20. Corps R(i) et domaine des entiers de Gauss.

20. Corps R(i) et domaine des entiers de Gauss.

Le corps quadratique $\mathbf{R}(i)$, caractérisé par le polynôme fondamental:

$$F(x) = x^2+1; \quad D = -4;$$

peut être obtenu, par *adjonction* au corps des nombres rationnels, du symbole i, qui se comporte comme un élément dont le carré est égal à —1; (**1**). C'est l'ensemble des expressions, ou des éléments:

$$\rho = r+si, \quad \text{ou} \quad \rho = q\times\alpha, \quad \alpha = x+yi;$$

r,s nombres rationnels, *coefficients* de ρ; q, p.g.c.d. positif de r,s, *facteur rationnel* de ρ; x,y nombres entiers premiers entre eux, coefficients de α, *entier canonique* du corps (**3**).

Deux *éléments conjugués* se déduisent l'un de l'autre en changeant i en $-i$ (**2**):

$$\rho = r+si \quad \Leftrightarrow \quad \rho' = r-si;$$

(ce sont, au sens général de la théorie des nombres complexes, des *imaginaires conjuguées*).

Les *entiers* (algébriques) du corps (**3**) sont donnés par des coefficients entiers rationnels (ou ont un diviseur rationnel entier); ils sont appelés **entiers de Gauss** (qui a étudié leur arithmétique); ils sont engendrés par la *base arithmétique libre* $1\ i$ (canonique).

Les diviseurs de l'unité (déjà indiqués; **3**) sont quatre éléments d'un groupe (cyclique d'ordre 4):

$$i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = +1.$$

On peut représenter géométriquement les éléments $r+si$, du corps $\mathbf{R}(i)$, par les points d'un plan, de coordonnées, r,s, relativement à deux axes rectangulaires. Des éléments conjugués sont représentés par des points symétriques relativement à l'axe réel (dont le vecteur unité représente le « symbole » 1).

Les points représentatifs des entiers sont les sommets d'un quadrillage de côtés parallèles aux axes et dont les côtés sont de longueur 1.

Les produits d'un élément par les quatre diviseurs de l'unité sont représentés par les sommets d'un carré, dont le centre est l'origine (représentant 0) et dont les solmets sont déduits de l'un d'eux par des rotations autour de cette origine, d'angles:

$$\pi : 2, \quad 2\times(\pi : 2) = \pi; \qquad 3\times(\pi : 2), \quad 4\times(\pi : 2) = 2\pi.$$

Pour étudier la *congruence fondamentale* (**5**), relativement à un *module premier* impair p, on peut considérer le corps des entiers, définis mod. p, ou, plus exactement le *groupe* des $p-1$ entiers non nuls [1]). Ce groupe est *cyclique*, c'est-à-dire engendré par les puissances d'un entier générateur convenable g, dont la puissance d'exposant $p-1$ est congrue à $+1$ et dont celle d'exposant $(p-1):2$ est égale à -1. [On sait qu'il y a ainsi $\varphi(p-1)$ générateurs possible, appelés *racines primitives.*]

Si $p-1$ n'est pas divisible par 4; -1 n'est pas congru à un carré; la congruence n'a pas de solution.

Sinon, c'est-à-dire si p est congru à $+1$, mod. 4, la congruence a deux solutions simples, qui sont congrues aux puissances de g, d'exposants $(p-1):4$ et $[3(p-1)]:4$; ce sont d'ailleurs des nombres opposés, mod. p.

Pour le *module* 2, la congruence a une solution double qui est 1, ce nombre annule en effet x^2+1 et $2x$, mod. p [1]).

Pour un *module composé* m (**6**), la congruence a des solutions si, et seulement si, le module m est le produit ou le double d'un produit de s puissances de nombres premiers, dont chacun est congru à $+1$, mod. 4; il y a alors 2^{s-1} couples de solutions conjuguées.

Ces considérations permettent de construire les idéaux canoniques du corps (**7**) qui sont:

$$(m, \ i-c); \qquad c^2+1 \equiv 0, \quad (\text{mod. } m).$$

On en déduit les expressions des idéaux ou des facteurs premiers du corps, ou du domaine $\mathbf{E}(i)$:

1. *Le nombre* 2 *est égal au produit de deux éléments conjugués* $1+i$ et $1-i$; qui sont égaux, au produit près par un diviseur de

1) L'étude de ce groupe est faite dans tous les Traités de Théorie élémentaire des Nombres.

l'unité donc sont deux bases possibles d'un même *idéal principal*, qui est *premier*; le facteur 2 est le carré d'un *facteur* premier.

2. *Un nombre premier q impair, congru à* —1, mod. 4, est la base d'un *idéal principal*; qui est *premier*; q est un *facteur* premier.

3. *Un nombre premier p impair, congru à* +1, mod. 4, est égal au *produit de deux idéaux principaux, conjugués*, qui sont *premiers*; p est produit de deux facteurs premiers.

La vérification de la propriété de 2 est immédiate:

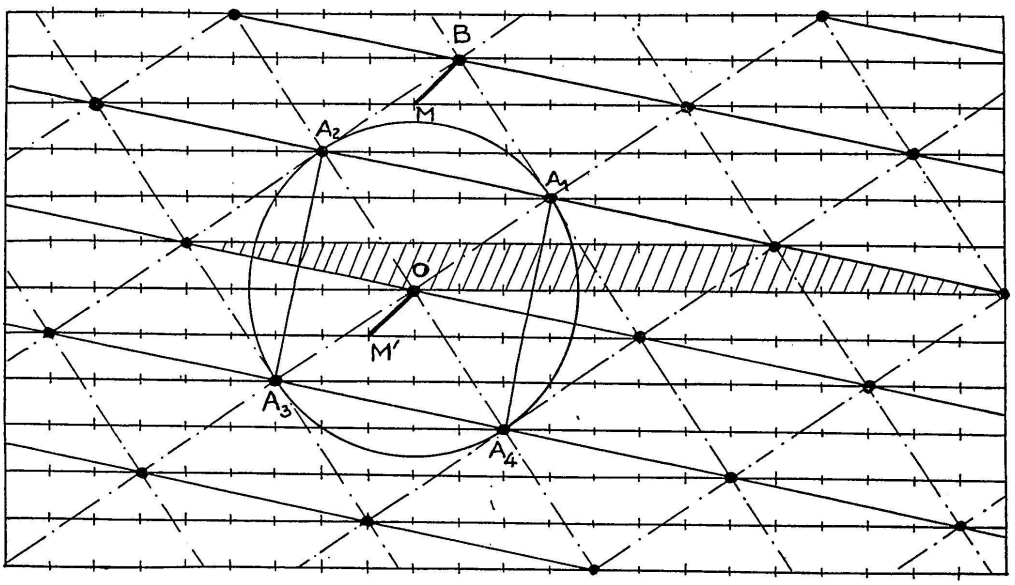
$$2 = (1+i)\times(1-i) = -i\times(1+i)^2.$$

Un nombre premier q, congru à —1, mod. 4, ne peut être la norme d'un idéal canonique; l'idéal principal (q) n'a donc pas de diviseur (entier) sauf lui-même et l'idéal unité.

Un nombre premier p, congru à +1, mod. 4, est la norme commune de deux idéaux canoniques, dont les racines sont deux zéros conjugués c,c', du polynôme x^2+1, considéré mod. p. L'idéal principal (p) en est le produit et chacun d'eux est premier:

$$(p) = (p,\ i-c)\times(p,\ i-c'); \qquad c+c' \equiv 0, \pmod{p}.$$

Reste à montrer que ces deux idéaux sont *principaux*, ceci résulte des propriétés générales, exposées ci-dessous sur les *idéaux réduits*. On peut en donner une démonstration directe par des considérations géométriques sur le *quadrillage* des points représentant les entiers du corps.



Les éléments de l'idéal $(p, i—c)$ sont les entiers algébriques exprimés par:

$$x \times p + y \times (i—c) = (xp—yc) + yi; \qquad x,y \text{ entiers rationnels.}$$

Les points représentatifs sont dans le quadrillage (de tous les entiers) l'ensemble **P** des sommets du réseau de parallélogrammes engendré par les vecteurs joignant l'origine 0 aux points de coordonnées $(p,0)$ et $(—c,1)$. Parmi les points de **P**, on peut distinguer ceux qui sont les plus proches de l'origine (de distance au moins égale à 1). Il en existe au moins 4 (A_1,A_2,A_3,A_4), à une même distance r, représentant des entiers:

$$a+bi, \quad —b+ai = (a+bi) \times i,$$
$$—a—bi = (a+bi) \times i^2, \quad b—ai = (a+bi) \times i^3;$$

ils forment un carré de centre 0. A l'intérieur du cercle circonscrit à ce carré (circonférence exclue) il n'y a pas de point de **P**. (La figure représente les entiers de l'idéal $(13, i—5)$; le point A_1, représente $3+2i = 13+2 \times (i—5)$.)

On peut alors vérifier que le réseau de parallélogrammes peut être engendré par deux vecteurs successifs OA_1 et OA_2, en constatant que le parallélogramme OA_1BA_2 construit avec ces deux vecteurs ne renferme pas de point de **P**. Effectivement un tel point M, étant à l'extérieur du cercle de centre 0 et de rayon r, ne pourrait être que dans le triangle BA_1A_2, et il serait à une distance de B inférieure à r, ce qui est impossible pour une raison évidente de translation, car le point M' extrémité du vecteur OM' équipolent à BM serait à une distance de 0 inférieure à r, tout en appartenant à **P**.

Les points A_1 et A_2 représentent donc des éléments d'une base arithmétique libre de l'idéal et l'élément p est égal à une expression linéaire, à coefficients entiers rationnels x, y:

$$p = x \times (a+bi) + y \times (—b+ai) \quad \Leftrightarrow \quad 0 = xb+ya \text{ et } p = xa—yb.$$

Mais p étant premier, la dernière relation exige que a, b d'une part, x, y d'autre part sont premiers entre eux. De plus, ni a, ni b ne sont nuls; car les idéaux $(bi, —b)$ et (a, ai) sont des idéaux principaux rationnels. L'avant-dernière relation exige donc que:

$$x = a \text{ ou } —a, \quad y = —b \text{ ou } b; \qquad p = a^2+b^2.$$

La dernière relation exprime que p est décomposable en un produit de deux entiers du corps; définis au produit près par des diviseurs de l'unité:

$$p = (a+bi)(a-bi) = (-b+ai)(-b-ai)$$
$$= (-a-bi)(-a+bi) = (b-ai)(b+ai).$$

Ces entiers sont les générateurs d'idéaux conjugués; les propriétés des produits d'idéaux montrent que ces idéaux principaux ont pour norme p et pour racines c et c', solutions de la congruence fondamentale, avec la correspondance:

$$a+bc \equiv 0, \quad a-bc' \equiv 0, \quad (\text{mod. } p).$$

Les propriétés générales de la congruence fondamentale permettent alors d'affirmer la propriété générale suivante:

un *facteur rationnel* m, est décomposable dans $\mathbf{R}(i)$ en un *produit de deux facteurs algébriques conjugués*, ou l'*entier positif* m *est égal à une somme de deux carrés* (de nombres entiers) si et seulement si il est égal au produit ou au double du produit de s puissances de nombres congrus à $+1$, mod. 4; il y a alors 2^{s-1} *décompositions en somme de deux carrés*, différentes (sans distinctoin d'ordre).

(A suivre)