a$. On en déduit que f est de degré 0 (i.e $f \in A$), en utilisant le Lemme 3.2.1. La même façon, $t \in (f)$, et il existe un $g \in A[t]$ tel que $fg = t$. Soit c le coefficient dominant de g. Puisque $f \in A$ et $fg = t$, on obtient que $cf = 1$. Autrement dit, $f \in A^\times$ et donc $(t, a)_{A[t]} = (f)_{A[t]} = A[t]$.

Considérons en ce point l'homomorphisme surjectif $\mathrm{ev}_0 : A[t] \to A$. En particulier, $\mathrm{ev}_0\left((t, a)_{A[t]}\right)$ est un idéal de A par Lemme 2.4.34, et

$$(a)_A \overset{\boxed{\text{Remarque 2.4.35}}}{=} \mathrm{ev}_0\left((t, a)_{A[t]}\right) \overset{\boxed{(t,a) = f}}{=} \mathrm{ev}_0\left((f)_{A[t]}\right) \overset{\boxed{\text{Remarque 2.4.35}}}{=} (f)_{A[t]} \overset{\boxed{f \in A^\times}}{=} A$$

On en déduit que $1 \in (a)_A$ et en particulier $a \in A^\times$. □

3.4 Éléments associés, premiers et irréductibles

Définition 3.4.1. Soit A un anneau intègre. Deux éléments $a, b \in A$ sont *associés* si il existe $u \in A^\times$ tel que $a = ub$.

Remarque 3.4.2. La relation "être associé" définit une relation d'équivalence entre les éléments de A. Nous noterons "$\sim$" cette relation pour la suite.

Lemme 3.4.3. *Soit A un anneau intègre. Alors*

$$a \sim b \iff (a) = (b)$$

Démonstration.

$\boxed{\Longrightarrow :}$ Par la Définition 3.4.1, il existe $u \in A^\times$ tel que $a = ub$. Alors le calcul suivant démontre cette direction :

$$(b) \supseteq (ub) = (a) \supseteq \left(u^{-1}a\right) = (b)$$

$\Longleftarrow$: si $(a) = (b)$ alors $\exists\, u \in A$ tel que $a = ub$, et $\exists\, v \in A$ tel que $b = va$. Alors $a = ub = uva$. On peut simplifier par a, parce que on travaille dans un anneau intègre. On en déduit que $u, v \in A^\times$. □

La fin du 6. cours, le 23.03.2021.

Définition 3.4.4. Soit A un anneau intègre, et $q \in A \setminus \{0\}$. On dit que :

(1) q est *irréductible* si $q \notin A^\times$, et si

$$\forall a, b \in A \ : \ q = ab \implies a \in A^\times \text{ ou } b \in A^\times.$$

(2) $s \in A$ et *divisible* par q s'il existe $t \in A$ tel que $qt = s$. Comme d'habitude on le dénote par $q|s$.

(3) q est *premier* si $q \notin A^\times$, et

$$\forall a, b \in A \ : \ q|ab \implies q|a \text{ ou } q|b.$$

Remarque 3.4.5. Par définition, $a|b$ si et seulement si $b \in (a)$ si et seulement si $(b) \subseteq (a)$. Attention, l'ordre de a et b est reversé pour la division en comparaison à l'inclusion des idéaux.

Remarque 3.4.6. Par définition, $q \in A \setminus \left\{A^\times \cup \{0\}\right\}$ est premier si et seulement si (q) est un idéal premier.

Exemple 3.4.7.

(1) Dans $\mathbb{Z}$, les éléments irréductibles et premiers sont les mêmes : les éléments de forme $\pm p$, où p est un nombre premier. On a démontré cette affirmation pendant le cours "Structures algébriques".

(2) Soit F un corps. On a vue dans Exemple 2.3.4 que pour un corps F on a $F[t]^\times = F \setminus \{0\}$. En particulier, pour chaque $f(t), g(t) \in F[t]$ on a $f(t) \sim g(t)$ si et seulement si $g(t) = cf(t)$ pour un $c \in F \setminus \{0\}$.

Par la Lemme 3.2.1, $t - d \in F[t]$ est irréductible pour chaque $d \in F$.

(3) On a appris dans Analyse III que si $f(t) \in \mathbb{C}[t]$, alors il existe un $d \in \mathbb{C}$ tel que $f(d) = 0$. Autrement dit $f(t) \in \ker \mathrm{ev}_d$. En utilisant Exemple 2.4.10, on obtient que $t - d|f(t)$. Par conséquence, on en déduit que

$$f(t) \in \mathbb{C}[t] \text{ est irréductible } \iff f(t) = at + b \text{ pour } b \in \mathbb{C} \text{ et } a \in \mathbb{C} \setminus \{0\}$$

(4) Soit F un corps et $f \in F[t]$ tel que $2 \leq \deg f \leq 3$. Si $f = gh$ est une factorisation de f dans $F[t]$ en facteurs non-inversible, alors par point (2) de cet exemple et par le Lemme 3.2.1 on voit que un de g ou de h doit être linéaire. Par symétrie on peut supposer que g est ce polynôme. Autrement dit $g \sim t - c$ pour un $c \in F$.

En somme, on a obtenu que f n'est pas irréductible, si et seulement si il existe un $c \in F$ tel que $t - c|f$. Par point (1) de l'Exemple 2.4.10 c'est équivalent à dire que $f(c) = 0$. Ainsi on a obtenu la condition simple suivante pour vérifier qu'un polynôme de degré au moins 2 et au plus 3 sur F est irréductible :

$$f \text{ est irréductible } \iff \forall c \in F\colon f(c) \neq 0$$

On donne des exemples spécifiques. Les polynômes suivants dans les anneaux suivants sont irréductibles :

(i) $t^2 + 1 \in \mathbb{R}[t]$: pour chaque $c \in \mathbb{R}\colon c^2 + 1 \geq 1 \implies c^2 + 1 \neq 0$.

(ii) $t^2 - 2 \in \mathbb{Q}[t]$: l'argument intuitive est que $\sqrt{2} \notin \mathbb{Q}$, et l'argument précise et que on suppose que $\frac{a}{b} \in \mathbb{Q}$ avec $\left(\frac{a}{b}\right)^2 - 2 = 0$, cela implique que $a^2 = 2b^2$ qui nous amène à une contradiction en comptant les multiplicités de 2 aux deux coté.

(iii) $t^3 - 2 \in \mathbb{Q}[t]$: l'argument est similaire au point précédent.

Attention : la méthode ne marche pas pour les polynômes de degré plus que 3. Par exemple $t^4 - 4$ n'a pas des zéros sur $\mathbb{Q}$ (la démonstration est similaire au cas de $t^2 - 2$), mais au même temps $t^4 - 4$ n'est pas irréductible sur $\mathbb{Q}$ parce que $t^4 - 4 = (t^2 - 2)(t^2 + 2)$.

(5) En utilisant Lemme 3.2.1, on obtient que pour un anneau intègre A et pour un élément $c \in A$, on peut écrire $c = ab$ pour $a, b \in A[t]$ si et seulement si a et b ont degré 0, ou autrement dire si et seulement is $a, b \in A$. On obtient que :

(i) $A[t]^\times = A^\times$,

(ii) $c \in A$ est irréductible si et seulement si c est irréductible dans $A[t]$.

Pour exemple particulier on obtient que pour chaque nombre premier p, l'élément $p \in \mathbb{Z}[t]$ est irréductible dans $\mathbb{Z}[t]$.

Cela nous donne aussi que une condition nécessaire pour un polynôme de $\mathbb{Z}[t]$ pour être irréductible est d'avoir le pgdc de ses coefficients égal à 1.

(6) Être irréductible peut changer quand on considère le même élément dans les anneaux différents. Par exemple, dans les points précédents on a vu que dans $\mathbb{R}[t]$ le polynôme $7 + 14t = 7(1 + 2t)$ est irréductible, mais il n'est pas irréductible dans $\mathbb{Z}[t]$.

(7) Soit $A = \mathbb{Z}_{(p)}$ l'anneau introduit dans point (4) de l'Exemple 3.2.7. Dans ce cas, on peut écrire un élément quelconque dans la forme $\frac{cp^j}{d}$ où $p \nmid c$, $p \nmid d$ et $j \in \mathbb{Z}$. Puisque $\frac{c}{d} \in A^\times$ et $p \notin A^\times$, on en déduit que p est le seule irréductible (modulo $\sim$).

Proposition 3.4.8. *Pour un nombre entier $d > 0$, l'anneau $A = \mathbb{Z}\left[\sqrt{-d}\right] = \mathbb{Z}\left[\sqrt{d}i\right] \subseteq \mathbb{C}$ possède les propriétés suivantes, où $x, y \in A$:*

(1) $A \cong \mathbb{Z}[t] \Big/ (t^2 + d)$

(2) $A = \left\{ \, a + b\sqrt{d}i \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z} \, \right\}$

(3) La norme $N : A \to \mathbb{N}$ donné par $N(x) = |x|^2$ satisfait $N(xy) = N(x)N(y)$. On a aussi la formule $N\left(a + b\sqrt{d}i\right) = a^2 + db^2$.

(4) Si $x|y$, alors $N(x)|N(y)$ (faites attention : la première division ici est dans A, et la deuxième est dans $\mathbb{Z}$).

(5) Si x est inversible (dans A), alors $N(x) = 1$. En particulier :

$$A^\times = \begin{cases} \{-1, 1, -i, i\} & \text{si } d = 1 \\ \{-1, 1\} & \text{si } d > 1 \end{cases}$$

(6) Pour un $x \in A$ si $N(x) \in \mathbb{Z}$ est irréductible (dans $\mathbb{Z}$), alors x est irréductible dans A.

Démonstration. Pour point (1), considérons l'homomorphisme d'évaluation $\mathrm{ev}_{\sqrt{-d}} : \mathbb{Z}[t] \to \mathbb{C}$. Verbatim la même preuve que dans l'Exemple 2.4.18 nous démontre que $\ker \mathrm{ev}_{\sqrt{-d}} = (t^2 - d)$. Après, on utilise le théorème d'isomorphisme (Corollaire 2.4.17).

Pour point (2), la preuve de l'Exemple 2.2.9 marche verbatim.

Les autres points découlent directement des points précédents et des définitions. □

Remarque 3.4.9. Les anneaux introduit dans la Proposition 3.4.8 s'appelle les anneaux d'entiers quadratiques quand $4 \nmid d + 1$ et d est un entier sans facteur carré. Si $4|d + 1$ et d est un entier sans facteur carré, alors il faut ajouter aussi $\frac{1+\sqrt{d}i}{2}$ à A pour obtenir l'anneau d'entiers quadratiques correspondants. Si d a un facteur carré, alors on peut écrire $d = ab^2$ tel que a est sans facteur carré. Dans ce cas $\mathbb{Z}\left[\sqrt{-d}\right] \subsetneq \mathbb{Z}\left[\sqrt{-a}\right]$ est on peut lié $\mathbb{Z}\left[\sqrt{-a}\right]$ aux anneaux d'entiers quadratiques en utilisant les premier 2 phrases de ce paragraphe.

Dans tous cas, les anneaux d'entiers quadratiques sont des anneaux fortement importants dans la théorie algébrique des nombres. Vous pouvez apprendre plus sur ce sujet dans le cours "Algebraic number theory", dans le traque "algebra and geometry".

Exemple 3.4.10. (1) 13 est irréductible dans $\mathbb{Z}$, mais pas dans $\mathbb{Z}[i]$. En effet dans $\mathbb{Z}[i]$ on a $13 = (2+3i)(2-3i)$, et on voit en utilisant la Proposition 3.4.8 que ni $2+3i$, ni $2-3i$ sont inversibles.

(2) $1+\sqrt{2}i$ est irréductible dans $\mathbb{Z}\left[\sqrt{-2}\right]$, parce que $N\left(1+\sqrt{2}i\right) = 3$ est premier dans $\mathbb{Z}$.

(3) Même si $N(x)$ n'est pas premier pour $x \in \mathbb{Z}\left[\sqrt{-d}\right]$ il peut arriver que x est irréductible. Par exemple, $x = 1+\sqrt{5}i \in A = \mathbb{Z}\left[\sqrt{-5}\right]$ est irréductible, même si $N(x) = 6$. On peut démontrer que x est irréductible en suivant les étapes prochaines :

- Par la Proposition 3.4.8 tous les diviseurs y de x doivent avoir $N(y) \leq N(x)$, et tous les diviseurs y non-inversieble et non-associés à x doivent avoir $1 < N(y) < N(x) = 6$ (pour ce dernier utilisons que seuls les éléments inversibles ont norme 1 dans cet anneau).
- En utilisant la formule $N\left(a+\sqrt{5}ib\right) = a^2+5b^2$ on trouve qu'il existe très peu d'éléments de norme strictement entre 1 et 6 : $2, -2, \sqrt{5}i, -\sqrt{5}i$. Le norme de ces éléments sont 2 et 5.
- Parce que $N\left(\sqrt{5}i\right) = 5 \nmid 6 = N(x)$ on obtient que seul 2 et -2 peuvent diviser x. Puisque ces deux éléments sont associés, il suffit démontrer que $2 \nmid x$ dans A.
- Supposons que $2|x$ dans A. Dans ce cas $\frac{x}{2} \in A$ est $N\left(\frac{x}{2}\right) = 3$. Mai il n'existe pas des éléments de norme 3 dans A.

On a vu beaucoup d'exemples des éléments irréductible en-dessus, mais aucune éléments premier dehors de cas de $\mathbb{Z}$. Une partie de la raison de cela est la proposition suivante :

Proposition 3.4.11. *Si A est un anneau intègre et $q \in A$ est premier, alors q est irréductible.*

Démonstration. Supposons que l'on puisse écrire $q = ab$ avec $a, b \in A$. Par primalité on a $q|a$ ou $q|b$. Par symétrie on peut supposer que $q|a$, ou autrement dit $a = qc$ pour un élément $c \in A$. Ainsi :

$$q = ab = qcb \underset{\uparrow}{\Longrightarrow} cb = 1 \Longrightarrow b \in A^\times$$

A est intègre

ce qui achève la preuve. □

L'inverse de la Proposition 3.4.11 n'est pas vrai :

Exemple 3.4.12. On a vue dans le point (3) de l'Exemple 3.4.10 que $x = 1+\sqrt{5}i \in A = \mathbb{Z}\left[\sqrt{5}i\right]$ est irréductible. Cependant, x n'est pas premier. En fait, $x|2\cdot 3$, parce que

$$\left(1+\sqrt{5}i\right)\left(1-\sqrt{5}i\right) = 2\cdot 3.$$

Au même temps, $2 \nmid (1+\sqrt{5}i)$ et $3 \nmid (1+\sqrt{5}i)$ par le point (3) de la Proposition 3.4.8 et le fait que $N(2) = 4$, $N(3) = 9$ et $N\left(1+\sqrt{5}i\right) = 6$.

En revanche, pour les anneau principaux, être premier et équivalent à être irréductible. En particulier, cela tient pour les anneaux euclidiens par Proposition 3.3.3, et par conséquence pour les anneaux de l'Exemple 3.2.7 :

Proposition 3.4.13. *Soit A un anneau principal et $q \in A \setminus \{0\}$. Alors les conditions suivantes sont équivalentes :*

(1) q est premier
(2) (q) est premier
(3) (q) est maximal
(4) q est irréductible

Démonstration. Premièrement, on note que si $q \in A^\times$, alors tous les quatre points sont faux. Par conséquent, on peut supposer que $q \notin A^\times$.

En utilisant la Remarque 3.4.6, la Proposition 3.4.11 et Corollaire 2.5.6, il suffit de démontrer l'implication (4) $\implies$ (3). Ainsi, on suppose que q et irréductible dans A, et on fixe un idéal $(q) \subseteq I \subsetneq A$. Il faut démontrer que $I = (q)$.

Puisque A est principal on peut écrire $I = (a)$ pour un $a \in A$. En particulier $q \in (a)$, et par conséquence on obtient une expression $q = ba$ for a $b \in A$. Parce que q est irréductible, soit a ou b est inversible. Puis que $(a) = I \neq A$, l'élément a ne peut pas être inversible. On obtient que b est inversible. Dans ce cas, l'équation $q = ba$ donne que $I = (a) = (q)$ qui est exactement ce qu'on voulait démontrer.

□

Remarque 3.4.14. Probablement le plus basiques anneau pur lequel on n'a pas discuté le lien entre être premier et irréductible est $\mathbb{Z}[t]$. On démontra dans Section 3.8 que en réalité ces deux notions sont les mêmes aussi dans $\mathbb{Z}[t]$.

3.5 ANNEAUX FACTORIELS

On introduit la définition d'un anneau factoriel. D'abord, soit A un anneau intègre et $a \in A \setminus \{0\}$. Supposons que l'on puisse écrire

$$a = u \prod_{i=1}^{r} p_i \tag{3.5.a}$$

où $u \in A^\times$, $r \in \mathbb{N}$ et les p_i sont irréductibles. Supposons désormais que $\forall i$ on a $p_i \sim q_i$ avec $p_i = v_i p_i$, et $v_i \in A^\times$. Alors

$$a = \left(u \prod_{i=1}^{r} v_i \right) \prod_{i=1}^{r} q_i$$

et remarquons que l'on a $u \prod_{i=1}^{r} v_i \in A^\times$.

Un anneau factoriel consiste en un anneau où chaque élément se décompose de façon unique "à association près" en produit d'un inversible et d'un produit de puissances d'irréductibles. Par exemple, dans $\mathbb{Z}$ les irréductibles sont les nombres premiers et leur inverses additifs. De plus on sait que dans $\mathbb{Z}$ chaque nombre se décompose de façon unique comme produit de puissances de nombres premiers (la convention veut que l'on prenne toujours les facteurs positifs). On pourrait changer le signe de quelques facteurs premiers et les remplacer par ses inverses additifs (i.e changer p en $-(-p)$, seuls associés de $\mathbb{Z}$), qui nous donnera aussi un décomposition de la forme (3.5.a). Ceci motive la définition suivante :

Définition 3.5.1. Soit A un anneau intègre, et $a \in A \setminus \{0\}$ quelconque.

(1) l'élément a admet une *décomposition en facteurs irréductibles* si il existe $u \in A^\times$, $r \in \mathbb{N}$ et éléments irréductibles p_i pour chaque $1 \leq i \leq r$ tel que $a = u \prod_{i=1}^{r} p_i$.

(2) si l'élément a admet une décomposition en facteurs irréductibles, alors on dit que *la décomposition est unique* quand la condition suivante est satisfait : pour chaque deux décompositions de a en facteurs irréductibles

$$u \prod_{i=1}^{r} p_i = a = v \prod_{i=1}^{r} q_i,$$

avec $u, v \in A^\times$, $r, s \in \mathbb{N}$ et les p_i, q_j irréductibles on a que

- $r = s$, et
- il existe une permutation $\sigma \in S_r$ tel que $p_i \sim q_{\sigma(i)}$.

(3) A est *factoriel* si pour chaque élément de $A \setminus \{0\}$ admet une décomposition en facteurs irréductibles unique (le nom anglais est UFD, l'abréviation de l'"unique factorization domain").

Exemple 3.5.2. L'anneau $A = \mathbb{Z}\left[\sqrt{5}i\right]$ n'est pas une anneau factoriel. En fait, on a vu déjà dans point (3) de l'Exemple 3.4.10, que $1 + \sqrt{5}i$ est irréductible dans A. Dans la même façon on peut démontrer que $1 - \sqrt{5}i$, 2 et 3 sont irréductibles. Au même temps on a l'égalité suivant dans A qui nous montre que 6 admet deux décompositions différentes en facteurs irréductibles :

$$6 = \left(1 + \sqrt{5}i\right)\left(1 - \sqrt{5}i\right) = 2 \cdot 3.$$

Donner des exemples des anneau factoriel est plus difficile d'habitude que donner des contre-exemples (comme en Exemple 3.5.2). Notre prochain but est d'arriver à une bonne caractérisation des anneaux factoriels, qui impliquera en particulier que les anneaux principaux sont factoriels.

Le premier pas est de trouver conditions intéressantes des anneaux factoriels. Plus précisément, on voudrait trouver des conditions, qui à la fin nous donne notre caractérisation désiré des anneaux factoriels :

~

Proposition 3.5.3. *Si A est un anneau factoriel, et $a \in A$ irréductible, alors a est premier.*

Démonstration. Supposons que $a|bc$ alors, a doit être un des facteurs irréductible de bc (modulo être associé), est alors il est un de facteurs irréductibles de soit b ou c. En particulier $a|b$ ou $a|c$. □

En fait la propriété de Proposition 3.5.3 implique au moins la partie d'unicité de la définition d'être factoriel :

Proposition 3.5.4. *Soit A un anneau intègre tel que tout élément irréductible de A est premier. Si $a \in A$ admet une décomposition en facteurs irréductibles, alors cette décomposition est unique.*

Démonstration. Supposons qu'il y a deux décompositions en facteurs irréductibles :

$$a = u\prod_{i=1}^{r} p_i = v\prod_{j=1}^{s} q_j \tag{3.5.b}$$

où les $p_i, q_j \in A$ sont irréductible (qui est équivalent à dire premier par notre supposition), et $u, v \in A^\times$. En échangeant si nécéssaire les p_i et les q_j, on peut supposer que $r \leq s$.

On démontre par induction sur s que les listes des p_i et des q_j est la même modulo leur ordre et modulo d'être associé. Si $s = 1$, alors $r = 1$, et il n'y a rien à démontrer.

Supposons que $s > 1$. Dans ce cas on a

$$q_1|a \iff q_1 \left| \prod_{i=1}^{r} p_i \right. .$$

Utilisant $r-1$ fois la contraposée de la définition d'être premier on obtient qu'il existe un indice l tel que $q_1|p_l$. Par notre supposition, p_l est irréductible. En utilisant que $q_1 \notin A^\times$, on obtient $q_1 \sim p_l$. Alors par (3.5.b) on obtient

$$A \ni \frac{a}{q_1} = \underbrace{u\frac{p_l}{q_1}}_{\in A^\times \text{ parce que } q_1 \sim p_l, \text{ et parce que } v \in A^\times} \prod_{1\leq i\leq r,\ i\neq l} p_i = v\prod_{j=2}^{s} q_j \tag{3.5.c}$$

En particulier $r > 2$, parce qu'autrement le premier produit dans (3.5.c) serait vide. Ça veut dire que l'on peut appliquer l'hypothèse d'induction pour les deux produits dans (3.5.c). Ceci conclut notre démonstration.

□

Remarque 3.5.5. Soit A un anneau factoriel. Grâce à la décomposition en facteurs irréductibles, il est possible de définir la notion de pgdc pour deux éléments non nuls a et b. En effet celui-ci correspond, lorsque l'on dispose d'une décomposition de a et b en produit d'irréductibles, au produit des éléments irréductibles communs dans leurs décompositions. En revanche, il y a un petit prix à payer pour avoir une définition qui marche dans telle généralité : le pgdc est bien-définie juste modulo être associé.

Nous pourrions ensuite définir la notion d'éléments premiers entre eux : a et b sont premiers entre eux si $\mathrm{pgdc}(a, b) \in A^\times$.

La fin du 7. cours, le 30.03.2021.

3.6 ANNEAUX NOETHÉRIENS

C'est la seule section de Chapitre 3 où les anneaux ne sont pas toujours supposé d'être commutatifs. Autrement dit, dans cette section on ne suppose rien des anneaux.

On a compris dans la Proposition 3.5.4 quand la décomposition en facteurs irréductibles est unique en supposant qu'elle existe. Notre but prochain est de comprendre l'existence d'une telle décomposition. Pour expliquer l'idée sous-jacente, prenons un élément $a \in A$ d'un anneau intègre qui admet une décomposition en facteurs irréductibles p_i. Dans ce cas on voit que modulo d'être associé il existe un nombre fini des diviseurs de a : tous les produits que l'on peut former des éléments p_i. En utilisant la langue d'idéaux c'est équivalent à dire que il existe un nombre fini des idéaux principaux qui contient (a). En particulier si $I_1 \subseteq I_2 \subseteq \dots$ est une chaîne croissante infinie des idéaux principaux de A, alors cette chaine stabilise après un indice adéquat. Autrement dit, il existe un entier $r > 0$ tel que pour tout entier $j \geq r$ on a $I_r = I_j$. Cette propriété sera exactement la propriété utilisée dans la caractérisation d'être factoriel dans le Théorème 3.7.1.

Si on remplace dans la condition en-dessus la notion d'idéal principal avec celle d'idéal arbitraire, on obtient une des notions plus centrales de la théorie d'anneaux :

Définition 3.6.1. Un anneau A est *noethérien à gauche* (resp. à droite) si toute chaîne d'idéaux à gauche (resp. à droite) croissante $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ stabilise, i.e. il existe $n \in \mathbb{N}$ tel que $I_m = I_n$ pour tout entier $m \geq n$.

L'anneau A est *noethérien* s'il est noethérien à gauche et à droite.

Remarque 3.6.2. Directement de la définition on obtient que si A est un anneau commutatif, alors A est noethérien à gauche si et seulement si il est noethérien à droite si et seulement si il est noethérien.

Exemple 3.6.3.

(1) On postule que si A est un anneau principal, alors A est noethérien. En particulier, en utilisant Proposition 3.3.3, tous nos exemples d'anneau euclidien de l'Exemple 3.2.7 sont noethérien.

Pour démontrer notre proposition, prenons un anneau principal A, et une chaine $I_1 \subseteq I_2 \subseteq \dots$ comme dans la Définition 3.6.1. Dénotons $J = \bigcup_j I_j$. Puis que A est principal, $J = (a)$ pour un élément $a \in A$. Choisissons un indice m tel que $a \in I_m$. Pour chaque entier $j \geq m$ on a

$$I_j \underset{\uparrow}{\supseteq} I_m \underset{\uparrow}{\supseteq} (a) = J \underset{\uparrow}{\supseteq} I_j. \tag{3.6.a}$$

on considère une chaine croissante | $a \in I_m$ | par la définition de J

Puis que l'idéal aux deux extrémités de (3.6.a) sont le même, on a égalité partout. On en déduit que $I_j = I_m$ pour chaque entier $j \geq m$

(2) Un cas particulier du point précédent nous donne que $F[t]$ est noethérien pour chaque corps F.

Si vous prenez le cours "Rings and modules", alors vous apprendrez que $F[t_1, \ldots, t_n]$ est noethérien aussi pour tout entier n. À l'autre coté, dans l'Exemple 3.8.17 on verra que l'idéal $(t_1, \ldots, t_n)$ n'est pas principal. Alors, anneaux non-principaux peuvent être aussi noethérien.

De plus, on démontrons dans l'Exemple 3.8.19 que l'anneau de polynômes à une infinité dénombrable d'indéterminées

$$F[t_1, t_2, t_3, \ldots] = \bigcup_n F[t_1, \ldots, t_n]$$

n'est pas noethérien.

(3) Soit A l'anneau suivant

$$A = \left\{ \; f : [0,1] \to \mathbb{R} \;\middle|\; f \text{ est continue} \; \right\}$$

avec les opérations habituelles des fonctions. Cet anneau n'est pas noethérien parce que les idéaux suivants forment une chaine croissante qui ne stabilise pas :

$$I_n = \left\{ \; f \in A \;\middle|\; f|_{[0,\frac{1}{2^n}]} \equiv 0 \; \right\}$$

En effet on a que $f_n \in I_n \setminus I_{n-1}$ où

$$f_n(x) = \begin{cases} 0 & \text{si } x \in \left[0, \frac{1}{2^n}\right] \\ x - \frac{1}{2^n} & \text{si } x \notin \left[0, \frac{1}{2^n}\right] \end{cases}$$

et on laisse en exercice de vérifier que les ensembles I_n sont vraiment des idéaux.

Le fait que A n'est pas noethérien est une des raisons pourquoi il y des limitations d'utiliser la théorie d'anneaux à comprendre les variétés topologique. En revanche si on remplace dans la définition de A la continuité avec être holomorphe, être une série formelle, où être un polynôme, alors on obtient des anneaux noethérien (Zsolt : je suis pas sûr si les cas holomorphe et formelle sont couvert par des courses ici à l'EPFL, le cas des polynômes était couvert dans le point (1) en-dessus). Cela correspond au fait que la théorie d'anneaux est utilisé largement pour étudier les variétés holomorphe et les variétés algébriques.

(4) On postule que l'anneau suivant n'est pas noethérien à gauche mais il est noethérien à droite

$$A = \left\{ \; \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a \in \mathbb{Z};\; b, d \in \mathbb{Q} \; \right\}$$

En réalité on démontre ici dans ce note seulement que A n'est pas noethérien à gauche. On laisse l'autre proposition pour une exercice de la série. Pour commencer la démonstration, notons la règle de la multiplication dans A :

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$$

Cela implique que les sous-ensembles suivants de A sont des idéaux à gauche (mais pas des idéaux à droite) :

$$I_n = \left\{ \; \begin{pmatrix} 0 & \frac{c}{2^n} \\ 0 & 0 \end{pmatrix} \;\middle|\; c \in \mathbb{Z} \; \right\}$$

Ainsi les idéaux I_n forme une chaîne croissante des idéaux à gauche qui ne stabilise pas, parce que

$$\begin{pmatrix} 0 & \frac{1}{2^n} \\ 0 & 0 \end{pmatrix} \in I_n \setminus I_{n-1}$$

Proposition 3.6.4. *Un anneau A est noethérien à gauche (resp. noethérien à droite) si et seulement si tout idéal à gauche (resp. idéal à droite) de A est engendré par un nombre fini d'éléments.*

Démonstration. On démontre seulement la version d'idéaux à gauche. Celle d'idéaux à droite est verbatim le même en échangeant chaque apparence de mot gauche à droite.

$\boxed{\Longleftarrow :}$ L'argument de cette direction est pratiquement le même que l'argument du point (1) de l'Exemple 3.6.3. Considérons une chaîne d'idéaux à gauche croissante $I_1 \subseteq I_2 \subseteq \dots$. On définit $J = \bigcup_j I_j$, ce qui est un idéal à gauche (comme dans la preuve de l'existence d'un idéal maximal, dans Proposition 2.5.11). Il existe donc des éléments $a_1, \dots, a_k \in A$ tels que $J = (a_1, \dots, a_k)$. Chaque élément a_i de J appartient donc à un idéal à gauche I_{j_i}, et si n est le plus grand des j_i on conclut que $I_n \subseteq J \subseteq I_n$. Ainsi $J = I_n$, la chaîne stabilise.

$\boxed{\Longrightarrow :}$ Considérons un idéal à gauche I qui n'est pas finiment engendré. On définit par récurrence une chaine croissante d'idéaux $(0) = I_0 \subsetneq I_1 \subsetneq \dots$ qui ne stabilise pas. Comme indiqué, on prend $I_0 = (0)$. Ainsi on peut supposer que $I_{j-1} \subsetneq I$ est défini, il est finiment engendré, et on définit I_j avec les mêmes propriétés aussi satisfaisant que $I_{j-1} \subsetneq I_j$:

- puisque $I_{j-1} \subsetneq I$ on peut choisir $a \in I \setminus I_{j-1}$, et
- on met $I_j := (a) + I_{j-1}$.

Ce choix est correct :

- $a \notin I_{j-1} \implies I_j \supsetneq I_{j-1}$,
- puis que I_{j-1} est finiment engendré, I_j est aussi finiment engendré (on ajoute a aux générateurs de I_{j-1} pour obtenir un ensemble des générateurs de I_j), et
- $I_j \subsetneq I$ parce que I n'est pas finiment engendré.

□

Voici encore une conséquence directe de la Proposition 3.6.4 et du théorème de correspondance pour les idéaux (Proposition 2.4.38).

Corollaire 3.6.5. *Si A est noethérien à gauche (resp. noethérien à droite) et I est un idéal bilatère de A, alors le quotient A/I est aussi noethérien à gauche (resp. noethérien à droite).*

Exemple 3.6.6. L'anneau $\mathbb{Q}\left[\sqrt{-5}\right]$ est un quotient de l'anneau principal $\mathbb{Q}[t]$, en utilisant l'homomorphisme $\mathrm{ev}_{\sqrt{-5}} : \mathbb{Q}[t] \to \mathbb{C}$. Ainsi $\mathbb{Q}\left[\sqrt{-5}\right]$ est donc noethérien par Corollaire 3.6.5.

3.7 Caractérisation d'être factoriel

Théorème 3.7.1. *Un anneau intègre A est factoriel si et seulement si les conditions suivantes sont satisfaites :*

(1) tout élément irréductible de A est premier,
(2) toute chaine croissante $(a_1) \subsetneq (a_2) \subsetneq \dots$ d'idéaux principaux de A stabilise.

Démonstration.
$\boxed{\Longleftarrow :}$ Par la Proposition 3.5.4 la décomposition en facteurs irréductibles est unique, alors il faut juste démontrer que telle décomposition existe pour chaque $a \in A$. Supposons la contraire, et soit $S \subseteq A$ le sous-ensemble des éléments qui ne admet pas une décomposition en facteurs irréductibles. Par notre supposition (2), on peut choisir $a \in S$ tel que (a) est maximal entre tels éléments. Autrement dit, avec des formules :

$$\forall b \in S\colon (a) \subseteq (b) \implies (a) = (b). \tag{3.7.a}$$

En effet, on peut produire tel $a \in A$ en remplaçant un élément quelconque de S récursivement par un des éléments de S pour lequel l'idéal engendré est plus grand. Ce processus doit terminer par supposition (2).

Avoir choisit le a dans le paragraphe en-dessus, notons que a ne peut pas être irréductible ou inversible, parce que dans ce cas a lui-même donnerait une décomposition avec un ou zéro facteurs. Par conséquence, en utilisant la définition d'être irréductible (Définition 3.4.4) on peut écrire $a = bc$ tel que b et c ne sont pas inversible. Ainsi le Lemme 3.4.3 nous donne que $(b) \supsetneq (a)$ et que $(c) \supsetneq (a)$. Par l'équation (3.7.a), on obtient que b et c admettent des décomposition en facteurs irréductibles. En concaténant ces deux décompositions on obtient une décomposition aussi pour a, qui est une contradiction avec la supposition que $S \neq \emptyset$.

$\boxed{\Longrightarrow :}$ Supposons que A est factoriel. Condition (1) est démontré dans Proposition 3.5.3. Alors, il suffit de démontré condition (2). Considérons une chaine $(a_1) \subsetneq (a_2) \subsetneq \dots$ croissante d'idéaux principaux. Par Lemme 3.4.3 on en déduit que a_i sont tous des diviseurs de a_1 que ne sont pas associé à l'un aux autre. Cependant, dans un anneau factoriel chaque élément admet seulement un nombre fini des diviseurs modulo être associé : les produit formé des irréductibles dans un décomposition en facteurs irréductibles.

□

Corollaire 3.7.2. *Si A est un anneau principal (en particulier si A est euclidien, e.g., $A = F[t]$ pour un corps F), alors A est factoriel.*

Démonstration. C'est une conséquence directe de Proposition 3.4.13 et du point (1) de l'Exemple 3.6.3. □

Remarque 3.7.3. La preuve du Théorème 3.7.1 montre que chaque élément d'un anneau intègre et noethérien admet une décomposition en facteur d'irréductibles, quelle décomposition néanmoins n'est pas unique d'habitude.

3.8 Les lemmes et le théorème de Gauss

Le but de cette section est démontrer le théorème suivant.

Théorème 3.8.1. Théorème de transfert. *Si A est un anneau factoriel, alors $A[t]$ est factoriel.*

Théorème 3.8.1 est démontré par une comparaison subtile d'être irréductible dans $A[t]$ et dans $K(t)$ ou K est le corps des fractions de A. Il s'avéra que ces deux notions sont les même exactement pour les polynômes primitifs définis dans Définition 3.8.5. Pour cette définition on a besoin de la notion de plus grand commun diviseur :

3.8.1 Le plus grand diviseur commun

Définition 3.8.2. Soit A un anneau intègre, et $a_1, \dots, a_r \in A$ tel que un des a_i ne sont pas zéro. Un *plus grand diviseur commun* des a_i est un élément $d \in A$ pour lequel les propriétés suivantes sont satisfaites :

(1) $\forall 1 \leq i \leq r : d | a_i$, et
(2) pour chaque $c \in A \setminus \{0\}$, on a

$$\Big(\forall 1 \leq i \leq r \ : \ c | a_i\Big) \implies c | d$$

Par Lemme 3.8.3, si le plus grand diviseur existe, alors il est bien défini modulo être associé. Par conséquence on peut introduire la notation $\mathrm{pgdc}(a_1, \dots, a_r)$ pour le dénoter.

Lemme 3.8.3. *Si d et d' sont deux plus grand diviseurs communs des éléments $a_1, \dots, a_r$ d'un anneau intègre A, alors $d \sim d'$.*

Démonstration. Par la condition (2) de la Définition 3.8.2, on a que $d | d'$ et $d' | d$. Cela implique que $(d) = (d')$, qui conclut notre démonstration en utilisant Lemme 3.4.3. □

Remarque 3.8.4. L'existence du plus grand diviseur commun n'est pas garanti dans un anneau intègre quelconque. Par exemple, considérons $A = \mathbb{Z}[i\sqrt{5}]$, $a = 6$ et $b = 2\left(1 + i\sqrt{5}\right)$. On a $N(6) = 36$ et $N(b) = 24$. Par l'Exemple 3.5.2, $c = 2$ et $c' = \left(1 + i\sqrt{5}\right)$ divisent à la fois a et b. De plus $N(c) = 4$ et $N(c') = 6$.

Supposons que $d = \text{pgdc}(a, b) \in A$ existe. En utilisant point (4) de la Proposition 3.4.8 on obtient que $4|N(d)$, $6|N(d)$, $N(d)|24$ et $N(d)|36$. Forcément on a $N(d) = 12$. Cependant, on ne peut pas écrire $12 = x^2 + 5y^2$ où $x, y \in \mathbb{N}$ (la démonstration est simplement un analyse des possibilités : il faut que $y = 0$ où $y = 1$, et $12 - 5y^2$ n'est pas un carré dans tous les deux cas). En particulier, il n'existe pas un élément de norme 12 dans A qui est une contradiction. Ainsi, $\text{pgdc}(a, b)$ n'existe pas.

Néanmoins, si A est factoriel et $a_1, \ldots, a_r \in A$ tel que un des a_i n'est pas zéro, alors le produit des facteurs irréductibles commun des a_i non-zéros nous donne un $\text{pgdc}(a_1, \ldots, a_r)$. En somme, si A est factoriel le plus grand diviseur commun existe.

De plus, si A est euclidien, l'algorithme d'Euclide permet de calculer le $\text{pgdc}(a, b)$.

3.8.2 Polynômes primitifs

Définition 3.8.5. Si A est un anneau factoriel, alors un polynôme $0 \neq f \in A[t]$ est *primitif* si le plus grand diviseur commun de ces coefficents est 1 (modulo être associé).

Remarque 3.8.6. Notons que une polynôme primitif est soit non-constant, soit constant pour un constant inversible dans A.

Remarque 3.8.7. Si $0 \neq f = \sum_{i=0}^{n} a_i t^i \in A[t]$ pour un anneau factoriel A, alors on peut écrire $f = c \cdot f_0$ où

- $c = \text{pgdc}(a_0, \ldots, a_n) \in A$, et
- $f_0 = \displaystyle\sum_{i=0}^{n} \frac{a_i}{c} t^i \in A[t]$.

En particulier, on obtient une décomposition $f = c \cdot f_0$ tel que f_0 est primitif.

De plus, telle décomposition est unique modulo une multiplication par un élément de $A^\times$: si $f = c \cdot f_0$ pour $c \in A$ et pour $f_0 \in A[t]$ primitif, alors c doit être forcément le plus grand diviseur commun des coefficients de f, et donc il est bien-défini modulo être associé.

Après ce point on utilisera beaucoup de fois quelque faits pour un anneau A intègre et un corps K, que l'on rappelle ici :

- $A[t]^\times = A^\times$ par le point (5) de l'Exemple 3.4.7,
- un élément de A est irréductible dans A si et seulement si il est irréductible dans $A[t]$ aussi par le point (5) de l'Exemple 3.4.7,
- Par l'Exemple 2.3.4 on a $K[t]^\times = K^\times$, ou autrement dit les inversibles dans $K[t]$ sont exactement les polynômes constants non-zéros.
- On note aussi que pour un polynôme $f \in A[t]$ on dit des fois que f est irréductible **sur** A. Cela signifie que f est irréductible **dans** $A[t]$. On utilisera dans ce texte le deuxième version, mais on peut parcourir dans la littérature la première version aussi, est donc c'est bon à savoir la sens de celle-là.

Remarque 3.8.8. Soit A un anneau factoriel. Par point (5) de l'Exemple 3.4.7, un élément irréductible de A est aussi irréductible dans $A[t]$. En particulier, si $f \in A[t]$ est irréductible et non-constant, alors f est nécessairement primitif.

La réciproque est fausse : dans $\mathbb{Z}[t]$, le polynôme $t^2 - 1$ est primitif. Cependant, il n'est pas irréductible, parce que $t^2 - 1 = (t - 1)(t + 1)$.

3.8.3 Le lemme de Gauss I

Lemme 3.8.9. Lemme de Gauss I. *Soit A un anneau factoriel. Si $f, g \in A[t]$ sont primitifs, alors $fg \in A[t]$ est primitif aussi.*

Démonstration. Soit p un élément irréductible dans A. On montre que p ne divise pas tous les coefficients du produit fg. Notons

$$f(t) = \sum_{i=0}^{m} a_i t^i \qquad \text{et} \qquad g = \sum_{i=0}^{n} b_i t^i.$$

Puisque f et g sont primitifs, p ne divise pas tous leur coefficients, et par conséquent les minimums suivants existent :

$$k = \min\left\{ 1 \leq i \leq m \;\middle|\; p \nmid a_i \right\} \qquad \text{et} \qquad l = \min\left\{ 1 \leq i \leq n \;\middle|\; p \nmid b_i \right\}.$$

Calculons le coefficient de degré $r = k + l$ dans fg. Ce coefficient n'est pas divisible par p par le calcul suivant :

$$\sum_{i=0}^{r} a_i b_{r-i} = \underbrace{a_k b_l}_{\uparrow} + \left(\sum_{i=0}^{k-1} a_i b_{r-i} \right)_{\uparrow} + \left(\sum_{j=0}^{l-1} a_{r-j} b_j \right)_{\uparrow}$$

$p \nmid a_k$ et $p \nmid a_l$; $p | a_i$ pour $i < k$; $p | b_j$ pour $j < l$

□

Lemme 3.8.10. *Soit A un anneau factoriel, K son corps des fraction, et $0 \neq f \in K[t]$ un polynôme sur K. Dans ce cas, il existe un polynôme primitif $f \in A[t]$ et un élément $d \in K$ tel que $f = d \cdot f_0$.*

Démonstration. En multipliant f par un élément adéquat b de A on obtient un polynôme $f' \in A[t]$. Autrement dit on peut écrire $f = \frac{f'}{b}$. En appliquant la Remarque 3.8.7 à f' on obtient $f' = cf_0$ pour $c \in A$ et $f_0 \in A[t]$ primitif. En somme, on a $f = \frac{f'}{b} = \frac{c}{b} f_0$. En introduisant $d = \frac{c}{b}$ on conclut la démonstration. □

3.8.4 Le lemme de Gauss II

Lemme 3.8.11. Lemme de Gauss II. *Soit A un anneau factoriel, K son corps des fractions, et $f, g \in A[t]$ des polynômes tel que g est primitif.*

Si $f = d \cdot g$ pour un $d \in K$, alors $d \in A$. De plus, si f est aussi primitif, alors $d \in A^\times$.

Démonstration. Écrivons $d = \frac{a}{b}$ où $a, b \in A$, et écrivons $f = c \cdot f_0$ dans la forme de la Remarque 3.8.7. Autrement dit, on a $c \in A$ et $f_0 \in A[t]$ est primitif. Si, f est déjà primitif, on prend $c = 1$.

L'égalité $f = dg$ nous donne $bcf_0 = ag$. En utilisant l'unicité de la Remarque 3.8.7 on obtient que $a = ubc$ pour un élément $u \in A^\times$. Les égalités suivantes des éléments de K conclut notre démonstration :

$$d = \frac{a}{b} = \underset{\uparrow}{uc} \in A$$

si f est primitif, alors $c = 1$, et alors $uc \in A^\times$

□

Exemple 3.8.12. On peut généraliser Exemple 2.4.32 en utilisant Lemme 3.8.11. Pour ce but, prenons un anneau factoriel A, son corps des fractions K, l'homomorphisme $\iota : A[t] \to K[t]$ (ce

qui est la généralisation de l'homomorphisme de Exemple 2.4.32), et un idéal $I = (f)$ principal de $K[t]$. Par le Lemme 3.8.10 on écrit $f = cf_0$ pour $c \in K$ et pour $f_0 \in A[t]$ primitif. On calcule

$$\iota^{-1}I = \left\{ gf \in A[t] \;\middle|\; g \in K[t] \right\} = \left\{ cdg_0f_0 \in A[t] \;\middle|\; d \in K, g_0 \in A[t] \text{ primitif} \right\}$$

$f = cf_0$, et dans une façon similaire par le Lemme 3.8.10 on écrit $g = dg_0$, où $d \in K$ et $g_0 \in A[t]$ est primitif

$$= \left\{ cdg_0f_0 \in A[t] \;\middle|\; d \in K, cd \in A, g_0 \in A[t] \text{ primitif} \right\}$$

Lemme 3.8.9 et Lemme 3.8.11

$$= \left\{ bg_0f_0 \in A[t] \;\middle|\; b \in A, g_0 \in A[t] \text{ primitif} \right\} = \underbrace{A[t] \cdot f_0}$$

$cd = b$ dans une direction, $d = \frac{b}{c}$ dans l'autre direction

Remarque 3.8.7

l'idéal engendré par f_0 dans $A[t]$

Pour un example particulier si $A = \mathbb{Z}$, $f = \frac{1}{2}t^2 - \frac{1}{3}t + \frac{1}{5} \in \mathbb{Q}[t]$, alors $\iota^{-1}\left(\frac{1}{2}t^2 - \frac{1}{3}t + \frac{1}{5}\right)$ est engendré par $15t^2 - 10t + 6$ dans $\mathbb{Z}[t]$.

Rappelons que un polynôme irréductible non-constant sur un anneau factoriel est toujours primitif (Remarque 3.8.8). On clarifie quand l'inverse implication est vrai :

3.8.5 Le lemme de Gauss III

Proposition 3.8.13. Lemme de Gauss III. *Soit A un anneau factoriel, K son corps des fractions. Alors, un polynôme primitif $0 \neq f \in A[t]$ est irréductible dans $A[t]$ si et seulement s'il est irréductible dans $K[t]$.*

Démonstration.

$\Longleftarrow$: On montre l'affirmation contraposée. Prenons un $0 \neq f$ non-irréductible dans $A[t]$. Alors on écrit $f = gh$ pour $g, h \in A[t]$ non-inversibles (dans $A[t]$).

On postule que ni g ni h n'est pas un polynôme constant. Par symétrie, il suffit de démontrer cela pour g. Supposons la contraire, que g est un polynôme constant non-inversible dans $A[t]$. Par (5) de l'Exemple 3.4.7 on connait que $A[t]^\times = A^\times$. Alors, g est aussi non-inversible dans A. Du coup, par l'égalité $f = gh$, tous les coefficients de f sont divisible par un élément non-invesible de A. C'est une contradiction avec le fait que f est primitif.

En somme, dans le paragraphe précédent, on a montré que ni g ni h n'est pas un polynôme constant. Cela implique que g et h ne sont pas inversible dans $K[t]$ (Exemple 2.3.4). Alors, l'égalité $f = gh$ nous donne que f n'est pas irréductible dans $K[t]$.

$\Longrightarrow$: Supposons $f \in A[t] \setminus \{0\}$ est primitif et irréductible, et que $f = gh$ pour $g, h \in K[t]$. Par le Lemme 3.8.10 on peut écrire $g = cg_0$ et $h = dh_0$ où $c, d \in K$ et $g_0, h_0 \in A[t]$ sont primitifs. On obtient les égalités suivantes dans $K[t]$:

$$f = gh = cg_0dh_0 = \underbrace{cd} \cdot \underbrace{g_0h_0}$$

$g_0, h_0 \in A[t]$ sont primitifs $\implies$ $g_0h_0 \in A[t]$ est primitif par Lemme 3.8.9

après que l'on connait que g_0h_0 est primitif, on a $cd \in A^\times$ par Lemme 3.8.11

Par l'irréducibilité de f dans $A[t]$ on obtient que $g_0 \in A[t]^\times$ ou $f_0 \in A[t]^\times$. Par point (5) de l'Exemple 3.4.7 cela implique g_0 ou h_0 est constant, qui à son tour implique que g ou h est constant aussi. Par l'Exemple 2.3.4 on en déduit qu g ou h sont inversibles dans $K[t]$. Cela conclut la démonstration que f est irréductible dans $K[t]$. □

Exemple 3.8.14. On démontre en utilisant Proposition 3.8.13 que $x^2+f \in F[x,y]$ est irréductible pour un corps F quelconque et pour chaque $f \in F[y]$ tel que $\deg f$ est impair. Par exemple on obtient que x^2+y^3 ou x^2+y^5 est irréductible dans $F[x,y]$. (On note que l'irréductibilité de tels polynômes est un fait crucial dans géométrie d'algébrique.)

Regardons $F[x,y]$ comme $(F[y])[x]$. Autrement dit, on travaille dans $A[x]$ pour $A = F[y]$. Notons que A est factoriel parce que c'est principal. Soit K le corps des fractions de A, qui est le corps des fonctions rationnelles $F(y)$ (point (3) de l'Exemple 2.3.18). Notons premièrement que $x^2+f \in F[x,y] = A[x]$ est primitif, parce que le coefficient de x^2 est $1 \in A$. De coup, par Proposition 3.8.13, x^2+f est irréductible si et seulement si il est irréductible dans $K(x)$. Par point (4) de l'Exemple 3.4.7 on voit que c'est équivalent à démontrer que x^2+f n'admet pas une racine dans K. Supposons la contraire, qui veut dire que il existe $\frac{g}{h} \in K = F(y)$ (où $g,h \in F[y]$) tel que

$$\left(\frac{g}{h}\right)^2 = f \iff \underbrace{h^2 f}_{\uparrow} = \underbrace{g^2}_{\uparrow}$$

$\deg f$ est impair $\implies \deg(h^2 f) = 2\deg h + \deg f$ est impair — $\deg(g^2) = 2\deg g$ est pair

C'est une contradiction. Alors, x^2+f n'admet pas une racine in K, et en particulier x^2+f est irréductible dans $F[x,y]$.

Finalement, on note que sans supposer que $\deg f$ est impair, l'irréductibilité de x^2+f n'est pas vrai. Par exemple, $x^2+y^2 \in \mathbb{C}[x,y]$ n'est pas irréductible, parce que $x^2+y^2 = (x+iy)(x-iy)$, où $x+iy$ et $x+iy$ ne sont pas inversibles parce que $\mathbb{C}[x,y]^\times = \mathbb{C}^\times$.

En se basant sur le fait que $K[t]$ est factoriel lorsque K est le corps des fractions d'un anneau factoriel A, on montre que $A[t]$ est également factoriel :

La fin du 8. cours, le 06.04.2021.

3.8.6 La preuve du théorème principal

Démonstration du Théorème 3.8.1 . On notera K le corps des fractions de A. On prend un élément $f \in A[t] \setminus \{0\}$ et on montre l'existence et l'unicité de la décomposition de f en facteurs irréductible.

Existence : Pour $f_i \in K[t]$ irréductibles adéquats et pour $g_i \in A[t]$ primitifs adéquats on peut écrire :

$$f \underset{\uparrow}{=} \prod_{i=1}^{n} f_i \underset{\uparrow}{=} \prod_{i=1}^{n} (d_i g_i) = \underbrace{\left(\prod_{i=1}^{n} d_i\right)}_{\uparrow} \underbrace{\prod_{i=1}^{n} g_i}_{\uparrow}$$

$K[t]$ est principal donc factoriel

$f_i = d_i g_i$ et la décomposition du Lemme 3.8.10, et alors $d_i \in K$ — $:= d \in K$ — $:= g$, qui est primitif par le Lemme 3.8.9

Puisque g_i est obtenu de f_i en multipliant avec un constant non-zéro, g_i est irréductible dans $K[t]$. De coup, en utilisant Proposition 3.8.13 et que g_i est primitif, on obtient que les g_i sont aussi irréductibles dans $A[t]$. Par Lemme 3.8.11 on obtient que $d \in A$. Soit, $d = \prod_{j=1}^{r} p_j$ une décomposition en facteurs irréductibles de d dans A. Compte tenu que les éléments de A sont irréductibles dans A si et seulement si ils sont irréductibles dans $A[t]$ (point (5) de l'Exemple 3.4.7), on obtient que les p_j sont irréductibles aussi dans $A[t]$. En somme l'expression suivante nous donne un décomposition de f en facteurs irréductibles :

$$f = \left(\prod_{j=1}^{r} p_j\right)\left(\prod_{=1}^{n} g_i\right).$$

Unicité : Considérons deux décomposition de f en facteurs irréductibles tel que on sépare les facteurs constants et non-constants

$$\underbrace{p_1 \dots p_r}_{\uparrow} \cdot \underbrace{f_1 \dots f_n}_{\uparrow} = f = \underbrace{q_1 \dots q_s}_{\uparrow} \cdot \underbrace{g_1 \dots g_m}_{\uparrow}$$

facteurs constants $\Longrightarrow$ le produit est dans A

facteurs non-constants $\Longrightarrow$ ils sont primitifs $\Longrightarrow$ le produit et aussi primitif par Lemme 3.8.9

facteurs constants $\Longrightarrow$ le produit est dans A

facteurs non-constants $\Longrightarrow$ ils sont primitifs $\Longrightarrow$ le produit et aussi primitif par Lemme 3.8.9

En utilisant l'unicité de la Remarque 3.8.7 on obtient que il existe un $u \in A^\times$ tel que

- $p_1 \dots p_r = uq_1 \dots q_s$
- $uf_1 \dots f_n = g_1 \dots g_m$.

On montre bijection entre les deux groupes des facteurs irréductibles un par un :

- Puis que les éléments de A sont irréductibles dans A si et seulement si ils sont irréductibles dans $A[t]$ (point (5) de l'Exemple 3.4.7), on obtient que $p_1 \dots p_r = uq_1 \dots q_s$ donne deux différents décompositions en facteurs irréductibles du même élément dans A. En utilisant que A est factoriel, on obtient que $r = s$ et qu'il existe un $\sigma \in S_r$ tel que p_i est associé à $q_{\sigma(i)}$ dans A pour chaque $1 \leq i \leq r$. Compte tenu $A[t]^\times = A^\times$, ils sont aussi associé dans $A[t]$.
- Puis que $K[t]$ est factoriel, de l'égalité $uf_1 \dots f_n = g_1 \dots g_m$ on obtient que $m = n$ et qu'il existe un $\tau \in S_n$ tel que f_i est associé à $g_{\tau(i)}$ pour chaque $1 \leq i \leq n$. Puis que $K[t]^\times = K^\times$, cela est équivalent à dire que $f_i = v_i g_{\tau(i)}$ pour un $v_i \in K^\times$. Compte tenu que tous les deux f_i et $g_{\tau(i)}$ sont primitifs dans $A[t]$, on obtient du Lemme 3.8.11 que $v_i \in A^\times$. Puis que $A[t]^\times = A^\times$, c'est équivalent à dire que $f_i \sim g_{\tau(i)}$ dans $A[t]$.

□

Corollaire 3.8.15. *Si A est un anneau factoriel, alors $A[x_1, .., x_n]$ est factoriel aussi.*

Démonstration. C'est un conséquence directe du Théorème 3.8.1 par récurrence sur n, en utilisant que $A[x_1, ..x_n] = \big(A[x_1..x_{n-1}]\big)[x_n]$. □

Exemple 3.8.16. Soit F un corps. Avoir démontré dans Corollaire 3.8.15 que $F[x_1, \dots, x_n]$ est factoriel, on peut commencer comprendre les irréductibles de $F[x_1, \dots, x_n]$. Par exemple, on démontre que $x_i \in F[x_1, \dots, x_n]$ est irréductible par induction sur n. Pour $n = 1$, c'est juste la proposition que dans un anneau des polynômes $F[x_1]$ sur un corps tous les polynômes linéaires sont irréductibles (point (2) de l'Exemple 3.4.7).

Pour le pas d'induction on peut supposer que $i \neq n$, parce que si non, on permute les variables. Du coup, on peut regarder $F[x_1, \dots, x_n]$ comme $F[x_1, \dots, x_{n-1}][x_n]$. Cela donne directement le pas d'induction, parce que par point (5) de l'Exemple 3.4.7 x_i est irréductible dans $F[x_1, \dots, x_n] = F[x_1, \dots, x_{n-1}][x_n]$ si et seulement si il est irréductible dans $F[x_1, \dots, x_{n-1}]$.

Exemple 3.8.17. On montre, en tant qu'une application de la Corollaire 3.8.15, que l'idéal $(x_1, \dots, x_n) \subseteq F[x_1, \dots, x_n]$ n'est pas principal si $n \geq 2$.

Supposons que $(x_1, \dots, x_n) = (f)$ pour un $f \in F[x_1, \dots, x_n]$. Dans ce cas on a f n'est pas inversible, et $f | x_i$ pour chaque $1 \leq i \leq n$. Puis que x_i sont irréductibles (Exemple 3.8.16) non-associés dans $F[x_1, \dots, x_n]$ et f n'est pas inversible, on obtient que f doit être associés à plusieurs irréductibles non-associés, qui est une contradiction.

Remarque 3.8.18. Par combinaison du Théorème 3.8.1 et du Théorème 3.7.1 on obtient que dans $F[x_1, \dots, x_n]$ tous les chaines croissantes des idéaux principaux stabilise. Cependant on ne sait pas la même proposition pour les chaines d'idéaux arbitraires. Autrement dit, on ne sais

pas si $F[x_1, \dots, x_n]$ est noethérien ou non. La réponse positive serait démontré dans le cours "Rings and modules".

Exemple 3.8.19. L'anneau $A = F[x_1, \dots] = \bigcup_n F[x_1, \dots, x_n]$ est factoriel main non-noethérien.

Le fait que A est factoriel découle des faits que $F[x_1, \dots, x_n]$ est factoriel, et que si $f \in F[x_1, \dots, x_n]$ est irréductible, alors il reste irréductible dans $F[x_1, \dots, x_i]$ pour chaque $i > n$ (point (5) de l'Exemple 3.4.7).

Pour démontrer que A n'est pas noethérien, on postule que la chaine donnée par les idéaux $I_n = (x_1, \dots, x_n)$ ne stabilise pas. La raison est que tout élément $f \in I_n$ est divisible par x_i pour quelque $1 \leq i \leq n$, mais à la même fois $x_{n+1} \in I_{n+1}$ ne satisfait pas cette condition de divisibilité.

3.9 Critères d'irréductibilité

Proposition 3.9.1. *Soit $A, B \neq 0$ deux anneaux intègres, $\phi : A \to B$ un homomorphisme d'anneau, $f \in A[t]$ un polynôme avec coefficient dominant inversible, et $\xi : A[t] \to B[t]$ l'homomorphism induit par ϕ (dans la manière de l'Exemple 2.4.32). Si $\xi(f)$ est irréductible, alors, f est aussi.*

Démonstration. Supposons que $f = gh$, avec $g = a_r t^r + \dots + a_1 t + a_0$ et $h = b_k t^k + \dots + b_1 t + b_0$. Le coefficient de degré $n = r + k$ de f est $a_r b_k$ qui est inversible par notre supposition. En particulier a_r et $b_k \in A^\times$ aussi. Cela implique que $a_r, b_k \notin \ker \phi$, et alors

$$\deg g = \deg \xi(g) \qquad \text{et} \qquad \deg h = \deg \xi(h). \tag{3.9.a}$$

Puis que ξ et on homomorphisme d'anneau on a $\xi(f) = \xi(g)\xi(h)$. En utilisant que $\xi(f)$ est irréductible, on obtient que $\xi(g)$ ou $\xi(h)$ est inversible dans $B[t]$. Par symétrie on peut supposer que c'est $\xi(g)$. Par point (5) de l'Exemple 3.4.7, on obtient que g doit être un élément inversible de B, et en particulier on a $\deg \xi(g) = 0$. Du coup, $\deg g = 0$ par l'équation (3.9.a). Compte tenu que le coefficient dominant de g est inversible dans A, on en déduit que $g \in A[t]^\times$ (en utilisant le point (5) de l'Exemple 3.4.7 encore une fois). Cela conclut la démonstration que f est irréductible. □

Exemple 3.9.2. On peut appliquer la Proposition 3.9.1 aux différentes choix de B, A et ϕ :

(1) Par exemple, si on prend $A = \mathbb{Z}$, $B = \mathbb{F}_2$ et $\phi : A \to B$ le homomorphisme quotient, alors on peut utiliser la Proposition 3.9.1 à démontrer que le polynôme $f = t^3 + 121t^2 + 42t + 17 \in \mathbb{Z}[t]$ est irréductible. Dans ce das $g = \xi(f)$ est simplement la réduction modulo 2 de f, qui est $g = \xi(f) = t^3 + t^2 + 1$. Notons que g est irréductible dans $\mathbb{F}_2[t]$ en utilisant point (4) de l'Exemple 3.4.7. En effet on peut utiliser celui-ci, parce que l'on a $\deg g = 3 \leq 3$ et $g([0]) = g([1]) = [1] \neq [0]$. En somme, on peut appliquer Proposition 3.9.1 dans cette situation, et on obtient que f est en effet irréductible dans $\mathbb{Z}[t]$.

Notons que pour appliquer Proposition 3.9.1, il faut que le coefficient dominant de f est inversible. Par exemple, le polynôme $2t^4 + 2t^3 + 3t^2 + t + 1 = (2t^2 + 1)(t^2 + t + 1)$ n'est pas irréductible dans $\mathbb{Z}[t]$, mais il l'est modulo 2 où il est $t^2 + t + 1$.

(2) Un autre exemple est d'appliquer Proposition 3.9.1 à la situation de $A = F[x_1, x_3]$, $B = F[x_1]$ et $\phi = \mathrm{ev}_0 : A \to B$, où F est un corps. Si on dénote t par x_2, alors ξ nous donne un homomorphisme $\xi : F[x_1, x_2, x_3] \to F[x_1, x_2]$ qui est aussi un homomorphisme de type ev_0. On connait de l'Exemple 3.8.14 que $x_1^3 + x_2^2 \in F[x_1, x_2]$ est irréductible, et il est aussi unitaire si il est regardé comme un polynôme en variable x_2. On obtient que si on ajoute des termes dans la variable x_3 à ce polynôme, alors on obtient un polynôme irréductible dans $F[x_1, x_2, x_3]$. Par exemple $x_1^3 + x_2^2 + x_3^2 \in F[x_1, x_2, x_3]$ est irréductible. (L'irréductibilité de ce polynôme est important dans la géométrie algébrique. C'est un exemple d'une des plus simples classes des singularités des surfaces.)

(3) Dans le manière similaire au point précédent on peut démontrer que chaque polynôme linéaire dans $F[x_1, \ldots, x_n|$ est irréductible.

(4) Soit $K \hookrightarrow L$ un plongement (homomorphisme d'anneau injectif) entre deux corps, qui on appellera dans Chapitre 4 une extension des corps. La Proposition 3.9.1 nous donne que si un $f \in K[x_1, \ldots, x_n]$ est irréductible dans le plus grand anneau $L[x_1, \ldots, x_n]$, alors c'est aussi irréductible dans $K[x_1, \ldots, x_n]$.

Par exemple dans le point (3) de l'Exemple 3.9.4 on démontre que $x^2 + y^2 + z^2 \in \mathbb{C}[x, y, z]$ est irréductible. Il suit que $x^2 + y^2 + z^2 \in \mathbb{Q}[x, y, z]$ est aussi irréductible.

Proposition 3.9.3. CRITÈRE D'EISENSTEIN. *Soit A un anneau factoriel, $p \in A$ un irréductible, et $f = \sum_{i=0}^{n} a_i t^i \in A[t]$ un polynôme primitif de degré n. Si*

(1) $p \nmid a_n$

(2) pour chaque $0 \leq i < n$ on a $p|a_i$, et

(3) $p^2 \nmid a_0$,

alors f est irréductible.

Démonstration. Prenons une décomposition $f = gh$, et utilisons la notation

$$g = \sum_{i=0}^{k} b_i t^i \qquad \text{et} \qquad h = \sum_{j=0}^{m} c_j t^j.$$

où $b_k \neq 0 \neq c_m$. De coup, on a $a_0 = b_0 \cdot c_0$. Par condition (2), on a $p|b_0$ ou $p|c_0$. Par symétrie on peut supposer que cela soit c_0. Par condition (3), on obtient que dans ce cas p ne divise pas b_0. De plus comme $a_n = b_k c_m$, par condition (1), on obtient que $p \nmid c_m$. Par conséquent le minimum suivant existe

$$r = \min \{\ j \in \mathbb{N} \mid p \nmid c_j\ \}.$$

Observons que

$$a_r = \underbrace{b_0 \cdot c_r}_{\uparrow} + \sum_{i=1}^{r} \underbrace{b_i \cdot c_{r-i}}_{\uparrow}$$

$$\boxed{p \nmid b_0, p \nmid c_r \implies p \nmid b_0 c_r} \qquad \boxed{1 \leq i \leq r \implies p|b_i \implies p|b_i c_{r-i}}$$

n'est pas divisible par p. Ainsi, par condition (2) on obtient que $r = n$. Par Lemme 3.2.1 cela nous dit que $\deg h = 0$. Puisque f est primitif, cela implique que $h \in A^\times$. □

Exemple 3.9.4.

(1) $f = 3x^4 + 15x^2 + 10 \in \mathbb{Z}[x]$ est irréductible parce que

- f est primitif,
- $5 \nmid 3$ dans $\mathbb{Z}$,
- $5 \mid 10, 15$ dans $\mathbb{Z}$, et
- $25 \nmid 10$ dans $\mathbb{Z}$.

(2) On déduite de la Proposition 3.9.3 que $f = t^{p-1} + \ldots + t + 1 \in \mathbb{Z}[t]$ est irréductible, où $p \in \mathbb{N}$ premier. Pour cela observons que $t^p - 1 = (t-1)f$. Considérons l'homomorphisme $\mathrm{ev}_{y+1} : \mathbb{Z}[t] \to \mathbb{Z}[y]$. C'est un isomorphism, parce que $\mathrm{ev}_{t-1} : \mathbb{Z}[y] \to \mathbb{Z}[t]$ donne l'inverse homomorphisme. Ainsi, puisque être irréductible est préservé par les automorphismes d'anneau, il suffit de démontrer que le polynôme $\mathrm{ev}_{y+1}(f)$ est irréductible. Notons

que

$$\sum_{i=1}^{p}\binom{p}{i}y^i = (y+1)^p - 1 = \mathrm{ev}_{y+1}(t^p-1) \underset{\uparrow}{=} \mathrm{ev}_{y+1}(t-1)\cdot\mathrm{ev}_{y+1}(f) = y\cdot\mathrm{ev}_{y+1}(f)$$

ev_{y+1} est un homomorphisme d'anneau

$$\implies \mathrm{ev}_{y+1}(f) = \sum_{i=0}^{p-1}\binom{p}{i+1}y^i = y^{p-1} + \left(\sum_{i=1}^{p-2}\underbrace{\frac{p!}{(i+1)!(p-i-1)!}}_{\uparrow}y^i\right) + p$$

$1 \le i \le p-2 \implies p \nmid (i+1)!$, et $p \nmid (p-i-1)! \implies p \Big| \frac{p!}{(i+1)!(p-i-1)!}$

On voit que les conditions de Proposition 3.9.3 sont satisfaites pour $\mathrm{ev}_{y+1}(f)$, et par conséquent $f \in \mathbb{Z}[t]$ est irréductible.

(3) On postule que $f = x^2+y^2+z^2 \in \mathbb{C}[x,y,z]$ est irréductible. Pour cela regardons $\mathbb{C}[x,y,z]$ comme $A[x]$ pour $A = \mathbb{C}[y,z]$. Si, a_i set le coefficient de $f \in A[x]$, alors $a_2 = 1$, $a_0 = y^2+z^2$, et tous les autres a_i sont zéro. Notons aussi que $y^2+z^2 = (y+iz)(y-iz)$, où $y+iz$ et $y-iz$ sont irréductibles dans A par le point (3) de l'Exemple 3.9.2. De coup, $y^2+z^2 = (y+iz)(y-iz)$ et la décomposition en facteurs irréductibles. De plus, $y+iz \not\sim y-iz$. Par conséquent on peut appliquer Proposition 3.9.3 avec $p = y+iz$ pour obtenir que $f \in A[x]$ est irréductible.

Matériel optionnel

3.10 APPLICATIONS

Le matériel du Chapitre 3 et utiliser dans les branches différentes de la mathématique :

- Il est primordial pour la théorie des corps en Chapitre 4, ce qui est notre but principal dans ce cours.
- Il est aussi primordial pour la géométrie algébriques, et pour l'algèbre commutative dont vous pouvez apprendre plus dans le track "algebra and geometry".
- Finalement, il est indispensable pour la théorie de nombres algébrique. On donne un petit goût de celui-ci ci-dessous. Par exemple on peut démontrer le théorème suivant :

Théorème 3.10.1 (Fermat, 1640)**.** THÉORÈME DE LA SOMME DES CARRÉS. *Soit $n \ge 1$ un entier. Il existe $a,b \in \mathbb{Z}$ tels que $a^2+b^2 = n$ si et seulement si les exposants des nombres premiers congrus à -1 modulo 4 dans la décomposition en facteurs premiers de n sont pairs.*

Le cadre de notre étude se fera dans l'anneau factoriel $\mathbb{Z}[i]$. Rapellons que la fonction euclidienne dans $\mathbb{Z}[i]$ est définie par $N(z) = |z|^2$, c.f., Exemple 3.2.7. Rapellons aussi Proposition 3.4.8 sur la connection entre irréducibilité de $N(z)$ (dans $\mathbb{Z}$) et de z (dans $\mathbb{Z}[i]$).

On commence par deux lemmes qui nous seront utiles par la suite.

Lemme 3.10.2. *Soit p un entier naturel premier. On a un isomorphisme*

$$\mathbb{Z}[i]\Big/(p) \cong \mathbb{F}_p[x]\Big/(x^2+1) \tag{3.10.a}$$

En particulier, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv -1 \mod 4$.

Démonstration. L'isomorphism de (3.10.a) tient parce que tous les deux cotés de (3.10.a) sont isomorphes à $\mathbb{Z}[x]\Big/(p, x^2+1)$ en utilisant le quotient en deux temps, c.f., Proposition 2.4.41. En effet, on a $\mathbb{Z}[x]\Big/(p) \cong \mathbb{F}_p[x]$ et $\mathbb{Z}[x]\Big/(x^2+1) \cong \mathbb{Z}[i]$, et donc le quotient en deux temps s'applique ici.

Puisque $\mathbb{F}_p[x]$ et $\mathbb{Z}[i]$ sont euclidiens (Exemple 3.2.7), ils sont factoriels (Proposition 3.3.3 et Corollaire 3.7.2). Alors, être irréductible est équivalent à être premier dans tous les deux anneaux $\mathbb{F}_p[x]$ et $\mathbb{Z}[i]$. En ajoutant l'isomorphism (3.10.a), on obtient :

$$
\begin{array}{l}
p \in \mathbb{Z}[i] \text{ est irréductible} \underset{\uparrow}{\iff} p \in \mathbb{Z}[i] \text{ est premier} \iff (p) \subseteq \mathbb{Z}[i] \text{ est premier} \\
\qquad\qquad \boxed{\text{Proposition 3.3.3 et Corollaire 3.7.2}} \\
\qquad \underset{\uparrow}{\iff} \mathbb{Z}[i]\Big/(p) \text{ est intègre} \underset{\uparrow}{\iff} \mathbb{F}_p[x]\Big/(x^2+1) \text{ est intègre} \\
\qquad\quad \boxed{\text{Proposition 2.5.2}} \qquad\qquad \boxed{\text{(3.10.a)}} \\
\qquad \underset{\uparrow}{\iff} (x^2+1) \subseteq \mathbb{F}_p[x] \text{ est irréductible} \iff x^2+1 \in \mathbb{F}_p[x] \text{ est premier} \\
\boxed{\text{Proposition 2.5.2}} \\
\qquad\qquad\qquad\qquad\qquad\qquad \underset{\uparrow}{\iff} x^2+1 \in \mathbb{F}_p[x] \text{ est irréductible} \\
\qquad\qquad\qquad\qquad\qquad\qquad \boxed{\text{Proposition 3.3.3 et Corollaire 3.7.2}}
\end{array}
$$

Donc, par Exemple 3.4.7.(4), $p \in \mathbb{Z}[i]$ est irréductible si et seulement si x^2+1 n'a pas des racines dans $\mathbb{F}_p$. Notons que une telle racine est automatiquement inversible dans $\mathbb{F}_p$. Alors, on obtient que $p \in \mathbb{Z}[i]$ n'est pas irréductible si et seulement si

$$\exists y \in \mathbb{F}_p^\times : y^2 = -1. \tag{3.10.b}$$

D'ici, la manière plus directe de conclure l'argument est d'utiliser Théorème 4.4.17, qui nous dit que la groupe multiplicatif $\mathbb{F}_p^\times$ est isomorphe au groupe additif $\mathbb{Z}\big/(p-1)\mathbb{Z}$. Cela ne fait pas un argument circulaire, parce que la Section 3.10 n'est pas utiliser dans les parties suivantes des notes. On a 3 cas :

- si $p = 2$, alors $-1 = 1 \in \mathbb{F}_2$, et par conséquent $y = 1$ satisfait (3.10.b). Alors, 2 n'est pas irréductibles dans $\mathbb{Z}[i]$.
- si $p \neq 2$, alors $-1 \neq 1 \in \mathbb{F}_p$, et le groupe multiplicatif de $\mathbb{F}_p^\times$ est cyclique d'ordre divisible par 2. Il suit, que $-1 \in \mathbb{F}_p^\times$ est le seul élément d'ordre 2. Autrement dit, c'est la puissance $\frac{p-1}{2}$-ième d'un générateur arbitraire du groupe multiplicatif $\mathbb{F}_p^\times$. De plus, on en déduit que $y \in \mathbb{F}_p^\times$ satisfait (3.10.b) si et seulement si le groupe multiplicatif $\mathbb{F}_p^\times$ contient un élément d'ordre 4. On a deux cas :
  - et $p \equiv 1 \mod 4$, alors le groupe multiplicatif de $\mathbb{F}_p^\times$ a l'ordre divisible par 4. Par conséquent dans ce cas p est non-irréductible dans $\mathbb{Z}[i]$.
  - si $p \equiv -1 \mod 4$, alors le groupe multiplicatif de $\mathbb{F}_p^\times$ a l'ordre divisible par 2 mais pas par 4. Par conséquent dans ce cas p est irréductible dans $\mathbb{Z}[i]$.

□

Dans le lemme suivant on utilise que la conjugaison $\mathbb{Z}[i] \ni z \mapsto \overline{z} \in \mathbb{Z}[i]$ et un automorphisme de $\mathbb{Z}[i]$, et par conséquent $z \in \mathbb{Z}[i]$ est irréductible si et seulement si $\overline{z} \in \mathbb{Z}[i]$ est irréductible.

Lemme 3.10.3. *Soit $q \in \mathbb{Z}[i]$ un élément premier. Il y a deux possibilités :*

(1) q est associé à un entier premier positif p tel que $p \equiv -1 \mod 4$ (on dit que c'est le cas non-scindé), ou

(2) $q = a + bi$, où $N(q) = a^2 + b^2$ est un entier premier, et de plus $N(q) \not\equiv -1 \mod 4$ (on dit que c'est le cas scindé).

Notons que dans le cas scindé $\overline{q}$ est aussi un premier dans $\mathbb{Z}[i]$.

Démonstration. Par Lemme 3.10.2, il suffit de démontrer que si $q \in \mathbb{Z}[i]$ est un irréductible non-associé à un entier (les inversibles sont $1, -1, i$ et -1), alors on est dans le deuxième cas. De toute façon, on a que $q\overline{q} = N(q) \in \mathbb{Z}$. Si $N(q)$ est irréductible dans $\mathbb{Z}$, alors il n'est pas irréductible dans $\mathbb{Z}[i]$ par l'équation $q\overline{q} = N(q)$. Par conséquent, dans ce cas forcément $N(q) \not\equiv -1$ en utilisant le Lemme 3.10.2.

Il nous reste de démontrer que $N(q) \in \mathbb{Z}$ est irréductible. Supposons la contraire : $N(q) = cd$ où $1 < c, d \in \mathbb{Z}$. La décomposition $N(q) = cd$ ne peut pas être la décomposition en facteurs irréductibles, parce que q est un facteur irréductible de q non-associé à un entier. Autrement dit, c où d devons avoir au moins 2 facteurs irréductibles, et par conséquent $N(q)$ a au moins 3 facteurs irréductibles dans $\mathbb{Z}[i]$. C'est une contradiction avec le fait que $N(q)$ a juste 2 facteurs irréductibles depuis l'équation $N(q) = q\overline{q}$.

□

Démonstration du Théorème 3.10.1. $\boxed{\Longrightarrow :}$ Si $n = a^2 + b^2$, alors $n = (a+bi)(a-bi)$ est une décomposition de n en facteurs dans $\mathbb{Z}[i]$. Soit

$$a + bi = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s \tag{3.10.c}$$

la décomposition de $a+bi$ en facteurs irréductibles dans $\mathbb{Z}[i]$, où les p_i sont non-scindé et les q_i sont scindé. Dans ce cas le produit suivant nous donne une décomposition de $a - bi$ en facteurs irréductibles :

$$a - bi = \overline{a + ib} = \overline{p}_1 \cdot \ldots \cdot \overline{p}_r \cdot \overline{q}_1 \cdot \ldots \cdot \overline{q}_s = p_1 \cdot \ldots \cdot p_r \cdot \overline{q}_1 \cdot \ldots \cdot \overline{q}_s. \tag{3.10.d}$$

En multipliant les décompositions des equations (3.10.c) et (3.10.d) on obtient :

$$n = (a+bi)(a-bi) = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s \cdot p_1 \cdot \ldots \cdot p_r \cdot \overline{q}_1 \cdot \ldots \cdot \overline{q}_s = \underbrace{p_1^2 \cdot \ldots \cdot p_r^2}_{\uparrow} \cdot \underbrace{(q_1\overline{q}_1) \cdot \ldots \cdot (q_s\overline{q}_s)}_{\uparrow}$$

p_i est un entier premier congrus à -1 modulo 4

$q_i\overline{q}_i = N(q_i)$ est un entier premier non-congrus à -1 modulo 4

Celui conclut la démonstration de cette direction.

$\boxed{\Longleftarrow :}$ Par notre supposition on peut écrire $n = m^2 l$, où la décomposition de m en irréductibles dans $\mathbb{Z}$ contient seulement premiers congrus à -1 modulo 4, et la décomposition de l dans $\mathbb{Z}$ contient seulement premiers non-congrus à -1 modulo 4. Disons cette décomposition de l est

$$l = r_1 \cdot \ldots \cdot r_t \tag{3.10.e}$$

Par Lemme 3.10.3, r_j n'est pas irréductible dans $\mathbb{Z}[i]$. Puisque $N(r_j) = r_j^2$, par Proposition 3.4.8, la factorisation de r_j en irréductibles contient deux irréductibles. Autrement dit, cette décomposition est de forme $r_j = x_j y_j$, où $N(x_j) = N(y_j) = r_j$. En particulier $x_j \notin \mathbb{Z}$. En utilisant Lemme 3.10.3 encore une fois, $x_j = a_j + b_j i$, où $a_j^2 + b_j^2 = N(x_j) = r_j$. En particulier, on a a $r_j = (a_j + b_j i)(a_j - b_j i)$. Puisque $N(a_j - b_j i) = a_j^2 + b_j^2 = r_j$, par Proposition 3.4.8, $a_j - b_j i$ est irréductible aussi. On obtient que

$$r_j = (a_j + b_j i)(a_j - b_j i) \tag{3.10.f}$$

est la décomposition en irréductibles de r_j. En appliquant (3.10.f) à (3.10.e) on obtient

$$l = \underbrace{(a_1 + b_1 i) \cdot \ldots \cdot (a_t + b_t i)}_{\uparrow} \cdot \underbrace{(a_1 - b_1 i) \cdot \ldots \cdot (a_t - b_t i)}_{\uparrow} = (c + di)(c - di) = c^2 + d^2$$

on définie cet entier de Gauss d'être $c + di$

$= \overline{c + di} = c - di$

De coup, $n = m^2(c^2 + d^2) = (mc)^2 + (md)^2$ est en effet une somme de carrés. □

La fin du 9. cours, le 13.04.2021.

Chapitre 4

Les corps

4.1 Algèbres sur un corps

Lorsqu'on travaille avec des anneaux qui contiennent un corps K fixé, tout devient K-linéaire : les anneaux, les idéaux, les anneaux engendrés, les quotients, les isomorphismes donnés par le théorème d'isomorphisme, etc. On traduit la phrase précédente dans un cadre précis en utilisant la notion de K-algèbres :

Lemme 4.1.1. *Si A est un anneau, alors le centre $Z(A)$ est un sous-anneau.*

Démonstration. C'est une conséquence directe de la Définition 2.1.11. Nous laissons le calcul précise en exercice. □

Définition 4.1.2. Un *algèbre sur un corps* K (ou simplement un K-algèbre) est un pair (A, ι), où A est un anneau, est $\iota : K \to Z(A)$ est un homomorphisme. On appelle l'opération $K \times A \ni (\lambda, a) \mapsto \iota(\lambda) \cdot a$ la multiplication par des scalaires (en utilisant le point (1) du Lemme 4.1.8).

Remarque 4.1.3. En dépit que ι est une donnée indispensable dans la structure d'algèbre de (A, ι), dans la plupart des situations on dénote (A, ι) simplement par A. La raison est que dans beaucoup d'instances (e.g., Exemple 4.1.4), K est un sous-anneau naturel de A, et donc on prend l'inclusion naturel de ce sous-anneau pour ι. Cependant, il est crucial de souvenir qu'il y a un ι fixé non-dénoté mais sous-entendu.

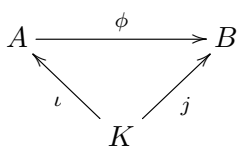
De plus on note que ι est toujours injectif, sauf si $A = 0$. En effet, $\ker \iota$ est un idéal de K mais K contient seulement 2 idéaux par Proposition 2.4.7 : (0) et K. Le deuxième peut arriver seulement dans lorsque $A = 0$, parce que $\iota(1) = 1$ (Définition 2.1.7).

Exemple 4.1.4. L'exemple plus basique d'une algèbre commutative sur K est l'anneau des polynômes $K[x]$. Dans ce cas, l'homomorphisme structural $\iota : K \to K[x]$ est obtenu en regardant les éléments de K comme des polynômes constants.

Exemple 4.1.5. Si $K[G]$ est un anneau de groupe, où K est un corps, alors $K[G]$ est un K-algèbre pour l'homorphisme structural $\iota : K \ni \lambda \mapsto \lambda \cdot e$, où $e \in G$ est l'élément neutre.

Définition 4.1.6. Soit (A, ι) un K-algèbre.

(1) Un homomorphisme des K-algèbres (A, ι) est (B, j) est un homomorphism $\phi : A \to B$ d'anneaux tel que le diagramme suivant commute :



(2) Un sous-K-algèbre de A est un sous-anneau $C \subseteq A$ tel que $\iota(K) \subseteq C$.

(3) Soit $\alpha_i, \ldots, \alpha_n \in A$ des éléments. Le *sous-K-algèbre* de A engendré par les élément α_i est $\iota(K)[\alpha_1, \ldots, \alpha_n]$, ce qui on écrit d'habitude dans une manière plus courte par $K[\alpha_1, \ldots, \alpha_n]$.

Exemple 4.1.7. $\mathbb{C}$ est un $\mathbb{Q}$-algèbre par l'inclusion naturelle $\mathbb{Q} \subseteq \mathbb{C}$. Dans ce cas $\mathbb{Q}\left[\sqrt{2}\right]$ peut être regardé au même temps comme les sous-$\mathbb{Q}$-algèbre de $\mathbb{C}$ engendré par $\sqrt{2}$, et aussi comme le sous-anneau engendré par $\mathbb{Q}$ est $\sqrt{2}$. On note que la notation est indépendante de quelle manière on choisit de penser à $\mathbb{Q}\left[\sqrt{2}\right]$.

Le lemme suivant nous dit que tout ce que l'on a fait dans ce cours devient K-linéaire si on le fait dans le cadre de K-algèbres.

Lemme 4.1.8. *Soit (A, ι) un K-algèbre pour un corps K. Les propositions suivantes sont vraies pour chaque $a \in A$ et $\lambda \in K$:*

(1) A est un espace vectoriel sur K avec l'addition donnée par l'addition de A est la multiplication scalaire par $(\lambda, a) \mapsto \iota(\lambda) \cdot a$.

(2) La multiplication $A \ni x \mapsto ax \in A$ est un endomorphisme K-linéaire.

(3) Si I est un idéal à gauche (resp. idéal à droite) de A, alors I est un sous-espace vectoriel de A sur K

(4) Si I est un idéal bilatère de A, et $\xi : A \to {}^{A}\!/_{I}$ est l'homomorphisme quotient, alors en donnant la structure d'algèbre sur ${}^{A}\!/_{I}$ par $\xi \circ \iota$ on obtient que ξ est un homomorphisme de K-algèbres (notons que si on définit la structure de K-algèbre sur ${}^{A}\!/_{I}$ en manière ci-dessus, alors la multiplication par un scalaire sur ${}^{A}\!/_{I}$ est donnée par $(\lambda, a) \mapsto (\iota(\lambda) + I) \cdot (a + I) = \big(\iota(\lambda) \cdot a\big) + I$).

(5) La Proposition 2.2.3 nous donne la suivante : en fixant un élément $a \in A$ il existe un unique homomorphisme de K-algèbres $\mathrm{ev}_a : K[t] \to A$ tel que $\mathrm{ev}_a(t) = a$.

(6) L'isomorphisme donné par le théorème d'isomorphisme (Corollaire 2.4.17) est un isomorphisme de K-algèbres.

(7) Si I est un idéal bilatère tel que $\dim_K \left({}^{A}\!/_{I}\right) < \infty$, et si $\phi : A \to B$ est un homomorphisme de K-algèbres tel que $\ker \phi = I$, alors $\dim_K \left({}^{A}\!/_{I}\right) = \dim_K (\operatorname{im} \phi)$.

Démonstration. On le laisse en exercice. □

Exemple 4.1.9. ${}^{\mathbb{Q}[x]}\!/_{(x^2-2)}$ est un $\mathbb{Q}$-algèbre tel que la multiplication par scalaire est donnée par $\big(\lambda, f + (x^2-2)\big) \mapsto \lambda \cdot f + (x^2-2)$. De plus, l'application $\mathrm{ev}_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ est un homomorphisme de $\mathbb{Q}$-algèbres (par point (5) du Lemme 4.1.8). Finalement, par le point (6) du Lemme 4.1.8, ${}^{\mathbb{Q}[x]}\!/_{(x^2-2)} \cong \mathbb{Q}\left[\sqrt{2}\right]$ est un isomorphisme de $\mathbb{Q}$-algèbres.

Proposition 4.1.10. *Si K est un corps et $f \in K[t]$ est un polynôme de degré n, alors*

$$S = \left\{ t^i + (f) \;\middle|\; 0 \leq i \leq n-1 \right\}$$

est une base K-linéaire de ${}^{K[t]}\!/_{(f)}$. En particulier, $\dim_K \left({}^{K[t]}\!/_{(f)}\right) = n$.

Démonstration.

S est une famille génératrice : prenons un élément $g + (f) \in {}^{K[t]}\!/_{(f)}$, où $g \in K[t]$ est arbitraire. En performant une division euclidienne on obtient $g = qf + r$ où $q, r \in K[t]$ et $degr < n$. En particulier on peut écrire

$$r = \sum_{i=0}^{n-1} b_i t^i \in K[t]$$

Les égalités suivantes des éléments de $K[t]/(f)$ nous démontre que l'on peut bien écrire $g+(f)$ en tant que une combinaison linéaire des éléments de S :

$$g+(f) = r+(f) = \sum_{i=0}^{n-1} b_i \cdot \big(t^i+(f)\big)$$

multiplication scalaire comme défini par la structure de K-algèbre sur $K[t]/(f)$ dans le point (4) du Lemme 4.1.8

S est une famille libre : Prenons une relation linéaire entre les éléments de S, où $c_i \in K$:

$$0 = \sum_{i=0}^{n-1} c_i \cdot \big(t^i+(f)\big) = \left(\sum_{i=0}^{n-1} c_i t^i\right) + (f) \iff \sum_{i=0}^{n-1} c_i t^i \in (f) \iff \exists g \in K[t] \colon \sum_{i=0}^{n-1} c_i t^i = \underbrace{g \cdot f}$$

par la structure de K-algèbre sur $K[t]/(f)$ définie dans le point (4) du Lemme 4.1.8

degré $\geq n$ par Lemme 3.2.1, sauf si $g=0$

On obtient que $g=0$, et par conséquence c_i sont aussi zéros. Cela implique que il n'y a que des relations linéaires triviales entre les éléments de S. □

Exemple 4.1.11. Par Proposition 4.1.10, $1+(x^2-2)$ et $x+(x^2-1) \in \mathbb{Q}[x]/(x^2-2)$ forment une base $\mathbb{Q}$-linéaire de $\mathbb{Q}[x]/(x^2-2)$. En utilisant l'isomorphisme $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}\left[\sqrt{2}\right]$ des $\mathbb{Q}$-algèbres donné dans Exemple 4.1.9, on obtient que $1, \sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$ est une base $\mathbb{Q}$-linéaire. En particulier, $\dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt{2}\right] = 2$.

4.2 Fondements des extensions de corps

4.2.1 Extensions des corps

Définition 4.2.1. Si L est un corps et $K \subseteq L$ est un sous-corps (i.e., K est un sous-anneau de L et K lui-même est aussi un corps), alors on dit que L est une *extension* de K.

Exemple 4.2.2. Il y a des extensions de corps que l'on connait déjà :

(1) Les extensions $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
(2) Les extensions $F \subseteq F(x) \subseteq F(x,y)$, où F est un corps, et $F(x)$ (resp. $F(x,y)$) est le corps de fractions de $F[x]$ (resp. de $F[x,y]$).
(3) L'extension $K = L^p = \{\, \alpha^p \in L \mid \alpha \in L \,\} \subseteq L$, où $\operatorname{car} L = p > 0$. On laisse en exercice que c'est un sous-corps ; il faut utiliser que $(x+y)^p = x^p + y^p$ lors que $\operatorname{car} L = p > 0$. On appelle cette *extension l'extension de Frobenius* de K.

Pour un exemple explicit on peut prendre $L = \mathbb{F}_p(t)$. Dans ce cas $K = L^p = \mathbb{F}_p(t^p)$.

Définition 4.2.3. Soit $K \subseteq L$ une extension de corps, et $\alpha_1, \dots, \alpha_r \in L$ des éléments de nombre fini. Le *sous-corps* $K(\alpha_1, \dots, \alpha_r)$ *de* L *engendré* par K et par les éléments α_i (aussi dit le *sous-extension* engendré par les α_i) est le plus petit sous-corps de L qui contient K et les α_i.

Comme d'habitude pour les sous-structures engendré, on peut construire ce sous-corps par

$$K(\alpha_1, \dots, \alpha_r) = \bigcap_{\substack{K \subseteq F \subseteq L \text{ sont les} \\ \text{extensions de corps,} \\ \text{tel que } \alpha_1, \dots, \alpha_r \in \\ F}} F$$

où on utilise que les intersections des sous-crops sont sous-corps.

Une *extension simple* des corps, et une extension engendré par un élément.

Dans la même façon que pour les éléments de nombre fini on peut définir aussi le sous-extension $K(S)$ engendré par un quelconque sous-ensemble $S \subseteq L$.

Remarque 4.2.4. Attention : la donnée de L est supprimé de la notation de la Définition 4.2.3. La raison est la suivante : on apprendra que modulo un isomorphisme de K-algèbres l'extension engendré est déterminée par les équations avec coefficients dans K satisfaites par les α_i (Remarque 4.2.26). Autrement dit, modulo un isomorphisme de K-algèbres, le L particulier que l'on prend ne fait pas la différence.

Remarque 4.2.5. Par la Définition 2.2.7 et la Définition 4.2.3, on a $K[\alpha_1, \ldots, \alpha_r] \subseteq K(\alpha_1, \ldots, \alpha_r)$.

4.2.2 Éléments algébriques et transcendants

Notation 4.2.6. Pour un anneau intègre A notons le corps des fractions par $\mathrm{Frac}(A)$, qui est bien défini modulo un unique isomorphisme par Proposition 2.3.19.

Avant la proposition suivante notons que si $A \subseteq L$ est une sous-anneau d'un corps, alors la propriété universelle du corps des fractions (Proposition 2.3.19) nous dit que l'on peut regarder $\mathrm{Frac}(A)$ comme un sous-anneau de L. Dans cette situation on peut bien identifié $\mathrm{Frac}(A)$ par $\left\{ \frac{a}{b} \in L \;\middle|\; a, b \in A \right\}$. On utilisera cette identification multiple fois pendant le reste du cours, sans explications additionnelles.

Proposition 4.2.7. *Soit $K \subseteq L$ une extension des corps, $\alpha \in L$ un élément et $\mathrm{ev}_\alpha : K[x] \to L$ l'unique homomorphisme de K-algèbres tel que $\mathrm{ev}_\alpha(x) = \alpha$. Puisque $K[x]$ est principal, on a $\ker \mathrm{ev}_\alpha = (m_\alpha)$ pour un élément $m_\alpha \in K[x]$. Il y a deux possibilités :*

(1) Si, $m_\alpha \neq 0$, alors m_α est irréductible dans $K[x]$ et

$$K(\alpha) = K[\alpha] = \left\{ f(\alpha) \in L \;\middle|\; f \in K[x] \right\} \underset{\text{en tant que } K\text{-algèbres}}{\cong} K[x]\Big/(m_\alpha). \tag{4.2.a}$$

(2) Si $m_\alpha = 0$, alors,

$$K(\alpha) = \mathrm{Frac}(K[\alpha]) = \left\{ \frac{f(\alpha)}{g(\alpha)} \in L \;\middle|\; f, g \in K[x] \right\} \underset{\text{en tant que } K\text{-algèbres}}{\cong} K(x). \tag{4.2.b}$$

Démonstration. (1) Il suffit de démontrer que $K(\alpha) = K[\alpha]$, parce que des que c'est connu, la deuxième égalité de l'équation (4.2.a) suit directement de la Définition 2.2.7, et la troisième égalité est donné par

$$K[\alpha] \cong K[x]\Big/(m_\alpha) \tag{4.2.c}$$

ce qui est une conséquence directe de l'appplication du théorème d'isomorphisme (Corollaire 2.4.17) à l'$\mathrm{ev}_\alpha : K[x] \to K[\alpha]$. De plus, pour démontrer que $K(\alpha) = K[\alpha]$, il suffit de montrer que $K[\alpha]$ est un corps. Celui-ci est démontré par les équivalences suivante :

$$\underset{\substack{\uparrow \\ \text{parce que } K[\alpha] \text{ et un} \\ \text{sous-anneu du corp } L}}{K[\alpha] \text{ est intègre}} \iff \underset{\substack{\uparrow \\ \text{par (4.2.c), et par Proposition 2.5.2}}}{(m_\alpha) \subseteq K[x] \text{ est premier}} \iff \underset{\substack{\uparrow \\ \text{Proposition 3.4.13, en utilisant crucialement} \\ \text{que } K[x] \text{ est un anneau principal}}}{(m_\alpha) \subseteq K[x] \text{ est maximal}} \iff \underset{\substack{\uparrow \\ \text{par (4.2.c), et par Proposition 2.5.2}}}{K[\alpha] \text{ est un corps}}$$

Notons, que un point de la Proposition 3.4.13 nous aussi donne que m_α est irréductible.

(2) Pour la première égalité de l'équation (4.2.b), notons que tous les deux $K(\alpha)$ et $\mathrm{Frac}(K[\alpha])$ sont le plus petit corps contenant $K[\alpha]$. La deuxième equation de l'(4.2.b) suit directement du paragraphe avant la présente proposition et le fait que $K[\alpha]$ est par définition l'image de ev_α (Définition 2.2.7). Pour la troisième equation, notons que lorsque $m_\alpha = 0$:

$$\ker \mathrm{ev}_\alpha = (0) \implies \mathrm{ev}_\alpha \text{ est injectif} \implies K[\alpha] = \mathrm{im}\, \mathrm{ev}_\alpha \underset{\boxed{\text{comme } K\text{-algèbres}}}{\overset{\cong}{\uparrow}} K[x]$$

Ainsi, $K(\alpha) = \mathrm{Frac}(K[\alpha]) \cong \mathrm{Frac}\left(K[x]\right) = K(x)$.

□

Définition 4.2.8. Si $K \subseteq L$ est un extension des corps, et $\alpha \in L$ est un élément, alors il y a deux possibilités :

(1) Soit on est dans la situation de point (1) de la Proposition 4.2.7. Dans ce cas, on dit que α est *algébrique* sur K, et que m_α est le *polynôme minimal* de α sur K.

Notons que puisque m_α est défini comme le générateur du $\ker \mathrm{ev}_\alpha$, m_α est bien-défini modulo être associé dans $K[x]$ (Lemme 3.4.3), ou autrement dit c'est unique modulo une multiplication par un non-zéro constant. Quelque fois m_α est dénoté par $m_{\alpha,K}$, quand il y a plusieurs possibilités de corps de base.

Dans le cas spécifique de $K = \mathbb{Q}$ et $L = \mathbb{C}$, si $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$, on dit aussi que α est un *nombre algébrique*.

(2) Soit on est dans la situation de point (2). Dans ce cas on dit que α est *transcendant* sur K.

Dans le cas spécifique de $K = \mathbb{Q}$ et $L = \mathbb{C}$, si $\alpha \in \mathbb{C}$ est transcendant sur $\mathbb{Q}$, on dit aussi que α est un *nombre transcendant*.

Autrement dit, un élément est algébrique sur un corps K si il existe un polynôme non-zéro sur K qui s'annule en α.

Remarque 4.2.9. La Proposition 4.2.7 implique aussi que si $g \in \ker \mathrm{ev}_\alpha$ est un polynôme irréductible dans $K[x]$, alors $g \sim m_\alpha$. En effet, $g \in \ker \mathrm{ev}_\alpha$ implique que $g \in (m_\alpha)$, ou autrement dit que $m_\alpha | g$. Puisque tous les deux g est m_α sont irréductibles, on obtient que $g \sim m_\alpha$.

Exemple 4.2.10. On trouve exemples des éléments algébriques, et on détermine des polynômes minimaux pour les uns qui sont algébriques en utilisant la Remarque 4.2.9 :

(1) L'élément $i \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ ou sur $\mathbb{R}$, parce que $x^2 + 1$ s'annule en i. De plus $x^2 + 1$ est irréductible sur tous les deux $\mathbb{Q}$ et $\mathbb{R}$ parce qu'il n'admet pas une racine sur ces corps (point (4) de l'Exemple 3.4.7). Ainsi, $x^2 + 1 = m_{i,\mathbb{Q}}$ et $x^2 + 1 = m_{i,\mathbb{R}}$.

(2) L'élément $\sqrt{2} \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ parce que $x^2 - 2 \in \mathbb{Q}[x]$ s'annule en $\sqrt{2}$. Dans une façon similaire à celle du point précédent on trouve que $m_{\sqrt{2},\mathbb{Q}} = x^2 + 2$.

(3) Considérons la situation du point (3) de l'Exemple 4.2.10. Cela veut dire que on a

$$K = L^p = \mathbb{F}_p(t^p) \underset{\boxed{\text{donné par } t \leftrightarrow u}}{\overset{\cong}{\uparrow}} \mathbb{F}_p(u) \quad \subseteq \quad L = \mathbb{F}_p(t) \quad \ni \quad t = \alpha$$
$$\boxed{\text{corps des fonctions algébriques en variable } u}$$

L'équation $x^p - u$ est irréductible par le critère d'Eisenstein (la Proposition 3.9.3) sur $\mathbb{F}_p[u]$. Par Gauss III (la Proposition 3.8.13), il est aussi irréductible sur $\mathbb{F}_p(u) = K$. On obtient que $m_{\alpha,K} = x^p - t^p$.

(4) π est transcendant sur $\mathbb{Q}$ (c'est un théorème d'analyse, Zsolt n'est pas sûr si vous l'avez appris ou non).

Remarque 4.2.11. On note que pendant les deux siècles passés, il s'avérait que l'on peut plus facilement comprendre les extensions des corps par des éléments transcendants avec les méthodes géométriques. Par example, si on connait les fondements de la géométrie algébrique, il découle facilement que les corps $\mathbb{Q}(x)[y]\Big/\big(x^2 - y(y+1)(y-1)\big)$ et $\mathbb{Q}(x)[y]\Big/\big(x^2 - y(y+1)(y-1)(y+2)(y+1)\big)$ ne sont pas isomorphes, ce qui est difficile à démontrer en utilisant des méthodes algébriques traditionnelles. On note que ici l'élément x est transcendant sur $\mathbb{Q}$, ce qui rend la compréhension difficile avec méthodes purement corps théorétiques.

En effet, il existe même un sous-domaine de la géométrie algébrique qui s'appelle géométrie birationnelle, dont l'objectif est de comprendre géométriquement les extensions des corps engendré par un nombre fini des éléments transcendants (et un nombre fini des éléments algébriques additionnels).

Par conséquent, dans ce cours on se concentre sur les extensions des corps par des éléments algébriques.

4.2.3 Le degré des extensions

Définition 4.2.12. Si $K \subseteq L$ est une extension de corps, alors le *degré* de l'extension, notée par $[L : K]$, est la dimension de L en tant qu'un K-espace vectoriel. Si $\alpha \in L$, alors le *degré* de α sur K est $[K(\alpha) : K]$.

Corollaire 4.2.13. *Soit $K \subseteq L$ une extension de corps. Un élément $\alpha \in L$ est algébriques si et seulement si son degré est fini.*

De plus, dans ce cas, $[K(\alpha) : K] = \deg m_{\alpha,K}$, et $\left\{\ \alpha^i \ \middle|\ 0 \leq i < \deg m_{\alpha,K}\ \right\}$ forme une base K-linéaire de $K(\alpha)$.

Démonstration. Le premier paragraphe est un corollaire direct de la Proposition 4.2.7, compte tenu que $\dim_K K(x) = \infty$: en effet $\left\{\ x^i \ \middle|\ i \in \mathbb{N}\ \right\}$ forme une famille libre en $K(x)$ parce qu'ils forme une famille libre déjà dans $K[x]$.

Le deuxième paragraphe est une conséquence directe de la Proposition 4.1.10, compte tenu que l'isomorphisme $K[x]\Big/(m_\alpha) \cong K(\alpha)$ envoie x sur α. □

Exemple 4.2.14. On utilise Corollaire 4.2.13 pour trouver le degré des éléments algébrique de l'Exemple 4.2.10 :

(1) $[\mathbb{C} : \mathbb{R}] = 2$, ou en autre mots le degré de i et 2 sur $\mathbb{R}$, parce que $m_{i,\mathbb{R}} = x^2 + 1$ a degré 2.
(2) Puisque $m_{i,\mathbb{Q}} = x^2 + 1$, le degré de i sur $\mathbb{Q}$ est 2 aussi. Autrement dit, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, et une base de $\mathbb{Q}(i)$ sur $\mathbb{Q}$ est donné par $\{1, i\}$.
(3) Puisque $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$, le degré de $\sqrt{2}$ sur $\mathbb{Q}$ est 2 aussi. Les éléments $\{1, \sqrt{2}\}$ forme une base $\mathbb{Q}$-linéaire de $\mathbb{Q}[\sqrt{2}]$.
(4) Dans la situation de $K = L^p = \mathbb{F}_p(t^p) \subseteq \mathbb{F}_p(t) = L \ni t = \alpha$, on a $m_{t,K} = x^p - t^p$. On en déduit que le degré de t sur K est p, ou autrement dit $[L, L^p] = p$. On verra dans les exercices que $[L, L^p]$ peut être égal aux autres puissances de p pour autre choix des corps de caractéristique $p > 0$.

On continue avec exemples qui ne viennent pas de l'Exemple 4.2.10 :

(5) Pour $n \geq 2$, le polynôme $x^n - 2$ est irréductible sur $\mathbb{Z}$ en utilisant le critère d'Eisenstein (Proposition 3.9.3) avec $p = 2$. Par Gauss III (Proposition 3.8.13), cela implique que $x^n - 2$ est aussi irréductible sur $\mathbb{Q}$. Du coup, par Remarque 4.2.9, $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$. En utilisant Corollaire 4.2.13 on obtient que le degré de $\sqrt[n]{2}$ sur $\mathbb{Q}$ est n et donc $\left\{\ \left(\sqrt[n]{2}\right)^i \ \middle|\ 0 \leq i \leq n-1\ \right\}$ est une base de $\mathbb{Q}\left(\sqrt[n]{2}\right)$ sur $\mathbb{Q}$.
(6) Considérons un entier premier $p \geq 3$ et une racine primitive p-ième de l'unité $\xi = e^{\frac{2\pi i}{p}}$. Le polynôme $x^p - 1$ s'annule en ξ, qui implique que $m_{\xi,\mathbb{Q}}$ est un facteur irréductible de

$x^p - 1$ sur $\mathbb{Q}$. Cependant, 1 est aussi une racine de $x^p - 1$, et par conséquent $x - 1 | x^p - 1$ (point (1) de l'Exemple 2.4.10). En particulier, $x^p - 1$ n'est pas irréductible sur $\mathbb{Q}$. Puisque $x - 1$ ne s'annule pas en ξ, il faut le jeter pour obtenir $m_{\xi,\mathbb{Q}}$. Faisons donc une division euclidienne : $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + 1 \in \mathbb{Q}[x]$. En utilisant que $x - 1$ ne s'annule pas en ξ, on obtient que $x^{p-1} + x^{p-2} + \ldots + 1$ s'annule en ξ. De plus, ce dernier polynôme est irréductible sur $\mathbb{Q}$ par point (2) de l'Exemple 3.9.4. Du coup, $m_{\xi,\mathbb{Q}} = x^{p-1} + x^{p-2} + \ldots + 1$, est donc le degré de ξ sur $\mathbb{Q}$ est $p - 1$.

(7) Si, ξ est une racine primitive n-ième de l'unité pour un entier n non-premier, alors le degré de ξ n'est pas forcément $n - 1$. Par exemple, i et $-i$ sont les racines primitive quatrième de l'unité, et ses degrés sont 2 sur $\mathbb{Q}$, par le point (1) de l'exemple présent.

Proposition 4.2.15. *Si $K \subseteq L \subseteq M$ sont des extensions de corps de degré fini, alors $[M : K] = [M : L] \cdot [L : K]$.*

La fin du 10. cours, le 20.04.2021.

Démonstration. Soient $r = [L : K]$ et $s = [M : L]$. Fixons de plus une base $\{ x_i \mid 1 \leq i \leq r \}$ de L sur K et une base $\{ y_j \mid 1 \leq j \leq s \}$ de M sur L. Nous montrons que

$$S = \{ x_i y_j \mid 1 \leq i \leq r,\ 1 \leq j \leq y \}$$

est une base de M sur K :

La famille S est libre sur K : Le calcul suivant démontre que chaque relation K-linéaire entre les éléments de S avec coefficients $\lambda_{i,j} \in K$ est trivial :

$$0 = \sum_{j=1}^{s} \sum_{i=1}^{r} \lambda_{i,j} x_i y_j = \sum_{j=1}^{s} \underbrace{\left(\sum_{i=1}^{r} \lambda_{i,j} x_i \right)}_{\in L} y_j \overset{\text{les } y_j \text{ forment une famille libres sur } L}{\Longrightarrow} \forall 1 \leq j \leq s : \ 0 = \sum_{i=1}^{r} \lambda_{i,j} x_i$$

$$\overset{\text{les } x_i \text{ forment une famille libres sur } L}{\Longrightarrow} \forall 1 \leq i \leq r, 1 \leq j \leq s : \ \lambda_{i,j} = 0$$

La famille S est une génératrice de M sur K : Soit $z \in M$. Puisque les y_j forme une base de M sur L, il existe $\mu_j \in L$ tels que

$$z = \sum_{j=1}^{s} \mu_j y_j$$

De même, puisque les x_i forment une base de L sur K, il existe $\lambda_{i,j} \in K$ tel que

$$\forall 1 \leq j \leq s : \ \mu_j = \sum_{i=1}^{r} \lambda_{i,j} x_i.$$

Par conséquent on a

$$z = \sum_{j=1}^{s} \mu_j y_j = \sum_{j=1}^{s} \sum_{i=1}^{r} \lambda_{i,j} x_i y_j.$$

□

Exemple 4.2.16.

(1) On démontre que $\left[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}\right] = 4$. Pour cela, pensons de $\mathbb{Q}(\sqrt{2},i)$ en tant que $\Big(\mathbb{Q}(\sqrt{2})\Big)(i)$. On a vu dans le point (3) de l'Exemple 4.2.14 que $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$. De plus, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, parce que $\mathbb{Q} \subseteq \mathbb{R}$ et $\sqrt{2} \in \mathbb{R}$. Alors, $i \notin \mathbb{Q}(\sqrt{2})$. En utilisant que i est une racine de x^2+1 on obtient que le degré de i sur $\mathbb{Q}(\sqrt{2})$ est 2. Du coup, $\left[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}(\sqrt{2})\right] = 2$. Une application de la Proposition 4.2.15 conclut notre démonstration :

$$\left[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}(\sqrt{2})\right] \cdot \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2 \cdot 2 = 4.$$

(2) Un argument similaire, qui au même temps contient des nouveaux pièges, montre que $\left[\mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}) : \mathbb{Q}\right] = 6$, où $\xi = e^{\frac{2\pi i}{3}}$ une racine primitive troisième d'unité. Le piège ici est que tous les deux $\sqrt[3]{2}$ et $\xi\sqrt[3]{2}$ satisfont la même equation $x^3 - 2$ sur $\mathbb{Q}$. De plus, comme démontré dans le point (3) de l'Exemple 4.2.14, c'est un polynôme irréductibles sur $\mathbb{Q}$. Cependant, il n'est pas irréductible sur $\mathbb{Q}(\sqrt[3]{2})$. La raison, est qu'il obtient une racine, $\sqrt[3]{2}$ lui-même, sur $\mathbb{Q}(\sqrt[3]{2})$. Par conséquent, en utilisant point (1) de l'Exemple 2.4.10, $x - \sqrt[3]{2} | x^3 - 2$ sur $\mathbb{Q}(\sqrt[3]{2})$, ou autrement dit dans l'anneau $\mathbb{Q}(\sqrt[3]{2})[x]$. D'une façon similaire à l'argument dans le point (6) de l'Exemple 4.2.14, on en déduit que $f = \frac{x^3-2}{x-\sqrt[3]{2}} = x^2 + \sqrt[3]{2}x + \left(\sqrt[3]{2}\right)^2 \in \Big(\mathbb{Q}(\sqrt[3]{2})\Big)[x]$ est un polynôme de degré 2 qui s'annule en $\xi\sqrt[3]{2}$. Par Remarque 4.2.9, ce polynôme est divisé par le polynôme minimal de $\xi\sqrt[3]{2}$ sur $\mathbb{Q}(\sqrt[3]{2})$. Cependant, $\xi\sqrt[3]{2} \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[3]{2})$. De coup, le polynôme minimal de $\xi\sqrt[3]{2}$ sur $\mathbb{Q}(\sqrt[3]{2})$ a au moins degré 2. Ainsi, f est ce polynôme minimal lui-même (modulo être associé dans $\Big(\mathbb{Q}(\sqrt[3]{2})\Big)[x]$). On obtient que la situation et la suivante :

$$\left[\mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}) : \mathbb{Q}\right] \underset{\text{Proposition 4.2.15}}{=\!\!\uparrow} \left[\mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})\right] \cdot \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 2 \cdot 3 = 6.$$

(3) Si $K \subseteq L$ est une extension de degré fini, alors le degré de tout élément $\alpha \in L$ divise $[K : L]$. En effet, par Proposition 4.2.15 on a $[K : L] = [K : L(\alpha)][L(\alpha) : L]$, où $[L(\alpha) : L]$ est le degré de α.

Par exemple, si on prend $L = \mathbb{Q}$ et $K = \mathbb{Q}(\sqrt[3]{2})$, alors dans le point (3) de l'Exemple 4.2.14 on a vu que $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$, et on obtient que chaque élément de $\mathbb{Q}(\sqrt[3]{2}) \setminus \mathbb{Q}$ a degré 3.

4.2.4 Extensions algébriques

Définition 4.2.17. Une extension $K \subseteq L$ est *algébrique* si tout élément α de L est algébrique sur K.

Proposition 4.2.18. *Si $K \subseteq L$ est une extension de degré fini, alors L est algébrique sur K. En particulier si $\alpha \in L$ est algébrique sur K, alors $K(\alpha)$ est une extension algébrique de K.*

Démonstration. Il suffit de démontrer la première proposition. Les implications suivantes démontre que quelconque $\beta \in L$ est algébriques sur K :

$$\dim_K L < \infty \underset{K(\beta) \subseteq L}{\Longrightarrow\!\!\uparrow} \dim_K K(\beta) < \infty \underset{\text{Proposition 4.2.15}}{\Longrightarrow\!\!\uparrow} \beta \text{ est algébrique sur } K$$

□

Exemple 4.2.19. Une extension algébrique n'est pas simplement une extension par un élément algébrique. Autrement dit il existe des extensions algébriques non-simple. On donne dans l'Exemple 4.2.22 un exemple d'une extension algébrique de degré infini, ce qui par conséquent ne peut pas être une extension simple.

Ici, on donne un exemple d'une extension qui est algébrique de degré fini mais elle n'est pas simple. Pour ce but, considérons l'extension Frobenius $K = L^p \subseteq L$ un corps L de caractéristique $p > 0$. C'est une extension algébrique parce que $\alpha \in K$ est une racine du polynôme $x^p - \alpha^p \in K[x]$. Notons, que cette idée était déjà utiliser dans le point (4) de l'Exemple 4.2.14, et elle implique aussi que le degré de chaque élément de K est au plus p.

Au même temps, il y a corps pour lesquels l'extension Frobenius ont degré plus que p. Par exemple, pour $L = \mathbb{F}_p(t,u)$ il est de degré p^2 comme démontré dans le calcul suivant

$$[L : L^p = \mathbb{F}_p(t^p,u^p)] = \underbrace{[\mathbb{F}_p(t,u) : \mathbb{F}_p(t^p,u)]}_{\text{Proposition 4.2.15}} \cdot \underbrace{[\mathbb{F}_p(t^p,u) : \mathbb{F}_p(t^p,u^p)]}_{= p, \text{ parce que } m_{u,\mathbb{F}_p(t^p,u^p)} = x^p - u^p \in (\mathbb{F}_p(t^p,u^p))[x]}$$

$= p$, parce que $m_{t,\mathbb{F}_p(t^p,u)} = x^p - t^p \in (\mathbb{F}_p(t^p,u))[x]$

D'autre coté on démontrera que toute extension *séparable* finie est simple dans la Section 4.5.

Remarque 4.2.20. Soit $K \subseteq L \subseteq M$ des extensions de corps, et $\alpha \in M$ un élément algébrique sur K. Dans ce cas α est aussi algébrique sur L : puisqu'il est algébrique sur K il existe $0 \neq f \in K[t]$ tel que $f(\alpha) = 0$, mais f peut être regarder aussi comme un polynôme avec des coefficients en L, ce qui montre que α est bien algébrique sur L aussi.

Corollaire 4.2.21. *Si $K \subseteq L$ est une extension de corps, alors l'ensemble*

$$L_{\text{alg},K} = \{\ \alpha \in L \mid \alpha \text{ est algébrique sur } K\ \}$$

est un sous corps de L qui contient K.

Démonstration. Prenons éléments non-zéros α et $\beta \in L_{\text{alg},K}$. Par Remarque 4.2.20. Les deux extensions de corps suivantes sont de degré fini :

$$\underbrace{K \subsetneq K(\alpha)}_{\alpha \text{ est algébrique sur } K} \qquad \text{et} \qquad \underbrace{K(\alpha) \subsetneq K(\alpha,\beta)}_{\substack{\beta \text{ est algébrique sur } K, \text{ et alors il est} \\ \text{aussi algébrique sur } K(\alpha) \text{ par la Re-} \\ \text{marque 4.2.20}}}$$

En utilisant Proposition 4.2.15, $[K(\alpha,\beta) : K] < \infty$, et ainsi par la Proposition 4.2.18 on obtient que $K(\alpha,\beta)$ est une extension algébrique de K. Cela implique que $\alpha + \beta$, $-\alpha$, $\alpha\beta$ et α^{-1} sont contenu dans L_{alg}, ce qui conclut notre démonstration. □

Exemple 4.2.22. On donne un exemple d'une extension algébrique de degré infini. Soit ξ_p pour chaque entier premier p une racine primitive p-ième d'unité et soit

$$L = \mathbb{Q}(\ \xi_p \mid p \text{ est un nombre premier }\ ).$$

Premièrement, $\xi_p \in L_{\text{alg},\mathbb{Q}}$ par le point (6) de l'Exemple 4.2.14. Il suit par Corollaire 4.2.21 que $L_{\text{alg},\mathbb{Q}}$ et un corps que contient tous les ξ_p. Ainsi, $L \subseteq L_{\text{alg},\mathbb{Q}}$, ce qui montre que L est une extension algébrique.

Supposons que $[L : \mathbb{Q}] < \infty$. En utilisant la Proposition 4.2.15 et le point (6) de l'Exemple 4.2.14, on obtient que $[L : \mathbb{Q}] \geq p - 1$ pour chaque nombre premier p. C'est une contradiction avec la finitude de $[L : \mathbb{Q}]$.

4.2.5 Construction (autonome) des extensions algébriques simples

On commence avec un corollaire direct de la Proposition 4.2.7.

Corollaire 4.2.23. *Si $K \subseteq L = K(\alpha)$ et $K \subseteq L' = K(\alpha')$ sont deux extensions simples de corps telles que $m_{\alpha,K} \sim m_{\alpha',K}$ dans $K[x]$, alors il existe un isomorphisme $\phi : K(\alpha) \xrightarrow{\cong} K(\alpha')$ de K-algèbres tel que $\phi(\alpha) = \alpha'$.*

Démonstration. On obtient ϕ par la composition des isomorphismes suivants des K-algèbres :

$$K(\alpha) \underset{\uparrow}{\cong} K[x]\Big/(m_{\alpha,K}) \underset{\uparrow}{\cong} K[x]\Big/(m_{\alpha',K}) \underset{\uparrow}{\cong} K(\alpha') = L'$$

Proposition 4.2.7 donne un isomorphisme qui envoie α sur $x + m_{\alpha,K}$	$m_{\alpha,K} \sim m_{\alpha',K}$ donne un isomorphisme qui envoie $x + m_{\alpha,K}$ sur $x + m_{\alpha',K}$	Proposition 4.2.7 donne un isomorphisme qui envoie $x + m_{\alpha',K}$ sur α'

□

Exemple 4.2.24. On montre que en effet l'isomorphisme du Corollaire 4.2.23 ne signifie pas que $K(\alpha) = K(\beta)$ en tant que sous-corps de L.

Pour cela prenons $\alpha = \sqrt[3]{2}$, $\beta = \xi\sqrt[3]{2}$ où $\xi = e^{\frac{2\pi i}{3}}$. On a $m_{\alpha,\mathbb{Q}} = m_{\beta,\mathbb{Q}} = t^3 - 2$ (point (3) de l'Exemple 4.2.14). En particulier, $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$ en tant que $\mathbb{Q}$-algèbres. Cependant, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ en tant que sous-corps de L.

On sait, de l'Analyse III, que si $f \in \mathbb{Q}[x]$ est un polynôme (irréductible), alors il existe une racine de f dans $\mathbb{C}$. En combinant cela avec le Corollaire 4.2.23, on obtient que chaque extension algébrique simple de $\mathbb{Q}$ est isomorphe à un sous-corps de $\mathbb{C}$.

Cependant, si on voudrait comprendre aussi les extensions de $\mathbb{F}_p$ ou de $F(t)$, alors on n'a pas une telle convenance. Autrement dit, il n'y a pas un corps dans le quel on peut comprendre des extensions de $\mathbb{F}_p$ ou de $F(t)$. Par conséquent, on a besoin de la proposition suivante :

Proposition 4.2.25. *Si $f \in K[x]$ est un polynôme irréductible pour un corps K, alors $K[x]\Big/(f)$ est une extension algébrique, simple de K de degré $\deg f$, contenant une racine de f.*

Démonstration. C'est une conséquence directe de les propositions suivantes : la Proposition 2.5.5, la Proposition 3.4.13 et la Proposition 4.1.10. La racine de f est $x + (f) \in K[x]\Big/(f)$. □

Remarque 4.2.26. En combinant la Corollaire 4.2.23 et la Proposition 4.2.25 il y a une bijection pour chaque corps K fixé :

$$\left\{ (K \subseteq L, \alpha \in L) \;\middle|\; \begin{array}{l} K \subseteq L \text{ est une} \\ \text{extension simple} \\ \text{de corps tel que} \\ K(\alpha) = L \end{array} \right\} \Big/ \begin{array}{l} (K \subseteq L, \alpha \in L) \equiv (K \subseteq L', \alpha' \in L'), \\ \text{s'il existe } \phi : L \xrightarrow{\cong} L' \text{ de } K\text{-algèbres} \\ \text{tel que } \phi(\alpha) = \alpha' \end{array} \longleftrightarrow \boxed{f \in K[x] \text{ irréductible}\Big/\sim}$$

On note que cette bijection peut est utile dans toutes les deux directions. Quelques fois le plus simple manière de comprendre l'irréductibilité d'un polynôme est de comprendre l'extension de corps associée. Un exemple est l'exercice dans une des séries de montrer que $x^5 - y^7 \in \mathbb{C}[x, y]$ est irréductible.

De plus, on note que on appelle l'extension qui correspond à $f \in K[x]$ irréductible le corps de rupture de f.

Exemple 4.2.27. (1) Dans $\mathbb{F}_2[x]$, il y a deux polynômes de degré 1 : les polynômes x et $x-1 \in \mathbb{F}_2[x]$. Si un polynôme de degré 2 est réductible, alors par le Lemme 3.2.1 il est un produit des deux polynômes linéaires. Du coup, il y a 3 polynômes réductibles de degré 2 dans $\mathbb{F}_2[x]$: x^2, $x(x+1) = x^2+x$ et $(x+1)^2 = x^2+1$. Par conséquent $x^2+x+1 \in \mathbb{F}_2[x]$ est le seul irréductible de degré 2. En utilisant Remarque 4.2.26 on obtient que il existe une seule extension L de $\mathbb{F}_2$ de degré 2 modulo un isomorphisme d'$\mathbb{F}_2$-algèbre. Cette extension ajoute des racines de x^2+x+1 à $\mathbb{F}_2$. Notons qu'une telle racine est aussi automatiquement une racine primitive troisième d'unité, parce que $(x+1)(x^2+x+1) = x^3+1$.

Par l'unicité, on appelle l'extension de $\mathbb{F}_2$ construit dans le paragraphe ci-dessus le corps $\mathbb{F}_4$. C'est un des corps que l'on construira dans la Section 4.4.

(2) Pour chaque corps K, le polynôme $x^2-(t+1) \in \big(K(t)\big)[x]$ est irréductible, par exemple en utilisant le critère d'Eisenstein et Gauss III(Proposition 3.9.3 et Proposition 3.8.13). On obtient que l'on peut ajouter à $K(t)$ une racine $\sqrt{t+1}$ de $t+1$, en obtenant le corps $L = \big(K(t)\big)[x] \Big/ \big(x^2-(t+1)\big)$.

4.3 Corps de décomposition

On a vu dans le point (2) de l'Exemple 4.2.16 une extension $K \subseteq L$ de corps telle que L contient toute troisième racine de 2. Autrement dit le polynôme t^3-2 scinde sur L. Cela est un exemple de :

Définition 4.3.1. Soit K un corps, et $f \in K[x]$ un polynôme (pas nécessairement irréductible). Une extension $K \subseteq L$ de K est un *corps de décomposition* de f sur K si elle est une extension minimale de K avec la propriété que f *scinde* sur L.

On note que :

(1) Minimal ici signifie que $K \subseteq L$ ne contient pas des autres extensions sur lesquelles f est scindé.

(2) La condition que f scinde sur L signifie que dans $L[x]$ on peut écrire f en tant qu'un produit des facteurs linéaires. En fusionnant les coefficients dominants de ces facteurs linéaires dans un seul constant c on obtient que c'est équivalent à l'existence d'un décomposition de forme

$$f = c\prod_{i=1}^{n}(x-\alpha_i).$$

où $c \in L$ et $\alpha_i \in L$ pour $1 \leq i \leq n$. De plus, en notant que c est le coefficient dominant de f, et que par conséquent il est dans K, on peut même supposer que $c \in K$.

Remarque 4.3.2. Notons que dans la Définition 4.3.1 les α_i sont uniquement déterminé par f et L, parce qu'ils viennent des facteurs irréductible de f sur L, qui sont déterminé uniquement, parce que $L[x]$ est un anneau factoriel.

Un point magique de la théorie des corps est que en effet les α_i sont même déterminé uniquement juste par f, modulo un isomorphisme de L. Cela est une conséquence de l'unicité de corps de décomposition modulo isomorphisme (Théorème 4.3.4). La démonstration de cette unicité est l'objectif principal de cette section.

Lemme 4.3.3. *Si K est un corps, et $f \in K[x]$ est un polynôme, alors :*

(1) Si $K \subseteq L$ est un corps de décomposition de f, alors $L = K(\alpha_1, \ldots, \alpha_n)$ où α_i sont les racines de f dans L. En particulier, L est algébriques sur K de degré fini.

(2) Il existe au moins un corps de décomposition de f.

Démonstration. (1) Si $L \neq K(\alpha_1, \ldots, \alpha_n)$ on pourrait remplacer L par $K(\alpha_1, \ldots, \alpha_n)$, qui serait une contradiction avec la minimalité dans la Définition 4.3.1.

(2) La preuve est similaire au point (2) de l'Exemple 4.2.16. Soit

$$f = \underbrace{\left(\prod_{i=1}^{r} f_i\right)}_{\text{facteurs non-linéaires}} \underbrace{\left(\prod_{j=1}^{s} g_j\right)}_{\text{facteurs linéaires}} \tag{4.3.a}$$

la décomposition en facteurs irréductibles de f. On démontre la proposition par récurrence sur $d = \sum_{i=1}^{r} \deg f_i$. Si $d = 0$, alors f déjà scinde sur K, et donc on peut prendre $L = K$.

Par conséquent, on suppose que $d > 0$ est que l'on connait l'existence du corps de décomposition pour les plus petites valeurs de d. Dans ce cas, par $d > 0$ on a $r \geq 1$. Prenons K' l'extension donné en appliquant la Proposition 4.2.25 à f_1, ce qui l'on appelle aussi le corps de rupture de f_1 (Remarque 4.2.26). En particulier on a une racine α de f_1 dans K'. Le point clé est que l'équation (4.3.a) s'arrête d'être une décomposition en facteurs irréductibles sur K' :

$$f_1(\alpha) = 0 \underbrace{\implies}_{\text{point (1) de l'Exemple 2.4.10}} x - \alpha | f_1 \implies f_1 = (x-\alpha) f_1' \quad \text{pour} \quad f_1' \in K'[x]$$

Par conséquent, sur K', la somme des degrés des facteurs irréductibles non-linéaires de f est moins que d. Par la supposition de la récurrence il existe un corps de décomposition $K' \subseteq L$ de f sur K'. Celui-ci serait aussi un corps de décomposition de f sur K.

□

L'objectif principal du théorème prochain est de démontrer que le corps de décomposition est unique, modulo des isomorphismes. Cependant, pour les applications dans la théorie de Galois (Section 4.6), on démontre une proposition un peu plus générale :

Théorème 4.3.4. *Considérons la situation suivante :*

(1) $\phi : K \to K'$ *est un isomorphisme des corps,*

(2) $K \subseteq L$ *un corps de décomposition de* $f \in K[x]$*, et*

(3) $K' \subseteq L'$ *un corps de décomposition de* $\xi(f) \in K'[x]$*, où* $\xi : K[x] \to K'[x]$ *est l'homomorphisme induit par* ϕ*.*

Dans ce cas, il existe un isomorphisme de corps ψ *qui étend* ϕ*, i.e :*

$$\begin{array}{ccc} L & \xrightarrow[\cong]{\psi} & L' \\ \text{corps de décomposition de } f \uparrow & & \uparrow \text{corps de décomposition de } \phi(f) \\ K & \xrightarrow[\cong]{\phi} & K' \end{array}$$

La fin du 11. cours, le 27.04.2021.

Démonstration. Par point (1) du Lemme 4.3.3, $K \subseteq L$ et $K' \subseteq L'$ sont des extensions algébriques de degré fini. Du coup, on peut faire la preuve par récurrence sur le degré $[L : K]$. Dénotons par $\xi : K[x] \to K'[x]$ l'homomorphisme induit par ϕ.

Cas de $[L : K] = 1$ *:* dans ce cas $L = K$ et :

$$f = c\prod_{i=1}^{r}(x - \alpha_i) \text{ dans } K[x] \quad \implies \quad \xi(f) = \phi(c)\prod_{i=1}^{r}\big(x - \phi(\alpha_i)\big) \text{ dans } K'[x].$$

Ceci montre que $L' = K'$, et on peut choisir $\psi = \phi$.

Pas d'induction : supposons désormais que $[L : K] > 1$, et que l'on connait la proposition pour plus petites valeurs de $[L : K]$. Par point (1) du Lemme 4.3.3, le polynôme f admet une racine α dans $L \setminus K$. On a

$$m_{\alpha,K} \big| f \text{ dans } K[x] \iff \exists g \in K[x] \colon\ m_{\alpha,K} \cdot g = f \underset{\uparrow}{\implies} \exists g \in K[x] \colon\ \xi(m_{\alpha,K})\,\xi(g) = \xi(f)$$

ξ est un homomorphisme

$$\implies \xi(m_{\alpha,K}) \big| \xi(f) \text{ dans } K'[x].$$

Puisque L' est un corps de décomposition de $\xi(f)$, il contient une racine de α' de $\xi(m_{\alpha,K})$. En particulier, on a $m_{\alpha',K'} = \xi(m_{\alpha,K})$. Dénotons l'isomorphisme suivant par $\phi(\alpha)$:

$$K(\alpha) \underset{\uparrow}{\cong} K[x]\Big/(m_{\alpha,K}) \cong K'[x]\Big/(m_{\alpha',K'}) \underset{\uparrow}{\cong} K'(\alpha') \qquad \text{(4.3.b)}$$

$\phi(\alpha)$

donné par point (1) de la Proposition 4.2.7 $\implies$ il est un isomorphisme de K-algèbres $\implies$ il fixe des éléments de K

donné par point (1) de la Proposition 4.2.7 $\implies$ il est un isomorphisme de K'-algèbres $\implies$ il fixe des éléments de K'

obtenu en applicant point (1) de la Proposition 2.4.16 à la composition $K[x] \xrightarrow[\cong]{\xi} K'[x] \longrightarrow K'[x]\Big/(m_{\alpha',K'})$, ce que est possible à faire parce que le noyau de cette composition est $(m_{\alpha,K})$ par l'équation $m_{\alpha',K'} = \xi(m_{\alpha,K})$
$\implies$ la restriction de cet isomoprhisme sur K s'identifie avec $\xi|_K = \phi$

En utilisant les remarques en-dessous chaque flèche dans le diagramme (4.3.b), on voit que $\phi(\alpha)|_K = \mathrm{id}_{K'} \circ \phi \circ \mathrm{id}_K = \phi$. Autrement dit, on a le diagramme suivant :

$$\begin{array}{ccc} L & & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow[\cong]{\phi(\alpha)} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow[\cong]{\phi} & K' \end{array}$$

De plus, on a

$$[L : K(\alpha)] = \underset{\uparrow}{\frac{[L : K]}{[K(\alpha) : K]}} < \underset{\uparrow}{[L : K]}$$

Proposition 4.2.15 — $[K(\alpha) : K] > 1$ parce que $\alpha \in L \setminus K$

Par conséquent, on peut appliquer notre supposition d'induction en remplaçant K, K' et ϕ par $K(\alpha)$, $K'(\alpha')$ et $\phi(\alpha)$. Cela nous donne $\psi : L \to L'$ qui étend $\phi(\alpha)$. Puisque $\phi(\alpha)$ étend ϕ, on obtient que ψ étend ϕ aussi, ce qui conclut notre démonstration. □

Corollaire 4.3.5. *Le corps de décomposition de $f \in K[t]$ est unique à isomorphisme près.*

Démonstration. C'est le cas spéciale du Théorème 4.3.4 obtenu en prenant $K = K'$ et $\phi = Id_K$. □

En utilisant le Corollaire 4.3.5 on peut dire **le** corps de décomposition d'un polynôme sur un corps, au lieu d'**un** corps de décomposition. Il nous aussi permet de démontrer que chaque extension de degré fini est contenu dans **le** corps de décomposition. Plus précisément :

Corollaire 4.3.6. *Soit $K \subseteq L = K(\alpha_1, \ldots, \alpha_r)$ une extension de corps de degré fini engendré par $\alpha_1, \ldots, \alpha_r$, et soit $f \in K[x]$ un polynôme qui s'annule en α_i pour chaque entier $1 \leq i \leq r$, et soit M le corps de décomposition de f sur K. Dans ce cas, il existe un plongement $\iota : L \to M$ de K-algèbres.*

Démonstration. Soit F le corps de décomposition de f sur L, et soit $\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_s$ la liste complète des racines de f sur L. En particulier par point (1) du Lemme 4.3.3, $F = L(\alpha_1, \ldots, \alpha_s)$ et $M = K(\alpha_1, \ldots, \alpha_s)$. Cependant, la supposition $L = K(\alpha_1, \ldots, \alpha_r)$ nous dit que ces deux sont les mêmes, ou autrement dit $F = M$. □

Corollaire 4.3.7. *Soit f et g deux polynômes dans $K[x]$ et soit L le corps de décomposition de $f \cdot g$. Dans ce cas, L contient un unique sous-corps F qui est un corps de décomposition de f.*

Démonstration. Soient $\alpha_1, \ldots, \alpha_r$ les racines de f dans L. Par définition $K(\alpha_1, \ldots, \alpha_r)$ est un corps de décomposition de f, et de plus cela est la seule option. □

4.4 Corps finis

4.4.1 Dérivations (algébriques), et racines multiples

Pour continuer à découvrir la théorie des corps, on a besoin d'une étude soigneuse du lien entre les racine multiples est les dérivatives algébriques. Ce qui est particulièrement important pour la théorie, est de comprendre quelles notions et propositions dans cette directions sont indépendants du passage aux extensions des corps. Ce qui signifie que cette notions et propositions sont vrais sur K si et seulement si il sont vrai sur L pour une extension $K \subseteq L$. C'est vraiment important que ici on parle d'équivalence. La direction particulièrement importante pour la théorie est d'habitude de descendre les propriétés de L à K.

Définition 4.4.1. Si K es un corps, alors $\frac{\partial}{\partial x} \colon K[x] \to K[x]$ est l'application K-linéaire tel que $\frac{\partial}{\partial x}(t^n) = n \cdot t^{n-1}$ pour chaque entier $n \geq 0$ (où n est regardé en tant qu'un élément de K travers l'homomorphisme d'anneau unique $\mathbb{Z} \to K$).

Remarque 4.4.2. L'élément $n \in K$ de la Définition 4.4.1 est zéro si et seulement si soit $n = 0$, soit $\operatorname{car} K = p > 0$ et $p | n$. Par conséquent, pour $f \in K[x]$ on a :

(1) Si $\operatorname{car} K = 0$, alors $\frac{\partial}{\partial x}(f) = 0$ si et seulement si f est constant.
(2) Si $\operatorname{car} K = p > 0$, alors $\frac{\partial}{\partial x}(f) = 0$ si et seulement si $f = \sum_{i=0}^{n} a_i x^{ip}$ pour des $a_i \in k$.

Exemple 4.4.3. On a $\frac{\partial}{\partial x}(x^3 - 2) = 3x^2$ ce qui est non-zéro si et seulement si on travaille dans un corps de caractéristique différent que 3. Par exemple, il est non-zéro si on travaille dans $\mathbb{C}[x]$ ou dans $\mathbb{F}_p[x]$ pour $p \neq 3$. D'autre coté, il est zéro si on travaille dans $\mathbb{F}_3[x]$.

Lemme 4.4.4. *Si K est un corps, et si $f, g \in K[x]$ sont polynômes, alors $\frac{\partial}{\partial x}(f \cdot g) = f \cdot \frac{\partial}{\partial x}(g) + \frac{\partial}{\partial x}(f) \cdot g$.*

Démonstration. Puisque $\frac{\partial}{\partial x}$ est K-linéaire, il suffit de démontrer l'identité sur des monômes :

$$x^r \cdot \frac{\partial}{\partial x}(x^s) + \frac{\partial}{\partial x}(x^r) \cdot x^s = x^r \cdot s x^{s-1} + r x^{r-1} x^s = (r+s) x^{r+s-1} = \frac{\partial}{\partial x}(x^{r+s})$$

□

Exemple 4.4.5. Par exemple

$$\begin{aligned}\frac{\partial}{\partial x}\big((x-1)^2(x^2+x+1)\big) &= \frac{\partial}{\partial x}\big((x-1)^2\big)(x^2+x+1) + (x-1)^2 \frac{\partial}{\partial x}(x^2+x+1) \\ &= 2(x-1)(x^2+x+1) + (x-1)^2(2x+1),\end{aligned}$$

où quelques termes peuvent être zéro dépendant la caractéristique de corps sur lequel on travaille. Par exemple en caractéristique 2 le résultat et simplement $(x-1)^2 = (x+1)^2 = x^2 + 1$.

Remarque 4.4.6. Si $K \subseteq L$ est une extension de corps, et $f \in K[x]$ est un polynôme, alors on peut prendre $\frac{\partial}{\partial x}(f)$ dans deux façons différentes :

(1) on peut regarder f en tant qu'un polynôme dans $K[x]$ est on peut appliquer $\frac{\partial}{\partial x} : K[x] \to K[x]$, ou

(2) on peut regarder f en tant qu'un polynôme dans $L[x]$ est on peut appliquer $\frac{\partial}{\partial x} : L[x] \to L[x]$, ou

Par la Définition 4.4.1, c'est deux façons de calculer $\frac{\partial}{\partial x}(f)$ sont les mêmes.

Définition 4.4.7. Soient K un corps, $\alpha \in K$ un élément, et $f \in K[x]$ un polynôme. On dit que α est une *racine multiple* de f si $(x-\alpha)^2 \big| f$ dans $K[x]$.

Par la Remarque 4.4.9, la condition $(x-\alpha)^2 \big| f$ ne change pas si elle est pris sur une quelconque extension $K \subseteq L$. Autrement dit, la notion de α être une racine multiple de f est indépendante du passage à une telle extension. C'est la raison pour laquelle on dit simplement "α est une *racine multiple* de f", au lieu de "α est une *racine multiple* de f sur K".

Lemme 4.4.8. *Soient $K \subseteq L$ une extension des corps, et $f, g \in K[x]$ des polynômes. Dans ce cas le* $\operatorname{pgdc}(f,g)$ *calculé dans $K[x]$ est aussi un plus grand diviseur commun de f et g dans $L[x]$.*

Démonstration. Puisque tous les deux $K[x]$ est $L[x]$ sont des anneaux euclidien, on peut calculer $\operatorname{pgdc}(f,g)$ dans tous les deux en utilisant l'algorithme euclidien. Cependant, même si on travaille dans $L[x]$, puisque $f, g \in K[x]$ on peut exécuter l'algorithme dans une manière que l'on prend des polynômes dans $K[x]$ pour les résultats et pour les restes des divisions euclidiennes. Par conséquent, tout polynôme qui apparaît est dans $K[x]$. Ainsi, le résultat final est au même temps un $\operatorname{pgdc}(f,g)$ dans $L[x]$ et dans $K[x]$. □

Remarque 4.4.9. Dans la situation de la Définition 4.4.7, la condition $(x-\alpha)^2 \big| f$ est équivalent à la condition que $\operatorname{pgdc}\left((x-\alpha)^2, f\right) = (x-\alpha)^2$. Celle-ci est indépendant de choix de corps, ce qui veut dire que si $K \subseteq L$ est une extension de corps, alors par le Lemme 4.4.8

$$\operatorname{pgdc}\left((x-\alpha)^2, f\right) = (x-\alpha)^2 \text{ dans } K[x] \iff \operatorname{pgdc}\left((x-\alpha)^2, f\right) = (x-\alpha)^2 \text{ dans } L[x].$$

Ainsi, on obtient le même équivalence pour la condition de divisibilité :

$$(x-\alpha)^2 \big| f \text{ dans } K[x] \iff (x-\alpha)^2 \big| f \text{ dans } L[x].$$

Proposition 4.4.10. *Soient $K \subseteq L$ une extension des corps, $\alpha \in L$ un élément et $f \in K[x]$ un polynôme. Dans ce cas les suivantes sont équivalents :*

(1) α est une racine multiple de f,

(2) $f(\alpha) = 0 = \left(\frac{\partial}{\partial x}(f)\right)(\alpha) = 0$,

(3) $x - \alpha \big| \operatorname{pgdc}\left(f, \frac{\partial}{\partial x}(f)\right)$.

(Notons que toutes notions dans $\operatorname{pgdc}\left(f, \frac{\partial}{\partial x}(f)\right)$ *sont les mêmes si ils sont pris sur K ou sur L, par la Remarque 4.4.6 et par le Lemme 4.4.8).*

Démonstration. Par la Remarque 4.4.6 et par le Lemme 4.4.8, on peut prendre $\frac{\partial}{\partial x}$ et pgdc sur L dans cette preuve. Par conséquent toutes divisions de la preuve seront aussi pris dans $L[x]$. Dans ce cas, on a

$$x-\alpha \Big| \operatorname{pgdc}\left(f, \frac{\partial}{\partial x}(f)\right) \iff x-\alpha \big| f, \text{ et } x-\alpha \Big| \frac{\partial}{\partial x}(f) \iff \alpha \text{ et une racine de } f, \text{ et } x-\alpha \Big| \frac{\partial}{\partial x}(f)$$

Ainsi, on peut supposer que α est une racine de f, et alors il suffit de démontrer que

$$x - \alpha \Big| \frac{\partial}{\partial x}(f) \iff \alpha \text{ et une racine multiple de } f \tag{4.4.a}$$

Pour démontrer (4.4.a), écrivons $f = (x-\alpha)^m g$ tel que $(t-\alpha) \nmid g$. Puisque on a supposé que $f(\alpha) = 0$, on a $m \geq 1$, et

$$\frac{\partial}{\partial x}(f) = \frac{\partial}{\partial x}\big((x-\alpha)^m g\big) \underset{\uparrow}{=} (x-\alpha)^m \frac{\partial}{\partial x}(g) + m(x-\alpha)^{m-1} g$$

le Lemme 4.4.4 et la Définition 4.4.1

Puisque $m \geq 1$ on obtient que

$$x-\alpha \Big| \frac{\partial}{\partial x} \iff (x-\alpha) \big| m(x-\alpha)^{m-1} g \underset{\uparrow}{\iff} m = 0 \text{ dans } K, \text{ ou } m \geq 2 \underset{\uparrow}{\iff} m \geq 2$$

$x-\alpha \nmid g$

si $m = 0$ dans K, alors $0 < \operatorname{car} K \big| m$, où $\operatorname{car} K$ est un nombre premier $\implies m \geq 2$

Cela conclut la démonstration de la (4.4.a). □

Exemple 4.4.11. Par la Proposition 4.4.10, le polynôme $x^5 - 1 \in \mathbb{C}[x]$ n'a aucune racine double, parce que $\frac{\partial}{\partial x}(x^5-1) = 4x^4$ qui ne s'annule pas en aucune racine d'unité.

En effet, on peut déduire cette proposition sans utiliser la Proposition 4.4.10 : les racines de x^5-1 sont les racines cinquième d'unité. On connait déjà 5 distincte telle racine, qui donne cinq distinct irréductible polynômes linéaires dans la décomposition de x^5-1 en facteurs irréductible. Puisque $\deg x^5 - 1 = 5$ on ne peut pas avoir d'autre facteurs irréductibles, donc il n'y a pas non plus de racines multiples.

Corollaire 4.4.12. *Soient $K \subseteq L$ une extension des corps, et $f \in K[x]$ un polynôme* irréductible. *S'il y a une racine multiple de f dans L, alors $\frac{\partial}{\partial x}(f) = 0$.*

Démonstration. Dans cette preuve on prends tous les pgdc, les $\frac{\partial}{\partial x}$ et les division dan $K[x]$. On a deux conditions sur $g = \operatorname{pgdc}\left(f, \frac{\partial}{\partial x}(f)\right)$:

- Puisque f est irréductible, $g \in K[x]^\times$ ou $g \sim f$ dans $K[x]$.
- Par le point (3) de la Proposition 4.4.10, $g \notin K[x]^\times$.

On obtient que $g \sim f$, et par conséquent $\deg g = \deg f$. Cependant $\deg\left(\frac{\partial}{\partial x}(f)\right) < \deg f$. Ainsi, $\frac{\partial}{\partial x}(f) = 0$, parce que sinon $\deg g$ serait forcément plus grand que $\deg f$, ce qui serait une contradiction. □

Exemple 4.4.13. On a vu dans le point (1) de l'Exemple 4.2.27 que $x^2 + x + 1 \in \mathbb{F}_2[x]$ est irréductible. Puisque $\frac{\partial}{\partial x}(x^2+x+1) = 1 \neq 0$, on en déduit par le Corollaire 4.4.12, que le $x^2 + x + 1$ n'obtient aucune racine multiple dans son corps de décomposition.

En effet, puisque sur $\mathbb{F}_2$ on a $(x^2+x+1)(x-1) = x^3 - 1$, les racines de $x^2 + x + 1$ sont exactement les racines primitives troisième d'unité. On obtient qu'il existe deux différentes telles racines dans une extension adéquate de $\mathbb{F}_2$, un comportement similaire que l'on voit sur $\mathbb{Q}$.

4.4.2 Exposant d'un groupe abélien fini

Définition 4.4.14. Si, G est un groupe, alors *l'exposant* $\exp(G)$ de G est le plus petit entier positif m tel que $g^m = e$ pour chaque $g \in G$.

Proposition 4.4.15. *Si G est un groupe abélien fini d'ordre n, alors $\exp(G) \big| n$, et on a une égalité si et seulement si G est cyclique.*

Démonstration. Soit $n = \prod_{i=1}^r p_i^{d_i}$ la décomposition en facteurs premiers, et $G \cong \bigtimes_{i=1}^s \mathbb{Z}/n_i\mathbb{Z}$ la décomposition en facteurs cycliques donnée par le théorème fondamental de groupes abéliens

de type fini. On voit que

$$n = \prod_i^s n_i \qquad \exp(G) \underset{\uparrow}{=} \operatorname{ppmc}(n_1, \ldots, n_s) \tag{4.4.b}$$

la puissiance $\operatorname{ppmc}(n_1, \ldots, n_s)$-ième de chaque élément est $(e, \ldots, e)$, et de plus $o(g_1, \ldots, g_s) = \operatorname{ppmc}(n_1, \ldots, n_s)$ où g_i est un génératuer cyclique de $\mathbb{Z}/n_i\mathbb{Z}$

Par (4.4.b) il suit que $\exp(G)|n$. Pour démontrer la proposition concernant le cas d'égalité, notons que si G est cyclique, alors $\exp(G) = n$ trivialement. En particulier, il suffit de démontrer que si $\exp(G) = n$, alors G est cyclique. Par (4.4.b), si $\exp(G) = n$, alors les n_i sont premiers entre eux. Cependant, dans ce cas la formule $o(g_1, \ldots, g_s) = \operatorname{ppmc}(n_1, \ldots, n_s)$, où g_i est un générateur de $\mathbb{Z}/n_i\mathbb{Z}$, implique que G est cyclique. □

4.4.3 Le théorème fondamental des corps finis

Lemme 4.4.16. *Si $f \in K[x]$ est un polynôme sur un corps K, alors f a au plus $\deg f$ racines distinctes dans K.*

Démonstration. Si $\alpha_1, \ldots, \alpha_r$ sont des racines distinctes de K, alors $\prod_{i=1}^r (x - \alpha_i) \Big| f$, et alors $r \leq \deg f$. □

Théorème 4.4.17.
LES RESTRICTIONS SUR L'ORDRE DES CORPS FINIS :

(1) Soit $q > 0$ un nombre entier. Il existe un corps à q éléments si et seulement si q est une puissance d'un entier premier p.

L'UNICITÉ, ET LES PROPRIÉTÉS : *pour les points suivants, fixons une n-ième puissance $q = p^n$ d'un entier premier p.*

(2) Modulo isomorphisme, il existe un unique corps $\mathbb{F}_q$ à q éléments.
(3) $\mathbb{F}_q$ est le corps de décomposition du polynôme $x^q - x \in \mathbb{F}_p[x]$.
(4) Tout élément de $\mathbb{F}_q$ est une racine de $x^q - x \in \mathbb{F}_p[x]$, où $\mathbb{F}_p$ est identifié (canoniquement) avec le corps premier de $\mathbb{F}_q$.
(5) L'extension $\mathbb{F}_p \subseteq \mathbb{F}_q$ est simple, où $\mathbb{F}_p$ s'identifie canoniquement avec le corps premier de $\mathbb{F}_q$.
(6) On a l'isomorphisme $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$ des $\mathbb{F}_p$-algèbres pour un polynôme arbitraire irréductible $f \in \mathbb{F}_p[x]$ de degré n (quel polynôme existe, en particulier).
(7) On a l'isomorphisme des groupes $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

Démonstration.

F est un corps fini $\implies |F| = p^n$: Parce que F est fini, car $F \neq 0$. Par la Section 2.4.3, cela implique que $\operatorname{car} F = p > 0$, et que le corps premier K de F est isomorphe à $\mathbb{F}_p$ par l'application

$$K \ni \underbrace{1 + \ldots + 1}_{r\text{-fois}} \leftrightarrow r + p\mathbb{Z} \in \mathbb{F}_p$$

En particulier, F est un espace vectoriel sur $\mathbb{F}_p$. Parce que F lui même est fini, sa dimension sur $\mathbb{F}_p$ est aussi finie. Si $n = \dim_{\mathbb{F}_p} F$, alors on obtient que $|F| = p^n$.

Fixons d'ici jusqu'à la fin de la preuve un entier $n > 0$, un entier premier p, et mettons $p = q^n$.

Si un corps F à q éléments existe, alors tout élément de F est une racine de $x^q - x \in \mathbb{F}_p[x]$:

La groupe multiplicatif de F est un groupe d'ordre $q-1$. Puisque l'ordre d'éléments dans un groupe divise toujours l'ordre du groupe, on obtient que

$$\alpha \in K \setminus \{0\} \implies 1 = \alpha^{q-1} \implies \alpha = \alpha(\alpha^{q-1} - 1) = \alpha^q - \alpha$$

On obtient que chaque élément de $K \setminus \{0\}$ est une racine de $x^q - x$. De plus, puisque 0 est une racine aussi, on conclut que en effet chaque élément de K est une racine de $x^q - x$.

Dénotons d'ici jusqu'à la fin de la preuve le corps de décomposition de $x^q - x \in \mathbb{F}_p[x]$ sur $\mathbb{F}_p$ par L. Le point dernier nous montre que si un corps à q éléments existe, alors il est isomorphe à L. Cependant, pour àrriver à cette conclusion il faut encore démontrer les deux points suivants :

Tout élément L est une racine de $x^q - x \in \mathbb{F}_p[x]$: Soit E l'ensemble des racines de $x^q - x$. Par point (1) du Lemme 4.3.3 il suffit démontrer que E est un sous-corps de L. Cela est démontré dans les points suivants où $\alpha, \beta \in E$:

(1) $0 \in E$ parce que $0^q = 0$,
(2) $\alpha + \beta \in E$ par le calcul suivant :

$$(\alpha+\beta)^q \underset{\uparrow}{=} \alpha^q + \beta^q \underset{\uparrow}{=} \alpha + \beta$$

on est dans caractéristique $p > 0$; $\alpha, \beta \in E \implies \alpha^q = \alpha$ et $\beta^q = \beta$

(3) $-\alpha \in E$ par le calcul suivant :

$$(-\alpha)^q = (-1)^q\alpha^q \underset{\uparrow}{=} (-1)^q\alpha \underset{\uparrow}{=} -\alpha$$

$\alpha \in E \implies \alpha^q = \alpha$

Il y a deux possiblités
- si p est impair, alors q est impair, est par conséquent $(-1)^q = -1$
- si $p = 2$, alors $-1 = 1$ dans L, est par conséquent $(-1)^q = 1^q = 1 = -1$

(4) $1 \in E$ parce que $1^q = 1$,
(5) $\alpha\beta \in E$ parce que $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$.
(6) si $\alpha \neq 0$, alors $\alpha^{-1} \in E$ parce que $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$.

L contient q éléments : $\frac{\partial}{\partial x}(x^q - x) = 1$, qui veut dire par point (3) de la Proposition 4.4.10 que $x^q - x$ n'a pas des racine multiples dans L. Cependant $x^q - x$ scinde dans facteurs linéaires sur L, où chaque facteur linéaire $x - \alpha$ correspond à un élément $\alpha \in L$. En utilisant que $x^q - x$ n'a pas des racines multiples, et que chaque élément de L est une racine de $x^q - x$, on obtient que L contient exactement $\deg(x^q - x) = q$ éléments.

D'ici jusqu'à la fin de la preuve on introduit la notation $\mathbb{F}_q = L$.

$\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$: Sinon, par la Proposition 4.4.15, il existe un entier $r < q-1$ tel que $x^r = 1$ pour chaque $x \in \mathbb{F}_p^\times$. En particulier chaque élément de $x \in \mathbb{F}_q$ satisfait $x^{r+1} - x$. Cela signifie par Lemme 4.4.16 que $q \leq r + 1$, ce qui est une contradiction avec $r < q - 1$.

L'extension $\mathbb{F}_p \subseteq \mathbb{F}_q$ est simple : prenons un élément $\alpha \in \mathbb{F}_q^\times$ qui est une générateur en tant qu'un groupe multiplicatif. Parce $\mathbb{F}_q^\times$ est cyclique, chaque non-zéro élément de $\mathbb{F}_q$ est une puissance de α. Cela montre que $\mathbb{F}_p(\alpha) = \mathbb{F}_q$. □

Remarque 4.4.18. En particulier, Théorème 4.4.17 nous dit que les éléments non-zéros de $\mathbb{F}_q$ sont des racines $q-1$-ième d'unité.

Remarque 4.4.19. Le fait démontré dans le Théorème 4.4.17, que chaque corps à p^n éléments sont isomorphes, n'implique pas que les éléments de tel corps sont identifiés canoniquement. En fait, on peut identifier canoniquement dans deux copies de $\mathbb{F}_{p^n}$ exactement les éléments fixés par des automorphismes. On voit que les éléments de corps premier de $\mathbb{F}_{p^n}$ sont tel éléments, parce qu'ils sont de forme $1 + \ldots + 1$, et donc ils sont fixés par chaque automorphisme. On démontrera dans le point (6) de l'Exemple 4.6.4 que les éléments de corps premier sont les seuls éléments avec cette propriété.

En somme, le corps premier de $\mathbb{F}_{p^n}$ s'identifie canoniquement avec $\mathbb{F}_p$, et on ne peut pas désigné aucun autre élément de $\mathbb{F}_{p^n}$ canoniquement. Par exemple, les deux éléments de $\mathbb{F}_4 \setminus \mathbb{F}_2$ sont deux racines primitives troisièmes d'unité. On verra dans le point (6) de l'Exemple 4.6.4 que l'homomorphisme de Frobenius donne un automorphisme de $\mathbb{F}_4$ et ces deux éléments sont échangés par cet automorphisme. Autrement dit, quand on identifie deux corps avec 4 éléments, ces deux éléments peuvent être mélangés. D'autre coté, les éléments de corps premier ne peuvent pas être mélangés par telles identifications.

On note aussi que l'identification canonique de corps premier de $\mathbb{F}_{p^n}$ avec $\mathbb{F}_p$ implique que chaque homomorphisme de corps finis est un homomorphisme de $\mathbb{F}_p$-algèbres.

Exemple 4.4.20. On peut utiliser la méthode du point (1) de l'Exemple 4.2.27 de trouver les irréductibles sur $\mathbb{F}_p$. Les résultats dans quelques cas sont :

p	2	2	3
n	2	3	2
les irréductibles unitaires dans $\mathbb{F}_p[x]$ de degré n	x^2+x+1	$x^3+x^2+1,\ x^3+x+1$	$x^2+1,\ x^2+x+2,\ x^2+2x+2$

(4.4.c)

On obtient le cas $p = 2$ et $n = 3$ en calculant que les réductibles sont

$$x^3,\quad x^2(x+1) = x^3+x^2,\quad x(x+1)^2 = x^3+x,\quad (x+1)^3 = (x+1)(x^2+1) = x^3+x^2+x+1,$$
$$x(x^2+x+1) = x^3+x^2+x,\quad (x+1)(x^2+x+1) = x^3+1$$

et on obtient le cas $p = 3$ et $n = 2$ en en calculant que les réductibles sont

$$x^2,\quad x(x+1) = x^2+x,\quad x(x+2) = x^2+2x,\quad (x+1)(x+1) = x^2+2x+1,\quad (x+1)(x+2) = x^2+2,$$
$$(x+2)(x+2) = x^2+x+1$$

En trouvant les irréductibles de degré n sur $\mathbb{F}_p$, on obtient des descriptions de $\mathbb{F}_{p^n}$. Par point (6) du Théorème 4.4.17 et par le tableau (4.4.c) on a

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]\Big/(x^3+x^2+1) \cong \mathbb{F}_2[x]\Big/(x^3+x+1)$$

et

$$\mathbb{F}_9 \cong \mathbb{F}_3[x]\Big/(x^2+1) \cong \mathbb{F}_3[x]\Big/(x^2+x+2) \cong \mathbb{F}_3[x]\Big/(x^2+2x+2).$$

Notons que la classe à gauche de x dans ces représentations sont toujours générateurs de $\mathbb{F}_q$ en tant qu'un $\mathbb{F}_p$-algèbre. Cependant, ces éléments ne sont pas générateurs nécessairement du groupe multiplicatif $\mathbb{F}_q^\times$. Par exemple, l'ordre multiplicatif de $x + (x^2+1) \in \mathbb{F}_3[x]\Big/(x^2+1)$ est $4 \neq 8$.

Remarque 4.4.21. Il y aura un exercice dans la série, ce qui montrera que dehors de cas de $p = 2$ et $n = 2$ il y a plusieurs polynômes irréductibles de degré $n > 1$ dans $\mathbb{F}_p[x]$. Par conséquent, il n'y a pas une représentation canonique de $\mathbb{F}_{p^n}$ en tant qu'un quotient de $\mathbb{F}_p[x]$ pour $n \geq 2$ (sauf le cas $p = 2$ et $n = 2$). Cela connecte aux phénomènes expliqué dans la Remarque 4.4.19, ce qui nous dit que l'on ne peut pas désigné éléments de $\mathbb{F}_{p^n}$ canoniquement dehors de son corps premier.

Corollaire 4.4.22. *Soit $\mathbb{F}_{p^r}$, $\mathbb{F}_{p^s}$ deux corps finis. Alors, il existe un sous-corps de $\mathbb{F}_{p^s}$ isomorphe à $\mathbb{F}_{p^r}$, si et seulement si $r|s$. De plus, dans ce cas il existe un seul sous-corps de tel type.*

Démonstration.
$\boxed{\Longrightarrow :}$ Si on a un tel sous-corps, alors $\mathbb{F}_{p^s}$ est un $\mathbb{F}_{p^r}$-espace vectoriel. Par conséquent il existe un entier $n > 0$ tel que $p^s = (p^r)^n$, et ainsi $s = rn$, ou autrement dit $r|s$.
$\boxed{\Longleftarrow :}$ Notons premièrement que $\frac{p^s-1}{p^r-1} = l$ est un entier où $l = \sum_{i=0}^{\frac{s}{r}-1} p^{ir}$. En effet :

$$(p^r - 1)l = (p^r - 1)\left(1 + p^r + p^{2r} + \ldots + p^{(\frac{s}{r}-1)r}\right) = p^s - 1$$

Par conséquent $x^{p^s} - x$ est divisible par $x^{p^r} - x$ dans $\mathbb{F}_p[x]$:

$$x^{p^s} - x = x\left(x^{p^s-1} - 1\right) = x\left(x^{p^r-1} - 1\right)\left(\sum_{i=0}^{l-1} x^{i(p^r-1)}\right)$$

Par Corollaire 4.3.7, on obtient que le corps de décomposition $x^{p^s} - x$ sur $\mathbb{F}_p$ contient un unique sous-corps, ce qui est un corps de décomposition sur $\mathbb{F}_p$ de $x^{p^r} - x$. Cela conclut notre démonstration, en utilisant Théorème 4.4.17. □

Exemple 4.4.23. On a $\mathbb{F}_2 \subseteq \mathbb{F}_4$, et $\mathbb{F}_2 \subseteq \mathbb{F}_8$, mais $\mathbb{F}_4 \not\subseteq \mathbb{F}_8$. Tous ces corps sont contenu dans $\mathbb{F}_{64}$

La fin du 12. cours, le 04.05.2021.

4.5 Extensions simples, extensions séparables

Dans cette section on examine quand extensions de degré fini sont simples. On note qu'un générateur en tant que K-algèbre d'un extension simple $K \subseteq L$ est aussi appelé un élément primitif dans la littérature. C'est la source du nom du Théorème 4.5.9, qui est le théorème principal de cette section.

4.5.1 Les définitions

Exemple 4.5.1. Par le Théorème 4.4.17 et par le Corollaire 4.4.22, on sait que $\mathbb{F}_{p_1^r} \subseteq \mathbb{F}_{p_2^s}$ si et seulement si $p_1 = p_2$ et $r|s$, et dans ce cas l'extension et simple.

Définition 4.5.2. (1) Si K est un corps, alors un polynôme $f \in K[x]$ est *séparable* s'il obtient $\deg f$ racines distinctes dans son corps de décomposition.
(2) Soit $K \subseteq L$ une extension des corps. Un élément algébrique $\alpha \in L$ est *séparable sur* K, si $m_{\alpha,K} \in K[x]$ est séparable.
(3) Une extension algébrique $K \subseteq L$ des corps est *séparable*, si tout élément de L est séparable sur K.
(4) Un corps K est *parfait*, si toute extension algébrique $K \subseteq L$ est séparable.
(5) Un corps K est *imparfait*, si il n'est pas parfait.

En effet plusieurs points de la Définition 4.5.2 pourraient être donnés dans une forme alternative. C'est le sujet des deux lemmes suivants :

Lemme 4.5.3. *Pour un corps K, les propositions suivantes sont équivalentes :*
(1) K est parfait.
(2) Toute extension de degré fini $K \subseteq L$ est séparable.
(3) Toute extension simple algébrique $K \subseteq L$ est séparable.

(4) Tout polynôme irréductible $f \in K[x]$ est séparable.

Démonstration. Toute implication dans le cycle (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (1) est directe. □

Lemme 4.5.4. *Si K est un corps, et $f \in K[x]$ est un polynôme, alors les affirmations suivantes sont équivalentes :*

(1) f est séparable.
(2) f obtient $\deg f$ racines distinctes dans une certaine extension de K.
(3) f n'admet pas des racines multiples dans son corps de décompositions.
(4) Pour toute extension $K \subseteq L$ algébrique (resp. de degré fini), f n'admet pas des racines multiples dans L.

Démonstration. C'est une conséquence directe du Corollaire 4.3.6, du Corollaire 4.3.7 et de la Remarque 4.4.9. □

Exemple 4.5.5. On postule que tout corps fini est parfait. En fait, fixons un corps fini $K = \mathbb{F}_q$ avec $q = p^n$, et prenons un extension simple algébrique $K \subseteq L = K(\alpha)$. Soit $L \subseteq E$ le corps de décomposition de $m_{\alpha,K}$. Puisque E est aussi un corps fini, il existe un $0 < r \in \mathbb{Z}$ tel que $\alpha^{p^r} - \alpha = 0$ (Théorème 4.4.17). On obtient que $m_{\alpha,K} | x^{p^r} - x$. Ainsi, il suffit de démontrer que $x^{p^r} - x \in K[x]$ est séparable. Cela découle de la Proposition 4.4.10 en utilisant que $\frac{\partial}{\partial x} x^{p^r} - x = -1$.

Exemple 4.5.6. Le corps $K = F(t)$ est imparfait pour quelconque corps F de caractéristique $p > 0$. En effet, prenons l'extension des corps $K \subseteq L = K(\alpha)$ où α est une racine de polynôme irréductible $x^p - t \in K[x]$ (on peut voir que ce polynôme est irréductible par le Proposition 3.8.13 et la Proposition 3.9.3). Par conséquent $[L : K] = p$ est on a dans $L[x]$ la factorisation :

$$(x - \alpha)^p = x^p - \alpha^p = x^p - t.$$

On voit, que en effet L est le corps de décomposition de $x^p - t$, et que ce polynôme obtient juste une racine, mais avec multiplicité p dans L. On en déduit que K est imparfait.

4.5.2 La caractérisation des corps parfaits

Proposition 4.5.7. CARACTÉRISATION DES CORPS PARFAITS. *Pour un corps K les propositions suivantes sont équivalents :*

(1) K est parfait.
(2) Si $f \in K[x]$ est un polynôme irréductible, alors $\frac{\partial}{\partial x}(f) \neq 0$.
(3) Une des conditions suivantes sont satisfaites :
  (i) $\operatorname{car} K = 0$.
  (ii) $\operatorname{car} K = p$ et $K^p = K$.

Démonstration.

(2) $\implies$ (1) : Si K est imparfait, alors le point (4) du Lemme 4.5.3 donne un polynôme irréductible $f \in K[x]$ qui obtient des racines multiples sur son corps de décomposition L. Par le Corollaire 4.4.12, il suit que $\frac{\partial}{\partial x}(f) = 0$.

(1) $\implies$ (2) : Supposons que K et parfait et prenons un polynôme irréductible $f \in K[x]$ tel que $\frac{\partial}{\partial x}(f) = 0$. Puisque être irréductible implique que f n'est pas inversible, on a $\deg f > 0$. En utilisant Remarque 4.4.2 on voit que $\operatorname{car} K = p > 0$, et $f = \sum_{i=0}^{r} a_i x^{ip}$ pour des $a_i \in K$. Cela

implique par le point (4) du Lemme 4.5.3 que K est imparfait : sur le corps de décomposition L de $\prod_{i=1}^{r}(x^p - a_i)$ on a des éléments β_i tels que $\beta_i^p = \alpha_i$, et par conséquent on a

$$\left(\sum_{i=0}^{r} \beta_i x^i\right)^p = \sum_{i=0}^{r} \beta_i^p x^{ip} = f$$

Par conséquent après passer au corps de décomposition de $\sum_{i=0}^{r} \beta_i x^i$ sur L, on voit que chaque racine de f a multiplicité au moins p sur ce dernier corps.

Si $\operatorname{car} K = 0$*, alors* K *est parfait :* C'est une conséquence directe de l'équivalence (1) $\iff$ (2) déjà montré (c.f., la Remarque 4.4.2).

Par conséquent, on suppose d'ici jusqu'à la fin de la preuve que $\operatorname{car} K = p > 0$.

(1) $\implies$ *(3) :* Si, $K^p \neq K$, alors on peut prendre $\alpha \in K \setminus K^p$. Prenons le corps de décomposition L de $x^p - \alpha$. On obtient $\beta \in L \setminus K$ (si β était contenu dans K alors α serait dans K^p), tel que $\beta^p = \alpha$. Par conséquent on a $m_{\beta,K} | x^p - \alpha = (x - \beta)^p$. Puisque $\deg m_{\beta,K} > 1$, on en déduit que $m_{\beta,K}$ n'est pas séparable, est par conséquent, K est imparfait.

(3) $\implies$ *(2) :* Supposons que $K^p = K$, et prenons un polynôme irréductible $f \in K[x]$ tel que $\frac{\partial}{\partial x} f = 0$. Par la Remarque 4.4.2 on a que $f = \sum_{i=0}^{r} a_i x^{ip}$. Dans ce cas, puisque $K^p = K$, on a $\beta_i \in K$ tels que $\beta_i^p = a_i$. En répétant l'argument de l'implication (1) $\implies$ (2), on voit que f est une puissance p-ième d'un autre polynôme qui est une contradictions avec l'irréductibilité de f.

□

Exemple 4.5.8. On peut redémontrer l'affirmation de l'Exemple 4.5.6, que $K = F(t)$ est imparfait pour quelconque corps F de caractéristique $p > 0$. En effet $K^p = F(t^p) \subsetneq F(t)$.

4.5.3 Le théorème de l'élément primitif

Théorème 4.5.9. THÉORÈME DE L'ÉLÉMENT PRIMITIF. *Toute extension séparable et de degré fini des corps $K \subseteq L$ est simple.*

Démonstration. Par l'Exemple 4.5.1 on peut supposer que $|K| = \infty$.

Puisque $[L : K] < \infty$, on peut écrire $L = K(\alpha_1, \ldots, \alpha_n)$ pour les éléments séparables α_i. On démontre la proposition par récurrence sur n. Si $n = 1$, alors il y a rien à démontrer. Ainsi, on suppose que $n > 1$ et que l'on connait la proposition pour les plus petites valeurs de n. Cela implique que l'on a $K \subseteq K(\alpha_1, \ldots, \alpha_{n-1}) = K(\delta)$. Autrement dit, on a $L = K(\delta, \alpha_n)$, et donc on peut supposer que $n = 2$. Pour éviter d'écrire des sous-indices, on écrit $\alpha = \alpha_1$ et $\beta = \alpha_2$, et donc on a $L = K(\alpha, \beta)$

On cherche γ tel que $K(\gamma) = L$, parmi les éléments de forme $c\alpha + \beta$ pour $c \in K$. Notons que la condition $K(\gamma) = L$ est équivalent à la condition $\alpha \in K(\gamma)$ (parce que dans ce cas $\beta = \gamma - c\alpha \in K(\gamma)$ aussi), ce qui à son tour est équivalent de dire que $\deg m_{\alpha,K(\gamma)} = 1$. Par conséquent, il suffit de démontrer qu'il existe un sous-ensemble fini $S \subseteq K$ tel que pour chaque $c \in K \setminus S$ et pour $\gamma = c\alpha + \beta$ on a $\deg m_{\alpha,K(\gamma)} = 1$.

Mettons $\gamma = c\alpha + \beta$ pour $c \in K$ quelconque pour le moment. Notre but et de trouver un S avec des propriétés demandées ci-dessus. Pour les notations plus faciles introduisons $f = m_{\alpha,K}$ et $g = m_{\beta,K}$. Observons que $h(x) = g(\gamma - cx) \in \big(K(\gamma)\big)[x]$, et que puisque $h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$, le polynôme h s'annule en α. Puisque tous les deux $f, h \in \big(K(\gamma)\big)[x]$ s'annulent en α, le $\operatorname{pgdc}(f, h) \in \big(K(\gamma)\big)[x]$ s'annule en α aussi.

Soit E le corps de décomposition de $f \cdot g$ (qui contient L), et soient $\alpha = \alpha_1, \ldots, \alpha_r \in E$ les racines de f et $\beta = \beta_1, \ldots, \beta_s \in E$ les racines de g. Dans ce cas, en supposant que $c \neq 0$, on voit que les éléments suivants de L donne la liste complète des racines de h :

$$\alpha'_j = \frac{\gamma - \beta_j}{c} = \alpha + \frac{\beta - \beta_j}{c}. \tag{4.5.a}$$

parce que

$$\prod_{j=1}^{s}(x-\alpha'_j)=\prod_{j=1}^{s}\left(x-\frac{\gamma-\beta_j}{c}\right)\sim\prod_{j=1}^{s}(cx-\gamma+\beta_j)\sim\prod_{j=1}^{s}\big((\gamma-cx)-\beta_j\big)\sim g(\gamma-cx)=h(x)$$

Notons aussi que par notre supposition f est un polynôme séparable, et par conséquent α n'est pas une racine multiple de f. De plus, notons que $\alpha'_1=\alpha+\frac{\beta-\beta}{c}=\alpha$. On en déduit que $x-\alpha|\operatorname{pgdc}(f,h)$, et on a égalité, si α et la seule racine commune de f et h.

En somme, le choix suivant pour S serait satisfaisant, si on démontrait qu'il est un ensemble fini :

$$\begin{aligned}
S&=\{0\}\cup\left\{\ c\in K\setminus\{0\}\ \middle|\ \deg\operatorname{pgdc}(f,h)>1\ \right\}\\
&=\{0\}\cup\left\{\ c\in K\setminus\{0\}\ \middle|\ \exists 2\le i\le r,\ 1\le j\le s:\ \alpha_i=\alpha'_j\ \right\}\\
&\underset{\uparrow}{=}\{0\}\cup\left\{\ c\in K\setminus\{0\}\ \middle|\ \exists 2\le i\le r,\ 2\le j\le s:\ \alpha_i=\alpha'_j\ \right\}\\
&\qquad\boxed{\forall i\neq 1:\ \alpha_i\neq\alpha'_1,\text{ parce que }\alpha'_1=\alpha=\alpha_1}\\
&\underset{\uparrow}{=}\{0\}\cup\left\{\ c\in K\setminus\{0\}\ \middle|\ \exists 2\le i\le r,\ 2\le j\le s:\ \alpha_i=\alpha+\frac{\beta-\beta_j}{c}\ \right\}\\
&\qquad\boxed{\text{par (4.5.a)}}\\
&\underset{\uparrow}{=}\{0\}\cup\left\{\ \frac{\beta-\beta_j}{\alpha_i-\alpha}\in K\ \middle|\ 2\le i\le r,\ 2\le j\le s\ \right\}\\
&\qquad\boxed{\text{puisque }K\subseteq L\text{ est séparable, }\alpha\neq\alpha_i\text{ pour }2\le i\le r}
\end{aligned}$$

Le dernier ensemble ci-dessus et fini, ce qui finit notre démonstration.

□

4.6 La théorie de Galois

4.6.1 Le groupe de Galois

On rappelle que les homomorphismes de corps sont simplement les homomorphismes d'anneaux. En particulier, pour un corps K, on dénote par $\operatorname{Aut}(K)$ est le groupe d'automorphismes de corps $K\to K$ (ou homomorphismes d'anneaux de manière équivalente), avec l'opération donné par la composition, et id_K pour l'élément neutre.

Si $K\subseteq L$ est une extension de corps, alors, le groupe de K-automorphismes de L

$$\operatorname{Aut}_K(L)=\left\{\ \sigma\in\operatorname{Aut}(L)\ \middle|\ \sigma|_K=\mathrm{id}_K\ \right\}$$

est un sous-groupe de $\operatorname{Aut}(L)$. Pour une extension quelconque, ce groupe peut être énorme et non particulièrement utile pour comprendre la structure de l'extension. Par exemple, on ne le démontre pas dans ce cours, mais il est connu, que le groupe de Cremona $\operatorname{Aut}_{\mathbb{C}}\mathbb{C}(x,y)$ n'est pas même finiment engendré. En particulier ce groupe est plutôt intéressant pour la géométrie algébrique et pour la théorie de groupe, que pour la théorie de corps.

Cependant $\operatorname{Aut}_L(K)$ s'avère d'être essentiel pour comprendre les extension $K\subseteq L$ algébrique, dans lequel cas on le donne un nome particulier :

Définition 4.6.1. Si $K\subseteq L$ est une extension algébrique, alors on appelle $\operatorname{Aut}_K(L)$ le *groupe de Galois*, et on le dénote par $\operatorname{Gal}(L/K)$.

Exemple 4.6.2. Si K est un corps de caractéristique $p>0$, alors $\operatorname{Gal}(K/K^p)\cong 1$, où 1 dénote le groupe avec un élément. Autrement dit, $\operatorname{Gal}(K/K^p)=\{\mathrm{id}_K\}$. Pour cela, fixons $\alpha\in K$ et

$\phi \in \mathrm{Gal}(K/K^p)$. Il suffit de démontrer que $\phi(\alpha) = \alpha$. Puisque $x^p - \alpha^p = (x-\alpha)^p$, l'élément $\alpha \in K$ est l'unique racine p-ième de α^p. Par conséquent, il suffit de démontrer que $\big(\phi(\alpha)\big)^p = \alpha^p$:

$$\big(\phi(\alpha)\big)^p \underset{\uparrow}{=} \phi(\alpha^p) \underset{\uparrow}{=} \alpha^p.$$

$\boxed{\phi \text{ est un homomorphisme}}$ $\boxed{\phi \in \mathrm{Gal}(K/K^p) \implies \phi|_{K^p} \text{ par la Définition 4.6.1}}$

Proposition 4.6.3. FAITS FONDAMENTAUX SUR LE GROUPE DE GALOIS. *Soient $K \subseteq L$ une extension de corps algébrique, $\alpha, \alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_n \in L$ des éléments, $f \in K[x]$ un polynôme, et $\sigma \in \mathrm{Gal}(L/K)$ un automorphisme.*

(1) Si $\alpha \in L$ est une racine de f, alors $\sigma(\alpha)$ est aussi une racine de f. En particulier, $\mathrm{Gal}(L/K)$ agit sur l'ensemble des racines de f dans L.

(2) Si $L = K(\alpha_1, \dots, \alpha_n)$, alors il existe au plus un $\tau \in \mathrm{Gal}(L/K)$ tel que $\tau(\alpha_i) = \alpha'_i$ pour tout $i = 1, \dots, n$. En particulier, si $\alpha_1, \dots, \alpha_n$ sont les racines de f, alors $\mathrm{Gal}(L/K)$ agit fidèlement sur $\{\alpha_1, \dots, \alpha_n\}$ (autrement dit l'homomorphisme $\mathrm{Gal}(L/K) \to S_n$ est injectif).

(3) Si L est le corps de décomposition de f, alors $m_{\alpha,K}$ scinde sur L, et $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de $m_{\alpha,K}$.

(Les extensions des corps pour lesquelles tout $m_{\alpha,K}$ scinde sont appelé les extensions normales *dans la littérature.)*

(4) Si L est le corps de décomposition de f, et $\alpha_1, \dots, \alpha_n \in L$ sont éléments séparables sur K tel que $L = K(\alpha_1, \dots, \alpha_n)$, alors $|\mathrm{Gal}(L/K)| = [L : K]$.

(Les α_i ne sont pas nécessairement des racines de f. Cependant si f est lui même séparable, alors on peut choisir les racines de f pour les α_i.)

Démonstration. (1) Si $\xi : L[x] \to L[x]$ est l'homomorphisme induit par $\sigma : L \to L$, alors

$$f\big(\sigma(\alpha)\big) \underset{\uparrow}{=} \big(\xi(f)\big)\big(\sigma(\alpha)\big) \underset{\uparrow}{=} \sigma\big(f(\alpha)\big) \underset{\uparrow}{=} 0$$

$\boxed{f \in K[x] \text{ et } \xi|_{K[x]} = \mathrm{id}_{K[x]}}$ $\boxed{\xi \text{ est induit de } \sigma}$ $\boxed{f(\alpha) = 0}$

(2) L est engendré par les α_i.

(3) Soit E le corps de décomposition de $f \cdot m_{\alpha,K}$. Soient $\beta_1, \dots, \beta_r$ les racines de f dans E et $\alpha = \gamma_1, \dots, \gamma_s$ les racines de $m_{\alpha,K}$ dans E. On a $K(\beta_1, \dots, \beta_r) = L$.

Par Corollaire 4.2.23, pour chaque $1 \le j \le s$ il existe un isomorphisme $\sigma_j^{\mathrm{pre}} \colon K(\alpha) \xrightarrow{\cong} K(\gamma_j)$ qui envoie α sur γ_j, et qui fixe K. De plus par Théorème 4.3.4 on obtient que pour chaque $1 \le j \le s$, l'isomorphisme σ_j^{pre} étend à un automorphisme σ_j de E. Par point (1), σ_j permute les β_i. On obtient que $\sigma_j(L) \subseteq L$ pour chaque $1 \le j \le s$. En utilisant que σ_j est un isomorphisme K-linéaire, et $\dim_K L < \infty$, on en déduit que $\sigma_j(L) = L$. Par conséquent :

- Pour chaque $1 \le j \le s$, on a $\sigma_j(\alpha) = \gamma_j \in L$ parce que $\alpha \in L$ et $\sigma_j(L) = L$. Ainsi, $m_{\alpha,K}$ scinde sur L.
- Les application $\sigma_i|_L$ donne des éléments de $\mathrm{Gal}(L/K)$. En particulier $\mathrm{Gal}(L/K)$ agit transitivement sur γ_j.

(4) On démontre la proposition par récurrence sur $[L : K]$. Si $[L : K] = 1$ il y a rien a démontrer. Ainsi, on suppose que $[L : K] > 1$, et que pour les valeurs plus petites de $[L : K]$ on connait l'affirmation.

On peut supposer que $\alpha_1 \notin K$ (sinon, on l'échange avec un $\alpha_i \notin K$ qui existe par la supposition que $[L : K] > 1$). Introduisons les notations $\alpha = \alpha_1$.

Notons que L est aussi le corps de décomposition de f sur $K(\alpha)$, et de plus on a

$$\underset{\text{Proposition 4.2.15}}{\big[L : K(\alpha)\big]} = \frac{[L : K]}{\big[K(\alpha) : K\big]} \underset{[K(\alpha):K]>1}{<} [L : K] \tag{4.6.a}$$

Ainsi, on a

$$\underset{\alpha \notin K}{[L : K]} \underset{\text{(4.6.a) et l'hypothèse d'induction}}{>} [L : K(\alpha)] = \Big|\operatorname{Gal}\big(L/K(\alpha)\big)\Big| = \operatorname{Stab}_{\operatorname{Gal}(L/K)}(\alpha) \tag{4.6.b}$$

$\operatorname{Gal}\big(L/K(\alpha)\big)$ contient les éléments de $\operatorname{Gal}(L/K)$ qui stabilise chaque élément de $K(\alpha)$, qui sont éxactement des éléments de $\operatorname{Gal}(L/K)$ qui stabilise α, parce que les éléments de $\operatorname{Gal}(L/K)$ stabilisent K de toute façon, et si ils stabilisent α, alors ils stabilisent forcément chaque élément dans le sous-anneau engendré par α

De plus par point précédent, et par la séparabilité de α sur K, on obtient que l'orbite de α par $\operatorname{Gal}(L/K)$ est $\deg m_{\alpha,K} = [K(\alpha) : K]$. Le calcul suivant conclut notre démonstration :

$$\operatorname{Gal}(L/K) \underset{\text{le théorème d'orbite-stabilisateur}}{=} \big|\text{l'orbite de } \alpha \text{ sur } \operatorname{Gal}(L/K)\big| \cdot \big|\operatorname{Stab}_{\operatorname{Gal}(L/K)}(\alpha)\big|$$

$$\underset{\text{(4.6.b) et le paragraphe précédent}}{=} \big[K(\alpha) : K\big] \cdot \big[L : K(\alpha)\big] \underset{\text{Proposition 4.2.15}}{=} [L : K]$$

□

Exemple 4.6.4. (1) Trouvons $G = \operatorname{Gal}(L/K)$ pour $K = \mathbb{R}$ est $L = \mathbb{C}$. On achèvera notre but en utilisant les points de la Proposition 4.6.3 de la Proposition 4.6.3. Notons que le polynôme irréductible $x^2 + 1 \in \mathbb{R}[x]$ à deux racines distinctes dans $\mathbb{C}$, les éléments i et $-i$. Par point (1) de la Proposition 4.6.3, chaque élément de G envoi i sur i ou sur $-i$. De plus, en utilisant point (2) de la Proposition 4.6.3 et que $\mathbb{C} = \mathbb{R}(i)$, on obtient que il existe au plus un tel élément pour chaque possibilité. Cependant, par point (4) de la Proposition 4.6.3 et par le fait que $\mathbb{C}$ est le corps de décomposition de polynôme séparable x^2+1, on a $|G| = 2$. Ainsi, on a exactement un élément de G qui envoie i sur i, le $\mathrm{id}_{\mathbb{C}}$, et un autre élément qui envoi i sur $-i$, appelons-le σ. En somme, $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$. Puisque σ est une application $\mathbb{R}$-linéaire, on a $\sigma(a + bi) = a - bi$, ou autrement dit σ est la conjugaison habituelle.

On note que par généralisation, beaucoup fois les éléments des groupes de Galois sont aussi appelés des conjugaisons. Cela peut causer confusion, mais c'est une pratique répandu dans la littérature. Par la même raison, les éléments dans un orbite du groupe de Galois sont appelé les conjugués d'un l'autre.

(2) Par un argument similaire au point précédent on peut démontrer que $\operatorname{Gal}\big(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\big) \cong \mathbb{Z}/2\mathbb{Z}$, et pour l'élément $\sigma \neq \mathrm{id}$ de ce groupe de Galois on a $\sigma\big(a + b\sqrt{2}\big) = a - b\sqrt{2}$ pour chaque $a, b \in \mathbb{Q}$.

(3) Soit $L = \mathbb{Q}\big[\sqrt{2}, i\big]$ et $K = \mathbb{Q}$. Dans une façon similaire aux points précédents on voit que $G = \operatorname{Gal}(L/K)$ envoyé $\sqrt{2}$ sur $-\sqrt{2}$ (ils sont les racines de x^2-2), et i est envoyé sur $-i$ (ils sont les racines de x^2+1). Cela donne 4 possibilités. Par points (2) de la Proposition 4.6.3 on voit, que il y a au plus 1 élément de G pour chaque de ces 4 possibilités. An ce point on combine beaucoup des faits et résultats précédents pour démontrer que $|G| = 4$, et par conséquent toutes les 4 possibilité réalise :

(i) L le corps de décomposition de $(x^2+1)(x^2-2)$
(ii) K et un corps parfait par la Proposition 4.5.7, et par conséquent $K \subseteq L$ est séparable
(iii) $[L:K] = 4$ par le point (1) l'Exemple 4.2.16
(iv) par point (4) de la Proposition 4.6.3, $|G| \geq 4$.

Dénotons σ et $\tau \in G$ les éléments pour lesquels

$$\sigma(i) = i,\ \sigma\left(\sqrt{2}\right) = -\sqrt{2} \qquad \tau(i) = -i,\ \tau\left(\sqrt{2}\right) = \sqrt{2}$$

On voit, que $\sigma\tau = \tau\sigma$ parce que tous les deux envoi i sur $-i$ et $\sqrt{2}$ sur $-\sqrt{2}$ (on utilise point (2) de la Proposition 4.6.3 ici). Dans la manière similaire on peut démontrer que $\sigma^2 = \mathrm{id}_L$ et $\tau^2 = \mathrm{id}_L$. On obtient que $\mathrm{Gal}\left(\mathbb{Q}\left[\sqrt{2}, i\right], \mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(4) Dans une manière similaire, $G = \mathrm{Gal}\left(\mathbb{Q}\left[\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}\right], \mathbb{Q}\right)$ permute l'ensemble $\left\{\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}, e^{\frac{4\pi i}{3}}\sqrt[3]{2}\right\}$, et par point (2) de la Proposition 4.6.3 il y a que un élément de G qui réalise chaque permutation. Autrement dit, G est un sous-groupe de S_3. Par point (2) de l'Exemple 4.2.16, et par la Proposition 4.5.7, $|G| = 6$, et par conséquent on obtient $G = S_3$.

(5) L'argument de point précédent en effet marche pour chaque corps de décomposition L de chaque polynôme séparable $f \in K[x]$ sur K. Cela veut dire que si $\alpha_1, \ldots, \alpha_r$ sont des racines de f dans L, alors l'action de $\mathrm{Gal}(L/K)$ sur $\{\alpha_1, \ldots, \alpha_r\}$ donne un plongement de $\mathrm{Gal}(L/K)$ dans S_r.

(6) Considérons la situation de l'extension $K = \mathbb{F}_p \subseteq \mathbb{F}_q = L$, où $q = p^n$. Par le Théorème 4.4.17, cette extension est un corps de décomposition, et au même temps elle est une extension simple. En utilisant le point (4) de la Proposition 4.6.3, on obtient que $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$.

Si on trouve un $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ d'ordre au moins n alors on a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z} = \langle\sigma\rangle$. On postule que l'homomorphisme Frobenius $F : \mathbb{F}_q \ni \alpha \mapsto \alpha^p \in \mathbb{F}_q$ est un tel σ.

- F *est injectif :* il est un endomorphisme d'un corps.
- F *est surjectif :* fixons $\alpha \in \mathbb{F}_q$. Par le Théorème 4.4.17 on sait que $\alpha^{p^n} = \alpha$. Alors, $F\left(\alpha^{p^{n-1}}\right) = \alpha^{p^n} = \alpha$.
- $o(F) = n$ *:* soit $\beta \in \mathbb{F}_q$ un générateur cyclique de $\mathbb{F}_q^\times$, qui existe par le Théorème 4.4.17. On voit que le plus petit entier positif i tel que $F^i(\beta) = \beta^{p^i}$ est égal à β est $i = n$.

On obtient que $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle F\rangle$ et que tout élément de $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ sont de forme $F^i : \mathbb{F}_q \ni \alpha \mapsto \alpha^{p^i} \in \mathbb{F}_q$.

Corollaire 4.6.5. *Si $K = L(\alpha_1, \ldots, \alpha_r)$ est un corps de décomposition de quelconque polynôme $f \in K[x]$, alors K est aussi le corps de décomposition de $\prod_{i=1}^r m_{\alpha_i, K}$.*

Démonstration. C'est une conséquence directe du point (3) de la Proposition 4.6.3. □

Corollaire 4.6.6. *Les facteurs irréductibles de $x^{p^n} - x \in \mathbb{F}_p[x]$ sont exactement les irréductibles de degré divisant n, chaque avec multiplicité* 1.

Démonstration. Soit f un irréductible de degré d dans $\mathbb{F}_p[x]$. Puisque $\mathbb{F}_p$ est parfait (Exemple 4.5.5), f est séparable. De plus, l'extension $\mathbb{F}_p \subseteq L = \mathbb{F}_p[x]/(f)$ est un corps fini à p^d éléments.

Si $f | x^{p^n} - x$, alors f scinde sur $\mathbb{F}_{p^n}$ (point (3) de la Proposition 4.6.3). Cela veut dire, par le Corollaire 4.3.6 que L est isomorphe à un sous-corps de $\mathbb{F}_{p^n}$, qui implique que $d|n$ par le Corollaire 4.4.22.

Dans l'autre direction, supposons que $d|n$. Par Corollaire 4.4.22 on obtient que L isomorphe à un sous-corps de $\mathbb{F}_{p^n}$. Par point (3) e la Proposition 4.6.3, on obtient que f scinde sur $\mathbb{F}_{p^n}$. Ainsi,

en utilisant le Théorème 4.4.17, toutes les racines de f sont racines de $x^{p^n} - x$. Cela implique que f est un produit des facteurs irréductibles de $x^{p^n} - x$ sur $\mathbb{F}_{p^n}$. On obtient que $f | x^{p^n} - x$ sur $\mathbb{F}_{p^n}$, qui implique que $f | x^{p^n} - x$ sur $\mathbb{F}_p$, par le Lemme 4.4.8. L'affirmation additionelle que f divise $x^{p^n} - x$ avec multiplicité 1, ou autrement dit $f^2 \nmid x^{p^n} - x$, suit directement du fait que $x^{p^n} - x$ est séparable sur $\mathbb{F}_p$ parce que $\frac{\partial}{\partial x}(x^{p^n} - x) = -1$.

□

Exemple 4.6.7. Exemples de Corollaire 4.6.6 sont des formulas des produits suivants. On les obtient en utilisant la liste d'irréductibles de l'Exemple 4.4.20 :

$$x^4 - x = x(x-1)(x^2 + x + 1) \in \mathbb{F}_2[x]$$

$$x^8 - x = x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1) \in \mathbb{F}_2[x]$$

$$x^9 - x = x(x-1)(x-2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 1) \in \mathbb{F}_3[x]$$

4.6.2 Extensions galoisiennes

Définition 4.6.8. Soient $K \subseteq L$ une extension, et G un sous-groupe de $\mathrm{Aut}_K(L)$. Notons que $\mathrm{Aut}(L) = \mathrm{Aut}_E(L)$, où E est le corps premier de L, et alors cette généralité inclut le cas de quelconque sous-groupe de $\mathrm{Aut}(L)$ aussi.

(1) Un *corps intermédiaire* de cette extension est un sous-corps de L tel que $K \subseteq F \subseteq L$.
(2) Le *corps fixé* de G est

$$L^G = \{\ \alpha \in L \mid \forall \sigma \in G :\ \sigma(\alpha) = \alpha\ \}$$

Nous laissons en exercice la vérification que c'est un corps intermédiaire (il découle de fait que les σ sont homomorphismes).
(3) Une extension de corps $K \subseteq L$ est *galoisienne* si elle est algébrique et $L^{\mathrm{Gal}(L/K)} = K$.

Exemple 4.6.9. En utilisant la descriptions explicites des groupes de Galois dans l'Exemple 4.6.4, on voit que les extensions des points (1), (2) et (3) de l'Exemple 4.6.4 sont galoisienne.

On démontre une description précise du polynôme minimal dans l'extension galoisiennes :

Proposition 4.6.10. *Soient L un corps, $G \subseteq \mathrm{Aut}(L)$ un sous-groupe, $K = L^G$, et $\alpha \in L$ un élément. Considérons une des situations suivantes*

- *G est fini, ou*
- *$K \subseteq L$ est algébrique.*

Dans tous les deux cas on a :

(1) La G-orbite de α est finie : $\{\alpha = \alpha_1, \ldots, \alpha_r\}$.
(2) α est algébrique sur K,
(3) α est séparable sur K,
(4) $m_{\alpha,K} = \prod_{i=1}^{r}(x - \alpha_i)$
(5) Si $|G|$ est finie, alors $[K(\alpha) : K] \big| |G|$.

Démonstration. Soit $f = \prod_{i=1}^{r}(x - \alpha_i) \in L[x]$.

Point (1) : Si G est fini, alors l'orbite est finie automatiquement. Ainsi, on peut supposer que l'on est dans l'autre cas. Cela veut dire que $K \subseteq L$ est algébrique, mais G peut-être infini. Cependant, par point (1) de la Proposition 4.6.3, la G-orbite de α peut contenir juste les racines de $m_{\alpha,K}$. Par conséquent, cette orbite contient au plus $\deg m_{\alpha,K}$ éléments.

$f \in K[x]$: Cela découle de la supposition $K = L^G$ par l'argument suivant. Fixons $\sigma \in G$ et

soit $\xi : L[x] \to L[x]$ l'homomorphisme induit par $\sigma : L \to L$. Puisque σ permute les α_i, ou autrement dit il envoie α_i sur $\alpha_{\pi(i)}$ pour un $\pi \in S_r$, on obtient que :

$$\xi(f) = \xi\left(\prod_{i=1}^{r}(x-\alpha_i)\right) \underset{\uparrow}{=} \prod_{i=1}^{r}\xi\left(x-\alpha_i\right) = \prod_{i=1}^{r}(x-\sigma(\alpha_i)) = \prod_{i=1}^{r}(x-\alpha_{\pi(i)}) \underset{\uparrow}{=} f.$$

ξ est un homomorphisme

les $\alpha_{\pi(i)}$ sont les mêmes que les α_i juste ordonnés différémment

Puisque cela est vrai pour chaque $\sigma \in \mathrm{Gal}(L/K)$ et $L^G = K$, on obtient que $f \in K[x]$.

Point (2) : C'est une supposition dans un des cas. Dans l'autre cas, α est une racine de f, qui est un polynôme non-nul sur K par le paragraphe précédent.

Point (4) : Par le point (1) de la Proposition 4.6.3 on sait que chaque α_i est une racine de $m_{\alpha,K}$. Il suit que $f \big| m_{\alpha,K}$. Puisque $f \in K[x]$ on obtient que $f \sim m_{\alpha,K}$.

Point (3) : par définition f est un polynôme avec des racines distinctes.

Point (5) : on a $[K(\alpha) : K] = \deg m_{\alpha,K} = \deg f = r$, et donc le théorème orbite-stabilisateur donne la divisibilité.

□

Exemple 4.6.11. En continuant l'Exemple 4.6.9, on voit que pour $a, b, c, d \in \mathbb{Q}$ et pour $\alpha = a + bi + c\sqrt{2} + di\sqrt{2} \in \mathbb{Q}\left[i, \sqrt{2}\right]$, les conjugués de α sont :

$$a + bi + c\sqrt{2} + di\sqrt{2},\ a - bi + c\sqrt{2} - di\sqrt{2},\ a + bi - c\sqrt{2} - di\sqrt{2},\ a - bi - c\sqrt{2} + di\sqrt{2}$$

Si ces 4 éléments sont différents, alors

$$m_{\alpha,\mathbb{Q}} = \Big(x-\big(a+bi+c\sqrt{2}+di\sqrt{2}\big)\Big)\Big(x-\big(a-bi+c\sqrt{2}-di\sqrt{2}\big)\Big)\Big(x-\big(a+bi-c\sqrt{2}-di\sqrt{2}\big)\Big)\Big(x-\big(a-bi-c\sqrt{2}+di\sqrt{2}\big)\Big)$$

On note que ces 4 éléments différents si les cordonnées sont non-zéros, parce que $\left\{1, i, \sqrt{2}, i\sqrt{2}\right\}$ forment une base de $\mathbb{Q}\left[i, \sqrt{2}\right]$ sur $\mathbb{Q}$. Par example cela donne le polynôme minimal de l'élément $1 + i + \sqrt{2} + i\sqrt{2}$.

La fin du 13. cours, le 11.05.2021.

Théorème 4.6.12. *Si L est un corps, et $G \subseteq \mathrm{Aut}(L)$ est un sous-groupe fini, alors $\left[L : L^G\right] = |G| = \left|\mathrm{Gal}\left(L/L^G\right)\right|$.*

Démonstration. Posons $K = L^G$. Par la Proposition 4.6.10, $K \subseteq L$ est algébrique et séparable. On démontre premièrement que elle est aussi une extension simple. Prenons

$$K \subsetneq K_1 = K(\alpha_1) \subsetneq \cdots \subsetneq K_n = K(\alpha_1, \ldots, \alpha_n) \subsetneq \ldots \tag{4.6.c}$$

On démontre que cette chaine stabilise. Par le théorème de l'élément primitif (Théorème 4.5.9), $K \subseteq K_i$ est un extension simple pour chaque entier $i \geq 1$. Notons que ici on utilise la séparabilité de $K \subseteq L$ donnée par Proposition 4.6.10.(3). Avoir démontré la simplicité de $K \subseteq K_i$, la Proposition 4.6.10 implique $[K_i : K] \big| |G|$, dont on en déduit que (4.6.c) stabilise.

La stabilisation de (4.6.c) implique en particulier que l'extension $K \subseteq L$ est finiment engendré. En utilisant le théorème de l'élément primitif (Théorème 4.5.9) encore une fois, on obtient que $L = K(\gamma)$ pour un élément $\gamma \in L$. Le calcul suivant conclut notre démonstration :

$$|G| \underset{\uparrow}{\geq} \deg m_{\gamma,K} = [K(\gamma) : K] = [L : K] \underset{\uparrow}{\geq} \left|\mathrm{Gal}(L/K)\right| \underset{\uparrow}{\geq} |G|$$

Proposition 4.6.10

$G \subseteq \mathrm{Gal}(L/K)$

Puisque $K(\gamma) = L$, chaque $\sigma \in \mathrm{Gal}(L/K)$ est uniquement déterminé par $\sigma(\gamma)$, ce qui doit être une racine de $m_{\gamma,K}$ (points (1) et (2) de la Proposition 4.6.3). De plus, on peut avoir au plus $[L : K]$ racines différentes de $m_{\gamma,K}$

□

On en déduit une caractérisation numérique des extensions galoisiennes de degré fini :

Corollaire 4.6.13. *Une extension de corps $K \subseteq L$ de degré fini est galoisienne si et seulement si $[K : L] = |\operatorname{Gal}(L/K)|$.*

Démonstration. On a $K = L^{\operatorname{Gal}(L/K)}$ si et seulement si $[L^{\operatorname{Gal}(L/K)} : K] = 1$ si et seulement si $[K : L] = \operatorname{Gal}(L/K)$, où le dernière équivalence est démontre par le calcul suivant :

$$\underset{\text{Proposition 4.2.15}}{\left[L^{\operatorname{Gal}(L/K)} : K\right]} = \frac{[L : K]}{\left[L : L^{\operatorname{Gal}(L/K)}\right]} \underset{\text{Théorème 4.6.12}}{=} \frac{[L : K]}{\operatorname{Gal}(L/K)}$$

□

Exemple 4.6.14. Par le Corollaire 4.6.13, tout exemple des extensions dans l'Exemple 4.6.4 est galoisienne. En combinant avec le Corollaire 4.4.22 et la Proposition 4.6.10 on obtient que

$$\forall \alpha \in \mathbb{F}_{p^n} \setminus \left(\bigcup_{d|n} \mathbb{F}_{p^d} \right) : \ m_{\alpha,\mathbb{F}_p} = \prod_{i=0}^{n-1} \left(x - \alpha^{p^i} \right).$$

Théorème 4.6.15. *Une extension de corps $K \subseteq L$ de degré fini est galoisienne si et seulement si L est un corps de décomposition sur K engendré par éléments séparable sur K.*

Cela veut dire que L est un corps d'un polynôme $f \in K[x]$ et $L = K(\alpha_1, \ldots, \alpha_r)$ pour α_i sont séparable sur K (les α_i ne sont pas forcément les racines de f).

Démonstration.

$\boxed{\Longrightarrow :}$ Prenons $K \subseteq L$ galoisienne. Le théorème de l'élément primitif (Théorème 4.5.9) et la séparabilité de l'extension (Proposition 4.6.10.(3)) nous dit que $L = K(\gamma)$, pour un $\gamma \in L$. Le polynôme $m_{\gamma,K}$ scinde sur L par la Proposition 4.6.10, et par conséquent L est le corps de décomposition de $m_{\gamma,K}$.

$\boxed{\Longleftarrow :}$ On a $[K : L] = \operatorname{Gal}(K/L)$ par le point (4) de la Proposition 4.6.3, et ainsi $K \subseteq L$ est galoisienne par le Corollaire 4.6.13. □

Corollaire 4.6.16. *Si $K \subseteq L = K(\alpha_1, \ldots, \alpha_r)$ est une extension de corps de degré fini telle que les α_i sont séparables sur K, alors l'extension elle-même est séparable aussi.*

Démonstration. Soit $f = \prod_{i=1}^{n} m_{\alpha_i,K}$, et soit $K \subseteq F$ le corps de décomposition de f. Par le Corollaire 4.3.6, un peut identifier L avec un sous-corps $L \subseteq F$. Notons que F est engendré sur K par des racines des $m_{\alpha_i,K}$ qui sont toutes séparable sur K (parce que α_i est, et donc $m_{\alpha_i,K}$). En appliquant Théorème 4.6.15 on obtient que $K \subseteq F$ est galoisienne, et donc séparable sur K (Proposition 4.6.10). Cela implique que $K \subseteq L$ est séparable. □

4.6.3 Le théorème fondamental de la théorie de Galois

Proposition 4.6.17. *Soit $K \subseteq L \subseteq E$ une sequence des extension de corps tel que $K \subseteq E$ est une extension galoisienne de degré fini. Dans ce cas :*

(1) L'extension $L \subseteq E$ est galoisienne.

(2) L'extension $K \subseteq L$ est galoisienne si et seulement si pour chaque $\sigma \in \operatorname{Gal}(E/K)$ on a $\sigma(L) = L$.

Démonstration. (1) Si $K \subseteq E$ est galoisienne, alors par le Théorème 4.6.15, le corps E est un corps de décomposition séparable sur K. Ainsi, E est aussi un corps de décomposition séparable sur L (si $\alpha \in E$, alors $m_{\alpha,L} | m_{\alpha,K}$, et donc si α est séparable sur K, alors il est aussi séparable sur L). En utilisant le le Théorème 4.6.15 encore une fois on obtient que $L \subseteq E$ est galoisienne.

(2) Parce que $K \subseteq E$ est séparable, $K \subseteq L$ est aussi séparable. Ainsi, par le Théorème 4.5.9 $L = K(\alpha)$ pour un élément $\alpha \in K$. On a

$$\begin{array}{l} \forall \sigma \in \mathrm{Gal}(E/K) : \ \sigma(L) = L \\ \uparrow \\ \boxed{\dim_K L < \infty} \\ \uparrow \\ \boxed{L = K(\alpha)} \\ \uparrow \\ \boxed{\text{Proposition 4.6.10}} \\ \uparrow \\ \boxed{L = K(\alpha)} \\ \uparrow \\ \boxed{\text{le Théorème 4.6.15 et le Corollaire 4.6.5}} \end{array} \quad \begin{array}{l} \iff \forall \sigma \in \mathrm{Gal}(E/K) : \ \sigma(L) \subseteq L \\ \\ \\ \iff \forall \sigma \in \mathrm{Gal}(E/K) : \ \sigma(\alpha) \in L \\ \\ \\ \iff m_{\alpha,K} \text{ scinde sur } L \\ \\ \\ \iff L \text{ est le corps de décomposition de } m_{\alpha,K} \\ \\ \\ \iff K \subseteq L \text{ est galoisienne} \end{array}$$

□

Théorème 4.6.18. THÉORÈME FONDAMENTAL DE LA THÉORIE DE GALOIS POUR DES EXTENSIONS DE DEGRÉS FINIS. *Pour une extension $K \subseteq L$ galoisienne de degré fini avec $G = \mathrm{Gal}(L/K)$, on a une bijection qui reverse l'inclusion :*

$$\begin{array}{ccc} \{ \text{ corps intermédiaire } K \subseteq F \subseteq L \} & \longleftrightarrow & \{ \text{ sous-groupe } H \leq G \} \\ \cup & & \cup \\ F & \longmapsto & \mathrm{Gal}(L/F) \\ L^H & \longmapsfrom & H \end{array} \tag{4.6.d}$$

De plus $K \subseteq F \subseteq L$ est galoisienne si et seulement si le H correspondant est un sous-groupe normal de G. Dans ce cas, on a ${}^{G}/_{H} \cong \mathrm{Gal}\left(L^H/K\right)$ donné par la restriction des automorphismes.

Démonstration. La bijection : Pour un corps intermédiaire $K \subseteq F \subseteq L$ et pour un sous-groupe $H \subseteq G$, on a

$$L^{\mathrm{Gal}(L/F)} = \{ \ \alpha \in L \ | \ \forall \sigma \in \mathrm{Gal}(L/F) : \ \sigma(\alpha) = \alpha \ \} \supseteq F \tag{4.6.e}$$

et

$$\mathrm{Gal}(L, F^H) = \{ \ \sigma \in G \ | \ \forall \alpha \in F^H : \ \sigma(\alpha) = \alpha \ \} \supseteq H. \tag{4.6.f}$$

Par conséquent, pour prouver la bijection il suffit de démontrer les inclusions dans l'autre sens. Ainsi, il suffit de démontrer que les dimensions sur K (resp. les nombres des éléments) aux deux cotés des inclusions sont les mêmes. De plus, par la multiplicativité de la dimension (Proposition 4.2.15), dans le cas de (4.6.e), il suffit de démontrer que $[L : F] = \left[L : L^{\mathrm{Gal}(L/F)}\right]$.

L'égalité correspondante à (4.6.f) est démontrée dans Théorème 4.6.12. Pour l'autre égalité prenons un corps intermédiaire $K \subseteq F \subseteq L$. L'extension $F \subseteq L$ est galoisienne par le point (1) de la Proposition 4.6.17. Par conséquent on a

$$[L : F] \underset{\uparrow}{=} |\operatorname{Gal}(L/F)| \underset{\uparrow}{=} \left[L : L^{\operatorname{Gal}(L/F)}\right]$$

Corollaire 4.6.13 — en appliquant Théorème 4.6.12 à $\operatorname{Gal}(L/F)$

La fin du 14. cours, le 18.05.2021.

$H \subseteq G$ *sous-groupe*, $\sigma \in G \implies \sigma H \sigma^{-1} = \operatorname{Gal}\left(L/\sigma\left(L^H\right)\right)$ Les nombres des éléments sont le même aux deux cotés, parce que

$$\left|\operatorname{Gal}\left(L/\sigma\left(L^H\right)\right)\right| \underset{\uparrow}{=} \left[L : \sigma\left(L^H\right)\right] \underset{\uparrow}{=} \frac{[L:K]}{\left[\sigma\left(L^H\right) : K\right]} \underset{\uparrow}{=} \frac{[L:K]}{\left[L^H : K\right]} \underset{\uparrow}{=} \left[L : L^H\right] \underset{\uparrow}{=} |H| \underset{\uparrow}{=} \left|\sigma H \sigma^{-1}\right|$$

Corollaire 4.6.13 — Proposition 4.2.15 — σ est un isomorphisme K-linéaire — Proposition 4.2.15 — Corollaire 4.6.13 — la conjugaison est un automorphisme d'un groupe

Ainsi, il suffit de démontrer l'inclusion dans un sens. Pour cela prenons $h \in H$. On a pour chaque $\alpha \in L^H$:

$$\sigma h \sigma^{-1}(\sigma(\alpha)) = \sigma h(\alpha) = \sigma(\alpha)$$

Par conséquent on obtient que $\sigma h \sigma^{-1} \in \operatorname{Gal}(L/\sigma(L^H))$ qui démontre l'inclusion $\sigma H \sigma^{-1} \subseteq \operatorname{Gal}\left(L/\sigma\left(L^H\right)\right)$

$H \subseteq G$ *normal* $\iff K \subseteq L^H$ *galoisienne :* Par l'affirmation précédente on voit que un sous-groupe $H \subseteq G$ est normal si et seulement si

$$\forall \sigma \in G : \ \operatorname{Gal}\left(L/\sigma\left(L^H\right)\right) = \operatorname{Gal}\left(L/L^H\right) \tag{4.6.g}$$

En utilisant la bijection (4.6.d), ce que l'on a déjà démontré, on obtient que (4.6.g) est équivalent à la condition $\sigma\left(L^H\right) = L^H$ pour chaque $\sigma \in G$. Finalement, par point (2), de la Proposition 4.6.17, c'est équivalent à la condition que $K \subseteq L^H$ est galoisienne.

$H \subseteq G$ *normal* $\implies {}^{G}\!/_{H} \cong \operatorname{Gal}\left(L^H/K\right)$ *:* Supposons que $H \subseteq G$ est normal ou dans une manière équivalente que $K \subseteq F = L^H$ est galoisienne. On a vu dans le paragraphe précédent cela implique que F est stable sur G. Autrement dit G peut être restreindre sur F. Cela nous donne un homomorphisme $G \to \operatorname{Gal}(F/K)$, dont le noyau est $\operatorname{Gal}(L/F) = H$. On obtient un homomorphisme injectif ${}^{G}\!/_{H} \hookrightarrow \operatorname{Gal}(F/K)$. Cet homomorphisme est bijectif si le coté droit ne contient pas plus d'éléments que le coté gauche :

$$\left|{}^{G}\!/_{H}\right| = \frac{|G|}{|H|} = \frac{[L:K]}{[L:F]} \underset{\uparrow}{=} [F : K] \underset{\uparrow}{=} \operatorname{Gal}(F/K)$$

Proposition 4.2.15 — Corollaire 4.6.13, en utilisant que $K \subseteq F$ est galoisienne

□

Exemple 4.6.19. Considérons l'extension $\mathbb{Q} = K \subseteq L = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}\right)$. On démontre en utilisant la théorie de Galois que $i \notin L$.

On a vu dans le point (4) de l'Exemple 4.6.4 que $G = \operatorname{Gal}(L/K) \cong S_3$. Il existe un unique sous-groupe de S_3 d'ordre 3. Il suit, par le Théorème 4.6.18, que il existe un unique corps intermédiaire $\mathbb{Q} \subseteq F \subseteq L$ tel que $[F : \mathbb{Q}] = 2$. Notons que

$$\frac{e^{\frac{2\pi i}{3}}\sqrt[3]{2} - e^{\frac{4\pi i}{3}}\sqrt[3]{2}}{\sqrt[3]{2}} = e^{\frac{2\pi i}{3}} - e^{\frac{4\pi i}{3}} = \sqrt{3}i \in L$$

De plus $\sqrt{3}i$ est une racine de x^2+3, et par conséquent $\sqrt{3}i$ est de degré 2 sur $\mathbb{Q}$. On obtient que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}i) \subseteq L$ est le seul corps intermédiaire de degré 2.

Il suit que $i \notin L$. En effet, supposons l'opposite. Dans ce cas, $\mathbb{Q}(i)$ est un corps intermédiaire de degré 2, est par conséquent on a $i \in \mathbb{Q}(\sqrt{3}i)$. Par conséquent il existe $c, d \in \mathbb{Q}$ tel que

$$i = c + i\sqrt{3}d \implies c = 0, \text{ et } 1 = \sqrt{3}d$$

unicité d'écrire un nombre complexe de façon $a+bi$ pour $a, b \in \mathbb{R}$

Cela est une contradiction avec la rationalité de d.

Remarque 4.6.20. Il y a une version du Théorème 4.6.18 pour des extensions de dimension infinie, mais malheureusement nous n'avons pas du temps d'en discuter dans ce cours.

4.7 Extensions purement inséparables, séparable-inséparable décompositions

Définition 4.7.1. Soit $K \subseteq L$ une extension algébrique des corps de caractéristique $p > 0$. Un élément $\alpha \in L \setminus K$ est *purement inséparable* (aussi appelé radiciel) sur K si il existe un entier $n > 0$ tel que $\alpha^{p^n} \in K$. Le plus petit tel entier n est appelé la *hauteur* de α sur K.

L'extension $K \subsetneq L$ est *purement inséparable* si chaque élément $\alpha \in L \setminus K$ est purement inséparable sur K. La hauteur d'une extension purement inséparable $K \subsetneq L$ est le supremum des hauteurs des éléments de $L \setminus K$ sur K.

Exemple 4.7.2. Si K n'est pas parfait, alors $K^p \subsetneq K$ est purement inséparable de hauteur 1, par la Proposition 4.5.7. Pour un example spécifique, on peut prendre $K = \mathbb{F}_p(t)$, par l'Exemple 4.5.6.

Lemme 4.7.3. *Si $K \subseteq L$ est un corps de caractéristique $p > 0$, et $\alpha \in L \setminus K$ est un élément de hauteur 1, alors $m_{\alpha,K} = x^p - \alpha^p$.*

Démonstration. L'élément α est une racine de $x^p - \alpha^p$. Ainsi, $m_{\alpha,K} | x^p - \alpha^p = (x-\alpha)^p$. Il suit que $m_{\alpha,K} = (x-\alpha)^i = x^i - i\alpha x^{i-1} + \dots$ pour un entier $2 \leq i \leq p$. En examinant le deuxième coefficient de $(x-\alpha)^i$, on voit que $i\alpha \in K$. Cela implique que $i = p$. □

Proposition 4.7.4. *Si $K \subseteq L$ est une extension algébrique des corps de caractéristique $p > 0$, et $\alpha \in L \setminus K$ est purement inséparable de hauteur n sur K, alors $m_{\alpha,K} = x^{p^n} - \alpha^{p^n}$.*

Démonstration. On démontre la proposition par récurrence sur n. Pour $n = 1$, l'affirmation est démontre dans le Lemme 4.7.3. Ainsi, on suppose que $n > 1$ et que l'on connait la proposition pour les plus petites valeurs de n. Puisque $x^{p^n} - \alpha^{p^n} \in K[x]$ s'annule en α, il suffit de démontrer que $|K(\alpha) : K| = p^n$. Notons que α^p a hauteur $n-1$ sur K. De coup, par l'hypothèse d'induction, $m_{\alpha^p,K} = x^{p^{n-1}} - \alpha^{p^n}$ et par conséquent $[K(\alpha^p) : K] = p^{n-1}$. De plus, en utilisant le Lemme 4.7.3, $[K(\alpha) : K(\alpha^p)| = p$. Par la Proposition 4.2.15, $[K(\alpha) : K] = [K(\alpha) : K(\alpha^p)] \cdot [K(\alpha^p) : K] = p \cdot p^{n-1} = p^n$. □

Corollaire 4.7.5. *Si $K \subseteq L$ une extension purement inséparable de degré fini, alors*

(1) il existe éléments α_i, tel que $L = K(\ \sqrt[p^{n_i}]{\alpha_i} \mid i = 1, \dots, r\ )$, où n_i est la hauteur de α_i, et
(2) $[L : K]$ est une puissance de p.

Démonstration. Tous les deux points suivent directement de la Proposition 4.7.4. □

Proposition 4.7.6. *Une extension $K \subsetneq L$ de corps est purement inséparable si et seulement si il n'existe pas un élément $\alpha \in L \setminus K$ tel que α est séparable sur K.*

Démonstration.

$\boxed{\Longrightarrow :}$ C'est une conséquence de la Proposition 4.7.4, parce que $x^{p^n} - \alpha^{p^n}$ a juste une racine (mais p^n-fois).

$\boxed{\Longleftarrow :}$ Supposons que il n'existe pas des éléments séparable dans $L \setminus K$, et prenons $\alpha \in L \setminus K$. Par le Corollaire 4.4.12, $\frac{\partial}{\partial x} m_{\alpha,K} = 0$, et par la Remarque 4.4.2 $m_{\alpha,K} = \sum_{i=0}^{r} a_i x^{pi}$. Notons, que puisque $\alpha \notin K$, on a $r \geq 1$.

On démontre que α est purement inséparable par induction sur $r = \frac{\deg m_{\alpha,K}}{p}$:

(1) Si $r = 1$, alors $\alpha^p = -a_0 \in K$, et alors α est purement inséparable sur K.

(2) Si $r > 1$, alors le degré de α est plus que p, et par conséquent $\alpha^p \notin K$. De plus, α^p est une racine de $\sum_{i=0}^{r} a_i x^i$, est par conséquent $\deg \frac{m_{\alpha^p,K}}{p} \leq \frac{r}{p}$. Ainsi, α^p satisfait l'hypothèse d'induction. On obtient que α^p est purement inséparable, et par conséquent α est purement inséparable.

□

Proposition 4.7.7. *Si $K \subseteq L$ et $L \subseteq F$ sont deux extensions algébriques séparables des corps, alors F est séparable sur K.*

Démonstration. C'est démontré dans une exercice de la série dernière. □

Corollaire 4.7.8. *Si $K \subseteq L$ est une extension algébrique de corps, alors*

$$L_{\mathrm{sep},K} = \left\{ \alpha \in L \;\middle|\; \alpha \text{ est algébrique et séparable sur } K \right\}$$

est un sous-corps de L.

De plus, L est purement inséparable sur L_{alg}.

Matériel optionnel

Démonstration. Prenons $\alpha, \beta \in L_{\mathrm{sep},K}$. Soit F le corps de décomposition de $m_{\alpha,K} \cdot m_{\beta,K}$ sur L, et soit E le sous-corps de F engendré par des racines de $m_{\alpha,K}$ et de $m_{\beta,K}$. Par définition, E est le corps de décomposition de $m_{\alpha,K} \cdot m_{\beta,K}$ sur K.

Puisque α et β sont séparables sur K, les polynômes $m_{\alpha,K}$ et $m_{\beta,K}$ sont séparables. Par conséquent, E est engendré par des éléments séparables sur K. Par le Corollaire 4.6.16, il suit que E et séparable sur K. En particulier, si $\alpha \neq 0$, alors $0, 1, \alpha + \beta, \alpha \cdot \beta, -\beta, \alpha^{-1} \in L_{\mathrm{sep},K}$. Cela conclut la démonstration du fait que $L_{\mathrm{sep},K}$ est un sous-corps de L.

Pour l'affirmation additionnelle, on postule que $L \setminus L_{\mathrm{sep},K}$ ne contient pas des éléments séparable sur $L_{\mathrm{sep},K}$. Pour montrer ce fait, prenons $\alpha \in L$ séparable sur $L_{\mathrm{sep},K}$, et appliquons Proposition 4.7.7 aux extensions $K \subseteq L_{\mathrm{sep},K} \subseteq L_{\mathrm{sep},K}(\alpha)$. Puisque $L_{\mathrm{sep},K} \subseteq L_{\mathrm{sep},K}(\alpha)$ et séparable par Corollaire 4.6.16, on obtient que α est séparable aussi sur K. Il suit que $\alpha \in L_{\mathrm{sep},K}$, ce qui conclut le fait postulé ci-dessus. Il suit que L est purement inséparable sur L_{sep} par la Proposition 4.7.6. □

Corollaire 4.7.9. *Si $K \subseteq L$ est une extension algébrique de corps, alors*

$$L_{\mathrm{insep},K} = \left\{ \alpha \in L \;\middle|\; \alpha \in K, \text{ ou } \alpha \text{ est purement inséparable sur } K \right\}$$

est un sous-corps de L.

Matériel optionnel

Démonstration. On a $K \subseteq L_{\text{insep},K}$, par la définition de celui-ci. Par conséquent on a aussi $0, 1, \in L_{\text{insep},K}$.

Prenons $\alpha, \beta \in L_{\text{insep},K}$. Par la Définition 4.7.1, il existe entiers $n, m > 0$ tels que $\alpha^{p^n}, \beta^{p^m} \in K$. De plus, en remplaçant le plus petit de n et m par l'autre, on peut supposer que $\alpha^{p^n}, \beta^{p^n} \in K$. Les inclusions suivantes conclut notre démonstration :

- $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \in K \implies \alpha+\beta \in L_{\text{insep},K}$
- $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} \in K \implies \alpha\beta \in L_{\text{insep},K}$
- Si $p > 2$, alors $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = -\alpha^{p^n} \in K$, et si $p = 2$, alors $(-\alpha)^{p^n} = \alpha^{p^n} \in K$. De toute façon, on a $-\alpha \in L_{\text{insep},K}$.
- Si $\alpha \neq 0$, alors $\left(\alpha^{-1}\right)^{p^n} = \left(\alpha^{p^n}\right)^{-1} \in K \implies \alpha^{-1} \in L_{\text{insep},K}$

□

Exemple 4.7.10. On donne un exemple que dans la situation du Corollaire 4.7.9, par contraire au Corollaire 4.7.8, L n'est pas nécessairement séparable sur $L_{\text{insep},K}$ (cependant cela marche si L est la clôture algébrique, qui est démontre dans la Section 4.8.5).

Notons que le polynôme $f = x^6 + x^4u + x^2uv + u \in \mathbb{F}_2(u,v)[x]$ est irréductible en appliquant la Proposition 3.9.3 avec $p = u$. Considérons l'extension $\mathbb{F}_2(u,v) = K \subseteq L = K[x]\Big/(f)$, et soit $\alpha = x+(f) \in L$ une racine de f dans L. Notons que $f = m_{\alpha,K}$. Ainsi, par la Proposition 4.7.4, α n'est pas purement inséparable sur K. On voit que si L était séparable sur $L_{\text{insep},K}$, alors, α devrait être séparable sur $L_{\text{insep},K}$.

Supposons l'affirmation plus faible que α est séparable sur un corps intérmediaire $K \subseteq F \subseteq L$ tel que $\alpha \in L \setminus F$. On en déduit une contradiction, qui montrera que en effet il peut arriver que L n'est pas séparable sur $L_{\text{insep},K}$.

Soit E le corps de décomposition de $f \cdot (x^2-u) \cdot (x^2-v)$, qui contient L naturellement (Corollaire 4.3.6 et Corollaire 4.3.7), et qui contient deuxième racines $\sqrt{u}$ et $\sqrt{v}$ de u et de v. En utilisant que la caractéristique et 2, sur E on a :

$$f = x^6 + x^4u + x^2uv + u = \left(x^3 + x^2\sqrt{u} + x\sqrt{u}\sqrt{v} + \sqrt{u}\right)^2. \tag{4.7.a}$$

Il suit que f n'est pas séparable, et donc α n'est pas séparable sur K. Du coup, par point (2) du Corollaire 4.7.5 et par le fait que $[L:K] = 6$ on a forcément que $[F:K] = 2$ et $[L:F] = 3$. Cela nous donne aussi que $L = F(\alpha)$. On en déduit que $m_{\alpha,F}$ est un polynôme séparable sur F de degré 3 tel que $m_{\alpha,F} | f$.

En utilisant (4.7.a), on voit que le plus grand diviseur séparable de f dans $E[x]$ est

$$g = x^3 + x^2\sqrt{u} + x\sqrt{u}\sqrt{v} + \sqrt{u} \in E[x].$$

Puisque $\deg m_{\alpha,F} = 3$ est aussi séparable, $m_{\alpha,F}$ dois être associé à g dans $E[x]$. Puisque le coefficient dominant de g 1 on obtient que $g \in F[x]$. En particulier, $\sqrt{u}, \sqrt{u}\sqrt{v} \in F$, et par conséquent $\sqrt{v} = \frac{\sqrt{u}\sqrt{v}}{\sqrt{u}} \in F$ est vrai aussi. Du coup, F contient $K(\sqrt{u}, \sqrt{v})$. Mais, $[K(\sqrt{u}, \sqrt{v}) : K] = 4$ ce qui est une contradiction.

4.8 Corps algébriquement clos

4.8.1 Les définitions

Exemple 4.8.1. Considérons le sous-corps $\mathbb{Q}_{\text{alg}}$ de $\mathbb{C}$ qui contient les éléments algébrique sur $\mathbb{Q}$, ou autrement dit les nombres algébriques. Par définition, tout polynôme $f \in \mathbb{Q}[t]$ obtient au moins une racine sur $\mathbb{Q}_{\text{alg}}$. On prétend qu'en effet même tout polynôme $g \in \mathbb{Q}_{\text{alg}}[t]$ s'annule en quelqu'un élément de $\mathbb{Q}_{\text{alg}}$:

On peut supposer que g est irréductible sur $\mathbb{Q}_{\text{alg}}$. Soient $b_0, \dots, b_n \in \mathbb{Q}_{\text{alg}}$ les coefficients de g, et soit α une racine de g dans $\mathbb{C}$. Par définition d'être algébriques (Définition 4.2.8), les degrés des b_i sont finis sur $\mathbb{Q}$. Ainsi, par Proposition 4.2.15, $[F : \mathbb{Q}] < \infty$ où $F = \mathbb{Q}(b_0, \dots, b_n)$. De plus, pour $L = F(\alpha)$ on a $[L : F] < \infty$, et par conséquent, en utilisant Proposition 4.2.15 encore une fois, on a $[L : \mathbb{Q}] < \infty$. Cela implique que $L \subseteq \mathbb{Q}_{\text{alg}}$, et donc $\mathbb{Q}_{\text{alg}}$ contient une racine de g.

Le lemme suivant dit qu'en fait $\mathbb{Q}_{\text{alg}}$ contient toute racine de g, où autrement dit g scinde sur $\mathbb{Q}_{\text{alg}}$.

Lemme 4.8.2. *Les conditions suivantes sont équivalentes pour un corps K.*

(1) Tout polynôme non constant de $K[x]$ admet une racine dans K.
(2) Tout polynôme $f \in K[x]$ est scindé.
(3) Tout polynôme irréductible de $K[x]$ est de degré 1.
(4) Toute extension algébrique L de K est de degré un, i.e. $[L : K] = 1$.

Démonstration. *(2) $\Longrightarrow$ (1) :* point (2) est un cas spécial du point (1).

(1) $\Longrightarrow$ (2) : On le montre par récurrence sur $\deg f$. Pour $\deg f = 1$, il y a rien à montrer. Ainsi, on peut supposer que $\deg f > 1$ et qu'on connait l'affirmation pour plus petites valeurs de $\deg f$. On a supposé aussi que f admet une racine $\alpha \in K$, qui implique que $x - a | f$ dans $K[x]$ (point (1) de l'Exemple 2.4.10). Il existe donc un polynôme $g \in K[x]$ de degré $\deg f - 1$ tel que $f = (x - a) \cdot g$. Par hypothèse de récurrence g est scindé, et on conclut alors que f est scindé aussi.

(2) $\Longleftrightarrow$ (3) : $K[t]$ est factoriel par Corollaire 3.7.2.

(3) $\Longleftrightarrow$ (4) : Par la Remarque 4.2.26, point (3) est équivalent à dire que toute extensions algébriques simples ont degré 1. De plus, on peut effacer ici la condition d'être simple, parce que toute extension algébriques non-triviale $K \subseteq L$ contient des extensions non-triviales algébriques simples, notamment $K \subseteq K(\alpha)$ pour quelconque $\alpha \in L \setminus K$. □

Définition 4.8.3. Un corps K est *algébriquement clos* si une des conditions équivalents du Lemme 4.8.2 sont satisfaites pour K.

Une *clôture algébrique* $\overline{K}$ de K est une extension algébrique de K qui est algébriquement close.

Exemple 4.8.4. Comme expliqué dans l'Exemple 4.8.1, $\mathbb{Q}_{\text{alg}}$ est une clôture algébrique de $\mathbb{Q}$.

Remarque 4.8.5. On note que le Théorème Fondamental de l'Algèbre (démontré dans le cours Analyse III) affirme que $\mathbb{C}$ est algébriquement clos.

Matériel optionnel

4.8.2 La construction

La clôture algébrique de K est une version universelle du corps de décomposition de $f \in K[x]$. Autrement dit c'est une extension où chaque polynôme scinde, pas

seulement les polynôme qui sont forcé de scinder pour que f scinde.

Par exemple $L = \mathbb{Q}\big(\sqrt[3]{2}, \xi\sqrt[3]{2}\big)$ est le corps de décomposition de $f = x^3 - 2$. Ainsi, sur L, le polynôme f scinde. De plus, quelques autres polynômes scindent aussi sur L, qui ne scinde pas sur $\mathbb{Q}$. Un exemple d'un tel polynôme est

$$x^3 - 3x^2 + 3x - 3 = \Big(x - \big(1 + \sqrt[3]{2}\big)\Big)\Big(x - \big(1 + \xi\sqrt[3]{2}\big)\Big)\Big(x - \big(1 + \xi^2\sqrt[3]{2}\big)\Big).$$

Cependant, on a vu dans l'Exemple 4.6.19 que $i \notin L$ est par conséquent $x^2 + 1$ ne scinde pas sur L.

Dans l'autre coté, sur $\mathbb{Q}_{\text{alg}}$ chaque polynôme dans $\mathbb{Q}[x]$, et même chaque polynôme dans $\mathbb{Q}_{\text{alg}}[x]$ scinde. Autrement dit, on peut penser à une clôture algébrique d'un corps K ne tant que l'union de toutes les corps de décompositions de K. Notre but dans la section présente et de formaliser cette idée. L'obstacle principal est que il n'y a pas une grands corps ambiant dans lequel on peut prendre cet union. Il y une manière générale de sursauter le problème de prendre l'union des ensembles qui ne sont pas contenu dans un grand ensemble ambiant : on prend l'union disjoint, et on passe au quotient par une relation d'équivalence qui identifie les éléments ce qui on voudrait identifier dans l'union (terminologie technique : on prend la limite directe du Lemme 4.8.7). Le problème est qu'il n y a pas une manière canonique de faire ces identifications grâce aux automorphismes des corps (Section 4.6).

Ce problème technique est résolu par prendre, au lieu du union des tous corps de décomposition sur K, une extension $K \subseteq K_1$ de corps qui ajoute une racine pour chaque polynôme au même temps, une autre $K_1 \subseteq K_2$ qui fait le même pur K_1, etc. Dans ce cas on peut en effet prendre l'union avec les identification expliqué dans le paragraphe précédent.

Le prix à payer et que $K \subseteq K_1$ est une extension algébrique de degré infinie. Par conséquent, il est un quotient d'un anneau des polynômes dans un nombre infini des variables : si X est un ensemble des variables (de quelconque cardinal), $K[X]$ est l'anneau des polynômes avec variables dans X (avec opérations habituelles). Puisque chaque polynôme dans $K[X]$ contient juste un nombre fini de variables, on obtient que

$$K[X] = \bigcup_{x_1,\dots,x_n \in X} K[x_1, \dots, x_n]$$

Lemme 4.8.6. *Considérons la situation suivante :*

- *K est un corps,*
- *X est un ensemble d'indéterminées,*
- *$x_i \in X$ indéterminées distinctes pour $1 \leq i \leq n$,et*
- *$f_i(x_i) \in K[x_i] \subseteq K[X]$ des polynômes.*

Dans ce cas, l'idéal $I = (f_1, \dots, f_n) \subseteq K[X]$ est un idéal propre.

Démonstration. Considérons l'homomorphisme $\phi : K[X] \to K[x_1, \dots, x_n]$ qui évalue $x \mapsto 0$ pour chaque $x \in X \setminus \{x_1, \dots, x_n\}$. On voit qu'il suffit de démontrer que $\phi(I) = \big(\phi(f_1), \dots, \phi(f_n)\big)$ est un idéal propre. Autrement dit, on peut supposer que $X = \{x_1, \dots, x_n\}$. Dénotons $K[x_1, \dots, x_n]$ par A.

Soit L le corps de décomposition de $\prod_{i=1}^n f_i(x) \in K[x]$, et soit $\alpha_i \in L$ une racine de $f_i(x)$. Supposons que I n'est pas propre. Par conséquent on peut écrire pour quelques

$h_i \in A$:

$$1 = \sum_{i=1}^{n} h_i f_i \implies \underset{\boxed{\text{par l'évaluation } x_i \mapsto \alpha_i}}{\uparrow} 1 = \sum_{i=1}^{n} h_i(\alpha_1, \ldots, \alpha_n) f_i(\alpha_i) = \underset{\boxed{\alpha_i \text{ est une racine de } f_i}}{\uparrow} \sum_{i=1}^{n} h_i(\alpha_1, \ldots, \alpha_n) \cdot 0 = 0$$

qui est une contradiction.

□

Lemme 4.8.7. *Soient $K_0 \overset{\iota_0}{\hookrightarrow} K_1 \overset{\iota_1}{\hookrightarrow} K_2 \overset{\iota_2}{\hookrightarrow} \ldots$ une séquence infinie des corps avec homomorphismes (injectifs) entre eux. Alors, la limite directe*

$$\varinjlim_i K_i = \bigsqcup_{i \in \mathbb{N}} K_i \Big/ \begin{array}{l} \bullet\ x \equiv \iota_{s-1} \circ \ldots \circ \iota_r(x) \text{ et } \iota_{s-1} \circ \ldots \circ \iota_r(x) \equiv x \text{ pour chaque entier } s > r, \text{ et } x \in K_r \\ \bullet\ x \equiv x \text{ pour chaque } x \in K_r \end{array}$$

$$\uparrow$$

quotient de l'union disjoint par une relation d'équivalence

est une corps, où $[x]+[y]$ et $[x]\cdot[y]$ pour $x \in K_r$ et $y \in K_s$ sont définis par le processus suivant : si $s > r$, alors $[x] = [\iota_{s-1} \circ \ldots \circ \iota_r(x)]$ qui veut dire que l'on peut supposer que $s = r$, et donc on définie

(1) $[x] + [y] = [x + y]$

(2) $[x] \cdot [y] = [x \cdot y]$

De plus, l'inclusion $K_0 \hookrightarrow \bigsqcup_{i \in \mathbb{N}} K_i$ donne un plongement des corps $K_0 \hookrightarrow \varinjlim_i K_i$.

Démonstration. On le laisse en exercice. □

Proposition 4.8.8. *Si K est un corps, alors il existe une extension algébrique $K \subseteq L$ telle que tout polynôme $f \in K[t]$ obtient au moins une racine dans L.*

Démonstration. Soit X l'ensemble de tous les polynômes de $K[t]$. On note x_f l'indéterminée dans X correspondant au polynôme $f \in K[t]$. Considérons l'idéal $I \subseteq K[t]$ défini par

$$I = \left(f(x_f) \;\middle|\; f \in K[t] \right) = \left\{ \sum_{i=1}^{m} h_i f_i(x_{f_i}) \;\middle|\; m \in \mathbb{N},\ h_i \in K[T],\ \ f_i \in K[t] \right\}$$

où on utilise la notation

$$f = \sum_{i=1}^{n} a_i t^i \ \rightsquigarrow\ f(x_f) = \sum_{i=1}^{n} a_i x_f^i$$

L'idéal $I \subseteq K[X]$ est un idéal proper par le Lemme 4.8.6. Soit $m \subseteq K[X]$ un idéal maximal contenant I, ce qui existe par le Théorème 2.5.10. On pose $L = K[X]/m$ qui est un corps. Considérons la composition d'homomorphismes

$$K \longrightarrow K[X] \xrightarrow{\xi} K[X]/m = L$$

C'est un homomorphisme entre deux corps, et donc il est injectif. De plus, chaque $f \in K[t]$ obtient une racine dans L, parce que pour $\alpha = x_f + I \in L$ on a

$$f(x_f + I) = \xi\big(f(x_f)\big) = 0.$$
$$\uparrow$$
$$\boxed{f(x_f) \in I}$$

Finalement, $K[X]$ ett par conséquent L aussi est engendré en tant qu'un K-algèbre par des éléments $x_f + I$ qui sont algébriques par le calcul ci-dessus. Cela démontre que L est algébrique sur K. □

Théorème 4.8.9. *Si K est un corps, alors il existe une clôture algébrique de K.*

Démonstration. Définissons une séquence $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots$ par récurrence, en prenant l'extension $K_i \subseteq K_{i+1}$ donnée par la Proposition 4.8.8. En utilisant le Lemme 4.8.7, on pose

$$\overline{K} = \varinjlim_n K_n.$$

Notons que par la Proposition 4.8.8, on a aussi $K \subseteq \overline{K}$. De plus, parce que chaque extension $K_i \subseteq K_{i+1}$ est algébrique, on obtient que chaque K_i est algébrique sur K. Par conséquent $\overline{K}$ est algébrique sur K car chaque élément de $\overline{K}$ vit dans K_i pour quelque $i \in \mathbb{N}$.

Enfin, $\overline{K}$ est algébriquement clos : soit $g \in \overline{K}[t]$. Il existe $n \in \mathbb{N}$ tel que $g \in K_n[t]$ puisque g est une somme finie de coefficients. Alors par notre récurrence g possède une racine dans $K_{n+1} \subseteq \overline{K}$ et donc $\overline{K}$ est algébriquement clos par le Lemme 4.8.2. □

4.8.3 Unicité

Théorème 4.8.10. *Si E et F sont deux clôtures algébriques du corps K, alors $E \cong F$ en tant que K-algèbres.*

Matériel optionnel

Démonstration. Considérons l'ensemble partiellement ordonné

$$(\mathcal{P}, \preceq) = \left\{ (L, M, \phi) \;\middle|\; \begin{array}{l} K \subseteq L \subseteq E, \text{ et } K \subseteq M \subseteq F \text{ sont des corps intermédiaires, et} \\ \phi : L \to M \text{ est un isomorphisme de } K\text{-algèbres} \end{array} \right\}$$

avec la relation

$$(L, M, \phi) \preceq (L', M', \phi') \iff L \subseteq L',\ M \subseteq M', \text{ et } \phi' \text{ étend } \phi$$

Cette relation est définie dans une manière que chaque chaine (L_i, M_i, ϕ_i) admet automatiquement un majorant $\big(\bigcup_{i\in I} L_i, \bigcup_i M_i, \phi\big)$, où chaque $\beta \in \bigcup_i L_i$ est contenu dans un L_j est alors $\phi(\beta)$ est défini d'être $\phi_j(\beta) \in M_j \subseteq \bigcup_i M_i$.

Par le lemme de Zorn (Lemme 2.5.12), il existe un élément maximal $(L_m, K_m, \phi_m) \in (\mathcal{P}, \preceq)$. Si $E = L_m$, alors on est prêt : dans ce cas L_m est algébriquement clos, et en utilisant l'isomorphisme ϕ_m, K_m est aussi algébriquement clos. Cela veut dire, que toute extension algébrique de K_m a degré 1, et en particulier $F = K_m$. Du coup, ϕ_m donne un isomorphisme $E \cong F$ de K-algèbres.

Ainsi, on peut supposer que $L_m \neq E$. Cela veut dire qu'il existe un polynôme $f \in L_m[x]$ tel que le corps de décomposition L' de f sur L_m est plus grand que L_m lui-même. Notons, que L' est contenu dans E, il est juste le sous-corps engendré par L_m est toutes les racines de f.

Soit, $\xi : L_m[x] \to M_m[x]$ l'homomorphisme induit par ϕ_m. Puis que F est aussi algébriquement clos, le corps de décomposition M' de $\xi(f)$ est contenu dans F. De plus, Théorème 4.3.4 nous dit, que ϕ_m étend à un isomorphisme $L' \to M'$ qui est une contradiction avec la maximalité de (L_m, M_m, ϕ_m). Cela conclut notre démonstration. □

Définition 4.8.11. En utilisant le Théorème 4.8.10, les clôture algébriques d'un corps K forme une seule classe d'isomorphisme d'extensions de K. On dénote par $\overline{K}$ une représentante arbitraire de cette classe d'isomorphisme, et on dit que c'est **le** clôture algébrique de K.

Remarque 4.8.12. Il y aura une exercice sur la série des exercices affirmant que si K est un corps dénombrable (ou fini), alors $\overline{K}$ est aussi dénombrable. En particulier $\overline{\mathbb{Q}}$ est dénombrable ou encore $\overline{\mathbb{F}}_p$.

4.8.4 La propriété galoisienne

Définition 4.8.13. Pour un corps K, la *clôture séparable* K^{sep} est le sous-corps des éléments séparable sur K dans la clôture algébrique $\overline{K}$ (qui est un corps par le Corollaire 4.7.8). Puisque $\overline{K}$ est unique modulo isomorphisme, le même est vrai pour K^{sep}.

Dans cette section on démontre que pour un corps quelconque K, la clôture séparable K^{sep} et une extension galoisienne de K. Notons, que $K^{\text{sep}} \subseteq \overline{K}$ est purement inséparable par le Corollaire 4.7.8, et donc K^{sep} est le plus grand sous-extension de $K \subseteq \overline{K}$ qui a de chance d'être galoisienne (Proposition 4.6.10).

De plus, on note que si K est parfait (c.f. Proposition 4.5.7), alors $K^{\text{sep}} = \overline{K}$, et par conséquent dans ce cas il suit que $K \subseteq \overline{K}$ est galoisienne. Ce le cas par exemple si $\operatorname{car} K = 0$ (Proposition 4.5.7).

Définition 4.8.14. Une extension $K \subseteq L$ de corps et *normale*, si pour chaque $\alpha \in L$, le polynôme $m_{\alpha,K}$ scinde sur L.

Remarque 4.8.15. On a vu dans le point (3) de la Proposition 4.6.3 que chaque corps de décomposition est normale. En combinant cette affirmation avec le Théorème 4.6.15, on obtient que pour extensions de degré fini, être galoisienne est le même que être normale et séparable.

Pour un corps quelconque l'extension $K \subseteq K^{\text{sep}}$ est normale et séparable par définition. On démontrera que c'est aussi galoisienne en montrant que l'équivalence d'être galoisienne et d'être normale est séparable tient aussi pour les extensions algébriques de degré infini. En particulier, le point clé de la proposition suivante est qu'elle est vrai aussi pour les extensions de degré infini.

Matériel optionnel

Proposition 4.8.16. *Si $K \subseteq L \subseteq M$ sont extension de corps te que $K \subseteq L$ et $K \subseteq M$ sont algébriques, normales et séparables, alors les restrictions des automorphisme donne une surjection* $\operatorname{Gal}(M/K) \twoheadrightarrow \operatorname{Gal}(L/K)$.

Démonstration.

La restriction fait sense : Prenons $\sigma \in \mathrm{Gal}(M/K)$. Il suffit de démontrer que $\sigma(L) \subseteq L$. En effet, si on l'a démontré pour tout élément de $\mathrm{Gal}(M/K)$, alors il est vrai aussi pour σ^{-1}. Cela implique que $\sigma|_L : L \to L$ est surjectif, et alors il est un automorphisme (K-linéaire).

Prenons $\alpha \in L$. Il suffit de démontrer que $\sigma(\alpha) \in L$. Notons que $\sigma(\alpha)$ est aussi une racine de $m_{\alpha,K}$ par point (1) de la Proposition 4.6.3. Ainsi, par la Définition 4.8.14, on obtient que $\sigma(\alpha) \in L$.

Surjectivité : Fixons $\sigma \in \mathrm{Gal}(L/K)$, ce qui on voudrait lever à $\mathrm{Gal}(M/K)$. Considérons l'ensemble partiellement ordonné :

$$(\mathcal{P}, \preceq) = \left\{ (F, \tau) \;\middle|\; \begin{array}{l} L \subseteq F \subseteq M \text{ est un corps intérmédiaire, et } \phi : F \to F \text{ est un} \\ \text{automorphisme qui étend } \sigma \end{array} \right\}$$

avec la relation

$$(F, \tau) \preceq (F', \tau') \iff F \subseteq F', \text{ et } \tau' \text{ étend } \tau.$$

Cette relation est définie dans une manière que chaque chaine (F_i, τ_i) admet automatiquement un majorant $\left(\bigcup_{i\in I} F_i, \tau\right)$, où chaque $\beta \in \bigcup_i F_i$ est contenu dans un F_j est alors $\tau(\beta)$ est défini d'être $\tau_j(\beta) \in F_j \subseteq \bigcup_{i\in I} F_i$.

Par le lemme de Zorn (Lemme 2.5.12), il existe un élément maximal $(F_m, \tau_m) \in (\mathcal{P}, \preceq)$. Si $M = F_m$, alors on est prêt. Ainsi, on peut supposer que $F_m \neq M$. Choisissons $\gamma \in M \setminus F_m$. Notons que par normalité $m_{\gamma,K}$ scinde sur M avec racines $\gamma = \gamma_1, \ldots, \gamma_r$. Le corps $E = F(\gamma_1, \ldots, \gamma_r)$ et le corps de décomposition de $m_{\gamma,K}$ sur F_m. Ainsi, en appliquant Théorème 4.3.4 on peut étendre τ_m de F_m à E, ce qui est une contradiction avec la maximalté de F_m. □

Comme dans le cas de la Proposition 4.8.16, le point clé du théorème suivant est qu'il est vrai aussi pour les extensions de degré infini.

Théorème 4.8.17. *Une extension algébrique $K \subseteq L$ est galoisienne si est seulement si elle est normale et séparable.*

Matériel optionnel

Démonstration.

$\Longrightarrow$: Cela est précisément l'affirmation de la Proposition 4.6.10, pour le cas d'une extension algébrique.

$\Longleftarrow$: Prenons $\alpha \in L \setminus K$. Il suffit de trouver un $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(\alpha) \neq \alpha$, ce que l'on fait dans le paragraphe ci-dessous.

Puisque $K \subseteq L$ est normale est séparable $m_{\alpha,K}$ scinde sur L avec racines distinctes $\alpha = \alpha_1, \ldots, \alpha_r$. Puisque $\alpha \notin K$, on a $r \geq 2$. Notons que $F = K(\alpha_1, \ldots, \alpha_r)$ est le corps de décomposition de $m_{\alpha,K}$. Par point (3) de la Proposition 4.6.3, il existe un $\tau \in \mathrm{Gal}(F/K)$ tel que $\tau(\alpha) = \alpha_2$. Ainsi, on peut utiliser la Proposition 4.8.16 pour l'extensions $K \subseteq F \subseteq L$, pour obtenir le σ désiré. □

Corollaire 4.8.18. *Pour un corps K, l'extension $K \subseteq K^{\text{sep}}$ est galoisienne, avec*

$$\mathrm{Gal}(K^{\text{sep}}/K) = \varprojlim_{\substack{K \subseteq L \text{ galoisienne de} \\ \text{degré fini}}} \mathrm{Gal}(L/K) \overset{\text{def}}{=} \left\{ (\sigma_L) \in \prod_{\substack{K \subseteq L \text{ galoisienne de} \\ \text{degré fini}}} \mathrm{Gal}(L/K) \;\middle|\; \begin{array}{l} \text{pour toutes extensions } K \subseteq \\ L \subseteq M \text{ telles que } K \subseteq L \text{ et} \\ K \subseteq M \text{ sont galoisiennes,} \\ \text{on a } \sigma_M|_L = \sigma_L \end{array} \right\}$$

De plus $K^{\text{sep}} \subseteq \overline{K}$ est purement inséparable.

Matériel optionnel

Démonstration. L'extension $K \subseteq K^{\text{sep}}$ est normale et séparable par définition. Le Théorème 4.8.17 implique donc que cette extension est aussi galoisienne. De plus le Corollaire 4.7.8 nous dit que $K^{\text{sep}} \subseteq \overline{K}$ est purement inséparable.

Il nous reste de démontrer la description de $\mathrm{Gal}(K^{\text{sep}}/K)$. Dans une direction, si $\sigma \in Gal(K^{\text{sep}}/K)$, alors la Proposition 4.8.16 donne une restriction à chaque sous-extension Galoisienne fini. De plus, ces restrictions doivent être compatible parce que ils viennent tous de σ. Dans l'autre direction, si on a un système compatible $\sigma_L \in \mathrm{Gal}(L/K)$, alors on peut définir $\sigma(\beta) = \sigma_L(\beta) \in L \subseteq K^{\text{sep}}$, où $\beta \in L$. Les compatibilités entre les σ_L nous garantissent que cette définition ne dépend pas du choix de L.

□

4.8.5 Clôture purement inséparable est parfait

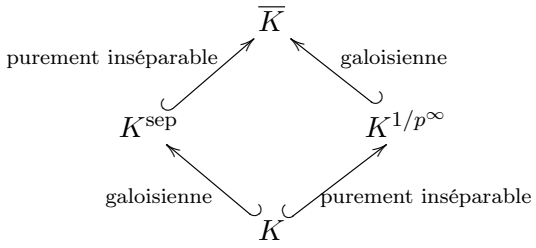
Définition 4.8.19. Pour un corps K de caractéristique $p > 0$, la *clôture purement inséparable* K^{1/p^∞} est le sous-corps des éléments purement inséparable sur K dans la clôture algébrique $\overline{K}$ (c'est un sous-corps par le Corollaire 4.7.9). Puisque $\overline{K}$ est unique modulo isomorphisme, le même est vrai pour K^{1/p^∞}.

Théorème 4.8.20. *Pour un corps K de caractéristique $p > 0$, K^{1/p^∞} est parfait, et par conséquent $K^{1/p^\infty} \subseteq \overline{K}$ est galoisienne (et en particulier $\overline{K}$ est séparable sur K^{1/p^∞}).*

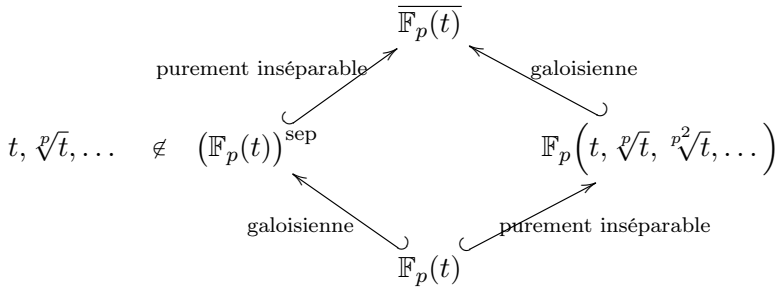
Démonstration. Il suffit de démontrer que K^{1/p^∞} est parfait. En effet, dans ce cas, la clôture séparable de K^{1/p^∞} est la même que la clôture algébrique, et donc on est prêt par le Corollaire 4.8.18.

Par la Proposition 4.5.7, il suffit de vérifier que $L^p = L$ pour $L = K^{1/p^\infty}$. Autrement dit, il suffit de démontrer que pour chaque $\alpha \in L$ si β est un racine p-ième de α dans $\overline{K}$, alors $\beta \in L$. Notons qu'il existe un entier $n \geq 0$ tel que $\alpha^{p^n} \in K$. Par conséquent, $\beta^{p^{n+1}} \in K$, ce qui dit que soit $\beta \in K$ où il est purement inséparable sur K. □

Remarque 4.8.21. On visualise ci-dessous les trois différents types des clôtures, pour un corps K de caractéristique $p > 0$:



Pour $K = \mathbb{F}_p(t)$ on obtient :



Remarque 4.8.22. La clôture purement inséparable, est ses variantes différentes pour d'anneaux, sont essentiel pour la théorie "perfectoid" de Scholze pour laquelle il a reçu la médaille Fields en 2018.