THÉORIE ANALYTIQUE DES NOMBRES, MASTER 1

par

Antoine Ducros, d'après les notes manuscrites de Javier Fresán

Table des matières

1. Anneaux principaux : généralités

L'objectif de ce cours est d'étudier, par des méthodes en grande partie analytiques, la façon dont les nombres premiers se répartissent parmi les entiers. Les résultats que nous obtiendrons et les outils que nous emploierons seront le plus souvent très spécifiques à l'anneau $\mathbb{Z}$; cela dit un certain nombre d'énoncés et propriétés de base que nous utiliserons valent dans tout anneau principal, et c'est par ces derniers que nous allons commencer avant d'entrer dans le vif du sujet.

1.1. Divisibilité dans un anneau intègre, PGCD, PPCM. — Soit A un anneau (commutatif, unitaire) *intègre* ; cela signifie par définition que A est non nul et que le produit de deux éléments non nuls de A est toujours non nul.

1.1.1. — On dit qu'un élément a de A est *inversible* s'il existe b dans A tel que $ab = 1$; un tel b est alors unique et est noté a^{-1}. L'ensemble des éléments inversibles de A est noté $A^\times$; il contient 1, ne contient pas 0 et est stable par multiplications ; cette dernière en fait un groupe abélien. On a par exemple $\mathbb{Z}^\times = \{-1, 1\}$. On dit que A est un corps si $A^\times = A\backslash\{0\}$.

Si a et b sont deux éléments de A on dit que a divise b, et l'on écrit $a|b$, s'il existe u dans A tel que $b = au$. Supposons que ce soit le cas. Un tel u est alors unique si $a \neq 0$, par intégrité de A, et on le note b/a ; et si $a = 0$ alors $b = 0$ et n'importe quel u convient.

Supposons que $a|b$ et $b|a$. Écrivons alors $b = au$ et $a = bv$. Il vient $a = auv$, donc $a(1 - uv) = 0$. Si $a = 0$ l'égalité $b = au$ entraîne que $b = 0$. Si $a \neq 0$ l'égalité $a(1 - uv) = 0$ entraîne que $uv = 1$, par intégrité de A. Par conséquent u et v sont inversibles. Ainsi si $a|b$ et $b|a$ il existe $u \in A^\times$ tel que $b = au$. Réciproquement si un tel u existe alors $b = au$ et $a = bu^{-1}$, donc $a|b$ et $b|a$.

On dit qu'un élément a de A est *irréductible* s'il est non nul, non inversible, et si pour tout couple (b, c) d'éléments de A tels que $a = bc$ alors b ou c est inversible. Si u est un élément inversible de A alors a est irréductible si et seulement si au est irréductible.

1.1.2. — Un *idéal* de A est un sous-groupe de $(A, +)$ stable par multiplication externe par les éléments de A. Si $a \in A$ on note aA ou (a) l'ensemble des multiples de a. C'est le plus petit idéal de A contenant a ; on dit aussi que c'est l'idéal engendré par a. Un idéal de A de la forme (a) avec $a \in A$ est dit *principal* ; on dit que A lui-même est principal si tout idéal de A est principal.

Si a et b sont deux éléments de A on a a divise b si et seulement si b appartient à (a), c'est-à-dire si et seulement si $(b) \subset (a)$; attention au renversement de l'ordre ! En particulier $(a) = (b)$ si et seulement si a divise b et b divise a c'est-à-dire, par le paragraphe différent, si et seulement si il existe $u \in A^\times$ tel que $a = bu$. Le générateur d'un idéal principal est donc unique *à multiplication par un inversible près*.

Remarque 1.1.3. — Supposons donné un système de représentants $\mathscr{S}$ du quotient de A par l'action (multiplicative) de $A^\times$, c'est-à-dire un sous-ensemble de A dont l'intersection avec chaque orbite sous $A^\times$ est un singleton. Alors tout idéal principal de A a par ce qui précède un unique générateur appartenant à $\mathscr{S}$. Il y a deux exemples

importants d'anneaux dans lesquels on dispose d'un tel système $\mathscr{S}$ naturel, très utilisé en pratique : l'anneau $\mathbb{Z}$, avec $\mathscr{S} = \mathbb{N}$; et l'anneau $k[T]$ lorsque k est un corps, avec $\mathscr{S}$ égal à l'ensemble constitué des polynômes unitaires et du polynôme nul.

1.1.4. — Soit (a_i) une famille d'éléments de A. Un PGCD (plus grand commun diviseur) de la famille (a_i) est un élément d de A tel que pour tout élément a de A, on ait équivalence entre «a divise d» et «a divise a_i pour tout i».

Si d est un PGCD de la famille des (a_i), il divise lui-même chacun des a_i (puisque d divise d). Si la famille des (a_i) possède un PGCD, ce dernier est unique modulo la multiplication par un inversible : en effet si d et e sont deux PGCD de la famille (a_i) alors d divise chacun des a_i comme on vient de voir, donc d divise e ; et par symétrie, e divise d, d'où l'assertion. En raison de cette unicité, on se permet de parler, lorsqu'il existe, *du* PGCD des a_i ; mais il faut garder en tête qu'il n'est défini qu'à un inversible près, à moins qu'on ait un système $\mathscr{S}$ comme dans la remarque 1.1.3, auquel cas on peut choisir ce PGCD dans $\mathscr{S}$ et ainsi le définir sans ambiguïté aucune.

1.1.5. — Soit (a_i) une famille d'éléments de A. Un PPCM (plus petit commun multiple) de la famille (a_i) est un élément m de A tel que pour tout élément a de A, on ait équivalence entre «m divise a» et «a_i divise a pour tout i».

Si m est un PPCM de la famille des (a_i), il est lui-même multiple de chacun des a_i (puisque m divise m). Si la famille des (a_i) possède un PPCM, ce dernier est unique modulo la multiplication par un inversible : en effet si m et n sont deux PPCM de la famille (a_i) alors m est multiple de chacun des a_i comme on vient de voir, donc n divise m ; et par symétrie, m divise n, d'où l'assertion. En raison de cette unicité, on se permet de parler, lorsqu'il existe, *du* PPCM des a_i ; mais il faut garder en tête qu'il n'est défini qu'à un inversible près, à moins qu'on ait un système $\mathscr{S}$ comme dans la remarque 1.1.3, auquel cas on peut choisir ce PPCM dans $\mathscr{S}$ et ainsi le définir sans ambiguïté aucune.

1.1.6. *Un critère pour être le PGCD.* — Soit (a_i) une famille d'éléments de A. Le plus petit idéal de A contenant les a_i, qu'on appelle aussi l'idéal engendré par les a_i, est l'ensemble des sommes $\sum \lambda_i a_i$ *où les* λ_i *sont presque tous nuls, c'est-à-dire tous nuls sauf un nombre fini* (en algèbre, on ne sait faire que des sommes finies !!) ; cet idéal est aussi noté $\sum a_i A$. Soit d un diviseur commun à tous les a_i appartenant à $\sum a_i A$. Alors d est un PGCD des a_i. En effet, soit $a \in A$. Si a divise d alors a divise chacun des a_i puisque d divise chacun des a_i ; et si a divise chacun des a_i alors a divise d puisque d est par hypothèse de la forme $\sum \lambda_i a_i$. Donc d est un (ou le) PGCD des a_i.

Définition 1.1.7. — On dit que A est *euclidien* s'il existe une application $\varphi\colon A\backslash\{0\} to \mathbb{N}$ telle que pour tout couple (a, b) d'éléments de A avec b non nul il existe deux éléments q et r de A vérifiant les conditions suivantes :

- $\diamond$ $r = 0$ ou $\varphi(r) < \varphi(b)$;
- $\diamond$ $a = bq + r$.

1.1.8. *Commentaires.* — Un tel φ comme dans la définition ci-dessus est appelé un *stathme* euclidien. On dit que l'écriture $a = bq + r$ est une *division euclidienne de* a

par b, dont q est le *quotient* et r le *reste*. Remarquez qu'on ne demande pas l'unicité du couple (q, r).

1.1.9. *Exemples.* — L'anneau $\mathbb{Z}$ est euclidien, la valeur absolue étant un stathme. On a unicité du quotient et du reste si on travaille dans $\mathbb{N}$, mais pas dans $\mathbb{Z}$ en général : ainsi, $7 = 3 \cdot 2 + 1 = 4 \cdot 2 - 1$.

L'anneau $k[T]$ est euclidien, le degré est un stathme, et on a ici unicité du quotient et du reste, sans restrictions.

Lemme 1.1.10. — *Supposons A euclidien. Il est alors principal.*

Démonstration. — Choisissons un stathme euclidien $\varphi\colon A\backslash\{0\} \to \mathbb{N}$; il en existe un par hypothèse. Soit I un idéal de A. Nous allons montrer que I est principal. Si $I = \{0\}$ alors $I = (0)$ et I est principal. Supposons I non nul. L'ensemble $\varphi(I\backslash\{0\})$ est alors une partie non vide de $\mathbb{N}$, qui a donc un plus petit élément e ; soit a un élément non nul de I tel que $\varphi(a) = e$; nous allons montrer que $I = (a)$, ce qui permettra de conclure. Comme $a \in I$ on a l'inclusion $(a) \subset I$. Montrons l'inclusion réciproque. Soit $b \in I$. Comme a est non nul on peut écrire $b = aq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a) = e$. Mais puisque $r = b - aq$ et que a et b appartiennent à I, l'élément r appartient à I ; si r était non nul on aurait donc $\varphi(r) \geqslant e$ par choix de e, ce qui est exclu ; par conséquent $r = 0$ et $b = aq$. □

1.2. Propriétés des anneaux principaux. — On fixe pour ce qui suit un anneau *principal* A.

1.2.1. *Existence des PGCD.* — Soit (a_i) une famille d'éléments de A. Puisque A est principal, l'idéal $\sum_i a_i A$ est égal à (d) pour un certain d appartenant à A (unique à multiplication près par un inversible). Chacun des a_i appartient à $\sum_i a_i A$, donc est multiple de d. Il résulte alors de 1.1.6 que d est le PGCD des a_i.

Notons que par sa construction d s'écrit $\sum \lambda_i a_i$ pour une certaine famille (λ_i) d'éléments presque tous nuls de A. Une telle écriture $d = \sum \lambda_i a_i$ est appelée une *relation de Bézout* entre les a_i.

1.2.2. *Existence des PPCM.* — Soit (a_i) une famille d'éléments de A. Puisque A est principal, l'idéal $\bigcap_i a_i A$ est égal à (m) pour un certain m appartenant à A (unique à multiplication près par un inversible). Par définition un élément a de A est multiple de m si et seulement si il est multiple de tous les a_i. Autrement dit, m est le PPCM des a_i.

1.2.3. — Si (a_i) est une famille d'éléments de A on dit que les a_i sont *premiers entre eux dans leur ensemble* si le PGCD des a_i est égal à 1 (attention : en disant ça on commet un petit abus, puisque le PGCD n'est défini qu'à multiplication par un inversible près). Cela revient à demander que tout diviseur commun à tous les a_i soit un diviseur de 1, c'est-à-dire un inversible.

Comme 1 est toujours un diviseur commun à tous les a_i, il résulte de 1.1.6 que les a_i sont premiers entre eux si et seulement s'il existe une famille (λ_i) d'éléments de A presque tous nuls tels que $\sum \lambda_i a_i = 1$.

Le cas le plus fréquent sera celui d'une famille à deux éléments a et b ; on dit alors simplement que a et b sont premiers entre eux, sans rajouter l'expression «dans leur ensemble» ; celle-ci est utile à partir de trois éléments, pour éviter toute confusion avec le cas des familles d'éléments *deux à deux* premiers entre eux.

***Lemme 1.2.4* (Lemme de Gauss).** — *Soient a, b et c trois éléments de A. Supposons que a divise bc et que a est premier avec b. Alors a divise c.*

Démonstration. — Comme a divise bc on peut écrire $bc = ad$ pour un certain d dans A. Comme a est premier avec b il existe une relation de Bézout $au + bv = 1$ entre a et b. On a alors

$$c = c(au + bv) = acu + bcv = acu + adv = a(cu + dv).$$ □

Corollaire 1.2.5. — *Soit r un entier $\geqslant 0$ et soient $a_1, \ldots, a_r$ des éléments de A. Soit a un élément de A premier à chacun des a_i. Il est alors premier à leur produit.*

Démonstration. — Par une récurrence immédiate il suffit de traiter le cas où $r = 2$. Soit d un diviseur commun à a et a_1a_2. Comme d divise a, tout diviseur commun de d et a_1 est un diviseur commun de a et a_1, donc est inversible puisque a est premier avec a_1. Ainsi d est premier avec a_1. Puisqu'il divise a_1a_2, le lemme de Gauss assure que d divise a_2. C'est donc un diviseur commun de a et a_2 ; comme a est premier avec a_2, il en résulte que d est inversible. □

Corollaire 1.2.6. — *Soient a et b deux éléments premiers entre eux de A. Le PPCM de a et b est égal à ab.*

Démonstration. — Le PPCM m de a et b est multiple de a, donc s'écrit au pour un certain u. Il est multiple de b, si bien que b divise au. Puisque b est premier avec a, le lemme de Gauss assure que b divise u ; Par conséquent ab divise $au = m$. Ainsi ab divise m ; mais comme ab est un multiple commun de a et b, il est multiple de m. Il s'ensuit que $ab = m$ (à un inversible près, ce qui suffit ici). □

Lemme 1.2.7. — *Soit (a_n) une suite d'éléments de A tels que a_{n+1} divise a_n pour tout n. Il existe alors N tel que a_n soit égal à a_N à multiplication par un inversible près pour tout $n \geqslant N$.*

Démonstration. — Pour tout n notons I_n l'idéal engendré par a_n. Comme a_{n+1} divise a_n pour tout n, la suite des I_n est une suite croissante d'idéaux de A. Leur réunion I est donc un idéal de A, et est en conséquence de la forme aA pour un certain $a \in A$. Puisque $a \in I$ l'élément a appartient à I_N pour un certain N. On a alors pour tout $n \geqslant N$ les inclusions $I = aA \subset I_N \subset I_n \subset I$, si bien que $I_n = I = aA$. Ainsi $aA = a_nA$, et a s'écrit donc a_nu_n pour un certain élément inversible u_n de A. On peut dès lors écrire $a_n = au_n^{-1} = a_Nu_Nu_n^{-1}$ pour tout n, ce qui permet de conclure. □

Corollaire 1.2.8. — *Soit a un élément non nul et non inversible de A. L'élément a possède un diviseur irréductible.*

Démonstration. — On construit récursivement une suite (a_n) de diviseurs non inversibles de a par le procédé suivant. On pose $a_0 = a$. Supposons a_n construit. S'il est irréductible on pose $a_{n+1} = a_n$. Sinon on choisit pour a_{n+1} un diviseur de a_n tel que a_n/a_{n+1} soit non inversible (un tel diviseur existe par hypothèse). L'élément a_{n+1} de A divise alors a_n pour tout n, et le lemme 1.2.7 assure de ce fait que pour tout n suffisamment grand, a_n/a_{n+1} est inversible. Mais cela entraîne par construction que a_n est irréductible pour n assez grand, ce qui achève la démonstration. □

Nous allons maintenant énoncer le théorème fondamental sur la décomposition des éléments de A en produits d'irréductibles. Pour ce faire nous aurons besoin de la notion suivante : deux irréductibles p et q de A seront dit associés s'ils sont égaux à multiplication près par un inversible.

***Théorème 1.2.9* (Décomposition en irréductibles).** — *Soit a un élément non nul de A. Il existe un élément inversible ε de A et une famille $(p_1, \dots p_r)$ d'éléments irréductibles de A (avec redondance possible) tels que $a = \varepsilon p_1 \dots, p_r$. De plus cette décomposition est unique «à permutation et inversibles près» : si a possède une autre écriture $\eta q_1 \dots, q_s$ de cette forme alors $s = r$ et il existe une permutation σ de $\{1, \dots, r\}$ telle que $q_{\sigma(i)}$ et p_i soient associés pour tout i.*

Démonstration. — Commençons par l'existence. Si a est inversible il n'y a rien à faire. Sinon a possède par le corollaire précédent un diviseur irréductible p_1. Posons $a_1 = a/p_1$; on a $a = a_1 p_1$. Si a_1 est inversible, on a terminé. Sinon a_1 possède par le corollaire précédent un diviseur irréductible p_2. Posons $a_2 = a_1/p_2$; on a alors $a = a_1 p_1 = a_2 p_1 p_2$. Si a_2 est inversible, on a terminé. Sinon a_2 possède par le corollaire précédent un diviseur irréductible p_3. Posons $a_3 = a_2/p_3$...Le processus s'arrête nécessairement à un moment, sinon on aurait une suite (a_n) d'éléments non nuls de A telle que a_{n+1} divise a_n et tels que a_n/a_{n+1} soit non inversible pour tout n, contredisant le lemme 1.2.7. Autrement dit il existe r tel que a_r soit inversible, et l'on a $a = a_r p_1 \dots p_r$.

Montrons maintenant l'unicité. On raisonne par récurrence sur r. Si $r = 0$ alors $a = \varepsilon$ est inversible, donc $\eta q_1 \dots q_s$ est inversible, donc chacun des termes de ce produit est inversible. Un irréductible n'étant jamais inversible, $s = 0$ et le théorème est démontré. Supposons $r > 1$ et le résultat vrai pour $r - 1$. L'irréductible p_1 divise alors $\eta q_1 \dots q_s$. Puisque p_1 est irréductible, un diviseur de p_1 est (à un inversible près) ou bien p_1 ou bien 1 ; par conséquent le PGCD de p_1 avec chacun des q_j est ou bien p_1, ou bien 1. Si ce PGCD valait 1 pour chacun des q_j alors p_1 serait premier avec $\eta q_1 \dots q_s$ par le corollaire 1.2.5 (notez que comme η est inversible, p_1 est automatiquement premier avec η), ce qui est absurde puisque p_1 divise $\eta q_1 \dots q_s$. Il existe donc j tel que p_1 divise q_j, et comme q_j est irréductible le quotient $\alpha := q_j/p_1$ est inversible : p_1 et q_j sont associés. Quitte à permuter les q_i on peut supposer que $j = 1$. On a alors $\varepsilon p_1 \dots, p_r = \eta \alpha p_1 q_2 \dots q_s$. Il vient $\varepsilon p_2 \dots p_r = \eta \alpha q_2 \dots q_s$ (rappelons que A est intègre). L'hypothèse de récurrence permet alors de conclure que $s = r$ et qu'on peut permuter les q_i pour $i \geqslant 2$ de sorte que q_i soit associé à p_i pour tout $i \geqslant 2$, ce qui achève la démonstration. □

1.2.10. *Commentaires.* — Supposons donné un *système complet d'irréductibles* $\mathscr{P}$ de A, c'est-à-dire un ensemble d'irréductibles de A tel que tout irréductible de A soit associé à un et un seul élément de $\mathscr{P}$. Le théorème ci-dessus peut alors se récrire comme suit : tout élément non nul a de A s'écrit de manière unique à permutation près comme produit d'un inversible et d'éléments de P. Une autre façon de le dire est que pour un tel a, il existe une unique écriture $a = \varepsilon \prod_{p\in\mathscr{P}} p^{v_p}$ où ε est inversible et où les v_p sont des entiers presque tous nuls. On dit que v_p est la *valuation p-adique* de a.

Il peut être commode de remarquer que ce résultat s'étend au corps des fraction K de A : tout élément λ de $K^\times$ a une unique écriture sous la forme $\varepsilon \prod_{p\in\mathscr{P}} p^{v_p}$ où ε appartient à $A^\times$ et où les v_p sont des entiers *relatifs* presque tous nuls ; on dit encore que v_p est la valuation p-adique de λ. Un élément de $K^\times$ appartient à A si et seulement si sa valuation p-adique est positive ou nulle pour tout p.

Lemme 1.2.11 **(Lemme chinois).** — *Soient $a_1, \dots, a_r$ des éléments de A deux à deux premiers entre eux. Le morphisme d'anneaux naturel $A \to A/(a_1) \times \cdots \times A/(a_r)$ (donné sur chaque composante par le morphisme quotient) induit un isomorphisme*

$$A/(a_1 \dots a_r) \simeq A/(a_1) \times \cdots \times A/(a_r).$$

Démonstration. — Remarquons tout d'abord que si $r \geqslant 2$ alors a_1 est premier à $(a_2 \dots a_r)$ par le corollaire 1.2.5. Cette remarque couplée à un raisonnement par récurrence sur r permet de se ramener au cas où $r = 2$. Soit φ le morphisme d'anneaux naturel de A vers $A/(a_1) \times A/(a_2)$. Il induit un isomorphisme d'anneaux de $A/\operatorname{Ker}\varphi$ vers $\operatorname{Im}\varphi$; il suffit donc pour conclure de montrer que $\operatorname{Ker}\varphi = (a_1a_2)$ et que φ est surjectif.

Étudions tout d'abord $\operatorname{Ker}\varphi$. Un élément a de A appartient au noyau de φ si et seulement si a est nul modulo a_1 et modulo a_2, c'est-à-dire encore si et seulement si a est multiple de a_1 et de a_2. Cela revient à demander que a soit multiple du PPCM de a_1 et a_2, qui est égal à a_1a_2 puisque a_1 et a_2 sont premiers entre eux (1.2.6). Ainsi $\ker\varphi = (a_1a_2)$.

Montrons maintenant que φ est surjective. Choisissons une relation de Bézout $a_1u_1 + a_2u_2 = 1$. Soit x un élément de $A/(a_1) \times A/(a_2)$. Choisissons α_1 et α_2 dans A tels que $x = (\overline{\alpha_1}, \overline{\alpha_2})$. Posons $y = \alpha_1a_2u_2 + \alpha_2a_1u_1$. On a alors modulo a_1 les égalités $\overline{y} = \overline{\alpha_1a_2u_2} = \overline{\alpha_1}$ puisque $\overline{a_2u_2} = \overline{1} - \overline{a_1u_1} = \overline{1}$ modulo a_1 ; et par symétrie des arguments $\overline{y} = \overline{\alpha_2}$ modulo a_2. On a en conséquence $\varphi(y) = x$ et φ est surjective. □

Nous allons terminer cette section consacrée aux anneaux principaux généraux par une brève étude des quotients $A/(a)$.

Lemme 1.2.12. — *Soit a un élément de A.*

1. *Pour tout b dans A, la classe $\overline{b}$ est inversible dans $A/(a)$ si et seulement si b est premier avec a.*
2. *Supposons a non nul. Alors les assertions suivantes sont équivalentes :*
   (i) *$A/(a)$ est intègre ;*
   (ii) *a est irréductible ;*

(iii) *$A/(a)$ est un corps.*

Démonstration. — Commençons par (1). L'élément $\overline{b}$ de $A/(a)$ est inversible si et seulement s'il existe $v \in A$ tel que $\overline{v}\overline{b} = 1$, c'est-à-dire encore tel que $bv - 1$ soit multiple de a. Autrement dit $\overline{b}$ est inversible dans $A/(a)$ si et seulement si il existe u et v dans A tels que $bv + au = 1$, c'est-à-dire si et seulement si a et b sont premiers entre eux.

Montrons maintenant (2). Supposons $A/(a)$ intègre. L'anneau $A/(a)$ est alors non nul par définition, donc a n'est pas inversible. Soient maintenant b et c deux éléments de A tels que $bc = a$. Alors $\overline{b}\overline{c} = 0$, donc par intégrité de $A/(a)$ ou bien $\overline{b} = \overline{0}$, ou bien $\overline{c} = 0$; autrement dit ou bien b est multiple de a, ou bien c est multiple de a. Mais comme a est lui-même multiple de b et c, cela revient à dire qu'ou bien b, ou bien c, est égal à a à multiplication par un inversible près. Par conséquent ou bien c ou bien b est inversible, et a est irréductible.

Supposons maintenant que a est irréductible. Il est alors non inversible, donc $A/(a)$ est non nul. Nous allons monter que c'est un corps, c'est-à-dire que tout élément non nul de $A/(a)$ est inversible. Soit donc $b \in A$ tel que $\overline{b}$ soit non nul, c'est-à-dire tel que a ne divise pas b. Comme a est irréductible, le PGCD de a et b vaut ou bien a ou bien 1 (à inversible près). Puisque a ne divise pas b, ce PGCD vaut 1. Il résulte alors de (1) que $\overline{b}$ est inversible.

Il est enfin immédiat que si $A/(a)$ est un corps, il est intègre. □

2. Premières propriétés spécifiques de $\mathbb{Z}$

À partir de maintenant nous travaillerons essentiellement sur $\mathbb{Z}$. C'est un anneau euclidien donc principal, et il vérifie par conséquent les propriétés générales établies du chapitre précédent.

2.1. Généralités. — L'anneau $\mathbb{Z}$ présente d'emblée quelques spécificités (au sein des anneaux principaux) faciles à mettre en évidence et que nous allons décrire.

2.1.1. — La multiplication de $\mathbb{Z}$ présente la particularité d'être essentiellement une notation abrégée pour la répétition de l'addition, alors que dans les anneaux généraux les deux lois sont totalement découplées. Il en résulte qu'un sous-groupe de $\mathbb{Z}$ est automatiquement stable par multiplication par n'importe quel élément de $\mathbb{Z}$. Autrement dit, les sous-groupes de $\mathbb{Z}$ sont exactement les idéaux de $\mathbb{Z}$. Cette propriété est héritée par les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$.

2.1.2. — Le groupe $\mathbb{Z}^\times$ est $\{-1, 1\}$. L'orbite d'un élément de $\mathbb{Z}$ sous l'action multiplicative de $\mathbb{Z}^\times$ contient donc au plus deux éléments (et $\{0\}$ est la seule qui n'en contienne qu'un), et exactement un élément positif ou nul. Tout idéal de $\mathbb{Z}$ (ou tout sous-groupe de $\mathbb{Z}$) est donc de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$.

De même, tout irréductible de $\mathbb{Z}$ est associé à un unique irréductible strictement positif. Les irréductibles strictement positifs de $\mathbb{Z}$ sont traditionnellement appelés les *nombres premiers*. Nous noterons désormais $\mathscr{P}$ l'ensemble des nombres premiers. Un irréductible de $\mathbb{Z}$ est donc de la forme $\pm p$ avec $p \in \mathscr{P}$. Tout élément de $\mathbb{N}\backslash\{0\}$ s'écrit de manière unique à permutation près comme produit d'éléments de $\mathscr{P}$.

2.1.3. — Soit $n \in \mathbb{N}$. Si $n = 0$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est naturellement isomorphe à $\mathbb{Z}$ et est donc infini. Supposons $n > 0$. Par division euclidienne tout élément de $\mathbb{Z}$ possède une unique écriture sous la forme $an + b$ avec a dans $\mathbb{Z}$ et $b \in \{0, \dots, n-1\}$; il s'ensuit que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble $\{\overline{a}\}_{0 \leqslant a \leqslant n-1}$, et que les $\overline{a}$ pour $a \in \{0, \dots, n-1\}$ sont deux à deux distincts. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n.

2.1.4. *Indicateur d'Euler.* — Pour tout entier $n \geqslant 1$, on note $\Phi(n)$ le nombre d'entiers entre 0 et $n-1$ qui sont premiers à n. Par ce qui précède et en vertu du lemme 1.2.12, c'est aussi le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. On dit que $\Phi(n)$ est l'*indicateur d'Euler* de n, ou que Φ est la fonction indicatrice d'Euler.

2.1.4.1. — Soient a et b deux entiers supérieurs ou égaux à 1 et premiers entre eux. Le lemme chinois fournit un isomorphisme d'anneaux $\mathbb{Z}/(ab\mathbb{Z}) \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, qui induit un isomorphisme de groupes de $(\mathbb{Z}/ab\mathbb{Z})^\times$ vers $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. Il en résulte que $\Phi(ab) = \Phi(a)\Phi(b)$; on dit que la fonction Φ est *multiplicative*. Attention à cette acception de «multiplicative» en arithmétique : cela signifie que $\Phi(1) = 1$ et que Φ commute à la multiplication *des entiers premiers entre eux*.

2.1.4.2. — Soit m un entier strictement positif et soit p un nombre premier. Le seul facteur premier de p^m étant p, un entier d est premier à p^m si et seulement si il n'est pas multiple de p. Or il y a p^{m-1} multiples de p entre 0 et $p^m - 1$, à savoir les pk pour $0 \leqslant k \leqslant p^{m-1} - 1$. Par conséquent il y a $p^m - p^{m-1}$ entiers premiers à p entre 0

et $p^m - 1$. Autrement dit $\Phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$. Notez qu'en particulier $\Phi(p) = p - 1$.

2.1.4.3. — Soit n un entier $\geqslant 1$. Écrivons $n = \prod p_i^{n_i}$ où les p_i sont premiers et deux à deux distincts, et où les n_i sont non nuls. En vertu de ce qui précède on a

$$\Phi(n) = \prod \Phi(p_i^{n_i}) = \prod p_i^{n_i - 1}(p_i - 1).$$

2.2. Quelques faits à propos des nombres premiers. — Nous allons maintenant énoncer quelques résultats spécifiques à $\mathbb{Z}$ portant sur les nombres premiers.

Lemme 2.2.1. — *Il existe une infinité de nombres premiers.*

Démonstration. — Il suffit de démontrer que pour tout ensemble fini E de nombres premiers il existe un nombre premier q qui n'appartient pas à E. Soit donc E un sous-ensemble fini de $\mathscr{P}$. Si E est vide on peut prendre $q = 2$. Si E est non vide, posons $x = 1 + \prod_{p \in E} p$. L'élément x est > 1 car E est non vide. Il est donc non inversible et admet dès lors un facteur irréductible q. Ainsi x est nul modulo q, mais il est égal à 1 modulo p pour tout $p \in E$. Par conséquent, $q \notin E$. □

2.2.2. *Commentaires.* — Pour bien percevoir l'intérêt du lemme ci-dessus, il faut avoir conscience qu'il existe des anneaux principaux n'admettant qu'un nombre fini d'éléments irréductibles (à multiplication près par un inversible, toujours). Le cas le plus trivial est celui d'un corps : un corps est principal (ses deux idéaux sont (0) et (1)) et il n'admet *aucun* élément irréductible.

Mais donnons un exemple moins idiot, et très utile en arithmétique. Soit p un nombre premier. On note $\mathbb{Z}_{(p)}$ l'ensemble des rationnels qui peuvent s'écrire a/b avec b premier à p. C'est un sous-anneau de $\mathbb{Q}$, et on peut démontrer (exercice !) qu'il est principal et a (à inversible près) *un seul* irréductible, à savoir p.

Il a donc fallu utiliser des propriétés spécifiques de $\mathbb{Z}$ pour montrer qu'il y a une infinité de nombres premiers. Lesquelles ? Si vous lisez attentivement la preuve vous verrez que ce qui a servi c'est l'existence d'une relation d'ordre compatible avec la structure d'anneau pour laquelle tout nombre premier est > 0 et pour laquelle un élément > 1 n'est jamais inversible. Remarquez que l'ordre usuel sur $\mathbb{Q}$ induit une relation d'ordre sur $\mathbb{Z}_{(p)}$ compatible avec sa structure d'anneau, pour laquelle $p > 0$ et $1 + p > 1$. Mais comme $1 + p$ est premier à p dans $\mathbb{Z}$ il est inversible dans $\mathbb{Z}_{(p)}$, d'inverse $1/(1 + p)$. La preuve utilisée pour $\mathbb{Z}$ ne marche donc absolument pas pour $\mathbb{Z}_{(p)}$.

Lemme 2.2.3. — *Soit n un entier > 1. Si n n'est pas premier, il possède un diviseur premier inférieur ou égal à $\sqrt{n}$.*

Démonstration. — Supposons que n n'est pas premier. Il s'écrit alors comme un produit $p_1 \dots p_r$ de nombres premiers (non nécessairement deux à deux distincts) avec $r \geqslant 2$. Si p_i était strictement supérieur à $\sqrt{n}$ pour tout indice i on aurait alors $n > \sqrt{n}^r \geqslant \sqrt{n}^2 = n$, ce qui est absurde. Il existe donc i tel que $p_i \leqslant \sqrt{n}$, ce qui achève la démonstration. □

2.2.4. — Le lemme précédent fournit ainsi une méthode théorique pour construire tous les nombres premiers. Plus précisément, supposons avoir construit tous les nombres premiers inférieurs ou égaux à un certain entier n. Alors pour savoir si $n+1$ est premier il suffit de tester sa divisibilité par tous les nombres premiers déjà construits et inférieurs ou égaux à $\sqrt{n+1}$. Mais même si la borne $\sqrt{n+1}$ est bien meilleure que la borne grossière $n+1$ (qui est celle qui se présente si on applique directement les définitions sans disposer de l'estimation fournie par le lemme ci-dessus), elle reste bien trop grande pour que cet algorithme (le *crible d'Ératosthène*) soit vraiment efficace.

2.2.5. *Le but de ce cours.* — Pour tout entier (ou même tout réel positif) x, notons $\pi(x)$ le cardinal de l'ensemble des nombres premiers majorés par x. Le premier objectif de ce cours sera de démontrer le *Théorème des nombres premiers*, qui assure que $\pi(x) \simeq \frac{x}{\log x}$ quand x tend vers l'infini (ici log désignera toujours le logarithme *népérien*, de base e).

Nous verrons ensuite le *Théorème de la progression arithmétique*. Il s'énonce comme suit : soient a et N deux entiers strictement positifs premiers entre eux ; il existe une infinité de nombres premiers égaux à a modulo N(notez qu'il est indispensable que a et N soient premiers entre eux : s'ils ont un facteur commun $d > 1$ alors tout nombre égal à a modulo N est multiple de d). Nous en verrons même une version raffinée : si l'on note $\theta(x, N, a)$ l'ensemble des nombres premiers $\leqslant x$ qui sont égaux à a modulo N alors $\theta(x, N, a) \simeq \frac{x}{\Phi(N)\log x}$ quand x tend vers l'infini.

2.2.6. *Quelques commentaires sur la répartition des nombres premiers.* — On voit ainsi que la probabilité qu'un entier inférieur ou égal à x soit premier est (quand x est grand) de l'ordre de $1/\log x$; elle diminue donc avec x, mais très lentement (elle est divisée par deux quand x est élevé au carré). Donnons quelques valeurs numériques arrondies (tirées de Wikipedia) :

x	$\pi(x)$	$\log x$	$x/\pi(x)$
10	4	2.303	2.5
10^2	25	4.605	4
10^3	168	6.908	5.952
10^6	78 498	13.816	12.74
10^9	50 847 534	20.723	19.67

On peut trouver en ligne des listes impressionnantes de nombres premiers. Ainsi à l'adresse

`http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php`

figurent *tous* les nombres premiers inférieurs ou égaux à 10^{18}.

On dispose par ailleurs de méthodes permettant d'exhiber des nombres premiers absolument gigantesques (mais «isolés» : quand ces méthodes fournissent un nombre premier p, elles ne donnent en aucun cas la liste de tous ceux qui le précèdent) ; le plus grand nombre premier qu'elles ont permis d'obtenir à la date où je rédige ce passage (le 20 janvier 2026) est $2^{146\,279\,841} - 1$ (l'exposant 146 279 841 est lui-même premier) qui possède 41 024 320 chiffres en base 10, et a été découvert le 11 octobre 2024.

2.2.7. *Quelques commentaires sur le théorème de la progression arithmétique.* — Si N est un entier strictement positif, il y a $\Phi(N)$ classes d'entiers inversibles modulo N, ou encore premiers à N. Et la version raffinée du théorème de la progression arithmétique que j'ai évoquée ci-dessus, couplée au théorème des nombres premiers, assure précisément que la probabilité qu'un nombre premier donné (disons non diviseur de N) appartienne à une classe fixée d'entiers inversibles modulo N est précisément $1/\Phi(N)$. Les nombres premiers se répartissent donc de manière uniforme, sans préférence, entre toutes les classes d'entiers inversibles modulo N : par exemple si vous prenez un nombre premier «au hasard» il a autant de chances de valoir $1, 5, 7$ ou 11 modulo 12 (une sur quatre à chaque fois).

2.3. Compléments d'algèbre. — La recherche de grands nombres premiers demande évidemment en pratique de disposer de tests de primalité aussi efficaces que possibles. Nous allons en présenter certains ; mais pour les décrire nous allons avoir besoin de quelques lemmes de théorie des groupes.

Lemme 2.3.1. — *Soit G un groupe abélien et soient a et b deux éléments de G dont les ordres respectifs m et n sont finis et premiers entre eux. Le produit ab est alors d'ordre mn.*

Démonstration. — On a $(ab)^{mn} = a^{mn}b^{mn} = e$ puisque mn est multiple de l'ordre de a et de l'ordre de b (la première égalité utilise le caractère abélien de G de manière essentielle). L'ordre d de ab est donc fini et divise mn. Il suffit pour conclure de montrer que mn divise d.

On a $(ab)^d = e$ donc $a^d b^d = e$, là encore parce que G est abélien. Ainsi $a^d = b^{-d}$ est un élément du sous-groupe $H := \langle a \rangle \cap \langle b \rangle$ de G. Or comme $H \subset \langle a \rangle$ son cardinal divise celui de $\langle a \rangle$, qui est égal à m ; et il divise celui de $\langle b \rangle$, qui est égal à n. Les entiers n et m étant premiers entre eux, $|H| = 1$ et H est trivial. Par conséquent $a^d = b^{-d} = e$, et b^d vaut également e. Il s'ensuit que d est multiple de l'ordre de a, à savoir m, et de l'ordre de b, à savoir n ; il est donc multiple du PPCM de m et n, qui vaut mn puisque m et n sont premiers entre eux. □

Lemme 2.3.2. — *Soit G un groupe abélien fini et soit S un sous-ensemble de G. Il existe un élément de G dont l'ordre est exactement le PPCM des ordres des éléments de S.*

Démonstration. — Soit m le PPCM des ordres des éléments de S. Écrivons m sous la forme $\prod p_i^{n_i}$ où les p_i sont des nombres premiers deux à deux distincts et les n_i des entiers strictement positifs. Fixons i. La valuation p_i-adique de m est le supremum des valuations p_i-adiques des ordres des éléments de S. Il existe donc $s_i \in S$ dont l'ordre est de la forme $p_i^{n_i} m_i$ avec m_i premier à p_i. L'élément $s_i^{m_i}$ de G est alors d'ordre $p_i^{n_i}$. En vertu du lemme précédent (et par une récurrence immédiate sur le nombre de facteurs) l'ordre de $\prod_i s_i^{m_i}$ est égal à $\prod p_i^{n_i}$, c'est-à-dire à m.

□

Indiquons tout de suite un premier corollaire fondamental de ce résultat.

Corollaire 2.3.3. — *Soit K un corps (commutatif) et soit G un sous-groupe fini de $K^\times$. Le groupe G est cyclique.*

Démonstration. — Soit d l'ordre de G, et soit m le PPCM des ordres de tous les éléments de G. Comme $g^d = 1$ pour tout $g \in G$ l'entier m divise d ; en particulier $m \leqslant d$.

Pour tout $g \in G$ on a $g^m = 1$ puisque m est multiple de l'ordre de G. Le polynôme $X^m - 1$ a donc au moins d racines dans K ; puisqu'il est de degré m il vient $d \leqslant m$; comme on avait déjà $m \leqslant d$ on a finalement $m = d$.

Or le lemme précédent assure que G possède un élément d'ordre m, donc d'ordre d. En conséquence, G est cyclique.

□

2.3.4. *Le cas de $\mathbb{F}_p^\times$.* — Soit p un nombre premier. L'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on note également $\mathbb{F}_p$ – précisons que cette notation n'est utilisée que lorsqu'on veut penser à $\mathbb{Z}/p\mathbb{Z}$ comme à un corps. Le corps $\mathbb{F}_p$ est fini, de cardinal p. Le corollaire précédent assure alors que $\mathbb{F}_p^\times$ est cyclique. Mais nous attirons votre attention sur un point : si vous dévissez la preuve de ce corollaire vous verrez qu'elle n'est *in fine* pas du tout effective, et qu'elle se contente de montrer abstraitement l'existence d'un élément d'ordre $(p-1)$ dans $\mathbb{F}_p^\times$ sans dire comment le construire.

On dispose cela dit d'un algorithme brutal pour exhiber un générateur de $\mathbb{F}_p^\times$. Il est fondé sur la remarque suivante : si x est un élément de $\mathbb{F}_p^\times$ qui n'est pas d'ordre $p-1$, il existe un diviseur strict d de $p-1$ différent de $p-1$ tel que $x^d = 1$; en choisissant un diviseur premier q de $(p-1)/d$ et en écrivant $(p-1)/d = qm$ on a alors $x^{md} = x^{(p-1)/q} = 1$. Ainsi trouver un générateur de $\mathbb{F}_p^\times$ revient à trouver un élément x de $\mathbb{F}_p^\times$ tel que $x^{(p-1)/q}$ soit différent de 1 pour tout diviseur premier q de $p-1$. Il suffit donc de tester cette propriété lorsque x parcourt toutes les classes d'entiers de 2 à $p-1$ en s'arrêtant dès qu'on trouve un x qui la satisfait.

Mais cet algorithme est en général lent. Nous allons montrer sur des exemples comment procéder de manière plus efficace.

Exemple 2.3.5. — Nous allons exhiber générateur de $\mathbb{F}_{23}^\times$, donc un élément d'ordre 22 (multiplicativement !). Soit x un élément de $\mathbb{F}_{23}^\times$. On a $x^{22} = 1$ et donc $(x^2)^{11} = 1$. Il en résulte, 11 étant premier, que si $x^2 \neq 1$ alors x^2 est d'ordre 11. Supposons que ce soit le cas ; comme (-1) est d'ordre 2 il découle alors du lemme 2.3.1 que $(-x^2)$ est d'ordre 22.

Il suffit donc d'exhiber un élément x de $\mathbb{F}_{23}^\times$ tel que $x^2 \neq 1$. On travaille modulo 23. Tentons notre chance avec 2. On a $2^2 = 4 \neq 1$; par conséquent 4 est d'ordre 11 et (-4) est d'ordre 22 ; c'est donc un générateur de $\mathbb{F}_{23}^\times$.

Exemple 2.3.6. — Nous allons maintenant exhiber un générateur de $\mathbb{F}_{29}^\times$. Ce groupe est de cardinal 28, il s'agit donc d'exhiber un élément d'ordre 28. Si x appartient à $\mathbb{F}_{29}^\times$ alors $x^{28} = 1$. Par conséquent $(x^4)^7 = 1$; comme 7 est premier, on en déduit que x^4 est d'ordre 7 dès qu'il est différent de 1. On a aussi $(x^7)^4 = 1$; il s'ensuit que x^7 est d'ordre 4 dès que $(x^7)^2$ est différent de 1, c'est-à-dire dès que $x^7 \notin \{1, -1\}$ (puisque $X^2 - 1 = (X-1)(X+1)$ a pour racines 1 et -1 dans le corps $\mathbb{F}_{29}$).

Utilisons ces remarques pour fabriquer un élément y d'ordre 7 et un élément z d'ordre 4 dans $\mathbb{F}_{29}^\times$; leur produit sera alors d'ordre 28 par le lemme 2.3.1.

Pour fabriquer un élément d'ordre 7, tentons notre chance avec 2. On travaille modulo 29. On a $2^4 = 16 \neq 1$, si bien que $2^4 = 16 = (-13)$ est d'ordre 7.

Pour fabriquer un élément d'ordre 4, tentons encore notre chance avec 2. On a $2^5 = 32 = 3$, si bien que $2^7 = 4 \cdot 3 = 12 \notin \{1, -1\}$. Ainsi $2^7 = 12$ est d'ordre 4.

On en déduit que 2^{11} est d'ordre 28. On peut le calculer rapidement :

$$2^{11} = 2 \cdot 2^{10} = 2 \cdot (2^5)^2 = 2 \cdot (32)^2 = 2 \cdot 3^2 = 18.$$

Ainsi, $18 = (-11)$ est un générateur de $\mathbb{F}_{29}^\times$.

Mais on aurait pu procéder autrement en exploitant le fait que le *même entier* (à savoir 2) nous a permis de fabriquer un élément d'ordre 4 et un élément d'ordre 7. On a en effet vu au cours de nos calculs que $2^4 \neq 1$, et que $2^7 \notin \{1, -1\}$, si bien que $2^{14} \neq 1$. Les deux diviseurs premiers de 28 sont 2 et 7, et l'on a $(28/2) = 14$ et $(28/7) = 4$. Il s'ensuit (voir l'algorithme brutal décrit en 2.3.4) que 2 est d'ordre 28, donc est un générateur de $\mathbb{F}_{29}^\times$.

2.4. Critères de primalité. — Nous nous proposons maintenant d'énoncer différents critères de primalité ou non-primalité.

2.4.1. *Utilisation du petit théorème de Fermat.* — Soit p un nombre premier. Puisque $\mathbb{F}_p^\times$ est de cardinal $p-1$ on a $x^{p-1} = 1$ pour tout $x \in \mathbb{F}_p^\times$ (notons que le caractère cyclique de $\mathbb{F}_p^\times$ n'intervient pas ici). Autrement si x est un entier compris entre 1 et $p-1$ alors x^{p-1} est égal à 1 modulo p : c'est le *petit théorème de Fermat*.

Par contraposition si n est un entier tel qu'il existe a entre 1 et $n-1$ pour lequel a^{n-1} est différent de 1 modulo n alors n n'est pas premier.

Mais attention : il existe des entiers n qui ne sont pas premiers mais sont tels que $a^{n-1} = 1$ modulo n pour tout a compris entre 1 et $n-1$ et premier à n ; c'est ce qu'on appelle les *nombres de Carmichael*, le plut petit d'entre eux est $561 = 3 \cdot 11 \cdot 17$ (voir les TD).

2.4.2. *Le critère de Miller-Rabin.* — Soit p un nombre premier impair. Écrivons $(p-1) = 2^r m$ avec m impair et $r \geqslant 1$. Soit a un entier premier à p. On a $a^{2^r m} = 1$; il existe donc un entier $s \geqslant 0$ tel que $a^{2^s m} = 1$ et qui est minimal pour cette propriété (notons qu'on a pour tout t l'égalité $a^{2^{t+1} m} = (a^{2^t m})^2$; par conséquent $a^{2^t m} = 1$ pour tout $t \geqslant s$).

Supposons que $s > 0$. Dans ce cas (la classe de) $x := a^{2^{s-1} m}$ est un élément de $\mathbb{F}_p^\times$ différent de 1 qui vérifie $x^2 = 1$. Ainsi x est une des deux racines du polynôme $X^2 - 1 = (X-1)(X+1)$, et il est donc égal à -1.

On en déduit le *critère de non-primalité de Miller-Rabin* : soit n un entier impair, écrivons $(n-1) = 2^r m$ avec m impair. S'il existe a premier à n tel que $a^m \neq 1$ modulo n et $a^{2^d m} \neq -1$ pour tout d entre 1 et $m-1$ alors n n'est pas premier – on dit qu'un tel a est un témoin de non-primalité de Miller-Rabin pour n.

***Théorème 2.4.3* (Critère de primalité de Lucas).** — *Soit n un entier $\geqslant 2$. Les assertions suivantes sont équivalentes :*

(i) *l'entier n est premier ;*

(ii) *pour tout diviseur premier q de $n-1$ de $n-1$ il existe un entier a_q tel que $a_q^{n-1} = 1$ et $a_q^{(n-1)/q} \neq 1$ modulo n.*

Démonstration. — Supposons n premier. On sait que $(\mathbb{Z}/n\mathbb{Z})^\times$ est alors cyclique, de cardinal $n-1$. Soit a un entier premier à n dont la classe modulo n est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$. Cette classe est alors d'ordre $n-1$ modulo n, si bien que $a^{n-1} = 1$ modulo n et que $a^{n(n-1)/q} \neq 1$ modulo n pour tout diviseur premier q de $n-1$ différent de $n-1$; l'assertion (ii) est alors valable avec $a_q = a$ pour tout q.

Réciproquement supposons que (ii) est vraie. Pour tout q, notons e_q l'ordre de a_q dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (notons que a_q est bien inversible dans $\mathbb{Z}/n\mathbb{Z}$ puisque $a_q^{n-1} = 1$ modulo n). Le lemme 2.3.2 assure l'existence d'un élément a de $(\mathbb{Z}/n\mathbb{Z})^\times$ dont l'ordre d est le PPCM des e_q. Les égalités $a_q^{n-1} = 1$ (dans $\mathbb{Z}/n\mathbb{Z}$) assurent que chacun des e_q divise $n-1$, si bien que d divise $n-1$. Et on ne peut avoir d différent de $n-1$. En effet sinon il existerait un diviseur premier q de $n-1$ divisant aussi $(n-1/d)$; écrivons $(n-1) = dbq$. On aurait alors (modulo n) les égalités

$$a_q^{(n-1)/q} = a_q^{db} = (a_q^d)^b = 1,$$

ce qui est absurde (la dernière égalité provient du fait que d est multiple de e_q). Par conséquent $d = n-1$; le sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ engendré par a est alors de cardinal $n-1$, d'où il résulte que $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$, puis que $\mathbb{Z}/n\mathbb{Z}$ est un corps, puis que n est premier. □

2.5. La loi de réciprocité quadratique. — Nous nous proposons maintenant d'établir un résultat majeur d'arithmétique, la *loi de réciprocité quadratique*. Ce théorème présente la particularité de posséder des *centaines* de preuves différentes, souvent extrêmement astucieuses ; elles reposent sur des calculs dont on ne saisit pas bien le sens *a priori*, et qui donnent le résultat comme par miracle. Mais avant de l'énoncer, nous allons commencer par introduire de *symbole de Legendre*.

2.5.1. — Soit p un nombre premier *impair*. L'application $x \mapsto x^2$ de $\mathbb{F}_p^\times$ dans lui-même est un morphisme de groupes, dont l'image est l'ensemble $(\mathbb{F}_p^\times)^2$ des carrés de $\mathbb{F}_p^\times$. Son noyau est $\{x \in \mathbb{F}_p^\times, x^2 = 1\}$, c'est-à-dire l'ensemble des racines dans $\mathbb{F}_p$ du polynôme $X^2 - 1 = (X-1)(X+1)$, qui n'est autre que $\{-1, 1\}$. Puisque p est impair 1 et (-1) sont deux éléments différents de $\mathbb{F}_p^\times$ et $\{-1, 1\}$ est donc de cardinal 2. Il s'ensuit que $(\mathbb{F}_p^\times)^2$ est de cardinal $|\mathbb{F}_p^\times|/2 = \frac{p-1}{2}$ (notez que cela a bien un sens puisque p est impair).

2.5.2. — L'application $x \mapsto x^{\frac{p-1}{2}}$ est un endomorphisme de groupes de $\mathbb{F}_p^\times$. Puisque $\mathbb{F}_p^\times$ est de cardinal $(p-1)$ on a pour tout $x \in \mathbb{F}_p^\times$ les égalités

$$(x^{\frac{p-1}{2}})^2 = x^{p-1} = 1,$$

si bien que $x \mapsto x^{\frac{p-1}{2}}$ peut être vu (en vertu de 2.5.1) comme un morphisme de $\mathbb{F}_p^\times$ dans $\{-1,1\}$, que l'on note traditionnellement $x \mapsto \left(\frac{x}{p}\right)$ et qu'on appelle le *symbole de Legendre*.

Lemme 2.5.3. — *Le symbole de Legendre $\mathbb{F}_p^\times \to \{-1,1\}, x \mapsto \left(\frac{x}{p}\right)$ est surjectif de noyau $(\mathbb{F}_p^\times)^2$.*

Démonstration. — Soit H le noyau du symbole de Legendre. C'est l'ensemble des $x \in \mathbb{F}_p^\times$ tels que $x^{\frac{p-1}{2}} = 1$, c'est-dire encore l'ensemble des racines dans $\mathbb{F}_p$ du polynôme $X^{\frac{p-1}{2}}$. Par conséquent $|H| \leqslant \frac{p-1}{2}$; pour montrer que $H = (\mathbb{F}_p^\times)^2$ il suffit donc de démontrer que H contient $(\mathbb{F}_p^\times)^2$, puisque ce dernier est déjà de cardinal $\frac{p-1}{2}$. Soit donc $x \in \mathbb{F}_p^\times$. On a alors $(x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$, ce qui montre l'inclusion souhaitée ; ainsi $H = (\mathbb{F}_p^\times)^2$.

L'image de $x \mapsto \left(\frac{x}{p}\right)$ a alors pour cardinal $|\mathbb{F}_p^\times|/|(\mathbb{F}_p^\times)^2| = 2$; par conséquent le symbole de Legendre est surjectif. □

Remarque 2.5.4. — L'expérience montre qu'il est commode d'étendre le symbole de Legendre de deux façons. D'une part, on le prolonge à $\mathbb{F}_p$ tout entier en posant $\left(\frac{0}{p}\right) = 0$; d'autre part on peut le voir comme une fonction définie sur $\mathbb{Z}$ en posant $\left(\frac{n}{p}\right) = \left(\frac{\overline{n}}{p}\right)$ pour tout entier n, où $\overline{n}$ désigne évidemment la réduction modulo p. Ainsi étendu, le symbole de Legendre reste multiplicatif.

Lorsqu'on a fixé p sans ambiguïté et qu'on travaille avec le symbole de Legendre sur $\mathbb{F}_p$, on le voit comme à valeurs dans $\{-1,0,1\} \subset \mathbb{F}_p$. Si l'on travaille sur $\mathbb{Z}$ et que p est susceptible de varier, on le voit comme à valeurs dans $\{-1,0,1\} \subset \mathbb{Z}$. Ces différences de point de vue n'ont guère de conséquences puisque la réduction modulo p est injective sur $\{-1,0,1\}$.

***Exemple 2.5.5* (Le cas de (-1)).** — Pour tout nombre premier impair p le symbole de Legendre $\left(\frac{-1}{p}\right)$ est égal à $(-1)^{\frac{p-1}{2}}$ et vaut donc 1 si $\frac{p-1}{2}$ est pair, c'est-à-dire si p vaut 1 modulo 4 ; et (-1) dans le cas contraire, c'est-à-dire si p vaut (-1) (ou encore 3) modulo 4.

Autrement dit (-1) est un carré modulo p si et seulement si p est égal à 1 modulo 4.

2.5.6. *Brefs rappels en théorie des corps.* — Pour le calcul du deuxième cas important de symbole de Legendre, à savoir $\left(\frac{2}{p}\right)$, nous aurons besoin du résultat suivant sur la théorie des extensions de corps, qui nous servira également pour la preuve de la loi de réciprocité quadratique : *si k est un corps et si P est un polynôme non nul à coefficients dans k il existe une extension finie L de k dans laquelle P est*

scindé. Indiquons simplement qu'on le démontre par récurrence sur le degré de P, et que le point clef de la démonstration est le suivant : si Q est un polynôme irréductible de $k[X]$ alors $k[X]/Q$ est une extension finie de k dans laquelle Q a une racine (à savoir $\overline{X}$).

Rappelons aussi que si p est un nombre premier, l'égalité $x^{p-1} = 1$ pour tout x de $\mathbb{F}_p^\times$ entraîne que $x^p = x$ pour tout x de $\mathbb{F}_p^\times$, et même en fait pour tout x de $\mathbb{F}_p$ puisque $0^p = 0$. Si L est une extension quelconque de $\mathbb{F}_p$ le polynôme $X^p - X$ a donc au moins p-racines dans L, à savoir les éléments de $\mathbb{F}_p$. Puisqu'il est de degré p il s'ensuit que ses racines sont exactement les éléments de $\mathbb{F}_p$ et que celles-ci sont simples ; autrement dit $X^p - X = \prod_{\lambda\in\mathbb{F}_p} X - \lambda$.

Enfin nous utiliserons le fait fondamental que dans un corps de caractéristique p on a la formule $(a+b)^p = a^p + b^p$; elle découle de la formule du binôme et du fait que $\binom{n}{p}$ est nul modulo p pour tout n tel que $0 < n < p$.

2.5.7. *Inversibles modulo 8.* — Nous allons également avoir besoin de la description de $(\mathbb{Z}/8\mathbb{Z})^\times$. Il est immédiat que ce groupe est égal à $\{1, -1, 3, -3\}$, et tous ses éléments sont de carré égal à 1. Par conséquent si n est un entier impair alors $n^2 - 1$ est multiple de 8. Par ailleurs soient a et k deux entiers. On a $(a+8k)^2 = a^2 + 16ak + 64k^2$, si bien que lorsque a est impair le quotient $\frac{(a+8k)^2-1}{8}$ est égal à $\frac{a^2-1}{8}$ modulo 2. Il s'ensuit qu'un entier impair n est égal à ± 1 (resp. ± 3) modulo 8 si et seulement si $\frac{n^2-1}{8}$ est pair (resp. impair).

Lemme 2.5.8. — *Soit p un nombre premier impair. On a alors*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p = \pm 1 \text{ modulo } 8 \\ -1 & \text{si } p = \pm 3 \text{ modulo } 8 \end{cases}.$$

Démonstration. — On commence par choisir une extension finie L de $\mathbb{F}_p$ dans laquelle existe un élément x tel que $x^4 = (-1)$ (2.5.6), ce qui entraîne que $x^8 = 1$ et donc que x^n ne dépend, pour tout entier n, que de la classe de n modulo 8. Posons $y = x + x^{-1}$. On a

$$y^2 = (x + x^{-1})^2 = x^2 + x^{-2} + 2 = x^{-1}(1 + x^4) + 2 = 2.$$

Ainsi y est une racine carrée de 2 dans L ; l'autre est alors nécessairement $(-y)$, et 2 appartient donc à $(\mathbb{F}_p^\times)^2$ si et seulement si $y \in \mathbb{F}_p$. Remarquons que comme p est impair, 2 est non nul dans $\mathbb{F}_p$ si bien que $y \neq 0$.

Supposons que $p = 1$ modulo 8. On a alors $x^p = x$ si bien que

$$y^p = (x + x^{-1})^p = x^p + x^{-p} = x + x^{-1} = y.$$

Ainsi $y^p = y$, et y appartient donc à $\mathbb{F}_p$.

Supposons que $p = -1$ modulo 8. On a alors $x^p = x^{-1}$, si bien que

$$y^p = (x + x^{-1})^p = x^p + x^{-p} = x + x^{-1} = y.$$

Ainsi $y^p = y$, et y appartient donc à $\mathbb{F}_p$.

Supposons que $p = 3$ modulo 8. On a alors $x^p = x^3 = -x^{-1}$ (puisque $x^4 = -1$), si bien que $y^p = (x + x^{-1})^p = x^p + x^{-p} = -x^{-1} - x = -y$. Or $(-y) \neq y$ puisque $y \neq 0$ et que $1 \neq (-1)$ (car p est impair). Ainsi $y^p \neq y$, et y n'appartient donc pas à $\mathbb{F}_p$.

Supposons que $p = -3$ modulo 8. On a alors $x^p = x^{-3} = -x$ (puisque $x^4 = -1$), si bien que $y^p = (x + x^{-1})^p = x^p + x^{-p} = -x - x^{-1} = -y$. Il s'ensuit comme ci-dessus que $y^p \neq y$, et y n'appartient donc pas à $\mathbb{F}_p$.

Compte-tenu des rappels faits en 2.5.7, ceci achève la démonstration du lemme. □

Commentaires 2.5.9. — La fin de la preuve utilise de manière essentielle la caractéristique p à travers la formule $(a + b)^p = a^p + b^p$. Mais le premier calcul qu'on y fait vaudrait dans un corps et même un anneau quelconque : il montre en fait que si A est un anneau et x un élément de A tel que $x^4 = -1$ (ce qui force x à être inversible) alors $(x + x^{-1})^2 = 2$ dans A. Vous aviez d'ailleurs sûrement déjà croisé cette égalité, sans probablement qu'elle vous soit présentée ainsi : vous savez bien en effet que dans $\mathbb{C}$ on a $e^{i\pi/4} + e^{-i\pi/4} = 2\cos \pi/4 = \sqrt{2}$.

***Théorème 2.5.10* (Loi de réciprocité quadratique).** — *Soient p et ℓ deux nombres premiers impairs distincts. On a alors*

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

Démonstration. — Choisissons une extension K de $\mathbb{F}_p$ dans laquelle le polynôme $P := X^{\ell-1} + X^{\ell-2} + \ldots + X + 1$ a une racine a (2.5.6). Puisque $(X - 1)P = X^\ell - 1$ on a $a^\ell = 1$; par ailleurs $P(1) = \ell$, et ℓ est non nul dans le corps K qui est de caractéristique p ; ainsi, a est une racine primitive ℓ-ième de l'unité

Comme $a^\ell = 1$ le morphisme $n \mapsto a^n$ de $\mathbb{Z}$ dans $K^\times$ passe au quotient par $\ell\mathbb{Z}$ et induit donc un morphisme de groupes de $\mathbb{F}_\ell$ dans $K^\times$ que nous noterons encore $x \mapsto a^x$. On pose alors

$$y = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) a^x.$$

Notons que la somme est indexée par $\mathbb{F}_\ell$, mais vit dans le corps K qui est lui de caractéristique p ; dans cette somme le symbole de Legendre $\left(\frac{x}{\ell}\right)$ doit être interprété comme étant à valeurs dans $\{0, 1, -1\} \subset \mathbb{F}_p$.

2.5.10.1. *Montrons que $y^2 = (-1)^{\frac{\ell-1}{2}}\ell$.* — On a

$$\begin{aligned} y^2 &= \sum_{(x,t)\in\mathbb{F}_\ell^2} \left(\frac{x}{\ell}\right)\left(\frac{t}{\ell}\right) a^{x+t} \\ &= \sum_{u\in\mathbb{F}_\ell} \left[\sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\left(\frac{u-x}{\ell}\right)\right] a^u, \end{aligned}$$

le passage à la seconde ligne se faisant en posant $u = x + t$. Pour alléger les notations on pose $S_u = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\left(\frac{u-x}{\ell}\right)$; on a donc $y^2 = \sum_{u\in\mathbb{F}_\ell} S_u a^u$.

Calculons tout d'abord S_0. On a

$$S_0 = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\left(\frac{-x}{\ell}\right) = \sum_{x\in\mathbb{F}_\ell} \left(\frac{-x^2}{\ell}\right) = \left(\frac{-1}{\ell}\right) \sum_{x\in\mathbb{F}_\ell} \left(\frac{x^2}{\ell}\right).$$

Or pour tout $x \in \mathbb{F}_\ell$ la quantité $\left(\frac{x^2}{\ell}\right)$ est égale à 1 si x est non nul et à 0 sinon. Par conséquent $S_0 = \left(\frac{-1}{\ell}\right)(\ell - 1)$.

Soit maintenant u un élément de $\mathbb{F}_\ell^\times$. On a

$$\begin{aligned} S_u &= \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\left(\frac{u-x}{\ell}\right) \\ &= \sum_{x\in\mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right)\left(\frac{u-x}{\ell}\right) \\ &= \sum_{x\in\mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right)\left(\frac{x}{\ell}\right)\left(\frac{ux^{-1}-1}{\ell}\right) \\ &= \sum_{x\in\mathbb{F}_\ell^\times} \left(\frac{ux^{-1}-1}{\ell}\right). \end{aligned}$$

Or comme u est non nul, l'application $x \mapsto ux^{-1} - 1$ définit une bijection de $\mathbb{F}_\ell^\times$ sur $\mathbb{F}_\ell \backslash \{-1\}$; la somme ci-dessus se récrit donc

$$\sum_{x\in\mathbb{F}_\ell, x\neq -1} \left(\frac{x}{\ell}\right) = \left[\sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\right] - \left(\frac{-1}{\ell}\right).$$

Si $x \in \mathbb{F}_\ell$ alors $\left(\frac{x}{\ell}\right)$ est nul si $x = 0$, vaut 1 si x appartient à $(\mathbb{F}_\ell^\times)^2$, et (-1) si x appartient au complémentaire de $(\mathbb{F}_\ell^\times)^2$ dans $\mathbb{F}_\ell^\times$. Mais $(\mathbb{F}_\ell^\times)^2$ et son complémentaire dans $\mathbb{F}_\ell^\times$ ont le même cardinal, à savoir $\frac{\ell-1}{2}$; en conséquence $\sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) = 0$, ce qui entraîne que

$$S_u = -\left(\frac{-1}{\ell}\right).$$

On a dès lors

$$\begin{aligned} y^2 &= \sum_{u\in\mathbb{F}_\ell} S_u a^u \\ &= S_0 + \sum_{u\in\mathbb{F}_\ell^\times} S_u a^u \\ &= \left(\frac{-1}{\ell}\right)(\ell-1) - \left(\frac{-1}{\ell}\right)\sum_{u\in\mathbb{F}_\ell^\times} a^u \\ &= \left(\frac{-1}{\ell}\right)(\ell-1) - \left(\frac{-1}{\ell}\right)\sum_{n=1}^{\ell-1} a^n \\ &= \left(\frac{-1}{\ell}\right)(\ell-1) + \left(\frac{-1}{\ell}\right) \\ &= \left(\frac{-1}{\ell}\right)\ell, \end{aligned}$$

où l'avant-dernière égalité provient du fait que $P(a) = \sum_{n=0}^{\ell-1} a^n$ est nul par choix de a, si bien que $\sum_{n=1}^{\ell-1} a^n = -1$.

2.5.10.2. *Montrons que* $y^{p-1} = \left(\frac{p}{\ell}\right)$. — On a les égalités

$$\begin{aligned} y^p &= \left[\sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)a^x\right]^p \\ &= \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)^p a^{px}. \end{aligned}$$

Or comme p est impair et comme $\left(\frac{x}{\ell}\right)$ appartient à $\{0,-1,1\}$ pour tout x on a $\left(\frac{x}{\ell}\right)^p = \left(\frac{x}{\ell}\right)$ quel que soit x appartenant à $\mathbb{F}_\ell$. Il vient

$$\begin{aligned} y^p &= \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)a^{xp} \\ &= \sum_{x\in\mathbb{F}_\ell}\left(\frac{p^{-1}}{\ell}\right)\left(\frac{xp}{\ell}\right)a^{xp} \\ &= \sum_{x\in\mathbb{F}_\ell}\left(\frac{p}{\ell}\right)\left(\frac{xp}{\ell}\right)a^{xp} \\ &= \left(\frac{p}{\ell}\right)\sum_{x\in\mathbb{F}_\ell}\left(\frac{xp}{\ell}\right)a^{xp} \\ &= \left(\frac{p}{\ell}\right)\sum_{t\in\mathbb{F}_\ell}\left(\frac{t}{\ell}\right)a^{t} \\ &= \left(\frac{p}{\ell}\right)y, \end{aligned}$$

où nous avons utilisé les faits suivants : p est non nul et donc inversible dans $\mathbb{F}_\ell$ (et le p^{-1} de la seconde ligne désigne l'inverse de p dans $\mathbb{F}_\ell$) ; tout élément de $\{-1,1\}$ est son propre inverse, d'où le passage de la seconde à la troisième ligne ; et $x \mapsto xp$ est une bijection de $\mathbb{F}_\ell$ sur lui-même, d'où le passage de la quatrième à la cinquième ligne (on pose $t = px$).

On a donc $y^p = \left(\frac{p}{\ell}\right) y$. Or y est non nul puisque $y^2 = (-1)^{\frac{\ell-1}{2}}\ell$ (2.5.10.1) et que ℓ est non nul dans le corps K qui est de caractéristique p ; il vient $y^{p-1} = \left(\frac{p}{\ell}\right)$, ce qu'on souhaitait établir.

2.5.10.3. *Fin de la démonstration.* — L'égalité $y^2 = (-1)^{\frac{\ell-1}{2}}\ell$ vue en 2.5.10.1 assure que y est un élément de $\mathbb{F}_p \subset K$, et $\left(\frac{y^2}{p}\right)$ a donc un sens – mais attention : on *ne peut pas* écrire $\left(\frac{y^2}{p}\right) = \left(\frac{y}{p}\right)^2 = 1$ pour la bonne raison que y appartient à K, mais pas *a priori* à $\mathbb{F}_p$!

On a alors

$$\begin{aligned}
\left(\frac{p}{\ell}\right) &= y^{p-1} \quad (2.5.10.2)\\
&= (y^2)^{\frac{p-1}{2}}\\
&= \left(\frac{y^2}{p}\right)\\
&= \left(\frac{(-1)^{\frac{\ell-1}{2}}\ell}{p}\right) \quad (2.5.10.1)\\
&= \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right)\\
&= (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right),
\end{aligned}$$

ce qui achève la démonstration. □

Remarque 2.5.11. — Le calcul fait en 2.5.10.1 n'utilise absolument pas le fait que le corps K est de caractéristique p. Par conséquent, dans n'importe quel corps K dans lequel existe un élément a tel que $\sum_{n=0}^{\ell-1} a^n = 0$, la somme $\sum_{x\in\mathbb{F}_l} \left(\frac{x}{\ell}\right) a^\ell$ est une racine carrée de $(-1)^{\frac{\ell-1}{2}}\ell$.

Illustrons cette observation par un exemple concret. On a $\mathbb{F}_7^\times = \{-3,-2,-1,1,2,3\}$ et les carrés de $\mathbb{F}_7^\times$ sont donc $1, 4$ et 9, soit encore $1, 2$ et -3. Le nombre complexe $e^{2i\pi/7}$ est une racine primitve 7-ème de l'unité, donc il annule $X^6 + X^5 + \ldots + X + 1$. Par conséquent $\left(\frac{x}{7}\right)$ est égal à 1 si $x \in \{1,2,-3\}$ et à (-1) si $x \in \{-2,-1,3\}$, et

$$e^{-6i\pi+7} - e^{-4i\pi/7} - e^{-2i\pi/7} + e^{2i\pi+7} + e^{4i\pi/7} - e^{6i\pi/7}$$

est une racine carrée de $(-1)^{\frac{7-1}{2}}7 = -7$ (par contre la méthode ne dit pas si c'est $i\sqrt{7}$ ou $-i\sqrt{7}$).

Exemple 2.5.12. — Montrons comment calculer rapidement $\left(\frac{37}{97}\right)$ à l'aide de la loi de réciprocité quadratique (et sans chercher à appliquer la définition directe, qui requerrait de calculer 37^{48} modulo 97).

On a

$$\left(\frac{37}{97}\right) = (-1)^{18\cdot 48}\left(\frac{97}{37}\right) = \left(\frac{97}{37}\right).$$

On a $3 \cdot 37 = 111$ si bien que $97 = (-14)$ modulo 37. Par conséquent

$$\left(\frac{97}{37}\right) = \left(\frac{-14}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)\left(\frac{7}{37}\right).$$

Or $\left(\frac{-1}{37}\right) = (-1)^{18} = 1$, et $\left(\frac{2}{37}\right)$ est égal à (-1) car $37 = 40 - 3$ est égal à (-3) modulo 8. En conséquence on a finalement

$$\left(\frac{37}{97}\right) = -\left(\frac{7}{37}\right) = -(-1)^{3\cdot 18}\left(\frac{37}{7}\right) = -\left(\frac{37}{7}\right) = -\left(\frac{2}{7}\right).$$

Et comme 7 est égal à (-1) modulo 8 le symbole $\left(\frac{2}{7}\right)$ est égal à 1 (ce qu'on pourrait voir directement en remarquant que $2 = 3^2$ modulo 7 !), si bien que $\left(\frac{37}{97}\right) = -1$; ainsi, 37 n'est pas un carré modulo 97.

3. Le théorème des nombres premiers

Cette longue section va être consacrée à la preuve du théorème des nombres premiers. Celle-ci repose sur des méthodes analytiques, mais un certain nombre de préliminaires algébriques vont être nécessaires.

3.1. Caractères d'un groupe abélien fini. — Nous allons tout d'abord étudier une construction très générale de théorie des groupes, qui est extrêmement utilisée, et pas uniquement en arithmétique.

3.1.1. *Structures sur les ensembles de morphismes de groupes.* — Soient G et H deux groupes. En général l'ensemble $\mathrm{Hom}(G,H)$ des morphismes de groupes de G vers H n'a pas de structure algébrique intéressante : c'est un simple ensemble (avec tout de même si l'on veut, un élément particulier qui est le morphisme trivial $g \mapsto e$, mais rien de plus).

Supposons maintenant que H est *abélien*. Soient φ et ψ deux morphismes de groupes de G vers H. Notons $\varphi\psi$ l'application $g \mapsto \varphi\psi$ de G vers H. *L'application $\varphi\psi$ est un morphisme de groupes.* En effet, soient g et g' deux éléments de G. On a alors

$$\begin{aligned}\varphi\psi(gg') &= \varphi(gg')\psi(gg')\\ &= \varphi(g)\varphi(g')\psi(g)\psi(g')\\ &= \varphi(g)\psi(g)\varphi(g')\psi(g')\\ &= \varphi\psi(g)\varphi\psi(g'),\end{aligned}$$

où la troisième égalité provient du caractère abélien de H (la première et la dernière découlent de la définition de $\varphi\psi$, et la seconde du fait que φ et ψ sont des morphismes).

On vérifie alors sans problème que le produit $(\varphi,\psi) \mapsto \varphi\psi$ fait de $\mathrm{Hom}(G,H)$ un groupe abélien ; le neutre est le morphisme trivial $g \mapsto e$, et l'inverse de φ est $\varphi^{-1} := g \mapsto \varphi(g)^{-1}$.

Définition 3.1.2. — Soit G un groupe abélien fini. On appelle *caractère* de G un morphisme de groupes de G dans $\mathbb{C}^\times$; l'ensemble des caractères de G est noté $\widehat{G}$; en vertu de 3.1.1, $\widehat{G}$ a une structure naturelle de groupe abélien ; nous dirons que c'est le *groupe des caractères* de G.

Remarque 3.1.3. — Soit G un groupe abélien fini et soit n son cardinal. Si χ est un caractère de G alors $\chi(g)^n = \chi(g^n) = \chi(e) = 1$ pour tout $g \in G$. Ainsi tout caractère de G est en fait à valeurs dans le groupe μ_n des racines de l'unité, qui est fini ; il s'ensuit d'ores et déjà que $\widehat{G}$ est fini.

Exemple 3.1.4. — Soit n un entier $\geqslant 1$. La propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ assure que pour tout groupe H, la formule $\varphi \mapsto \varphi(\overline{1})$ établit une bijection entre $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},H)$ et $\{h \in H, h^n = e\}$. Lorsque H est abélien, il résulte de 3.1.1 que $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},H)$ a une structure naturelle de groupe abélien, et $\{h \in H, h^n = e\}$ est un sous-groupe de H ; on vérifie alors sans difficulté que la bijection ci-dessus entre $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z},H)$ et $\{h \in H, h^n = e\}$ est un isomorphisme de groupes.

En prenant $H = \mathbb{C}^\times$ on en déduit que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe via $\chi \mapsto \chi(\overline{1})$ au sous-groupe μ_n de $\mathbb{C}^\times$ constitué des racines n-ième de l'unité. Ce groupe lui-même est cyclique de cardinal n, engendré par $e^{2i\pi/n}$. Il s'ensuit que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, mais non canoniquement (il faut choisir un générateur de μ_n).

Lemme 3.1.5. — *Soit G un groupe abélien fini, soit H un sous-groupe de G et soit χ un caractère de H. Il existe exactement $[G : H]$ caractères de G prolongeant χ.*

Démonstration. — On raisonne par récurrence forte sur l'indice $[G : H]$. Si celui-ci vaut 1 alors $H = G$ et l'assertion à montrer est triviale. Supposons $[G : H] > 1$ et le résultat vrai pour les indices $< [G : H]$. Puisque $[G : H] > 1$ il existe un élément g de G qui n'appartient pas à H. Soit H' le sous-groupe de G engendré par H et g ; c'est l'ensemble des éléments de G de la forme $g^n h$ avec $n \in \mathbb{Z}$ et $h \in H$.

3.1.5.1. *Les prolongements de χ à H'.* — Le quotient H'/H est fini et engendré par $\overline{g}$; son cardinal m est l'ordre de $\overline{g}$. Nous nous proposons de montrer qu'il y a exactement m caractères de H' prolongeant χ.

Posons $h_0 = g^m$; puisque $\overline{g}^m = e$, l'élément h_0 de G appartient à H ; soit ξ l'élément $\chi(h_0)$ de $\mathbb{C}^\times$.

Observons tout d'abord que si θ est un caractère de H' prolongeant χ alors nécessairement

$$\theta(g)^m = \theta(g^m) = \theta(h_0) = \chi(h_0) = \xi.$$

Ainsi, $\theta(g)$ est une racine m-ième de ξ. Remarquons aussi que si ζ est une racine m-ième de ξ, il y a au plus un caractère θ de H' prolongeant χ tel que $\theta(g) = \zeta$: pour un tel θ on aura en effet nécessairement $\theta(g^n h) = \zeta^n \theta(h) = \zeta^n \chi(h)$ pour tout $(n, h) \in \mathbb{Z} \times H$.

Comme l'élément ξ de $\mathbb{C}^\times$ a exactement m racines m-ièmes dans $\mathbb{C}^\times$, il suffit en vertu de ce qui précède, pour établir que χ admet exactement m prolongements à H', de prouver que toute racine m-ième ζ de ξ il existe un caractère θ de H' prolongeant χ et prenant la valeur ζ en g. Fixons donc une telle ζ.

L'application $\pi : \mathbb{Z} \times H \to G, (n, h) \mapsto g^n h$ est un morphisme de groupes d'image H'. Montrons que son noyau est l'ensemble E des couples de la forme (km, h_0^{-k}) avec $k \in \mathbb{Z}$. On a pour tout $k \in \mathbb{Z}$ l'égalité

$$\pi(km, h_0^{-k}) = g^{km} h_0^{-k} = h_0^k h_0^{-k} = e,$$

ce qui montre que $E \subset \operatorname{Ker} \pi$. Réciproquement, soit $(n, h) \in \operatorname{Ker} \pi$. On a alors $g^n h = e$, et donc $g^n = h^{-1}$. Ceci entraîne que $\overline{g}^n = e$ dans le groupe quotient H'/H, ce qui signifie que m divise n. Écrivons $n = km$. On a alors $h = g^{-n} = g^{-km} = h_0^{-k}$, et (n, h) appartient donc à E. Ainsi $E = \operatorname{Ker} \pi$, et π induit dès lors un isomorphisme entre $(\mathbb{Z} \times H)/E$ et H'.

Soit maintenant θ le morphisme de groupes de $\mathbb{Z} \times H$ vers $\mathbb{C}^\times$ défini par la formule $\theta(n, h) = \zeta^n \chi(h)$. Pour tout $k \in \mathbb{Z}$ on a $\theta(mk, h_0^{-k}) = \zeta^{mk} \xi^{-k} = \xi^k \xi^{-k} = 1$; ainsi $E \subset \operatorname{Ker} \theta$, et θ passe donc au quotient par E. Au vu de ce qui précède θ induit donc un morphisme de groupes $\overline{\theta}$ de H' vers $\mathbb{C}^\times$, et l'on a par construction

$$\overline{\theta}(g^n h) = \overline{\theta}(\pi(n, h)) = \theta(n, h) = \zeta^n \chi(h)$$

pour tout (n, h) ; ainsi $\overline{\theta}$ est un caractère de H' qui prolonge χ et prend la valeur ζ en g.

3.1.5.2. *Conclusion.* — Le caractère χ admet par ce qui précède exactement $[H' : H]$ prolongements à H'. Et H' contient strictement H, puisque $g \in H'$ et que $g \notin H$. Il s'ensuit que $[G : H'] < [G : H]$. L'hypothèse de récurrence assure donc que tout caractère de H' admet exactement $[G : H']$ prolongements à G. Par conséquent χ admet exactement $[G : H][H' : H] = [G : H]$ prolongements à G. □

Théorème 3.1.6. — *Soit G un groupe abélien fini.*

(1) *Le groupe $\widehat{G}$ a même cardinal que G.*

(2) *Pour tout $g \neq e$ dans G il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq e$.*

Démonstration. — La restriction de tout caractère de G à $\{e\}$ est égal au caractère trivial $e \mapsto 1$. Or il résulte du lemme 3.1.5 que le caractère trivial $e \mapsto 1$ admet $[G : \{e\}] = |G|$ prolongements à G. Ainsi $|\widehat{G}| = |G|$, d'où (1).

Montrons maintenant (2). Soit $g \neq \{e\}$ dans G. Le sous-groupe $\langle g \rangle$ possède un caractère non trivial φ : pour le voir on peut ou bien invoquer (1) qu'on vient de prouver ou bien plus simplement (et donc plus élégamment) remarquer que $\langle g \rangle$ est cyclique, et citer l'exemple 3.1.4 ; comme φ est non trivial et que g engendre $\langle g \rangle$, on a $\varphi(g) \neq 1$. En vertu du lemme 3.1.5, φ admet $[G : \langle g \rangle]$ prolongements à G ; il en admet en particulier au moins un, ce qui achève de prouver (2). □

Remarque 3.1.7. — On dispose en fait d'un résultat nettement plus fort que l'énoncé (1) du théorème ci-dessus : on peut en effet montrer que le groupe $\widehat{G}$ est isomorphe (non canoniquement en général) au groupe G. Cela fera l'objet d'un exercice en TD ; nous l'avons pour le moment simplement constaté lorsque G est cyclique (exemple 3.1.4).

3.1.8. *Morphismes induits entre groupes de caractères.* — Soit $f : H \to G$ un morphisme entre groupes abéliens finis. L'application $\chi \mapsto \chi \circ f$ de $\widehat{G}$ vers $\widehat{H}$ (attention au renversement du sens) est un morphisme de groupes que nous noterons $\widehat{f}$. On a $\widehat{\mathrm{Id}_G} = \mathrm{Id}_{\widehat{G}}$ et $\widehat{f_1 \circ f_2} = \widehat{f}_2 \circ \widehat{f}_1$ lorsque ceci a un sens. Si f est un isomorphisme $\widehat{f}$ l'est aussi et $\widehat{f}^{-1} = \widehat{f^{-1}}$.

Lorsque H est un sous-groupe de G et que f est l'inclusion de H dans G, le morphisme $\widehat{f}$ est simplement la restriction des caractères. Le lemme 3.1.5 assure que dans ce cas $\widehat{f}$ est surjectif, et plus précisément que $\widehat{f}^{-1}(\chi)$ est de cardinal $[G : H]$ pour tout $\chi \in \widehat{H}$.

Proposition 3.1.9. — *Soit G un groupe abélien fini.*

(1) *Soit χ un caractère de G. On a*

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \\ |G| & \text{si } \chi = 1 \end{cases},$$

où l'on note 1 le caractère trivial $g \mapsto 1$.

(2) *Soit g un élément de G. On a On a*

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}0 & si\ g\neq e\\ |G| & si\ g=e\end{cases}.$$

Démonstration. — Montrons d'abord (1). Si $\chi=1$ on a $\sum_{g\in G}\chi(g)=\sum_{g\in G}1=|G|$. Supposons $\chi\neq 1$. Il existe alors $h\in G$ tel que $\chi(h)\neq 1$. On a

$$\begin{aligned}\sum_{g\in G}\chi(g) &= \sum_{g\in G}\chi(h)\chi(h^{-1}g)\\ &= \chi(h)\sum_{g\in G}\chi(h^{-1}g)\\ &= \chi(h)\sum_{g\in G}\chi(g),\end{aligned}$$

où la troisième égalité provient du fait que $g\mapsto h^{-1}g$ est une bijection de G sur lui-même. Puisque $\chi(h)\neq 1$, il vient $\sum_{g\in G}\chi(g)=0$.

Montrons maintenant (2). Si $g=e$ on a $\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}1=|\widehat{G}|=|G|$, la dernière égalité provenant du théorème 3.1.6.

Supposons $g\neq e$. Par le même théorème il existe alors $\varphi\in\widehat{G}$ tel que $\varphi(g)\neq 1$. On a

$$\begin{aligned}\sum_{\chi\in\widehat{G}}\chi(g) &= \sum_{\chi\in\widehat{G}}\varphi(g)(\varphi^{-1}\chi)(g)\\ &= \varphi(g)\sum_{\chi\in\widehat{G}}(\varphi^{-1}\chi)(g)\\ &= \varphi(g)\sum_{\chi\in\widehat{G}}\chi(g),\end{aligned}$$

où la troisième égalité provient du fait que $\chi\mapsto\varphi^{-1}\chi$ est une bijection de $\widehat{G}$ sur lui-même. Puisque $\varphi(g)\neq 1$, il vient $\sum_{\chi\in\widehat{G}}\chi(g)=0$. □

3.2. Caractères modulaires. — Après ces généralités sur les caractères d'un groupe abélien fini, nous allons nous intéresser à ces derniers dans un contexte arithmétique.

Définition 3.2.1. — Soit N un entier $\geqslant 1$. Un *caractère de Dirichlet modulo N* est un caractère du groupe abélien fini $(\mathbb{Z}/N\mathbb{Z})^\times$.

Commentaires 3.2.2. — Un caractère de Dirichlet modulo N est donc un morphisme de groupes $\chi\colon(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$. On peut l'étendre comme on l'avait fait pour le symbole de Legendre : on le prolonge tout d'abord en une application (notée encore χ) -de $\mathbb{Z}/N\mathbb{Z}$ tout entier vers $\mathbb{C}$, en posant $\chi(x)=0$ si x est non inversible. Cette application reste multiplicative (si x est non inversible, xy est non inversible pour tout $y\in\mathbb{Z}/N\mathbb{Z}$, si bien que $\chi(xy)=0=\chi(x)\chi(y)$).

On peut aussi composer χ avec la réduction modulo N et définir ainsi une application $n\mapsto\chi(\overline{n})$ de $\mathbb{Z}$ dans $\mathbb{C}$, qu'on note encore χ par abus, et qui est

complètement multiplicative, c'est-à-dire que $\chi(1) = 1$ et que $\chi(ab) = \chi(a)\chi(b)$ quels que soient a et b (et pas uniquement lorsque a et b sont premiers entre eux). On peut donc également définir un caractère de Dirichlet modulo N comme une application χ de $\mathbb{Z}$ dans $\mathbb{C}$ complètement multiplicative telle que $\chi(n)$ ne dépende que de la classe de n modulo N, et soit nul si et seulement si n *n'est pas* premier avec N. Et bien entendu il suffit de se donner une telle application sur l'ensemble des entiers premiers à N (il n'y a plus ensuite qu'à la prolonger en la décrétant nulle sur tout entier non premier à N).

Exemple 3.2.3. — Pour tout nombre premier impair p, le symbole de Legendre $n \mapsto \left(\frac{n}{p}\right)$ est un caractère de Dirichlet modulo p. C'est l'unique caractère d'ordre 2 de $\mathbb{F}_p^\times$, c'est-à-dire encore son unique caractère non trivial à valeurs dans $\{-1, 1\}$. En effet si χ est un tel caractère son image est $\{-1, 1\}$ et son noyau est donc de cardinal $(p-1)/2$. Et l'on a par ailleurs $\chi(x^2) = \chi(x)^2 = 1$ pour tout x de $\mathbb{F}_p^\times$, si bien que $\operatorname{Ker}\chi$ contient $(\mathbb{F}_p^\times)^2$. Comme ce dernier est de cardinal $(p-1)/2$, le noyau de χ est exactement $(\mathbb{F}_p^\times)^2$; ainsi $\chi(x)$ vaut 1 si x est un carré et (-1) sinon, ce qui veut dire que $\chi(x) = \left(\frac{x}{p}\right)$.

3.2.4. — La loi de réciprocité quadratique va permettre de construire un exemple plus sophistiqué de caractère modulaire d'ordre 2. Il sera commode pour ce faire d'introduire les deux notations suivantes : pour tout entier impair a on notera $\varepsilon(a)$ la classe modulo 2 de $\frac{a-1}{2}$ et $\omega(a)$ celle de $\frac{a^2-1}{8}$ (*cf.* 2.5.7).

On remarque que $\varepsilon(a)$ est égal à 0 si $a = 1$ modulo 4 et à 1 si $a = (-1)$ modulo 4 ; on a par conséquent pour tout couple (a, b) d'entiers impairs l'égalité $\varepsilon(ab) = \varepsilon(a) + \varepsilon(b)$.

On sait aussi (2.5.7) que $\omega(a)$ est égal à 0 si $a = \pm 1$ modulo 8 et à 1 si $a = \pm 3$ modulo 8. Il s'ensuit aisément que l'on a pour tout couple (a, b) d'entiers impairs l'égalité $\omega(ab) = \omega(a) + \omega(b)$.

Comme $(-1)^n$ ne dépend pour tout n que de la classe de n modulo 2, les expressions $(-1)^{\varepsilon(a)}$ et $(-1)^{\omega(a)}$ ont un sens pour tout entier impair a. Et l'on a alors pour tout nombre premier p impair

$$\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)} \text{ et } \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

(la première égalité est la définition du symbole de Legendre ; la seconde est le lemme 2.5.8).

Lemme 3.2.5. — *Soit a un entier relatif non nul et sans facteur carré (c'est-à-dire que $v_p(a) \leqslant 1$ pour tout nombre premier p) ; posons $N = 4|a|$. Il existe alors un unique caractère de Dirichlet modulo N noté χ_a tel que $\chi_a(p) = \left(\frac{a}{p}\right)$ pour tout p ne divisant pas N. On $\chi_a^2 = 1$, et χ_a est différent de 1 dès que $a \neq 1$.*

Démonstration. — Commençons par l'unicité. Soit $\mathscr{S}$ l'ensemble des entiers relatifs premiers à N, et soit $\mathscr{S}^+$ son intersection avec $\mathbb{N}$. Soit $x \in \mathscr{S}^+$. Il s'écrit $\prod p_i$ où

les p_i sont des nombres premiers ne divisant pas N (non nécessairement deux à deux distincts), et l'on a alors nécessairement $\chi_a(x) = \prod \chi_a(p_i) = \prod_i \left(\frac{a}{p_i}\right)$. Ceci montre que χ_a est uniquement déterminé sur $\mathscr{S}^+$. Mais il l'est alors sur $\mathscr{S}$ tout entier : il suffit en effet de choisir pour tout entier x de $\mathscr{S}$ un entier x' de $\mathscr{S}^+$ égal à x modulo N, et de remarquer qu'on a nécessairement $\chi_a(x) = \chi_a(x')$.

Montrons maintenant l'existence, en nous inspirant de la formule exhibée ci-dessus. Écrivons $a = (-1)^u 2^v \prod_j \ell_j$ où u et v appartiennent à $\{0,1\}$ et où les ℓ_i sont des nombres premiers impairs deux à deux distincts ; posons $b = \prod_j \ell_j$.

Pour tout entier $x \in \mathscr{S}^+$, posons $\chi_a(x) = \prod_i \left(\frac{a}{p_i}\right)$, où $\prod p_i$ est l'écriture de x comme produit de nombres premiers (non nécessairement deux à deux distincts) ne divisant pas N. Il est immédiat que χ_a est une application complètement multiplicative à valeurs dans $\{-1,1\}$, prenant la valeur $\left(\frac{a}{p}\right)$ pour tout nombre premier p ne divisant pas N. Nous allons expliquer comment décrire χ_a par une autre formule qui permettra de l'étendre naturellement en une fonction complètement multiplicative de $\mathscr{S}$ vers $\{-1,1\}$ et montrera que $\chi_a(x)$ ne dépend que de la classe de x modulo N.

Soit donc $x = \prod_i p_i$ un élément de $\mathscr{S}^+$. On a

$$\begin{aligned}
\chi_a(x) &= \prod_i \left(\frac{a}{p_i}\right) \\
&= \left(\prod_i \left(\frac{(-1)^u}{p_i}\right)\right)\left(\prod_i \left(\frac{2^v}{p_i}\right)\right)\prod_{i,j}\left(\frac{\ell_j}{p_i}\right) \\
&= \left(\prod_i (-1)^{u\varepsilon(p_i)}\right)\left(\prod_i (-1)^{v\omega(p_i)}\right)\prod_{i,j}(-1)^{\varepsilon(p_i)\varepsilon(\ell_j)}\left(\frac{p_i}{\ell_j}\right) \\
&= (-1)^{u\sum_i \varepsilon(p_i) + v\sum_i \omega(p_i) + (\sum_i \varepsilon(p_i))(\sum_j \varepsilon(\ell_j))}\prod_j \left(\frac{\prod_i p_i}{\ell_j}\right) \\
&= (-1)^{u\varepsilon(x) + v\omega(x) + \varepsilon(x)\varepsilon(b)}\prod_j \left(\frac{x}{\ell_j}\right),
\end{aligned}$$

où la troisième égalité résulte de la loi de réciprocité quadratique et la dernière du fait que ε et ω transforment les produits en somme.

On peut dès lors étendre χ_a en une fonction définie sur $\mathscr{S}$ en posant

$$\chi_a(x) = (-1)^{u\varepsilon(x) + v\omega(x) + \varepsilon(x)\varepsilon(b)}\prod_j \left(\frac{x}{\ell_j}\right)$$

pour tout $x \in \mathscr{S}$. C'est une application à valeurs dans $\{-1,1\}$ qui est complètement multiplicative puisque ε et ω transforment les produits en somme.

Soit $x \in \mathscr{S}$. L'élément $\chi_a(x)$ de $\{-1,1\}$ ne dépend visiblement que des données suivantes :

- ◇ pour tout i, la classe de x modulo ℓ_i (*via* le terme $\left(\frac{x}{\ell_i}\right)$) ;
- ◇ si $v = 0$, la classe de x modulo 4 (*via* le terme $\varepsilon(x)$) ;
- ◇ si $v = 1$, la classe de x modulo 8 (*via* le terme $\omega(x)$; notez que si la classe de x modulo 8 est connue, sa classe modulo 4 l'est *a fortiori*, et $\varepsilon(x)$ est dès lors connu).

Le lemme chinois assure alors que $\chi_a(x)$ ne dépend que de la classe de x modulo $4\ell_1 \dots \ell_n$ si $v = 0$ et modulo $8\ell_1 \dots \ell_n$ si $v = 1$; autrement $\chi_a(x)$ ne dépend dans tous les cas que de la classe de x modulo $4|a|$, c'est-à-dire modulo N. Ains χ_a est bien un caractère de Dirichlet modulo N, à valeurs dans $\{-1, 1\}$ et donc de carré égal à 1, prenant la valeur $\left(\frac{a}{p}\right)$ en tout nombre premier p ne divisant pas N.

Supposons maintenant que $a \neq 1$ et montrons que χ_a est non trivial. Supposons d'abord que $r \geqslant 1$, et fixons un entier m premier à ℓ_1 tel que $\left(\frac{m}{\ell_1}\right) = -1$. Le lemme chinois assure qu'il existe un entier x égal à 1 modulo 8 (ce qui implique que $\omega(x)$ et $\varepsilon(x)$ sont pairs), à m modulo ℓ_1, et à 1 modulo ℓ_j pour tout $j \geqslant 2$. On a alors $\chi_a(x) = -1$, si bien que χ_a est non trivial.

Supposons maintenant que $r = 0$, c'est-à-dire que $a = (-1)^u 2^v$ et que $b = 1$ (notez qu'alors $\varepsilon(b) = 0$) ; comme $a \neq 1$, les entiers u et v ne sont pas tous les deux nuls. On a pour tout x premier à N l'égalité $\chi_a(x) = (-1)^{u\varepsilon(x)+v\omega(x)}$.

Il n'y a plus qu'à distinguer trois cas :

- ◇ le cas $(u, v) = (1, 0)$, c'est-dire $a = (-1)$; on a $\chi_{-1}(x) = (-1)^{\varepsilon(x)}$, si bien que $\chi_{-1}(3) = -1$;
- ◇ le cas $(u, v) = (0, 1)$, c'est-dire $a = 2$; on a $\chi_{-1}(x) = (-1)^{\omega(x)}$, si bien que $\chi_2(3) = -1$;
- ◇ le cas $(u, v) = (1, 1)$, c'est-dire $a = (-2)$; on a $\chi_{-1}(x) = (-1)^{\varepsilon(x)+\omega(x)}$, si bien que $\chi_{-2}(5) = -1$.

Ainsi χ_a est là encore non trivial. □

Année universitaire 2025-2026

Antoine Ducros