JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

VERA MYLLER-LEBEDEFF

Sur les racines primitives et les systèmes de bases et indices dans le corps quadratique général

Journal de mathématiques pures et appliquées 8^e série, tome 2 (1919), p. 81-98.
<http://www.numdam.org/item?id=JMPA_1919_8_2__81_0>

Sur les racines primitives et les systèmes de bases et indices dans le corps quadratique général;

PAR Mme VERA MYLLER-LEBEDEFF.

On sait qu'un idéal premier P d'un corps algébrique quelconque possède des racines primitives au nombre de $\varphi(p^f-1)$. On ne sait pas si les racines primitives existent ou non, si le module est un idéal quelconque (1). Cette question est étudiée dans ce qui suit pour le corps quadratique général $R(\sqrt{m})$. Les trois corps où l'étude analogue a été faite, mais où l'on n'a pas besoin d'introduire les idéaux, à savoir le corps rationnel (2), le corps $R(i)$ (3) et le corps $R(\sqrt{-3})$ (4), y sont compris comme cas particuliers. On peut résumer les résultats ainsi :

1° *Puissances d'un idéal premier.* — Les racines primitives n'existent que pour une seule catégorie, notamment pour les puissances d'un idéal premier du premier degré différent de son conjugué, et provenant de la décomposition d'un nombre premier $p \neq 2$. Si l'idéal provient de la décomposition du nombre 2, les racines primitives n'existent pas pour les puissances supérieures à la deuxième. Dans le cas d'un idéal du second degré, il n'y a pas de racines primi-

(1) HILBERT, *Jahresber. d. D. M. V. IV* (1894-1895) : *Theorie der algebr. Zahlkörper*, § 9.

(2) GAUSS, *Disqu. Arithm.*, n° 89-92, et DIRICHLET, *Zahlentheorie Suppl. V.*

(3) DIRICHLET, *Werke I Theorie der complexen Zahlen*, § 2.

(4) Fl. VASILESCO, *Etude des racines prim. dans le corps de la racine cubique de l'unité* (*Bulletin de l'Académie Roumaine*, 1919).

tives pour les puissances supérieures à la première. Quant au cas d'un idéal du premier degré égal à son conjugué (idéal premier ambige), les racines primitives cessent d'exister à partir de P^3 pour $p \neq 2$ et à partir de P^4 pour $p = 2$.

2° *Idéal composé quelconque.* — Les racines primitives existent si l'idéal contient seulement deux facteurs premiers entre eux, dont un est engendré par le nombre 2 (*voir* le théorème XX pour l'énoncé précis).

Pour les idéaux qui n'ont pas de racines primitives, on peut généraliser les notions de système de bases et indices introduites par Dirichlet pour les corps R et R (i) (¹). Soit le module $N = P^\pi$. On appelle *base de représentation des restes* un système de plusieurs nombres α, β, ..., λ tels que tous les restes premiers avec le module soient congrus aux produits $\alpha^a \beta^b \ldots \lambda^l$ par rapport au module, a, b, ..., l variant dans certaines limites qui dépendent du module. Les nombres a, b, ..., l s'appellent *indices du reste*. Pour $N = P^\pi P'^{\pi'} \ldots$, on définit comme base et indices la totalité des bases et indices par rapport aux facteurs $P^\pi, P'^{\pi'}, \ldots$ premiers entre eux.

Le maximum d'un indice a est l'exposant auquel la base correspondante α appartient par rapport au module P^π. On peut donc établir les bases en partageant les restes premiers avec P^π en catégories $\alpha + \alpha_i$ où α est premier avec P et α_i un multiple de P^i non divisible par P^{i+1} et en déterminant les exposants auxquels les nombres $\alpha + \alpha_i (i = 1, 2, \ldots)$ appartiennent (mod P^π). De cette façon, on construit les bases pour les puissances d'un idéal premier du premier degré différent de son conjugué et les puissances d'un idéal du second degré. Mais dans certains cas d'idéaux premiers ambiges, à savoir :

$$R = (3, \omega) \quad \text{resp.}(3, 1+\omega), \quad \left(\frac{d}{3}\right) = 0, \quad \frac{m}{3} \equiv -1, (3)$$

et

$$R = (2, \omega) \quad \text{resp.}\,(2, 1+\omega), \quad \left(\frac{d}{2}\right) = 0,$$

(¹) Dirichlet, *Zahlenth.*, § 130, 131, et *Theorie d. compl. Zahlen*, § 2.

il arrive que les bases ainsi établies ne peuvent représenter que $\frac{1}{3}$ resp. $\frac{1}{4}$ des restes. On est alors obligé d'introduire la notion de reste primaire. On définit comme primaire un nombre congru à un nombre rationnel (mod R^2), pour $R^2=(3)$ et congru à 1 (mod R^3), pour $R^2=(2)$. Pour avoir tous les restes premiers avec le module, on n'a qu'à compléter les bases par certains nombres non primaires (ω ou $1+\omega$) qui appartiennent à l'exposant 3 (mod R^2), resp. à l'exposant 4 (mod R^2).

I. — Idéaux premiers du premier degré différents de leurs conjugués.

Premier cas : $\left(\frac{d}{p}\right)=1 \qquad (p\neq 2)$ (1).

On représente ces idéaux par les bases canoniques

$$P=(p,\ a+\sqrt{m})$$
$$P=\left(p,\ \frac{a+\sqrt{m}}{2}\right) \qquad [m\equiv a^2,\ (p)],$$

suivant que m est $\not\equiv 2$ ou 3 (mod 4), ou bien $\equiv 1$ (mod 4). Mais s'apercevant que dans le dernier cas on a $\omega=\frac{1+\sqrt{m}}{2}$ et $a=2a'+1$, tandis que dans les deux premiers cas on a $\omega=\sqrt{m}$, on peut poser pour m quelconque

$$P=(p,\ a+\omega),$$

où $m\equiv a^2$, (p) pour $m\not\equiv 2$ ou 3, (4) et $m\equiv(2a+1)^2$, (p) pour $m\equiv 1$, (4).

Lemme. — P^π *a pour base canonique* $(p^\pi,\ c+\omega)$ *où* $c\not\equiv a$, (p).

Le lemme étant vrai pour P, admettons-le pour $P^{\pi-1}$. Soit

$$P^{\pi-1}=(p^{\pi-1},\ b+\omega) \qquad [b\equiv a,(p)].$$

(1) Pour les notations, *voir* Hilbert, *loc. cit.*, § 60, ou L.-W. Reid, *Elements of the Theory of Algebr. Numbers.*

On aura

$$P^\pi = [p^\pi, p^{\pi-1}(a+\omega), p(b+\omega), ab+(a+b)\omega+\omega^2],$$

P^π contient le nombre $c+\omega$, car on peut trouver x et y rationnels, tels que

$$px+(a+b)y=1 \qquad [m \equiv 2 \text{ ou } \equiv 3, (4)],$$

d'où

$$c = pbx+(ab+m)y = b+(m-b^2)y \equiv b, (p) \equiv a, (p)$$

ou bien tels que

$$px+(a+b+1)y=1 \qquad [m \equiv 1, (4)],$$

d'où

$$c = pbx+\left(ab+\frac{m-1}{4}\right)y = b+\frac{m-(2b+1)^2}{4}y \equiv a, (p),$$

$(p^\pi, c+\omega)$ est une base canonique, car $n(P^\pi) = p^\pi$.

THÉORÈME I. — *Une racine primitive du module rationnel p^π l'est aussi pour $P^\pi = (p^\pi, c+\omega)$ et inversement.*

Soit g une racine primitive de p^π, on a

$$\varphi(P^\pi) = p^{\pi-1}(p-1) = \varphi(p^\pi);$$

les nombres

$$1, \quad g, \quad g^2, \quad \ldots, \quad g^{\varphi(P^\pi)-1}$$

sont incongrus (mod P^π), car, d'après le lemme, la relation

$$g^i \equiv g^k, (P^\pi) \qquad [i, k < \varphi(P^\pi)-1]$$

donnerait

$$g^{i-k}-1 = Mp^\pi \quad (1),$$

contrairement à l'hypothèse. Soit inversement g une racine primitive de P^π; d'après le lemme on peut supposer g entier et rationnel. Si l'on avait

$$g^\delta \equiv 1, (p^\pi) \qquad [\delta < \varphi(p^\pi)],$$

il en résulterait

$$g^\delta \equiv 1, (P^\pi).$$

(1) Nous désignerons partout le multiple d'un nombre a par Ma, M étant rationnel ou algébrique suivant le cas.

En nous rappelant des théorèmes sur les racines primitives du module rationnel p^π, nous pouvons donc déduire.

THÉORÈME II. — *Toutes les racines primitives des puissances supérieures d'un idéal premier* P *sont tous les individus des* $(p-1)\varphi(p-1)$ *classes de nombres différents par rapport au module* p^2.

Nous pouvons ajouter cette remarque. Le nombre de racines primitives de P^π incongrues suivant le module est $\varphi(p^{\pi-1}(p-1))$. D'après le théorème précédent, c'est vrai pour P^2. Admettons-le pour $P^{\pi-1}$ et soit a une racine primitive de $P^{\pi-1}$,

$$b = a + Mp^{\pi-1}$$

le sera aussi pour P^π. On obtient les b incongrues suivant P^π en donnant à Mp valeurs incongrues (mod p).

Second cas : $\left(\frac{d}{2}\right) = 1, \qquad m \equiv 1, (8); \ P = (2, \omega).$

On constate aisément comme dans le lemme que

$$(2, \omega)^\pi = (2^\pi, c + \omega),$$

c étant pair. Il suit de cette représentation canonique que les racines primitives de $(2, \omega)^\pi$ le sont aussi pour 2^π, d'où l'on déduit :

THÉORÈME III. — $(2, \omega)$ a une seule racine primitive $\equiv 1, (2, \omega)^2$ aussi une seule $\equiv 3$, les puissances supérieures de $(2, \omega)$ n'en ont pas du tout.

THÉORÈME IV. — *Tout nombre* μ *premier avec* $(2, \omega)^\pi$ *satisfait à la congruence*

$$\mu \equiv (-1)^c \alpha^a \qquad [(2, \omega)^\pi],$$

où α *est un nombre de la forme* $4M \pm 1$, M *impair rationnel,* $0 \leq a < 2^{\tau-2}$ *et* $0 \leq c < 2$; *autrement dit* $(-1, \alpha)$ *est une base pour le module* $(2, \omega)^\pi$.

Il suit de la représentation canonique qu'on peut prendre comme

système complet de restes [mod $(2, \omega)^\pi$] la suite $0, 1, \ldots, 2^\pi - 1$. Les restes premiers avec le module sont de la forme $8M \pm 1$, $8M \pm 3$. On voit immédiatement que ceux de la forme $8M \pm 3 = 4M_1 \pm 1$, M_1 impair, appartiennent à l'exposant $2^{\pi-2}$ [mod $(2, \omega)^\pi$], tandis que ceux de la forme $8M \pm 1$ appartiennent aux exposants plus petits. Mais $\varphi[(2, \omega)^\pi] = 2^{\pi-1}$, et la moitié des restes impairs, *est* $\equiv 1$, (4), la moitié est $\equiv -1$, (4). Le théorème est donc démontré.

II. — Idéaux premiers du second degré.

$$\left(\frac{d}{q}\right) = -1, \quad Q = (q) \qquad \text{et} \qquad \left(\frac{d}{2}\right) = -1, \quad Q = (2) \quad m \equiv 5, (8).$$

THÉORÈME V. Q^π, $\pi > 1$, *n'a pas de racines primitives ; chaque nombre* μ *premier avec* Q^π *satisfait à*

$$\mu^{q^{2\pi-3}(q^2-1)} \equiv 1, (Q^\pi).$$

D'après le théorème de Fermat pour les idéaux, un nombre μ premier avec $Q^{\pi-1}$ satisfait à

$$\mu^{\varphi(Q^{\pi-1})} = 1, \ (Q^{\pi-1})$$

ou

$$\mu^{\varphi(Q^{\pi-1})} = 1 + MQ^{\pi-1}.$$

Il en suit pour $q = 2$ et $\neq 2$

$$\mu^{q\varphi(Q^{\pi-1})} = (1 + MQ^{\pi-1})^q = 1 + M_1 q^\pi \equiv 1, (Q^\pi) \qquad (\pi > 1),$$

tandis que

$$\varphi(Q^\pi) = q^2 \varphi(Q^{\pi-1}).$$

Pour établir les bases on doit distinguer deux cas.

Premier cas : $\left(\frac{d}{q}\right) = -1 \qquad [q \neq 2; \ Q = (q)].$

Soit γ une racine primitive de Q et α_i comme partout dans ce qui suit, un nombre divisible par la puissance $i^{\text{ième}}$ de l'idéal en question (ici Q), mais non divisible par la puissance $(i+1)^{\text{ième}}$.

THÉORÈME VI. — *On peut déterminer* α_1 *tel que le nombre* $\alpha = \gamma + \alpha_1$ *appartienne à l'exposant* $q^{\pi-1}(q^2-1) \pmod{Q^\pi}$. *Le nombre* $\beta = 1 + \alpha'_1$ *appartient à l'exposant* $q^{\pi-1}$.

Observons qu'on a $\alpha'_1 = \alpha^{i'}$ et $\alpha_i + \alpha_k = \alpha'_i$ si $i < k$. $q^2 - 1$ est la plus petite puissance de γ telle que

$$\gamma^{q^2-1} \equiv 1, (Q) = 1 + \mu q.$$

On a

$$\alpha^{q^2-1} = \gamma^{q^2-1} + (q^2-1)\gamma^{q^2-2}\alpha_1 + \alpha_2 \equiv 1 + \alpha'_1,$$

si l'on a choisi $x \not\equiv 0, (q)$ dans $\alpha_1 = xq$ tel que

$$\mu - \gamma^{q^2-2} x \not\equiv 0, (q).$$

En élevant à la puissance q^i on a la formule générale

$$\alpha^{(q^2-1)q^i} = (1 + \alpha'_1)^{q^i} \equiv 1 + \alpha_{i+1},$$

qui démontre le théorème.

THÉORÈME VII. *α étant choisi comme plus haut, on peut trouver* $\beta = 1 + \alpha''_1$ *tel que* α *et* β *soient indépendants, c'est-à-dire que la congruence*

$$\alpha^a \equiv \beta^b, (Q^\pi)$$

soit impossible, si les exposants varient dans les limites

$$0 < a < (q^2-1)q^{\pi-1} \qquad (0 < b < q^{\pi-1}).$$

α, β *ainsi choisis forment une base du module* Q^π.

Supposons au contraire la congruence satisfaite. En l'élevant à la puissance $q^{\pi-1}$, on a

$$\alpha^{aq^{\pi-1}} \equiv 1, (Q^\pi),$$

d'où $a = (q^2-1)a'$. Or $\alpha^{q^{\pi-1}} = 1 + \alpha'_1$. Donc la congruence se réduit à

$$(1 + \alpha'_1)^{a'} \equiv (1 + \alpha''_1)^b, (Q^\pi)$$

ou

$$(1 + \alpha'_1)^{a'} - (1 + \alpha''_1)^b \equiv M q^\pi.$$

Mais $\alpha'_1 = \mu q$, $\alpha''_1 = xq$, $\mu, x \not\equiv Mq$. On n'a qu'à répéter le raison-

nement de Dirichlet dans le cas analogue du corps $R(i)$ [1] pour voir que α étant donné, il reste pour x $q^2-1-(q-1)$ valeurs incongrues [mod (q)], telles que la congruence de ci-dessus ne soit pas satisfaite.

Second cas : $\left(\frac{d}{2}\right)=-1 \qquad [m\equiv 5,(8);Q=(2)].$

Ici encore, on trouve des nombres α de la forme $\gamma+\alpha_1$ qui appartiennent à l'exposant $2^{\pi-1}.3\,[\mathrm{mod}\,(2)^\pi]$. De même, le nombre $\beta=1+\alpha_1$ appartient à l'exposant $2^{\pi-1}$ pour certaines valeurs de α_1, sinon pour toutes comme dans le cas précédent. Mais α et β ne sont pas indépendants. Par conséquent on doit chercher une autre base.

Désignons par γ une des deux racines primitives de (2) ω ou $1+\omega$.

THÉORÈME VIII. — *On peut choisir x tel que $\alpha=\gamma+2x$ appartienne à l'exposant $2^{\pi-1}.3\,[\mathrm{mod}\,(2)^\pi]$. Le nombre $\beta=1+\alpha_2$ appartient à l'exposant $2^{\pi-2}$.*

En donnant à x les quatre valeurs 0, 1, ω et $1+\omega$ incongrues [mod (2)], on aura pour μ dans

$$\alpha^3=(\gamma+2x)^3=1+2\mu,$$

encore quatre valeurs incongrues (mod 2), car autrement en posant $\alpha=\gamma+2x$, $\alpha_1=\gamma+2x_1$ on aurait

$$\alpha^3-\alpha_1^3\equiv 0,\ (4),$$

d'où l'on tirerait

$$\alpha^2+\alpha\alpha_1+\alpha_1^2\equiv 0,\ (2)$$

ou

$$3\gamma^2\equiv 0,\ (2),$$

contre l'hypothèse. Excluons les deux valeurs de x qui font $\mu\equiv 0,(2)$ et $\mu\equiv 1,(2)$. Les valeurs restantes de x donneront $\mu\equiv\omega,(2)$ et $\mu\equiv 1+\omega$, (2), en tout cas $\mu(\mu+1)\not\equiv 0,(2)$. Par conséquent

$$\alpha^{3.2}=1+4\mu(\mu+1)=1+\alpha_2,$$
$$\alpha^{3.2^2}=1+\alpha_3,$$

---

[1] *Théorie d. compl. Zahlen*, § 2, p. 518.

et, en général,

$$\alpha^{3.2^l} = 1 + \alpha_{l+1} \qquad \text{Q. E. D.}$$

Notons encore qu'en posant $\gamma = \omega$ on aura $x = 0$ ou ω si $m_1 = \frac{m-5}{8}$ est pair et $x = 1$ ou $1+\omega$ si m_1 est impair. Donc α a la forme $\gamma + \alpha_1$ ou $\gamma + \alpha_2$ pour m_1 pair et la forme $\gamma + \alpha_1$ pour m_1 impair. On a des conclusions analogues si l'on pose $\gamma = 1 + \omega$. Dans tous les cas, on a $\mu(\mu+1) \equiv 1$, (2).

THÉORÈME IX. — *α étant choisi comme ci-dessus, on peut déterminer $\beta = 1 + \alpha_2$ tel que α et β soient indépendants.*

Soit $\beta = 1 + 4z$, $z \not\equiv 0$, (2). Choisissons z de sorte que la congruence

$$(1) \qquad \beta \equiv \alpha^a, [(2)^\pi] \qquad (0 < a < 3.2^{\pi-1};\ \pi > 2)$$

soit impossible. Soit au contraire la congruence (1) satisfaite. En l'élevant à la puissance $2^{\pi-2}$, on en tire $a = 2.3a'$. Si a' est pair, il suit

$$\beta \equiv \alpha^{3.2^{\pi}a''} \equiv 1 + 8\mu_1 [(2)^\pi],$$

donc

$$z \equiv 0, (2),$$

ce qui est contraire à l'hypothèse. Si a' est impair, (1) donne

$$1 + 4z \equiv (1 + 4\nu)^{2a''+1}, [(2)^\pi],$$

où $\nu = \mu(\mu+1)$. Mais

$$(1 + 4\nu)^{2a''+1} \equiv 1 + (2a''+1)\,4\nu + \text{M}\,16,$$

donc

$$z \equiv (2a''+1)\nu + \text{M}\,4, [(2)^{\pi-2}].$$

Pour que cette congruence ne soit pas satisfaite, il suffit de prendre

$$z \not\equiv \nu, (2),$$

c'est-à-dire

$$z \not\equiv 1, (2).$$

z étant ainsi choisi, aucune puissance supérieure de β ne peut être congrue à une puissance de α. Soit au contraire

$$\alpha^a \equiv \beta^b, [(2)^\pi] \qquad (0 < a < 3.2^{\pi-1};\ 0 < b < 2^{\pi-2}).$$

On peut supposer $b = 2^i$, car

$$(1+4z)^{2^{i+1}} = 1 + 4z_1,$$

où $z_1 \equiv z, (2)$. Soit donc $\beta^{2^i} \equiv \alpha', [(2)^\pi]$, d'où $a = 3.2^{i+1}a'$. On aura

$$(1+4z)^{2^i} \equiv (1+4\nu)^{2^i a'}, [(2)^\pi],$$

a' est impair, parce que $1+4z$ et $1+4\rho$ appartiennent au même exposant $2^{\pi-2}$. On peut le prendre $=1$ d'après une remarque précédente; i étant $<\pi-2$, il suffit de montrer l'impossibilité de la congruence pour $i = \pi-3$. Or

$$(1+4z)^{2^{\pi-3}} = 1 + 2^{\pi-1}z + M2^\pi.$$

On aurait par suite

$$z \equiv \nu, (2),$$

contre l'hypothèse

THÉORÈME X. — *Le produit* $(-1)^c \alpha^a \beta^b$ *donne tous les restes premiers avec* $(2)^\pi$, *les indices variant dans les limites*

$$0 \leq a < 3.2^{\pi-1}, \qquad 0 \leq b < 2^{\pi-2}, \qquad 0 \leq c < 2 \qquad (\pi > 2).$$

On n'a qu'à démontrer l'impossibilité de la congruence

$$\alpha^a \equiv -\beta^b, [(2^\pi)] \tag{2}$$

pour les indices ci-dessus. En élevant (2) au carré et en appliquant le théorème précédent, on aura $2a = 3.2^{\pi-1}a' < 3.2^\pi$ et $2b = 2^{\pi-2}b' < 2^{\pi-1}$, donc $a = 3.2^{\pi-2}$, $b = 2^{\pi-3}$. Par suite

$$\beta^{2^{\pi-3}} \equiv -\alpha^{3.2^{\pi-2}}$$

ou

$$1 + \alpha_{\pi-1} \equiv -(1+\alpha'_{\pi-1}), [(2)^\pi].$$

ce qui est évidemment impossible pour $\pi > 1$.

Remarque. — Pour le module $(2)^2$, il est aisé de voir qu'on peut prendre comme base α et $\beta = 1 + 2z$, z étant $\not\equiv 0$ et $\not\equiv \mu$, (2).

III. — Idéaux premiers ambiges.

Premier cas : $\left(\frac{d}{r}\right) = 0 \qquad (r \nmid 2).$

Ces idéaux sont représentés par les bases canoniques

$$\left.\begin{aligned} \mathfrak{R} &= (r, \sqrt{m}) = (r, \omega) \\ \mathfrak{R}^{2k} &= (r^k, r^k\omega) \\ \mathfrak{R}^{2k+1} &= (r^{k+1}, r^k\omega) \end{aligned}\right\} \quad [m = 2 \text{ ou } \equiv 3. (4)].$$

$$\left.\begin{aligned} \mathfrak{R} &= \left(r, \frac{r+\sqrt{m}}{2}\right) = \left(r, \frac{r-1}{2} + \omega\right) \\ \mathfrak{R}^{2k} &= \left[r^k, r^k\left(\frac{r-1}{2} + \omega\right)\right] \\ \mathfrak{R}^{2k+1} &= \left[r^{k+1}, r^k\left(\frac{r-1}{2} + \omega\right)\right] \end{aligned}\right\} \quad [m \equiv 1. (4)].$$

THÉORÈME XI. — *Une racine primitive de* $\mathfrak{R}^\pi$ *l'est aussi pour* $\mathfrak{R}^{\pi-1}$ $(\pi > 2)$.

On peut voir aisément que si

$$\alpha^\delta \equiv 1, (\mathfrak{R}^{\pi-1}).$$

alors

$$\alpha^{\delta r} \equiv 1, (\mathfrak{R}^\pi).$$

Cela permet de démontrer le théorème de la même manière que pour le corps rationnel (1).

THÉORÈME XII. — $\mathfrak{R}^\pi$, $\pi > 2$, *n'a pas de racines primitives. Un nombre* μ *premier avec* $\mathfrak{R}^\pi$ *satisfait à*

$$\mu^{r^k(r-1)} \equiv 1, (\mathfrak{R}^\pi) \qquad (\pi = 2k \text{ et } 2k+1).$$

Soit a un nombre du système réduit des restes (mod R) $1, 2, \ldots, r-1$. Désignons par $\overline{\alpha_i}$ un nombre quelconque de l'idéal $\mathfrak{R}^i$ qui peut être

(1) *Voir* DIRICHLET, *Zahlentheorie*, § 128.

divisible aussi par une puissance supérieure de R. Un nombre μ premier avec R^{π} est $\mu = \alpha + \overline{\alpha}_1$.

On a

$$\mu^{r-1} = (\alpha + \overline{\alpha}_1)^{r-1} = 1 + \overline{\alpha}'_1,$$
$$\mu^{r(r-1)} = 1 + \overline{\alpha}_2,$$

ce qui prouve que R^3 n'a pas de racines primitives, puisque

$$\varphi(R^3) = r^2(r-1).$$

Il résulte du théorème XI qu'aucune puissance supérieure à R^2 ne peut pas en avoir non plus. La seconde partie du théorème se démontre par induction en observant que de la relation

$$\mu^{r^k(r-1)} = 1 + \overline{\alpha}_{2(k-1)+1},$$

il suit

$$\mu^{r^k(r-1)} = 1 + \overline{\alpha}_{2k+1}.$$

THÉORÈME XIII. — R^2 *possède des racines primitives au nombre de* $\varphi(r^2)\,\varphi(r-1)$. *C'est la conséquence de l'observation suivante :* f *étant une racine primitive de* R (*qu'on peut supposer entier et rationnel*), *les racines correspondantes de* R^2 *sont*

$$f + lr + n\omega \quad \text{resp. } f + lr + n\left(\frac{r-1}{2} + \omega\right),$$

où l *peut prendre toutes les* r *valeurs rationnelles incongrues* (mod r), *et* n *toutes ces valeurs sauf zéro.*

Pour établir les bases, on doit distinguer deux cas: 1° r impair $\neq 3$ ou $r = 3$ avec $\frac{m}{3} \equiv 1, (3)$; 2° $r = 3$ avec $\frac{m}{3} \equiv -1, (3)$. La raison en est la suivante.

THÉORÈME XIV. — $1 + \alpha_1$ *appartient à l'exposant* r^k (mod R^{π}), $\pi = 2k$ et $2k+1$ *dans le cas* 1°; *dans le cas* 2°, $1 + \alpha_1$ *appartient à l'exposant* 3^{k-1} (mod R^{2k}), *et* 3^k (mod R^{2k+1}), *si* α_1 *représenté par*

$$\left.\begin{array}{ll} \alpha_1 = 3l + n\omega & [m \equiv 2, 3, (4)] \\ \text{resp. } \alpha_1 = 3l + n(1+\omega) & [m \equiv 1, (4)] \end{array}\right\} \quad (n \not\equiv M3),$$

satisfait à la condition

$$2l+1 \not\equiv 0,(3), \quad \text{resp. } 2l+n+1 \not\equiv 0,(3).$$

On le constate en développant le binome

$$(1+\alpha_1)^r = 1 + r\alpha_1 + \alpha_4 = 1 + \alpha_3 + \alpha_4 = 1 + \alpha'_3,$$

si r est impair $\not\equiv 3$.

Pour $r = 3$, on a

$$\alpha_1^2 = \frac{3[3l^2 + n^2 m_1 + 2ln\omega]}{3\left[3\left(l^2 + n^2\frac{m-1}{4}\right) - 2n^2 m_1 + n(2l+n)(1+\omega)\right]},$$

où l'on a posé $m = 3m_1$

$$3\alpha_1 + \alpha_1^3 = \frac{3\alpha_1[1 + n^2 m_1 + 3l^2 + 2ln\omega]}{3\alpha_1\left[1 - 2n^2 m_1 + 3\left(l^2 + n^2\frac{m-1}{4}\right) + (2l+n)n(1+\omega)\right]};$$

donc

$$(1+\alpha_1)^3 = \frac{1 + 3\alpha_1[1 + n^2 m_1 + 3(l^2+l) + (2l+1)n\omega]}{1 + 3\alpha_1\left[1 - 2n^2 m_1 + 3\left(l^2 + n^2\frac{m-1}{4} + l\right) + (2l+n+1)n(1+\omega)\right]}.$$

Dans le cas 1°, on a

$$(1+\alpha_1)^3 = 1 + 3\alpha'_1 = 1 + \alpha_3,$$

comme pour $r \not\equiv 3$ et en général

$$(1+\alpha_1)^{r^k} = 1 + \alpha_{2k+1},$$

ce qui prouve la première partie du théorème. Au contraire, dans le cas 2°, on a

$$(1+\alpha_1)^3 = 1 + 3\alpha_1\alpha'_1 = 1 + \alpha_4,$$

si l'on impose la condition complémentaire de l'énoncé. Si cette condition n'est pas satisfaite, on peut avoir $(1+\alpha_1)^3 = 1 + \alpha_5$ et même $1 + \alpha_6$. Si on la suppose satisfaite, on a la formule générale

$$(1+\alpha_1)^{3k-1} = 1 + \alpha_{2k} \qquad (k \geqq 2),$$

qui prouve la seconde partie du théorème. Étudions d'abord le cas:

$$r \not\equiv 3 \quad \text{ou} \quad r = 3, \qquad \frac{m}{3} \equiv 1,(3).$$

THÉORÈME XV. — *Soit* γ *une racine primitive de* R. *On peut choisir* $\beta = \gamma + \alpha_2$ *de telle façon que* β *appartienne à l'exposant* $r^{k-1}(r-1) \pmod{R^{2k}}$ *et à* $r^k(r-1) \pmod{R^{2k+1}}$.

On peut supposer γ entier et rationnel, alors M dans $\gamma^{r-1} = 1 + Mr$ est aussi rationnel. On aura

$$\beta^{r-1} = \gamma^{r-1} + (r-1)\gamma^{r-2}\alpha_2 + \alpha_3 = 1 + \alpha_2',$$

si $l \not\equiv 0, (r)$ dans $\alpha_2 = r(l + n\omega)$ resp. $r\left[l + n\left(\frac{r-1}{2} + \omega\right)\right]$ est choisi tel que

$$M - \gamma^{r-2} l \not\equiv 0, (r).$$

Pour $r = 3$, on a toujours

$$\beta^{r-1} = (-1 + \alpha_2)^2 = 1 + \alpha_2'.$$

Par conséquent,

$$\beta^{r(r-1)} = 1 + \alpha_4,$$

et en général

$$\beta^{r^{k-1}(r-1)} = 1 + \alpha_{2k} \qquad \text{Q. E. D.}$$

THÉORÈME XVI. — *Les nombres* $a = 1 + \alpha_1$, $\beta = \gamma + \alpha_2$ *constituent une base pour le module* R^π, *les indices variant dans les limites*

$$0 \leq a < r^k, \qquad 0 < b < r^{k-1}(r-1) \qquad (\pi = 2k),$$
$$\text{»} \qquad 0 \leq b < r^k \quad (r-1) \qquad (\pi = 2k+1).$$

On doit démontrer l'impossibilité de la congruence

$$\alpha^a \equiv \beta^b \qquad (R^\pi),$$

a, b variant dans les limites indiquées, 0 exclus. Supposons $a = r^\rho$, car $\alpha^{a'}$ est encore un α si $a' = M\,r$. Soit

$$\alpha^{r^\rho} \equiv \beta^b, (R^{2k}) \qquad (\rho < k).$$

En élevant à la puissance $r^{k-\rho}$, on obtient $b = r^{\rho-1}(r-1)\,b'$ où $b' \not\equiv Mr$, car α^{r^ρ} et $\beta^{r(r-1)}$ appartiennent au même exposant (mod R^{2k}). Dans la congruence

$$\alpha^{r^\rho} \equiv \beta^{r^{\rho-1}(r-1)b'}, (R^{2k}),$$

il suffit de poser $\rho = k-1$. On aura

$$1 + \alpha_{2k-1} \equiv (1 + \alpha_{2k-2})^{b'}, (R^{2k}).$$

Mais $(1+\alpha_{2k-2})^{b'} = 1+\alpha'_{2k-2}$. On aura donc

$$\alpha_{2k-1} - \alpha_{2k-2} \equiv 0, (R^{2k}),$$

ce qui est impossible.

La démonstration de l'indépendance pour le module R^{2k+1} est analogue. Passons au cas:

$$r = 3, \quad \frac{m}{3} \equiv -1, (3).$$

Construisons le Tableau suivant des exposants et des nombres qui leur appartiennent; α_1 y est soumis aux conditions du théorème XIV.

	(mod R^{2k}).	(mod R^{2k+1}).
$1+\alpha_1$	3^{k-1}	3^k
$-1+\alpha_1$	2.3^{k-1}	2.3^k
$1+\alpha_2$	3^{k-1}	3^k
$-1+\alpha_2$	2.3^{k-1}	2.3^k
$1+\alpha_3$	3^{k-1}	3^{k-1}
$-1+\alpha_3$	2.3^{k-1}	2.3^{k-1}

On en déduit que deux bases ne peuvent pas suffire à représenter tous les 2.3^{2k-1} resp. 2.3^{2k} restes. Mais si l'on définit comme restes primaires les restes $\equiv 1$ et $\equiv 2 \pmod{R^2}$, on voit que les bases $\alpha = 1+\alpha_2$, $\beta = -1+\alpha_3$ représentent tous les restes primaires. L'indépendance de ces bases s'établit de la même façon que dans le théorème XVI.

On obtient tous les restes en multipliant les restes primaires dans le cas $m = 2,3, (4)$, $R = (3, \omega)$ par $1+\omega$, $(1+\omega)^2$ et dans le cas $m \equiv 1, (4)$, $R = (3, 1+\omega)$ par ω, ω^2, car on a

$$\left.\begin{aligned} 1+\omega &\equiv 1+\omega, \ (R^2) \\ (1+\omega)^2 &\equiv 1+2\omega, (R^2) \\ 2(1+\omega) &\equiv 2+2\omega, (R^2) \\ 2(1+\omega)^2 &\equiv 2+\omega, \ (R^2) \end{aligned}\right\} \quad [m \equiv 2, 3, (4)]$$

$$\left.\begin{aligned} \omega &\equiv \omega, \ (R^2) \\ \omega^2 &\equiv 2+\omega, \ (R^2) \\ 2\omega &\equiv 2\omega, \ (R^2) \\ 2\omega^2 &\equiv 1+2\omega, (R^2) \end{aligned}\right\} \quad [m \equiv 1, (4)].$$

On conclut

THÉORÈME XVII. — *Tous les restes premiers avec* R^π *sont congrus à*

$$\begin{matrix} \alpha^a\beta^b\omega^c \\ \text{resp. } \alpha^a\beta^b(1+\omega)^c \end{matrix} \pmod{R^\pi} \qquad \begin{matrix} [m \equiv 1, (4)]. \\ [m \equiv 2, 3(4)]. \end{matrix}$$

les indices variant dans les limites

$$\begin{aligned} &0 \leqq a < 3^{k-1}, \quad 0 \leqq b < 2.3^{k-1}, \quad 0 \leqq c < 3 \qquad (\pi = 2k), \\ &0 \leqq a < 3^k, \qquad\quad » \qquad\quad » \qquad (\pi = 2k+1). \end{aligned}$$

Second cas: $\left(\frac{d}{2}\right) = 0$ $\quad R = (2, 1+\omega)$ $\quad [m \equiv 3, (4)]$,
$\quad R = (2, \omega)$ $\quad [m \equiv 2, (4)]$.

On constate directement que R a une seule racine primitive $= 1$, R^2 a ω, resp. $1+\omega$,, R^3 a deux racines ω, $2+\omega$ resp. $1+\omega$, $3+\omega$.

On démontre le théorème XI d'une façon analogue au cas r impair.

THÉORÈME XVIII. — R^π, $\pi > 3$ *n'a pas de racines primitives. Un nombre* μ *premier avec* R^π *satisfait à*

$$\mu^{2k} \equiv 1, (R^\pi) \qquad (\pi = 2k \text{ et } 2k+1).$$

Soit d'abord $m \equiv 2$, (4). Prenons un nombre μ premier avec R de la forme $1+\alpha_1$. On constate

$$\mu^2 = (1+\alpha_1)^2 = 1+\alpha_2.$$

où, dans $\alpha_2 = 2(l+n\omega)$, l et n sont impairs. A cause de cela

$$\mu^4 = (1+\alpha_1)^4 = 1+\alpha_3.$$

Ceci prouve que R^4 et par conséquent R^π, $\pi > 4$, n'ont pas de racines primitives. On déduit ensuite la formule générale

$$\mu^{2^k} = 1+\alpha_{2^{k-1}} \qquad (k \geqq 2).$$

c'est-à-dire μ appartient à l'exposant 2^k (mod R^π). Si α_1 dans μ était divisible par une puissance supérieure de R, μ appartiendrait à un exposant plus petit que 2^k, donc le théorème est démontré.

Soit maintenant $m \equiv 3$, (4) et $\mu = 1+\alpha_1 = 1+l+n\omega$, où l et n sont nécessairement impairs. On a encore

$$\mu^2 = 1+\alpha_2,$$

où dans $\alpha_2 = 2(l' + n'(1+\omega)\ l'$ est impair, mais n' pair. En calculant μ^1, on constate que $\frac{1+l'}{2} = 1 + \frac{m-3}{4} + M2$ est impair, si $m \equiv 3, (8)$, et pair si $m \equiv 7, (8)$; d'où il suit

$$\mu^1 = 1 + \alpha_6 \quad \text{si} \quad m \equiv 3, (8),$$
$$\mu^1 \equiv 1 + \bar{\alpha}_7 \quad \text{si} \quad m \equiv 7, (8),$$

$\bar{\alpha}_7$ pouvant être divisible par R^2. On a les formules générales

$$\mu^{2k-1} = 1 + \alpha_{2k} \qquad [m \equiv 3, (8)],$$
$$\mu^{2k-1} = 1 + \bar{\alpha}_{2k+1} \qquad [m \equiv 7, (8)]$$

qui prouvent le théorème.

Puisque le nombre $1 + \alpha_1$ appartient à des exposants différents suivant que $m \equiv 3, (8)$, ou $= 7, (8)$, nous n'emploierons pas ce nombre pour former la base. Construisons le Tableau

	(mod R^{2k}).	(mod R^{2k+1}).
$1 + \alpha_2$	2^{k-1}	2^{k-1}
$1 + \alpha_3$	»	»
$1 + \alpha_4$	2^{k-2}	2^{k-1}

$\alpha_2 = 2(l + n\omega)$ resp. $2(l + n(1+\omega))$ est soumis ici à la condition n impair, autrement α_2 appartient à un exposant plus petit. Comme évidemment deux bases ne sont pas suffisantes, choisissons $\alpha = 1 + \alpha_3$, $\beta = 1 + \alpha_4$ dont on peut démontrer l'indépendance comme dans les cas précédents. Les nombres de la forme $\alpha^a \beta^b$ représentent seulement $\frac{1}{4}$ des restes (mod R^π), notamment ceux congrus à 1 (mod R^3). Nous les nommerons *primaires* et nous obtiendrons tous les autres en les multipliant par ω, ω^2, ω^3 si $m \equiv 3, (4)$ et par $1 + \omega$, $(1+\omega)^2$, $(1+\omega)^3$, si $m \equiv 2, (4)$, car ω resp. $1 + \omega$ appartient à l'exposant 4 (mod R^3). On a donc

THÉORÈME XIX. — *Tout nombre premier avec* R^π *est congru à*

$$\alpha^a \beta^b \omega^c, \qquad \text{mod } (2, 1+\omega)^\pi,$$
$$\text{resp. } \alpha^a \beta^b (1+\omega)^c, \qquad \text{mod } (2, \omega)^\pi,$$

où $\alpha = 1 + \alpha_3$, $\beta = 1 + \alpha_4$ et

$$0 \leq a < 2^{k-1}, \quad 0 \leq b < 2^{k-2}, \quad 0 \leq c < 4 \quad (\pi = 2k),$$
$$\text{»} \quad 0 \leq b < 2^{k-1}, \quad \text{»} \quad (\pi = 2k+1).$$

IV. — Idéaux composés de plusieurs facteurs différents.

Soit $M = P^{\pi}, P'^{\pi'}\ldots$ Une condition nécessaire de l'existence des racines primitives de M est que les facteurs P^{π}, $P'^{\pi'}$, ... les possèdent, la condition suffisante est alors que $\varphi(P^{\pi})$, $\varphi(P'^{\pi'})$, ... soient premiers entre eux. Prenons pour exemple le cas $m \equiv 2, (4)$. M peut avoir les facteurs suivants aux racines primitives :

$$P^{\pi},\ Q,\ R \quad \text{ou} \quad R^2\ (^1),\quad (2,\sqrt{m}),\ (2,\sqrt{m})^2 \quad \text{ou} \quad (2,\sqrt{m})^3$$

avec les φ correspondants

$$p^{\pi-1}(p-1),\ q^2-1,\ r-1 \quad \text{ou} \quad r(r-1),\quad 1,\ 2 \quad \text{ou} \quad 4.$$

Par suite M a des racines primitives seulement s'il est égal au produit de $(2,\sqrt{m})$ par l'un des idéaux : P^{π}, Q, R ou R^2.

En appliquant ce raisonnement aux différents cas qui peuvent se présenter on conclut.

THÉORÈME XX. — *Les racines primitives n'existent que pour les produits suivants :*

1° $m \equiv 2$ ou $\equiv 3, (4)$: Produit de $(2,\sqrt{m})$ resp. $(2, 1+\sqrt{m})$ par P^{π}, Q, R ou R^2.

2° $m \equiv 1, (8)$: Produit de $\left(2, \frac{1+\sqrt{m}}{2}\right)$ par P^{π}, Q, R ou R^2.

3° $m \equiv 5, (8)$: Produit de (2) par un des idéaux

$$\begin{array}{lll} P^{\pi} & \text{si} & p \not\equiv 1, (3), \\ \left(3, \frac{1+\sqrt{m}}{2}\right) & \text{si} & \left(\frac{m}{3}\right) = 1, \\ (3) & \text{si} & \left(\frac{m}{3}\right) = -1, \\ R & \text{si} & r \not\equiv 1, (3), \\ R^2 & \text{si} & r \not\equiv 1, (3), \end{array}$$

ou

$$\left(3, \frac{3+\sqrt{m}}{2}\right) \quad \text{si} \quad \left(\frac{m}{3}\right) = 0.$$

(1) P, Q, R proviennent des nombres rationnels impairs.