26. Propriétés générales des groupes de classes d'idéaux.

On peut remplacer la racine minimum négative $\overline{c'}$ par la plus petite racine positive $\overline{c'}+m = m+S-\overline{c}$.

Exemple 1 (tableau I). — Dans le corps de discriminant $D = -39$, la valeur de r, déterminée par comparaison avec $|D|$ est 2:

$$3.(2\times 1+1)^2 = 27 < 39 < 3.(2\times 2+1)^2 = 75.$$

Il suffit de chercher les diviseurs de $F(0) = 10$ et de $F(1) = 12$, qui vérifient les conditions de réduction (compris entre $2c+1$ et la racine carrée de $|F(c)|$). On obtient deux idéaux doubles, de normes 1 et 3 (diviseurs de 39):

$$(1,\ \theta-0),\qquad (3,\ \theta-1)$$

et deux idéaux conjugués distincts, de norme 2:

$$(2,\ \theta-0)\qquad (2,\ \theta+1) = (2,\ \theta-1).$$

Il y a quatre idéaux réduits différents, donc au plus quatre classes, on vérifie ci-dessous que c'est effectivement le nombre de classes.

Exemple 2 (tableau II) — Dans le corps de discriminant $D = +60$ la valeur de r est 2:

$$5\times(2\times 1)^2 = 20 < 60 < 5\times(2\times 2)^2 = 80.$$

Il suffit de chercher les diviseurs de $|F(0)| = 15$ et de $|F(1)| = 14$, qui vérifient les conditions de réduction. On obtient ainsi trois idéaux doubles, de normes 1, 3, 2 (diviseurs de 60):

$$(1,\ \theta-0),\qquad (3,\ \theta-0),\qquad (2,\ \theta-1).$$

Il y a au plus trois classes; on vérifie ci-dessous qu'il n'y en a que deux, la classe principale contenant l'idéal de norme 1, d'ailleurs égal à (1) et une classe double contenant les deux idéaux de normes 3 et 2 (dont on peut vérifier qu'ils sont congrus).

26. Propriétés générales des groupes de classes d'idéaux.

Certaines relations entre les classes d'idéaux, d'un corps quadratique, sont des applications de propriétés générales des groupes abéliens d'ordre fini qu'on va indiquer sommairement [1]).

---

[1]) Ces propriétés sont exposées et démontrées dans de nombreux ouvrages. Je me permets de citer: *Arithmétique et Algèbre modernes*, ch. II, § 5 et 7; ch. III, n° 35 (1954 et 1955), ou, pour plus de développements: *Les groupes abéliens finis* (1925).

Deux puissances, d'exposants entiers quelconques, *d'une même classe* (**23**) —ou plus généralement d'un élément A, appartenant à un groupe $\mathfrak{A}$, d'ordre fini, (même non commutatif)— *sont égales*, si et seulement si *les exposants sont congrus*, suivant un certain module n:

$$A^x = A^{x'} \Leftrightarrow \{x \equiv x', \quad (\text{mod. } n)\}$$

On peut exprimer cette condition caractéristique d'égalité en disant que:

la (valeur de la) *puissance* A^x *est caractérisée* —ou représentée proprement— *par l'exposant* x, *entier défini* mod. n —ou par la progression arithmétique $x+\lambda n$, de raison n; ou par la classe d'entiers mod. n (**5**)— .

L'entier (positif) n est appelé l'**ordre** de l'élément A, —ou de la classe— dans le groupe $\mathfrak{A}$ ou $\mathcal{G}|\mathcal{R}$. Si A est l'*élément unité* du groupe, désigné par E, ou (1) —ou $\mathcal{R}$ dans $\mathcal{G}|\mathcal{R}$— son ordre est égal à 1, il est égal à toutes ses puissances, dont les expressions forment la progression arithmétique, de raison 1.

Cette propriété est bien connue et sa vérification est immédiate. Les puissances A^x, x entier quelconque, ne constituent qu'un nombre fini d'éléments différents, au plus égal à l'ordre —ou au nombre d'éléments— du groupe $\mathfrak{A}$. Il y a donc des puissances, d'exposants différents égales entre elles; en choisissant l'une d'elles A^h, on peut construire le plus petit entier positif n, tel que:

$A^{h+n} = A^h$; donc $A^n = A^{-n} = E$, ou (1), élément unité.

La conséquence est obtenue en multipliant les deux membres de l'égalité par l'inverse $(A^h)^{-1} = A^{-h}$. On en déduit, λ étant un entier quelconque:

$$A^{n\lambda} = E^\lambda = E \quad \text{et} \quad x' = x+n\lambda \Rightarrow A^{x'} = A^x \times A^{n\lambda} = A^x;$$

c'est la condition *suffisante* d'égalité.

D'autre part, pour tout entier positif r, la puissance A^{h+r} ne peut être égale à A^h et A^r ne peut être égal à E. On en déduit l'implication réciproque de la précédente:

$$A^{x'} = A^x \Rightarrow A^{(x'-x)} = E \Rightarrow \{x'-x = \lambda n; \quad \lambda \text{ entier}\}.$$

Il suffit de former le reste de la division (arithmétique) de $x'—x$ par n:

$$x'—x = \lambda n+r; \quad 0 \leqslant r < n; \quad \lambda \text{ entier};$$

la puissance d'exposant $x'—x$ est égale à celle d'exposant r, elle ne peut être égale à E, que si r est nul.

L'entier n, dont l'existence est ainsi établie, est indépendant de la puissance A^h, choisie pour le construire. Comme il y a n progressions arithmétiques, de raison n, définies notamment par les entiers de 0 à $n—1$, il y a n éléments différents, égaux aux puissances de A. On justifie ainsi la définition suivante.

DÉFINITION. — *On appelle* **groupe cyclique**, de *générateur* A, et d'*ordre* n, *le système de* n *valeurs des puissances* A^x (x entier défini mod. n), d'un élément A, d'ordre n, dans le groupe $\mathfrak{A}$ —ou $\mathcal{G}|\mathcal{R}$—. Ces valeurs se composent par multiplication dans $\mathfrak{A}$; leur groupe qui sera désigné par **A**, est un *sous-groupe* de $\mathfrak{A}$.

Un groupe cyclique, multiplicatif —ou noté comme tel— d'ordre n, est *isomorphe* au *groupe additif* de ses exposants, définis mod. n.

Il est manifeste que les n valeurs des puissances de A forment un groupe (multiplicatif) puisque leur multiplication, définie dans $\mathfrak{A}$, et réalisée par l'addition des exposants, est associative et que deux puissances d'*exposants opposés* sont *inverses* —ou de produit égal à l'élément unité E— :

$A^x \times A^y = A^{x+y}$, $A^{-x} \times A^x = E$; $x,y,x+y,(—x)$, définis mod. n.

La représentation d'un élément A^x par son exposant x, mod. n, est *propre* —ou est une correspondance biunivoque— elle fait correspondre l'opération de multiplication (alors nécessairement commutative) avec l'addition; ce sont ces deux qualités qu'exprime le terme d'*isomorphisme*.

On peut représenter le groupe additif des entiers, mod. n, par les *rotations*, autour d'un axe —ou autour d'un point dans un plan— d'angles multiples de $(2\pi : n)$. Au produit —ou composition— commutatif de deux rotations correspond la somme des arcs —ou de leurs mesures, au module 2π près—. Cette représentation explique le qualificatif *cyclique*.

On peut aussi bien construire le groupe cyclique **A**, de générateur A et d'ordre n, en formant *les puissances d'un de ses éléments* A^a, construit toutefois avec un exposant a, *premier avec* n:

$$(A^a)^y = A^{a\times y}; \quad y \text{ défini mod. } n;$$

on peut notamment prendre pour valeurs de y, les n entiers de 0 à n—1.

On constate en effet que les nouveaux exposants y vérifient la même condition caractéristique d'égalité des puissances:

$$\{(ay'—ay) = a(y'—y) \equiv 0, \pmod{n}\} \Leftrightarrow \{y' \equiv y, \pmod{n}\}.$$

L'équivalence résulte du fait que n, premier avec a, ne peut diviser le produit $a(y'—y)$ qu'en divisant le second facteur.

Une telle puissance A^a est encore un *générateur* du groupe cyclique **A**. Un groupe cyclique, d'ordre n, a ainsi $\varphi(n)$ générateurs.

On rappelle que la fonction $\varphi(n)$, de l'entier (positif) n, appelée l'*indicateur* d'EULER, est le nombre d'entiers, positifs, inférieurs à n —ou d'entiers, définis mod. n— premiers avec n.

Sa valeur, pour n égal à une puissance p^h, d'un nombre premier, est

$$\varphi(p^h) = (p—1)\times p^{h-1}; \quad \varphi(2^h) = 2^{h-1}.$$

Pour un produit de puissances de nombres premiers différents —et, plus généralement, pour un produit de nombres m_i premiers entre eux, deux à deux— sa valeur est égale au produit des valeurs pour chacun des facteurs:

$$\varphi(\Pi m_i) = \Pi(\varphi(m_i)); \quad m_i = p_i^{hi}.$$

Il est équivalent de dire qu'*une puissance* A^h, d'un élément A, d'ordre n, *est aussi un élément d'ordre* n, lorsque h *est premier avec* n. Dans le cas général, il est aisé de constater que l'ordre de cette puissance est égal au quotient de n par le p.g.c.d. de h et n.

Lorsque, dans un groupe $\mathfrak{A}$, d'ordre fini —notamment dans $\mathcal{G}|\mathcal{R}$— *il existe un élément A dont l'ordre est égal à celui du groupe* —ou au nombre de ses éléments— le groupe, qui est alors

évidemment formé des seules puissances de A, est, lui-même, *un groupe cyclique, de générateur A* —ou est égal à **A**— .

Un raisonnement, usuel et simple, montre que, dans un groupe, même non commutatif, d'ordre fini, l'ordre de tout sous-groupe, et, notamment, *l'ordre de tout élément est diviseur de* (et éventuellement égal à) *l'ordre du groupe.*

Un sous-groupe définit une *répartition* des éléments du groupe en classes, dont chacune est formée des produits des éléments du sous-groupe par un élément du groupe n'appartenant pas à une autre classe —et défini lui-même au produit près par un élément du sous-groupe—. L'ordre du groupe est, par suite, égal au produit de l'ordre du sous-groupe par le nombre de classes, ainsi constituées.

En rapprochant ces deux propriétés, on constate que: *un groupe, dont l'ordre g est un nombre premier, est cyclique*, puisque l'ordre de tout élément, à l'exception de E, ou (1), étant diviseur de g, ne peut que lui être égal, en sorte que cet élément est un générateur du groupe, qui en a $\varphi(g) = g-1$.

DÉFINITION. — *Dans un groupe abélien* —ou commutatif— $\mathfrak{A}$, d'ordre fini —notamment dans $\mathfrak{G}|\mathfrak{R}$—, *deux éléments*, différents de l'unité E:

$$A, \text{ d'ordre } u; \qquad B, \text{ d'ordre } v;$$

—ou *les sous-groupes cycliques* **A** et **B**, qu'ils engendrent— *sont* qualifiés **indépendants**, lorsque *ces sous-groupes n'ont, en commun, que le seul élément unité E*:

$$A^x = B^y \iff \{x \equiv 0, \pmod{u} \text{ et } y \equiv 0, \pmod{v}\};$$

dans le vocabulaire de l'algèbre des ensembles: l'intersection [**A**,**B**] des deux sous-groupes est égal au sous-groupe trivial, formé du seul élément unité E.

Il est équivalent de dire que le monôme $A^x \times B^y$ n'est égal à l'élément unité E que si x et y sont respectivement congrus à 0, suivant les modules u et v.

Deux éléments sont notamment indépendants, lorsque leurs

ordres u et v sont *premiers entre eux*. Car, dans ce cas:

$$A^x = B^y \Rightarrow A^{xv} = B^{yv} = E$$
$$\Rightarrow xv \equiv 0, \pmod{u} \Rightarrow x \equiv 0;$$
$$\Rightarrow B^y = E \Rightarrow y \equiv 0, \pmod{v}.$$

DÉFINITION. — On appelle **produit direct** *de deux sous-groupes cycliques indépendants*, **A** de générateur A, d'ordre u et **B** de générateur B, d'ordre v, *le sous-groupe constitué par le système de monômes*;

$$A^x \times B^y; \quad x, \text{ mod. } u, \quad y, \text{ mod. v};$$

—ou par les produits, en nombre $u \times v$, de chaque élément de **A** par chaque élément de **B** (dans un ordre quelconque, puisque $\mathfrak{A}$ est *abélien*)— .

Ce produit direct est désigné par $\mathbf{A} \times \mathbf{B}$ et le *couple* de générateurs A,B en est appelé une *base*.

Les monômes ainsi constitués sont bien inégaux, car, en raison de la *commutativité de la multiplication*, dans le groupe $\mathfrak{A}$ et de l'*indépendance des générateurs*:

$$A^x \times B^y = A^{x'} \times B^{y'}$$
$$\Rightarrow A^{x'-x} \times B^{y'-y} = E \quad \text{ou} \quad (1)$$
$$\Rightarrow \{x'-x \equiv 0, \pmod{u} \text{ et } y'-y \equiv 0, \pmod{v}\}.$$

Ils constituent un groupe, car le produit (ou le quotient) de deux monômes est encore un monôme, obtenu par les sommes (ou les différences) des exposants respectifs:

$$(A^x \times B^y) \times (A^{x'} \times B^{y'}) = A^{x+x'} \times B^{y+y'};$$
$$(A^x \times B^y) \times (A^{-x} \times B^{-y}) = E.$$

Les monômes sont représentés proprement par les couples d'exposants $\|x\ y\|$. On dit encore que le produit direct $\mathbf{A} \times \mathbf{B}$, des groupes cycliques multiplicatifs est isomorphe au *produit direct des groupes additifs*, des entiers, mod. u et mod. v.

Le sous-groupe cyclique **A**, de générateur A, peut être considéré comme égal à son produit direct par le sous-groupe trivial (E), formé du seul élément unité E.

On peut étendre par *récurrence* les notions d'*indépendance* et de *produit direct* à un nombre quelconque s, d'éléments d'un groupe abélien et aux sous-groupes cycliques qu'ils engendrent.

Des éléments d'un groupe abélien, en nombre s:

$$A_i, \quad \text{d'ordre } u_i, \qquad (i \text{ de } 1 \text{ à } s);$$

—ou les sous-groupes cycliques $\mathbf{A}_i$, qu'ils engendrent— sont qualifiés **indépendants**, lorsque: les s—1 premiers le sont et que *leur produit direct* $\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}$ *et le groupe cyclique* $\mathbf{A}_s$, engendré par le dernier élément A_s, *n'ont en commun que le seul élément unité* E; [l'intersection $[\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}, \ \mathbf{A}_s]$ est égal à (E)].

On appelle **produit direct** de s sous-groupes cycliques indépendants, $\mathbf{A}_i$ engendré par l'élément A_i, le système des produits de tout élément du produit direct $\mathbf{A}_1 \times \ldots \times \mathbf{A}_{s-1}$ par tout élément de $\mathbf{A}_s$.

L'indépendance et le produit direct ayant été définis pour $s = 2$, sont ainsi définis, ou construits, de proche en proche pour $s = 3$, puis 4, ... puis s. On en déduit des propriétés caractéristiques, indépendantes de l'ordre adopté pour les éléments.

Les éléments A_i —ou les sous-groupes $\mathbf{A}_i$— sont *indépendants* si un monôme formé avec les A_i n'est égal à l'élément unité E, que pour des exposants respectivement congrus à 0, relativement à l'ordre de l'élément qu'ils affectent:

$$A_1^{x_1} \times \ldots A_s^{x_s} = E \quad \Leftrightarrow \quad \{x_i \equiv 0, \pmod{u_i}; \quad \text{tout } i\}$$

Le *produit direct* des sous-groupes cycliques $\mathbf{A}_i$, est le système des monômes, en nombre $u_1 \times \ldots \times u_s$;

$$A_1^{x_1} \times \ldots \times A_s^{x_s}; \quad x_i \text{ défini mod. } u_i.$$

Ces monômes sont inégaux; ils constituent un sous-groupe de $\mathfrak{A}$, leur multiplication, définie dans $\mathfrak{A}$, est réalisée par l'addition des exposants respectifs. Ils sont représentés proprement par les systèmes —ou le s-uple— de leurs exposants. On dit encore que leur groupe est

isomorphe au *produit direct des s groupes additifs*, des entiers définis respectivement suivant les modules u_i.

On généralise aisément les propriétés indiquées pour $s = 2$ et $s = 1$.

1. *Des éléments* A_i, d'ordre u_i, *sont*, notamment, *indépendants lorsque leurs ordres* u_i *sont premiers entre eux, deux à deux*, chacun d'eux étant, par suite, premier avec le produit des autres.

2. *L'ordre d'un produit direct*, de s sous-groupes cycliques indépendants (dans un groupe abélien $\mathfrak{A}$) est égal au produit Πu_i, des ordres u_i, des sous-groupes composants.

3. Si, dans un groupe abélien $\mathfrak{A}$, d'ordre fini g, il existe s éléments indépendants A_i, dont le produit des ordres Πu_i est égal à l'ordre g, de $\mathfrak{A}$, ce groupe, qui est évidemment formé des seuls monômes des A_i, est égal au produit direct des groupes cycliques $\mathbf{A}_i$, qu'ils engendrent:

$$u_1 \times \ldots \times u_s = g \quad \Rightarrow \quad \mathfrak{A} = \mathbf{A}_1 \times \ldots \times \mathbf{A}_s.$$

En particulier *un groupe cyclique* $\mathbf{A}$, de générateur A, dont l'ordre g est décomposable en un produit d'entiers g_i (i de 1 à s), premiers entre eux, deux à deux, —notamment puissances de nombres premiers différents— *est égal au produit direct des sous-groupes cycliques*, engendrés par les s générateurs:

$$A_i^{g:g_i}, \quad \text{d'ordre } g_i.$$

Exemple. — Dans un groupe cyclique, d'ordre $15 = 3 \times 5$:

$$A^z, \quad [z, \text{ mod. } 15] = (A^3)^x \times (A^5)^y; \quad [x, \text{ mod. } 5; \ y, \text{ mod. } 3].$$

La relation entre les entiers z et x,y est exprimée par les congruences:

$$z \equiv 3x+5y, \quad (\text{mod. } 15)$$

$$\Rightarrow \quad \{z \equiv 3x, \quad (\text{mod. } 5) \quad \text{et} \quad z \equiv 5y, \quad (\text{mod. } 3)\}$$

$$\Rightarrow \quad \{x \equiv 2z, \quad (\text{mod. } 5) \quad \text{et} \quad y \equiv 2z, \quad (\text{mod. } 3)\}.$$

Réciproquement, *un produit direct de groupes cycliques, d'ordres premiers entre eux, deux à deux,* —notamment de puissances de nombres premiers différents— *est égal à un groupe cyclique*, dont un générateur est égal au produit des générateurs des groupes composants.

THÉORÈME de decomposition des groupes abéliens d'ordre fini. *Tout groupe abélien* $\mathfrak{A}$, d'ordre fini, *est égal à un produit direct de groupes cycliques*, dont les générateurs sont des éléments indépendants, convenablement choisis dans $\mathfrak{A}$, différents de **E**.

Pour cette construction qui peut, en général être réalisée de diverses façons, on peut toujours disposer des sous-groupes composants $\mathbf{A}_i$ et de leur numérotage, de façon que *l'ordre* g_i, de chacun d'eux, *soit diviseur de* —ou égal à— *l'ordre* g^{i+1} *du suivant* [1]).

Ceci peut encore être réalisé, en général, par divers choix possibles des sous-groupes cycliques; toutefois *leur nombre* r, *est déterminé, ainsi que leurs ordres* g_i. Toute décomposition du groupe en produit cyclique comporte alors au moins r groupes composants et *la décomposition*, ainsi formée, *est*, en quelque sorte, *minimum.*

D'une façon opposée, on peut construire une *décomposition maximum*, en un produit direct de groupes cycliques, *dont les ordres sont des puissances de nombres premiers*, en remplaçant dans la décomposition minimum éventuellement chaque sous-groupe cyclique par un produit de cette forme. Les ordres ainsi obtenus sont encore déterminés.

EXEMPLE. — Un groupe abélien, d'ordre 12, produit direct de groupes cycliques d'ordre 2 et 6 a pour éléments 12 monômes:

$$A^x \times B^y; \quad x, \text{ mod. } 2; \quad y, \text{ mod. } 6.$$

Aucun n'est d'ordre 12 (leurs ordres étant 6, ou 3, ou 2 —ou 1 pour

---

[1]) La démonstration de ce théorème et des précisions qui en sont données est plus complexe que celles des propriétés précédentes. On peut la rattacher à une analyse linéaire diophantienne, ou à des propriétés générales de décomposition d'un module —ou groupe additif— en somme —ou produit— directe. Je renvoie aux ouvrages cités ci-dessus.

l'élément unité—, le groupe n'est donc pas cyclique et sa décomposition est *minimum*. Elle peut être réalisée en remplaçant A par un des trois éléments d'ordre 2, et B par un des quatre éléments d'ordre 6, dont les puissances ne contiennent pas A; ceci donne 12 décompositions possibles:

A et B;	A et B^5;	A et $A\times B$;	A et $A\times B^5$
B^3 et $A\times B$;	B^3 et $A\times B^5$;	B^3 et $A\times B^2$;	B^3 et $A\times B^4$
$B^3\times A$ et $B^2\times A$;	$B^3\times A$ et $B^4\times A$;	$B^3\times A$ et A;	$B^3\times A$ et A^5

On peut encore construire une décomposition *maximum*, en groupes cycliques d'ordres 2, 2, 3, par exemple:

$$A^x\times(B^3)^{y'}\times(B^2)^{y''};\quad x,y',\ \text{mod. } 2,\quad y''\ \text{mod. } 3.$$