COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 8 Lois de réciprocité

Cours de l'institut Fourier, tome 4 (1971), p. 1-24

<http://www.numdam.org/item?id=CIF_1971__4__A8_0>

Chapitre 8

Lois de réciprocité

(Attention: exceptionnellement, dans ce chapitre, nous aurons à considérer des corps finis de caractéristiques p, q, ... distinctes: q ne désignera donc plus, comme c'était le cas dans les chapitres 1 à 7, et comme ce sera à nouveau le cas au chapitre 9, une puissance de p ; ce sera "au contraire", répétons-le, un nombre premier distinct de p).

(8.1). Introduction.

Soient p un nombre premier impair et φ l'unique caractère multiplicatif d'ordre 2 sur F_p, entièrement défini, rappelons-le, par

$\varphi(x) = 0$ si $x = 0$;

$\varphi(x) = 1$ si $x \in F_p^{*2}$, donc si $x^{(p-1)/2} = 1$;

$\varphi(x) = -1$ si $x \in F_p^{*}$ mais si $x \notin F_p^{*2}$, donc si $x^{(p-1)/2} = -1$.

Définition 0. - Soit a un entier relatif. On note $\left(\frac{a}{p}\right)$ (symbole de Legendre) le nombre complexe (égal à 0, 1 ou -1) défini par

$$\left(\frac{a}{p}\right) = \varphi(\bar{a}) ,$$

où $\bar{a} \in F_p = Z/pZ$ désigne la classe de a modulo p.

Dans ces conditions, $\left(\frac{a}{p}\right) = 0$ équivaut à " p divise a "; $\left(\frac{a}{p}\right) = 1$ équivaut à " p ne divise pas a, et a est reste quadratique modulo p ";

enfin, $\left(\frac{a}{p}\right) = -1$ équivaut à " p ne divise pas a , et a est non-reste quadratique modulo p ". Par ailleurs, il est clair que le symbole de Legendre est "multiplicatif": quels que soient les entiers relatifs a et b , on a

$$(1) \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) .$$

Pour a et p donnés, a ne divisant pas p , la relation (1) montre que le problème de savoir si a est reste ou non-reste quadratique modulo p se ramène, après décomposition de a en facteurs premiers, au calcul explicite de $\left(\frac{-1}{p}\right)$ (si a est négatif), de $\left(\frac{2}{p}\right)$ (si a est pair) et de symboles du type $\left(\frac{q}{p}\right)$ (q premier impair, distinct de p et diviseur de a). Les deux premiers des trois symboles ci-dessus valent respectivement $(-1)^{(p-1)/2}$ et $(-1)^{(p^2-1)/8}$ ("lois complémentaires"); quant au troisième, il est bien entendu calculable théoriquement grâce au critère d'Euler, mais sa détermination effective dans des cas particuliers n'est possible que grâce à la loi de réciprocité de Legendre-Gauss:

$$(2) \qquad \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

(et au fait que, dans le symbole de Legendre, la dépendance par rapport au "numérateur" n'a lieu en réalité que modulo le "dénominateur"). (Pour une démonstration absolument élémentaire de la loi de réciprocité et des lois complémentaires, voir [HW] , chapitre VI, paragraphes 11 à 13).

*

Plus généralement, étant donné un nombre premier p et un exposant d non divisible par p , on peut se poser le problème de caractériser les restes

et les non-restes de puissances $d^{\text{ièmes}}$ modulo p par un procédé analogue à celui décrit ci-dessus pour $d = 2$; ce problème se dédouble alors de la façon suivante:

I) Construire un "symbole" $\left(\frac{a}{p}\right)_d$ généralisant convenablement le symbole de Legendre, et ayant notamment les propriétés suivantes:

i) être nul si et seulement si p divise a ;

ii) valoir 1 si et seulement si p ne divise pas a et si a est reste de puissance $d^{\text{ième}}$ modulo p ;

iii) dépendre "multiplicativement" de a ;

iv) enfin, coïncider avec le symbole de Legendre quand $d = 2$.

II) Etablir pour ce symbole une "loi de réciprocité" analogue à la loi de réciprocité quadratique (plus des "lois complémentaires" convenables...).

En fait, si on "reste" dans l'anneau Z des entiers relatifs, le problème ci-dessus n'admet pas de solution (sauf pour $d = 2$ ...): en effet, il est à peu près évident que le symbole évoqué en I) aura pour valeurs des racines $d^{\text{ièmes}}$ de l'unité dans le corps des nombres complexes; le "bon" cadre pour l'étude des restes de puissances $d^{\text{ièmes}}$ est donc l'anneau $A = O_L$ des entiers du corps cyclotomique $L = Q(e^{2\pi i/d})$, et c'est dans ce cadre que nous nous placerons. A titre anecdotique, signalons d'ailleurs que c'est en cherchant à établir la loi de réciprocité biquadratique ($d = 4$) que Gauss a été amené à étudier systématiquement l'anneau $A = Z[i]$ des entiers du corps $Q(i) = Q(e^{2\pi i/4})$: et c'est ainsi que $Z[i]$ est devenu l'"anneau des entiers de Gauss".

*

Le but de ce chapitre est de résoudre le problème posé plus haut pour $d = 3$ et 4, et notamment d'énoncer et de démontrer (à l'aide des propriétés des sommes de Gauss et de Jacobi vues au chapitre 5) les lois de réciprocité cubique et biquadratique (et aussi, ce qui sera instantané, la loi de réciprocité quadratique). On utilisera au paragraphe 2 quelques résultats élémentaires relatifs à la décomposition des nombres premiers dans les corps cyclotomiques $Q(e^{2\pi i/d})$: à ce sujet, voir par exemple [Ws], chapitre 7; on se limitera d'ailleurs presque immédiatement à $d = 2$, 3 et 4, et on aura donc essentiellement besoin des résultats classiques sur l'arithmétique dans Z, $Z[e^{2\pi i/3}]$ et $Z[i]$: pour ces deux derniers anneaux, voir [HW], chapitre XV, paragraphe 1 et 2.

(8.2). Symboles de restes de puissances; énoncé des lois de réciprocité quadratique, cubique et biquadratique.

Soient donc d un entier $\geqslant 2$, ρ une racine primitive $d^{\text{ième}}$ de l'unité dans le corps des nombres complexes, $L = Q(\rho)$ le corps cyclotomique correspondant et $A = O_L = Z[\rho]$ l'anneau des entiers de L.

Définition 1. - Si $a \in A$ et si $\mathfrak{p}$ est un idéal premier de A ne divisant pas d, nous définirons le symbole de restes de puissances $d^{\text{ièmes}}$ modulo $\mathfrak{p}$, que nous noterons $\left(\frac{a}{\mathfrak{p}}\right)_d$, comme étant l'élément de A

- égal à 0, si $a \in \mathfrak{p}$;
- égal à l'unique racine $d^{\text{ième}}$ de l'unité (dans A) congrue à $a^{(N\mathfrak{p}-1)/d} \pmod{\mathfrak{p}}$, si au contraire $a \notin \mathfrak{p}$.

Ceci a un sens du fait que le groupe multiplicatif K^* du corps résiduel

$K = A/\mathfrak{p}$ est d'ordre divisible par d : si en effet q désigne la caractéristique de K, on a $\mathrm{card}(K) = q^f$, où f est le plus petit entier positif tel que $q^f \equiv 1 \pmod{d}$. (Rappel: $N\mathfrak{p} = \mathrm{card}(A/\mathfrak{p})$).

Proposition 1. - (i) L'application $a \longmapsto \left(\frac{a}{\mathfrak{p}}\right)_d$ est un caractère multiplicatif modulo $\mathfrak{p}$ sur A, et ce caractère est d'ordre d ; ainsi, le symbole de reste de puissances $d^{\text{ièmes}}$ modulo $\mathfrak{p}$ s'identifie à un caractère multiplicatif d'ordre d sur $A/\mathfrak{p} = F_{q^f} = K$.

(ii) Pour que $a \in A$ mais $\notin \mathfrak{p}$ soit reste de puissance $d^{\text{ième}}$ modulo $\mathfrak{p}$, il fait et il suffit que $\left(\frac{a}{\mathfrak{p}}\right)_d = 1$.

Beweis. Klar.

Supposons maintenant pour simplifier A principal (c'est le cas notamment pour $d = 2$, 3 ou 4) et soient $\mathfrak{p} = (\ell)$ et $\mathfrak{p}' = (\ell')$ deux idéaux premiers de A, distincts et ne divisant pas d ; convenons d'écrire

$\left(\frac{a}{\ell}\right)_d$ et $\left(\frac{a}{\ell'}\right)_d$ au lieu de $\left(\frac{a}{\mathfrak{p}}\right)_d$ et de $\left(\frac{a}{\mathfrak{p}'}\right)_d$:

Problème (recherche de la loi de réciprocité pour les puissances $d^{\text{ièmes}}$). - Les "nombres premiers" ℓ et ℓ' étant convenablement normalisés, établir une relation entre les symboles "réciproques" $\left(\frac{\ell}{\ell'}\right)_d$ et $\left(\frac{\ell'}{\ell}\right)_d$.

Pour $d = 2$, on a $\rho = -1$, $L = Q$ et $A = Z$; si on normalise ℓ et ℓ' en leur imposant $\ell > 0$, $\ell' > 0$ (ℓ et ℓ' sont alors tout simplement des nombres premiers au sens habituel), les symboles ci-dessus sont des symboles de Legendre, et le problème est résolu, comme on l'a déjà dit plus haut, par la loi de réciprocité quadratique de Legendre-Gauss:

(3) $$\left(\frac{\ell}{\ell'}\right)_2 = (-1)^{(\ell-1)(\ell'-1)/4}\left(\frac{\ell'}{\ell}\right)_2 .$$

Pour $d = 3$, on a $\rho = e^{2\pi i/3} = (-1+\sqrt{-3})/2$, $L = Q(\sqrt{-3})$ et naturellement $A = Z[\rho]$. Les unités de A sont les racines $6^{\text{ièmes}}$ de l'unité, ± 1, $\pm \rho$, $\pm \rho^2$; si on convient de dire qu'un élément $x + y\rho \in A$ (x, $y \in Z$) est <u>primaire</u> lorsque $x \equiv 1$ et $y \equiv 0 \pmod 3$, on peut montrer que tout élément de A premier avec 3 admet <u>un associé primaire et un seul</u>. Si alors $\mathfrak{p} = (\ell)$ est un idéal premier de A ne divisant pas 3, on peut normaliser ℓ en lui imposant d'être primaire; l'unique diviseur premier de 3 étant (λ) avec $\lambda = 1 - \rho$ (qu'on considérera comme normalisé), les éléments irréductibles normalisés de A se répartissent ainsi en trois types:

I. Les éléments $\ell = -q$, avec q premier rationnel $\equiv -1 \pmod 3$.

II. Les éléments $\ell = x + y\rho$ (x, $y \in Z$) primaires, tels que $N\ell = x^2 - xy + y^2$ soit un nombre premier (rationnel) $\equiv 1 \pmod 3$.

III. L'élément $\lambda = 1 - \rho$.

Avec cette normalisation, le problème posé plus haut est alors résolu par la <u>loi de réciprocité cubique d'Eisenstein</u>:

(4) $$\left(\frac{\ell}{\ell'}\right)_3 = \left(\frac{\ell'}{\ell}\right)_3 .$$

Pour $d = 4$, on a $\rho = i = \sqrt{-1}$, $L = Q(i)$ et $A = Z[i]$. Les unités de A sont les racines $4^{\text{ièmes}}$ de l'unité, ± 1, $\pm i$; si on convient de dire qu'un élément $x + yi \in A$ (x, $y \in Z$) est <u>primaire</u> lorsque $x - 1$ et y sont simultanément congrus, soit à 0, soit à 2, $\pmod 4$, on vérifie sans peine que tout élément de A premier avec 2 admet <u>un associé primaire et un seul</u>. Si alors $\mathfrak{p} = (\ell)$ est un idéal pre-

mier de A ne divisant pas 2, on peut normaliser $\mathfrak{l}$ en lui imposant d'être primaire; l'unique diviseur premier de 2 étant (λ) avec $\lambda = 1 + i$ (qu'on considérera comme normalisé), les éléments irréductibles normalisés de A se répartissent finalement en trois types:

I. Les éléments $\mathfrak{l} = -q$, avec q premier rationnel $\equiv -1 \pmod 4$.

II. Les éléments $\mathfrak{l} = x + yi$ (x, $y \in Z$) primaires, tels que $N\mathfrak{l} = x^2 + y^2$ soit un nombre premier (rationnel) $\equiv 1 \pmod 4$.

III. L'élément $\lambda = 1 + i$.

Avec cette normalisation, on peut alors énoncer la loi de réciprocité biquadratique de Gauss:

$$(5) \qquad \left(\frac{\mathfrak{l}}{\mathfrak{l}'}\right)_4 = (-1)^{(N\mathfrak{l}-1)(N\mathfrak{l}'-1)/16} \left(\frac{\mathfrak{l}'}{\mathfrak{l}}\right)_4 .$$

Le reste de ce chapitre va être essentiellement consacré à la démonstration des formules de réciprocité (3), (4) et (5); comme on l'a annoncé dans l'introduction, on se servira des propriétés des sommes de Gauss, et des sommes de Jacobi à deux caractères: à ce sujet, se reporter au chapitre 5, paragraphes 3 et 4.

(8.3). Intermède: sommes de Gauss et de Jacobi associées à un symbole de restes de puissances.

Conservons les hypothèses et notations du paragraphe 2 (à l'exception de " A principal", provisoirement inutile). Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers de $A = O_L$ ($L = Q(e^{2\pi i/d})$), distincts et ne divisant pas d. Supposons en outre que $\mathfrak{p}$ est de degré (absolu) égal à 1, autrement dit que $N\mathfrak{p} = p$, où p est un nombre premier rationnel $\equiv 1 \pmod d$;

le corps résiduel $A/\mathfrak{p}$ s'identifie alors à F_p, le corps premier de caractéristique p, et le symbole de restes de puissances $d^{\text{ièmes}}$ modulo $\mathfrak{p}$, $\left(\frac{\cdot}{\mathfrak{p}}\right)_d$, s'identifie à un caractère multiplicatif d'ordre d sur $K = F_p$: dans la suite, nous désignerons ce caractère par χ ; ζ sera une racine primitive $p^{\text{ième}}$ de l'unité dans le corps des nombres complexes, et $\tau(\chi)$ désignera bien entendu la somme de Gauss $\sum_x \chi(x)\zeta^x$.

Proposition 2. - En posant comme au paragraphe 2 $N\mathfrak{p} = q^f$ (q premier) et comme au chapitre 5 (paragraphe 4, proposition 5 et corollaire)

$$\omega(\chi) = \tau(\chi)^d , \tag{6}$$

on a la relation

$$\left(\frac{\omega(\chi)}{\mathfrak{p}}\right)_d = \left(\frac{q^{d-f}}{\mathfrak{p}}\right)_d \tag{7}$$

Démonstration. - (Les congruences sans module explicite seront des congruences modulo $\mathfrak{p}$). Le corps résiduel $A/\mathfrak{p}$ étant de caractéristique q (*), on a

$$\tau(\chi)^{q^f} \equiv \sum_x \chi^{q^f}(x)\zeta^{q^f x} = \tau_{q^f}(\chi^{q^f}) = \overline{\chi}^{q^f}(q^f)\tau(\chi^{q^f}) \tag{8}$$

(voir chapitre 5, (18)). Comme $q^f = N\mathfrak{p} \equiv 1 \pmod{d}$ (voir paragraphe 2) et que χ est d'ordre d, on a $\chi^{q^f} = \chi$, $\overline{\chi}^{q^f}(q^f) = \chi(q^{d-f})$, et (8) peut se réécrire

$$\tau(\chi)^{N\mathfrak{p}} \equiv \chi(q^{d-f})\tau(\chi) . \tag{9}$$

D'après le chapitre 5, (20), on a $\tau(\chi)\overline{\tau(\chi)} = p$; dans $A[\zeta]$, $\tau(\chi)$ est donc inversible modulo $\mathfrak{p}$, ce qui permet de simplifier (9) par $\tau(\chi)$; comme $\tau(\chi)^d = \omega(\chi)$, (9) devient alors

(*) ... et $\mathfrak{p}$ ne se ramifiant pas dans $A[\zeta]$ ...

(10) $$\omega(\chi)^{(N\mathfrak{y}-1)/d} \equiv \chi(q^{d-f}) ,$$

ce qui, compte tenu de la définition de χ, de celle des symboles de restes de puissances et du fait que dans (10) le module de congruence est $\mathfrak{y}$, est précisément le résultat à démontrer.

Proposition 3. - Pour $1 \leq j \leq d-2$, on a la congruence

(11) $$\pi(\chi, \chi^j) \equiv 0 \pmod{\mathfrak{y}} .$$

Démonstration. Par définition de χ,

(12) $$\pi(\chi, \chi^j) \equiv \sum_x x^{(p-1)/d} (1-x)^{j(p-1)/d} \pmod{\mathfrak{y}},$$

x décrivant dans A un système complet de restes modulo $\mathfrak{y}$, par exemple $\{0, 1, \ldots, p-1\}$; la congruence (11) résulte alors du théorème 3 du chapitre 2, appliqué à $F(X) = X^{(p-1)/d} (1-X)^{j(p-1)/d}$, polynôme à une variable X sur le corps fini $F_p = A/\mathfrak{y}$.

Proposition 4. - Si l'exposant d est premier, on a la congruence

(13) $$\omega(\chi) \equiv -1 \pmod{d} .$$

(Noter que l'idéal (d) de A, module de la congruence (13), n'est pas premier, sauf si $d = 2$, puisque d se ramifie dans $L = \mathbb{Q}(e^{2\pi i/d})$).

Démonstration. L'exposant d étant premier, tous les coefficients multinomiaux mixtes relatifs à d sont divisibles par d, les autres étant égaux à 1 ; d'où (la congruence étant une congruence modulo d)

$$\omega(\chi) = \tau(\chi)^d = \left\{\sum_x \chi(x)\zeta^x\right\}^d \equiv$$

$$\equiv \sum_x \chi^d(x)\,\zeta^{dx} = \sum_{x\neq 0} \zeta^{dx} = -1 , \text{ c.q.f.d.}$$

(on s'est servi du fait que $\chi^d = 1$; noter que ζ^d est une racine

primitive $p^{\text{ième}}$ de l'unité).

(8.4). Démonstration de la loi de réciprocité quadratique (3).

On a $d = 2$, $A = Z$, et on peut appliquer la formule (7) avec $\ell = p$, $\ell' = q$, $f = 1$:

$$\left(\frac{\omega(\chi)}{\ell'}\right)_2 = \left(\frac{\ell'}{\ell}\right)_2 \quad ; \tag{14}$$

mais, χ étant le caractère d'ordre 2 sur $F_\ell^* = F_p^*$, on a

$$\omega(\chi) = \tau(\chi)^2 = \tau(\chi)\tau(\bar{\chi}) = \chi(-1)p = \chi(-1)\ell \quad ;$$

de plus (critère d'Euler), $\chi(-1) = (-1)^{(\ell-1)/2}$; la relation (14) devient ainsi

$$\left(\frac{(-1)^{(\ell-1)/2}\ell}{\ell'}\right)_2 = \left(\frac{\ell'}{\ell}\right)_2 \quad ;$$

d'où immédiatement (3), par multiplicativité du symbole de restes quadratiques modulo ℓ', et du fait que $\left(\frac{-1}{\ell'}\right)_2 = (-1)^{(\ell'-1)/2}$. (Noter que le symbole de restes quadratiques coïncide bien avec le symbole de Legendre...)

(8.5). Démonstration de la loi de réciprocité cubique (4).

On a donc $d = 3$, $A = Z[\rho]$, avec $\rho = (-1 + \sqrt{-3})/2$; il s'agit de prouver (4), et on est amené à distinguer trois cas, selon les types respectifs de ℓ et ℓ'.

1er cas: ℓ et ℓ' sont de type I. On a donc $\ell = -q$, $\ell' = -q'$, et $\left(\frac{\ell}{\ell'}\right)_3 = \left(\frac{q}{q'}\right)_3$, $\left(\frac{\ell'}{\ell}\right)_3 = \left(\frac{q'}{q}\right)_3$ (puisque -1 est un cube:

$-1 = (-1)^3$); de plus, q et q' sont congrus à $-1 \pmod 3$): mais ceci entraîne $(q-1, 3) = (q'-1, 3) = 1$, de sorte (voir chapitre 1, paragraphe 4) que, dans Z et a fortiori dans A, q est un cube modulo q', et réciproquement: de là $\left(\frac{q}{q'}\right)_3 = \left(\frac{q'}{q}\right)_3 = 1$, et finalement l'égalité (4) se trouve vérifiée dans ce premier cas du fait que ses deux membres sont égaux à 1.

2ème cas: $\mathfrak{l}$ est de type I et $\mathfrak{l}'$ est de type II. On a maintenant $\mathfrak{l} = -q$ ($q \equiv -1 \pmod 3$) et $\mathfrak{l}' = x + y\rho$ ($x - 1 \equiv y \equiv 0 \pmod 3$), $N\mathfrak{l}' = x^2 - xy + y^2 = p \equiv 1 \pmod 3$). Posons $(\mathfrak{l}) = \mathfrak{w}$, $(\mathfrak{l}') = \mathfrak{y}$, et utilisons les résultats du paragraphe 3; on a d'abord $f = 2$; la proposition 3 montre ensuite que $\pi(\chi,\chi)$ est un élément irréductible associé à $\mathfrak{l}'$; mais (chapitre 5, proposition 5 et corollaire) $\omega(\chi) = \tau(\chi)^3 = \chi(-1)\, p\, \pi(\chi,\chi) = p\pi(\chi,\chi)$ (χ est en effet un caractère cubique relatif au corps $A/\mathfrak{y} = F_p$); comme $p \equiv 1 \pmod 3$ et que 3 est premier, la proposition 4 donne alors $\omega(\chi) \equiv -1 \pmod 3$, ce qui prouve que $-\pi(\chi,\chi)$, associé à $\mathfrak{l}'$, est primaire (comme $\mathfrak{l}'$), et par conséquent lui est égal; d'où finalement, en revenant à $\omega(\chi)$:

$$\omega(\chi) = -p\mathfrak{l}';$$

portons ceci dans la formule (7); il vient

$$(15) \qquad \left(\frac{-p\mathfrak{l}'}{\mathfrak{l}}\right)_3 = \left(\frac{-p}{\mathfrak{l}}\right)_3 \left(\frac{\mathfrak{l}'}{\mathfrak{l}}\right)_3 = \left(\frac{\mathfrak{l}}{\mathfrak{l}'}\right)_3 ;$$

mais $-p$ est un cube modulo $\mathfrak{l}$ (voir premier cas); le premier facteur du second membre vaut donc 1, et la seconde égalité (15) est alors exactement l'égalité (4) à démontrer: ce qui règle le deuxième cas.

3ème cas: ℓ et ℓ' sont de type II. On a alors $N\ell = q \equiv 1 \pmod 3$, $N\ell' = p \equiv 1 \pmod 3$. Posons $(\ell) = \mathfrak{p}$, $(\ell') = \mathfrak{P}$. Avec les notations du paragraphe 3, $f = 1$; d'autre part, comme dans le deuxième cas, $\omega(\chi) = -p\ell'$; portons dans la formule (7):

$$\left(\frac{-p\ell'}{\ell}\right)_3 = \left(\frac{q^2}{\ell'}\right)_3 \quad ; \tag{16}$$

ℓ et ℓ' jouant dans ce troisième cas des rôles symétriques, on peut écrire également

$$\left(\frac{-q\ell}{\ell'}\right)_3 = \left(\frac{p^2}{\ell}\right)_3 \quad ; \tag{16'}$$

multiplions le second membre de (16) par le premier membre de (16') et vice versa:

$$\left(\frac{-q^3\ell}{\ell'}\right)_3 = \left(\frac{-p^3\ell'}{\ell}\right)_3 \quad ; \tag{17}$$

comme $-q^3$ et $-p^3$ sont des cubes, ceci se réduit en fait à

$$\left(\frac{\ell}{\ell'}\right)_3 = \left(\frac{\ell'}{\ell}\right)_3 ,$$

ce qui règle le troisième cas et achève de démontrer la loi de réciprocité cubique (4).

(8.6). Démonstration de la loi de réciprocité biquadratique (5).

On a maintenant $d = 4$, $A = \mathbb{Z}[i]$, avec $i = \sqrt{-1}$; il s'agit de démontrer (5), et on est amené comme au paragraphe 5 à distinguer trois cas, selon les types de ℓ et ℓ'.

1er cas: ℓ et ℓ' sont de type I. On voit immédiatement (comme au

paragraphe 5, premier cas) qu'on a séparément $\left(\frac{\ell'}{\ell}\right)_4 = 1$, $\left(\frac{\ell}{\ell'}\right)_4 = 1$ (en effet, si par exemple $\ell = -q$, $q = 4h-1$, et $\ell' = -q'$, on a dans F_q , corps premier à q éléments,

$$(\ell')^{(N\ell-1)/4} = (-q')^{(q^2-1)/4} = ((-q')^h)^{q-1} = 1 ;$$

ainsi, ℓ' (mod q) est une puissance quatrième dans F_q et a fortiori dans $A/(\ell) \simeq F_{q^2}$, etc...); mais la double égalité ci-dessus implique évidemment l'égalité (5), ce qui règle ce premier cas.

$2^{\text{ème}}$ cas: ℓ est de type I et ℓ' est de type II. On a maintenant $\ell = -q$ ($q \equiv -1$ (mod 4)) et $\ell' = x + yi$ ($x - 1 \equiv y \equiv 0$ ou 2 (mod 4), $N\ell' = x^2 + y^2 = p \equiv 1$ (mod 4)). Comme au paragraphe 5, deuxième cas, nous poserons $(\ell) = \mathfrak{y}$, $(\ell') = \mathfrak{p}$, et nous utiliserons les résultats du paragraphe 3; nous noterons φ le caractère χ^2 (c'est l'unique caractère multiplicatif d'ordre 2 sur $A/\mathfrak{p} \simeq F_p$) et nous poserons

$$\pi(\chi, \varphi) = \varpi \quad . \tag{18}$$

Lemme 1. - On a la congruence

$$\varpi^q \equiv \overline{\varpi} \pmod{\mathfrak{y}} . \tag{19}$$

Démonstration. Le nombre premier $q = -\ell$ étant inerte dans $L = Q(i)$, le groupe de Galois $G(L/Q)$ est égal au groupe de décomposition de q dans L , lui-même canoniquement isomorphe par le passage au quotient modulo $\mathfrak{y}$ (dans A) au groupe de Galois de l'extension résiduelle F_{q^2} / F_q : l'isomorphisme en question fait évidemment correspondre à la conjugaison complexe (unique élément d'ordre 2 dans $G(L/Q)$) l'automorphisme "élévation à la

puissance q " (unique élément d'ordre 2 dans $G(F_{q^2}/F_q)$); ainsi, on a $a^q \equiv \bar{a} \pmod{\eta}$ pour tout $a \in A$; il suffit de faire $a = \varpi$ dans cette congruence pour obtenir la relation (19).

Lemme 2. - Posons comme précédemment $\omega(\chi) = \tau(\chi)^d = \tau(\chi)^4$. Alors

(20) $$\omega(\chi) = p\varpi^2 .$$

Démonstration. Appliquons tout d'abord aux trois caractères χ , χ et φ la formule (32) du chapitre 5: nous obtenons

(21) $$\pi(\chi,\chi,\varphi) = -\varphi(-1)\pi(\chi,\chi) = -\chi(-1)\pi(\chi,\varphi) ,$$

soit, comme $\varphi(-1) = (-1)^{(p-1)/2} = 1$,

(22) $$\pi(\chi,\chi) = \chi(-1)\varpi .$$

Mais la formule (27) du chapitre 5 donne par ailleurs

(23) $$\omega(\chi) = \chi(-1)p\pi(\chi,\chi)\pi(\chi,\chi^2) ;$$

comme par définition $\chi^2 = \varphi$, l'égalité (20) résulte immédiatement des formules (18), (22) et (23).

Lemme 3. - On a l'égalité

(24) $$\varpi = -\ell' .$$

Démonstration. La proposition 3 du paragraphe 3 montre que $\pi(\chi,\varphi)$ est congru à 0 modulo $\mathfrak{p}$; il en résulte déjà que ϖ et ℓ' sont associés, et le lemme 3 va résulter alors du

Lemme 4. - L'élément $-\varpi = u + vi$ est primaire.

Démonstration. Considérons a priori la courbe d'équation $X^4 + Y^2 = 1$,

"tracée dans le plan affine $(F_p)^2$ ", et soit N le nombre de ses points. Comme $p \equiv 1 \pmod 4$, F_p contient quatre racines quatrièmes de l'unité (chapitre 1, théorème 4), et les points de la courbe étudiée se répartissent de la façon suivante:

quatre points sur l'axe des abscisses;

deux points sur l'axe des ordonnées;

enfin, les points en dehors des axes, qui se groupent huit par huit de manière naturelle (une énumération analogue sera faite en détail au chapitre 9, dans la démonstration du lemme 1: s'y reporter, et regarder notamment la figure jointe à la démonstration). Il résulte de ce décompte que

$$N \equiv 6 \pmod 8 . \tag{25}$$

Par ailleurs, le théorème 3 du chapitre 6 permet d'écrire

$$N = p + \pi(\chi,\varphi) + \pi(\varphi,\varphi) + \pi(\overline{\chi},\varphi) . \tag{26}$$

Comme $\pi(\varphi,\varphi) = -\varphi(-1) = -1$, les formules (25) et (26), jointes à la double définition $\pi(\chi,\varphi) = \varpi = -(u + vi)$, donnent

$$p - 1 - 2u \equiv 6 \equiv -2 \pmod 8 , \tag{27}$$

d'où immédiatement

$$u \equiv (p + 1)/2 \pmod 4 . \tag{28}$$

Par ailleurs, on a évidemment

$$|\varpi|^2 = u^2 + v^2 = p \tag{29}$$

(module d'une somme de Jacobi relative à F_p ...).

Cela étant, distinguons deux cas:

1) $p \equiv 1 \pmod 8$: (28) donne alors $u \equiv 1 \pmod 4$ et par conséquent

$u^2 \equiv 1 \pmod 8$; portant ceci dans (29), on trouve $v^2 \equiv 0 \pmod 8$ et par conséquent $v \equiv 0 \pmod 4$; finalement, $u - 1 \equiv v \equiv 0 \pmod 4$, et $u + vi$ est primaire, ce qui règle ce premier cas.

2) $p \equiv 5 \pmod 8$: un calcul analogue mène à la double congruence

$$u - 1 \equiv v \equiv 2 \pmod 4 ,$$

$u + vi$ est encore primaire, et ce second cas est également réglé.

Ainsi, dans les deux cas, $-\varpi = u + vi$ est primaire, ce qui démontre le lemme 4 et par conséquent le lemme 3.

Ces divers lemmes étant établis, venons-en à la démonstration de l'égalité (5). Un raisonnement analogue au début de la démonstration de la proposition 2 donne $\tau(\chi)^q \equiv \bar{\chi}^q(q)\tau(\chi^q) \pmod \eta$, soit, puisque χ est d'ordre 4 et que $q \equiv -1 \pmod 4$,

$$\tau(\chi)^q \equiv \chi(q)\tau(\bar{\chi}) \pmod \eta . \tag{30}$$

Par ailleurs (chapitre 5, formule (19)),

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p ; \tag{31}$$

enfin (lemmes 2 et 3):

$$\tau(\chi)^4 = p\varpi^2 = p\ell'^2 . \tag{32}$$

Par des calculs analogues à ceux des paragraphes 3 et 5, on déduit successivement de là

d'abord $\tau(\chi)^{q+1} \equiv \chi(-q)p = \chi(\ell)p \pmod \eta$,

puis $\omega(\chi)^{(q+1)/4} = (p\varpi^2)^{(q+1)/4} \equiv \chi(\ell)p \pmod \eta$,

puis $\varpi^{(q+3)(q+1)/4} \equiv \chi(\ell)p \pmod \eta$

(on a utilisé le fait que $p = \varpi\overline{\varpi}$, et le lemme 1), enfin (en simplifiant par $p = \varpi\overline{\varpi} \equiv \varpi^{q+1} \pmod{\eta}$, facteur évidemment inversible modulo η),

$$\varpi^{(q^2-1)/4} \equiv \chi(\ell) \pmod{\eta}. \tag{33}$$

Mais $\varpi = -\ell'$, et l'exposant $(q^2-1)/4$ est pair; (33) devient ainsi

$$\ell'^{(q^2-1)/4} \equiv \chi(\ell) \pmod{\eta}; \tag{34}$$

c'est la formule (5) à démontrer, compte tenu de la définition de χ, de celle des symboles de restes biquadratiques, et du fait que, $(q^2-1)/4$ étant pair, $(-1)^{(N\ell-1)(N\ell'-1)/16} = (-1)^{\{(q^2-1)/4\}\{(p-1)/4\}} = 1$.

Le deuxième cas est ainsi réglé.

*

Pour l'étude du troisième et dernier cas, nous aurons besoin du symbole (biquadratique) de Jacobi; introduisons-le dès maintenant:

Définition 2. - Soient a et m deux éléments de $A = Z[i]$, m étant supposé premier avec 2 et avec a, et de décomposition en facteurs irréductibles normalisés

$$m = i^{\alpha} \prod_{\ell} \ell^{\beta_\ell} \tag{35}$$

On pose alors ("symbole de Jacobi")

$$\left(\frac{a}{m}\right)_4 = \prod_{\ell} \left(\frac{a}{\ell}\right)_4^{\beta_\ell}. \tag{36}$$

Noter que pour m irréductible de type I ou II, on retombe (heureusement) sur le symbole biquadratique précédemment défini.

Les propriétés suivantes du symbole de Jacobi sont évidentes:

— si $a \equiv b \pmod{m}$, on a $\left(\frac{a}{m}\right)_4 = \left(\frac{b}{m}\right)_4$;

— le symbole de Jacobi dépend multiplicativement de son "numérateur" et de son "dénominateur" (à condition bien entendu que les "numérateurs" soient premiers avec les "dénominateurs"...);

— par conjugaison complexe, le symbole de Jacobi se transforme selon la règle ci-dessous:

$$\left(\frac{\bar{a}}{\bar{m}}\right)_4 = \left(\frac{a}{m}\right)_4^3 \tag{37}$$

(les deux membres de (37) sont complexes conjugués, puisque les valeurs du symbole de Jacobi sont des racines quatrièmes de l'unité).

On a également les deux lemmes suivants:

Lemme 5. - Si m et n sont deux entiers rationnels premiers entre eux (m impair), on a

$$\left(\frac{n}{m}\right)_4 = 1 . \tag{38}$$

Démonstration. Il suffit évidemment de vérifier (38) pour m premier dans Z . Si $m = q \equiv 3 \pmod{4}$, on raisonne comme au début de ce paragraphe (premier cas). Si $m = \ell\bar{\ell} \equiv 1 \pmod{4}$, on a

$$\left(\frac{n}{m}\right)_4 = \left(\frac{n}{\ell}\right)_4 \left(\frac{n}{\bar{\ell}}\right)_4 = \left(\frac{n}{\ell}\right)_4^4 = 1 ,$$

en utilisant (37) et le fait que $\bar{n} = n$. Le lemme est prouvé.

Lemme 6. - Si m est un entier rationnel impair, on a

$$\left(\frac{i}{m}\right)_4 = (-1)^{(m^2-1)/8} . \tag{39}$$

Démonstration. Comme au lemme 5, on peut se limiter au cas où m est premier dans Z. Si $m = q \equiv 3 \pmod 4$, on a par définition

$$\left(\frac{i}{m}\right)_4 = \left(\frac{i}{q}\right)_4 = i^{(q^2-1)/4} = (-1)^{(m^2-1)/8}. \tag{40}$$

Si au contraire $m = p \equiv 1 \pmod 4$, avec par conséquent $p = \mathfrak{l}\bar{\mathfrak{l}}$ dans A, on a

$$\left(\frac{i}{m}\right)_4 = \left(\frac{i}{\mathfrak{l}}\right)_4\left(\frac{i}{\bar{\mathfrak{l}}}\right)_4 = i^{(N\mathfrak{l}-1)/4}\, i^{(N\bar{\mathfrak{l}}-1)/4} = \ldots \tag{41}$$

$$\ldots = i^{(p-1)/2} = (-1)^{(p-1)/4},$$

puisque $N\mathfrak{l} = N\bar{\mathfrak{l}} = p$; mais on voit facilement que pour $p \equiv 1 \pmod 4$, les entiers $(p-1)/4$ et $(p^2-1)/8 = (m^2-1)/8$ ont même parité, et donc "se valent" en tant qu'exposants de -1 ; l'égalité (41) donne donc en définitive

$$\left(\frac{i}{m}\right)_4 = (-1)^{(m^2-1)/8}, \tag{42}$$

ce qui, compte tenu également de (40), prouve le lemme 6.

*

Venons-en à la démonstration de la loi de réciprocité biquadratique dans le

3ème cas: $\mathfrak{l}$ et $\mathfrak{l}'$ sont de type II. On a donc maintenant $\mathfrak{l} = u + vi$ ($u - 1 \equiv v \equiv 0$ ou $2 \pmod 4$, $N\mathfrak{l} = u^2 + v^2 = q \equiv 1 \pmod 4$) et de même $\mathfrak{l}' = x + yi$ ($x - 1 \equiv y \equiv 0$ ou $2 \pmod 4$, $N\mathfrak{l}' = x^2 + y^2 = p \equiv 1 \pmod 4$); on posera $(\mathfrak{l}) = \eta$, $(\mathfrak{l}') = \zeta$; les lettres χ, φ et ϖ garderont la même signification qu'au paragraphe précédent (2ème cas): en particulier, on aura toujours

(20) $\omega(\chi) = p\varpi^2$, (24) $\varpi = -\ell'$.

On aura encore besoin de deux lemmes.

Lemme 7. - On a, entre symboles biquadratiques de Jacobi, l'égalité

(43) $$\left(\frac{\ell'}{q}\right)_4 = \left(\frac{q}{\ell'}\right)_4 .$$

Démonstration. Par un calcul d'un type déjà fait, on obtient la congruence

(44) $$\tau(\bar\chi)^q \equiv \chi(q)\tau(\bar\chi) \pmod{\mathfrak{y}} .$$

Mais $\tau(\bar\chi)$ est inversible modulo $\mathfrak{y}$, et par ailleurs $\tau(\bar\chi)^4 = \omega(\bar\chi) = p\bar\varpi^2 = p\bar\ell'^2 = \ell'\bar\ell'^3$. (44) donne donc successivement

$$\omega(\bar\chi)^{(q-1)/4} \equiv \chi(q) \pmod{\mathfrak{y}} ,$$

$$\left(\frac{p\bar\ell'^2}{\ell}\right)_4 = \left(\frac{q}{\ell'}\right)_4 ,$$

et enfin (45) $$\left(\frac{\ell'}{\ell}\right)_4 \left(\frac{\bar\ell'}{\ell}\right)_4^3 = \left(\frac{q}{\ell'}\right)_4 .$$

Mais d'après la formule (37), on peut remplacer $\left(\frac{\bar\ell'}{\ell}\right)_4^3$ par $\left(\frac{\ell'}{\bar\ell}\right)_4$;

le premier membre de (45) devient ainsi

$$\left(\frac{\ell'}{\ell}\right)_4 \left(\frac{\ell'}{\bar\ell}\right)_4 = \left(\frac{\ell'}{\ell\bar\ell}\right)_4 = \left(\frac{\ell'}{q}\right)_4 ,$$

et l'égalité (45) devient elle-même

$$\left(\frac{\ell'}{q}\right)_4 = \left(\frac{q}{\ell'}\right)_4 , \text{ c.q.f.d.}$$

Lemme 8. - Soient $m \in Z$ et $n \in A = Z[i]$, premiers entre eux et tels que $m \equiv 1 \pmod 4$ et $n \equiv 1 \pmod 2$. On a alors l'égalité

(46) $$\left(\frac{m}{n}\right)_4 = \left(\frac{n}{m}\right)_4 .$$

Démonstration. Il suffit de décomposer m et n en facteurs irréductibles (dans A), d'utiliser la multiplicativité du symbole de Jacobi par rapport à son "numérateur" et à son "dénominateur", et d'appliquer les formules (37), (38) et (43): c'est là un calcul facile mais fastidieux, donc laissé au lecteur.

Ces deux lemmes étant établis, notons que

$$u(x + yi) = ux + vy + yi(u + vi) \equiv ux + vy \pmod{(\ell) = (u + vi)},$$

d'où évidemment

(47) $$\left(\frac{u}{\ell}\right)_4 \left(\frac{\ell'}{\ell}\right)_4 = \left(\frac{ux + vy}{\ell}\right)_4 .$$

On a de même

(48) $$\left(\frac{x}{\ell'}\right)_4 \left(\frac{\ell}{\ell'}\right)_4 = \left(\frac{ux + vy}{\ell'}\right)_4 .$$

Compte tenu de (37) et du fait que les valeurs du symbole de Jacobi sont des racines quatrièmes de l'unité, on obtient, par élévation de (48) au cube, puis multiplication membre à membre avec (47) et enfin rejet dans le second membre d'un certain nombre de choses

(49) $$\left(\frac{\ell'}{\ell}\right)_4 \left(\frac{\ell}{\ell'}\right)_4^3 = \left(\frac{u}{\ell}\right)_4^3 \left(\frac{x}{\ell'}\right)_4 \left(\frac{ux + vy}{\ell\bar{\ell}'}\right)_4 = P .$$

Reste à calculer P : introduisons $e = \pm 1$ et $f = \pm 1$ tels que $ex \equiv fu \equiv 1 \pmod 4$; comme y et v sont pairs, on a aussi

(50) $$ef(ux + vy) \equiv 1 \pmod 4 .$$

D'autre part, en utilisant les diverses propriétés du symbole de Jacobi établies précédemment, on voit facilement que

$$(51) \qquad P = \left(\frac{fu}{\ell}\right)_4^3 \left(\frac{ex}{\ell'}\right)_4 \left(\frac{ef(ux + vy)}{\ell\ell'}\right)_4 \left(\frac{f}{\ell'}\right)_4 \left(\frac{e}{\ell}\right)_4$$

Mais le lemme 8, la définition de e et f et la congruence (50) nous permettent d'"inverser" les trois premiers symboles du membre de droite, qui valent donc respectivement

le premier,

$$\left(\frac{u + vi}{fu}\right)_4^3 = \left(\frac{v}{u}\right)_4^3 \left(\frac{i}{u}\right)_4^3 = \left(\frac{i}{u}\right)_4 = (-1)^{(u^2 - 1)/8}$$

(on a utilisé les lemmes 5 et 6);

le second, de la même manière, $(-1)^{(x^2 - 1)/8}$;

et le troisième, $(-1)^{((ux + vy)^2 - 1)/8}$.

Le produit des trois premiers termes du membre de droite de (51) est donc égal à $(-1)^{(u^2 + x^2 + u^2x^2 + v^2y^2 + 2uvxy - 3)/8}$, ce qui, compte tenu des parités respectives de u , v , x et y (voir la définition de ces quatre nombres), vaut $(-1)^{vy/4}$. Par ailleurs, les deux derniers termes du membre de droite de (51) valent respectivement $f^{(p - 1)/4}$ et $e^{(q - 1)/4}$, et on voit sans peine que dans tous les cas ($e = \pm 1$, $f = \pm 1$), le produit de ces deux quantités est égal à 1 . Au total, (51) donne donc

$$(52) \qquad P = (-1)^{vy/4} .$$

Mais on vérifie immédiatement que l'exposant de -1 a même parité que $(p - 1)(q - 1)/16 = (N\ell - 1)(N\ell' - 1)/16$, d'où

(53) $$P = (-1)^{(N\ell - 1)(N\ell' - 1)/16} .$$

Il suffit alors de porter ceci dans (49) et de multiplier les deux membres par $\left(\frac{\ell}{i}\right)_4$ pour obtenir l'égalité (5). Ce qui règle le troisième cas et achève la démonstration de la loi de réciprocité biquadratique.

(8.7). Compléments et remarques.

1) Les "lois complémentaires" pour $d = 3$ et 4 sont les suivantes:

pour $d = 3$, $\rho = e^{2\pi i/3}$, $\lambda = 1 - \rho$, $\ell = x + y\rho$ (primaire),

$$\left(\frac{\rho}{\ell}\right)_3 = \rho^{(N\ell - 1)/3} , \quad \left(\frac{\lambda}{\ell}\right)_3 = \rho^{2(1 - x)/3} ;$$

pour $d = 4$, $\rho = i$, $\lambda = 1 + i$, $\ell = x + yi$ (primaire),

$$\left(\frac{i}{\ell}\right)_4 = i^{(N\ell - 1)/4} , \quad \left(\frac{\lambda}{\ell}\right)_4 = i^{(x - y - y^2 - 1)/4} .$$

Les "premières lois complémentaires" résultent de la définition du symbole de restes de puissances; les "secondes lois" sont plus délicates à démontrer: à ce sujet, voir par exemple [Ba], p. 224 sqq. et p. 181 sqq.

2) Les démonstrations des lois de réciprocité quadratique, cubique et biquadratique proposées ci-dessus sont, à peu de chose près, certaines des démonstrations primitives de Gauss, Jacobi et Eisenstein, pionniers de la "Cyclotomie". Pour plus de détails à ce sujet, on pourra se reporter aux Oeuvres Complètes des Grands Ancêtres précités, ainsi qu'au livre de Bachmann [Ba]. Naturellement, le bon cadre pour la démonstration (et même simplement l'énoncé) des lois de réciprocité générales est la théorie du corps de classes: à ce

sujet, voir notamment [Hb] ou [AT] . Signalons également qu'on peut démontrer très élégamment les lois de réciprocité cubique et biquadratique à l'aide des propriétés des fonctions elliptiques: voir [25] , [26] , [27] .

3) La démonstration de la loi de réciprocité biquadratique est nettement plus compliquée que celle des lois de réciprocité quadratique et cubique: cela tient à ce que $d = 4$ n'est pas un nombre premier, contrairement à $d = 2$ ou 3 ; la proposition 4 n'est donc plus valable, et par ailleurs la formule (7) perd pratiquement tout intérêt.

4) Les lois de réciprocité cubique et biquadratique nous ont fait sortir de notre anneau initial Z : pour l'application de ces lois à la "résiduacité" (comme ils disent) cubique ou biquadratique modulo p dans Z , voir par exemple [Mo] , chapitre 15, pp. 124-126, et surtout [28].