Module d'algèbre « MDI223 » :
Arithmétique modulaire et théorie des corps finis
(pour le codage et la cryptographie)

Hugues RANDRIAM

Version provisoire, octobre 2009

Avertissement

Ce polycopié provisoire est formé de deux parties.

La première, en cours de rédaction, traite essentiellement de l'arithmétique modulaire. La seconde est l'ancien polycopé – encore inachevé – de la partie dédiée aux corps finis du cours qui allait devenir « MDI223 ».

Malgré leur caractère provisoire, ces textes sont bien avancés et couvrent environ les trois quarts de ce qui sera abordé en cours. Si le temps le permet, une version mise à jour sera distribuée prochainement (ou pas).

Les élèves désirant approfondir certains sujets sont invités à consulter les références suivantes, disponibles à la bibliothèque de l'école.

Couvrant à peu près tout le contenu du cours :

- Zémor Gilles. *Cours de cryptographie.* (7.25 ZEMO) chapitre 1
- Baldoni M. W., Ciliberto C., Piacentini Cattaneo G.M. *Elementary Number Theory, Cryptography and Codes.* (1.32 BALD) chapitres 3, 4, 5
- Tauvel Patrice. *Algèbre.* (1.3 TAUV) chapitres 6, 10, 14, 17
- Hungerford Thomas. *Abstract Algebra.* (1.3 HUNG) tout
- Koblitz Neal. *A Course in Number Theory and Cryptography.* (1.32 KOBL) chapitres 1 et 2
- Ireland K., Rosen M. *A Classical Introduction to Modern Number Theory.* (1.32 IREL) chapitres 1 à 7
- Yan Song Y. *Primality testing and integer factorization in public-key cryptography.* (1.3 YAN) chapitre 1

Plus spécifiquement sur l'arithmétique modulaire :

- Mollin Richard A. *Fundamental number theory with applications.* (1.3 MOLL) chapitres 1 à 4

Plus spécifiquement sur les corps finis :

- Zémor Gilles. Polycopié *Master CSI, Bordeaux, Arithmétique 1 : corps finis et applications.*
  `http://www.math.u-bordeaux.fr/~zemor/arit06.pdf`
- Lidl R., Niederreiter H. *Finite fields.* (1.36 LIDL) chapitres 1 à 4

- Lang Serge. *Algèbre*. (1.3 LANG) chapitre 5
- Calais Josette. *Extensions de corps et théorie de Galois*. (1.36 CALA) chapitres 1 à 4
- Koblitz Neal. *Algebraic Aspects of Cryptography*. (1.32 KOBL) chapitre 3

Première partie

Table des matières

Chapitre 1

Groupes abéliens

1.1 Relations d'équivalence, structures quotient

Définition 1.1.1. — Une relation $\mathcal{R}$ sur un ensemble E est la donnée d'une partie $\mathcal{R} \subset E \times E$.

Pour une meilleure lisibilité on écrira souvent

$$x\mathcal{R}y$$

pour signifier que

$$(x, y) \in \mathcal{R}$$

et on dira alors que « x est en relation avec y selon $\mathcal{R}$ ».

Définition 1.1.2. — Une relation $\mathcal{R}$ sur un ensemble E est dite :
- réflexive, si : $\forall x \in E \quad x\mathcal{R}x$
- symétrique, si : $\forall x, y \in E \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- transitive, si : $\forall x, y, z \in E \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$

et on dit que c'est une *relation d'équivalence* si ces trois conditions sont vérifiées.

Plutôt que « $\mathcal{R}$ », des notations courantes pour les relations d'équivalence sont « $\sim$ », ou encore « $\equiv$ ».

Exemple 1.1.3. — Soit $f : E \longrightarrow F$ une application entre deux ensembles. On définit une relation $\sim$ sur E par « $x \sim y$ si et seulement si $f(x) = f(y)$ ». Alors $\sim$ est une relation d'équivalence.

On verra plus loin que cet exemple est fondamental : toute relation d'équivalence peut s'obtenir par ce procédé.

Définition 1.1.4. — Soient $\sim$ une relation d'équivalence sur un ensemble E, et A une partie de E. On dira que A est une *classe d'équivalence* pour la relation $\sim$ si :
- A est non vide
- pour tous $x, y \in A$ on a $x \sim y$
- pour tous $x \in A$ et $y \notin A$ on a $x \not\sim y$.

On notera $E/\sim$ l'ensemble des classes d'équivalence pour $\sim$, appelé *ensemble quotient* de E par la relation $\sim$.

Ainsi on prendra garde qu'avec cette définition les éléments de $E/\sim$ sont des parties de E. [1]

On vérifie facilement que les classes d'équivalence forment une *partition* de E, c'est-à-dire qu'elles sont deux à deux disjointes et que leur réunion est E tout entier. Ainsi tout élément de E appartient à une et une seule classe d'équivalence.

Si A est une classe d'équivalence et si $x \in A$, on dira indifféremment que A est la classe de x (pour la relation $\sim$) ou que x est un *représentant* de A.

On dira qu'une partie S de E est un *système de représentants* si pour toute classe d'équivalence A il existe un et un seul $x \in S$ qui soit un représentant de A. Cela équivaut aussi à demander que tout élément de E soit équivalent à un élément de S, et à un seul.

Quelques notations courantes pour la classe d'un élément x sont : « x modulo $\sim$ » ou « $x \mod \sim$ », parfois $\mathrm{Cl}_\sim(x)$, ou plus simplement $[x]$ ou encore $\overline{x}$ s'il n'y a pas d'ambiguïté. On a donc formellement

$$\overline{x} = \{y \in E \mid x \sim y\}.$$

On dispose par ailleurs naturellement d'une application

$$\begin{array}{rccc} \pi : & E & \longrightarrow & E/\sim \\ & x & \mapsto & \overline{x} \end{array}$$

surjective, qui à tout élément de E associe sa classe d'équivalence. On dira que π est la *projection canonique* de E sur $E/\sim$. On a ainsi

$$x \sim y \iff \overline{x} = \overline{y} \iff \pi(x) = \pi(y).$$

On rapprochera cela de l'exemple 1.1.3.

Théorème 1.1.5. — *Soient E et F deux ensembles, $\sim$ une relation d'équivalence sur E, et $f : E \longrightarrow F$ une application. On a alors équivalence entre les deux assertions suivantes :*

[1] Ceci étant dit, on verra plus bas (remarque 1.1.7) que la nature précise des éléments de $E/\sim$ n'est pas une information essentielle.

1. *L'application f est compatible à $\sim$, c'est-à-dire :*

$$\forall x, y \in E, \quad x \sim y \implies f(x) = f(y).$$

2. *Il existe une application $g : E/\sim \longrightarrow F$ telle que f se factorise en*

$$f = g \circ \pi,$$

où $\pi : E \longrightarrow E/\sim$ est la projection canonique.

Si ces conditions sont vérifiées, cette application g est alors unique.

Définition 1.1.6. — Sous les hypothèses du théorème, on dit que g est l'application déduite de f par *passage au quotient* par la relation $\sim$. La construction de cette application g est détaillée ci-dessous dans la preuve du théorème.

Remarque 1.1.7. — La propriété de l'ensemble quotient (et de la projection canonique) mise en évidence dans ce théorème est importante conceptuellement en ce qu'elle constitue une « propriété universelle » qui caractérise complètement l'ensemble quotient : si on dispose d'un autre ensemble vérifiant cette même propriété, on disposera aussi automatiquement d'une bijection « naturelle » permettant d'identifier cet ensemble à l'ensemble quotient. Autrement dit, on aurait pu choisir une définition différente de l'ensemble quotient, la seule chose importante étant qu'il vérifie la propriété du théorème. D'ailleurs, la plupart du temps, dans la suite du texte, on n'utilisera pas la définition précise de l'ensemble quotient donnée au début de la section, mais uniquement le fait qu'il vérifie cette propriété.

Démonstration du théorème.

$1 \Rightarrow 2$. Pour tout $A \in E/\sim$ choisissons un représentant $x_A \in A$. Si l'on veut avoir $f = g \circ \pi$, il faut nécessairement qu'on ait

$$g(A) = g(\pi(x_A)) = f(x_A),$$

ce qui montre que si g existe, elle est unique. Définissons donc g au moyen de cette formule, et vérifions qu'on a bien $f = g \circ \pi$. En effet, considérons $y \in E$ arbitraire, et notons $A = \pi(y)$ sa classe d'équivalence. Puisque les éléments y et x_A appartiennent à la même classe, on a $y \sim x_A$, de sorte que la compatibilité de f à $\sim$ implique $f(y) = f(x_A)$. On a alors bien $f(y) = f(x_A) = g(A) = g(\pi(y))$, ce qu'il fallait montrer.

$2 \Rightarrow 1$. Supposons qu'on puisse écrire $f = g \circ \pi$, et considérons $x, y \in E$ tels que $x \sim y$, c'est-à-dire $\pi(x) = \pi(y)$. Alors on a bien $f(x) = g(\pi(x)) = g(\pi(y)) = f(y)$. □

Remarque 1.1.8. — On peut interpréter la partie $1 \Rightarrow 2$ de la preuve comme suit : on a construit g en faisant certains choix, et on a montré que g était « bien définie » en vérifiant que le résultat ne dépendait pas des choix faits. Cette technique sera utilisée à plusieurs reprises dans la suite du texte.

1.2 Généralités sur les groupes

Groupes et sous-groupes

Définition 1.2.1. — Un groupe $(G, *, e)$ (souvent abrégé en G tout court) est la donnée d'un ensemble non vide G, d'une loi de composition interne

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (x, y) & \mapsto & x * y \end{array}$$

et d'un élément $e \in G$ vérifiant les trois propriétés suivantes :

- la loi $*$ est associative : $\forall x, y, z \in G \quad (x * y) * z = x * (y * z)$
- e est neutre pour $*$: $\forall x \in G \quad e * x = x * e = x$
- tout élément est inversible : $\forall x \in G \quad \exists y \in G \quad x * y = y * x = e$ (et on montre alors facilement que cet inverse est unique).

On dit que ce groupe est *abélien* (ou commutatif) si en outre :

- la loi $*$ est commutative : $\forall x, y \in G \quad x * y = y * x$.

On note x^{-1} l'inverse de x, et $x^n = x * \cdots * x$ le composé de x avec lui-même n fois (pour $n \in \mathbb{N}$, puis pour $n \in \mathbb{Z}$ par passage à l'inverse). Parfois on écrira aussi xy pour $x * y$. On parle de « notation multiplicative ».

Une autre notation courante, pour les groupes *abéliens*, est la notation « additive » : $(G, +, 0)$. L'inverse de x est alors noté $-x$ et $nx = \underbrace{x + \cdots + x}_{n \text{ fois}}$.

Exemple 1.2.2. — 1. L'ensemble des permutations d'un ensemble E forme un groupe, avec pour loi la composition usuelle et pour neutre la permutation identité ; ce groupe n'est pas abélien dès que E a au moins trois éléments.

2. Le triplet $(\mathbb{Z}, +, 0)$ est un groupe abélien.
3. Le triplet $(\mathbb{R}, +, 0)$ est un groupe abélien.
4. Le triplet $(\mathbb{R}^\times, \times, 1)$ est un groupe abélien.
5. Si $(G_1, *_1, e_1)$ et $(G_2, *_2, e_2)$ sont deux groupes, le produit direct $G_1 \times G_2$ est un groupe pour la loi de composition interne $*$ définie par

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1,\ x_2 *_2 y_2),$$

de neutre (e_1, e_2) ; ce groupe est abélien si et seulement si G_1 et G_2 le sont.

Définition 1.2.3. — Soit $(G, *, e)$ un groupe. Un sous-ensemble H de G est appelé *sous-groupe* si :

– il contient l'élément neutre : $e \in H$
– il est stable par inverse : $\forall x \in H \quad x^{-1} \in H$
– il est stable par composition : $\forall x, y \in H \quad x * y \in H$.

On vérifie facilement alors que la restriction à H de la loi de G munit H d'une structure de groupe, qui en outre est abélien dès lors que G l'est.

Lemme 1.2.4. — *Si G est un groupe et si $(H_i)_{i\in I}$ est une famille quelconque de sous-groupes de G, leur intersection $H = \bigcap_{i\in I} H_i$ est encore un sous-groupe de G.*

Démonstration. On vérifie facilement que H contient l'élément neutre et est stable par inverse et par composition dès lors que c'est le cas pour chacun des H_i. □

Proposition 1.2.5. — *Soient G un groupe et S une partie quelconque de G. Notons $< S >$ la partie de G définie comme l'intersection de tous les sous-groupes de G qui contiennent S. Alors $< S >$ est un sous-groupe de G contenant S, et c'est le plus petit d'entre eux : tout sous-groupe de G contenant S contient aussi $< S >$.*

Définition 1.2.6. — Avec ces notations, on dira que $< S >$ est le *sous-groupe engendré* par S dans G.

Démonstration de la proposition. Par le lemme, $< S >$ est bien un sous-groupe de G. Tout le reste découle immédiatement de la construction. □

Ensemble quotient d'un groupe par un sous-groupe

Proposition 1.2.7. — *Soient G un groupe (dont la loi sera notée multiplicativement) et H un sous-groupe. On définit une relation $\sim$ sur G en posant $x \sim y$ si et seulement si $x^{-1}y \in H$. Alors $\sim$ est une relation d'équivalence.*

Démonstration. On vérifie aisément que :
– $\sim$ est réflexive car H contient l'élément neutre
– $\sim$ est symétrique car H est stable par inverse
– $\sim$ est transitive car H est stable par composition.

□

L'ensemble quotient $G/\sim$ est traditionnellement noté G/H, et la classe d'équivalence d'un élément x est

$$(x \bmod H) \;=\; xH \;=\; \{xh \mid h \in H\}.$$

On écrira aussi

$$x \equiv y \mod H$$

(ou même parfois : $x = y \mod H$) pour signifier $(x \bmod H) = (y \bmod H)$, c'est-à-dire $y \in xH$.

Bien sûr si on a affaire à un groupe abélien $(G, +, 0)$ dont la loi est notée additivement, les classes d'équivalence s'écrivent alors

$$(x \bmod H) \;=\; x + H \;=\; \{x + h \mid h \in H\}$$

et on a $x \equiv y \mod H$ si et seulement si $x - y \in H$.

Définition 1.2.8. — Si H est un sous-groupe d'un groupe G, on définit l'*indice* de H dans G, noté $[G : H]$, comme le cardinal (éventuellement infini) de l'ensemble quotient G/H :

$$[G : H] = |G/H| \,.$$

Exemple 1.2.9. — 1. Si N est un entier strictement positif,

$$N\mathbb{Z} = \{Nk \mid k \in \mathbb{Z}\}$$

est un sous-groupe d'indice N dans $(\mathbb{Z}, +, 0)$. Les éléments l'ensemble quotient $\mathbb{Z}/N\mathbb{Z}$ sont les classes $\overline{0} = N\mathbb{Z}$, $\overline{1} = 1 + N\mathbb{Z}$, …, $\overline{N-1} = N - 1 + N\mathbb{Z}$. [2]

2. De même $\mathbb{R}_+^\times$ est un sous-groupe d'indice 2 dans $(\mathbb{R}^\times, \times, 1)$.

Proposition 1.2.10. — *Soit G un groupe* fini. *Alors tout sous-groupe H de G est fini et d'indice fini, et on a*

$$|G| = |H| \times [G : H]$$

ou, ce qui revient au même : $|G/H| = |G|/|H|$.

On en retiendra en particulier que *l'ordre d'un sous-groupe divise l'ordre du groupe.*

Démonstration. Pour chaque classe $A \in G/H$ choisissons un représentant x_A. Définissons alors une application

$$\begin{array}{rccc} \varphi : & (G/H) \times H & \longrightarrow & G \\ & (A, h) & \mapsto & x_A h \end{array}$$

et montrons que cette application φ est bijective, ce qui achèvera la preuve. Or en effet :

[2] Dans certains problèmes, il pourra parfois être utile de choisir un autre système de représentants. Par exemple, on peut aussi décrire les éléments de $\mathbb{Z}/N\mathbb{Z}$ comme les classes $\overline{-(m-1)}, \overline{-(m-2)}, \ldots, \overline{m-1}, \overline{m}$ pour $N = 2m$ pair, ou comme les classes $\overline{-m}, \overline{-(m-1)}, \ldots, \overline{m-1}, \overline{m}$ pour $N = 2m+1$ impair.

- φ est injective, car si on a $\varphi(A,h) = \varphi(A',h')$, c'est-à-dire $x_A h = x_{A'} h'$, on en déduit ${x_A}^{-1} x_{A'} = h{h'}^{-1} \in H$ donc, $x_A \sim x_{A'}$, $A = A'$, d'où $x_A = x_{A'}$ et aussi finalement $h = h'$;
- φ est surjective, car si $x \in G$ est arbitraire, en notant A la classe de x modulo H, on a $x \sim x_A$ et donc x peut s'écrire $x = x_A h$ pour un certain $h \in H$.

□

Pour une seconde preuve de la proposition, voir l'exercice 1.5.2.

Morphismes

Définition 1.2.11. — Un *(homo)morphisme* d'un groupe $(G, *, e)$ dans un groupe $(G', *', e')$ est une application $f : G \longrightarrow G'$ qui « respecte les structures », en ce sens que :

- $f(e) = e'$
- pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$
- pour tous $x, y \in G$, $f(x * y) = f(x) *' f(y)$.

Un morphisme d'un groupe dans lui-même est appelé *endomorphisme* ; un morphisme bijectif est appelé *isomorphisme* (alors son inverse est aussi un morphisme) ; un morphisme qui est à la fois un endomorphisme et un isomorphisme est appelé *automorphisme*.

Les trois conditions données ci-dessus dans la définition d'un morphisme sont redondantes : en fait la troisième implique les deux premières (exercice 1.5.3).

Exemple 1.2.12. — L'exponentielle (réelle, en n'importe quelle base) est un isomorphisme de $(\mathbb{R}, +, 0)$ sur $(\mathbb{R}_+^\times, \times, 1)$.

Proposition 1.2.13. — *Soit $f : (G, *, e) \longrightarrow (G', *', e')$ un morphisme entre deux groupes. Alors :*

1. *Si H' est un sous-groupe de G', l'ensemble*

$$f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$$

est un sous-groupe de G.

2. *Si H est un sous-groupe de G, l'ensemble*

$$f(H) = \{g' \in G' \mid \exists g \in H,\ g' = f(g)\}$$

est un sous-groupe de G'.

Démonstration. 1. Il s'agit de vérifier que $f^{-1}(H')$ contient e et est stable par inverse et par composition. La preuve est immédiate :
- on a $f(e) = e' \in H'$, donc $e \in f^{-1}(H')$
- si $x \in f^{-1}(H')$, on a $f(x) \in H'$, d'où $f(x^{-1}) = f(x)^{-1} \in H'$, et donc $x^{-1} \in f^{-1}(H')$
- si $x, y \in f^{-1}(H')$, on a $f(x) \in H'$ et $f(y) \in H'$, d'où $f(x * y) = f(x) *' f(y) \in H'$, et donc $x * y \in f^{-1}(H')$,

ce qu'il fallait démontrer.

2. Il s'agit de vérifier que $f(H)$ contient e' et est stable par inverse et par composition, ce qui est tout aussi immédiat que précédemment. □

Deux cas particuliers importants où la proposition s'applique sont ceux où $H' = \{e'\}$, et $H = G$:

Définition 1.2.14. — Soit $f : (G, *, e) \longrightarrow (G', *', e')$ un morphisme entre deux groupes. Alors :

1. L'ensemble
$$\ker f = f^{-1}(e') = \{g \in G \mid f(g) = e'\}$$
est un sous-groupe de G, appelé *noyau* de f.
2. De même, l'*image* de f
$$\operatorname{im} f = f(G) = \{g' \in G' \mid \exists g \in G,\ g' = f(g)\}$$
est un sous-groupe de G'.

Exemple 1.2.15. — L'exponentielle (complexe) est un morphisme surjectif de $(\mathbb{C}, +, 0)$ sur $(\mathbb{C}^\times, \times, 1)$, de noyau $2i\pi\mathbb{Z}$.

Proposition 1.2.16. — *Un morphisme $f : (G, *, e) \longrightarrow (G', *', e')$ entre deux groupes est injectif si et seulement si* $\ker f = \{e\}$.

Démonstration. Supposons f injectif. Alors $\ker f = f^{-1}(e')$ est soit vide soit réduit à un singleton. Mais on a $e \in \ker f$, donc $\ker f = \{e\}$. Réciproquement supposons $\ker f = \{e\}$ et considérons un élément arbitraire g' de G'. Alors si $g_1, g_2 \in f^{-1}(g')$ on a $f(g_1) = f(g_2)$ donc $f(g_1 * (g_2)^{-1}) = e'$, autrement dit $g_1 * (g_2)^{-1} \in \ker f = \{e\}$. Ainsi $g_1 * (g_2)^{-1} = e$, et $g_1 = g_2$. □

Groupe quotient d'un groupe abélien par un sous-groupe

Lemme 1.2.17. — *Soient $(G, +, 0)$ un groupe abélien et H un sous-groupe. Alors si A et B sont deux classes modulo H, les éléments du type $a + b$ pour $a \in A$ et $b \in B$ sont tous dans la même classe modulo H.*

Démonstration. En effet, si $a, a' \in A$ et $b, b' \in B$, on a $a'-a \in H$ et $b'-b \in H$ et donc, G étant abélien,

$$(a'+b')-(a+b) = (a'-a)+(b'-b) \in H.$$

□

Ceci permet de construire une loi de composition interne sur G/H, loi que l'on notera aussi « + », en définissant $A+B$ comme la classe commune de ces éléments. Ainsi si on écrit $A = a+H$ et $B = b+H$ on a

$$(a+H) \ + \ (b+H) \ = \ (a+b)+H$$

ou, de façon plus concise,

$$\overline{a}+\overline{b} = \overline{a+b}\ .\ ^{3}$$

On montre facilement que la loi ainsi construite munit G/H d'une structure de groupe *abélien* :

- l'associativité et la commutativité découlent directement de celles de la loi de G
- le neutre est la classe de 0
- pour l'inverse, on a $-\overline{a} = \overline{-a}$.

Définition 1.2.18. — L'ensemble quotient G/H muni de cette loi est appelé *groupe quotient* de G par H.

Remarque 1.2.19. — La construction de la loi du groupe quotient repose sur le lemme 1.2.17, qui suppose G abélien. Si l'on supprime cette hypothèse, la conclusion du lemme n'est plus forcément vérifiée Ainsi en général G/H peut toujours être défini en tant qu'ensemble quotient, mais pas en tant que groupe (en tout cas, pas de façon « naturelle »). Toutefois les choses fonctionnent à nouveau si on fait une hypothèse supplémentaire sur H, celle d'être un sous-groupe *distingué* (ou *normal*). Dans un groupe abélien, tous les sous-groupes sont distingués (la réciproque n'est pas vraie). Nous ne ferons pas appel à cette notion dans la suite du cours.

Proposition 1.2.20. — *Si G est un groupe abélien et H un sous-groupe, la projection canonique $\pi : G \longrightarrow G/H$ est un morphisme de groupes, surjectif, et de noyau H.*

Démonstration. Cela résulte directement des constructions. □

Théorème 1.2.21. — *Soient $(G, +, 0)$ un groupe abélien et H un sous-groupe. Alors les sous-groupes de G/H sont naturellement en bijection avec les sous-groupes de G contenant H.*

[3] *Exercice de lecture :* dans cette formule, pour chaque symbole « + », identifier s'il s'agit de l'addition de G ou de celle de G/H.

De façon plus précise, notons $\mathcal{A}$ l'ensemble des sous-groupes de G/H et $\mathcal{B}$ l'ensemble des sous-groupes de G contenant H. Pour $A \in \mathcal{A}$ posons

$$\Phi(A) = \pi^{-1}(A) = \{x \in G \mid x + H \in A\}$$

et pour $B \in \mathcal{B}$ posons

$$\Psi(B) = \pi(B) = \{y + H \mid y \in B\} = B/H$$

où $\pi : G \longrightarrow G/H$ est la projection canonique. Alors Φ envoie $\mathcal{A}$ dans $\mathcal{B}$, Ψ envoie $\mathcal{B}$ dans $\mathcal{A}$, et ces deux applications sont des bijections inverses l'une de l'autre.

Démonstration. Toutes les vérifications sont immédiates, montrons par exemple que $\Phi(\Psi(B)) = B$ pour tout $B \in \mathcal{B}$. En effet on a $x \in \Phi(\Psi(B)))$ si et seulement si $x + H \in \Psi(B)$, ce qui équivaut à demander qu'il existe $y \in B$ tel que $x + H = y + H$; mais puisque B contient H, cela équivaut encore à demander $x \in B$. □

Morphisme défini par passage au quotient

Théorème 1.2.22 (de factorisation)**.** — *Soient $f : G \longrightarrow G'$ un morphisme de groupes abéliens, H un sous-groupe de G, et $\pi : G \longrightarrow G/H$ la projection canonique. Alors les deux assertions suivantes sont équivalentes :*

- $\ker(f)$ *contient* H
- *il existe un morphisme $g : G/H \longrightarrow G'$ tel que f se factorise en*

$$f = g \circ \pi.$$

Lorsque c'est le cas, ce morphisme g est unique, et on dit qu'il se déduit de f par passage au quotient par H. De plus, on a alors $\operatorname{im} g = \operatorname{im} f$ *et* $\ker g = \ker f/H$.

Démonstration. On vérifie facilement que la condition $\ker f \supset H$ équivaut à demander que $f(x) = f(y)$ si $x \equiv y \mod H$. L'existence et l'unicité d'une application g donnant la factorisation est alors assurée par le théorème 1.1.5, et on vérifie sans peine qu'il s'agit bien d'un morphisme. La condition $f = g \circ \pi$ implique $\operatorname{im} f \subset \operatorname{im} g$, et comme π est surjective on a même $\operatorname{im} f = img$. Enfin on a $\overline{x} \in \ker g$ si et seulement si pour tout représentant x de $\overline{x}$ on a $f(x) = g(\overline{x}) = e'$, autrement dit $x \in \ker f$, et $\overline{x} \in \ker f/H$. □

Corollaire 1.2.23. — *Si $f : G \longrightarrow G'$ est un morphisme de groupes abéliens, f induit par passage au quotient un isomorphisme*

$$G/\ker f \xrightarrow{\sim} \operatorname{im} f.$$

En particulier si G est fini, on a

$$|G| = |\ker f| \times |\operatorname{im} f|.$$

Démonstration. On applique le théorème avec $H = \ker f$. □

Exemple 1.2.24. — L'exponentielle complexe induit par passage au quotient un isomorphisme

$$\mathbb{C}/2i\pi\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times.$$

Sous-groupes monogènes, ordre d'un élément

Définition 1.2.25. — Si x est un élément d'un groupe G (dont la loi sera notée multiplicativement), on définit l'*ordre* de x, noté $\omega(x)$, comme le plus petit entier $n > 0$ tel que $x^n = e$ si un tel entier existe, et $+\infty$ sinon.

(Pour un groupe abélien en notation additive, cela devient : le plus petit entier $n > 0$ tel que $nx = 0$.)

Lemme 1.2.26. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes* injectif *(par exemple, un isomorphisme). Alors pour tout $x \in G$, on a $\omega(f(x)) = \omega(x)$.*

Démonstration. Puisque f est injectif, pour tout entier n on a $f(x)^n = f(x^n) = e'$ si et seulement si $x^n = e$. □

Lemme 1.2.27. — *Soient G un groupe (de loi notée multiplicativement) et $x \in G$ un élément d'ordre $\omega(x)$ fini. Alors pour tout diviseur d de $\omega(x)$ on a*

$$\omega(x^d) = \frac{\omega(x)}{d}.$$

(Pour G abélien en notation additive, cela devient : $\omega(d.x) = \frac{\omega(x)}{d}$.)

Démonstration. On a $(x^d)^{\frac{\omega(x)}{d}} = x^{\omega(x)} = e$, et si $n > 0$ vérifie $n < \frac{\omega(x)}{d}$, on a $dn < \omega(x)$ donc $(x^d)^n = x^{dn} \neq e$. □

Lemme 1.2.28. — *Soit G un groupe (dont la loi sera notée multiplicativement). Alors, pour tout élément x de G, il existe un unique morphisme de groupes de $\mathbb{Z}$ dans G envoyant 1 sur x. Ce morphisme est l'application*

$$\begin{array}{rccc} f_x : & \mathbb{Z} & \longrightarrow & G \\ & k & \mapsto & x^k \end{array}$$

et son image est $< x >$, le sous-groupe de G engendré par x.

On dit parfois que f_x est l'« exponentielle de base x ».

(Dans le cas où G est abélien de loi notée additivement, tout cela reste valable en prenant pour définition de $f_x : k \mapsto kx$.)

Démonstration. Si $f : \mathbb{Z} \longrightarrow G$ est un morphisme de groupes envoyant 1 sur x, une récurrence immédiate donne $f(k) = x^k$ pour tout $k \in \mathbb{N}$, puis par compatibilité à l'inverse, $f(k) = x^k$ pour tout $k \in \mathbb{Z}$, d'où l'unicité.

On vérifie alors facilement que l'application f_x ainsi définie est un morphisme. On en déduit que $\operatorname{im} f_x = \{x^k | k \in \mathbb{Z}\}$ est un sous-groupe de G, qui par ailleurs contient x, et donc contient $< x >$ par minimalité de celui-ci.

Inversement, appliquant ce qu'on vient de démontrer en remplaçant G par $< x >$, on trouve qu'il existe un unique morphisme $f'_x : \mathbb{Z} \longrightarrow < x >$ envoyant 1 sur x. Alors si $\iota : < x > \longrightarrow G$ est le morphisme naturel d'inclusion, la composée $\iota \circ f'_x$ est un morphisme de $\mathbb{Z}$ dans G envoyant 1 sur x. Par unicité on en déduit $f_x = \iota \circ f'_x$, donc $\operatorname{im} f_x \subset \operatorname{im} \iota =< x >$. □

On rappelle que $(\mathbb{Z}, +, 0)$ est un groupe abélien et que si N est un entier strictement positif, $N\mathbb{Z}$ en est un sous-groupe, d'indice N. Réciproquement :

Lemme 1.2.29. — *Tout sous-groupe non nul H de $(\mathbb{Z}, +, 0)$ est de la forme*

$$H = N\mathbb{Z}$$

où N est un entier strictement positif uniquement déterminé par H comme suit :

- *N est le plus petit élément strictement positif de H*
- *N est égal à l'indice $[\mathbb{Z} : H]$ de H dans $\mathbb{Z}$.*

Démonstration. Puisque H est non nul, H contient un élément non nul n, et en tant que sous-groupe contient donc aussi $-n$; l'un parmi n et $-n$ est strictement positif, de sorte que H contient au moins un élément strictement positif. Notant N le plus petit d'entre eux, H contient alors aussi le sous-groupe (additif) qu'il engendre : $< N > = N\mathbb{Z} \subset H$.

Réciproquement, soit n un élément arbitraire de H, et par division euclidienne écrivons $n = qN + r$ avec $0 \leqslant r < N$. Alors $n \in H$ et $qN \in H$ impliquent $r \in H$, et par minimalité de N on a $r = 0$. Ainsi $H \subset N\mathbb{Z}$. □

Proposition 1.2.30. — *Soient G un groupe et x un élément de G. Alors :*

1. *Si x est d'ordre infini, le morphisme f_x est injectif, donc définit un isomorphisme sur son image :*

$$f_x : \mathbb{Z} \xrightarrow{\sim} < x > .$$

2. Si x est d'ordre $\omega(x)$ fini, le morphisme f_x a pour noyau

$$\ker f_x = \omega(x)\mathbb{Z}$$

et induit par passage au quotient un isomorphisme

$$\begin{array}{rccc} \overline{f_x}: & \mathbb{Z}/\omega(x)\mathbb{Z} & \xrightarrow{\sim} & < x > \\ & (k \mod \omega(x)) & \mapsto & x^k. \end{array}$$

Démonstration. Par définition, l'ensemble des entiers relatis $n \in \mathbb{Z}$ tels que $x^n = e$ est le noyau de f_x, c'est donc un sous-groupe de $\mathbb{Z}$. Par le lemme 1.2.29, ou bien ce sous-groupe est nul, auquel cas f_x est injectif (proposition 1.2.16), ou bien ce sous-groupe est de la forme $N\mathbb{Z}$ où N est son plus petit élément strictement positif, ce qui permet de conclure. □

Corollaire 1.2.31. — *Si x est un élément d'un groupe G, le cardinal du sous-groupe $< x >$ est égal à l'ordre de x, fini ou infini :*

$$| < x > | = \omega(x).$$

Si de plus x est d'ordre fini, la liste des éléments de $< x >$ est donnée par

$$< x > = \{e, x, x^2, \ldots, x^{\omega(x)-1}\},$$

deux à deux distincts. [4]

Démonstration. Cela se lit immédiatement sur les isomorphismes donnés par la proposition. □

Corollaire 1.2.32. — *Soient G un groupe et $x \in G$ un élément d'ordre fini. Alors si $n \in \mathbb{Z}$ est un entier, on a $x^n = e$ si et seulement si $\omega(x)|n$.* [5]

Démonstration. C'est une reformulation de l'assertion $\ker f_x = \omega(x)\mathbb{Z}$ de la proposition. □

Théorème 1.2.33 (Lagrange)**.** — *Soit G un groupe fini. Alors tout élément $x \in G$ vérifie*

$$x^{|G|} = e$$

et $\omega(x)$ divise $|G|$.

Démonstration. Par le corollaire 1.2.31, le sous-groupe $H = < x >$ est de cardinal $\omega(x)$, et $|H|$ divise $|G|$ par la proposition 1.2.10. On conclut au moyen du corollaire 1.2.32. □

Dans le cas où G est *abélien*, une seconde preuve du théorème est proposée dans l'exercice 1.5.9.

[4] Pour G abélien en notation additive, cela devient : $< x >= \{0, x, 2x, \ldots, (\omega(x)-1)x\}$.

[5] Pour G abélien en notation additive, cela devient : $nx = 0$ si et seulement si $\omega(x)|n$.

1.3 Groupes cycliques et fonction indicatrice d'Euler

Groupes cycliques

Proposition 1.3.1. — *Soit $(G, *, e)$ un groupe fini. Notons $N = |G|$ son ordre. Alors si g_0 est un élément de G, les assertions suivantes sont équivalentes :*

1. *L'élément g_0 est d'ordre N.*
2. *On a $G = < g_0 >$.*
3. *Il existe un isomorphisme $\varphi : \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} G$ qui envoie la classe de 1 sur g_0.*
4. *Tout élément $g \in G$ peut s'écrire $g = (g_0)^n$ pour un certain $n \in \mathbb{N}$.*

Définition 1.3.2. — Un groupe fini G dans lequel il existe un élément g_0 vérifiant ces assertions est appelé groupe *cyclique* (d'ordre N). On dit alors aussi que g_0 est un *générateur* de G.

Remarque 1.3.3. — Il arrive parfois qu'un groupe isomorphe à $(\mathbb{Z}, +, 0)$ soit aussi qualifié de groupe cyclique (infini). Dans ce cours cependant, nous n'utiliserons cette terminologie que pour des groupes finis.

Démonstration de la proposition.

$1 \Leftrightarrow 2$. On a $< g_0 > \subset G$, avec égalité $< g_0 > = G$ si et seulement si il y a égalité des cardinaux $| < g_0 > | = |G|$, et on conclut au moyen du corollaire 1.2.31.

(1 et 2) $\Rightarrow 3$. On prend pour φ l'isomorphisme $\overline{f_{g_0}}$ donné par le point 2. de la proposition 1.2.30.

$3 \Rightarrow 1$. L'élément $\overline{1}$ de $\mathbb{Z}/N\mathbb{Z}$ est d'ordre N (pour l'addition), de sorte que par le lemme 1.2.26 l'élément $g_0 = \varphi(\overline{1}) \in G$ est aussi d'ordre N (pour la loi $*$).

$3 \Rightarrow 4$. Soit $\varphi : \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} G$ un isomorphisme tel que $\varphi(\overline{1}) = g_0$. Alors tout $g \in G$ peut s'écrire $g = \varphi(\overline{n})$ pour un certain $\overline{n} \in \mathbb{Z}/N\mathbb{Z}$, et si $n \in \mathbb{N}$ est un représentant de $\overline{n}$, on a bien $g = \varphi(\overline{n}) = \varphi(n.\overline{1}) = \varphi(\overline{1})^n = (g_0)^n$.

$4 \Rightarrow 2$. L'assertion 4. implique $G \subset < g_0 >$, et l'inclusion inverse est triviale.

□

Proposition 1.3.4. — *Soit N un entier strictement positif. Notons*

$$\mathbb{Z}/N\mathbb{Z} = \{ \overline{0}, \overline{1}, \ldots, \overline{N-1} \}.$$

Alors :

1. *Si d est un diviseur de N, le sous-ensemble*

$$d\mathbb{Z}/N\mathbb{Z} = \left\{ \overline{0}\,,\, \overline{d}\,,\, \overline{2d}\,,\, \ldots\,,\, \overline{\left(\tfrac{N}{d}-1\right)d} \right\}$$

est un sous-groupe de $\mathbb{Z}/N\mathbb{Z}$.
Inversement, tout sous-groupe de $\mathbb{Z}/N\mathbb{Z}$ est de cette forme pour un entier d divisant N uniquement déterminé. Cette construction met donc en bijection les sous-groupes de $\mathbb{Z}/N\mathbb{Z}$ et les diviseurs de N.
De plus, si d_1 et d_2 sont deux diviseurs de N, on a $d_1\mathbb{Z}/N\mathbb{Z} \supset d_2\mathbb{Z}/N\mathbb{Z}$ si et seulement si $d_1|d_2$.

2. *Le sous-groupe $d\mathbb{Z}/N\mathbb{Z}$ est cyclique, d'ordre*

$$|d\mathbb{Z}/N\mathbb{Z}| = \frac{N}{d}$$

et d'indice

$$[\mathbb{Z}/N\mathbb{Z} : d\mathbb{Z}/N\mathbb{Z}] = d.$$

3. *Les éléments de $d\mathbb{Z}/N\mathbb{Z}$ sont les éléments de $\mathbb{Z}/N\mathbb{Z}$ dont l'ordre (pour l'addition) divise $\frac{N}{d}$.*

4. *Si $x \in \mathbb{Z}$ est un entier relatif et si $\overline{x}$ est la classe de x modulo N, le sous-groupe (additif) de $\mathbb{Z}/N\mathbb{Z}$ engendré par $\overline{x}$ est*

$$< \overline{x} > = d\mathbb{Z}/N\mathbb{Z}$$

où

$$d = \mathrm{pgcd}(x, N).$$

Alors $\overline{x}$ est d'ordre (pour l'addition) exactement $\frac{N}{d}$.
En particulier, $\overline{x}$ est un générateur de $\mathbb{Z}/N\mathbb{Z}$ si et seulement si N et x sont premiers entre eux.

Démonstration. 1. Le théorème 1.2.21 montre que tout sous-groupe de $\mathbb{Z}/N\mathbb{Z}$ est de la forme $B/N\mathbb{Z}$, où B est un sous-groupe de $\mathbb{Z}$ contenant $N\mathbb{Z}$ uniquement déterminé. Par le lemme 1.2.29, B est de la forme $d\mathbb{Z}$, et B contient $N\mathbb{Z}$ si et seulement si d divise N. Enfin, on a $d_1\mathbb{Z}/N\mathbb{Z} \supset d_2\mathbb{Z}/N\mathbb{Z}$ si et seulement si $d_1\mathbb{Z} \supset d_2\mathbb{Z}$, ce qui équivaut à $d_1|d_2$.

2. On vérifie facilement que l'application

$$\begin{array}{ccc} \mathbb{Z}/\frac{N}{d}\mathbb{Z} & \longrightarrow & d\mathbb{Z}/N\mathbb{Z} \\ (k \bmod \frac{N}{d}) & \mapsto & (kd \bmod N) \end{array}$$

est un isomorphisme de groupes, de sorte que $d\mathbb{Z}/N\mathbb{Z}$ est bien cyclique d'ordre $\frac{N}{d}$ et donc d'indice d dans $\mathbb{Z}/N\mathbb{Z}$.

3. Par le point précédent et par le thórème de Lagrange, tout élément de $d\mathbb{Z}/N\mathbb{Z}$ est d'ordre divisant $\frac{N}{d}$. Inversement, si $\overline{x} \in \mathbb{Z}/N\mathbb{Z}$ est d'ordre divisant $\frac{N}{d}$, et si $x \in \mathbb{Z}$ est un représentant de $\overline{x}$, on a $\frac{N}{d}\overline{x} = \overline{0}$ donc $\frac{N}{d}x \in N\mathbb{Z}$, d'où $x \in d\mathbb{Z}$ et $\overline{x} \in d\mathbb{Z}/N\mathbb{Z}$.

4. Notons $d = \text{pgcd}(x, N)$. On sait qu'on a $< \overline{x} >= d'\mathbb{Z}/N\mathbb{Z}$ pour un certain entier d' divisant N, il s'agit de montrer $d' = d$. On a par hypothèse $\overline{x} \in d'\mathbb{Z}/N\mathbb{Z}$, donc $x \in d'\mathbb{Z}$, donc $d'|x$, et par ailleurs $d'|N$; ceci implique $d'|d$. Réciproquement d est un diviseur de N vérifiant $x \in d\mathbb{Z}$, de sorte que $\overline{x} \in d\mathbb{Z}/N\mathbb{Z}$, donc $d'\mathbb{Z}/N\mathbb{Z} =< \overline{x} > \subset d\mathbb{Z}/N\mathbb{Z}$, ce qui implique $d|d'$ par le point 1. □

On déduit facilement du dernier point de la proposition le théorème de Bézout dans $\mathbb{Z}$:

Corollaire 1.3.5 (Bézout)**.** — *Soient $a, b \in \mathbb{Z}$ non tous les deux nuls. Alors il existe $m, n \in \mathbb{Z}$ tels que*

$$ma + nb = \text{pgcd}(a, b).$$

Démonstration. Supposons par exemple $b \neq 0$, et appliquons le point 3. de la proposition avec $N = |b|$ et $x = a$. On a donc $< \overline{x} >= d\mathbb{Z}/N\mathbb{Z} = \left\{ \overline{0}, \overline{d}, \overline{2d}, \ldots, \overline{\left(\frac{N}{d} - 1\right) d} \right\}$ avec $d = \text{pgcd}(x, N) = \text{pgcd}(a, b)$. Par ailleurs on a aussi $< \overline{x} >= \left\{ \overline{0}, \overline{x}, 2\overline{x}, \ldots, \left(\frac{N}{d} - 1\right) \overline{x} \right\}$ (par le corollaire 1.2.31, en notation additive) de sorte qu'il existe un entier $m \in \mathbb{Z}$ (on peut même imposer $m \in \left\{0, 1, \ldots, \frac{N}{d} - 1\right\}$). tel qu'on ait $\overline{d} = m\overline{x}$, autrement dit, $d \in mx + N\mathbb{Z}$, ce qui donne bien la relation souhaitée. □

Remarque 1.3.6. — Puisqu'un isomorphisme préserve sous-groupes, indice, ordre, etc., et puisque par définition un groupe cyclique est isomorphe à un certain $\mathbb{Z}/N\mathbb{Z}$, la proposition 1.3.4 s'étend facilement à n'importe quel groupe cyclique. Par exemple, en notation multiplicative, si $(G, *, e)$ est un groupe cyclique d'ordre $|G| = N$, on trouve :

1. Si d est un diviseur de N, l'ensemble H_d formé des éléments de G qui sont des puissances d-ièmes est un sous-groupe de G ; cette construction met en bijection les diviseurs de N et les sous-groupes de G, et cette bijection est décroissante (si on ordonne les diviseurs de N par la relation de divisibilité, et les sous-groupes de G par la relation d'inclusion).
2. Le sous-groupe H_d est cyclique d'ordre $\frac{N}{d}$, et d'indice d dans G.
   Ainsi la bijection inverse de la bijection construite au point précédent associe à tout sous-groupe son indice.
3. Pour $x \in G$, on a $x \in H_d$ si et seulement si $x^{\frac{N}{d}} = e$.

4. Si g_0 est un générateur de G et si $g \in G$ s'écrit $g = (g_0)^k$ pour $k \in \mathbb{Z}$, alors $< g >= H_d$ pour $d = \text{pgcd}(N, k)$, et $\omega(g) = \frac{N}{d}$.
   En particulier, g est un générateur de G si et seulement si k est premier avec N.

On en déduit notamment :

Corollaire 1.3.7. — *Soit $(G, *, e)$ groupe cyclique d'ordre $|G| = N$. Alors pour tous y dans G et d diviseur de N on a l'équivalence :*

$$\exists x \in G \quad y = x^d \qquad \Leftrightarrow \qquad y^{\frac{N}{d}} = e.$$

Démonstration. En effet, avec les notations de la remarque, ces conditions sont équivalentes à demander $y \in H_d$. □

Corollaire 1.3.8. — *Avec les mêmes notations, pour $k \in \mathbb{N}_{>0}$, on a l'équivalence :*

$$\exists x \in G \quad y = x^k \qquad \Leftrightarrow \qquad y^{\frac{N}{\text{pgcd}(N,k)}} = e.$$

En particulier, si k est premier avec N, tout élément de G est une puissance k-ième.

(En notation additive, cette denière assertion devient : si k est un entier premier avec N, l'application de multiplication par k est un endomorphisme surjectif du groupe $(\mathbb{Z}/N\mathbb{Z}, +, \overline{0})$ sur lui-même.)

Démonstration. Notons $d = \text{pgcd}(N, k)$ et écrivons $k = k'd$, de sorte que k' est premier avec N. Si $y = x^k$, on a

$$y^{\frac{N}{d}} = x^{\frac{Nk}{d}} = (x^{k'})^N = e$$

par le théorème de Lagrange.

Réciproquement, supposant $y^{\frac{N}{d}} = e$, on peut par le corollaire précédent écrire $y = g^d$ pour un certain $g \in G$. Choisissons par ailleurs un générateur g_0 de G. Puisque k' est premier avec N, $g_0' = (g_0)^{k'}$ est aussi un générateur de G, de sorte qu'on peut écrire $g = (g_0')^n$ pour un certain entier n. Posons alors $x = (g_0)^n$. On trouve bien :

$$x^k = ((g_0)^n)^{k'd} = (((g_0)^{k'})^n)^d = ((g_0')^n)^d = g^d = y.$$

□

Fonction indicatrice d'Euler

Définition 1.3.9. — Pour tout entier $N \geqslant 1$ on note

$$\varphi(N) = |\{\overline{k} \in \mathbb{Z}/N\mathbb{Z} \mid \omega(\overline{k}) = N\}|$$

le nombre de générateurs du groupe additif $\mathbb{Z}/N\mathbb{Z}$. Ceci définit une fonction $\varphi : \mathbb{N}_{>0} \longrightarrow \mathbb{N}$, appelée *fonction indicatrice d'Euler*.

Puisque $\{0, 1, \ldots, N-1\}$ est un ensemble de représentants de $\mathbb{Z}/N\mathbb{Z}$, la dernière assertion de la proposition 1.3.4 permet aussi de caractériser $\varphi(N)$ comme le nombre d'entiers k vérifiant $0 \leqslant k < N$ qui sont premiers avec N.

Par ailleurs, deux groupes cycliques de même ordre étant isomorphes, le lemme 1.2.26 montre qu'ils ont chacun autant éléments d'un même ordre donné. On voit donc en particulier que $\varphi(N)$ est aussi le nombre de générateurs de n'importe quel groupe cyclique d'ordre N.

Lemme 1.3.10. — *Soient N et k deux entiers strictement positifs et G un groupe cyclique d'ordre N (par exemple $G = \mathbb{Z}/N\mathbb{Z}$). Notons $G_{(k)}$ l'ensemble des éléments de G d'ordre k. Alors le cardinal de $G_{(k)}$ est*

$$|G_{(k)}| = \begin{cases} \varphi(k) & \text{si } k \text{ divise } N \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. Par le théorème de Lagrange, on sait que G n'a aucun élément d'ordre k si k ne divise pas N. Si maintenant k divise N, et si on pose $d = \frac{N}{k}$, avec les notations de la remarque 1.3.6, un élément de G est d'ordre divisant k si et seulement si il appartient au sous-groupe H_d, qui est cyclique d'ordre k, de sorte que ce même élément est d'ordre exactement k si et seulement si c'est un générateur de H_d. Or en tant que groupe cyclique d'ordre k, H_d admet $\varphi(k)$ générateurs. □

Lemme 1.3.11. — *Pour tout entier N strictement positif on a*

$$N = \sum_{k|N} \varphi(k).$$

Démonstration. Avec les notations du lemme précédent, les $G_{(k)}$ forment une partition de G, de sorte que $N = |G| = \sum_{k>0} |G_{(k)}|$, ce qui donne la formule recherchée. □

Lemme 1.3.12. — *Soient $m, n \in \mathbb{N}_{>0}$ deux entiers premiers entre eux. Alors pour tous $k|m$ et $l|n$, le produit kl est un diviseur du produit mn, et inversement, tout $d|mn$ peut s'écrire de la sorte d'une unique façon.*

Ceci met donc en bijection l'ensemble des diviseurs de mn avec l'ensemble des couples formés d'un diviseur de m et d'un diviseur de n.

Démonstration. Notons

$$mn = \prod_{i \in I} p_i^{\nu_i}$$

la décomposition en facteurs premiers du produit mn, où les p_i sont des nombres premiers deux à deux distincts et les ν_i des entiers strictement positifs. Dire que m et n sont premiers entre eux signifie que I se partitionne en $I = I_1 \sqcup I_2$ avec $m = \prod_{i \in I_1} p_i^{\nu_i}$ et $n = \prod_{i \in I_2} p_i^{\nu_i}$. Tout diviseur d de mn s'écrit de façon unique $d = \prod_{i \in I} p_i^{\mu_i}$ où les μ_i décrivent l'ensemble défini par les inégalités $0 \leqslant \mu_i \leqslant \nu_i$ (pour tout i), et on vérifie facilement que le couple (k, l) qui est associé à un tel d est donné par $k = \prod_{i \in I_1} p_i^{\mu_i}$ et $l = \prod_{i \in I_2} p_i^{\mu_i}$. □

Proposition 1.3.13. — *On a :*

- $\varphi(1) = 1$,
- $\varphi(p^\nu) = (p-1)p^{\nu-1}$ *pour p premier et $\nu \in \mathbb{N}_{>0}$, et*
- $\varphi(mn) = \varphi(m)\varphi(n)$ *si $m, n \in \mathbb{N}_{>0}$ sont premiers entre eux.*

Les deux premières identités peuvent se prouver directement (ou presque) à partir des définitions ; la preuve « classique » de la troisième repose quant à elle sur le théorème chinois, et utilise de la sorte la structure d'anneau de $\mathbb{Z}/N\mathbb{Z}$, qui ne sera introduite que dans la section suivante (voir remarque 2.1.23). Cela étant, par souci d'économie, et surtout peut-être par désir d'originalité, on va quand même donner ici une preuve complète de la proposition, reposant uniquement sur des notions vues jusqu'à présent, et notamment ne mettant en jeu que la structure de groupe (additif) de $\mathbb{Z}/N\mathbb{Z}$; plus précisément, on va voir comment ces trois identités peuvent se déduire essentiellement du lemme 1.3.11.

Démonstration. On trouve la première identité en posant $N = 1$ dans le lemme 1.3.11.

Pour prouver la deuxième, on commence par remarquer que les diviseurs de p^ν sont les p^μ pour $0 \leqslant \mu \leqslant \nu$, de sorte que le lemme 1.3.11 avec $N = p^\nu$ puis avec $N = p^{\nu-1}$ donne

$$p^\nu = \sum_{0 \leqslant \mu \leqslant \nu} \varphi(p^\mu)$$

et

$$p^{\nu-1} = \sum_{0 \leqslant \mu \leqslant \nu-1} \varphi(p^\mu).$$

Soustrayant ces deux relations on trouve

$$p^\nu - p^{\nu-1} = \varphi(p^\nu),$$

ce qu'il fallait démontrer.

Quant à la troisième identité, il s'agit de montrer que pour tout entier $N > 0$, si l'on peut écrire $N = mn$ avec m et n premiers entre eux, alors $\varphi(N) = \varphi(m)\varphi(n)$. Pour cela on va procéder par récurrence sur N. Le résultat est vrai pour $N = 1$ (car alors nécessairement $m = n = 1$ et on conclut à l'aide de la première identité). Supposons donc que pour tout $N' < N$, si l'on peut écrire $N' = m'n'$ avec m' et n' premiers entre eux, alors $\varphi(N') = \varphi(m')\varphi(n')$, et montrons que le résultat analogue vaut aussi pour $N = mn$. En effet, le lemme 1.3.11 donne alors

$$\begin{aligned} mn &= \sum_{d|mn} \varphi(d) \\ &= \varphi(mn) \ + \sum_{\substack{d|mn \\ d\neq mn}} \varphi(d) \\ &= \varphi(mn) \ + \sum_{\substack{d=kl \\ k|m,\ l|n \\ (k,l)\neq(m,n)}} \varphi(d), \end{aligned}$$

la dernière égalité résultant du lemme 1.3.12.

Pour $k|m$ et $l|n$ on a $\operatorname{pgcd}(k,l)|\operatorname{pgcd}(m,n) = 1$, et lorsque le couple (k,l) n'est pas égal au couple (m,n), c'est-à-dire lorsque $d = kl$ est un diviseur *strict* de mn, on a $d < mn = N$, ce qui permet d'appliquer l'hypothèse de récurrence avec $N' = d$, soit $\varphi(d) = \varphi(k)\varphi(l)$. De là on trouve ainsi :

$$mn = \varphi(mn) \ + \sum_{\substack{k|m,\ l|n \\ (k,l)\neq(m,n)}} \varphi(k)\varphi(l).$$

D'autre part, le lemme 1.3.11 appliqué à m et à n séparément donne

$$\begin{aligned} mn &= \sum_{k|m} \varphi(k) \ \times \sum_{l|n} \varphi(l) \\ &= \sum_{k|m,\ l|n} \varphi(k)\varphi(l) \\ &= \varphi(m)\varphi(n) \ + \sum_{\substack{k|m,\ l|n \\ (k,l)\neq(m,n)}} \varphi(k)\varphi(l). \end{aligned}$$

Soustrayant les deux dernières relations obtenues, on trouve bien $\varphi(mn) = \varphi(m)\varphi(n)$. □

Corollaire 1.3.14. — *Pour tout entier $n > 0$ admettant la décomposition en facteurs premiers*

$$n = \prod_{i=1}^{r} p_i^{\nu_i}$$

(où les p_i sont des nombres premiers deux à deux distincts, et où les ν_i sont strictement positifs), on a

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{\nu_i - 1}$$

d'où aussi

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Démonstration. C'est une conséquence immédiate de la proposition. □

1.4 Théorèmes de structure des groupes abéliens finis

Décomposition en facteurs primaires

Exposant d'un groupe abélien fini

Théorème des diviseurs élémentaires, facteurs invariants

1.5 Exercices

Exercice 1.5.1
Considérons deux ensembles E et E', chacun étant muni d'une relation d'équivalence, $\sim$ et $\sim'$ respectivement. Notons $\pi : E \longrightarrow E/\sim$ et $\pi' : E' \longrightarrow E'/\sim'$ les projections canoniques correspondantes. On dira qu'une application $f : E \longrightarrow E'$ est compatible à ces relations si pour tous $x, y \in E$ on a

$$x \sim y \quad \Longrightarrow \quad f(x) \sim' f(y).$$

Si cette condition est vérifiée, montrer alors qu'il existe une et une seule application

$$\overline{f} : \ E/\sim \longrightarrow E'/\sim'$$

vérifiant

$$\pi' \circ f = \overline{f} \circ \pi$$

(ou, de façon équivalente et peut-être plus parlante : telle que pour tout $x \in E$ on ait $\overline{f}(\overline{x}) = \overline{f(x)}$).

Exercice 1.5.2
Soient G un groupe fini et H un sous-groupe. Montrer que $|H|$ divise $|G|$ en établissant les faits suivants :
- l'ordre de G est la somme des ordres des classes modulo H
- toutes les classes modulo H ont même ordre, égal à celui de H.

Ceci donne une seconde preuve de la proposition 1.2.10.

Exercice 1.5.3
Soient G et G' deux groupes, et $f : G \longrightarrow G'$ une application vérifiant $f(xy) = f(x)f(y)$ pour tous $x, y \in G$. Montrer que f est un homomorphisme.

Exercice 1.5.4
Soient G un groupe et H un sous-ensemble de G.

1. Montrer que H est un sous-groupe si et seulement si $x^{-1}y \in H$ pour tous $x, y \in H$.
2. Si H est *fini*, montrer que H est un sous-groupe si et seulement si $xy \in H$ pour tous $x, y \in H$.

Exercice 1.5.5
Montrer que les groupes quotients $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{R}^\times/\mathbb{R}_+^\times$ sont isomorphes.

Exercice 1.5.6
Quel est l'isomorphisme inverse de l'isomorphisme $\mathbb{C}/2i\pi\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times$ décrit dans l'exemple 1.2.24 ?

Exercice 1.5.7
Soient $f : G \longrightarrow G'$ un morphisme de groupes abéliens, H un sous-groupe de G et H' un sous-groupe de G', et π et π' les projections canoniques associées. Montrer que les deux assertions suivantes sont équivalentes :
- $f(H) \subset H'$
- il existe un morphisme $\overline{f} : G/H \longrightarrow G'/H'$ tel que se factorise en

$$\overline{f} \circ \pi = \pi' \circ f.$$

Lorsque c'est le cas, ce morphisme $\overline{f}$ est unique, et on dit qu'il se déduit de f par passage au quotient par H et H'.

Exercice 1.5.8
Soient $(G, +, 0)$ un groupe abélien et H un sous-groupe. Montrer que pour tout sous-groupe B de G contenant H, on a un isomorphisme naturel

$$G/B \xrightarrow{\sim} (G/H)/(B/H).$$

Indication : considérer la composée des projections canoniques $G \longrightarrow G/H$ et $G/H \longrightarrow (G/H)/(B/H)$, montrer que le noyau est B, et passer au quotient.

Exercice 1.5.9
Soit G un groupe *abélien*. Montrer que tout élément x de G vérifie

$$x^{|G|} = e,$$

en établissant d'abord la formule

$$\prod_{y \in G} y = \prod_{y \in G} (xy)$$

(la loi est ici notée multiplicativement).

Remarque : ceci fournit une seconde preuve du théorème de Lagrange, mais qui ne fonctionne que sous l'hypothèse que le groupe est abélien, contrairement à celle donnée page 21, qui reste valable en toute généralité.

Exercice 1.5.10
Le groupe produit

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$$

est-il cyclique ?
Le groupe produit

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}) (\overline{1}, \overline{2})\}$$

est-il cyclique ?

Chapitre 2

Arithmétique modulaire

L'objectif principal de ce chapitre est l'étude de l'anneau $\mathbb{Z}$ des entiers relatifs et de l'anneau $K[X]$ des polynômes sur un corps, ainsi que de leurs quotients.

La propriété commune de $\mathbb{Z}$ et de $K[X]$ sur laquelle cette étude reposera est que ces anneaux sont *euclidiens* ; on travaillera donc autant que possible dans ce cadre unifié et un peu plus général. Au passage, et notamment afin de voir quelles hypothèses précises sont utilisées pour chaque résultat, on introduira progressivement différents types d'anneaux « classiques » :

- anneaux factoriels, où les notions liées à la divisibilité (éléments irréductibles, ppcm et pgcd, etc.) disposent de propriétés agréables
- anneaux principaux, où l'on dispose du théorème de Bézout, qui trouve des applications à l'inversion dans les anneaux quotients et au théorème chinois
- anneaux euclidiens, où l'algorithme d'Euclide (étendu) permet en pratique de trouver de telles relations de Bézout, et donc de résoudre effectivement les problèmes évoqués ci-dessus.

Avant d'en arriver là, on commence par rappeler quelques définitions de base qui seront utilisées par la suite.

2.1 Anneaux et idéaux, corps, polynômes

Définition 2.1.1. — Un anneau $(A, +, \times, 0_A, 1_A)$ (souvent abrégé en A tout court) est la donnée d'un ensemble A, de deux lois de composition interne $+$ (addition) et $\times$ (multiplication) sur A, d'un élément $0_A \in A$ (élément nul), et d'un élément $1_A \in A$ (élément unité), vérifiant les propriétés suivantes :

- $(A, +, 0_A)$ est un groupe abélien
- 1_A est neutre pour $\times$: $\quad \forall a \in A \quad a \times 1_A = 1_A \times a = a$

– $\times$ est associative : $\forall a, b, c \in A \quad (ab)c = a(bc)$
– $\times$ est distributive par rapport à $+$: $\forall a, b, c \in A \quad a(b+c) = ab + ac$ et $(a+b)c = ac + bc$.

On dit que cet anneau est commutatif si en outre :
– $\times$ est commutative : $\forall a, b \in A \quad ab = ba$.

Dans ce cours on n'étudiera que des anneaux commutatifs. L'algèbre non commutative est très riche et intéressante, mais on aura déjà suffisamment à faire avec la théorie commutative. Ainsi, dans la suite du texte, et sauf mention du contraire, *tous les anneaux considérés seront commutatifs.*

Exemple 2.1.2. — 1. La donnée $(\mathbb{Z}, +, \times, 0, 1)$ définit un anneau.

2. La donnée $(\mathbb{R}, +, \times, 0, 1)$ définit un anneau.
3. Si $(A, +_A, \times_A, 0_A, 1_A)$ et $(B, +_B, \times_B, 0_B, 1_B)$ sont deux anneaux, le produit direct $A \times B$ est muni naturellement d'une structure d'anneau ; l'addition et la multiplication sont définies terme à terme :

$$(a, b) + (a', b') = (a +_A a', b +_B b') \qquad (a, b) \times (a', b') = (a \times_A a', b \times_B b'),$$

l'élément nul est $(0_A, 0_B)$, et l'élément unité $(1_A, 1_B)$. L'anneau ainsi construit est appelé *anneau produit* de A et B.
4. Le singleton $A = \{0_A\}$ dispose naturellement d'une unique structure d'anneau, qui en fait l'*anneau nul* ; dans cet anneau, l'élément nul et l'élément unité coïncident : $1_A = 0_A$.

Définition 2.1.3. — Un élément x d'un anneau (commutatif) A est dit inversible s'il existe $y \in A$ tel que $xy = 1_A$. On note $A^\times$ le sous-ensemble de A formé des éléments inversibles.

Lemme 2.1.4. — *Avec les notations de la définition, l'élément $y \in A$ est unique (on le note $y = x^{-1}$). L'ensemble des éléments inversibles est stable par multiplication, et forme un groupe $(A^\times, \times, 1_A)$.*

Démonstration. Si y_1 et y_2 sont deux inverses de x, on a $y_1 = y_1(xy_2) = (y_1x)y_2 = y_2$, d'où l'unicité. Si x et x' sont inversibles, xx' l'est aussi : son inverse est $(xx')^{-1} = x'^{-1}x^{-1}$; ainsi $A^\times$ est stable par multiplication. De même si x est inversible, x^{-1} l'est aussi : son inverse est $(x^{-1})^{-1} = x$; ainsi $A^\times$ est stable par inversion. Enfin $A^\times$ contient 1_A (qui est son propre inverse), ce qui achève de montrer que $(A^\times, \times, 1_A)$ est un groupe. □

Remarque 2.1.5. — Le lemme précédent reste valable pour un anneau non commutatif à condition de définir un élément inversible comme admettant un inverse *de chaque côté.*

Exemple 2.1.6. — On a $\mathbb{Z}^\times = \{1, -1\}$, isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Définition 2.1.7. — Un élément a d'un anneau A est dit *diviseur de zéro* (dans A) si $a \neq 0_A$ et s'il existe $b \in A$, $b \neq 0_A$, tel que $ab = 0_A$.

Définition 2.1.8. — Un anneau A est dit *intègre* si A n'est pas l'anneau nul et s'il n'admet pas de diviseur de zéro : $\forall a, b \in A \quad a, b \neq 0 \Rightarrow ab \neq 0$.

Définition 2.1.9. — corps

Définition 2.1.10. — Soient $(A, +_A, \times_A, 0_A, 1_A)$ et $(B, +_B, \times_B, 0_B, 1_B)$ deux anneaux. On dit qu'une application $f : A \longrightarrow B$ est un morphisme (ou homomorphisme) d'anneaux si :
- f est un morphisme de groupes abéliens de $(A, +_A, 0_A)$ dans $(B, +_B, 0_B)$
- $f(1_A) = 1_B$
- $f(a \times_A a') = f(a) \times_B f(a')$ pour tous $a, a' \in A$.

Un morphisme d'un anneau dans lui-même est appelé endomorphisme ; un morphisme bijectif est appelé isomorphisme (alors son inverse est aussi un morphisme) ; un morphisme qui est à la fois un endomorphisme et un isomorphisme est appelé automorphisme.

Définition 2.1.11. — Soit $(A, +, \times, 0_A, 1_A)$ un anneau. On dit qu'une partie A' de A est un sous-anneau si :
- A' est un sous-groupe abélien de $(A, +, 0_A)$
- A' contient 1_A et est stable par $\times_A$.

On vérifie alors facilement que les lois restreintes font de $(A', +, \times, 0_A, 1_A)$ un anneau.

Exemple 2.1.12. —
1. L'anneau $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
2. Si $f : A \longrightarrow B$ est un morphisme d'anneaux, son image $\operatorname{im} f$ est un sous-anneau de B.
3. L'anneau $\mathbb{Z}$ n'admet d'autre sous-anneau que lui-même. En effet :
   - un sous-anneau de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc soit nul, soit de la forme $N\mathbb{Z}$ pour $N > 0$
   - un sous-anneau de $\mathbb{Z}$ contient l'élément unité 1 de $\mathbb{Z}$, ce qui élimine le sous-groupe nul, et force $N = 1$.

Remarque 2.1.13. — On retiendra en particulier de l'exemple précédent que *l'anneau nul n'est pas un sous-anneau de* $\mathbb{Z}$ (ni d'aucun autre anneau, pour la même raison).

De même, on définira plus tard une structure d'anneau sur $\mathbb{Z}/N\mathbb{Z}$, et on prendra garde que $\mathbb{Z}/M\mathbb{Z}$ *n'est pas un sous-anneau de* $\mathbb{Z}/N\mathbb{Z}$ (sauf évidemment pour $M = N$).

Lemme 2.1.14. — *Si B est un anneau et si $(B_i)_{i\in I}$ est une famille quelconque de sous-anneaux de B, leur intersection $B' = \bigcap_{i\in I} B_i$ est encore un sous-anneau de B.*

Démonstration. On vérifie facilement que B' est un sous-groupe additif de B contenant l'élément unité et stable par multiplication, dès lors que c'est le cas pour chacun des B_i. □

Proposition 2.1.15. — *Soient B un anneau, A un sous-anneau de B, et S une partie quelconque de B. Notons $A[S]$ la partie de B définie comme l'intersection de tous les sous-anneaux de B qui contiennent A et S. Alors $A[S]$ est un sous-anneau de B contenant A et S, et c'est le plus petit d'entre eux : tout sous-anneau de B contenant A et S contient aussi $A[S]$.*

En outre, A est un sous-anneau de $A[S]$.

Définition 2.1.16. — Avec ces notations, on dira que $A[S]$ est le sous-anneau de B engendré par S sur A.

Démonstration de la proposition. Par le lemme précédent, $A[S]$ est bien un sous-anneau de B. Tout le reste découle immédiatement de la construction. □

Définition 2.1.17. — Une partie I d'un anneau A est un *idéal* si :
- I est un sous-groupe additif de A
- I est stable par multiplication par les éléments de A :

$$\forall x \in I \quad \forall a \in A \qquad ax \in I.$$

Soit I un idéal d'un anneau A. Alors I est un sous-groupe du groupe additif de A, et on rappelle que ceci permet de définir une relation d'équivalence sur A en posant $a \equiv b \mod I$ pour signifier $a - b \in I$, et que l'ensemble quotient A/I, dont les éléments sont les parties de A de la forme $\overline{a} = a + I$, dispose naturellement d'une structure de groupe abélien.

Lemme 2.1.18. — *Avec les notations précédentes, pour tous $a, b, b' \in A$, on a l'implication :*

$$b \equiv b' \mod I \qquad \Longrightarrow \qquad ab \equiv ab' \mod I.$$

Démonstration. Si $b - b' = i \in I$, alors $ab - ab' = ai \in I$ puisque I est stable par multiplication par a. □

Proposition 2.1.19. — *Avec les notations précédentes, le groupe abélien A/I dispose naturellement d'une loi de multiplication qui le munit d'une structure d'anneau, et pour laquelle la projection canonique $A \longrightarrow A/I$ est un morphisme d'anneaux.*

Démonstration. Si $a \equiv a' \mod I$ et $b \equiv b' \mod I$, en appliquant deux fois le lemme précédent on trouve $ab \equiv ab' \equiv a'b' \mod I$. On en déduit que l'application

$$\begin{array}{ccc} A \times A & \longrightarrow & A/I \\ (a,b) & \mapsto & \overline{ab} \end{array}$$

passe au quotient en

$$\begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ \left(\overline{a},\overline{b}\right) & \mapsto & \overline{ab}, \end{array}$$

et on vérifie sans peine que la loi de multiplication sur A/I ainsi définie satisfait bien à toutes les conditions demandées. □

Lemme 2.1.20. — *Soient A et B deux anneaux et $f : A \longrightarrow B$ un morphisme. Alors :*

1. *Pour tout idéal J de B, $f^{-1}(J)$ est un idéal de A.*
   En particulier le noyau $\ker f = f^{-1}(0_B)$ *est un idéal de A.*
2. *Si de plus f est* surjectif, *alors pour tout idéal I de A, $f(I)$ est un idéal de B.*

Démonstration. C'est une conséquence immédiate des définitions. Par exemple, dans le point 2., montrons que $f(I)$ est stable par multiplication par les éléments de B : en effet, si $j \in f(I)$, il existe $i \in I$ tel que $j = f(i)$, et si $b \in B$, il existe $a \in A$ tel que $b = f(a)$ puisque f est surjectif ; alors $ai \in I$ car I est un idéal de A, et $bj = f(a)f(i) = f(ai) \in f(I)$. □

Lemme 2.1.21. — *Si A est un anneau, il existe un unique morphisme d'anneau $f : \mathbb{Z} \longrightarrow A$. Ce morphisme vérifie $f(n) = n.1_A$ pour tout $n \in \mathbb{Z}$.*

Démonstration. Un morphisme d'anneau $f : \mathbb{Z} \longrightarrow A$ est un morphisme de groupes additifs et il vérifie $f(1) = 1_A$. Par le lemme 1.2.28, un tel morphisme de groupes est unique et est donné par la formule indiquée. On vérifie alors facilement que ce morphisme de groupes est en fait un morphisme d'anneaux. □

Définition 2.1.22. — caractéristique d'un anneau intègre

Remarque 2.1.23. —

2.2 Anneaux factoriels

On rappelle que si a et b sont deux éléments d'un anneau intègre A, on note $b|a$ pour signifier que b divise a (dans A), c'est-à-dire qu'il existe $c \in A$ tel que $a = bc$.

Dire qu'un élément u de A est inversible équivaut à demander $u|1$. Les éléments inversibles forment un groupe (pour la multiplication), noté $A^\times$.

On rappelle aussi qu'un idéal non nul I de A est dit principal s'il existe $x \in I$ tel que $I = Ax = \{ax \mid a \in A\}$. On dit alors que x est un générateur de I.

Proposition-définition 2.2.1. — *Soient A un anneau intègre, et a et b deux éléments non nuls de A. Alors les trois assertions suivantes sont équivalentes :*

1. *on a $a|b$ et $b|a$*
2. *il existe $u \in A^\times$ tel que $a = ub$*
3. *les idéaux principaux Aa et Ab sont égaux.*

Lorsque ces conditions sont vérifiées, on dit que a et b sont deux éléments associés *dans A, ce que l'on note*

$$a \sim b.$$

Cette relation $\sim$ est une relation d'équivalence sur $A \smallsetminus \{0\}$.

Démonstration. Dire que $a|b$ et $b|a$ signifie qu'il existe $u, v \in A$ avec $b = ua$ et $a = vb$. On a alors $a = uva$, soit $a(1 - uv) = 0$, et puisque A est intègre et $a \neq 0$, nécessairement $1 - uv = 0$, autrement dit, u est inversible (et v est son inverse). Tout le reste de la proposition se démontre sans aucune difficulté. □

Exemple 2.2.2. — Dans $\mathbb{Z}$ on a $m \sim n$ si et seulement si $m = \pm n$. Ainsi parmi les éléments associés à n il en existe un et un seul qui soit positif. Autrement dit, les entiers positifs forment un système de représentants pour la relation $\sim$ sur $\mathbb{Z} \smallsetminus \{0\}$.

Dans $K[X]$ on a $P \sim Q$ si et seulement si $P = \lambda Q$ pour un certain $\lambda \in K^\times$. Ainsi parmi les polynômes associés à P il en existe un et un seul qui soit unitaire. Autrement dit, les polynômes unitaires forment un système de représentants pour la relation $\sim$ sur $K[X] \smallsetminus \{0\}$.

Définition 2.2.3. — Soient A un anneau intègre, et $a, b \in A \smallsetminus \{0\}$.

On dira qu'un élément $d \in A \smallsetminus \{0\}$ est un *plus grand diviseur commun* (ou pgcd) de a et b si on a $d|a$ et $d|b$, et si pour tout $x \in A \smallsetminus \{0\}$ vérifiant $x|a$ et $x|b$ on a $x|d$.

On dira de même qu'un élément $m \in A \smallsetminus \{0\}$ est un *plus petit multiple commun* (ou ppcm) de a et b si on a $a|m$ et $b|m$, et si pour tout $y \in A \smallsetminus \{0\}$ vérifiant $a|y$ et $b|y$ on a $m|y$.

Lemme 2.2.4. — *Avec les notations de la proposition, supposons que a et b admettent un* pgcd*. Alors tous les* pgcd *de a et b sont associés entre eux, et réciproquement, tout élément associé à un* pgcd *de a et b est encore un* pgcd *de a et b.*
De même, si a et b admettent un ppcm*, alors tous les* ppcm *de a et b sont associés entre eux, et tout élément associé à un* ppcm *de a et b est encore un* ppcm *de a et b.*

Démonstration. Soient d et d' deux pgcd de a et b. Alors $d'|a$ et $d'|b$, donc $d'|d$; par symétrie on trouve aussi $d|d'$, donc $d \sim d'$. Inversement si d est un pgcd de a et b et si $d \sim d'$, alors $d'|d$, $d|a$ et $d|b$ impliquent $d'|a$ et $d'|b$, et si $x \in A \setminus \{0\}$ vérifie $x|a$ et $x|b$, alors $x|d$ et $d|d'$ impliquent $x|d'$; autrement dit, d' est bien un pgcd de a et b. Le cas des ppcm se traite de la même façon. □

Ainsi, on voit que dans un anneau intègre général, deux éléments n'admettent pas forcément de pgcd ni de ppcm, mais lorsque c'est le cas, ceux-ci sont définis uniquement à multiplication par un inversible près. On peut lever cette indétermination comme suit :

Définition 2.2.5. — Soit A un anneau intègre muni d'un système de représentants S pour la relation $\sim$. Si a et b sont deux éléments de A qui admettent un pgcd, alors parmi les pgcd de a et b il en existe un et un seul qui appartienne à S ; on le note

$$\mathrm{pgcd}(a, b).$$

De même si a et b admettent un ppcm, on note

$$\mathrm{ppcm}(a, b)$$

l'unique ppcm de a et b qui appartient à S.

Ainsi conformément à l'exemple 2.2.2, dans $\mathbb{Z}$ on prendra les pgcd et ppcm positifs, et dans $K[X]$ on les prendra unitaires.

Définition 2.2.6. — Soit A un anneau intègre. Un élément non nul a de A sera dit irréductible si a n'est pas inversible, et si pour toute décomposition en produit

$$a = bc$$

l'un parmi b et c est nécessairement inversible (et l'autre est donc associé à a).

Définition 2.2.7. — On dit qu'une partie P de A est un système représentatif d'éléments irréductibles si P est formé d'éléments irréductibles, et si tout élément irréductible de A est associé à un élément de P, et à un seul.

Lemme 2.2.8. — *Si A est un anneau intègre, et si $a, a' \in A$ vérifient $a \sim a'$ avec a irréductible, alors a' est irréductible.*

Démonstration. Par l'absurde supposons a' non irréductible, de sorte qu'on peut écrire $a' = b'c'$ avec b' et c' non inversibles. Puisque a est associé à a', on a $a = ua'$ avec u inversible. Alors $a = bc$ où $b = ub'$ et $c = c'$, de sorte que b et c ne sont pas inversibles, ce qui contredit l'irréductibilité de a. □

Du lemme on déduit que si A est muni d'un système de représentants S pour la relation $\sim$, on peut le munir d'un système représentatif d'éléments irréductibles P, en prenant pour P l'ensemble des éléments de S qui sont irréductibles. En particulier :

Exemple 2.2.9. — Dans $\mathbb{Z}$ les nombres premiers (positifs !) forment un système représentatif d'éléments irréductibles. Ainsi un entier n est irréductible si et seulement si $n = \pm p$ avec p premier.

Dans $K[X]$ les polynômes irréductibles unitaires forment un système représentatif d'éléments irréductibles.

Définition 2.2.10. — Soit A un anneau intègre muni d'un système représentatif d'éléments irréductibles P. On dit que A est un anneau *factoriel* si pour tout $a \in A$ non nul il existe une unique partie $I \subset P$ finie, une unique famille d'entiers strictements positifs $(\mu_p)_{p\in I}$, et un unique $u \in A^\times$, tels que

$$a = u \prod_{p\in I} p^{\mu_p}. \qquad (*)$$

On dit que (*) est la décomposition de a en produits de facteurs irréductibles (relativement au système représentatif P).

Remarque 2.2.11. — On vérifie facilement que la propriété pour A d'être factoriel ne dépend pas du choix du système représentatif. En outre si Q est un autre système représentatif et si $a = v \prod_{q\in J} q^{\nu_q}$ est la décomposition de a relativement à Q, où $J \subset Q$ fini, $\nu_q > 0$ et $v \in A^\times$, alors on a $|J| = |I|$ et il existe une bijection $\sigma : J \longrightarrow I$ telle que pour tout $q \in J$ et $p = \sigma(q) \in I$ on ait $p \sim q$ et $\mu_p = \nu_q$.

Remarque 2.2.12. — On a vu que si A est un anneau intègre, on peut déduire de tout système de représentants pour la relation $\sim$ un système représentatif d'éléments irréductibles. Inversement on vérifie facilement que si A est factoriel et si P est un système représentatif d'éléments irréductibles, l'ensemble S des éléments de A de la forme $\prod_{p\in I} p^{\mu_p}$ (pour $I \subset P$ fini et $\mu_p > 0$) est un système de représentants pour la relation $\sim$.

Théorème 2.2.13. — *Soient A un anneau factoriel et $a, b \in A \setminus \{0\}$. Alors a et b admettent un* pgcd *et un* ppcm*. De plus on a*

$$\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b) \sim ab.$$

(Autrement dit il existe $u \in A^\times$ tel que $\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b) = uab$*.)*

Démonstration. Soit P un système représentatif d'éléments irréductibles de A. Notons $a = u\prod_{p\in I} p^{\mu_p}$ et $b = v\prod_{p\in J} p^{\nu_p}$ les décompositions de a et b en produits d'irréductibles. On peut alors aussi écrire

$$a = u \prod_{p\in I\cup J} p^{\mu_p} \qquad \text{et} \qquad b = v \prod_{p\in I\cup J} p^{\nu_p}$$

en posant $\mu_p = 0$ (resp. $\nu_p = 0$) pour $p \in J \smallsetminus I$ (resp. $I \smallsetminus J$). On vérifie alors facilement qu'on a

$$\mathrm{pgcd}(a,b) = \prod_{p \in I \cup J} p^{\min(\mu_p, \nu_p)}$$

et

$$\mathrm{ppcm}(a,b) = \prod_{p \in I \cup J} p^{\max(\mu_p, \nu_p)}.$$

Le dernière assertion de la proposition s'en déduit, grâce à l'identité

$$\mu_p + \nu_p = \min(\mu_p, \nu_p) + \max(\mu_p, \nu_p).$$

□

Exemple 2.2.14. — L'anneau $\mathbb{Z}$ est factoriel. Un corps est un anneau factoriel. L'anneau $K[X]$ des polynômes sur le corps K est factoriel. Plus généralement, l'exercice 2.8.3 montre que si A est factoriel, alors $A[X]$ l'est aussi.

2.3 Anneaux principaux

2.4 Anneaux euclidiens

2.5 Théorème de l'élément primitif

Théorème 2.5.1 (de l'élément primitif)**.** —

Corollaire 2.5.2. — *Soient K un corps de cardinal $|K| = q$ fini, et d un diviseur de $q-1$. Alors pour $y \in K^\times$, on a l'équivalence :*

$$\exists x \in K^\times \quad y = x^d \qquad \Longleftrightarrow \qquad y^{\frac{q-1}{d}} = 1.$$

Autrement dit, y est une puissance d-ième dans K si et seulement si y est racine $\frac{q-1}{d}$-ième de l'unité dans K.

2.6 Réciprocité quadratique

Critère d'Euler et symbole de Legendre

Théorème 2.6.1 (critère d'Euler)**.** —

Corollaire 2.6.2. — *Si p est un nombre premier impair, on a*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & si \quad p \equiv 1 \mod 4 \\ -1 & si \quad p \equiv 3 \mod 4 \end{cases}$$

ou autrement dit -1 est résidu quadratique modulo p si p est de la forme $4k+1$, et est non-résidu si p est de la forme $4k+3$.

Démonstration. C'est une application directe du critère d'Euler. □

Lemme de Gauss

Lemme 2.6.3 (Gauss)**.** — *Soit p un nombre premier impair et $a \in \mathbb{Z}$ un entier premier à p. Notons $S = \{1, \ldots, \frac{p-1}{2}\}$, de sorte que $(\mathbb{Z}/p\mathbb{Z})^\times$ est réunion disjointe de $\overline{S}$ et de $-\overline{S}$. En particulier, pour tout $s \in S$, on peut écrire la classe de as sous la forme*

$$as \equiv \varepsilon_s(a) s_a \mod p$$

avec $\varepsilon_s(a) = \pm 1$ et $s_a \in S$ déterminés de façon unique. Alors, avec ces notations, l'application qui à s associe s_a est une permutation de S, et on a l'identité

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_a(s).$$

Démonstration. Si $s, s' \in S$ vérifient $s_a = s'_a$, on a $s \equiv \pm s' \mod p$, donc $s = s'$ par choix de S. Ainsi l'application de S dans lui-même qui à s associe s_a est injective, donc bijective. Posant alors

$$P = \prod_{s \in S} s = \prod_{s \in S} s_a$$

on a $P \not\equiv 0 \mod p$, et

$$a^{\frac{p-1}{2}} P \equiv \prod_{s \in S} as \equiv \prod_{s \in S} \varepsilon_s(a) s_a \equiv \left(\prod_{s \in S} \varepsilon_s(a)\right) P \mod p$$

d'où

$$a^{\frac{p-1}{2}} \equiv \prod_{s \in S} \varepsilon_s(a) \mod p.$$

□

Proposition 2.6.4. — *Si p est un nombre premier impair, on a*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \text{ ou } 7 \mod 8 \\ -1 & si \quad p \equiv 3 \text{ ou } 5 \mod 8 \end{cases}$$

ce qui peut aussi s'écrire

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Démonstration. On applique le lemme de Gauss avec $a = 2$. On a $\varepsilon_s(2) = 1$ si $s \leqslant \frac{p-1}{4}$ et $\varepsilon_s(2) = -1$ si $s > \frac{p-1}{4}$, de sorte que $\left(\frac{2}{p}\right) = (-1)^{|S'|}$ où

$$S' = \{s \in \{1, \ldots, \tfrac{p-1}{2}\} \mid s > \tfrac{p-1}{4}\} = \mathbb{N} \cap]\tfrac{p-1}{4}, \tfrac{p-1}{2}].$$

Alors :
- si $p = 8k+1$, on a $S' = \{2k+1, \ldots, 4k\}$ et $|S'| = 2k$ pair
- si $p = 8k+3$, on a $S' = \{2k+1, \ldots, 4k+1\}$ et $|S'| = 2k+1$ impair
- si $p = 8k+5$, on a $S' = \{2k+2, \ldots, 4k+2\}$ et $|S'| = 2k+1$ impair
- si $p = 8k+7$, on a $S' = \{2k+2, \ldots, 4k+3\}$ et $|S'| = 2k+2$ pair

ce qui prouve la première assertion.

Pour prouver la seconde, un calcul immédiat montre que pour $p \equiv 1$ ou $7 \bmod 8$ on a $p^2 \equiv 1 \bmod 16$ donc $\frac{p^2-1}{8}$ est bien un entier pair, tandis que pour $p \equiv 3$ ou $5 \bmod 8$ on a $p^2 \equiv 9 \bmod 16$ donc $\frac{p^2-1}{8}$ est bien un entier impair. □

Une identité trigonométrique

Lemme 2.6.5. — *Soit $q \in \mathbb{N}$ un entier* impair. *On a alors la relation*

$$\frac{\sin qx}{\sin x} = (-4)^{\frac{q-1}{2}} \prod_{t=1}^{\frac{q-1}{2}} \left(\sin^2 x - \sin^2 \tfrac{2\pi t}{q}\right).$$

Démonstration. La preuve consiste à écrire $\frac{\sin qx}{\sin x}$ comme un polynôme en $\sin^2 x$, polynôme dont on explicite le degré, le coefficient dominant, et les racines. De façon détaillée, on procède en trois étapes :

Première étape. On montre que pour tout entier $n \geqslant 1$ on peut écrire

$$\frac{\sin nx}{\sin x} = U_n(\cos x)$$

pour un certain polynôme $U_n(X) \in \mathbb{Z}[X]$ à coefficients entiers déterminé de façon unique, vérifiant en outre les propriétés suivantes : U_n est un polynôme

pair (resp. impair) pour n impair (resp. pair), de degré $\deg(U_n) = n-1$, et de coefficient dominant $\text{c. d.}(U_n) = 2^{n-1}$.

En effet, ceci se prouve par récurrence. On a clairement $U_1(X) = 1$, et l'identité $\sin 2x = 2\cos x \sin x$ donne $U_2(X) = 2X$. Supposant maintenant le résultat vrai jusqu'à l'ordre n, en divisant l'identité

$$\sin(n+1)x + \sin(n-1)x = 2\cos x \sin nx$$

par $\sin x$ on trouve

$$U_{n+1}(X) = 2XU_n(X) - U_{n-1}(X),$$

et toutes les propriétés énoncées s'en déduisent aisément.

(Les polynômes $U_n(X)$ ainsi construits s'appellent polynômes de Tchebycheff de seconde espèce.)

Deuxième étape. Supposons maintenant $n = q$ impair. Alors $U_q(X)$ est un polynôme pair, et on peut écrire

$$U_q(X) = V_q(X^2) = V_q(1-(1-X^2)) = W_q(1-X^2)$$

où $W_q(T) = V_q(1-T)$ est un polynôme à coefficients entiers, de degré

$$\deg W_q = \deg V_q = \frac{1}{2}\deg U_q = \frac{q-1}{2}$$

et de coefficient dominant

$$\text{c. d.}(W_q) = (-1)^{\frac{q-1}{2}}\,\text{c. d.}(V_q) = (-1)^{\frac{q-1}{2}}\,\text{c. d.}(U_q) = (-1)^{\frac{q-1}{2}}2^{q-1}.$$

Ainsi on a

$$\frac{\sin qx}{\sin x} = W_q(\sin^2 x)$$

avec $\deg W_q = \frac{q-1}{2}$, $\text{c. d.}(W_q) = (-1)^{\frac{q-1}{2}}2^{q-1} = (-4)^{\frac{q-1}{2}}$.

Troisième étape. Pour $x_t = \frac{2\pi t}{q}$, $t \in \{1, \ldots, \frac{q-1}{2}\}$, on a

$$W_q(\sin^2 x_t) = \frac{\sin qx_t}{\sin x_t} = 0,$$

de sorte que $y_t = \sin^2 x_t$ est racine de W_q. Montrons que les y_t sont deux à deux distincts. Une fois ceci prouvé, on aura exhibé $\frac{q-1}{2}$ racines distinctes de W_q, de sorte qu'on les aura ainsi toutes, et on pourra alors écrire

$$W_q(X) = \text{c. d.}(W_q)\prod_{t=1}^{\frac{q-1}{2}}(X-y_t) = (-4)^{\frac{q-1}{2}}\prod_{t=1}^{\frac{q-1}{2}}\left(X - \sin^2\tfrac{2\pi t}{q}\right)$$

ce qui terminera la preuve du lemme.

Or pour $t, t' \in \{1, \dots, \frac{q-1}{2}\}$, on a les équivalences

$$\begin{aligned} \sin^2 \tfrac{2\pi t}{q} = \sin^2 \tfrac{2\pi t'}{q} &\iff \sin \tfrac{2\pi t}{q} = \pm \sin \tfrac{2\pi t'}{q} \\ &\iff \tfrac{2\pi t}{q} \equiv \pm \tfrac{2\pi t'}{q} \mod \pi\mathbb{Z} \\ &\iff 2t \equiv \pm 2t' \mod q\mathbb{Z} \\ &\iff t \equiv \pm t' \mod q\mathbb{Z} \end{aligned}$$

(où l'on s'est servi du fait que q est impair donc 2 inversible modulo q), ce qui finalement impose $t = t'$. Ceci termine la preuve. □

Réciprocité quadratique pour le symbole de Legendre

Théorème 2.6.6. — *Soient p et q deux nombres premiers impairs distincts. Alors on a*

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} 1 & \text{si } p \text{ ou } q \equiv 1 \text{ mod } 4 \\ -1 & \text{si } p \equiv q \equiv 3 \text{ mod } 4 \end{cases} \end{aligned}$$

ou autrement dit :

- *si l'un des deux au moins parmi p et q est de la forme $4k+1$, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, et ils sont tous les deux résidus ou tous les deux non-résidus l'un par rapport à l'autre*
- *si p et q sont tous les deux de la forme $4k+3$, on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, et ils sont l'un résidu et l'autre non-résidu l'un par rapport à l'autre.*

Démonstration. On commence par calculer $\left(\frac{q}{p}\right)$ au moyen du lemme de Gauss. Posant $S = \{1, \dots, \frac{p-1}{2}\}$, pour $s \in S$ on a

$$qs \equiv \varepsilon_s(q) s_q \mod p$$

donc

$$\frac{2\pi qs}{p} \equiv \varepsilon_s(q) \frac{2\pi s_q}{p} \mod 2\pi\mathbb{Z}$$

d'où

$$\sin \frac{2\pi qs}{p} = \varepsilon_s(q) \sin \frac{2\pi s_q}{p},$$

de sorte que

$$\left(\frac{q}{p}\right) = \prod_{s\in S} \varepsilon_s(q)$$
$$= \prod_{s\in S} \frac{\sin\frac{2\pi qs}{p}}{\sin\frac{2\pi s_q}{p}} = \frac{\prod_{s\in S}\sin\frac{2\pi qs}{p}}{\prod_{s\in S}\sin\frac{2\pi s_q}{p}} = \frac{\prod_{s\in S}\sin\frac{2\pi qs}{p}}{\prod_{s\in S}\sin\frac{2\pi s}{p}} = \prod_{s\in S}\frac{\sin\frac{2\pi qs}{p}}{\sin\frac{2\pi s}{p}}$$

où l'on a utilisé le fait que l'application $s \mapsto s_q$ était une permutation de S. On applique maintenant le lemme 2.6.5 avec $x = \frac{2\pi s}{p}$, ce qui donne

$$\frac{\sin\frac{2\pi qs}{p}}{\sin\frac{2\pi s}{p}} = (-4)^{\frac{q-1}{2}} \prod_{t\in T}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right)$$

où $T = \{1, \ldots, \frac{q-1}{2}\}$. En remplaçant dans l'équation précédente on trouve finalement

$$\left(\frac{q}{p}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{s\in S}\prod_{t\in T}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right).$$

Par symétrie on a alors aussi

$$\left(\frac{p}{q}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{s\in S}\prod_{t\in T}\left(\sin^2\frac{2\pi t}{q} - \sin^2\frac{2\pi s}{p}\right)$$

et en comparant ces deux expressions on trouve bien

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right),$$

ce qu'il fallait démontrer. □

Symbole de Jacobi

Définition 2.6.7. — Soient $m \in \mathbb{Z}$ un entier relatif et $n \in \mathbb{N}_{>0}$ un entier naturel strictement positif. On définit le symbole de Jacobi $\left(\frac{m}{n}\right) \in \{-1, 0, 1\}$ comme suit : si $n = p_1^{\nu_1} \ldots p_r^{\nu_r}$ est la décomposition de n en facteurs premiers, alors

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\nu_1} \cdots \left(\frac{m}{p_r}\right)^{\nu_r}$$

où $\left(\frac{m}{p_i}\right)$ est le symbole de Legendre, défini précédemment.

(On remarque en particulier que si $n = p$ est premier, le symbole de Jacobi coïncide avec le symbole de Legendre.)

Proposition 2.6.8. — *Le symbole de Jacobi ainsi défini vérifie les propriétés suivantes :*

1. *Pour tous $m \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$, on a*
$$\mathrm{pgcd}(m,n) \neq 1 \iff \left(\frac{m}{n}\right) = 0.$$
2. *Si $\mathrm{pgcd}(m,n) = 1$, on a l'implication*
$$m \text{ est un carré modulo } n \implies \left(\frac{m}{n}\right) = 1.$$
Si de plus $n = p$ est premier (avec toujours $\mathrm{pgcd}(m,p) = 1$), on a l'équivalence
$$m \text{ est un carré modulo } p \iff \left(\frac{m}{p}\right) = 1.$$
3. *Pour tous $m, m' \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$, on a*
$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right).$$
4. *Pour tous $m \in \mathbb{Z}$ et $n, n' \in \mathbb{N}_{>0}$, on a*
$$\left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right).$$
5. *On a*
$$m \equiv m' \mod n \implies \left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right).$$
6. *Pour tout $n > 0$ impair, on a*
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & si \quad n \equiv 1 \mod 4 \\ -1 & si \quad n \equiv 3 \mod 4. \end{cases}$$
7. *Pour tout $n > 0$ impair, on a*
$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & si \quad n \equiv 1 \text{ ou } 7 \mod 8 \\ -1 & si \quad n \equiv 3 \text{ ou } 5 \mod 8. \end{cases}$$
8. *Pour tous $m, n > 0$ impairs, on a*
$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right),$$
c'est-à-dire : $\begin{cases} \left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) & si \quad m \text{ ou } n \equiv 1 \mod 4 \\ \left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) & si \quad m \equiv n \equiv 3 \mod 4. \end{cases}$

2.7 Une autre preuve du théorème de réciprocité quadratique

$G = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$
$H = \{(1,1),(-1,-1)\}$

2.8 Exercices

Exercice 2.8.1
Soit A un anneau. Montrer l'équivalence entre :
- $1_A = 0_A$
- 0_A est inversible
- A est l'anneau nul.

Exercice 2.8.2
Construire un anneau B, un sous-anneau $A \subset B$, et un élément $a \in A$, tels que a soit diviseur de zéro dans B mais pas dans A.

Exercice 2.8.3
Soit A un anneau factoriel. Si $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$ est un polynôme non nul à coefficients dans A, on définit le contenu de P, noté $c(P)$, par la formule

$$c(P) = \mathrm{pgcd}(a_0, \ldots, a_n).$$

Montrer que pour $P, Q \in A[X]$ non nuls on a

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

En déduire que $A[X]$ est factoriel.

Pour tout entier k, montrer que l'anneau $K[X_1, \ldots, X_k]$ des polynômes en k indéterminées sur le corps K est factoriel.

Seconde partie : corps finis

Introduction à la théorie des corps finis
Brique CQFD

Hugues Randriam

10 décembre 2004

1 Prérequis et rappels sur les structures fondamentales de l'algèbre

On rappelle brièvement les définitions des structures de base de l'algèbre qu'on utilisera continuellement.

Un *groupe* est un ensemble muni d'une loi de composition interne associative qui admet un élément neutre et pour laquelle tout élément est inversible. Le groupe est dit commutatif (ou *abélien*) si sa loi l'est.

Un *anneau* est un ensemble muni de deux lois de composition interne, appelées addition et multiplication, qui vérifient les propriétés suivantes :
- l'addition définit sur l'anneau une structure de groupe abélien, dont l'élément neutre est appelé l'élément nul (ou zéro, noté 0) de l'anneau
- la multiplication est associative, admet un élément neutre (appelé élément unité de l'anneau, noté 1) et est distributive par rapport à l'addition.

L'anneau est dit commutatif si sa multiplication l'est.

Dans ce cours on n'étudiera que des anneaux commutatifs. L'algèbre non-commutative est très riche et intéressante, mais on aura déjà suffisamment à faire avec la théorie commutative. Ainsi, dans la suite du texte, et sauf mention du contraire, *tous les anneaux considérés seront commutatifs.*

Dans un anneau A, les éléments inversibles forment un groupe pour la multiplication, noté $A^\times$.

Un *corps* est un anneau dans lequel un élément est inversible si et seulement s'il est non nul (remarquons que cette définition implique $0 \neq 1$).

Un anneau A est dit *intègre* si $0 \neq 1$ et si le produit de deux éléments non nuls est non nul. Cela équivaut à demander qu'il existe un corps admettant A comme sous-anneau. Un corps minimal pour l'inclusion parmi ceux qui possèdent cette propriété est appelé *corps de fractions* de A.

Soit A un anneau. On appellera A-module la donnée d'un groupe abélien V et d'une application

$$\begin{array}{ccc} A \times V & \longrightarrow & V \\ (a, v) & \mapsto & av \end{array}$$

appelée multiplication scalaire, telle que, notant 0_A l'élément nul de A, 1_A son élément unité, et 0_V l'élément neutre de V, pour tous $a, b \in A$ et $v, w \in V$ on ait $0_A v = 0_V$, $a 0_V = 0_V$, $1_A v = v$, $(ab)v = a(bv)$, $(a+b)v = av + bv$, et $a(v+w) = av + aw$.

Dans le cas particulier où l'anneau A est un corps K, on parlera indifféremment de K-module ou de *K-espace vectoriel*.

Un *morphisme* (ou *homomorphisme*) entre deux groupes, deux anneaux, deux corps, ou deux K-espaces vectoriels, est une application entre ces deux ensembles qui respecte leurs structures (envoie élément neutre sur élément neutre, respecte addition, multiplication,...).

Exemple 1.1. — Les nombres réels forment un groupe (abélien) pour l'addition, $(\mathbb{R}, +, 0)$. Les nombres réels non nuls forment un groupe (abélien) pour la multiplication, $(\mathbb{R}^\times, \times, 1)$. L'exponentielle (peu importe la base) de $\mathbb{R}$ dans $\mathbb{R}^\times$ est un morphisme de groupes, car on a bien $\exp(0) = 1$ et $\exp(x+y) = \exp(x)\exp(y)$ pour tous x et y dans $\mathbb{R}$.

Un morphisme entre deux K-espaces vectoriels est aussi appelé une *application K-linéaire*.

Une famille d'éléments d'un K-espace vectoriel V est dite *génératrice* si tout élément de V peut s'écrire comme combinaison linéaire (finie, à coefficients dans K) d'entre eux. Une famille d'éléments de V est dite *libre* si toute combinaison linéaire non triviale de ces éléments est non nulle. Une telle famille est appelée *base* de V si elle est à la fois libre et génératrice ; cela revient à demander que tout élément de V puisse s'écrire d'une unique façon comme combinaison linéaire de ces éléments. De toute famille génératrice d'un espace vectoriel on peut extraire une base, et toute famille libre peut se compléter en une base.

Toutes les bases de V ont même cardinal (éventuellement infini), appelé *dimension* de V (sur K). Dans ce cours on considérera principalement des espaces de dimension finie.

Exemple 1.2. — Les applications K-linéaires d'un K-espace vectoriel de dimension m dans un K-espace vectoriel de dimension n forment un K-espace vectoriel de dimension mn.

Un morphisme d'un objet dans lui-même est appelé *endomorphisme*. Un morphisme bijectif (et dont l'inverse est alors aussi un morphisme) est appelé *isomorphisme*. Un morphisme qui est à la fois un endomorphisme et un isomorphisme est appelé *automorphisme*.

Exemple 1.3. — La conjugaison complexe de $\mathbb{C}$ dans lui-même est un automorphisme de corps. En effet, elle est son propre inverse, et on a bien $\overline{0} = 0$, $\overline{1} = 1$, $\overline{x+y} = \overline{x} + \overline{y}$, et $\overline{xy} = \overline{x}.\overline{y}$ pour tous x et y dans $\mathbb{C}$.

2 Généralités sur les extensions de corps

Définition 2.1. — Soit L un corps. Un *sous-corps* de L est une partie de L qui contient 0 et 1, est stable par addition et multiplication, et telle que ces opérations la munissent d'une structure de corps.

On dira de façon équivalente que K est un sous-corps de L ou que L est une *extension* de K.

Un morphisme entre deux extensions L_1 et L_2 d'un même corps K est un morphisme de corps de L_1 dans L_2 dont la restriction à K est l'identité.

Proposition 2.2. — *Soit $f : K \longrightarrow L$ un morphisme de corps. Alors f est injectif.*

Démonstration. Il suffit de montrer que si x n'est pas nul, $f(x)$ non plus. Or tout x non nul admet un inverse x^{-1}, et on a

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1_K) = 1_L \neq 0_L$$

donc $f(x) \neq 0_L$. □

Interprétation de la proposition : f injectif permet d'identifier K à son image $f(K)$ qui est un sous-corps de L ; ainsi tout morphisme de corps permet de considérer le corps d'arrivée comme une extension du corps de départ.

Si $K \subset L$ est une extension de corps, on peut considérer L comme un K-espace vectoriel : la structure de groupe abélien de ce K-espace vectoriel est définie par l'addition usuelle de L, et la multiplication scalaire $K \times L \longrightarrow L$ est définie par la restriction de la multiplication usuelle de L.

Définition 2.3. — Le *degré* de l'extension $K \subset L$, noté $[K : L]$, est la dimension de L considéré comme K-espace vectoriel :

$$[L : K] = \dim_K L.$$

Une extension de degré fini sera aussi parfois appelée une extension *finie*.

Proposition 2.4 (multiplicativité du degré)**.** — *Soient $K \subset L \subset M$ trois corps extensions l'un de l'autre. Alors*

$$[M : K] = [M : L][L : K].$$

Démonstration. Considérons des éléments $e_i \in M$ qui forment une base de M sur L et, de même, des $f_j \in L$ formant une base de L sur K. Alors tout élément $m \in M$ s'écrit de façon unique comme combinaison linéaire (finie) $m = \sum_i l_i e_i$ pour des l_i dans L, et de même chaque l_i s'écrit de façon unique $l_i = \sum_j k_{i,j} f_j$ pour des $k_{i,j}$ dans K. Ainsi m s'écrit de façon unique $m = \sum_{i,j} k_{i,j} e_i f_j$ de sorte que les $e_i f_j$ forment une base de M sur K. □

Soient $K \subset L$ une extension de corps de degré fini n, et $e_1, \ldots, e_n \in L$ une base de L sur K. Deux éléments x et y de L s'écrivent de façon unique $x = \sum_{i=1}^n \lambda_i e_i$ et $y = \sum_{i=1}^n \mu_i e_i$ avec les λ_i et μ_i dans K. Il est encore facile d'exprimer la somme de x et y dans la base : on a $x + y = \sum_{i=1}^n (\lambda_i + \mu_i) e_i$.

Pour le produit, on a $xy = \sum_{i,j=1}^n \lambda_i \mu_j e_i e_j$, et on voit qu'il peut être utile de savoir exprimer chaque produit $e_i e_j$ dans la base.

Définition 2.5. — Les constantes de structure de la base $(e_1, \ldots, e_n)$ de L sur K sont les $\alpha_{i,j,k} \in K$, pour $i, j, k \in \{1, \ldots, n\}$, définis par

$$e_i e_j = \sum_{k=1}^n \alpha_{i,j,k} e_k.$$

Avec les notations qui précèdent, on a donc

$$xy = \sum_{k=1}^n \nu_k e_k$$

avec

$$\nu_k = \sum_{i,j=1}^{n} \alpha_{i,j,k} \lambda_i \mu_j.$$

On vérifie que la commutativité de la multiplication implique

$$\alpha_{i,j,k} = \alpha_{j,i,k}$$

et l'associativité

$$\sum_{p=1}^{n} \alpha_{i,j,p} \alpha_{p,k,l} = \sum_{q=1}^{n} \alpha_{i,q,l} \alpha_{j,k,q}$$

pour tous i, j, k, l. L'existence d'un élément unité et de l'inverse peuvent s'exprimer dans les mêmes termes.

Exemple 2.6. — Prenant $K = \mathbb{R}$ et $L = \mathbb{C}$ on a $n = [\mathbb{C} : \mathbb{R}] = 2$, et choisissant la base formée de $e_1 = 1$ et $e_2 = i = \sqrt{-1}$ on trouve $\alpha_{1,1,1} = \alpha_{1,2,2} = \alpha_{2,1,2} = 1$, $\alpha_{1,1,2} = \alpha_{1,2,1} = \alpha_{2,1,1} = \alpha_{2,2,2} = 0$, et $\alpha_{2,2,1} = -1$.

La multiplication de L pouvant se lire sur les constantes de structure, il importe de trouver une base pour laquelle celles-ci sont particulièrement simples.

Définition 2.7. — Soit L une extension finie de K, de degré n. On dit que L est une extension *élémentaire*, ou *simple* (ou encore parfois *primitive*), de K s'il existe $x \in L$ tel que $(1, x, x^2, \ldots, x^{n-1})$ soit une base de L sur K.

On dit alors que x est un *générateur* de L sur K.

Quelques remarques :

- La définition équivaut à demander qu'il existe un élément $x \in L$ tel que les éléments de L soient exactement les valeurs en x des polynômes à coefficients dans K de degré inférieur ou égal à $n - 1$.
- En particulier l'élément x^n de L doit être égal à la valeur en x d'un polynôme à coefficients dans K de degré inférieur ou égal à $n - 1$: il existe $a_0, a_1, \ldots, a_{n-1} \in K$ tels que $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Notant alors $P(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$, on a $P(x) = 0$.
- Si $y = F(x) \in L$ et $z = G(x) \in L$, alors $y+z = (F+G)(x)$ et $yz = H(x)$ où H est le reste de la division euclidienne de FG par P. En effet, si $FG = PQ + H$, on a $yz = F(x)G(x) = P(x)Q(x) + H(x) = H(x)$ puisque $H(x) = 0$.

Définition 2.8. — Soient K un corps et $P \in K[X]$ un polynôme de degré n. L'*anneau quotient* $K[X]/P$ est construit comme suit :

- en tant que groupe abélien, c'est l'ensemble des polynômes à coefficients dans K de degré inférieur ou égal à $n-1$, muni de l'addition usuelle ;
- si F et G sont deux éléments de $K[X]/P$, leur produit dans $K[X]/P$ est le reste de la division euclidienne par P du produit usuel FG.

Des remarques qui précèdent il découle immédiatement le résultat suivant :

Lemme 2.9. — *Soient $K \subset L$ une extension élémentaire de degré n et x un générateur de L sur K. Il existe alors un polynôme $P \in K[X]$ de degré n annulant x, et l'application de $K[X]/P$ dans L qui envoie F sur $F(x)$ est un isomorphisme d'anneaux.*

On peut encore préciser le lemme comme suit.

Théorème 2.10. — *Soit K un corps.*

1. *Soit $P \in K[X]$ un polynôme de degré n. Les assertions suivantes sont équivalentes :*
   - *l'anneau quotient $K[X]/P$ est intègre*
   - *le polynôme P est irréductible*
   - *l'anneau quotient $K[X]/P$ est un corps.*

   Si l'une de ces conditions équivalentes est vérifiée, $K[X]/P$ est alors une extension élémentaire de K, de degré n.
2. *Inversement, si L est une extension finie de K, alors L est élémentaire si et seulement s'il existe un polynôme* irréductible *$P \in K[X]$ tel que L soit isomorphe à $K[X]/P$ en tant qu'extension de K (on peut choisir par exemple le polynôme P et l'isomorphisme donnés dans le lemme).*

Démonstration. Supposons $K[X]/P$ intègre et P non irréductible, de sorte que $P = FG$ avec $\deg F \leq n-1$ et $\deg G \leq n-1$. Le produit de F et G dans $K[X]/P$ est le reste de la division euclidienne par P du produit usuel FG, c'est-à-dire 0. Puisque $K[X]/P$ est supposé intègre, on doit donc avoir $F = 0$ ou $G = 0$, ce qui est absurde. Si maintenant P est irréductible et si A est un polynôme non nul de degré inférieur ou égal à $n-1$, alors le théorème de Bézout fournit B et Q de degrés inférieurs ou égaux à $n-1$ et tels que $AB + PQ = 1$, de sorte que B est un inverse de A dans $K[X]/P$. Ainsi $K[X]/P$ est un corps. Tout corps étant intègre, on a démontré l'équivalence

des trois assertions. Ceci étant fait, $K[X]/P$ est une extension élémentaire de K puisqu'elle admet X comme générateur.

Si maintenant L est une extension élémentaire de K, x un générateur, et P un polynôme de degré n qui annule x, l'application donnée dans le lemme étant un isomorphisme d'anneaux, et L étant un corps, $K[X]/P$ est aussi un corps, de sorte que l'irréductibilité de P résulte de la première partie du théorème. L'isomorphisme entre $K[X]/P$ et L est alors un isomorphisme de corps, et puisqu'il laisse les éléments de K inchangés, c'est même un isomorphisme d'extensions de K. □

Pour l'étude de la structure de $K[X]/P$ pour un polynôme P quelconque, on consultera l'exercice 7.1.

Proposition 2.11. — *Soient $K \subset L$ une extension finie de corps et x un élément de L. Alors il existe un unique polynôme irréductible P à coefficients dans K et de coefficient dominant 1 qui annule x.*

Si l'on note $K[x]$ le plus petit sous-anneau de L qui contient K et x, alors $K[x]$ est un corps, et plus précisément c'est une extension élémentaire de K isomorphe à $K[X]/P$.

Démonstration. Notons n le plus petit entier naturel tel que $(1, x, \ldots, x^{n-1})$ soit une famille libre dans le K-espace vectoriel L (on a donc $n \leq [L : K]$). Alors x^n est combinaison linéaire à coefficients dans K de ces éléments : $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Alors on a $P(x) = 0$ où $P(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$, et $K[x]$ s'identifie à $K[X]/P$. Cet anneau étant intègre (puisque sous-anneau d'un corps), l'irréductibilité de P et le reste de la proposition découlent du théorème précédent. □

Définition 2.12. — Le polynôme irréductible P ainsi défini dans la proposition est appelé le polynôme minimal de x sur K.

Un polynôme à coefficients dans K annule x si et seulement s'il est multiple de P.

Proposition 2.13. — *Toute extension finie de corps s'obtient par composition d'extensions élémentaires.*

Démonstration. On procède par récurrence. Soit $K \subset L$ une extension finie de corps. Si $L = K$, l'assertion à prouver est triviale. Sinon, soit $x \in L$, $x \notin K$. Alors on a $K \subset K[x] \subset L$ où $K[x]$ est une extension élémentaire de

K, et où L est une extension de $K[x]$ de degré strictement inférieur à $[L : K]$. On peut donc conclure en appliquant l'hypothèse de récurrence à l'extension $K[x] \subset L$. □

Si L est une extension finie de K et si $x_1, \ldots, x_r \in L$, on note $K[x_1, \ldots, x_r]$ le plus petit sous-anneau de L qui contient K et $x_1, \ldots, x_r$. Les faits qui précèdent et une récurrence immédiate montrent que $K[x_1, \ldots, x_r]$ est un corps. On dit que c'est le sous-corps de L engendré par $x_1, \ldots, x_r$ sur K.

Proposition 2.14. — *Soient K un corps et $P \in K[X]$ un polynôme non constant. Alors il existe une extension finie L de K dans laquelle P admet une racine.*

Démonstration. Sans perte de généralité on peut supposer P irréductible. Alors l'extension élémentaire $L = K[X]/P$ de K convient, puisque l'élément X de L est bien racine de P. □

Proposition 2.15. — *Soient K un corps et $P \in K[X]$ un polynôme de degré $r \geq 1$. Alors il existe une extension finie L de K dans laquelle P se décompose en produit de facteurs linéaires : il existe $c \in K$ et $\alpha_1, \ldots, \alpha_r \in L$ tels que*

$$P(X) = c(X - \alpha_1) \ldots (X - \alpha_r).$$

Démonstration. On procède par récurrence sur r. Par la proposition précédente il existe une extension finie K_1 de K telle que P admette une racine α_1 dans K_1. Notant alors $P(X) = (X - \alpha_1)P_1(X)$ avec $P_1 \in K_1[X]$, on conclut en appliquant l'hypothèse de récurrence avec K_1 et P_1 à la place de K et P. □

Définition 2.16. — On appelle *corps de décomposition* de P sur K une extension L de K de degré minimal dans laquelle P se décompose en produit de facteurs linéaires.

Avec les notations de la proposition, la minimalité du degré signifie que le corps de décomposition L est engendré par les racines de P : on a $L = K[\alpha_1, \ldots, \alpha_r]$.

Proposition 2.17. — *Soit $\sigma : K_1 \xrightarrow{\sim} K_2$ un isomorphisme de corps, P_1 un polynôme non constant à coefficients dans K_1, $P_2 = \sigma(P_1)$, L_1 un corps de décomposition de P_1 sur K_1 et L_2 un corps de décomposition de P_2*

sur K_2. Alors L_1 et L_2 sont isomorphes, et plus précisément, il existe un isomorphisme de L_1 sur L_2 qui étend σ.

En particulier, prenant $K_1 = K_2 = K$ et σ l'identité, on voit que le corps de décomposition d'un polynôme est unique (à isomorphisme près).

Démonstration. On procède par récurrence sur le degré de P_1. Soit Q_1 un facteur irréductible de P_1. Par définition d'un corps de décomposition, Q_1 admet une racine x_1 dans L_1, et $Q_2 = \sigma(P_2)$ une racine x_2 dans L_2. Par la proposition 2.11, $K_1' = K_1[x_1]$ est naturellement isomorphe à $K_1[X]/P_1$, et $K_2' = K_2[x_2]$ à $K_2[X]/P_2$, les isomorphismes envoyant x_1 et x_2 sur X. L'isomorphisme σ de K_1 sur K_2 s'étend naturellement en un isomorphisme de $K_1[X]/P_1$ sur $K_2[X]/P_2$, et donc de K_1' sur K_2', noté σ', qui vérifie $\sigma'(x_1) = x_2$. Ecrivant $P_1(X) = (X - x_1)R_1(X)$ avec $R_1 \in K_1'[X]$, $P_2(X) = (X - x_2)R_2(X)$ avec $R_2 = \sigma'(R_1) \in K_2'[X]$, et remarquant que L_1 est un corps de décomposition de R_1 sur K_1', et L_2 de R_2 sur K_2', on peut conclure en appliquant l'hypothèse de récurrence. □

3 Construction des corps finis et étude de leurs propriétés élémentaires

On supposera connue la théorie des anneaux quotient $\mathbb{Z}/n\mathbb{Z}$, en particulier le fait que $\mathbb{Z}/n\mathbb{Z}$ est intègre (et même, est un corps) si et seulement si n est un nombre premier.

Proposition 3.1. — *Soit K un corps. Alors ou bien K est une extension du corps $\mathbb{Q}$ des nombres rationnels, ou bien K est une extension de $\mathbb{Z}/p\mathbb{Z}$ pour un nombre premier p uniquement déterminé.*

Définition 3.2. — Dans le premier cas de la proposition on dit que K est de caractéristique 0, et dans le second que K est de caractéristique p.

Démonstration. On dispose naturellement d'un homomorphisme d'anneaux f de $\mathbb{Z}$ dans K qui envoie $1 \in \mathbb{Z}$ sur l'élément unité de K. Si f est injectif, alors K contient son image $f(\mathbb{Z})$ qui est isomorphe à $\mathbb{Z}$, et son corps de fractions qui est isomorphe à $\mathbb{Q}$. Sinon il existe un plus petit entier non nul p tel que $f(p) = 0$. Alors l'image $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et est intègre (puisque sous-anneau d'un corps), de sorte que p est premier. □

Proposition 3.3. — *Soit K un corps fini. Alors le cardinal de K est une puissance d'un nombre premier. Plus précisément, il existe p premier tel que K soit une extension de $\mathbb{Z}/p\mathbb{Z}$, et le cardinal de K vaut p^r où $r = [K : \mathbb{Z}/p\mathbb{Z}]$ est le degré de cette extension.*

Démonstration. Le corps K étant fini, il ne peut contenir $\mathbb{Q}$, donc est nécessairement extension d'un $\mathbb{Z}/p\mathbb{Z}$. Notant $r = [K : \mathbb{Z}/p\mathbb{Z}]$, K est alors un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension r, donc de cardinal p^r. □

Lemme 3.4. — *Soit K un corps de caractéristique p. Alors pour tous $a, b \in K$ on a $(a+b)^p = a^p + b^p$, et plus généralement, pour tout entier $r \geq 1$,*

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}.$$

Démonstration. La formule du binôme donne

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Or, pour $1 \leq i \leq p-1$, l'entier $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ est divisible par p donc nul dans $\mathbb{Z}/p\mathbb{Z}$. Ceci prouve le cas $r = 1$ du lemme, et le cas général en découle par une récurrence évidente. □

Théorème 3.5. — *Soient p un nombre premier et $r \geq 1$ un entier.*

1. *Le corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p^r.*
2. *Inversement, si K est un corps fini de cardinal p^r, alors K est corps de décomposition de $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Plus précisément, les racines de $X^{p^r} - X$ sont exactement les éléments de K avec multiplicité 1.*

Démonstration. Notons K le corps de décomposition de $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$, de sorte qu'on ait

$$X^{p^r} - X = \prod_{i=1}^{p^r} (X - \alpha_i)$$

pour des $\alpha_i \in K$ qui engendrent K sur $\mathbb{Z}/p\mathbb{Z}$.

Montrons d'abord que les α_i sont tous distincts (*i.e.* que $X^{p^r} - X$ est à racines simples). Dans le cas contraire, si $\alpha_i = \alpha_j = \alpha$, alors on peut écrire

$$X^{p^r} - X = (X - \alpha)^2 Q(X)$$

d'où en dérivant et en utilisant le fait que p est nul dans $\mathbb{Z}/p\mathbb{Z}$,

$$-1 = p^r X^{p^r-1} - 1 = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X),$$

de sorte que $(X-\alpha)$ divise 1, ce qui est absurde.

Les α_i forment donc p^r éléments deux à deux distincts de K. Montrons maintenant que l'ensemble E des α_i est un sous-corps de K (d'où l'on déduira, par minimalité du corps de décomposition, que ce sous-corps est K tout entier). On a clairement $0^{p^r} = 0$ et $1^{p^r} = 1$, donc 0 et 1 font bien partie de E. Par le lemme, si α et β sont dans E, alors

$$(\alpha+\beta)^{p^r} = \alpha^{p^r} + \beta^{p^r} = \alpha + \beta,$$

donc $\alpha + \beta \in E$. De la même façon, $(\alpha\beta)^{p^r} = \alpha^{p^r}\beta^{p^r} = \alpha\beta$ donc $\alpha\beta \in E$. Ainsi E est stable par addition et multiplication. Si $\alpha \in E$ est non nul, alors $(\alpha^{-1})^{p^r} = (\alpha^{p^r})^{-1} = \alpha^{-1}$, donc $E \setminus \{0\}$ est stable par inverse. Enfin, reste à voir que si α est dans E, alors $-\alpha$ aussi. Si $p = 2$ c'est évident, puisqu'alors $-\alpha = \alpha$, et sinon p est impair, de sorte que $(-\alpha)^{p^r} = -\alpha^{p^r} = -\alpha$, ce qu'il fallait démontrer. Ceci termine la preuve de la première assertion du théorème.

Soit maintenant K un corps de cardinal p^r. Alors $K^\times$ est un groupe abélien de cardinal $p^r - 1$, donc par le théorème de Lagrange tout élément x de $K^\times$ vérifie $x^{p^r-1} = 1$. Ainsi tout élément non nul de K est racine de $X^{p^r-1} - 1$, donc de $X^{p^r} - X$. Par ailleurs 0 est aussi clairement racine de $X^{p^r} - X$. Les p^r éléments distincts de K sont donc tous racines de $X^{p^r} - X$, qui est de degré p^r, de sorte qu'on peut écrire

$$X^{p^r} - X = \prod_{x \in K} (X - x),$$

et K est bien corps de décomposition de $X^{p^r} - X$. □

Corollaire 3.6. — *Tout corps fini est de cardinal une puissance d'un nombre premier. Inversement, si $q = p^r$ est une puissance d'un nombre premier, il existe un corps fini de cardinal q, et celui-ci est unique à isomorphisme près.*

Démonstration. C'est une conséquence immédiate du théorème, l'unicité résultant de l'unicité du corps de décomposition. □

On notera $\mathbb{F}_q$, ou parfois aussi $GF(q)$, l'unique corps à q éléments. Si $q = p$ est un nombre premier, on a donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On prendra garde à l'inverse que si $q = p^r$ avec $r \geq 2$, alors $\mathbb{F}_q$ n'est pas isomorphe à $\mathbb{Z}/q\mathbb{Z}$, ce dernier anneau n'étant même pas intègre.

Décrivons explicitement $\mathbb{F}_q$ pour les petites valeurs de q :

– $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

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

– $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\} = \{0, 1, -1\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

– $\mathbb{F}_4$ n'est pas égal à $\mathbb{Z}/4\mathbb{Z}$! En tant que corps de caractéristique 2, il contient $\mathbb{F}_2 = \{0, 1\}$, et deux autres éléments, qu'on notera α et β. On vérifie que les seules tables d'addition et de multiplication possibles sont les suivantes :

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

On vérifie que ces opérations sont associatives et commutatives et que la multiplication est distributive par rapport à l'addition. Le corps $\mathbb{F}_4$ est bien corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$ puisqu'on a $0^4 = 0$, $1^4 = 1$, $\alpha^4 = \alpha$ et $\beta^4 = \beta$, de sorte que

$$X^4 - X = X(X - 1)(X - \alpha)(X - \beta).$$

On vérifie enfin qu'on a $\alpha^2 = \alpha + 1$, de sorte que α est racine de $X^2 + X + 1$ (l'autre racine est β), d'où l'on tire une représentation

$$\mathbb{F}_4 \simeq \mathbb{F}_2[X]/X^2 + X + 1.$$

– $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$
– Il n'y a pas de corps de cardinal 6.
– $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$
– $\mathbb{F}_8$ est une extension de degré 3 de $\mathbb{F}_2$, qu'on va décrire plus précisément.

Considérons un élément $x \in \mathbb{F}_8 \setminus \mathbb{F}_2$, et notons $K = \mathbb{F}_2[x]$. On a alors $[K : \mathbb{F}_2] > 1$ et $[\mathbb{F}_8 : K][K : \mathbb{F}_2] = [\mathbb{F}_8 : \mathbb{F}_2] = 3$, donc nécessairement $[K : \mathbb{F}_2] = 3$, et $K = \mathbb{F}_8$. Ainsi $\mathbb{F}_8$ est une extension élémentaire de $\mathbb{F}_2$, et tout élément de $\mathbb{F}_8 \setminus \mathbb{F}_2$ en est un générateur ; le polynôme minimal P d'un tel élément est irréductible de degré 3 sur $\mathbb{F}_2$, et on a alors $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/P$.

Quels sont les polynômes irréductibles de degré 3 sur $\mathbb{F}_2$? Il y a 8 polynômes de degré 3 sur $\mathbb{F}_2$, parmi lesquels 6 sont multiples de X ou de $X+1$. Éliminant ceux-ci, il reste X^3+X+1 et X^3+X^2+1, qui sont irréductibles. On dispose donc de deux isomorphismes,

$$\mathbb{F}_8 \simeq \mathbb{F}_2[X]/X^3+X+1 \qquad \text{et} \qquad \mathbb{F}_8 \simeq \mathbb{F}_2[X]/X^3+X^2+1,$$

qui vont donner deux descriptions différentes du même corps $\mathbb{F}_8$.

Notons α une racine de X^3+X+1 dans $\mathbb{F}_8$. Les éléments de $\mathbb{F}_8$ sont les polynômes en α de degré au plus 2 :

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}.$$

Utilisant la relation $\alpha^3 = \alpha+1$ on peut décomposer successivement les puissances de α dans la base $(1, \alpha, \alpha^2)$ de $\mathbb{F}_8$ sur $\mathbb{F}_2$. On peut aussi faire la même chose en partant d'une racine β de X^3+X^2+1, qui vérifie donc $\beta^3 = \beta^2+1$.

On trouve :

	α^2	α	1
1	0	0	1
α	0	1	0
α^2	1	0	0
α^3	0	1	1
α^4	1	1	0
α^5	1	1	1
α^6	1	0	1

	β^2	β	1
1	0	0	1
β	0	1	0
β^2	1	0	0
β^3	1	0	1
β^4	1	1	1
β^5	0	1	1
β^6	1	1	0

et $\alpha^7 = \beta^7 = 1$.

Le corps $\mathbb{F}_8$ étant unique à isomorphisme près, ces deux descriptions doivent être équivalentes. On vérifie que les racines de X^3+X+1 sont $\{\alpha, \alpha^2, \alpha^4\}$, et celles de X^3+X^2+1, $\{\alpha^3, \alpha^5, \alpha^6\}$. On peut donc prendre pour β n'importe lequel de ces trois derniers éléments. Choisissant par exemple le premier, on voit que la correspondance $\beta \mapsto \alpha^3$, $\beta^2 \mapsto \alpha^6$, $\beta^3 \mapsto \alpha^2$, $\beta^4 \mapsto \alpha^5$, $\beta^5 \mapsto \alpha$, $\beta^6 \mapsto \alpha^4$ respecte l'addition et la multiplication, de sorte que les écritures en termes de α et en termes de β sont bien deux représentations équivalentes de la même structure de corps.

4 Polynômes primitifs et structure multiplicative des corps finis

Un phénomène agréable dans l'exemple étudié précédemment est que tous les éléments de $\mathbb{F}_8^*$ sont des puissances de α. L'exponention $i \mapsto \alpha^i$ définit un morphisme surjectif de groupes de $\mathbb{Z}$ sur $\mathbb{F}_7^*$ qui, puisque α est d'ordre 7, définit par passage au quotient un isomorphisme

$$\begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathbb{F}_8^* \\ i \mod 7 & \mapsto & \alpha^i. \end{array}$$

Plus généralement :

Définition 4.1. — Soient q une puissance d'un nombre premier et $\mathbb{F}_q$ le corps fini à q éléments. On dira qu'un élément $\gamma \in \mathbb{F}_q$ est (multiplicativement) *primitif* s'il est d'ordre $q-1$ dans $\mathbb{F}_q^*$.

Puisque $\mathbb{F}_q^*$ est d'ordre $q-1$, cela revient à demander que tout élément non nul de $\mathbb{F}_q$ soit une puissance de γ, ou encore que l'application d'exponentiation

$$\begin{array}{ccc} \mathbb{Z}/(q-1)\mathbb{Z} & \longrightarrow & \mathbb{F}_q^* \\ i \mod q-1 & \mapsto & \gamma^i \end{array}$$

soit un isomorphisme de groupes. L'isomorphisme inverse est appelé logarithme en base γ :

$$\log_\gamma : \mathbb{F}_{q-1}^* \xrightarrow{\sim} \mathbb{Z}/(q-1)\mathbb{Z}.$$

Proposition 4.2. — *Soient p un nombre premier et $n \geq 1$ un entier. On suppose que $\mathbb{F}_{p^n}$ admet un élément primitif γ. Alors $\mathbb{F}_{p^n}$ est une extension élémentaire de $\mathbb{F}_p$ et γ en est un générateur. En particulier, le polynôme minimal de γ est de degré n.*

Définition 4.3. — Un polynôme de degré n à coefficients dans $\mathbb{F}_p$ est dit *primitif* s'il est polynôme minimal d'un élément primitif de $\mathbb{F}_{p^n}$.

Remarquons qu'un polynôme primitif est donc par définition irréductible.

Lemme 4.4. — *Soient G un groupe abélien et $m_1, \ldots, m_n$ des entiers deux à deux premiers entre eux. Si, pour tout i, G contient un élément d'ordre m_i, alors G contient un élément d'ordre $m_1 \ldots m_n$.*

Définition 4.5. — Soit G un groupe abélien fini. On appelle *exposant* de G, noté $\omega(G)$, le plus petit commun multiple des ordres des éléments de G :

$$\omega(G) = \operatorname*{ppcm}_{g \in G} \omega(g).$$

Lemme 4.6. — *Soit G un groupe abélien fini. Alors G admet un élément d'ordre $\omega(G)$.*

On rappelle qu'un groupe abélien fini G est dit cyclique s'il est isomorphe au groupe $\mathbb{Z}/\#G\mathbb{Z}$. Cela revient à demander que G possède un élément d'ordre $\#G$.

Théorème 4.7. — *Soit G un groupe abélien fini tel que pour tout n divisant $\#G$, il y ait dans G au plus n éléments d'ordre divisant n. Alors G est cyclique.*

Corollaire 4.8. — *Soit K un corps. Alors tout sous-groupe fini de K^* est cyclique.*

Corollaire 4.9. — *Tout corps fini admet un élément primitif. Pour tout nombre premier p et pour tout entier $n \geq 1$, il existe un polynôme primitif (donc, a fortiori, irréductible) de degré n à coefficients dans $\mathbb{F}_p$.*

Blah table de Zech.
Blah sous-groupes de puissances.

5 Extensions de corps finis : propriétés relatives, Frobenius, racines conjuguées, norme et trace

On a vu que tout corps fini contenait un sous-corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On se propose maintenant d'étudier les extensions $\mathbb{F}_q \subset \mathbb{F}_{q'}$ de corps finis en général.

Lemme 5.1. — *Soient m et n deux entiers naturels, m supposé non nul, et r le reste de la division euclidienne de n par m. Alors dans $\mathbb{Z}[X]$ on a*

$$X^n - 1 \equiv X^r - 1 \mod X^m - 1.$$

Démonstration. Écrivons $n = dm + r$. Alors

$$\begin{aligned}(X^n - 1) - (X^r - 1) &= X^n - X^r \\ &= X^r(X^{dm} - 1) \\ &= X^r(X^m - 1)(X^{(d-1)m} + X^{(d-2)m} + \cdots + X^m + 1)\end{aligned}$$

est bien divisible par $X^m - 1$. □

Lemme 5.2. — *Soient m, n et p trois entiers naturels, m et p non nuls. Alors $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si m divise n.*

Démonstration. Simplifiant par X, la première condition équivaut à demander que $X^{p^m-1} - 1$ divise $X^{p^n-1} - 1$, ce qui par le lemme précédent èquivaut à ce que $p^m - 1$ divise $p^n - 1$. Appliquant à nouveau ce lemme, en évaluant en p les polynômes considérés, on trouve

$$p^n - 1 \equiv p^r - 1 \mod p^m - 1,$$

de sorte que $p^m - 1$ divise $p^n - 1$ si et seulement si m divise n. □

Théorème 5.3. — *Soient p un nombre premier, n un entier non nul, $q' = p^n$, et q un entier naturel. Alors $\mathbb{F}_{q'}$ admet un sous-corps de cardinal q si et seulement si $q = p^m$ avec m divisant n (i.e. si et seulement si q' est une puissance de q), et un tel sous-corps est alors unique : ses éléments sont les racines de $X^q - X$.*

Corollaire 5.4. — *Soient q une puissance d'un nombre premier et $d \geq 1$ un entier naturel. Alors $\mathbb{F}_q$ admet une extension élémentaire de degré d (isomorphe à $\mathbb{F}_{q^d}$). Autrement dit, $\mathbb{F}_q[X]$ admet des polynômes irréductibles en tout degré.*

Démonstration. En effet, q^d est encore une puissance de nombre premier, et par le théorème, $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{q^d}$. Ceci étant, n'importe quel élément primitif de $\mathbb{F}_{q^d}^*$ engendre alors $\mathbb{F}_{q^d}$ comme extension de $\mathbb{F}_q$. □

Exemple 5.5. — Les corps $\mathbb{F}_4$ et $\mathbb{F}_8$ sont des extensions de $\mathbb{F}_2$, mais il n'existe pas d'inclusion de $\mathbb{F}_4$ dans $\mathbb{F}_8$. Le plus petit corps fini contenant simultanément $\mathbb{F}_4$ et $\mathbb{F}_8$ est $\mathbb{F}_{64}$.

Soient q une puissance d'un nombre premier et $d \geq 1$ un entier naturel. Considérons l'application

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{q^d} & \longrightarrow & \mathbb{F}_{q^d} \\ & x & \mapsto & x^q. \end{array}$$

On a alors $\varphi(0) = 0$, $\varphi(1) = 1$ et, pour tous $x, y \in \mathbb{F}_{q^d}$, $\varphi(x+y) = x + y$ et $\varphi(xy) = \varphi(x)\varphi(y)$ (l'avant-dernière égalité résultant du lemme 3.4). Ainsi φ est un endomorphisme du corps $\mathbb{F}_{q^d}$. Ceci implique que φ est injectif (proposition 2.2), donc bijectif puisque $\mathbb{F}_{q^d}$ est fini. En fait pour tout $x \in \mathbb{F}_{q^d}$ on a $\varphi^d(x) = x^{q^d} = x$, de sorte que φ^d est l'identité de $\mathbb{F}_{q^d}$, et l'on voit que l'inverse de φ est φ^{d-1}. Remarquons par ailleurs que $\mathbb{F}_{q^d}$ contient $\mathbb{F}_q$ comme sous-corps, et qu'un élément x de $\mathbb{F}_{q^d}$ appartient à $\mathbb{F}_q$ si et seulement s'il vérifie $x^q = x$, autrement dit, si et seulement s'il est laissé invariant par φ. Les éléments de $\mathbb{F}_q$ étant invariants sous φ, on conclut que φ est un automorphisme de $\mathbb{F}_{q^d}$ vu comme extension de $\mathbb{F}_q$.

Définition 5.6. — L'application ainsi définie, notée $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q}$ ou $\mathrm{Frob}_{\mathbb{F}_{q^d}/\mathbb{F}_q}$, est appelée automorphisme de Frobenius de $\mathbb{F}_{q^d}$ sur $\mathbb{F}_q$.

Proposition 5.7. — *Les corps intermédiaires entre $\mathbb{F}_q$ et $\mathbb{F}_{q^d}$ sont les $\mathbb{F}_{q^k}$ pour k divisant d. Pour un tel k on a*

$$\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_{q^k}} = (\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q})^k$$

et un élément x de $\mathbb{F}_{q^d}$ appartient à $\mathbb{F}_{q^k}$ si et seulement s'il est invariant sous $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_{q^k}}$, autrement dit, s'il vérifie $x^{q^k} = x$.

Démonstration. C'est une conséquence directe du théorème 5.3 et de la définition du Frobenius. □

Lemme 5.8. — *Soit φ un automorphisme d'une extension L d'un corps K. Alors pour tous $P \in K[X]$ et $x \in L$ on a*

$$\varphi(P(x)) = P(\varphi(x)).$$

Démonstration. Notons $P(X) = \sum_i a_i X^i$, avec $a_i \in K$, de sorte que $\varphi(a_i) =$

a_i. Alors

$$\begin{aligned}\varphi(P(x)) &= \varphi(\sum_i a_i x^i) \\ &= \sum_i \varphi(a_i)\varphi(x)^i \\ &= \sum_i a_i \varphi(x)^i \\ &= P(\varphi(x)),\end{aligned}$$

ce qu'il fallait démontrer. □

Théorème 5.9. — *Soient q une puissance d'un nombre premier et $d \geq 1$ un entier.*

1. *Si x est un élément de $\mathbb{F}_{q^d}$, le plus petit entier non nul k tel que $x^{q^k} = x$ est un diviseur de d. Le polynôme*

$$P(X) = (X - x)(X - x^q)(X - x^{q^2}) \dots (X - x^{q^{k-1}}),$$

   à coefficients dans $\mathbb{F}_{q^d}$, est en fait à coefficients dans $\mathbb{F}_q$, et est irréductible sur $\mathbb{F}_q$; c'est donc le polynôme minimal de x sur $\mathbb{F}_q$.

2. *Inversement, soient $P \in \mathbb{F}_q[X]$ un polynôme irréductible, et k son degré. Alors P admet une racine x dans $\mathbb{F}_{q^d}$ si et seulement si k divise d, et alors P y admet toutes ses racines, qui sont x, x^q, ..., $x^{q^{k-1}}$.*

Démonstration. Les entiers j tels que $x^{q^j} = x$ forment un sous-groupe additif de $\mathbb{Z}$. Ce sous-groupe contenant d, son générateur positif k est un diviseur de d. Puisque $x^{q^k} = x$, le Frobenius $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q}$ induit une permutation de $\{x, x^q, \dots, x^{q^{k-1}}\}$, donc laisse P inchangé. Les éléments de $\mathbb{F}_{q^d}$ invariants sous le Frobenius étant précisément ceux qui appartiennent au sous-corps $\mathbb{F}_q$, on voit que P est bien à coefficients dans $\mathbb{F}_q$. Supposons maintenant $P = QR$ avec Q et R unitaires à coefficients dans $\mathbb{F}_q$. Puisque x est racine de P, on peut supposer par exemple x racine de Q. Alors, par le lemme (appliqué avec pour φ le Frobenius), x^q, x^{q^2}, ..., $x^{q^{k-1}}$ sont aussi racines de Q, et la minimalité de k implique que les k racines ainsi obtenues sont toutes distinctes. On a donc $Q = P$, ce qui prouve l'irréductibilité. Plaçons-nous maintenant sous les hypothèses de la seconde assertion. On peut sans perte de généralité supposer P unitaire. Si P admet une racine x dans $\mathbb{F}_{q^d}$, alors P est le polynôme

minimal de x sur $\mathbb{F}_q$, et on conclut à l'aide du point précédent. Inversement, si P est de degré k divisant d, considérons une extension $\mathbb{F}_{q^{\lambda d}}$ de $\mathbb{F}_{q^d}$ dans laquelle P admette une racine x. Alors $\mathbb{F}_q[x] \simeq \mathbb{F}_q[X]/P$ est un sous-corps de cardinal q^k de $\mathbb{F}_{q^{\lambda d}}$ et donc, par le résultat d'unicité dans le théorème 5.3, coïncide avec l'unique sous-corps de cardinal q^k de $\mathbb{F}_{q^d}$. Ainsi on a $x \in \mathbb{F}_{q^d}$, et on conclut comme précédemment. □

Corollaire 5.10. — *Les groupe des automorphismes de $\mathbb{F}_{q^d}$ au-dessus de $\mathbb{F}_q$ est cyclique de cardinal d, engendré par le Frobenius.*

Démonstration. On rappelle que $\mathbb{F}_{q^d}$ est une extension élémentaire de $\mathbb{F}_q$. Soient x un générateur de cette extension et φ un automorphisme de $\mathbb{F}_{q^d}$ au-dessus de $\mathbb{F}_q$. Tout élément de $\mathbb{F}_{q^d}$ peut s'écrire sous la forme $Q(x)$ où Q est un polynôme à coefficients dans $\mathbb{F}_q$, et alors, par le lemme, l'image de cet élément par φ est $Q(\varphi(x))$. Ainsi φ est déterminé par sa valeur en x. Mais par ailleurs, toujours par le lemme, φ doit permuter les racines du polynôme minimal de x, qui sont précisément les images de x sous les puissances du Frobenius. Ainsi φ est bien une puissance du Frobenius. □

Définition 5.11. — Soit $K \subset L$ une extension finie de corps. On dit que deux éléments de L sont *conjugués* sur K s'ils ont même polynôme minimal sur K.

Corollaire 5.12. — *Deux éléments x et y de $\mathbb{F}_{q^d}$ sont conjugués sur $\mathbb{F}_q$ si et seulement s'il existe j tel que $y = x^{q^j}$.*

Soit $K \subset L$ une extension finie de corps. Si x est un élément de L, la multiplication par x est un endomorphisme K-linéaire du K-espace vectoriel L.

Définition 5.13. — Avec ces notations, on définit la *trace* de x, notée $\mathrm{Tr}_{L/K}(x)$, et la *norme* de x, notée $\mathrm{N}_{L/K}(x)$, comme la trace et le déterminant de cette application linéaire.

Remarque 5.14. — Après choix d'une base de L sur K, la construction qui précède permet de voir les éléments de L comme des matrices carrées de taille $n = [L : K]$ à coefficients dans K, l'addition et la multiplication de L correspondant à l'addition et à la multiplication usuelle des matrices, et les éléments de $K \subset L$ s'identifiant aux matrices diagonales.

Exemple 5.15. — $\mathbb{R} \subset \mathbb{C}$

Proposition 5.16. — *Soit $K \subset L$ une extension de corps. Alors la trace est une application K-linéaire de L dans K, et la norme induit un homomorphisme de groupes de L^* dans K^*. Plus précisément, pour $\lambda \in K$ et $x, y \in L$, on a :*

- $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$
- $\mathrm{Tr}(\lambda x) = \lambda \,\mathrm{Tr}(x)$
- $\mathrm{Tr}(1) = [L : K]$
- $N(xy) = N(x)N(y)$
- $N(\lambda) = \lambda^{[L:K]}$.

Lemme 5.17. — $F \subset K \subset L$ $x \in K$ $\mathrm{Tr}_{L/F}(x) = [L : K]\,\mathrm{Tr}_{K/F}(x)$ $\mathrm{N}_{L/F}(x) = \mathrm{N}_{K/F}(x)^{[L:K]}$

Théorème 5.18. — *Trace somme puissances Frobenius, norme produit...*

Corollaire 5.19. — $F \subset K \subset L$ *corps finis* $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}$ $\mathrm{N}_{L/F} = \mathrm{N}_{K/F} \circ \mathrm{N}_{L/K}$

Définition 5.20. — caractère

Lemme 5.21 (d'indépendance des caractères)**.** —

Proposition 5.22. — *corps finis, norme et trace surjectives*

6 Algorithme de factorisation de Berlekamp

Blah.

7 Exercices

Exercice 7.1 a) Soient K un corps, F et G deux polynômes à coefficients dans K premiers entre eux, et $P = FG$. Considérons l'application

$$\begin{array}{rccc} f : & K[X]/P & \longrightarrow & K[X]/F \times K[X]/G \\ & H \mod P & \mapsto & (H \mod F, H \mod G). \end{array}$$

i. Montrer que f est un homomorphisme d'anneaux et de K-espaces vectoriels.

ii. Quel est le noyau de f ? Quelles sont les dimensions sur K des espaces de départ et d'arrivée ? En déduire que f est bijectif.

iii. Trouver des éléments de $K[X]/P$ dont l'image par f est $(1,0)$ ou $(0,1)$ (on pourra utiliser une relation de Bézout entre F et G). Expliciter l'isomorphisme inverse de f.

b) Soit $P \in K[X]$ se décomposant en produit $P = P_1^{e_1} \dots P_r^{e_r}$, les P_i étant irréductibles et deux à deux distincts, et les e_i non nuls.

i. Montrer qu'on a un isomorphisme d'anneaux et de K-espaces vectoriels
$$K[X]/P \simeq K[X]/P_1^{e_1} \times \cdots \times K[X]/P_r^{e_r}$$
qui envoie X sur $(X, \dots, X)$. Expliciter l'isomorphisme inverse.

ii. On rappelle qu'un élément a d'un anneau est dit *idempotent* s'il vérifie $a^2 = a$, ce qui équivaut à demander que la multiplication par a soit un projecteur. Montrer que le nombre d'idempotents de $K[X]/P$ est égal à 2^r (on pourra commencer par montrer que dans un anneau de la forme $K[X]/Q^e$ avec Q irréductible et $e \geq 1$, les seuls idempotents sont 0 et 1).

iii. On rappelle qu'un élément a d'un anneau est dit *nilpotent* si une certaine puissance de a est nulle. Un anneau est dit *réduit* s'il n'admet pas d'élément nilpotent non nul. Montrer que $K[X]/P$ est réduit si et seulement s'il est isomorphe à un produit de corps, ou encore si et seulement si P est sans facteurs multiples dans $K[X]$.

Exercice 7.2 a) Donner la liste des polynômes irréductibles de degré 1, 2, 3 et 4 sur $\mathbb{F}_2$.

b) Soit γ un élément de $\mathbb{F}_{16}$ racine du polynôme X^4+X+1. Écrire les puissances de γ comme des polynômes en γ de degré au plus 3 à coefficients dans $\mathbb{F}_2$. En déduire que $X^4 + X + 1$ est primitif sur $\mathbb{F}_2$.

c) Quels sont les sous-groupes du groupe multiplicatif $\mathbb{F}_{16}^*$?

d) Quels sont les sous-corps de $\mathbb{F}_{16}$?

e) Parmi les polynômes obtenus à la question a), quels sont ceux qui admettent des racines dans $\mathbb{F}_{16}$? Pour chacun, dire quelles sont ces racines.

f) Quels sont les polynômes primitifs de degré 4 sur $\mathbb{F}_2$?

g) Quel est le degré minimal possible d'un polynôme non nul à coefficients dans $\mathbb{F}_2$ qui s'annule en γ^5, γ^6 et γ^7 ?

Exercice 7.3 a) Combien y a-t-il de polynômes irréductibles de degré 3 sur $\mathbb{F}_3$? Parmi ceux-ci, combien sont-ils primitifs, et combien ne le sont-ils pas ?

b) Même question pour les polynômes de degré 5 sur $\mathbb{F}_2$.

c) Même question pour les polynômes de degré 6 sur $\mathbb{F}_2$.

d) Même question pour les polynômes de degré 12 sur $\mathbb{F}_2$.

Soit d un entier. On rappelle qu'un élément x d'un corps K est dit être une racine primitice d-ième de l'unité si on a $x^d = 1$ mais $x^c \neq 1$ pour tout diviseur strict c de d.

On définit le d-ième polynôme cyclotomique Φ_d, à coefficients dans $\mathbb{Z}$, par la formule

$$\Phi_d(X) = \frac{X^d - 1}{\text{ppcm}(X^c - 1)_{c|d, c\neq d}}.$$

On note φ la fonction indicatrice d'Euler.

Exercice 7.4 a) Montrer que Φ_d est de degré $\varphi(d)$.

b) Soit K un corps. Montrer qu'un élément x de K est une racine primitive d-ième de l'unité si et seulement si $\Phi_d(x) = 0$.

Exercice 7.5
Soient $q \geq 2$ une puissance d'un nombre premier et $n \geq 1$ un entier.

a) Notons $\mathcal{S}$ l'ensemble des polynômes irréductibles sur $\mathbb{F}_q$ de degré divisant n. Montrer :

$$\prod_{P \in \mathcal{S}} P(X) = X^{q^n} - X.$$

b) Notons $\mathcal{T}$ l'ensemble des polynômes primitifs de degré n sur $\mathbb{F}_q$. Montrer :

$$\prod_{P \in \mathcal{T}} P(X) = \Phi_{q^n - 1}(X).$$

Exercice 7.6
Soient $q \geq 2$ une puissance d'un nombre premier et d un entier premier à q. Quels sont les entiers k tels que $\mathbb{F}_{q^k}$ contienne une racine primitive d-ième de l'unité ?

Exercice 7.7
Soient $q \geq 2$ une puissance d'un nombre premier et P un polynôme à coefficients dans $\mathbb{F}_q$.

a) Soit d un diviseur de $q-1$. Notons $\mathcal{U}$ l'ensemble des racines non nulles de P dans $\mathbb{F}_q$ qui sont des puissances d-ièmes. Montrer :

$$\mathrm{pgcd}(P(X), X^{\frac{q-1}{d}} - 1) = \prod_{\alpha \in \mathcal{U}} (X - \alpha).$$

b) Soit $n \geq 1$ un entier. Notons $\mathcal{V}$ l'ensemble des racines de P dans $\mathbb{F}_{q^n}$. Montrer que le polynôme

$$\prod_{\alpha \in \mathcal{V}} (X - \alpha)$$

sur $\mathbb{F}_{q^n}$ est en fait à coefficients dans $\mathbb{F}_q$. Donner une formule permettant de calculer facilement ce polynôme.

Exercice 7.8
Soient $q \geq 2$ une puissance d'un nombre premier et n un entier. Soit x un élément primitif de $\mathbb{F}_{q^n}$. Montrer que la norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$ de x est un élément primitif de $\mathbb{F}_q$.

Exercice 7.9
Factoriser le polynôme

$$X^{11} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^3 + X + 1$$

sur $\mathbb{F}_2$.