CHAPITRE I

GÉNÉRALITÉS : ANNEAUX, CORPS, POLYNÔMES

Sauf exceptions explicitement signalées, tous les anneaux considérés dans ce livre seront des anneaux commutatifs et unitaires (c'est–à–dire dotés d'un neutre multiplicatif distinct du neutre additif) et tous les corps étudiés seront commutatifs.

Nous donnons dans ce chapitre quelques rappels de premier cycle et résultats concernant des structures sur lesquelles porte cet ouvrage : anneaux et corps; et quelques notions sur les polynômes. Le lecteur pourra aussi consulter son cours de premier cycle favori.

1. Anneaux et corps

1.1 Généralités

Proposition I.1 [et définition]**. —** *Soit A un anneau.*

- *Soit $a \in A$.*

  - On dit que a' est un inverse de a si, et seulement si, $aa' = a'a = 1_A$.

  - On dit que a est inversible lorsque a admet un inverse. Celui–ci est alors unique : on le note a^{-1}.

- *L'ensemble $U(A)$ des **éléments inversibles** de A, muni de la multiplication, est un groupe, appelé **groupe des unités de A**.*

Preuve : Soient a un élément inversible de A et a' et a'' deux inverses de a. Alors $a'' = 1_A a'' = (a'a)a'' = a'(aa'') = a'1_A = a'$.
$U(A)$ est non vide (car $1_A \in U(A)$) et la multiplication définit bien une loi de composition *interne* dans $U(A)$ puisque clairement, si $(a, b) \in U(A)^2$, $b^{-1}a^{-1}$ est un inverse de ab. Evidemment cette loi est associative et 1_A est neutre pour la multiplication dans $U(A)$. Enfin si $x \in U(A)$, l'inverse x^{-1} de x est dans $U(A)$ (son inverse est x), donc x^{-1} est le symétrique de x dans $(U(A), .)$.

Exemple I.2. — $U(\mathbb{Z}) = \{-1, 1\}$.

Définition I.3. — *Soient A et B deux anneaux, f une application de A dans B. On dit que f est un **homomorphisme d'anneaux** si, et seulement si :*
$(\forall (x, y) \in A^2,\ f(x + y) = f(x) + f(y)$ *et* $f(xy) = f(x)f(y))$ *et* $f(1_A) = 1_B$.
Le noyau $Ker(f)$ de f est alors un idéal de A.

Propriété I.4. — *Soient A et B deux anneaux, f un homomorphisme d'anneaux de A dans B. Alors $f(U(A)) \subseteq U(B)$ et $(\forall x \in U(A),\ (f(x))^{-1} = f(x^{-1}))$.*

En effet, pour $x \in U(A)$, on a :
$1_B = f(1_A) = f(xx^{-1}) = f(x)f(x^{-1}) = f(x^{-1}x) = f(x^{-1})f(x)$.

Proposition I.5 [et définition]**. —** *Soit k un anneau. Les conditions suivantes sont équivalentes :*

(i) *tout élément non nul de k est inversible ($k^* \subseteq U(k)$) ;*

(ii) *l'ensemble $k^* = k\backslash\{0\}$ des éléments non nuls de k, muni de la multiplication, est un groupe.*

Si elles sont vérifiées, on dit que k est un corps.

Proposition I.6. — *Soit k un corps. Alors k est un anneau intègre.*

Preuve : Tout élément de k^*, étant inversible, est régulier pour le produit.
Remarquons que la réciproque de cette proposition est bien sûr fausse ($\mathbb{Z}$ . . .), mais qu'on verra plus tard (VII.1) qu'un anneau intègre *fini* est un corps.

Proposition I.7. — *Soit k un anneau. k est un corps si, et seulement si, les seuls idéaux de k sont (0) et k.*

Preuve : Soit k un corps et I un idéal de k, avec $I \neq (0)$. Fixons $i \in I \setminus (0)$. Alors, pour chaque $x \in k$, $x = (xi^{-1})i \in I$. Donc $I = k$.
Soit k un anneau ayant (0) et k pour seuls idéaux. Pour $x \in k^*$, (x) est un idéal de k non réduit à (0), donc égal à k. En particulier $1 \in (x)$, c'est–à–dire : il existe $y \in k$ tel que $yx = xy = 1$.

Remarque I.8. — Cette proposition est fausse si l'on supprime l'hypothèse (ici implicite) de commutativité de l'anneau k. Par exemple, pour $n \geq 2$, l'anneau $\mathcal{M}_n(K)$ des matrices carrées de taille n à coefficients dans un corps commutatif K a pour seuls idéaux (0) et lui–même, mais n'est certes pas un corps.

Corollaire I.9. — *Soit k un corps. Tout homomorphisme d'anneaux f de k dans un anneau A (en particulier tout homomorphisme de corps f de k dans un corps $\mathbb{K}$) est injectif. (On dit parfois que f est un monomorphisme).*

Preuve : Ker(f) est un idéal de k et comme $f(1_k) = 1_A \neq 0$, il est distinct de k. Donc (proposition précédente) Ker$(f) = (0)$.

Proposition I.10. — *Soit A un anneau intègre, K un corps. Soit u un homomorphisme d'anneaux injectif de A dans K.* Frac(A) *désignant le corps des fractions de l'anneau A, u peut être prolongé en un homomorphisme de corps (injectif) de* Frac(A) *dans K.*

Preuve : On définit $\mathcal{U}$ de Frac(A) dans K de la façon suivante :

$$\forall r \in \mathrm{Frac}(A), \text{ si } r = z/d \text{ où } (z,d) \in A \times A^*, \mathcal{U}(r) = (u(z))(u(d))^{-1}.$$

On vérifie alors que cette définition est légitime (i.e. que $\mathcal{U}(r)$ ne dépend pas de l'écriture en fraction choisie). En effet si $r = a/b = a_1/b_1$, alors $ab_1 = a_1b$ dans A, donc

$u(a)u(b_1) = u(ab_1) = u(a_1b) = u(a_1)u(b)$, d'où $u(a)(u(b))^{-1} = u(a_1)(u(b_1))^{-1}$. On montre aisément que $\mathcal{U}$ est un homomorphisme d'anneaux de $\mathrm{Frac}(A)$ dans K, et prolonge u : $\forall z \in A$, $\mathcal{U}(z) = \mathcal{U}(z/1) = u(z)(u(1))^{-1} = u(z)$.

1.2 Anneau $\mathbb{Z}/n\mathbb{Z}$. Indicateur d'Euler

Proposition I.11. — *Soit n un entier naturel, $n \geq 2$, $a \in \mathbb{N}$, et $\bar{a}$ la classe de a modulo n. Les conditions suivantes sont équivalentes :*

(1) *a et n sont premiers entre eux (soit : $a \wedge n = 1$);*

(2) *$\bar{a}$ est un élément régulier de l'anneau $\mathbb{Z}/n\mathbb{Z}$;*

(3) *$\bar{a}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$;*

(4) *$\bar{a}$ est un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : • (3) $\Rightarrow$ (2) est trivial.

• (2) $\Rightarrow$ (3) : $\bar{a}$ est un élément régulier de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, l'application f de $\mathbb{Z}/n\mathbb{Z}$ dans lui–même, qui à x associe $x\bar{a}$, est injective. L'ensemble de départ et l'ensemble d'arrivée étant finis de même cardinal, f est bijective, donc surjective, et en particulier $\bar{1}$ a un antécédent par f : il existe $\bar{v} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a}\bar{v} = \bar{1}$, soit $\bar{a} \in U(\mathbb{Z}/n\mathbb{Z})$.

• (1) $\Leftrightarrow$ (3) : D'après le théorème de Bezout, n est premier avec a si, et seulement si, il existe $(u, v) \in \mathbb{Z}^2$ tel que $nu + va = 1$. Or cela équivaut à : $(\exists (u, v) \in \mathbb{Z}^2$ tel que, dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{1} = \bar{n}\bar{u} + \bar{v}\bar{a} = \bar{v}\bar{a})$, soit à : $(\exists \bar{v} \in \mathbb{Z}/n\mathbb{Z}$ t.q. $\bar{a}\bar{v} = \bar{1})$, soit à : $\bar{a} \in U(\mathbb{Z}/n\mathbb{Z})$.

• (3) $\Leftrightarrow$ (4) : $(\bar{a} \in U(\mathbb{Z}/n\mathbb{Z})) \Leftrightarrow (\exists \bar{t} \in \mathbb{Z}/n\mathbb{Z}$ t.q. $\bar{t}\bar{a} = \bar{1}) \Leftrightarrow (\exists t \in \mathbb{Z}$ t.q. $t\bar{a} = \bar{1}) \Leftrightarrow (\forall k \in \mathbb{Z}, \exists z \in \mathbb{Z}$ t.q. $z\bar{a} = \bar{k}) \Leftrightarrow (\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z}, \exists z \in \mathbb{Z}$ t.q. $z\bar{a} = \bar{k}) \Leftrightarrow (\bar{a}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z})$.

Proposition I.12. — *Soit $n \in \mathbb{N}$, $n \geq 2$. Les conditions suivantes sont équivalentes :*

(i) *n est un nombre premier;*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre;*

(iii) *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Remarque I.13. — *Terminologie* : Pour p nombre *premier*, $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$. $\mathbb{F}_p$ est donc un *corps* fini, de cardinal p.

Preuve : • (iii) $\Rightarrow$ (ii) résulte de I.6.

• (ii) $\Rightarrow$ (i) Si n n'est pas premier, $n = ab$ où $1 < a, b < n$. Alors, dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{a}$ et $\bar{b}$ sont distincts de $\bar{0}$ et $\bar{0} = \bar{n} = \bar{a}\bar{b}$.

• (i) $\Rightarrow$ (iii) Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$, z un représentant de x. n ne divise pas z (sinon x serait nul), donc puisque n est premier, n est premier avec z. Donc, d'après la proposition précédente, $x = \bar{z} \in U(\mathbb{Z}/n\mathbb{Z})$.

Définition I.14 [Indicateur d'Euler]**. —** *Pour tout entier naturel $n \geq 1$, on note G_n l'ensemble des entiers naturels x tels que $(1 \leq x \leq n$ et $x \wedge n = 1)$.*

On définit l'application φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ appelée fonction indicatrice d'Euler par : $\forall n \in \mathbb{N}^*$, $\varphi(n) = card(G_n)$.

Propriétés I.15. — *$\varphi(1) = 1$. Si $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ (donc, par isomorphisme, $\varphi(n)$ est le nombre de générateurs de tout groupe cyclique d'ordre n); et $\varphi(n)$ est l'ordre du groupe $U(\mathbb{Z}/n\mathbb{Z})$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Proposition I.16. — *Soit p un nombre premier et $n \in \mathbb{N}^*$. On a :*

$$\boxed{\varphi(p^n) = p^n - p^{n-1}.}$$

Preuve : Comme p est premier, G_{p^n} est l'ensemble des entiers naturels x tels que ($1 \leq x \leq p^n$ et $x \wedge p = 1$); son complémentaire est l'ensemble des multiples de p compris entre 1 et p^n, c'est–à–dire l'ensemble des pd, d compris entre 1 et p^{n-1} : il a donc pour cardinal p^{n-1}.

Théorème I.17 [EULER]**. —** *Soit $n \geq 2$ un entier naturel. Soit a un entier relatif premier avec n. Alors $a^{\varphi(n)} \equiv 1\,[mod.\ n]$.*

Preuve : On considère l'élément $\bar{a}$ du groupe $U(\mathbb{Z}/n\mathbb{Z})$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. D'après le théorème de Lagrange, son ordre divise $\varphi(n)$. Donc $\bar{a}^{\varphi(n)} = \bar{1}$, soit $a^{\varphi(n)} \equiv 1\,[\text{mod. } n]$.

REMARQUE I.18. — Comme lorsque p est premier, $\varphi(p) = p - 1$, ce théorème est une généralisation du *petit théorème de FERMAT*, dont nous rappelons l'énoncé :
Soit p un nombre premier. Soit a un entier relatif non divisible par p. Alors $a^{p-1} \equiv 1\,[mod.\ p]$.

Théorème I.19 [des restes chinois]**. —** *Soient m et n deux entiers naturels ≥ 2, premiers entre eux. Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.*

Preuve : x étant un entier relatif, on note $r(x)$ [resp. $s(x)$] la classe de x dans $\mathbb{Z}/m\mathbb{Z}$ [resp. $\mathbb{Z}/n\mathbb{Z}$]. Si $x \equiv x'[\text{mod. } mn]$, soit si $x - x'$ est divisible par mn, alors $x - x'$ est divisible par m et par n, soit $r(x) = r(x')$ et $s(x) = s(x')$. Cela permet de définir l'application f de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ par :

$$\forall C \in \mathbb{Z}/mn\mathbb{Z},\ f(C) = (r(x), s(x)) \text{ où } x \text{ est } \textit{un} \text{ élément de } C.$$

Clairement f est un homomorphisme d'anneaux. Si $C \in \text{Ker}(f)$ et si k est un élément de C, alors k est divisible par m et par n, donc par leur P.P.C.M.; lequel P.P.C.M. est le produit mn puisque m et n sont premiers entre eux, donc $C = \bar{k} = \bar{0}$. Ainsi f est injective. Donc, l'ensemble de départ et l'ensemble d'arrivée étant finis de même cardinal, f est bijective. □

Corollaire I.20. — *Soient m et n deux entiers naturels supérieurs ou égaux à 2, premiers entre eux. Alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Preuve : Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, donc les groupes $U(\mathbb{Z}/mn\mathbb{Z})$ et $U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$ sont isomorphes, donc ont même ordre.

Proposition I.21. — *Soit $n \geq 2$ un entier naturel. Soit $n = {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k}$ (les p_i premiers distincts, les $\alpha_i \in \mathbb{N}^*$) une décomposition de n en produit de facteurs premiers. Alors :*

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).}$$

Preuve : Raisonner par récurrence sur le nombre k de facteurs et utiliser I.16 et I.20.

Lemme I.22. — *Soit $n \geq 2$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ possède, pour chaque diviseur d de n, un et un seul sous–groupe d'ordre d : ce sous–groupe est $< (n/d)\bar{1} >$, il est cyclique.*

Preuve : • *Existence :* Notons $n = kd$, et $G =< k\bar{1} >= \{zk\bar{1}, z \in \mathbb{Z}\}$. On a $dk\bar{1} = \bar{0}$, et pour chaque $i \in [\![1, d-1]\!]$, $ik\bar{1} \neq \bar{0}$ car $1 \leq ik \leq (d-1)k < n$. Donc $k\bar{1}$ est d'ordre d, et $G =< k\bar{1} >$ est cyclique d'ordre d.
• *Unicité :* Notons $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Soit G un sous–groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. $s^{-1}(G)$ est un sous–groupe de $\mathbb{Z}$, donc il existe $k \in \mathbb{N}$ tel que $s^{-1}(G) = k\mathbb{Z}$. $n \in s^{-1}(G) = k\mathbb{Z}$, donc k (est non nul et) divise n, donc $n\mathbb{Z} \subseteq k\mathbb{Z}$. Il vient $G = s(s^{-1}(G)) = k\mathbb{Z}/n\mathbb{Z} =< k\bar{1} >$, d'où l'unicité (d'où aussi (cf. partie "existence") le fait que $k = n/d$).

Proposition I.23 [Formule de Gauss]**. —** *Pour $n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.*

Preuve : Notons D_n l'ensemble des entiers naturels diviseurs de n ; et notons, pour $d \in D_n$, $\mathcal{G}_d$ *le* sous–groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ et E_d l'ensemble des générateurs de $\mathcal{G}_d$: d'après I.15, $\text{card}(E_d) = \varphi(d)$.
Si $d \neq d'$, les éléments de E_d étant d'ordre d et ceux de $E_{d'}$ d'ordre d', E_d et $E_{d'}$ sont disjoints. Soit $x \in \mathbb{Z}/n\mathbb{Z}$. Soit d l'ordre de x. D'après le théorème de Lagrange, $d \in D_n$. Vu le lemme, $< x >= \mathcal{G}_d$. Donc $x \in E_d$.
Ainsi les $E_d, d \in D_n$, forment une partition de $\mathbb{Z}/n\mathbb{Z}$. Donc

$$n = \sum_{d \in D_n} \text{card}(E_d) = \sum_{d \in D_n} \varphi(d).$$

Théorème I.24. — *Soit G un groupe fini d'ordre n, noté multiplicativement, d'élément neutre e, dans lequel pour chaque diviseur d de n, l'équation $x^d = e$, à l'inconnue $x \in G$, a au plus d solutions distinctes. Alors G est un groupe cyclique.*

Preuve : Pour d diviseur de n, notons $T_d = \{x \in G / x^d = e\}$, Ω_d l'ensemble des éléments d'ordre d de G et $\psi(d) = \text{card}(\Omega_d)$. Clairement $\Omega_d \subseteq T_d$.
• Supposons $\psi(d) \geq 1$. Soit $x \in \Omega_d$. Alors $x \in T_d$, par conséquent $< x > \subseteq T_d$ (car $< x >= \{x^i, 0 \leq i \leq d-1\}$ et $(x^i)^d = (x^d)^i = e^i = e$). Comme $d = \text{card}(< x >)$ et $\text{card}(T_d) \leq d$, il vient $< x >= T_d$. Donc T_d est un groupe cyclique d'ordre d. Il a donc exactement $\varphi(d)$ générateurs, c'est–à–dire $\varphi(d)$ éléments d'ordre d. Or $\Omega_d \subseteq T_d$. Donc $\psi(d) = \varphi(d)$. Ainsi :

(I) pour tout diviseur d de n, le nombre $\psi(d)$ d'éléments d'ordre d de G est 0 ou $\varphi(d)$.
• Or les Ω_d, d diviseur de n, forment une partition de G (car ils sont clairement disjoints, et il résulte du théorème de Lagrange que leur union recouvre G). Donc (II) $n = \sum_{d|n} \psi(d)$.
• De (I), (II) et de la formule de GAUSS $n = \sum_{d|n} \varphi(d)$ découle : pour tout diviseur d de n, le nombre $\psi(d)$ d'éléments de G d'ordre d est égal à $\varphi(d)$. En particulier $\psi(n) = \varphi(n) \geq 1$. Donc G est cyclique. □

1.3 Sous–corps

Proposition I.25 [et définition]**. —** *Soit k un corps. Soit P une partie de k. Les conditions suivantes sont équivalentes :*

(i) *P est non vide, est une partie stable (pour $+$ et $\times$) de k, et P muni des lois induites par celles de k est lui–même un corps;*

(ii) *P est un sous–anneau de k, $1 \in P$, et $(x \in P \Rightarrow x^{-1} \in P)$;*

(iii) *P est un sous–groupe de $(k, +)$ et $P^* = P \setminus \{0\}$ est un sous–groupe du groupe multiplicatif $(k^*, \times)$.*

On dit alors que P est un sous–corps de k.

EXEMPLES I.26. — $\mathbb{Q}$ est un sous–corps de $\mathbb{R}$, $\mathbb{R}$ est un sous–corps de $\mathbb{C}$.

Proposition I.27. — *Soit k un corps. Toute intersection de sous–corps de k est un sous–corps de k.*

Preuve : Soit $(F_i)_{i \in I}$ une famille de sous–corps de k. 0 et 1 appartiennent à chacun des F_i, donc à l'intersection F de tous les F_i. Donc F est non vide. Soit $(a, b) \in F^2$. Pour chaque $i \in I$, $(a, b) \in {F_i}^2$, donc $a + b \in F_i$ et $ab \in F_i$. Par conséquent $a + b$ et ab appartiennent à F. Soit $x \in F$ avec $x \neq 0$. Alors pour chaque $i \in I$, $x \in F_i \setminus \{0\}$, donc $x^{-1} \in F_i$. Donc $x^{-1} \in F$.

Proposition I.28 [et définition]**. —** *Soit k un corps. Soit T une partie de k. L'ensemble E des sous–corps de k qui contiennent T est non vide, et possède, au sens de l'inclusion, un élément minimum : ce minimum est appelé le sous–corps de k engendré par T.*

Preuve : E est non vide car $k \in E$. Clairement, l'intersection des éléments de E est le plus petit élément de E (au sens de $\subseteq$).

2. Caractéristique d'un anneau, d'un corps

2.1 La caractéristique. Ses propriétés

Définition I.29 [Caractéristique d'un anneau]**. —** *Soit A un anneau. Il existe un unique homomorphisme d'anneaux de $\mathbb{Z}$ dans A : l'application f définie par $(\forall n \in \mathbb{Z},\ f(n) = n1_A)$. $Ker(f)$ est un idéal de $\mathbb{Z}$; donc il existe un entier naturel c, et un seul, tel que $Ker(f) = c\mathbb{Z}$. Comme $f(1) = 1_A \neq 0$, c est distinct de 1. Ce nombre c est appelé la caractéristique de l'anneau A, et on note $c = caract(A)$.*

Remarques I.30. — **1)** $\mathrm{Im}(f) = \{z1_A, z \in \mathbb{Z}\} = \mathbb{Z}1_A$ est un sous–anneau de A (c'est d'ailleurs le sous–anneau engendré par 1_A) et la décomposition canonique de l'homomorphisme f montre que $\mathrm{Im}(f)$ est isomorphe à $\mathbb{Z}/c\mathbb{Z}$.
2) Si $\mathrm{caract}(A) \neq 0$, alors $\mathrm{caract}(A)$ est l'ordre additif de l'élément 1_A.
3) Un anneau et un quelconque de ses sous–anneaux (en particulier un corps et un quelconque de ses sous–corps) ont la même caractéristique.

Exemple I.31. — La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n.

Proposition I.32. — *Soit A un anneau fini. Alors $\mathrm{caract}(A) \neq 0$ et $\mathrm{caract}(A)$ divise le cardinal de A.*

Preuve : Si $\mathrm{caract}(A)$ était nulle, $\mathrm{Im}(f)$ serait isomorphe à $\mathbb{Z}$ donc infini : ce qui est absurde puisque $\mathrm{Im}(f)$ est inclus dans A fini. La seconde affirmation résulte du théorème de Lagrange et du fait que $\mathrm{caract}(A)$ est l'ordre additif de l'élément 1_A.

Proposition I.33. — *Soit A un anneau intègre. Alors $\mathrm{caract}(A)$ est ou bien nulle, ou bien un nombre premier.*

Preuve : Comme A est intègre, le sous–anneau $\mathrm{Im}(f)$ l'est aussi. Or $\mathrm{Im}(f)$ est isomorphe à $\mathbb{Z}/\,\mathrm{caract}(A)\mathbb{Z}$, donc $\mathbb{Z}/\,\mathrm{caract}(A)\mathbb{Z}$ est intègre. Donc $\mathrm{caract}(A)$ est 0 ou un nombre premier.

Corollaire I.34. — *Soit k un corps. Alors $\mathrm{caract}(k)$ est ou bien nulle, ou bien un nombre premier.*

Preuve : Un corps est un anneau intègre...

Proposition I.35. — *Soit p un nombre premier et A un anneau de caractéristique p. Alors :*

$$\forall (a,b) \in A^2,\ (a+b)^p = a^p + b^p.$$

Preuve : Soit $k \in [\![1, p-1]\!]$: alors aucun des naturels $1, 2, \ldots, k$ n'est divisible par p; donc, puisque p est premier, ils sont tous premiers avec p; donc leur produit $k!$ est premier avec p; or p divise $k!C_p^k = p(p-1)\ldots(p-k+1)$; donc (théorème de Gauss) p divise C_p^k. La formule du binôme de Newton $(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}$ donne alors le résultat annoncé.

2.2 Sous–corps premier d'un corps

Définition I.36 [Corps premier]**. —** *Un corps K est dit premier si, et seulement si, K n'a pas d'autre sous–corps que lui–même.*

Exemples I.37. — **1)** $\mathbb{Q}$ est un corps premier. En effet tout sous–corps de $\mathbb{Q}$ contient nécessairement le sous–corps de $\mathbb{Q}$ engendré par 1, qui n'est autre que $\mathbb{Q}$ lui–même.
2) Pour chaque $p \in \mathbb{P}$, $\mathbb{F}_p$ est un corps premier. En effet soit k un sous–corps de $\mathbb{F}_p$. k est en particulier un sous–groupe additif de $\mathbb{F}_p$, donc vus le théorème de

Lagrange et le fait que p admet 1 et p pour seuls diviseurs, k est égal à $\{\bar{0}\}$ ou à $\mathbb{F}_p$. Comme $\bar{1} \in k$, le premier cas est exclu.

Définition I.38. — *Soit K un corps. Notons P le sous–corps de K engendré par 1_K, c'est–à–dire l'intersection de tous les sous–corps de K. Le corps P est bien sûr un corps premier. On l'appelle le sous–corps premier de K.*

Remarques I.39. — 1) K est un corps premier si, et seulement si, $P = K$.
2) Un corps et l'un quelconque de ses sous–corps ont le même sous–corps premier.

Proposition I.40. — *Soit K un corps, P son sous–corps premier, et c sa caractéristique. On a :*

▷ *Ou bien $c = 0$ et alors P est isomorphe à $\mathbb{Q}$.*

▷ *Ou bien c est un nombre premier p et alors P est isomorphe à $\mathbb{F}_p$.*

Remarque I.41. — Dans tous les cas, que K soit ou non commutatif, P est commutatif.

Preuve : Reprenons l'unique homomorphisme d'anneaux de $\mathbb{Z}$ dans K, à savoir l'application $f : z \mapsto z1_K$. Deux cas se présentent :

▷ Si c est un nombre premier p, alors la décomposition canonique de l'homomorphisme f fournit un isomorphisme d'anneaux $\widetilde{f}$ de $\mathbb{F}_p$ dans $\mathrm{Im}(f)$. $\mathrm{Im}(f) = \widetilde{f}(\mathbb{F}_p)$ est donc un sous–corps de K, donc P est inclus dans (donc est un sous–corps de) $\mathrm{Im}(f)$. Mais $\mathrm{Im}(f)$, étant isomorphe à $\mathbb{F}_p$, est un corps premier, donc $P = \mathrm{Im}(f)$.

▷ Si $c = 0$, f est injectif. Donc f se prolonge de façon unique en un homomorphisme de corps $\mathcal{F}$ de $\mathbb{Q}$ dans K (cf. I.10 : $\forall r \in \mathbb{Q}$, si $r = z/d$, où $(z, d) \in \mathbb{Z} \times \mathbb{N}^*$, $\mathcal{F}(r) = (z1_K)(d1_K)^{-1}$). $\mathrm{Im}(\mathcal{F}) = \mathcal{F}(\mathbb{Q})$ est donc un sous–corps de K, donc P est inclus dans (donc est un sous–corps de) $\mathrm{Im}(\mathcal{F})$. Mais $\mathrm{Im}(\mathcal{F})$, étant isomorphe à $\mathbb{Q}$, est un corps premier, donc $P = \mathrm{Im}(\mathcal{F})$.

Proposition I.42. — *Soit p un nombre premier. Tout corps fini de cardinal p est isomorphe à $\mathbb{F}_p$.*

Preuve : Soit K un corps fini. Il résulte de I.32 et I.34 que c = caract(K) est un nombre premier qui divise card(K). Si card(K) $= p$ premier, il vient caract(K)= p. Appliquant I.40, on voit que P est isomorphe à $\mathbb{F}_p$. L'égalité des cardinaux montre que $P = K$. Donc K est isomorphe à $\mathbb{F}_p$.

3. Polynômes irréductibles

Définition I.43 [Polynôme irréductible]**. —** *Soit A un anneau. Un polynôme P de $A[X]$ est dit irréductible dans $A[X]$ si, et seulement si, son degré est supérieur ou égal à 1 et ses seuls diviseurs dans $A[X]$ sont les polynômes uP, où $u \in U(A)$, et les éléments de $U(A)$.*