Algèbre L3 S6

Lie Fu

1 Anneaux

1.1 Définition, exemples et premières propriétés

1.1.1 Définition. Un *anneau* est un ensemble A muni de deux lois de composition internes, notées $+$ resp. $\cdot$ et appelées addition resp. multiplication, vérifiant les axiomes suivants.

— $(A, +)$ est un groupe commutatif ; on note donc 0 son élément neutre.
— La loi $\cdot$ est associative.
— Pour tous $x, y, z \in A$ on a (loi de *distributivité*)

$$(x + y)z = xz + yz, \quad z(x + y) = zx + zy,$$

où on écrit xy au lieu de $x \cdot y$ etc.

Si A contient un élément neutre pour la loi $\cdot$, alors cet élément est noté 1_A, ou simplement 1 si cela ne risque pas de causer de confusion. Dans ce cas on dit que A est *unitaire*.
Si la loi $\cdot$ est commutative, on dit que l'anneau est *commutatif*.

1.1.2 Remarques. (i) L'élément 1 est unique (s'il existe). En fait, si $1, 1'$ sont deux éléments neutres pour la loi $\cdot$, on a $1 = 1 \cdot 1' = 1'$.

(ii) Dans tout anneau A on a les règles de calcul suivants :

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x,$$

donc $0 \cdot x = 0$ pour tout $x \in A$ (même si A n'est pas unitaire) et

$$0 = 0 \cdot x = (1 + (-1)) \cdot x = x + (-1) \cdot x,$$

donc $(-1) \cdot x = -x$ pour tout $x \in A$. On voit de la même façon (laissé comme exercice !)

$$(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$$

pour tous $x, y \in A$, même si A est non-unitaire et que $(-x) \cdot (-y) = x \cdot y$.

(iii) $\{0\}$ est un anneau unitaire dans lequel $1 = 0$. Si A est un anneau unitaire contenant au moins deux éléments, alors $0 \neq 1$. En fait, si $x \neq 0$ on a $1 \cdot x = x$, $0 \cdot x = 0$, donc $1 \neq 0$.

1.1.3 Exemples. (i) L'anneau 0. C'est le seule anneau unitaire avec $1 = 0$.

(ii) Munis des opérations habituelles, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs unitaires. L'ensemble $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$, muni de l'addition et la multiplication des entiers est un anneau non-unitaire.

(iii) Si $n > 1$ est un entier, alors $\mathbb{Z}/n\mathbb{Z}$ est un anneau unitaire commutatif dans lequel $1 \neq 0$. On reviendra plus tard sur la construction générale des anneaux quotient.

(iv) Pour tout anneau unitaire commutatif, l'ensemble $M_n(A)$ des matrices $n \times n$ à coefficients dans A, muni de l'addition et de la multiplication matricielle, est un anneau unitaire. Il est non-commutatif si $n \geq 2$ et $A \neq \{0\}$.

(v) Si E est un ensemble et A est un anneau, alors A^E, l'ensemble des applications de E dans A, muni de l'addition et de la multiplication point par point, est un anneau. Il est commutatif resp. unitaire, si A l'est. Si $E = \mathbb{N}$ ou $E = \mathbb{N}^*$ alors un élément de A^E est une suite dans A indexé par les entiers $i \geq 0$, resp. $i \geq 1$.

(vi) On peut interpréter l'exemple précédent comme l'espace des fonctions sur un ensemble à valeurs dans un anneau A. De manière similaire, l'espace des fonctions continues sur un espace topologique à valeurs dans un anneau topologique A est un anneau, avec la loi "point par point".

(vii) L'anneau des endomorphismes d'un groupe *abélien*, avec la loi d'addition "point par point" et la loi de multiplication donnée par composition. C'est un anneau *non commutatif* en générale.

Dans la suite, sauf mention du contraire, on entend par anneau toujours un *anneau unitaire*.

1.1.4 Polynômes.

Si A est un anneau commutatif (unitaire) alors on définit l'annéau des polynômes à coefficients dans A, noté $A[X]$ de la manière suivante.
Si E est un ensemble, alors on note $A^{(E)} \subset A^E$ l'ensemble des applications f telles que $\{x \in E \mid f(x) \neq 0\}$ est fini. Si $E = \mathbb{N}$ alors $A^{(\mathbb{N})}$ est donc l'ensemble des suites $(\lambda_0, \lambda_1, \ldots)$ d'éléments de A tel qu'il existe un $N \in \mathbb{N}$ avec $\lambda_i = 0$ pour $i > N$. On munit $A^{(\mathbb{N})}$ de l'addition habituelle des suites et de la multiplication définie par

$$(\lambda_0, \lambda_1, \ldots) \cdot (\mu_0, \mu_1, \ldots) = (\nu_0, \nu_, \ldots)$$

où $\nu_n = \sum_{i=0}^{n} \lambda_i \mu_{n-i}$. On vérifie que la somme et le produit de deux éléments de $A^{(\mathbb{N})}$ appartiennent bien à $A^{(\mathbb{N})}$ et que les deux opérations donnent bien lieu à la structure d'anneau. On note $A[X]$ ce anneau.
L'élément $(0, 1, 0, \ldots) \in A[X]$ est désigné par X et on écrit simplement λ pour la suite $(\lambda, 0, \ldots)$. On vérifie alors que, pour $i \geq 0$ on a $X^i = (0, \ldots, 0, 1, 0, \ldots)$ et plus généralement $\lambda \cdot X^i = (0, \ldots, 0, \lambda, 0, \ldots)$, avec le 1 resp. le λ à la $i$ème position. Le polynôme $P = (\lambda_0, \lambda_1, \ldots) \in A[X]$ est alors égal à la somme finie $\sum_{i \geq 0} \lambda_i X^i$.

1.1.5 Définition. (i) Soient A et B deux anneaux unitaires. Une application $\varphi\colon A \to B$ est appelé *morphisme d'anneaux* si φ vérifie les conditions
— $\varphi(x + y) = \varphi(x) + \varphi(y)$ pour tous $x, y \in A$
— $\varphi(xy) = \varphi(x)\varphi(y)$ pour tous $x, y \in A$
— $\varphi(1_A) = 1_B$.

(ii) Un sous-ensemble B d'un anneau A est appelé *sous-anneau* si $1_A \in B$ et les lois $+$ et $\cdot$ définissent sur B la structure d'un anneau.

1.1.6 Remarques. (i) Dans 1.1.5(i), la première condition dit que φ est un morphisme de groupes additifs $(A, +) \to (B, +)$. En particulier, $\varphi(0_A) = 0_B$. Par contre, la deuxième condition n'entraîne pas la dernière. En effet, l'application $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \quad n \mapsto (n, 0)$ (avec l'addition et multiplication évidente sur $\mathbb{Z} \times \mathbb{Z}$) satisfait les deux premières conditions mais pas la dernière et ce n'est donc pas un morphisme.

(ii) De même, dans la partie 1.1.5(ii) il faut exiger que $1_A \in B$ car les opérations $+$ et $\cdot$ définissent sur l'ensemble $\mathbb{Z} \times \{0\} \subset \mathbb{Z} \times \mathbb{Z}$ la structure d'anneau unitaire mais $\mathbb{Z} \times \{0\}$ n'est pas un sous-anneau de $\mathbb{Z} \times \mathbb{Z}$.

(iii) Il est évident que pour tout anneau A, l'identité id_A est un morphisme d'anneaux. Si $B \subset A$ est un sous-anneau alors l'inclusion naturelle est un morphisme d'anneaux. Le composé de deux morphismes d'anneaux est un morphisme d'anneaux.

(iv) Un morphisme d'anneaux $\varphi\colon A \to B$ est un *isomorphisme* si et seulement s'il existe un morphisme d'anneaux $\psi\colon B \to A$ tels que φ et ψ sont inverses l'une de l'autre. En fait, si φ est un morphisme bijectif d'anneaux, alors l'inverse est également un morphisme d'anneaux. Un isomorphisme d'un anneau A dans lui-même est appelé *automorphisme* de l'anneau A.

(v) Si $\varphi\colon A \to B$ est un morphisme d'anneau, alors *le noyau* de φ est l'énsemble $\{x \in A \mid \varphi(x) = 0\}$. Il est noté $\operatorname{Ker} \varphi$.

1.1.7 Exemples. (i) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ est une suite des inclusions des sous-anneaux.

(ii) Si A est un anneau commutatif alors A est un sous-anneau de $A[X]$. Il est également isomorphe au sous-anneau des matrices diagonales de $M_n(A)$.

(iii) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ et $\mathbb{Z}[i] = \{x + yi \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ sont des anneaux commutatifs unitaires, ce sont en effet des sous-anneaux de $\mathbb{C}$ (et le premier est aussi un sous-anneau de $\mathbb{R}$).

(iv) L'ensemble
$$\left\{ \frac{p}{10^n} \mid p \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$$
des nombres décimaux est un sous-anneau de $\mathbb{Q}$.

(v) Si A est un anneau, les ensembles
$$\left\{ P = \sum_{i=1}^{d} \lambda_i X^i \in A[X] \mid \lambda_1 = 0 \right\}$$
et $\{P \in A[X] \mid P(1) = P(-1)\}$ sont des sous-anneaux de $A[X]$.

(vi) Pour tout anneau A il existe un morphisme $\varphi\colon \mathbb{Z} \to A$ d'anneaux et un seul. Il est donné par $\varphi(n) = 1_A + \cdots + 1_A$ pour $n \in \mathbb{N}^*$ (où la somme comporte n termes), $\varphi(0) = 0$ et $\varphi(-n) = -\varphi(n)$ pour $n \in \mathbb{N}^*$.

(vii) L'anneau des *quaternions* réels est l'ensemble
$$\mathbb{H} = \left\{ \begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix} \in M_2(\mathbb{C}) \right\}.$$
C'est un sous-anneau unitaire non-commutatif de $M_2(\mathbb{C})$. L'application $\mathbb{C} \to \mathbb{H}$ donnée par $z \mapsto \left(\begin{smallmatrix} z & 0 \\ 0 & \bar{z} \end{smallmatrix}\right)$ est un morphisme injectif d'anneaux qui identifie $\mathbb{C}$ avec un sous-anneau (commutatif) de $\mathbb{H}$.

1.1.8 Évaluation des polynômes.

Soient $\varphi\colon A \to B$ un morphisme d'anneaux avec A commutatif et $b \in B$ tel que $\varphi(a)b = b\varphi(a)$ pour tout $a \in A$. Alors il existe un unique morphisme d'anneaux $\tilde{\varphi}_b\colon A[X] \to B$ tel que $\tilde{\varphi}_b|_A = \varphi$ et $\tilde{\varphi}_b(X) = b$. En effet, pour $P = \sum_{i=0}^{n} \lambda_i X^i \in A[X]$ on a nécessairement
$$\tilde{\varphi}(P) = \sum_{i=0}^{n} \varphi(\lambda_i) b^i$$
et on vérifie que cette formule définit bien un morphisme d'anneaux. L'anneau $A[X]$ est caractérisé par cette propriété.
Si $A \subset B$ est un sous-anneau, et φ l'inclusion naturelle, alors le morphisme $\tilde{\varphi}_b$ est noté ev_b et appelé *l'évaluation* en b. On note généralement $P(b) = \mathrm{ev}_b(P)$.

1.1.9 Remarque. La construction s'applique notamment à l'inclusion $A \subset M_n(A)$ des matrices scalaires dans l'ensemble des matrices carrés à coefficients dans A.

1.1.10 Définition. Soient A un anneau et $x \in A$. On dit que x est un *inversible* de A s'il existe $y \in A$ tel que $yx = xy = 1$. L'ensemble des inversibles de A est noté $A^\times$.

1.1.11 Remarques. (i) Pour que $x \in A$ soit une unité il faut et il suffit qu'il existe un inverse à gauche y et un inverse à droite z pour la multiplication. En fait, si y et z sont des inverses à gauche et à droite respectivement alors on a $y = y1_A = y(xz) = (yx)z = 1_A z = z$.

(ii) L'inverse de x, s'il existe, est unique. Il est noté x^{-1}.

(iii) Dans la littérature on trouve aussi la terminologie « unité »au lieu de « élément inversible ».

1.1.12 Proposition. *L'ensemble des inversibles de A est un groupe pour la multiplication dans A.*

Démonstration. Si x et y sont inversibles alors xy est une unité ; en fait $y^{-1}x^{-1}$ est l'inverse de xy. Donc la multiplication determine une loi interne sur $A^\times$ et il est laissé comme exercice à vérifier que $A^\times$ est un groupe pour cette loi. □

1.1.13 Exemples. (i) $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Q}^\times = \mathbb{Q}\setminus\{0\}, \mathbb{R}^\times = \mathbb{R}\setminus\{0\}, \mathbb{C}^\times = \mathbb{C}\setminus\{0\}$.

(ii) Si $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ on a $A[X]^\times = A^\times$. En fait, si P, Q sont des polynômes de degré n resp. m, alors $P \cdot Q$ est un polynôme de degré $n+m$, donc les seules polynômes qui peuvent être inversibles sont de degré 0 et un polynôme de degré 0 est inversible si et seulement si il l'est en tant qu'élément de A.

Notons que dans l'anneau $\mathbb{Z}/4\mathbb{Z}[X]$, le polynôme $2X + 1$ est inversible sans appartenir à $(\mathbb{Z}/4\mathbb{Z})^\times$.

(iii) Pour les quaternions on a $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$.

1.1.14 Définition. (i) Soit A un anneau commutatif. Un élément $x \in A$ est appelé *diviseur de* 0 si $x \neq 0$ et s'il existe $y \in A$ avec $y \neq 0$ tel que $xy = 0$.

(ii) Un anneau A commutatif est *intègre* si $0 \neq 1$ et si A ne contient pas de diviseurs de 0.

1.1.15 Remarques. (i) Si A est un anneau commutatif et si $x \in A^\times$ alors x n'est pas un diviseur de 0. En effet, si $xz = 0$ alors $0 = x^{-1} \cdot 0 = x^{-1}xz = z$.

(ii) Un anneau commutatif est donc intègre si et seulement si $1 \neq 0$ et si $xy = 0$ implique $x = 0$ ou $y = 0$.

1.1.16 Exemples. (i) Les diviseurs de 0 dans $\mathbb{Z} \times \mathbb{Z}$ sont les éléments $(n, 0)$ et $(0, n)$ avec $n \neq 0$. L'anneau $\mathbb{Z} \times \mathbb{Z}$ n'est donc pas intègre.

(ii) Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[i]$ sont intègres.

(iii) Si A est intègre, alors $A[X]$ l'est aussi et dans ce cas on a $A[X]^\times = A^\times$. En fait, l'argument de l'exemple 1.1.13(ii) fonctionne pour tout anneau intègre A.

1.1.17 Proposition. *Soient $n > 0$ un entier et $0 \neq x \in \mathbb{Z}/n\mathbb{Z}$. On fixe un représentant a de x. Alors les conditions suivantes sont équivalentes.*

(i) x est une unité dans $\mathbb{Z}/n\mathbb{Z}$.

(ii) x n'est pas un diviseur de 0 dans $\mathbb{Z}/n\mathbb{Z}$.

(iii) n et a sont premiers entre eux.

Démonstration. Il est clair que 1.1.17(i) entraîne 1.1.17(ii).
Si $x \neq 0$ n'est pas un diviseur de 0, alors l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, y \mapsto xy$ est injective, donc bijective, donc x est une unité dans $\mathbb{Z}/n\mathbb{Z}$, c.-à.-d. 1.1.17(ii) entraîne 1.1.17(i).
Des entiers a et n sont premiers entre eux si et seulement s'il existe des entiers r et s tel que $ar + ns = 1$. C'est le cas si et seulement si il existe r tel que $\overline{a} \cdot \overline{r} = 1$, ce qui est équivalent à ce que $x = \overline{a}$ est une unité dans $\mathbb{Z}/n\mathbb{Z}$. On a montré que 1.1.17(i) est équivalent à 1.1.17(iii). □

1.1.18 Corollaire. *Soit $n \geq 0$ un entier. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si est seulement si $n = 0$ ou $n = p$ avec p un nombre premier.*

1.2 Idéaux.

Dans la suite on va étudier surtout les anneaux commutatifs unitaires. En fait, sauf explicite au contraire, dans la suite le mot *algèbre* signifera anneau commutatif unitaire.

1.2.1 Définition. Soit A un anneau commutatif. Un sous-ensemble $I \subset A$ est appelé *idéal* de A si I vérifie les conditions suivantes :
— I est un sous-groupe additif et
— pour tous $x \in I$, $a \in A$ on a $ax \in I$.

1.2.2 Exemples. (i) Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ est un idéal.

(ii) Si $\varphi\colon A \to B$ est un morphisme d'anneaux, alors le noyau de φ est un idéal de A.

(iii) En généralisant le premier exemple, pour tous anneau commutatif A et $a \in A$,

$$(a) = aA = \{ax \mid x \in A\}$$

est un idéal dans A, appelé *l'idéal principal engendré par a*.
On voit en particulier que $(0) = \{0\}$ et $(1) = A$ sont des idéaux. Un élément $a \in A$ est une unité dans A si et seulement $(a) = A$ (laissé comme exercice !).

1.2.3 Proposition. *Soient A un anneau commutatif unitaire et $I \subset A$ un idéal. On note A/I le groupe quotient du groupe additif de A par le sous-groupe (distingué) I.*

(i) Il existe sur A/I une structure d'anneau, et une seule, telle que la projection canonique $\pi_I \colon A \to A/I$ est un morphisme d'anneau. L'anneau A/I est commutatif.

(ii) Le morphisme $\pi_I \colon A \to A/I$ vérifie la propriété universelle *suivante. Si $\varphi \colon A \to B$ est un morphisme d'anneaux tel que $I \subset \operatorname{Ker} \varphi$, alors il existe un unique morphisme d'anneaux $\overline{\varphi} \colon A/I \to B$ tel que $\varphi = \overline{\varphi} \circ \pi_I$.*

Démonstration. Prouvons 1.2.3(i). On sait de la théorie des groupes que A/I est un groupe abélien et l'application canonique $\pi \colon A \mapsto A/I$ qui associé à un élément $a \in A$ sa classe $\overline{a} = \pi(a)$ est un morphisme des groupes. Pour $a, b \in A$ et $x, y \in I$ on a

$$(a + x)(b + y) = ab + xb + ay + xy$$

et comme $xb + ay + xy \in I$, l'application

$$A/I \times A/I \to A/I, \quad \overline{a} \cdot \overline{b} \mapsto \overline{ab}$$

est bien défini. C'est la seule loi multiplicative sur A/I pour laquelle π_I peut-être un morphisme d'anneaux. Parce que π est surjective, l'associativié, la distributivité et la commutativité dans A/I sont des conséquences de l'associativié, de la distribituvité et de la commutativité dans A. De même il est clair que $\overline{1}$ est l'unité dans A/I. La définition de la multiplication dans A/I entraîne immédiatement que π est un morphisme d'anneaux.
Passons à 1.2.3(ii). On sait que l'application $\overline{\varphi} \colon A/I \to B$, définie par $\overline{\varphi}(\overline{a}) = \varphi(a)$ est bien définie et que c'est un morphisme des groupes. De plus on a clairement $\overline{\varphi}(\overline{1}) = \varphi(1_A) = 1_B$ et, pour $\overline{a}, \overline{b}$ on a

$$\overline{\varphi}(\overline{a}\overline{b}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}),$$

donc $\overline{\varphi}$ est un morphisme d'anneaux. L'unicité de $\overline{\varphi}$ est également garantie par la théorie des groupes. □

1.2.4 Corollaire. *Soit $\varphi \colon A \to B$ un morphisme surjectif d'anneaux commutatifs unitaires. Alors φ induit un isomorphisme $\overline{\varphi} \colon A/\operatorname{Ker} \varphi \to B$.*

Démonstration. On applique la Proposition 1.2.3 avec $I = \operatorname{Ker} \varphi$. On vérifie facilement que le morphisme $\overline{\varphi} \colon A/\operatorname{Ker} \varphi \to B$ est un isomorphisme. □

1.2.5 Exemples. (i) Pour $A = \mathbb{Z}$ et $I = n\mathbb{Z}$ on obtient l'anneau $A/I = \mathbb{Z}/n\mathbb{Z}$. Si n, m sont des entiers et si n est un multiple de m, alors $n\mathbb{Z} \subset m\mathbb{Z}$ et donc le noyau de la projection canonique $\pi \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ contient $n\mathbb{Z}$. On obtient alors un morphisme d'anneaux (canonique) $\overline{\pi} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

(ii) Soit $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Fixons $a \in A$ et posons $I = (X - a)$, alors l'évaluation $\mathrm{ev}_a \colon A[X] \to A$ est un morphisme d'anneaux surjectif. On verra dans la suite que son noyau est I (cela utilise la division euclidiennes de polynômes, on reviendra là-dessus plus tard) donc ev_a induit un isomorphisme $\overline{\mathrm{ev}_a} \colon A[X]/I \cong A$.

(iii) L'application $\mathbb{R}[X] \to \mathbb{C}$, $P = \sum_k \lambda_k X^k \mapsto P(i)$ est un morphisme surjectif d'anneaux, son noyau est $I = (X^2 + 1)$ (on justifiera cela formellement plus tard par la division euclidienne des polynômes). On obtient un isomorphisme $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

1.2.6 Proposition. *Soient A un anneau commutatif unitaire, E un ensemble non-vide et pour tout $\alpha \in E$ soit I_α un ideal de A. Soit enfin $X \subset A$ un sous-ensemble de A.*

(i) L'intersection $\bigcap_{\alpha \in E} I_\alpha$ est un idéal.

(ii) L'ensemble de tous les idéaux de A contenant X est non-vide et

$$\bigcap_{\substack{I \text{ est un idéal} \\ X \subset I \subset A}} I$$

est le plus petit l'idéal de A qui contient X. Il est appelé l'idéal engendré *par X et il est noté (X).*

(iii) Si $E = \{1, \ldots, n\}$ et si $\prod_{k=1}^n I_k$ désigne l'idéal engendré par l'ensemble $\{\prod_{k=1}^n x_k \mid x_k \in I_k\}$ alors

$$\prod_{k=1}^n I_k \subset \bigcap_{k=1}^n I_k.$$

(iv) Si $E = \{1, \ldots, n\}$ et si $I_{k_1} + I_{k_2} = A$ pour tous $k_1 \neq k_2$, alors on a une égalité $\prod_{k=1}^n I_k = \bigcap_{k=1}^n I_k$.

Démonstration. Montrons 1.2.6(i). On sait de la théorie des groupes que $\bigcap_{\alpha \in E} I_\alpha$ est un sous-groupe de $(A, +)$. Soient $x \in \bigcap_{\alpha \in E} I_\alpha$ et $a \in A$. Alors pour tout $\alpha \in E$ on a $x \in I_\alpha$, donc $ax \in I_\alpha$, donc $ax \in \bigcap_{\alpha \in E} I_\alpha$.
Pour 1.2.6(ii), notons que l'ensemble des idéaux de A est non-vide parce que A lui-même est un idéal qui contient X. D'après 1.2.6(i), l'intersection considérée ici est un idéal. Il contient X par construction et il est contenu dans tout idéal contenant X.
En ce qui concerne 1.2.6(iii), il est clair que l'ensemble

$$\left\{ \prod_{k=1}^n x_k \mid x_k \in I_k \right\}$$

est contenu dans l'idéal $\bigcap_{k=1}^n I_k$, donc l'idéal engendré par cet ensemble est contenu dans $\bigcap_{k=1}^n I_k$.
On démontre enfin 1.2.6(iv) par recurrence sur n. Pour $n = 1$ il n'y a rien à montrer. Si $n = 2$ l'hypothèse dit qu'il existe $x \in I_1, y \in I_2$ tel que $x + y = 1$. Soit $z \in I_1 \cap I_2$. Alors $z = z \cdot 1 = z(x + y) = zx + zy \in I_1 I_2$ parce que zx et zy appartiennent tous les deux à $I_1 I_2$.
Supposons maintenant que la conclusion est vraie au rang $n \geq 2$. Pour tout $1 \leq k \leq n$ il existe $x_k \in I_{n+1}$ et $y_k \in I_k$ tel que $x_k + y_k = 1$. Alors $1 = \prod_{k=1}^n (x_k + y_k)$ est une somme des 2^n produits, le produit $\prod_{k=1}^n y_k$ appartient à $\prod_{k=1}^n I_k$ et tous les autres produits appartiennent à I_{n+1}. On en déduit que

$$\prod_{i=1}^n I_k + I_{n+1} = A$$

et cela implique que l'hypothèse du cas $n = 2$ est donc vérifiée pour les idéaux $\prod_{k=1}^n I_k$ et I_{n+1}. Avec cette observation et l'hypothèse de récurrence on obtient

$$\bigcap_{k=1}^{n+1} I_k = \bigcap_{k=1}^{n} I_k \cap I_{n+1} = \left(\prod_{k=1}^n I_k\right) \cap I_{n+1} = \left(\prod_{k=1}^n I_k\right) \cdot I_{n+1} = \prod_{k=1}^{n+1} I_k.$$

□

1.2.7 Remarque. Si $a \in A$, alors on a $(\{a\}) = (a)$ où (a) est l'idéal principal engendré par a, voir la définition 1.2.2(iii). Plus généralement, si $X = \{a_1, \ldots, a_n\}$ est un ensemble fini, on écrit $(a_1, \ldots, a_n)$ au lieu de $(X) = (\{a_1, \ldots, a_n\})$.

1.2.8 Définition. Soient E et les idéaux I_α, pour $\alpha \in E$ comme dans la proposition 1.2.6. Alors on note

$$\sum_{\alpha \in E} I_\alpha$$

l'idéal engendré par $\cup_{\alpha \in E} I_\alpha$.

On utilise la 1.2.6(iv) pour établir une généralisation du lemme chinois.

1.2.9 Théorème. *Soit A un anneau commutatif unitaire et, pour $k = 1, \ldots, n$, soit I_k un idéal de A tel que $I_{k_1} + I_{k_2} = A$ si $k_1 \neq k_2$. En notant par π_k le morphisme π_{I_k} de la proposition 1.2.3, l'application $\pi \colon A \to \prod_{k=1}^n A/I_k$ définie par $\pi(a) = (\pi_1(a), \ldots, \pi_n(a))$ induit un isomorphisme*

$$\overline{\pi} \colon A \Big/ \bigcap_{k=1}^n I_k \to \prod_{k=1}^n A/I_k.$$

Démonstration. Il est clair que l'application π est un morphisme d'anneaux de noyau $\bigcap_{k=1}^{n} I_n$. D'après le corollaire 1.2.4 il suffit de montrer que π est surjectif. On raisonne par récurrence.
Si $n = 2$ et si $x_1 \in I_1$ et $x_2 \in I_2$ satisfont $x_1 + x_2 = 1$ alors

$$(1,1) = 1 = \pi(1) = \pi(x_1) + \pi(x_2) = (\pi_1(x_1) + \pi_1(x_2), \pi_2(x_1) + \pi_2(x_2)) = \\ (\pi_1(x_2), \pi_2(x_1)).$$

Pour $z = (z_1, z_2) \in A/I_1 \times A/I_2$ il existe $a_1, a_2 \in A$ tels que $z = (\pi_1(a_1), \pi_2(a_2))$. Alors on a

$$\pi(a_1x_2 + a_2x_1) = (\pi_1(a_1x_2), \pi_2(a_2x_1)) = (\pi_1(a_1), \pi_2(a_2)) = (z_1, z_2) \ .$$

Supposons ensuite que l'énoncé est vrai au rang $n \geq 2$. Pour $n + 1$ on écrit π comme composition des morphismes canoniques suivants

$$A \to \left(A \Big/ \prod_{k=1}^{n} I_k, A/I_{n+1} \right) = \left(A \Big/ \bigcap_{k=1}^{n} I_k, A/I_{n+1} \right) \to \prod_{k=1}^{n} A/I_k \times A/I_{n+1} \ .$$

Comme $\prod_{k=1}^{n} I_k + I_{n+1} = A$ d'après la démonstration de la proposition 1.2.6(iv) et le dernier morphisme est un isomorphisme par l'hypothèse de récurrence, π est surjective au rang $n + 1$. □

1.2.10 Définition. On définit la fonction *indicatrice d'Euler* $\varphi\colon \mathbb{N}^* \to \mathbb{N}$ par $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

1.2.11 Proposition. *(i) Si m et $n \in \mathbb{N}^*$ sont premiers entre eux, alors on a $\varphi(mn) = \varphi(m)\varphi(n)$.*

(ii) Soient p un nombre premier et $n > 0$ un entier. Alors $\varphi(p^n) = (p-1)p^{n-1}$.

Démonstration. Si m et n sont premiers entre eux alors le théorème 1.2.9 s'applique à l'anneau $\mathbb{Z}$ et aux idéaux (m) et (n) et affirme que l'application

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

est un isomorphisme d'anneaux. On en déduit la première affirmation.
La deuxième affirmation est une conséquence immédiate de la proposition 1.1.17 car $\overline{a}$ est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$ si et seulement si $(a, p^n) = 1$ si et seulement si a n'est pas divisible par p. □

1.2.12 Exemples. (i) $\varphi(8) = 4$ et le groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^\times$ est isomorphe au groupe aditif $(\mathbb{Z}/2\mathbb{Z})^2$. En fait les éléments non-triviaux de $(\mathbb{Z}/8\mathbb{Z})^\times$ sont $\overline{3}, \overline{5}, \overline{7}$ et ils sont d'ordre 2 parce que $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod (8)$.

(ii) $\varphi(9) = 6$ et le groupe $(\mathbb{Z}/9\mathbb{Z})^\times$ est un groupe abélien de cardinal 6, donc il est cyclique d'ordre 6. En fait, on voit facilement que $\overline{2}$ est un générateur.

1.2.13 Définition. Soit A un anneau commutatif unitaire. On dit qu'un idéal $P \subset A$ est un *idéal premier* si $P \neq A$ et pour tous $a, b \in A$ la condition $ab \in P$ implique $a \in P$ ou $b \in P$.

1.2.14 Proposition. *Soit A un anneau commutatif unitaire. Un idéal $P \subset A$ est premier si et seulement si A/P est intègre.*

Démonstration. Supposons que P est un idéal premier et soient $x, y \in A/P$ tel que $xy = 0$. Alors il existe $a, b \in A$ tel que $x = \overline{a}$ et $y = \overline{b}$ et on a $0 = xy = \overline{ab}$, donc $ab \in P$ et comme P est premier on a $a \in P$ ou $b \in P$, donc $x = 0$ ou $y = 0$. Comme $P \neq A$ on a $\overline{0} \neq \overline{1}$, donc A/P est intègre.
Supposons que A/P est intègre, alors $\overline{0} \neq \overline{1}$ dans A/P donc $1 \notin P$ et $P \neq A$. Si $a, b \in A$ tel que $ab \in P$ alors $\overline{a}\overline{b} = \overline{ab} = 0$ et donc $\overline{a} = 0$ ou $\overline{b} = 0$, c.-à.-d. $a \in P$ ou $b \in P$. On conclut que P est premier. □

1.2.15 Définition. Soit A un anneau commutatif unitaire. On dit qu'un idéal $M \subset A$ est un *idéal maximal* si
— $M \neq A$ et
— pour tout idéal $I \neq A$ avec $M \subset I$ on a $I = M$.

1.2.16 Définition. Un anneau commutatif K est appelé *corps* si $1 \neq 0$ et tout $x \in K \setminus \{0\}$ est une unité. Autrement dit, K est un corps si et seulement si $K \setminus \{0\}$ est un groupe pour la multiplication.

1.2.17 Exemples. (i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps mais $\mathbb{Z}$ n'est pas un corps. Il résulte de la proposition 1.1.17 que, pour $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.

(ii) Si K est un corps, alors $K[X]$ n'est jamais un corps.

(iii) La remarque 1.1.15(i) implique qu'un corps est un anneau intègre.

1.2.18 Proposition. *Soit A un anneau commutatif unitaire. Un idéal $M \subset A$ est maximal si et seulement si A/M est un corps.*

Démonstration. Supposons que M est maximal, alors $M \neq A$ donc $1 \notin M$ et $\overline{0} \neq \overline{1}$ dans A/M. Soit $0 \neq x \in A/M$. Alors il existe $a \in A \setminus M$ tel que $x = \overline{a}$. L'idéal $I = (M \cup \{a\})$ (cf. 1.2.6(ii)) est un idéal qui contient strictement M, donc $I = A$ parce que M est maximal. Cela implique qu'il existe $r \in A$ et $m \in M$ tel que $ar + m = 1$. Alors on a $x\overline{r} = \overline{ar + m} = \overline{1}$, donc x est inversible dans A/M et A/M est un corps.

Supposons que A/M est un corps, alors $\overline{0} \neq \overline{1}$ donc $1 \notin M$ et $M \neq A$. Soient I un idéal de A qui contient strictement M et $a \in I \setminus M$. Alors $\overline{a} \neq 0$, donc il existe $x \in A/M$ tel que $\overline{a}x = \overline{1}$. Il existe $b \in A$ avec $\overline{b} = x$ et donc $\overline{1 - ab} = \overline{1} - \overline{ab} = 1 - \overline{a}x = \overline{0}$, c.-à.-d. $1 - ab \in M$, donc $1 = ab + (1 - ab) \in I$, ce qui montre que $I = A$ et M est maximal. □

1.3 Anneaux principaux

1.3.1 Définition. Soit A un anneau commutatif unitaire et soient $a, b \in A$.

(i) On dit que b *divise* a, que b est un *diviseur* de a ou encore que a est un *multiple* de b s'il existe $c \in A$ tel que $a = bc$. On écrit alors $b|a$.

(ii) On dit que a est *irréductible* si $a \neq 0$, si a n'est pas inversible et si pour $c, d \in A$ avec $a = cd$ on a que soit c soit d est inversible.

1.3.2 Remarques. (i) Dans les anneaux $\mathbb{Z}$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ les notions de diviseur et du multiple sont les notions habituelles bien connues.

(ii) Dans $\mathbb{Z}$ un entier n est irréductible si et seulement si $n = \pm p$ avec p un nombre premier.

1.3.3 Lemme. *Soit A un anneau commutatif unitaire et soient $a, b \in A$.*

(i) b divise a si et seulement si $(a) \subset (b)$.

(ii) S'il existe $u \in A^\times$ tel que $a = ub$ alors $(a) = (b)$.

(iii) Si A est intègre alors $(a) = (b)$ si et seulement s'il existe $u \in A^\times$ tel que $a = ub$.

Démonstration. Les deux implications de 1.3.3(i) sont évidentes.
Pour 1.3.3(ii), supposons qu'il existe $u \in A^\times$ tel que $a = ub$, alors b divise a donc $(a) \subset (b)$. Mais on a également $b = u^{-1}a$, donc a divise b et $(b) \subset (a)$.
Pour la dernière affirmation, on vient de prouver l'implication réciproque. Pour l'implication directe supposons que $(a) = (b)$. Si $a = 0$ alors $(b) = (a) = (0) = \{0\}$ donc $b = 0 = 1 \cdot a$. Si $a \neq 0$ alors l'hypothèse implique qu'il existe $u, v \in A$ tels que $b = ua$ et $a = vb$ et donc $a = vua$. On en déduit que $0 = a - vua = a(1 - vu)$ et comme A est intègre cela donne $uv = 1$, c'est-à-dire que $u, v \in A^\times$. □

1.3.4 Définition. Un anneau commutatif unitaire A est appelé *anneau principal* si A est intègre et tout ideal I de A est principal, c.-à.-d. pour tout idéal $I \subset A$ il existe $a \in A$ tel que $I = (a) = \{\lambda a \mid \lambda \in A\}$.

1.3.5 Exemple. $\mathbb{Z}$ est un anneau principal. En fait, $\mathbb{Z}$ est intègre. De plus, si I est un idéal de $\mathbb{Z}$ alors I est en particulier un sous-groupe de $\mathbb{Z}$, donc il existe un entier $n \geq 0$ tel que $I = n\mathbb{Z}$. Or, $n\mathbb{Z} = (n)$ est un idéal principal. Notons qu'on vient de montrer que tout sous-groupe additif de $\mathbb{Z}$ est un idéal et que tous les idéaux de $\mathbb{Z}$ sont de la forme de l'exemple 1.2.2(i).

1.3.6 Proposition. *Soient A un anneau principal et $a \in A$ avec $a \neq 0$. Alors les conditions suivantes sont équivalentes.*

- *L'idéal (a) est maximal.*
- *L'idéal (a) est premier.*
- *L'élément a est irréductible.*

Démonstration. D'après les propositions 1.2.14 et 1.2.18, la première condition implique la deuxième.
Supposons ensuite que (a) est un idéal premier, alors $(a) \neq A = (1)$ et a n'est pas une unité. Si $a = bc$ alors $b \in (a)$ ou $c \in (a)$. Supposons que $c \in (a)$, alors il existe $u \in A$ tel que $c = ua$ donc $a = bc = bua$ et enfin $a(1 - bu) = 0$. Comme A est intègre et $a \neq 0$ on en déduit $1 = bu$ donc $b \in A^\times$. De même, si $b \in (a)$ alors $c \in A^\times$ et a est donc irréductible.
Finalement supposons que a est irréductible. Il suffit de montrer que (a) est un idéal maximal. Notons d'abord que $(a) \neq A$, sinon on voit comme avant que $a \in A^\times$, en contradiction avec l'hypothèse que a est irréductible. Soit $I \subset A$ un idéal qui contient (a). Comme A est principal I est un idéal principal donc il existe $b \in A$ tel que $I = (b)$. Comme $a \in (b)$, il existe $c \in A$ tel que $a = bc$ et a étant irréductible on a soit $b \in A^\times$, soit $c \in A^\times$. Dans le premier cas $I = A$ et dans le deuxième cas $I = (a)$. L'idéal (a) est donc bien un idéal maximal. □

Dans un anneau principal A les élements $a \neq 0$ se factorisent de manière essentiellement unique comme un produit des facteurs irréductibles.

1.3.7 Définition. On dit que deux élements irréductibles p, q d'un anneau commutatif unitaire A sont *associés* s'il existe $u \in A^\times$ tel que $p = uq$.

1.3.8 Remarques.
(i) Il est facile à voir que cette rélation est une rélation d'équivalence.
(ii) Si p et q sont irréductibles et $p|q$ alors p et q sont associés.

1.3.9 Définition. On note I l'ensemble des classes d'équivalence et on choisit pour chaque classe $i \in I$ un représentant p_i de cette classe.

1.3.10 Théorème. *Soit A un anneau principal et soit $0 \neq a \in A$.*

(i) Il existe des entiers $\alpha_i \geq 0$ qui sont nuls sauf pour un nombre fini de i et une unité u tels que

$$a = u \prod_{i \in I} p_i^{\alpha_i}.$$

(ii) Si on a encore

$$a = v \prod_{i \in I} p_i^{\beta_i},$$

où les $\beta_i \geq 0$ sont nuls sauf pour un nombre fini de i et $v \in A^\times$, alors $u = v$ et $\alpha_i = \beta_i$ pour tout i.

1.3.11 Définition. On dit que a admet une *(unique) factorisation* en éléments irréductibles. Un anneau intègre A qui satisfait les conclusions du théorème est appélé *anneau factoriel.*

1.3.12 Lemme. *Soient A un anneau principal et $I_1 \subset I_2 \subset \ldots$ une suite croissante des idéaux dans A. Alors la suite des I_k est* stationnaire*, c'èst-à-dire il existe $n \in \mathbb{N}$ tel que $I_k = I_n$ pour tout $k \geq n$.*

Démonstration. Posons $I = \bigcup_{k\geq 1} I_k$. Alors, I est un idéal. En fait, il est clair que $0 \in I$. Si $a, b \in I$ alors il existe k tel que $a, b \in I_k$ et donc $a - b \in I_k \subset I$, donc I est bien un sous-groupe de A. De plus, si $a \in I$ et $x \in A$, alors il existe k tel que $a \in I_k$ et donc $xa \in I_k \subset I$ parce que I_k est un idéal.
Comme A est principal il existe $c \in A$ tel que $I = (c)$. Il existe n tel que $c \in I_n$ donc, pour $k \geq n$, la suite d'inclusions

$$I = (c) \subset I_n \subset I_k \subset I$$

montre que $I_k = I_n$ si $k \geq n$. □

1.3.13 Lemme. *Soient A un anneau et $a, b \in A$.*

(i) Si $c \in A$ tel que $(a, c) = A$ et $c|ab$, alors $c|b$ (lemme de Gauss).

(ii) Soient A principal et $p \in A$ un élément irréductible. Alors $p|ab$ implique que $p|a$ ou $p|b$ (lemme d'Euclide).

Démonstration. Dans 1.3.13(i), l'hypothèse que $(a, c) = A$ implique qu'il existe $u, v \in A$ tels que $ua + vc = 1$. En multipliant par b on en déduit que c divise $uab + vbc = b$ donc si $c|ab$ alors $c|b$.
Pour le lemme d'Euclide notons que l'idéal (p) est premier d'après la proposition 1.3.6. Si $p|ab$ alors $ab \in (p)$ donc $a \in (p)$ ou $b \in (p)$ par définition d'un idéal premier et on conclut que $p|a$ ou $p|b$. □

Démonstration du Théorème 1.3.10. Pour prouver la première affirmation supposons qu'il existe $a_1 \in A$ qui ne possède pas de factorisation. Alors a_1 n'est ni une unité ni un élément irréductible donc il existe a_2 et b_2 tels que $a_1 = a_2 b_2$ et que ni a_2 ni b_2 n'est une unité. Si a_2 et b_2 admettent chacun une factorisation alors a_1 aussi admet une factorisation. Quitte à échanger a_2 et b_2 on peut donc supposer que a_2 n'admet pas de factorisation. On a $(a_1) \subset (a_2)$ et d'après le lemme 1.3.3 cette inclusion est stricte. En itérant l'argument avec on trouve une suite strictement croissante des idéaux

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$$

dans A. C'est une contradiction avec le lemme 1.3.12 donc il n'existe pas d'élément a_1 sans factorisation.
Pour la deuxième affirmation on considère une relation

$$a = u\prod_{i\in I} p_i^{\alpha_i} = v\prod_{i\in I} p_i^{\beta_i} \qquad (*)$$

avec $u, v \in A^\times$ et $(\alpha_i) \neq (\beta_i)$ et où $M = \max\left(\sum_i \alpha_i, \sum_i \beta_i\right)$ minimal parmi toutes les relations de ce type. On a alors $M \geq 1$ et on peut alors supposer que $\sum_i \alpha_i \geq 1$. Il existe j tel que $\alpha_j > 0$ donc p_j divise a. Comme p_j ne divise pas p_i si $i \neq j$, le lemme d'Euclide 1.3.13(ii) implique que $\beta_j > 0$. Comme A est intègre on peut simplifier l'identité $(*)$ à gauche et à droite par un facteur p_j et on obtient une relation du même type avec $\max(\sum_i \alpha_i, \sum_i \beta_i) = M-1$, contredisant la minimalité de M. □

1.3.14 Définition. Soient A un anneau intègre et $a, b \in A$ non nuls.
- On dit que $d \in A$ est un *diviseur commun* de a et b si d divise a et b.
- On dit que d est un *plus grand diviseur commun* de a et b, et on note $d = \text{pgcd}(a, b)$ si d est un diviseur commun de a et b et si tout diviseur commun de a et b divise d.
- On dit que a et b sont *premiers entre eux* si 1 est un pgcd de a et b.

1.3.15 Remarques. (i) Dans un anneau intègre quelconque, deux éléments non nuls a et b n'ont pas forcément un pgcd.

(ii) Si d est un pgcd de a et b et $u \in A^\times$ alors ud est aussi un pgcd de a et b. Réciproquement, si d, d' sont des pgcd de a et b alors d' divise d parce que d est un pgcd et d' est un diviseur commun et de même d divise d'. Le lemme 1.3.3 implique alors qu'il existe $u \in A^\times$ tel que $d' = ud$. Le pgcd, s'il existe, est donc déterminé à la multiplication avec une unité près.

(iii) De manière analogue, on définit les notions de *multiple commun* et de *plus petit multiple commun* (ppcm) de deux éléments non nuls $a, b \in A$.

1.3.16 Proposition. *Soient A un anneau intègre et $a, b, d \in A$ avec $a, b \neq 0$ tels que $(a, b) = (d)$. Alors d est un* pgcd *de a et b.*

Démonstration. Le fait que $a, b \in (d)$ implique que d est un diviseur commun de a et b. Si d' est un diviseur commun de a et b alors $a, b \in (d')$ donc $(d) = (a, b) \subset (d')$ d'où enfin $d'|d$. □

1.3.17 Corollaire (Bézout)**.** *Soit A un anneau principal et soient a, b deux éléments non-nuls de A. Alors a et b ont un* pgcd*. Si d est un* pgcd *de a et b alors $(a, b) = (d)$ et il existe $x, y \in A$ tels que $d = ax + by$.*

Démonstration. L'idéal (a, b) est principal donc il existe $d \in A$ avec $(a, b) = (d)$. La proposition 1.3.16 implique que d est un pgcd. Si d' est un pgcd de a et b alors il existe une unité u tel que $d' = ud$ donc

$$(d') = (d) = (a, b) = \{ax + by \mid x, y \in A\},$$

d'où la dernière affirmation. □

1.3.18 Corollaire. *Si A et $a, b \in A$ sont comme dans le corollaire précédent alors les conditions suivantes sont équivalentes.*

- *a et b sont premiers entre eux.*
- *$(a, b) = A$.*
- *Il existe $x, y \in A$ avec $ax + by = 1$.*

Démonstration. On a déjà montré que le première condition implique la deuxième et la deuxième condition implique clairement la troisième. Supposons qu'il existe $x, y \in A$ avec $ax + by = 1$, alors si $d = \text{pgcd}(a, b)$ on a $d|1$ donc $d \in A^\times$ et 1 est donc un pgcd de a et b. □

1.3.19 Corollaire (Lemme de Gauss)**.** *Soient A un anneau principal et $a, b, c \in A$ non nuls. Si a et c sont premiers entre eux et $c|ab$ alors $c|b$.*

Démonstration. Compte tenu du corollaire précédent c'est une reformulation du lemme de Gauss 1.3.13(i). □

1.3.20 Remarques.

(i) En pratique il peut être très difficile à décider si un anneau donné est principal ou non. Par exemple il existe des entiers $d > 0$ pour lesquels il n'est pas connu si $\mathbb{Z}[\sqrt{d}]$ est principal ou non.

(ii) Si A est principal il est en généreal difficile de trouver un générateur d'un idéal donné. En particulier, il peut être difficile de trouver $\text{pgcd}(a, b)$ pour $a, b \in A$.

1.4 Anneaux euclidiens

1.4.1 Définition. Un anneau commutatif unitaire et intègre est appélé *anneau euclidien* s'il est muni d'une application, appelé *stathme* ou parfois *fonction euclidienne* $s \colon A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a, b \in A$ avec $b \neq 0$ il existe q et $r \in A$ tel que

$$a = bq + r \quad \text{et soit } r = 0, \text{ soit } s(r) < s(b).$$

On appelle r le *reste* de la division euclidienne de a par b.

1.4.2 Exemples.

(i) L'anneau $\mathbb{Z}$ est un anneau euclidien avec stathme donné par $s(x) = |x|$.

(ii) L'anneau $\mathbb{Z}[i]$ est un anneau euclidien avec stathme $s(z) = z\bar{z} = |z|^2$.

1.4.3 Proposition. *Soit A un annneau euclidien. Alors A est principal.*

Démonstration. Soit I un idéal de A. Si $I = \{0\}$ alors $I = (0)$ donc I est principal. Sinon l'ensemble $\{s(x) \mid x \in I \setminus \{0\}\}$ est un sous-ensemble non vide de $\mathbb{N}$ donc il admet un minimum. Soit $b \in I$ non nul tel que $s(b)$ est minimal. On va montrer que $I = (b)$. Supposons pour cela que $a \in I$. La division euclidienne de a par b donne $q, r \in A$ avec $a = bq + r$ et soit $r = 0$, soit $s(r) < s(b)$. Comme $r = a - bq \in I$, le cas $r \neq 0$ est exclu par la minimalité de $s(b)$. On a donc $r = 0$, d'où $a \in (b)$ et il s'ensuit que $I = (b)$. □

1.4.4 Remarque. Il existe des anneaux principaux qui ne sont pas euclidiens. On verra un tel exemple dans une des feuilles d'exercices. En fait, l'exemple « classique » est donné par le plus petit sous-anneau de $\mathbb{C}$ qui contient $\frac{1+i\sqrt{19}}{2}$.

1.4.5 Définition. Soient A un anneau commutatif unitaire et $P = \lambda_0 + \lambda_1 X + \ldots$ un polynôme non-nul à coefficients dans A. Le *degré* de P est le plus grand entier d tel que $\lambda_d \neq 0$, il est noté $\deg(P)$. Le degré de polynôme 0 est par convention $-\infty$.
Si P est un polynôme non-nul de degré d, alors l'élément λ_d est appelé le *coefficient dominant*. On dit qu'un polynôme P de degré d est *unitaire* si $\lambda_d = 1$.

1.4.6 Lemme. *Soient A un anneau commutatif unitaire et $P, Q \in A[X]$. Alors*

(i) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$,

(ii) $\deg(PQ) \leq \deg(P) + \deg(Q)$ *et*

(iii) si A est intègre alors $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. L'affirmation 1.4.6(i) et évidente. Si $P = 0$ ou $Q = 0$ les 1.4.6(ii) et 1.4.6(iii) sont faciles compte tenu de la convention que $-\infty + n = -\infty$ pour $n \in \mathbb{N} \cup \{-\infty\}$. Si $P = \sum_{i \geq 0} \lambda_i X^i$ et $Q = \sum_{i \geq 0} \mu_j X^j$ sont non-nuls, de degrés n et m, alors pour $i > n + m$ le coefficient ν_i du polynôme PQ est nul et, si A est intègre, $\nu_{n+m} = \lambda_n \mu_m \neq 0$. □

1.4.7 Théorème. *Soit A un anneau intègre et soient $P_1, P_2 \in A[X]$ où P_2 est un polynôme dont le coefficient dominant est inversible. Alors il existe des polynômes $Q, R \in A[X]$ tels que*

— $P_1 = QP_2 + R$ *et*

— $\deg(R) < \deg(P_2)$.

Les polynômes Q et R sont uniquement déterminés par P_1 et P_2.

Démonstration. Montrons d'abord l'unicité de Q et R. Supposons donc que

$$P_1 = QP_2 + R = Q'P_2 + R'$$

avec $\deg(R)$ et $\deg(R') < \deg(P_2)$. Alors $R - R' = (Q' - Q)P_2$. Si $Q \neq Q'$ alors le lemme 1.4.6 donne la contradiction

$$\deg(P_2) > \deg(R - R') = \deg(Q' - Q) + \deg(P_2) \geq \deg(P_2).$$

On a donc $Q = Q'$ et alors également $R = R'$.
L'existence est démontré par récurrence sur la différence $\deg(P_1) - \deg(P_2)$. Si $\deg(P_1) < \deg(P_2)$ on peut prendre $Q = 0$ et $R = P_1$. Supposons donc que $k = \deg(P_1) - \deg(P_2) \geq 0$ et que l'existence de Q et R est prouvé dans le cas où $\deg(P_1) - \deg(P_2) < k$. Soit $d = \deg(P_2)$, alors $\deg(P_1) = d + k$ et on peut écrire $P_1 = \lambda_{d+k}X^{d+k} + \cdots + \lambda_0$. Le polynôme P_2 est de la forme $P_2 = \mu_d X^d + \ldots \mu_0$ où $\mu_d \in A^\times$. On considère alors le polynôme $\widetilde{P_1} = P_1 - \lambda_{d+k}\mu_d^{-1}X^k P_2$. On a $\deg(\widetilde{P_1}) < d + k$ donc l'hypothèse de récurrence implique qu'il existe Q' et R tels que $\widetilde{P_1} = Q'P_2 + R$ et $\deg(R) < \deg(P_2)$. En posant $Q = Q' + \lambda_{d+k}\mu_k^{-1}X^k$ on obtient $P_1 = QP_2 + R$. □

1.4.8 Corollaire. *Soit K un corps. Alors l'anneau des polynômes $K[X]$ est euclidien avec stathme* $\deg\colon K[X] \setminus \{0\} \to \mathbb{N}$ *donc principal.*

1.4.9 Définition. Soient A un anneau commutatif unitaire et $P \in A[X]$. On dit qu'un élément $a \in A$ est une *racine* de P si $\mathrm{ev}_a(P) = P(a) = 0$.

1.4.10 Proposition. *Soient A un anneau intègre et $P \in A[X]$. Alors $a \in A$ est une racine de P si et seulement si $X - a$ divise P.*

Démonstration. Soit $P \in A[X]$ quelconque. Comme $X - a$ est un polynôme unitaire, le lemme 1.4.7 implique qu'il existe $Q, R \in A[X]$ tels que $P = (X - a)Q + R$ et R est un polynôme de degré < 1. On a donc $R \in A$. L'évaluation en a donne $P(a) = ev_a((X - a)Q + R) = R$, donc a est une racine de P si et seulement si $R = 0$ si et seulement si P est divisible par $X - a$. □

1.4.11 Théorème (Algorithme d'Euclide)**.** *Soient A un anneau euclidien avec stathme s et $a, b \in A$ non nuls. On définit, par récurrence, une suite $(r_n)_{n\geq -1}$ dans A par*

- *$r_{-1} = a$ et $r_0 = b$ et*
- *si, pour $n \geq 0$, les éléments $r_{-1}, \ldots, r_n \in A$ sont définis alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n si ce reste est non nul, la suite s'arrête au rang n sinon.*

Cette suite se termine à un rang fini N et $r_N = \mathrm{pgcd}(a, b)$.

Démonstration. La suite des $s(r_n)$, pour $n \geq 0$, est une suite strictement décroissante d'entiers positifs donc elle est finie. Soit r_N le dernier terme de la suite (r_n). Pour $0 \leq n < N$, soit q_n le quotient de la division euclidienne de r_{n-1} par r_n, de sorte que $r_{n+1} = r_{n-1} - q_n r_n$. Cette expression montre que l'ensemble des diviseurs communs de r_{n-1} et r_n coïncide avec l'ensemble des diviseurs communs de r_n et r_{n+1}. On a donc $\mathrm{pgcd}(r_{n-1}, r_n) = \mathrm{pgcd}(r_n, r_{n+1})$, d'où par récurrence $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_{N-1}, r_N)$. Comme la suite des r_n se termine au rang N, le terme r_N divise r_{N-1} donc le dernier pgcd vaut r_N. □

1.4.12 Remarque. D'après le corollaire 1.3.17, il existe $u, v \in A$ tels qu'on a $\mathrm{pgcd}(a, b) = ua + vb$. Il est laissé comme exercice de voir comment l'algorithme d'Euclide permet de déterminer de tels u, v.

1.5 Corps des fractions d'un anneau intègre

1.5.1 Théorème. *Soit A un anneau commutatif unitaire intègre.*

(i) Il existe un corps F_A et un morphisme d'anneaux injectif $\iota\colon A \to F_A$ avec la propriété universelle *suivante. Pour tout anneau commutatif unitaire B et tout morphisme d'anneaux $\varphi\colon A \to B$ tel que $\varphi(a) \in B^\times$ pour tout $a \in A$ avec $a \neq 0$, il existe un unique morphisme d'anneaux $\widetilde{\varphi}\colon F_A \to B$ tel que $\varphi = \widetilde{\varphi} \circ \iota$.*

Le corps F_A est appelé le corps des fractions de A.

(ii) Si F' est un corps et $\iota'\colon A \to F'$ un morphisme d'anneaux qui possède la propriéte universelle ci-dessus alors il existe un unique isomorphisme d'anneaux $\widetilde{\iota'}\colon F_A \to F'$ tel que $\iota' = \widetilde{\iota'} \circ \iota$. En particulier, ι' est injectif.

Démonstration. Montrons d'abord 1.5.1(i). On note $A^* = A \setminus \{0\}$ et on considère l'ensemble $A \times A^*$ qu'on munit d'une relation binaire en posant $(a_1, b_1) \sim (a_2, b_2)$ si et seulement si $a_1 b_2 - a_2 b_1 = 0$. Cette relation est une rélation d'équivalence : elle est clairement symétrique et réflexive. Supposons que $(a_1, b_1) \sim (a_2, b_2) \sim (a_3, b_3)$. Alors $a_1 b_2 - a_2 b_1 = 0 = a_2 b_3 - a_3 b_2$. On a

$$a_1 b_2 b_3 - a_2 b_1 b_3 = b_3(a_1 b_2 - a_2 b_1) = 0$$
$$a_2 b_1 b_3 - a_3 b_1 b_2 = b_1(a_2 b_3 - a_3 b_2) = 0$$

et en prenant la somme de ces deux équations on obtient $b_2(a_1 b_3 - a_3 b_1) = 0$, d'où $a_1 b_3 - a_3 b_1$ car A est intègre et $b_2 \in A^*$. Cela montre que $(a_1, b_1) \sim (a_3, b_3)$ donc la transitivité de $\sim$.
En tant que ensemble on définit F_A comme l'ensemble de classes d'équivalence. La classe d'équivalence de (a, b) sera noté $\frac{a}{b}$ ou ab^{-1} On définit sur $A \times A^*$ deux lois

internes + et · dont les définitions sont motivées par par les formules usuelles pour l'addition et la multiplication dans $\mathbb{Q}$:

$$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + a_2b_1, b_1b_2) \quad \text{et}$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2).$$

On laisse comme exercice la vérification que ces deux lois sont compatibles avec la relation d'équivalence, donc elles induisent une addition et une multiplication sur F_A, données par

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + b_2a_1}{b_1b_2} \quad \text{et}$$
$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}.$$

Il est élémentaire de vérifier que F_A avec ces deux lois est un anneau commutatif unitaire. L'élément neutre pour l'adddition est $\frac{0}{1}$ et l'unité pour la multiplication est $\frac{1}{1}$. Il est encore clair que l'application $\iota\colon A \to F_A$, $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux. Il est injectif car $\frac{a}{1} = \frac{0}{1}$ si et seulement si $a = a \cdot 1 - 0 \cdot 1 = 0$. De plus, pour $a, b \neq 0$ on a $\frac{0}{1} \neq \frac{a}{b} \in F_A$ et $\frac{b}{a}\frac{a}{b} = \frac{ba}{ab} = \frac{1}{1}$, donc F_A est un corps.
Finalement, si $\varphi\colon A \to B$ est un morphisme d'anneaux et si $\varphi(b) \in B^\times$ pour tout $b \in A^*$, alors on vérifie que l'application $\widetilde{\varphi}\colon F_A \to B$, $\frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$ est bien définie et que c'est un morphisme d'anneaux qui satisfait $\varphi = \widetilde{\varphi} \circ \iota$. L'unicité de $\widetilde{\varphi}$ résulte de ce que pour tous $a \in A$ et $b \in A^*$ on doit avoir

$$\varphi(b)\widetilde{\varphi}\left(\frac{a}{b}\right) = \widetilde{\varphi}(\iota(b))\widetilde{\varphi}\left(\frac{a}{b}\right) = \widetilde{\varphi}\left(\frac{b}{1} \cdot \frac{a}{b}\right) = \widetilde{\varphi}\left(\frac{ab}{b}\right) = \widetilde{\varphi}\left(\frac{a}{1}\right) = \widetilde{\varphi}(\iota(a)) = \varphi(a)$$

d'où $\widetilde{\varphi}(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$ parce que $\varphi(b) \in B^\times$.
Montrons 1.5.1(ii). Les propriétés universelles de ι et ι' donnent des morphismes d'anneaux $\widetilde{\iota'}\colon F_A \to F'$ et $\widetilde{\iota}\colon F' \to F_A$ tels que $\iota' = \widetilde{\iota'} \circ \iota$ et $\iota = \widetilde{\iota} \circ \iota'$. On a donc

$$\iota' = \widetilde{\iota'} \circ \iota = \widetilde{\iota'} \circ \widetilde{\iota} \circ \iota'$$

et en appliquant la propriété universelle de ι' avec ι' dans le rôle de $\varphi\colon A \to B$, l'unicité du morphisme $F' \to F'$ implique que $\widetilde{\iota'} \circ \widetilde{\iota} = \mathrm{id}_{F'}$. On voit de même façon que $\widetilde{\iota} \circ \widetilde{\iota'} = \mathrm{id}_{F_A}$. □

1.5.2 Remarques. (i) On utilise ι pour identifier A avec $\iota(A) \subset F_A$.

(ii) Si $u \in A^\times$ alors pour tout $a \in A$ on a $\frac{a}{u} = \frac{au^{-1}}{1} = au^{-1}$ où $u^{-1} \in A$ est l'inverse de A. Pour $a \in A$ non nul, $\frac{1}{a}$ est l'inverse de a dans K et on écrira souvent a^{-1} pour cet élément.

1.5.3 Exemples. (i) Pour $A = \mathbb{Z}$ on obtient $F_A = \mathbb{Q}$, le corps des nombres rationnels.

(ii) Si K est un corps et $A = K[X]$ l'anneau des polynômes à coefficients dans K alors $F_A = K(X)$, le corps des fractions rationnelles à coefficients dans K.

(iii) Si A est un corps, alors $\iota\colon A \to F_A$ est un isomorphisme.

1.5.4 Remarque. Soit A un anneau commutatif et unitaire. Un sous-ensemble $S \subset A$ est une *partie multiplicative* de A si

— $1 \in S$ et

— S est stable par multiplication, c.-à.-d. si $s_1, s_2 \in S$ alors $s_1 s_2 \in S$.

Étant donné une partie multiplicative $S \subset A$ on peut construire un anneau $S^{-1}A$ et un morphisme d'anneaux $\iota_S\colon A \to S^{-1}A$ tel que $\iota_S(s) \in (S^{-1}A)^\times$ pour tout $s \in S$ et qui possèdent une propriété universelle similaire à celle de l'inclusion d'un anneau intègre dans son corps de fractions.
Cette construction s'applique notamment si $A = A \setminus P$ où $P \subset A$ est un idéal premier. Dans ce cas, l'anneau $S^{-1}A$ est noté A_P et appelé la *localisé de A en P*.

1.5.5 Définition. Soit P un polynôme à coefficients dans un anneau commutatif unitaire A et soit $l > 0$ un entier. On dit que $a \in A$ est une *racine de P de multiplicité l* s'il existe un polynôme Q tel que $P = (X - a)^l Q$ et $Q(a) \neq 0$.

1.5.6 Corollaire. *Soit A un anneau intègre et soit P un polynôme à coefficients dans A de degré $n > 0$. Alors P a au plus n racines dans A, en tenant compte de leur multiplicités.*

Démonstration. Si A est intègre alors A se plonge dans son corps des fractions donc il suffit à établir le corollaire dans le cas d'un corps. Si A est un corps, alors $A[X]$ est principal d'après le corollaire 1.4.8. Soient $a_1, \dots a_r$ les racines distinctes de P, avec multiplicités m_i, alors P est divisible par $(X - a_i)^{l_i}$ pour $i = 1, \dots, r$. Il est clair que dans le cas d'un corps les polynômes de degré 1 sont irréductibles et des polynômes disctints et unitaire de degré 1 ne sont pas associés. Le lemme de Gauss implique que P est divisible par le produit $\prod_{i=1}^r (X - a_i)^{l_i}$ et par le lemme 1.4.6 on a $\sum_{i=1}^r l_i \leq \deg(P)$. □

1.5.7 Exemple. Dans le corollaire, il est essentiel de supposer que l'anneau A est intègre. En effet, soit $A = \mathbb{Z}/6\mathbb{Z}[X]$ et $P \in A[X]$ le polynôme $X^3 - X$. Alors tous les 6 éléments de A sont de racines de P.

1.6 Anneaux factoriels.

On rappelle la définition 1.3.11 d'anneau factoriel. Dans toute la section 1.6, A désigne un anneau factoriel. Comme dans la définition 1.3.9, on note I l'ensemble

des classes d'équivalence des éléments irréductibles pour la relation d'être associés et on fixe, pour tout $i \in I$, un représentant p_i de la classe i. L'anneau factoriel A est intègre par hypothèse et on note $K = F_A$ son corps des fractions.

1.6.1 Proposition. *Soient $a, b \in A$ non nuls avec factorisations*

$$a = u \prod_{i \in I} p_i^{\alpha_i} \quad et \quad b = v \prod_{i \in I} p_i^{\beta_i}. \tag{\dagger}$$

(i) L'élément b divise a si et seulement si $\beta_i \leq \alpha_i$ pour tout $i \in I$.

(ii) Si pour tout $i \in I$ on pose $\delta_i = \min(\alpha_i, \beta_i)$ alors $d = \prod_{i \in I} p_i^{\delta_i}$ est un pgcd *de a et b. En particulier deux éléments non nuls de A admettent un* pgcd*.*

(iii) Si $x \in K$ avec $x \neq 0$ alors il existe des $\xi_i \in \mathbb{Z}$ (pour $i \in I$), tous nuls sauf un nombre fini, et un élément $w \in A^\times$ tels que

$$x = w \prod_{i \in I} p_i^{\xi_i}.$$

Ici on convient que si $\xi_i < 0$ alors $p_i^{\xi_i} = \frac{1}{p_i^{-\xi_i}}$. Étant donné x, l'élément w et les ξ_i sont uniques.

Démonstration. Pour l'affirmation 1.6.1(i), notons que si $\beta_i \leq \alpha_i$ pour tout i alors on a $\gamma_i = \alpha_i - \beta_i \geq 0$ pour tout $i \in I$ et $\gamma_i = 0$ pour tous sauf un nombre fini de i. L'élément $c = uv^{-1} \prod p_i^{\gamma_i} \in A$ vérifie alors $a = bc$ donc b divise a. Réciproquement, si b divise a alors il existe $c \in A$ tel que $a = bc$ et en écrivant $c = w \prod p_i^{\gamma_i}$ et en utilisant l'unicité des factorisations on voit que $\alpha_i = \beta_i + \gamma_i \geq \beta_i$ pour tout $i \in I$. La première affirmation implique que l'élément d défini dans 1.6.1(ii) est un diviseur commun de a et b. Si $d' = w \prod_{i \in I} p_i^{\delta'_i}$ est un diviseur commun de a et b alors la 1.6.1(i) implique que $\delta'_i \leq \alpha_i$ et $\delta'_i \leq \beta_i$ pour tout $i \in I$, d'où le fait que d' divise d qui est donc bien un pgcd de a et b.
Pour la dernière affirmation, si $x \in K$ avec $x \neq 0$ alors il existe $a, b \in A$, différents de 0 tels que $x = ab^{-1}$. En factorisant a et b comme dans (†), on voit que $x = w \prod_{i \in I} p_i^{\xi_i}$ avec $w = uv^{-1}$ et $\xi_i = \alpha_i - \beta_i$ qui sont tous nuls sauf un nombre fini. Cela démontre l'existence de la factorisation. Supposons enfin que

$$w \prod_{i \in I} p_i^{\xi_i} = w' \prod_{i \in I} p_i^{\xi'_i}$$

alors on définit les ensembles finis

$$I_1 = \{i \in I \mid \xi_i > 0\}, \quad I_2 = \{i \in I \mid \xi_i < 0\},$$

$$I_3 = \{i \in I \mid \xi_i > 0\} \quad \text{et} \quad I_4 = \{i \in I \mid \xi_i < 0\}$$

et on multiplie l'égalité ci-dessus par $\prod_{i\in I_2} p_i^{-\xi_i} \prod_{i\in I_4} p_i^{-\xi'_i}$ pour obtenir

$$w \prod_{i\in I_1} p_i^{\xi_i} \prod_{i\in I_4} p_i^{-\xi'_i} = w' \prod_{i\in I_2} p_i^{-\xi_i} \prod_{i\in I_3} p_i^{\xi'_i}.$$

En utilisant l'unicité de la factorisation dans A et le fait que I_1 et I_2 ainsi que I_3 et I_4 sont disjoints on conclut que $\xi_i = \xi'_i$ pour tout $i \in I_1 \cup I_2 = I_3 \cup I_4$. Comme les ξ_i et les ξ'_i sont nuls pour i en dehors de cet ensemble, cela établit l'unicité de la factorisation. □

1.6.2 Définition. (i) Pour $x \in K$ non-nul et $i \in I$ on note $\mathrm{ord}_i(x) = \mathrm{ord}_{p_i}(x)$ l'exposant ξ_i de la factorisation de x comme dans la proposition 1.6.1(iii).

(ii) Si $P = \sum_{j=0}^{d} \lambda_j X^j \in K[X]$ avec $P \neq 0$ on pose, pour $i \in I$,

$$\mathrm{ord}_i(P) = \mathrm{ord}_{p_i}(P) = \min\{\mathrm{ord}_p(\lambda_j) \mid j = 0, \ldots, d \text{ tel que } \lambda_j \neq 0\}.$$

1.6.3 Lemme. *(i) Si $x, y \in K$ alors on a $\mathrm{ord}_i(xy) = \mathrm{ord}_i(x) + \mathrm{ord}_i(y)$ pour tout $i \in I$.*

(ii) Si $x \in K$ (resp. $P \in K[X]$) alors $\mathrm{ord}_i(x) = 0$ (resp. $\mathrm{ord}_i(P) = 0$) pour tous sauf un nombre fini de i.

(iii) On a $x \in A$ si et seulement si $\mathrm{ord}_i(x) \geq 0$ pour tout $i \in I$ et que $x \in A^\times$ si et seulement si $\mathrm{ord}_i(x) = 0$ pour tout $i \in I$.

Démonstration. La première affirmation résulte du fait que pour $x = u \prod p_i^{\xi_i}$ et $y = v \prod p_i^{\upsilon_i}$ avec $u, v \in A^\times$ on a

$$xy = uv \prod p_i^{\xi_i + \upsilon_i}.$$

La deuxième affirmation est évidente pour $x \in K$. Pour les polynômes elle résulte du fait que pour chaque j tel que $\lambda_j \neq 0$, il existe un ensemble fini $I_j \subset I$ tel que $\mathrm{ord}_i(\lambda_j) = 0$ pour $i \notin I_j$. Par conséquent, $\mathrm{ord}_i(P) = 0$ pour tout i en dehors de l'ensemble fini $\cup_j I_j$.
Pour la dernière affirmation, il est clair que $x \in A$ si $\mathrm{ord}_i(x) \geq 0$ pour tout i. Réciproquement, si $x \in A$ alors $x = w \prod_{i\in I} p_i^{\xi_i}$ avec $w \in A^\times$ et $\xi_i = \mathrm{ord}_i(x) \geq 0$ pour tout i. Comme $x \in A^\times$ si et seulement si $x \in A$ et $\frac{1}{x} \in A$, la dernière partie de l'affirmation en résulte. □

1.6.4 Définition. Soit A un anneau factoriel et soit $P \in K[X]$ un polynôme non-nul. Alors le *contenu* de P, noté $\mathrm{cont}(P)$ est

$$\mathrm{cont}(P) = \prod_{i\in I} p_i^{\mathrm{ord}_i(P)}.$$

1.6.5 Lemme. *Soit $P \in K[X]$ non nul.*
— *On a* $\mathrm{cont}(P) \in A$ *si et seulement si* $P \in A[X]$.
— *Il existe* $P_1 \in A[X]$ *avec* $\mathrm{cont}(P_1) = 1$ *tel que* $P = \mathrm{cont}(P)P_1$.

Démonstration. Soit $P = \sum_{j=0}^{d} \lambda_j X^j$. On a $\mathrm{cont}(P) \in A$ si et seulement si $\mathrm{ord}_i(P) = \mathrm{ord}_i(\mathrm{cont}(P)) \geq 0$ pour tout $i \in I$ si et seulement si $\mathrm{ord}_i(\lambda_j) \geq 0$ pour tout j et tout i si et seulement si $\lambda_j \in A$ pour tout j.
Pour $j = 0, \ldots, d$, posons $\mu_j = \mathrm{cont}(P)^{-1}\lambda_j$ et $P_1 = \sum_{j=0}^{d} \mu_j X^j \in K[X]$. On a alors $P = \mathrm{cont}(P)P_1$. En plus $\mathrm{ord}_i(\mu_j) = \mathrm{ord}_i(\lambda_j) - \mathrm{ord}_i(P) \geq 0$ pour tout $i \in I$ et tout $j = 0, \ldots, d$ et pour tout i il existe j tel que

$$\mathrm{ord}_i(\mu_j) = \mathrm{ord}_i(\lambda_j) - \mathrm{ord}_i(P) = 0.$$

Il s'ensuit que $\mathrm{cont}(P_1) = 1$ et la première partie du lemme implique alors que $P_1 \in A[X]$. □

1.6.6 Lemme (Gauss)**.** *Soient $P, Q \in K[X]$ non-nuls. Alors*

$$\mathrm{cont}(PQ) = \mathrm{cont}(P)\mathrm{cont}(Q).$$

Démonstration. On traite d'abord le cas où $\mathrm{cont}(P) = \mathrm{cont}(Q) = 1$, ce qui implique que $P, Q \in A[X]$. On peut écrire $P = \sum_{j=0}^{d} \lambda_j X^j$ et $Q = \sum_{j=0}^{d} \mu_j X^j$ avec les λ_j et les μ_j dans A. Il suffit de montrer que pour tous $i \in I$ il existe un coefficient de PQ qui n'est pas divisible par p_i. Fixons donc $i \in I$. Comme $\mathrm{cont}(P) = \mathrm{cont}(Q) = 1$, il existe $k, \ell \geq 0$ tels que $\lambda_k \neq 0 \neq \mu_\ell$ et $\mathrm{ord}_i(\lambda_k)$ et $\mathrm{ord}_i(\mu_\ell) = 0$. Choisissons k et ℓ minimaux avec ces propriétés. Si $PQ = \sum_{j=0}^{2d} \nu_j X^j$ alors le coefficient $\nu_{k+\ell}$ est donné par

$$\nu_{k+\ell} = \lambda_k\mu_\ell + \sum_{j=0}^{k-1} \lambda_j\mu_{k+\ell-j} + \sum_{j=k+1}^{k+\ell} \lambda_j\mu_{k+\ell-j}.$$

Le premier terme n'est pas divisible par p_i mais pour tout $j \neq k$ avec $0 \leq j \leq k+\ell$ au moins un de λ_j et $\mu_{k+\ell-j}$ est divisible par p_i. Cela implique que les deux sommes ci-dessus sont divisibles par p_i et on obtient $p_i \nmid \nu_{k+\ell}$.
Si $\mathrm{cont}(P)$ et $\mathrm{cont}(Q)$ sont quelconques alors le lemme précédent fournit P_1, Q_1 avec $P = \mathrm{cont}(P)P_1$ et $Q = \mathrm{cont}(Q)Q_1$ et $\mathrm{cont}(P_1) = \mathrm{cont}(Q_1) = 1$ et on a

$$\mathrm{cont}(PQ) = \mathrm{cont}(\mathrm{cont}(P)\mathrm{cont}(Q)P_1Q_1) = \mathrm{cont}(P)\mathrm{cont}(Q)\mathrm{cont}(P_1Q_1).$$

Comme $\mathrm{cont}(P_1Q_1) = 1$ d'après le cas particulier qu'on vient de traiter, l'affirmation générale en résulte. □

1.6.7 Proposition. *Les éléments irréductibles de $A[X]$ sont*

— *les élements irréductibles de A et*
— *les polynômes non constants $P \in A[X]$ tels que* $\mathrm{cont}(P) = 1$ *et P est irréductible dans $K[X]$.*

Démonstration. Si $a \in A$ est irréductible et $a = PQ$ avec $P, Q \in A[X]$ alors $\deg(P) = \deg(Q) = 0$ d'après le lemme 1.4.6(iii). Cela implique que $P, Q \in A$ et comme a est irréductible, un des deux est une unité dans A donc aussi dans $A[X]$. Cela implique que a est irréductible dans $A[X]$. Considérons ensuite un polynôme non constant $P \in A[X]$ avec $\mathrm{cont}(P) = 1$ et qui est irréductible dans $K[X]$. Si $P = QR$ dans $A[X] \subset K[X]$ alors un des facteurs, disons Q, est dans $K[X]^\times$, c'est donc une constante, appartenant à A car $Q \in A[X]$. D'après le lemme de Gauss on a alors $1 = \mathrm{cont}(P) = \mathrm{cont}(Q)\mathrm{cont}(R)$ et cela implique que $\mathrm{cont}(Q) = \mathrm{cont}(R) = 1$ donc $Q \in A^\times$. On a prouvé que P est irréductible dans $A[X]$.
Réciproquement, supposons que P est irréductible dans $A[X]$. Si $P \in A$ et si on a $P = ab$ avec $a, b \in A$ alors l'irréductibilité de P dans $A[X]$ implique que a ou b est une unité dans $A[X]$ donc une unité dans A et on conclut que P est irréductible dans A. Si P n'est pas constant alors le lemme 1.6.5 affirme que $P = \mathrm{cont}(P)P_1$ pour un polynôme $P_1 \in A[X]$. Comme P est irréductible et P_1 non-constant cela implique que $\mathrm{cont}(P) \in A^\times$ d'où $\mathrm{cont}(P) = 1$. Supposons que $P = QR$ avec $Q, R \in K[X]$. En appliquant à nouveau le lemme 1.6.5, on trouve $Q_1, R_1 \in A[X]$ de contenu 1 tels que $Q = \mathrm{cont}(Q)Q_1$ et $R = \mathrm{cont}(R)R_1$. On a $P = \mathrm{cont}(Q)\mathrm{cont}(R)Q_1R_1$ et comme $\mathrm{cont}(P) \in A$ et $\mathrm{cont}(Q_1R_1) = 1$ on a $\mathrm{cont}(Q)\mathrm{cont}(R) \in A$. Cela donne une factorisation dans $A[X]$, à savoir $P = (\mathrm{cont}(Q)\mathrm{cont}(R)Q_1)R_1$ et comme P est irréductible, soit $\mathrm{cont}(Q)\mathrm{cont}(R)Q_1$ soit R_1 est constant. Il en est de même pour Q ou R et on conclut que P est irréductible dans $K[X]$. □

1.6.8 Représentants des éléments irréductibles.

Comme $A[X]^\times = A^\times$, deux éléments irréductible de $A[X]$ ne peuvent être associés que s'ils sont soit tous les deux des irréductibles de A, soit tous les deux des polynômes non-constants. Des irréductibles $p, q \in A \subset A[X]$ sont associés dans A si et seulement s'ils sont associés dans $A[X]$. L'ensemble I des classes d'irréductibles associés dans A s'identifie donc avec un sous-ensemble de l'ensemble des classes d'irréductibles dans $A[X]$ et pour tout $i \in I$, le représentant $p_i \in A$ est également un représentant dans $A[X]$.
Notons J l'ensemble des classes de polynômes irréductibles de $K[X]$ pour la relation d'être associés. D'après le lemme 1.6.5, toute classe $j \in J$ contient un polynôme $P_j \in A[X]$ avec $\mathrm{cont}(P_j) = 1$. D'après la proposition 1.6.7, P_j est irréductible dans $A[X]$ et tous les polynômes irréductibles non-constants de $A[X]$ sont obtenus de cette façon. Soient $P, Q \in A[X]$ irréductibles non-constants. Si P et Q sont

associés dans $A[X]$ ils le sont aussi dans $K[X]$. Réciproquement, s'ils sont associés dans $K[X]$ alors il existe $x \in K$ tel que $P = xQ$ et comme $\mathrm{cont}(P) = \mathrm{cont}(Q) = 1$ on a alors $\mathrm{cont}(x) = 1$ donc $x \in A^\times$ et P et Q sont alors associés dans $A[X]$. On conclut que J s'identifie avec un sous-ensemble de l'ensemble des classes d'irréductibles dans $A[X]$ et pour tout $j \in J$, le polynôme P_j est un représentant de cette classe dans $A[X]$ aussi bien que dans $K[X]$. L'ensemble des classes d'irréductibles dans $A[X]$ pour la relation d'association est donc la réunion $I \cup J$.

1.6.9 Théorème. *Si A est un anneau factoriel alors l'anneau $A[X]$ est factoriel.*

Démonstration. Rappelons que l'anneau $K[X]$ est euclidien, donc principal, donc factoriel. Si $P \in A[X]$ il existe donc des $\beta_j \geq 0$ pour $j \in J$, tous nuls sauf un nombre fini et un élément $x \in K$ non-nul tels que $P = x \prod_{j\in J} P_j^{\beta_j}$. Les polynômes P_j appartiennent à $A[X]$ et sont de contenu 1 donc

$$\mathrm{cont}(x) = \mathrm{cont}(x) \prod_{j\in J} \mathrm{cont}(P_j)^{\beta_j} = \mathrm{cont}(P) \in A$$

et on déduit que $x \in A$. Il existe alors des $\alpha_i \geq 0$ pour $i \in I$, tous nuls sauf un nombre fini et $u \in A^\times$ tels que $x = u \prod_{i\in I} p_i^{\alpha_i}$. On en déduit une factorisation de P dans $A[X]$.
Supposons qu'on a des $\alpha'_i \geq 0$ pour $i \in I$, des $\beta'_j \geq 0$ pour $j \in J$ et une unité $u' \in A^\times$ tels que

$$u \prod_{i\in I} p_i^{\alpha_i} \prod_{j\in J} P_j^{\beta_j} = P = u' \prod_{i\in I} p_i^{\alpha'_i} \prod_{j\in J} P_j^{\beta'_j}.$$

L'unicité de la factorisation dans $K[X]$ implique alors que $\beta_j = \beta'_j$ pour tout $j \in J$ et $u \prod_{i\in I} p_i^{\alpha_i} = u' \prod_{i\in I} p_i^{\alpha'_i}$. L'unicité de la factorisation dans A implique que $\alpha_i = \alpha'_i$ pour tout $i \in I$ et $u = u'$. Cela établit l'unicité de la factorisation dans $A[X]$. □

1.6.10 Exemple. Le théorème implique que $\mathbb{Z}[X]$ est un anneau factoriel. C'est un exemple d'un anneau factoriel qui n'est pas principal.

1.6.11 Définition. Soient A un anneau commutatif et $n \geq 1$ un entier. On définit, par récurrence sur n, l'anneau $A[X_1, \ldots, X_n]$ des polynômes à a variables à coefficients dans A par

— $A[X_1]$ est l'anneau des polynôme en une variable X_1 défini dans 1.1.4 et
— pour $n \geq 2$ on pose $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$.

1.6.12 Remarques. (i) Tout $P \in A[X_1, \ldots, X_n]$ s'écrit

$$P = \sum_{\underline{i}=(i_1,\ldots,i_n)\in\mathbb{N}^n} \lambda_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n} = \sum_{\underline{i}\in\mathbb{N}^n} \lambda_{\underline{i}} \underline{X}^{\underline{i}}$$

où les $\lambda_{\underline{i}} \in A$ sont tous nuls sauf pour un nombre finie de $\underline{i}$.

(ii) On peut définir l'évaluation des polynômes en $X_1 \ldots, X_n$ comme dans 1.1.8. Si B est un anneau commutatif, $\varphi\colon A \to B$ est un morphisme d'anneaux et $b_1, \ldots, b_n \in B$ alors il existe un unique morphisme d'anneaux

$$\tilde{\varphi}_{\underline{b}}\colon A[X_1, \ldots, X_n] \to B$$

tel que $\tilde{\varphi}_{\underline{b}}|_A = \varphi$ et $\tilde{\varphi}_{\underline{b}}(X_i) = b_i$ pour $i = 1, \ldots, n$.

1.6.13 Corollaire. *Soit A factoriel et soit $n > 0$ un entier. Alors l'anneau $A[X_1, X_2, \ldots, X_n]$ est factoriel.*

1.6.14 Remarque. Une question évidente est comment est-ce qu'on peut décider si un polynôme $P \in A[X]$, A factoriel, est irréductible. Il y a un critère suffisant élémentaire : Si $I \subset A$ est un idéal et si l'image $\overline{P} \in (A/I)[X]$ est irréductible et du même degré que P, alors P est irréductible dans $K[X]$. En effet si $P = QR$ dans $A[X]$, on a $\overline{P} = \overline{Q} \cdot \overline{R}$ donc soit $\overline{Q}$ soit $\overline{R}$ est constant. Comme $\deg(\overline{Q}) \leq \deg(Q)$, $\deg(\overline{R}) \leq \deg(R)$ et $\deg(\overline{Q}) + \deg(\overline{R}) = \deg(\overline{P}) = \deg(P) = \deg(Q) + \deg(R)$ on conclut que Q ou R est constant.

1.6.15 Exemples. (i) Le polynôme $3X^2 + X$ est irréductible modulo 3 mais pas dans $\mathbb{Q}[X]$.

(ii) Par exemple $X^2 + 1$ est irréductible dans $(\mathbb{Z}/3\mathbb{Z})[X]$ parce que le polynôme $X^2 + \overline{1}$ n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$. On en déduit que pour tout $n \in \mathbb{Z}$ avec $n \equiv 1 \bmod 3$, le polynôme $X^2 + n$ est irréductible dans $\mathbb{Z}[X]$.

(iii) Par contre $X^2 + 1 = (X - \overline{2})(X - \overline{3})$ dans $(\mathbb{Z}/5\mathbb{Z})[X]$ donc $X^2 + 1$ n'est pas irréductible dans $(\mathbb{Z}/5\mathbb{Z})[X]$.

1.6.16 Proposition (Critère d'Eisenstein)**.** *Soit A un anneau factoriel et soit $P = \sum_{i=0}^{n} \lambda_i X^i \in A[X]$ un polynôme de degré $n \geq 1$ avec* $\mathrm{cont}(P) = 1$. *Supposons qu'il existe un élément irréductible $p \in A$ tel que $p \nmid \lambda_n$, $p \mid \lambda_i$ pour $i < n$ et $p^2 \nmid \lambda_0$. Alors P est irréductible dans $A[X]$.*

Démonstration. Supposons que $P = QR$ où

$$Q = \mu_d X^d + \ldots \mu_0 \quad \text{et} \quad R = \nu_e X^e + \ldots \nu_0 \in A[X]$$

avec $d = \deg(Q)$ et $e = \deg(R)$ On a $\lambda_0 = \mu_0 \nu_0$ et comme $p^2 \nmid \lambda_0$, l'élement p divise μ_0 ou ν_0, mais pas les deux. Supposons que $p \mid \mu_0$. On a $p \nmid \lambda_n$ donc il existe un $1 \leq j \leq e$ tel que $p \nmid \mu_j$. Soit j_0 minimal avec cette propriété. Alors

$$\lambda_{j_0} = \mu_{j_0}\nu_0 + \sum_{j=0}^{j_0-1} \mu_j \nu_{j_0-j} \ .$$

Le premier terme du membre de droite n'est pas divisible par p alors que tous les autres termes sont divisible par p. Il s'ensuit que λ_{j_0} n'est pas divisible par p et on doit alors avoir $j_0 = n$. Cela implique que $d = \deg(Q) = n$ et que R est constant. Comme $\mathrm{cont}(P) = 1$ on a $\mathrm{cont}(R) = 1$ donc R est alors une unité. Cela montre que P est irréductible dans $A[X]$. □

1.6.17 Exemples. (i) Le polynôme $P = 3X^5+2X^3-4X^2+2 \in \mathbb{Z}[X]$ est irréductible. En fait on a $\mathrm{cont}(P) = 1$ et les hypothèses du critère d'Eisenstein sont satisfaites pour $p = 2$.

(ii) Le polynôme $P = X^4+1 \in \mathbb{Z}[X]$ est irréductible. En fait P est irréductible si est seulement si $Q = (Y+1)^4+1 = Y^4+4Y^3+6Y^2+4Y+2 \in \mathbb{Z}[Y]$ est irréductible. On a de nouveau $\mathrm{cont}(Q) = 1$ et on peut de nouveau utiliser le critère d'Eisenstein avec $p = 2$.

(iii) Soient p un nombre premier et $n > 0$ un entier, alors $X^n \pm p \in \mathbb{Z}[X]$ est irréductible.

1.6.18 Proposition. *Soit p un nombre premier alors $X^{p-1} + \ldots + X + 1 \in \mathbb{Z}[X]$ est irréductible.*

Démonstration. On fait le changement de variables $X = Y + 1$. On a

$$(X^{p-1}+\ldots+X+1)(X-1) = X^p-1 = (Y+1)^p-1 = \sum_{i=1}^{p} \binom{p}{i} Y^i = Y \sum_{i=1}^{p} \binom{p}{i} Y^{i-1}$$

donc $(X^{p-1} + \ldots + X + 1) = \sum_{i=1}^{p} \binom{p}{i} Y^{i-1}$. Le critère d'Eisenstein est satisfait pour le nombre premier p et le polynôme $\sum_{i=1}^{p} \binom{p}{i} Y^{i-1}$. □

2 Corps

2.1 Généralités.

On rappelle la définition 1.2.16 d'un corps. Un corps est donc en particulier un anneau et si K et L sont des corps, une application $\varphi\colon K \to L$ est un *morphisme de corps* si c'est un morphisme d'anneaux. Notons que par hypothèse on a $\varphi(1_K) = 1_L$ donc $\mathrm{Ker}(\varphi) \neq K$ et comme $\{0\}$ et K sont les seuls idéaux de K on déduit que φ est injectif. On dit $K \subset L$ est un *sous-corps* si c'est un sous anneau. Dans ce dernier cas on dit aussi que L est une *extension* de K.

2.1.1 Exemples. (i) Les anneaux $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps ; $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un entier premier. Si p est un nombre premier on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (consideré comme corps). Si A est un anneau intègre, son corps de fractions F_A construit dans le théorème 1.5.1 est un corps.

(ii) L'anneau $\mathbb{Z}$ n'est pas un corps. Si A est un anneau, alors $A[X]$ n'est jamais un corps.

(iii) $\mathbb{R}$ est un sous-corps de $\mathbb{C}$ et $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et de $\mathbb{C}$.

2.1.2 Définition. Soit K un anneau. Alors d'après l'exemple 1.1.7(vi), il existe un unique morphisme $\varphi\colon \mathbb{Z} \to K$ et il existe alors un unique $n \in \mathbb{Z}$ avec $n \geq 0$ tel que $\mathrm{Ker}(f) = (n)$. On dit que n est la *caractéristique de* K et on écrit $n = \mathrm{car}(K)$.

2.1.3 Proposition. *La caractéristique d'un corps est soit* 0*, soit un nombre premier.*

Démonstration. L'image du morphisme $\varphi\colon \mathbb{Z} \to K$ est un sous anneau de l'anneau intègre K donc c'est un anneau intègre. On a $\mathrm{Im}(\varphi) \cong \mathbb{Z}/\mathrm{Ker}(\varphi)$, donc la proposition 1.2.14 implique que $\mathrm{Ker}(\varphi) \subset \mathbb{Z}$ est un idéal premier. La caractéristique n est le générateur positif de $\mathrm{Ker}(\varphi)$ donc la proposition 1.3.6 implique que soit $n = 0$ soit n est un nombre premier. □

2.2 Extensions de corps

2.2.1 Lemme. *Soient K un corps et L une extension de K. Alors L possède une structure naturelle de K-espace vectoriel.*

Démonstration. Pour définir sur L une structure de K-espace vectoriel il faut définit une addition interne sur L et une multiplication externe des éléments de L par des éléments de K. Pour l'addition interne on prend l'addition du corps L, pour la multiplication externe on prend la restriction à $K \times L$ de la multiplication $L \times L \to L$. Une vérification facile, utilisant les propriétés de l'addition et de la multiplication de L établit que le résultat est bien une structure de K-espace vectoriel sur L. □

2.2.2 Définition. Si L est une extension de K, alors le *degré* de cette extension (noté $[L : K]$ ou $\dim_K L$) est la dimension de L vu comme K-espace vectoriel. On dit que l'extension est une *extension finie* si L est un K-espace vectoriel de dimension finie.

2.2.3 Exemples. (i) $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré 2.

(ii) $\mathbb{Q}[X]/(X^2 + 1)$ est une extension de $\mathbb{Q}$ de degré 2.

(iii) $\mathbb{Q}[X]/(X^3 + 2)$ est une extension de $\mathbb{Q}$ de degré 3.

(iv) $\mathbb{F}_2[X]/(X^2 + X + 1)$ est une extension de $\mathbb{F}_2$ de degré 2.

(v) $\mathbb{F}_3[X]/(X^3 + 2X + 1)$ est une extension de $\mathbb{F}_3$ de degré 3.

(vi) $K(X)$ est une extension de K de degré infini.

(vii) $\mathbb{C}$ est une extension de $\mathbb{Q}$ de degré infini. Pour montrer cela, il peut utiliser qu'il existe des éléments de $\mathbb{C}$ qui ne sont pas algébriques sur $\mathbb{Q}$.

2.2.4 Proposition. *Soit K un corps fini. Alors $p = \mathrm{car}(K) > 0$ donc c'est un nombre premier. Le corps K est alors une extension de $\mathbb{F}_p$ de degré fini $d > 0$ et on a $|K| = p^d$.*

Démonstration. Si K est fini, alors l'image du morphisme $\varphi\colon \mathbb{Z} \to K$ est fini donc $\mathrm{Ker}(\varphi) \neq 0$. Il résulte de la proposition 2.1.3 que $\mathrm{car}(K) = p > 0$ est un nombre premier. On identifie $\mathrm{Im}(\varphi)$ avec $\mathbb{Z}/\mathrm{Ker}(\varphi) = \mathbb{Z}/(p) = \mathbb{F}_p$, de sorte que K est une extension de $\mathbb{F}_p$. Comme K est fini, il peut être engendré, en tant que $\mathbb{F}_p$-espace vectoriel, par un ensemble fini donc $[K : \mathbb{F}_p]$ est fini, disons égal à $d > 0$. Cela implique que $K \cong \mathbb{F}_p^d$ comme $\mathbb{F}_p$-espace vectoriel d'où $|K| = p^d$. □

2.2.5 Proposition. *Soient K, L et M des corps, L une extension de K et M une extension de L. Alors $[M : K]$ est finie si et seulement si $[M : L]$ et $[L : K]$ le sont et dans ce cas on a $[M : K] = [M : L][L : K]$.*

Démonstration. Supposons d'abord que M est une extension finie de K. Comme L est un sous-K-espace vectoriel de M, cela implique que L est une extension finie de K. Soit $(c_1, \cdots, c_e)$ une famille finie qui engendre M comme K-espace vectoriel, alors la même famille engendre aussi M comme L-espace vectoriel ce qui implique que $[M : L]$ est fini.
Réciproquement, supposons que $[L : K]$ et $[M : L]$ sont finis, disons égaux à d et e. On fixe une K-base $(b_1, \cdots, b_d)$ de L et une L-base $(c_1, \cdots, c_e)$ de M. On affirme que $\mathcal{B} = (b_i c_j)_{\substack{i=1,\ldots,d \\ j=1,\ldots,e}}$ est une K-base de M. Cela implique à la fois que $[M : K]$ est fini et que $[M : K] = [M : L][L : K]$. Pour montrer l'affirmation sur $\mathcal{B}$, on montre que cette famille est libre et génératrice.
Pour montrer qu'elle est libre, supposons qu'on a $\lambda_{i,j} \in K$, pour $i = 1, \ldots, d$ et $j = 1, \ldots, e$, tels que $\sum_{i,j} \lambda_{i,j} b_i c_j = 0$. Alors

$$0 = \sum_{i,j} \lambda_{i,j} b_i c_j = \sum_{j=1}^{e} \left(\sum_{i=1}^{d} \lambda_{i,j} b_i \right) c_j$$

d'où $\sum_{i=1}^{d} \lambda_{i,j} b_i = 0$ pour tout j car (c_j) est une famille libre sur L. Pour j fixé, le fait que (b_i) est libre sur K implique que $\lambda_{i,j} = 0$ pour tout i. On conclut que $\lambda_{i,j} = 0$ pour tous i et j.
On montre enfin que $\mathcal{B}$ engendre M comme K-espace vectoriel. Soit donc $x \in M$. Comme (c_j) engendre M comme L-espace vectoriel, il existe $\mu_j \in L$, pour $j = 1, \ldots, e$ tels que $x = \sum_{j=1}^{e} \mu_j c_j$. Pour j fixé, le fait que (b_i) engendre L sur K implique qu'il existe $\lambda_{i,j} \in K$, pour $i = 1, \cdots, d$, tels que $\mu_j = \sum_{i=1}^{d} \lambda_{i,j} b_i$. En substituant dans l'expression pour x, on obtient que $x = \sum_{i,j} \lambda_{i,j} b_i c_j$. □

2.2.6 Définition. Soient $K \subset L$ des corps et $a_1, \ldots, a_n \in L$. Alors *l'extension de K engendrée par $a_1, \ldots, a_n$*, notée $K(a_1, \ldots, a_n)$, est l'intersection des sous-corps de L contenant K et $\{a_1, \ldots, a_n\}$.

2.2.7 Remarque. Il est laissé comme exercice de montrer que $K(a_1, \ldots, a_n)$ est bien un corps.

2.2.8 Définition. Soit $K \subset L$ une extension de corps. Un élément α de L est *algébrique sur K* s'il existe un polynôme non nul $P \in K[X]$ tel que $P(\alpha) = 0$. S'il existe un tel polynôme, alors il en existe un (et un seul) qui est de degré minimal et unitaire. Ce polynôme s'appelle le *polynôme minimal* de α sur K. On appelle *degré (sur K)* d'un élément algébrique $\alpha \in L$ le degré de son polynôme minimal. Une extension $K \subset L$ est *algébrique* si tout élément de L est algébrique sur K.

2.2.9 Théorème. *Soient K un corps, L une extension de K et $\alpha \in L$. Alors les conditions suivantes sont équivalentes.*

(i) *α est algébrique sur K.*

(ii) *Le morphisme $\mathrm{ev}_\alpha \colon K[X] \to L$ n'est pas injectif.*

(iii) *$[K(\alpha) : K]$ est finie.*

(iv) *Il existe une extension finie $L' \subset L$ de K contenant α.*

(v) *On a $\mathrm{Im}(\mathrm{ev}_\alpha) = K(\alpha)$.*

Si ces conditions sont vérifiées, alors $\mathrm{Ker}(\mathrm{ev}_\alpha) = (M_\alpha)$ où M_α est le polynôme minimal de α sur K, le polynôme M_α est irréductible dans $K[X]$ et le corps $K(\alpha)$ est isomorphe à $K[X]/(M_\alpha)$. On a alors une égalité $[K(\alpha) : K] = \deg(M_\alpha)$, le degré de α sur K. Si on note $d = [K(\alpha) : K]$, alors $(1, \alpha, \ldots, \alpha^{d-1})$ est une K-base de $K(\alpha)$.

Démonstration. L'équivalence des conditions 2.2.9(i) et 2.2.9(ii) résulte directement de la définition d'un élément algébrique.
Si la condition 2.2.9(iii) est vérifiée, alors la 2.2.9(iv) l'est aussi, il suffit de prendre $L' = K(\alpha)$. Réciproquement, supposons qu'il existe une extension finie $L' \subset L$ de K contenant α. Alors on a $K(\alpha) \subset L'$ donc la proposition 2.2.5 implique que $[K(\alpha) : K]$ est fini. On a montré l'équivalence des conditions 2.2.9(iii) et 2.2.9(iv).
L'image de ev_α est contenu dans $K(\alpha)$ car cette image est contenu dans L' pour toute extension $L' \subset L$ de K contenant α. Supposons maintenant que ev_α est injectif. Alors $K[X] \cong \mathrm{Im}(\mathrm{ev}_\alpha) \subset K(\alpha)$ et l'inclusion ne peut pas être une égalité car $K(\alpha)$ est un corps et $K[X]$ n'en est pas. En plus, l'anneau $K[X]$ est de dimension infinie comme K-espace vectoriel donc $\mathrm{Im}(\mathrm{ev}_\alpha)$ est également de dimension infinie sur K. Il s'ensuit que $[K(\alpha) : K]$ est infini. Cela montre que chacune des conditions 2.2.9(iii) et 2.2.9(v) implique 2.2.9(ii).

Si ev_α n'est pas injectif alors, comme $K[X]$ est un anneau principal, il existe $P \in K[X]$ non-nul tel que $\mathrm{Ker}(\mathrm{ev}_\alpha) = (P)$. On a $K[X]/(P) \cong \mathrm{Im}(\mathrm{ev}_\alpha)$ et cet anneau est intègre car c'est un sous-anneau d'un corps. La proposition 1.2.14 implique que (P) est un idéal premier et donc, d'après la proposition 1.3.6, c'est un idéal maximal. La proposition 1.2.18 implique que $\mathrm{Im}(\mathrm{ev}_\alpha) \cong K[X]/(P)$ est un corps. C'est un sous-corps de L contenant α donc $K(\alpha) \subset \mathrm{Im}(\mathrm{ev}_\alpha)$. L'autre inclusion étant évidente on déduit que $\mathrm{Im}(\mathrm{ev}_\alpha) = K(\alpha)$. On a prouvé que 2.2.9(ii) implique 2.2.9(v).
Supposons enfin que la condition 2.2.9(i), donc aussi les 2.2.9(ii) et 2.2.9(v) sont vérifiées. Alors $\mathrm{Ker}(\mathrm{ev}_\alpha) \subset K[X]$ est un idéal non nul et le polynôme minimal M_α est un élément non nul de cet idéal de degré minimal. On a donc $\mathrm{Ker}(\mathrm{ev}_\alpha) = (M_\alpha)$ et les arguments qui précèdent donnent un isomorphisme de corps (et de K-espaces vectoriels)

$$K(\alpha) = \mathrm{Im}(\mathrm{ev}_\alpha) \cong K[X]/(M_\alpha).$$

En notant $e = \deg(M_\alpha)$, un argument élémentaire montre que $(1, X, \cdots, X^{d-1})$ est une K-base de $K[X]/(M_\alpha)$ donc

$$e = \dim_K K[X]/(M_\alpha) = \dim_K K(\alpha) = [K(\alpha) : K].$$

On en déduit que la condition 2.2.9(iii) est vérifiée.
Tout cela montre que les cinq conditions du théorème sont équivalentes et que si elles sont vérifiés alors $\mathrm{Ker}(\mathrm{ev}_\alpha) = (M_\alpha)$ et $K(\alpha) \cong K[X]/(M_\alpha)$. Par le même argument qu'auparavant, cela implique que M_α est irréductible. On a vu aussi que $d = [K(\alpha) : K] = \deg(M_\alpha)$ et que $(1, X, \cdots, X^{d-1})$ est une K-base de $K[X]/(M_\alpha)$. Comme $\overline{\mathrm{ev}}_\alpha \colon K[X]/(M_\alpha) \to K(\alpha)$ est un isomorphisme et $\overline{\mathrm{ev}}_\alpha(X^i) = \alpha^i$ on en déduit la dernière affirmation. □

2.2.10 Remarque. Si $\alpha \in L$ n'est pas algébrique sur K, alors le morphisme $\mathrm{ev}_\alpha \colon K[X] \to L$, $P \mapsto P(\alpha)$ induit un isomorphisme $K(X) \cong K(\alpha)$.

2.2.11 Corollaire. *Soient K et L des corps, L une extension de K et soit $\alpha \in L$ algébrique sur K. Si $P \in K[X]$ est un polynôme irréductible et unitaire tel que $P(\alpha) = 0$ alors $P = M_\alpha$, le polynôme minumal de α sur K.*

Démonstration. Si $P(\alpha) = 0$ alors $P \in \mathrm{Ker}(\mathrm{ev}_\alpha) = (M_\alpha)$ donc M_α divise P. Comme P est irréductible et M_α non constant, cela implique que $P = cM_\alpha$ pour un élément $c \in K$. L'hypothèse que P et M_α sont unitaires implique alors que $P = M_\alpha$. □

2.2.12 Corollaire. *Soient K un corps et L une extension finie de K. Alors L est une extension algébrique de K.*

Démonstration. Si $\alpha \in L$ alors $K(\alpha) \subset L$ donc la condition 2.2.9(iv) du théorème précédent est vérifiée avec $L' = L$. Ce théorème implique alors que α est algébrique sur K. □

2.2.13 Corollaire. *Soient K un corps et L une extension de K. Alors*

$$M = \{\alpha \in L \mid \alpha \text{ est algébrique sur } K\}$$

est un sous-corps de L (contenant K).

Démonstration. Il est évident que $K \subset M$. Soient $\alpha, \beta \in M$, alors le théorème 2.2.9 implique que $K(\alpha)$ est une extension finie de K. L'élément $\beta \in M$ est algébrique sur K donc aussi sur $K(\alpha)$ et il s'ensuit que $K(\alpha, \beta) = K(\alpha)(\beta)$ est une extension finie de $K(\alpha)$. La proposition 2.2.5 implique alors que $K(\alpha, \beta)$ est une extension finie de K. Le théorème 2.2.9 implique alors que

$$-\alpha, \alpha + \beta, \alpha\beta \in K(\alpha, \beta)$$

sont algébriques sur K. De même, si $\alpha \neq 0$, alors α^{-1} est algébrique. □

2.2.14 Remarque. Le corollaire implique que somme, produit, opposé et inverse d'éléments de L qui sont algébriques sur K sont algébriques sur K.

2.2.15 Corollaire. *Soient K un corps, L une extension algébrique de K et M une extension algébrique de L. Alors M est une extension algébrique de K.*

Démonstration. Soient $\alpha \in M$ et $P(X) = X^d + \sum_{i=0}^{d-1} \lambda_i X^i \in L[X]$ le polynôme minimal de α sur L. Les λ_i sont algébriques sur K. Pour $i = 1, \ldots, d-1$ soit $L_i = K(\lambda_0, \ldots, \lambda_{i-1}) \subset L$. Alors d'après le théorème 2.2.9, L_1 est une extension finie de K et pour $i = 2, \ldots, d-1$, l'extension $L_i \supset L_{i-1}$ est également finie. La proposition 2.2.5 implique que $K \subset L_d$ est une extension finie. Comme $P \in L_d[X]$, l'extension $L_d(\alpha) \supset L_d$ est finie et il en va alors de même pour $L_d(\alpha) \supset K$. Il en résulte que α est algébrique sur K. □

2.2.16 Lemme. *Soit K un corps. Les conditions suivantes sont équivalentes.*

(i) Tout polynôme irréductible dans $K[X]$ est de degré 1.

(ii) Toute extension finie de K est de degré 1 (c'est-à-dire, est égale à K).

(iii) Toute extension algébrique de K est de degré 1.

Démonstration. Supposons que la condition 2.2.16(i) est vérifiée et soit L une extension algébrique de K. Si $\alpha \in L$ alors le polynôme minimal $M_\alpha \in K[X]$ de α sur K est irréductible d'après le théorème 2.2.9 donc de degré 1 par hypothèse, c'est-à-dire $M_\alpha(X) = X - \alpha$, donc $\alpha \in K$. Cela implique que $L = K$ donc $[L : K] = 1$.

Comme toute extension finie est algébrique, il est évident que la troisième condition implique la deuxième.
Supposons enfin que toute extension finie de K est de degré 1. Si $P \in K[X]$ est irréductible alors $K[X]/(P)$ est un corps. C'est une extension finie de K de degré $\deg(P)$ et il s'ensuit que $\deg(P) = 1$. □

2.2.17 Définition. Un corps K est *algébriquement clos* si les conditions équivalentes du lemme sont vérifiées.

2.2.18 Exemple. D'après le théorème de d'Alembert–Gauss, le corps $\mathbb{C}$ est algébriquement clos. Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{F}_p$ (p premier) ne le sont pas.

2.2.19 Définition. Soit K un corps. Une extension $\overline{K}$ de K est une *clôture algébrique de* K si $\overline{K}$ est algébriquement clos et si c'est une extension algébrique de K.

2.2.20 Exemple. Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$. D'après le corollaire 2.2.13,

$$\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid x \text{ est algébrique sur } \mathbb{Q}\}$$

est un sous corps de $\mathbb{C}$. C'est clairement une extension algébrique de $\mathbb{Q}$ et d'après le corollaire 2.2.15, c'est une clôture algébrique de $\mathbb{Q}$.

2.3 Adjonction de racines, corps de décomposition

2.3.1 Théorème. *Soit K un corps. Alors il existe une clôture algébrique de K ; deux clôtures algébriques de K sont isomorphes.*

2.3.2 Proposition. *Soient K un corps et $P \in K[X]$ irréductible. Alors il existe un corps L contenant K et un élément α de L tels que*

(i) $L = K(\alpha)$ *et*

(ii) $P(\alpha) = 0$.

Si (L', α') est un tel couple, alors (L, α) et (L', α') sont K-isomorphes, c'est-à-dire qu'il existe un unique isomorphisme $L \cong L'$ envoyant α sur α' et dont la restriction à K est l'identité.

Démonstration. Pour l'existence, on prend $L = K[X]/(P)$, c'est un corps car P est irréductible, et $\alpha = \bar{X}$.
Si $L' = K(\alpha')$ est une extension de K et $P(\alpha') = 0$, on considère le morphisme $\mathrm{ev}_{\alpha'} \colon K[X] \to L'$. On a $(P) \subset \mathrm{Ker}(\mathrm{ev}_{\alpha'})$ et comme $(P) \subset K[X]$ est un idéal maximal, cette inclusion est une égalité. On en déduit un morphisme injectif $\varphi \colon L = K[X]/(P) \to L' = K(\alpha')$ tel que $\varphi(\alpha) = \alpha'$. Comme $\mathrm{Im}(\varphi) \subset L'$ est

un sous-corps contenant α' ce morphisme est surjectif. Si enfin $\varphi' : L \to L'$ est un autre isomorphisme, alors on vérifie facilement que $M = \{x \in L \mid \varphi(x) = \varphi'(x)\}$ est un sous-corps de L contenant K et α, donc $M = L$ et par conséquent $\varphi = \varphi'$. □

2.3.3 Définition. Dans la situation de la proposition, on dit que L est obtenu *par adjonction d'une racine de P à K* ou encore que L est un *corps de rupture de P sur K*.

2.3.4 Définition. Soient K corps, $P \in K[X]$ et L une extension de K. Alors P est *décomposé sur L* si P est un produit de facteurs linéaires dans $L[X]$. On dit que L est *un corps de décomposition de P sur K* si

(i) P est décomposé sur L et

(ii) P n'est décomposé sur aucune extension de K strictement contenue dans L.

2.3.5 Remarques. (i) La deuxième condition de la définition peut être remplacée par la condition que $L = K(\alpha_1, \ldots, \alpha_n)$ où $\alpha_1, \ldots, \alpha_n$ sont les racines de P dans L.

(ii) Un corps de décomposition L de $P \in K[X]$ est une extension finie de K. En effet, si $\alpha_1, \ldots, \alpha_n \in L$ sont les racines de P, alors toute extension dans la suite

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = L$$

est finie.

2.3.6 Exemples. (i) Le corps $\mathbb{Q}(\sqrt{3}, i)$ est un corps de décomposition du polynôme $(X^2 - 3)(X^3 + 1)$ sur $\mathbb{Q}$, c'est une extension de degré 4.

(ii) Deux polynômes distincts peuvent avoir le même corps de décomposition. Par exemple $X^2 - 3$ et $X^2 - 2X - 2$ sur $\mathbb{Q}$.

(iii) Pour P irréductible de degré 2, le corps obtenu par adjonction d'une racine est un corps de décomposition.

(iv) Pour P de degré 3 irréductible, le corps obtenu par adjonction d'une racine n'est pas toujours un corps de décomposition. Par exemple $X^3 - 2$ sur $\mathbb{Q}$.

(v) Pour P de degré 3 irréductible, le corps obtenu par adjonction d'une racine peut être un corps de décomposition. Pour le polyôme $X^3 - 3X + 1 \in \mathbb{Q}[X]$ par exemple, les racines dans $\mathbb{Q}[X]/(X^3 - 3X + 1)$ sont $\bar{X}$, $-2 + \bar{X}^2$ et $2 - \bar{X} - \bar{X}^2$.

(vi) Soient k de caractéristique $p > 0$ et $K = k(X)$. Alors $L = K[T]/(T^p - X)$ est un corps de décomposition de $T^p - X$ sur K.

(vii) Soit $K = \mathbb{C}(X)$, alors $L = K[T]/(T^n - X)$ est un corps de décomposition de $T^n - X$ sur K.

(viii) $L = \mathbb{F}_3[T]/(T^3 - T + 1)$ est un corps de décomposition de $X^3 - X + 1$ sur $\mathbb{F}_3$.

2.3.7 Théorème. *Soient K un corps et $P \in K[X]$. Alors il existe un corps de décomposition L de P sur K. Le corps L est une extension finie de K.*

Démonstration. Il résulte de la remarque 2.3.5(ii) que L est une extension finie de K. On démontre par récurrence sur $d \geq 1$ que pour tout corps K et tout polynôme $P \in K[X]$ de degré d, il existe un corps de décomposition de P sur K.
Si $P \in K[X]$ est de degré 1 alors P est décomposé sur K donc K est un corps de décomposition de P sur K.
Supposons maintenant que $d > 1$, que $P \in K[X]$ est un polynôme de degré d et que notre énoncé est vrai pour $d - 1$. Soit alors Q un facteur irréductible de P. D'après la proposition 2.3.2, il existe une extension $K' = K(\alpha)$ de K où α est une racine de Q. C'est aussi une racine de P. Le polynôme $X - \alpha$ divise alors P dans $K'[X]$, soit $R \in K'[X]$ le quotient. L'hypothèse de récurrence implique qu'il existe un corps de décomposition L de R sur K'. Montrons que L est aussi un corps de décomposition de P sur K. En effet $P(X) = (X - \alpha)R(X)$ dans $K'[X]$ donc P est décomposé sur L. Si P est décomposé sur un sous-corps $L' \subset L$ contenant K, alors l'unicité de la factorisation dans $L[X]$ implique que $\alpha \in L'$ donc $K' \subset L'$ et que R est décomposé sur L' donc $L' = L$ parce que L est un corps de décomposition de P sur K'. □

2.3.8 Théorème. *Soient $\varphi\colon K \to L'$ un morphisme de corps, $P \in K[X]$ et L un corps de décomposition de P sur K. On suppose que $\varphi(P)$ est décomposé sur L'. Alors il existe un morphisme de corps $\psi\colon L \to L'$ tel que $\psi|_K = \varphi$.*

Démonstration. La démonstration se fait encore par récurrence, sur $d = [L : K]$, pour tous les corps de décomposition de degré d fixe.
Si $[L : K] = 1$ alors $L = K$ et $\psi = \varphi$ convient. Supposons ensuite que L est un corps de décomposition sur K d'un polynôme P, que $d = [L : K] > 1$ et que le théorème est prouvé pour les corps de décomposition de degré $\leq d - 1$. Il existe alors une racine $\alpha \in L$ de P avec $\alpha \notin K$. Notons $K_1 = K(\alpha) \subset L$ est soit $Q \in K[X]$ un facteur irréductible de P tel que $Q(\alpha) = 0$, de sorte que $K_1 \cong K[X]/(Q)$. Comme $\varphi(Q)$ divise $\varphi(P)$ dans $L'[X]$ et P est décomposé sur L', il existe une racine $\alpha' \in L'$ de $\varphi(Q)$. Il existe donc un morphisme $\tilde{\varphi}\colon K[X] \to L'$ tel que $\tilde{\varphi}|_K = \varphi$ et $\tilde{\varphi}(X) = \alpha'$. Comme dans la démonstration de 2.3.2, on voit que $\mathrm{Ker}(\tilde{\varphi}) = (Q)$ et que $\tilde{\varphi}$ induit un morphisme injectif $\varphi_1\colon K_1 \cong K[X]/(Q) \to L'$. Comme L est un corps de décomposition de P sur K_1 et $[L : K_1] < [L : K] = d$, l'existence de $\psi\colon L \to L'$ prolongeant φ_1 résulte de l'hypothèse de récurrence. Ce morphisme ψ prolonge également φ. □

2.3.9 Corollaire. *Dans la situation du théorème, notons $K' = \varphi(K)$ et supposons que L' est un corps de décomposition de $\varphi(P)$ sur K'. Alors tout morphisme $\psi\colon L \to L'$ prolongeant φ est un isomorphisme.*

Démonstration. Il suffit de montrer que ψ est surjectif. Clairement $\psi(L) \subset L'$ est un corps sur lequel $\varphi(P)$ est décomposé. On a $K' = \varphi(K) = \psi(K) \subset \psi(L)$ donc $\psi(L)$ est une extension de K' contenue dans L' sur lequel P est décomposé. Comme L' est un corps de décomposition de $\varphi(P)$ sur K' on conclut que $L' = \psi(L)$. □

2.3.10 Corollaire. *Soient K un corps et $P \in K[X]$. Deux corps de décomposition de P sur K sont isomorphes en tant qu'extensions de K. En particulier, ils ont le même degré sur K.*

Démonstration. On applique les résultats précédent à $\mathrm{id}\colon K \to K$. □

2.4 Corps finis.

Soit K un corps fini. On a montré dans ce qui précède qu'il existe un nombre premier p et un entier d tels que K est une extension de $\mathbb{F}_p$ de degré d donc que $q = |K| = p^d$.

2.4.1 Proposition. *Soit K un corps fini de cardinal $q = p^d$ où p est un nombre premier. Alors K est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*

Démonstration. Comme $K^\times$ est un groupe d'ordre $q-1$ on a $\alpha^{q-1} = 1$ pour tout $\alpha \in K^\times$. Tous les éléments de K sont donc racines de $X^q - X$ et comme un polynôme de degré q possède au plus q racines, il s'ensuit que $X^q - X$ est décomposé (à racines simples) sur K. Il est évident que $X^q - X$ n'est décomposé sur aucun sous-corps de K qui est donc un corps de décomposition de ce polynôme sur $\mathbb{F}_p$. . □

2.4.2 Corollaire. *Si K est un corps fini d'ordre q alors le groupe multiplicatif $K^\times$ est cyclique d'ordre $q-1$.*

Démonstration. Soient ℓ un nombre premier divisant $q-1$ et e l'exposant de ℓ dans la factorisation de $q-1$. Le polynôme $X^{(q-1)/\ell} - 1$ a au plus $(q-1)/\ell$ racines dans $K^\times$ donc il existe $\alpha \in K$ tel que $\alpha^{(q-1)/\ell} \neq 1$. On voit facilement que $\beta_\ell = \alpha^{(q-1)/\ell^e}$ est d'ordre ℓ^e dans $K^\times$. Le produit des β_ℓ, pour ℓ parcourant l'ensemble des facteurs premiers de $q-1$ est d'ordre $q-1$ dans $K^\times$. □

2.4.3 Remarque. La même démonstration montre que si K est un corps quelconque et $G \subset K^\times$ un sous-groupe fini alors G est cyclique.

2.4.4 Théorème. *Soient p un nombre premier, $d > 0$ un entier et $q = p^d$. Soit $\mathbb{F}_q$ un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Alors $\mathbb{F}_q$ est un corps fini d'ordre q. Tout corps fini est isomorphe à un corps $\mathbb{F}_q$ pour exactement un entier q comme ci-dessus.*

Démonstration. Soient p, d et $q = p^d$ comme dans l'énoncé et soit $\mathbb{F}_q$ un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Notons $S \subset \mathbb{F}_q$ l'ensemble de racines de $X^q - X$. Admettons pour l'instant que S est un sous-corps de $\mathbb{F}_q$, ce qui implique que $S = \mathbb{F}_q$ et que $|\mathbb{F}_q| \leq q$. Comme $(X^q - X)' = -1$, le polynôme $X^q - X$ est à racines simples donc on a $|\mathbb{F}_q| = q$. Comme tout autre corps de cardinal q est aussi un corps de décomposition de $X^q - X$, l'unicité résulte du corollaire 2.3.10.
Il reste à prouver que S est un sous-corps de $\mathbb{F}_q$. Pour cela, notons que $F\colon x \mapsto x^p$ est un automorphisme de corps $\mathbb{F}_q$ donc $F^d\colon x \mapsto x^q$ aussi. On en déduit que $S = \{x \in \mathbb{F}_q \mid x^q = x\}$ est bien un sous-corps de $\mathbb{F}_q$. □

2.4.5 Lemme. *Soient $d, d' \geq 1$ tels $d'|d$, alors $X^{d'} - 1$ divise $X^d - 1$ dans $\mathbb{Z}[X]$.*

Démonstration. Le polynôme $Y - 1$ divise $Y^{d/d'} - 1$ et le lemme en résulte en substituant $Y = X^{d'}$. □

2.4.6 Théorème. *Soient p un nombre premier, $d, d' > 0$ des entiers et $q = p^d$, $q' = p^{d'}$. Alors $\mathbb{F}_q$ contient un sous-corps isomorphe à $\mathbb{F}_{q'}$ si et seulement si d' divise d.*

Démonstration. Si $\mathbb{F}_{q'} \subset \mathbb{F}_q$ alors $d' = [\mathbb{F}_{q'} : \mathbb{F}_p]$ divise $d = [\mathbb{F}_q : \mathbb{F}_p]$ d'après la proposition 2.2.5. Supposons réciproquement que $d'|d$, alors le lemme implique que $q' - 1 = p^{d'} - 1$ divise $q - 1 = p^d - 1$ donc, par le même lemme, $X^{q'-1} - 1$ divise $X^{q-1} - 1$ d'où enfin $X^{q'} - X$ divise $X^q - X$. Le polynôme $X^{q'} - X$ est donc décomposé sur $\mathbb{F}_q$ et le théorème 2.3.8 implique qu'il existe un morphisme injectif $\mathbb{F}_{q'} \to \mathbb{F}_q$. □

2.4.7 Corollaire. *Soit K corps fini de caractéristique p, alors il existe $P \in \mathbb{F}_p[X]$ (irréductible) tel que $K \cong \mathbb{F}_p[X]/(P)$.*

Démonstration. Soit $\alpha \in K$ un générateur de $K^\times$, alors $K = \mathbb{F}_p[\alpha] \cong \mathbb{F}_p[X]/(M_\alpha)$ où M_α est le polynôme minimal de α sur $\mathbb{F}_p$. □

2.4.8 Corollaire. *Soit p un nombre premier. Pour tout entier $d > 0$, il existe un polynôme irréductible de degré d dans $\mathbb{F}_p[X]$. Le polynôme $X^{p^d} - X$ est le produit des polynômes irréductibles unitaires dont le degré divise d.*

Démonstration. La première affirmation résulte du corollaire précédent. Si $d'|d$ et si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré d' alors $K = \mathbb{F}_p[X]/(P)$ est un corps de cardinal $q' = p^{d'}$. Ce corps est alors isomorphe à un sous-corps de

$\mathbb{F}_q$, où $q = p^d$ et il s'ensuit que P possède une racine dans $\mathbb{F}_q$. Cela implique que, dans $\mathbb{F}_q[X]$, on a $\text{pgcd}(P, X^q - X) \neq 1$ donc dans $\mathbb{F}_p[X]$ on a également $\text{pgcd}(P, X^q - X) \neq 1$. Comme P est irréductible, cela implique que P divise $X^q - X$. Réciproquement, si P est un facteur irréductible de $X^q - X$ alors P possède une racine dans $\mathbb{F}_q$, donc $\mathbb{F}_p[X]/(P)$ s'identifie à un sous-corps de $\mathbb{F}_q$. Cela implique que $\deg(P) = [\mathbb{F}_p[X]/(P) : \mathbb{F}_p]$ divise $[\mathbb{F}_q : \mathbb{F}_p] = d$. Comme $(X^q - X)' = -1$, le polynôme $X^q - X$ n'a pas de facteurs multiples donc $X^q - X$ est bien le produit des polynômes irréductibles unitaires distincts de $\mathbb{F}_p[X]$. □

2.4.9 Exemples. Le corollaire permet de trouver tous les polynômes irréductibles de degré donné sur $\mathbb{F}_p$.

A Dérivation de polynômes

Dans tout cet appendice K désigne un corps.

A.1 Définition. Si $P(X) = \sum_{i=0}^{n} \lambda_i X^i \in K[X]$ alors on définit la *dérivée* (formelle) de P par

$$P'(X) = \sum_{i=1}^{n} i\lambda_i X^{i-1} \in K[X].$$

A.2 Proposition. *(i) L'application $K[X] \to K[X]$ donnée par $P \mapsto P'$ est K-linéaire.*

(ii) L'application $P \mapsto P'$ vérifie la règle de Leibniz *: pour tous $P, Q \in K[X]$ on a $(PQ)' = P'Q + PQ'$.*

Démonstration. Il est évident que $P \mapsto P'$ est linéaire. Par linéarité de la dérivation et par distributivité, il suffit ensuite de prouver la règle de Leibniz pour des monômes $P(X) = X^d$ et $Q(X) = X^e$ au quel cas elle est évidente. □

A.3 Corollaire. *Si $P, Q \in K[X]$ tels que Q^2 divise P alors Q divise P'.*

Démonstration. Supposons que $P = Q^2 R$ pour $R \in K[X]$. En appliquant la règle de Leibniz deux fois on obtient

$$P' = (Q^2)'R + Q^2 R' = 2QQ'R + Q^2 R' = Q(2Q'R + QR').$$

□