SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

FRANÇOIS GAUTHIER

Ensemble des nombres premiers représentés par une forme quadratique binaire

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 6, p. 1-34

<http://www.numdam.org/item?id=STNG_1974-1975__4__A6_0>

17 avril 1975
Grenoble

ENSEMBLE DES NOMBRES PREMIERS REPRESENTES PAR UNE FORME QUADRATIQUE BINAIRE

par François GAUTHIER

Chapitre I

ENSEMBLES D'IDEAUX PREMIERS A TYPE DE DECOMPOSITION PRESCRIT

Remarque préliminaire : La présente rédaction ne reflète pas exactement l'exposé du 17 avril. Nous avons en effet incorporé une étude des ensembles $Spl(K)$ et $Spl^1(K)$ qui donne une plus grande consistance à la première partie ; de même la deuxième partie se voit agrémentée d'exemples que (faute de temps) nous n'avions pas pu traiter lors de l'exposé.

Notations.

Si A et B sont deux ensembles, on désigne par $A\backslash B$ la différence de A et B, c'est-à-dire l'ensemble des x appartenant à A, mais non à B ; et par $A\Delta B$ la différence symétrique de A et B, c'est-à-dire l'ensemble $(A\backslash B)\cup(B\backslash A)$; alors $A \hat{\subset} B$ (resp. $A \hat{=} B$) signifie que l'ensemble $A\backslash B$ (resp. $A\Delta B$) est fini (c'est-à-dire que A est inclus dans B (resp. est égal à B) à une partie finie près ; dans les cas qui vont nous intéresser, A et B seront des ensembles d'idéaux premiers d'un corps de nombres, et la partie finie en question sera constituée d'idéaux ramifiés dans une extension finie dudit corps de nombres). Par ailleurs si A est un ensemble, on note $|A|$ son cardinal.

Si Q est un corps de nombres quelconque, on désigne par $\mathfrak{M}_Q$

l'ensemble des idéaux maximaux de Q ; en particulier si $Q = \mathbb{Q}$, corps des rationnels, et si P désigne l'ensemble des nombres premiers, $\mathfrak{M}_{\mathbb{Q}}$ s'identifie à P. Si K est une extension galoisienne (finie) de Q, de groupe de Galois G, et si on désigne par S_Q l'ensemble des $\mathfrak{p} \in \mathfrak{M}_Q$ qui sont ramifiés dans K, et par $S_{K/Q}$ l'ensemble des $\mathfrak{P} \in \mathfrak{M}_K$ qui divisent les $\mathfrak{p}$ appartenant à S_Q, on note $\sigma_{K/Q}$ l'application de Frobénius de $\mathfrak{M}_K \backslash S_{K/Q}$ dans G, et $F_{K/Q}$ l'application d'Artin de $\mathfrak{M}_Q \backslash S_Q$ dans l'ensemble des classes de conjugaison de G. Si $E = \{C_i ; 1 \leq i \leq t\}$ est un ensemble de classes de conjugaison de G, on désigne par $F_{K/Q}^{-1}[\bigcup_{i=1}^{t} C_i]$ l'ensemble des $\mathfrak{p} \in \mathfrak{M}_Q \backslash S_Q$ tels que

$$F_{K/Q}(\mathfrak{p}) \in E \quad .$$

Soit K une extension <u>quadratique</u> de $\mathbb{Q}$ (corps des rationnels) ; si $\mathfrak{O}$ est un ordre de K, on désigne par f son conducteur ; par $\mathfrak{O}_K$ l'anneau des entiers de K ; par $\mathfrak{I}_{\mathfrak{O}}$ (resp. $\mathfrak{I}_K$) le groupe des idéaux fractionnaires inversibles de $\mathfrak{O}$ (resp. de K) ; par $\mathfrak{P}_{\mathfrak{O}}$ le sous-groupe de $\mathfrak{I}_{\mathfrak{O}}$ formé des idéaux principaux ; par $\mathfrak{P}_{\mathfrak{O}}^{+}$ le sous-groupe de $\mathfrak{P}_{\mathfrak{O}}$ formé des idéaux principaux (α), tels que $N_{K/\mathbb{Q}}(\alpha) > 0$; par $\mathfrak{I}_K^f$ (resp. $\mathfrak{I}_{\mathfrak{O}}^f$) le sous-groupe de $\mathfrak{I}_K$ (resp. de $\mathfrak{I}_{\mathfrak{O}}$) formé des idéaux premiers avec f ; et enfin par $(\mathfrak{P}_{\mathfrak{O}}^f)^+$ le sous-groupe $(\mathfrak{P}_{\mathfrak{O}}^+) \cap (\mathfrak{I}_{\mathfrak{O}}^f)$. Considérons l'application de l'ensemble des idéaux maximaux de $\mathfrak{O}$, premiers avec f, dans l'ensemble des idéaux maximaux de K, premiers avec f, et définie par $\mathfrak{p} \longmapsto \mathfrak{p}\mathfrak{O}_K$ ([La] pp. 91-95) ; cette application est une bijection et induit par linéarité une bijection que nous notons i entre $\mathfrak{I}_{\mathfrak{O}}^f$ et $\mathfrak{I}_K^f$.

§1 - Etude des ensembles Spl(K) ou $Spl^1(K)$.

On désigne par Q un corps de nombres quelconque, fixé une fois pour toutes. On choisit une clôture algébrique $\overline{Q}$ de Q et on ne considère que des extensions finies de Q contenues dans $\overline{Q}$. Si K est une telle extension, on rappelle que l'enveloppe normale de K (au-dessus de Q) est le plus petit sous-corps de $\overline{Q}$, contenant K et ses conjugués.

1.1. Caractérisation de Spl(K) et $Spl^1(K)$.

Si K est une extension (finie) de Q , on rappelle qu'on désigne par $Spl_Q(K)$ (ou plus simplement Spl(K)) l'ensemble des $p \in \mathfrak{M}_Q$ qui sont complètement décomposés dans K . De même :

DEFINITION.- On désigne par $Spl_Q^1(K)$ (ou plus simplement $Spl^1(K)$) l'ensemble des $p \in \mathfrak{M}_Q$ qui admettent au moins en facteur de degré 1 dans K .

Soit K une extension (finie) de Q ; désignons par L l'enveloppe normale(*) de K (au-dessus de Q) , par G (resp. H) le groupe de Galois de l'extension L/Q (resp. L/K), par S l'ensemble des $p \in \mathfrak{M}_Q$ qui sont ramifiés dans L ; nous avons la caractérisation suivante :

PROPOSITION I .1.1.- Pour $p \in \mathfrak{M}_Q \backslash S$, les assertions suivantes sont équivalentes :

(i) $p \in Spl^1(K)$ (resp. $p \in Spl(K)$) ;

(ii) il existe $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}|p$ et que $\sigma_{L/Q}(\mathfrak{P}) \in H$ (resp. pour tout $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}|p$ on a $\sigma_{L/Q}(\mathfrak{P}) \in H$).

(*) ou simplement une extension galoisienne de Q , contenant K .

COROLLAIRE 1.- (i) $\mathrm{Spl}^1(K) \triangleq F_{L/Q}^{-1}[\bigcup_{\tau\in G} \tau H\tau^{-1}]$;

(ii) $\mathrm{Spl}(K) \triangleq F_{L/Q}^{-1}[\bigcap_{\tau\in G} \tau H\tau^{-1}]$.

COROLLAIRE 2.- (i) $\mathrm{Spl}^1(K)$ admet une densité analytique δ^1 égale à : $|\bigcup_{\tau\in G} \tau H\tau^{-1}|.|G|^{-1}$;

(ii) $\mathrm{Spl}(K)$ admet une densité analytique δ égale à : $|\bigcap_{\tau\in G} \tau H\tau^{-1}|.|G|^{-1}$;

(iii) δ^1 (resp. δ) est égal à 1 si et seulement si $K = Q$.

Démonstration de la proposition I .1.1 : Si $p \in \mathfrak{M}_Q \backslash S$, si $\mathfrak{P} \in \mathfrak{M}_L$ et si $\mathfrak{P}/p$, désignons par $G_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$ (dans G) , par $K_{\mathfrak{P}}$ le corps des invariants de $G_{\mathfrak{P}}$ dans L , par $\mathfrak{q}$ l'idéal $\mathfrak{P} \cap K$.

Supposons $p \in \mathrm{Spl}^1(K)$; alors il existe $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}/p$ et $f(\mathfrak{q}/p) = 1$; comme $\sigma_{L/K}(\mathfrak{P}) = [\sigma_{L/Q}(\mathfrak{P})]^{f(\mathfrak{q}/p)} = \sigma_{L/Q}(\mathfrak{P})$ et $\sigma_{L/K}(\mathfrak{P}) \in H$, on a $\sigma_{L/Q}(\mathfrak{P}) \in H$.

Réciproquement, s'il existe $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}/p$ et $\sigma_{L/Q}(\mathfrak{P}) \in H$, alors $G_{\mathfrak{P}} \subset H$ donc $K \subset K_{\mathfrak{P}}$; or on sait (voir par ex. [Sa]) que $f[(\mathfrak{P} \cap K_{\mathfrak{P}})/p] = 1$, par suite $f(\mathfrak{q}/p) = 1$ et $p \in \mathrm{Spl}^1(K)$.

La démonstration de l'équivalence concernant $\mathrm{Spl}(K)$ est analogue ■

Démonstration du corollaire 1 : Pour le (i) il suffit de remarquer que l'assertion (ii) de la proposition I .1.1 équivaut (toujours pour $p \in \mathfrak{M}_Q \backslash S$) à

($\mathcal{C}^1$) "la classe de conjugaison $F_{L/Q}(p)$ et H ont au moins un élément commun".

Pour le (ii), remarquons que l'assertion (ii) de la proposition I .1.1 équivaut à :

(C) "la classe de conjugaison $F_{L/Q}(\mathfrak{p})$ est contenue dans H" .

Soit alors $\mathfrak{P}_o$ un idéal particulier de $\mathfrak{M}_L$ tel que $\mathfrak{P}_o/\mathfrak{p}$; (C) équivaut à :

"pour tout $\tau \in G$ on a $\tau\sigma_{L/Q}(\mathfrak{P}_o)\tau^{-1} \in H$" ,

donc à :

"pour tout $\tau \in G$ on a $\sigma_{L/Q}(\mathfrak{P}_o) \in \tau^{-1}H\tau$ "

et par conséquent au résultat annoncé ∎

Démonstration du corollaire 2 : (i) et (ii) résulte immédiatement du théorème d'Artin-Tchebotarev ; remarquons qu'il faut vérifier que $\bigcap_{\tau\in G} (\tau H\tau^{-1})$ est une réunion de classes de conjugaison de G , mais cette vérification est immédiate. Pour le (iii) remarquons que si $K \neq Q$, on a l'inclusion stricte $H \subsetneq G$ et que par suite on a aussi l'inclusion stricte $\bigcup_{\tau\in G} (\tau H\tau^{-1}) \subsetneq G$ (résultat "bien connu" voir par ex. [D.D] p. 73, th.5) donc $\delta^1 < 1$ ∎

1.2. Application I : Caractérisation des extensions galoisiennes.

Soit K une extension (finie) de Q ; désignons par δ^1 (resp. δ) la densité de l'ensemble $Spl^1(K)$ (resp. Spl(K)) , nous avons alors la :

PROPOSITION I .1.2.- Les assertions suivantes sont équivalentes

(i) K/Q est galoisienne.

(ii) $Spl^1(K) \triangleq Spl(K)$.

(iii) $\delta^1 = [K:Q]^{-1}$.

(iv) $\delta = [K:Q]^{-1}$.

(v) pour tout $\mathfrak{p} \in \mathfrak{M}_Q$, on a dans K : $\mathfrak{p} = \prod_{i=1}^{g(\mathfrak{p})} \mathfrak{P}_i^{e(\mathfrak{P}_i/\mathfrak{p})}$ avec $e(\mathfrak{P}_i/\mathfrak{p})$ et $f(\mathfrak{P}_i/\mathfrak{p})$ indépendants de i (mais dépendant naturellement de $\mathfrak{p}$).

Démonstration : On sait que la première assertion entraîne les 4 autres. D'autre part, si nous conservons les notations du paragraphe 1.1 et si nous supposons l'extension K/Q non galoisienne alors H n'est pas un sous-groupe distingué de G et par suite il existe au moins un $\tau \in G$ tel que $\tau H \tau^{-1} \neq H$ donc

$$\left| \bigcap_{\tau \in G} \tau H \tau^{-1} \right| < |H| < \left| \bigcup_{\tau \in G} \tau H \tau^{-1} \right|$$

et par suite

$$\delta < [K:Q]^{-1} < \delta^1 .$$

Les quatre premières assertions sont donc équivalentes.

Supposons maintenant (v) réalisé en particulier cela entraîne $Spl^1(K) = Spl(K)$, et K/Q est donc galoisienne, d'après "(ii) implique (i)" ∎

1.3. Application II : "théorème de Bauer".

THEOREME I.1.3. - Soit K/Q (resp. L/Q) une extension galoisienne (resp. quelconque) de corps de nombres ; les deux assertions suivantes sont équivalentes :

(i) $K \subset L$;

(ii) $Spl^1(L) \hat{\subset} Spl^1(K)$ $(= Spl(K))$.

Démonstration : Si $K \subset L$ il est clair que $Spl^1(L) \subset Spl^1(K)$; on peut noter que pour cette implication l'hypothèse K/Q galoisienne n'est pas nécessaire.

Supposons maintenant que $Spl^1(L) \hat{\subset} Spl^1(K) = Spl(K)$. Désignons par N l'enveloppe normale de KL au-dessus de Q , par G (resp. J, resp. H) le groupe de Galois de l'extension N/Q (resp. N/K, resp. N/L) , par S l'ensemble (fini) des $\mathfrak{p} \in \mathfrak{M}_Q$ qui sont ramifiés dans N ou qui appartiennent à $[Spl^1(L)] \setminus [Spl^1(K)]$. Soit alors $\mu \in H$;

comme l'application $\sigma_{N/Q}$ est surjective, il existe $\mathfrak{P} \in \mathfrak{M}_N$ tel que $\mathfrak{P} \cap Q \in \mathfrak{M}_Q \backslash S$ et que $\sigma_{N/Q}(\mathfrak{P}) = \mu$; par suite $\mathfrak{p} = \mathfrak{P} \cap Q \in Spl^1(L)$ (proposition I .1.1) ; donc $\mathfrak{p} \in Spl^1(K) = Spl(K)$ puisque K/Q est galoisienne ; mais alors $\mu = \sigma_{N/Q}(\mathfrak{P}) \in J$ (proposition I .1.1) ; il en résulte que $H \subset J$, c'est-à-dire $K \subset L$ ■

Remarque 1 : Si on fait l'hypothèse supplémentaire : "L/Q est galoisienne", on a une démonstration beaucoup plus courte de l'implication (ii) ⇒ (i) : en effet, les hypothèses impliquent

$$Spl(KL) \triangleq [Spl(K)] \cap [Spl(L)] \hat{=} Spl(L)$$

il résulte alors du théorème d'Artin-Tchebotarev que $[KL:Q] = [L:Q]$ donc $KL = L$ et $K \subset L$ (cf. [C.F] p. 362).

Remarque 2 : Les ensembles Spl( ) "classifient" les extensions galoisiennes, car si K/Q et L/Q sont galoisiennes , $K = L$ équivaut à $Spl(K) \hat{=} Spl(L)$. On peut noter que si L/Q n'est pas galoisienne, l'équivalence ne subsiste pas, comme le montre l'exemple suivant : avec $Q = \mathbb{Q}$ corps des rationnels, $K = \mathbb{Q}^{(3)}(\sqrt[3]{2})$ et $L = \mathbb{Q}(\sqrt[3]{2})$, on a $Spl(K) = Spl(L)$.

Remarque 3 : On ne peut pas enlever l'hypothèse "K/Q galoisienne" dans l'énoncé du théorème de Bauer ; on peut en effet trouver deux extensions $K/\mathbb{Q}$ et $L/\mathbb{Q}$ ($\mathbb{Q}$= le corps des rationnels) non galoisiennes et non isomorphes, mais telles que $Spl^1(K) \hat{=} Spl^1(L)$; un exemple de cette situation est le suivant : ([Gas] ou [C.F] pp. 362-363) :

Soit $G = \mathfrak{S}_6$, le groupe symétrique permutant 6 lettres (x_i) , notons :

$$H_1 = \{1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)\}$$

$$H_2 = \{1, (x_1x_2)(x_3x_4), (x_1x_2)(x_5x_6), (x_3x_4)(x_5x_6)\} \quad ;$$

désignons par N une extension galoisienne de $\mathbb{Q}$ admettant G pour groupe de Galois (une telle extension existe [H_i]), par K (resp.L) le corps des invariants de H_1 (resp. de H_2) dans N , par S l'ensemble des $p \in P$ qui sont ramifiés dans N .

On vérifie facilement que si une classe de conjugaison de G contient un élément (autre que 1) de H_1 ou de H_2, alors elle contient tous les éléments (autres que 1) de H_1 et de H_2 ; il en résulte que pour $p \in P\backslash S$, $F_{N/\mathbb{Q}}(p) \cap H_1 \neq \emptyset$ équivaut à $F_{N/\mathbb{Q}}(p) \cap H_2 \neq \emptyset$ et par suite $Spl^1(K) \hat{=} Spl^1(L)$ alors que K et L ne sont pas conjugués (donc ne sont pas isomorphes) puisque H_1 et H_2 ne sont pas conjugués (H_1 laisse fixe x_5 et x_6 alors que H_2 ne laisse aucune lettre fixe).

§2 - Etude particulière des extensions abéliennes de $\mathbb{Q}$.

Dans ce paragraphe, on se limite à $Q = \mathbb{Q}$, corps des rationnels.

Si m est un entier ≥ 2, on désigne par $G(m)$ le groupe $(\mathbb{Z}/m\mathbb{Z})^*$ d'ordre $\varphi(m)$; par ζ_m une racine primitive m-ième de l'unité ; par $K^{(m)}$ le corps $K(\zeta_m)$; et par G_m le groupe de Galois de $\mathbb{Q}^{(m)}/\mathbb{Q}$. Si de plus r est un entier premier avec m, on désigne par $r \bmod m$ l'image de r dans $G(m)$; et par $P_m(r)$ l'ensemble des $p \in P$ tels que $p \equiv r \pmod m$.

Nous avons alors la caractérisation bien classique suivante :

PROPOSITION I .2.- *Soit $K/\mathbb{Q}$ une extension galoisienne, les deux assertions suivantes sont équivalentes* :

(i) *$K/\mathbb{Q}$ est une extension abélienne* ;

(ii) *il existe un entier $m \geq 2$ et des entiers r_i, $1 \leq i \leq t$, premiers avec m tels que*

$$Spl(K) \hat{=} \bigcup_{i=1}^{t} P_m(r_i) ,$$

l'ensemble $\{r_i \bmod m / 1 \leq i \leq t\}$ étant un sous-groupe de $G(m)$.

Démonstration : Soit $K/\mathbb{Q}$ une extension abélienne, alors il existe un entier $m \geq 2$ tel que $K \subset \mathbb{Q}^{(m)}$ [théorème de Kronecker-Weber]. Désignons par S l'ensemble des diviseurs premiers de m. Si $p \in P \backslash S$, l'assertion $p \in Spl(K)$ équivaut à $F_{K/\mathbb{Q}}(p) = 1$ donc à $F_{\mathbb{Q}^{(m)}/\mathbb{Q}}(p) \in Gal(\mathbb{Q}^{(m)}/K)$. Soit $\mathfrak{R} = \{r\}$ un système de représentants de $G(m)$, on sait que G_m est formé par l'ensemble des λ_r, pour r parcourant $\mathfrak{R}$, où λ_r est caractérisé par $\lambda_r(\zeta_m) = \zeta_m^r$; on sait d'autre part que $F_{\mathbb{Q}^{(m)}/\mathbb{Q}}(p)$ est caractérisé par $F_{\mathbb{Q}^{(m)}/\mathbb{Q}}(p)(\zeta_m) = \zeta_m^r$; donc $F_{\mathbb{Q}^{(m)}/\mathbb{Q}}(p) = \lambda_r$ équivaut à $p \in P_m(r)$; par suite $Spl(K)$ est à une partie finie près la réunion des $P_m(r)$, pour λ_r parcourant le groupe $Gal(\mathbb{Q}^{(m)}/K)$. Choisissons des indices tels que l'ensemble des λ_{r_i}, $1 \leq i \leq t = |Gal(\mathbb{Q}^{(m)}/K)|$ coïncide avec le groupe $Gal(\mathbb{Q}^{(m)}/K)$ et désignons par θ l'isomorphisme $G_m \mapsto G(m)$ "inverse" en un sens évident de l'application d'Artin $F_{\mathbb{Q}^{(m)}/\mathbb{Q}}$, alors l'ensemble $\{r_i \bmod m / 1 \leq i \leq t\}$ est l'image par θ du groupe $Gal(\mathbb{Q}^{(m)}/K)$.

Réciproquement, si (ii) est réalisée, le sous-groupe $\{r_i \bmod m / 1 \leq i \leq t\}$ de $G(m)$ contient l'élément neutre 1 mod m et par suite :

$$P_m(1) = Spl(\mathbb{Q}^{(m)}) \hat{\subset} Spl(K)$$

donc $K \subset \mathbb{Q}^{(m)}$ et $K/\mathbb{Q}$ est abélienne ∎

Remarque : Nous verrons plus loin (corollaire 3 de la proposition I .3.4) que (ii) peut être remplacée par la condition moins forte suivante :

(ii') il existe $m \geq 2$ et r premier avec m tels que

$$P_m(r) \hat{\subset} Spl(K) .$$

§3 - Etude des ensembles $F_{K/Q}^{-1}(C)$.

3.1. Préliminaires de théorie des groupes.

Soient G un groupe fini, H un sous-groupe distingué ; désignons par ψ l'homomorphisme canonique de G sur G/H .

LEMME 1.- *Soit $\sigma \in G$, désignons par C_σ (resp. par $C_{\psi(\sigma)}$) la classe de conjugaison de σ dans G (resp. de $\psi(\sigma)$ dans G/H) alors :*

$$\psi(C_\sigma) = C_{\psi(\sigma)} .$$

Démonstration : La classe C_σ est l'ensemble des $\tau\sigma\tau^{-1}$, pour τ parcourant G ; $\psi(C_\sigma)$ est l'ensemble des $\psi(\tau)\psi(\sigma)\psi(\tau)^{-1}$ pour τ parcourant G ; ψ étant surjectif, $\psi(C_\sigma)$ est bien une classe de conjugaison de G/H , plus précisément celle de $\psi(\sigma)$ ∎

Remarque 1 : Désignons encore par ψ l'application de l'ensemble des classes de conjugaison de G sur l'ensemble des classes de conjugaisons de G/H , définie dans le lemme 1. En général ψ n'est pas injective ; par exemple si $G = \mathfrak{S}_3$, groupe des permutations de l'ensemble $\{a,b,c\}$, désignons par σ le cycle (abc) , par τ la transposition (ab) , alors $G = \{1,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$ avec $\sigma\tau = \tau\sigma^2$. Le sous-groupe $H = \{1,\sigma,\sigma^2\}$ est distingué et les classes $C_1 = \{1\}$ et $C_\sigma = \{\sigma,\sigma^2\}$ ont même image dans G/H .

Remarque 2 : Puisque ψ est un homomorphisme de noyau H il est clair que $|C_\sigma| \leq |C_{\psi(\sigma)}||H|$.

LEMME 2.- *Soit C une classe de conjugaison de G/H , alors $\psi^{-1}(C)$ est une réunion de classes de conjugaison de G .*

Démonstration : évident ∎

Soient G un groupe fini, H_1 et H_2 deux sous-groupes distingués de G ; désignons par ψ_1 (resp. par ψ_2) l'homomorphisme canonique de G sur G/H_1 (resp. sur G/H_2) .

DEFINITION.- Si C_1 (resp. C_2) est une classe de conjugaison de G/H_1 (resp. de G/H_2) , nous désignons par $E(C_1,C_2)$ l'ensemble $[\psi_1^{-1}(C_1)] \cap [\psi_2^{-1}(C_2)]$; les classes C_1 et C_2 sont dites compatibles si $E(C_1,C_2)$ est non vide.

Remarque : Il est clair que $E(C_1,C_2)$ est une réunion (éventuellement vide) de classes de conjugaison de G .

3.2. Application à un problème de relèvement.

Q désigne à nouveau un corps de nombres quelconque.

PROPOSITION I .3.2.- Soit L/Q une extension galoisienne. Désignons par G son groupe de Galois, par H un sous-groupe distingué de G , par K le corps des invariants de H dans L , par C une classe de conjugaison de G/H et par ψ l'homomorphisme canonique de G sur G/H ; alors :

$$F_{K/Q}^{-1}(C) \;\hat{=}\; F_{L/Q}^{-1}[\psi^{-1}(C)] \ .$$

Démonstration : Désignons par S l'ensemble des $p \in \mathfrak{M}_Q$ qui sont ramifiés dans L/Q . Soit $p \in [F_{K/Q}^{-1}(C)] \backslash S$, désignons par $\mathfrak{P}$ un idéal de $\mathfrak{M}_L$ tel que $\mathfrak{P}/p$ et soit q l'idéal $\mathfrak{P} \cap K$; $\sigma_{K/Q}(q)$ est la restriction de $\sigma_{L/Q}(\mathfrak{P})$ à K , donc $\sigma_{L/Q}(\mathfrak{P})$ appartient à $\psi^{-1}(C)$.

Réciproquement, soit $p \in F_{L/Q}^{-1}[\psi^{-1}(C)]$, on a $\sigma_{L/Q}(\mathfrak{P}) \in \psi^{-1}(C)$ pour tout $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}/p$. Soit $q \in \mathfrak{M}_K$ tel que q/p , alors il existe $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}/q$, par suite

$$\sigma_{K/Q}(q) = \sigma_{L/Q}(\mathfrak{P})|K = \psi[\sigma_{L/Q}(\mathfrak{P})] \in C \quad \blacksquare$$

COROLLAIRE 1.- Soit C_σ une classe de conjugaison de G contenue dans $\psi^{-1}(C)$; si $F^{-1}_{K/Q}(C)$ et $F^{-1}_{L/Q}(C_\sigma)$ ont même densité analytique, alors $C_\sigma = \psi^{-1}(C)$ et par suite $F^{-1}_{K/Q}(C) \hat{=} F^{-1}_{L/Q}(C_\sigma)$.

Démonstration : Il suffit de remarquer que si $\psi^{-1}(C)$ est réunion de plusieurs classes $C_{\sigma_1} = C_\sigma$, $C_{\sigma_2}, \ldots, C_{\sigma_s}$, alors $F^{-1}_{K/Q}(C)$ est à une partie finie près la réunion des ensembles $F^{-1}_{L/Q}(C_{\sigma_i})$ pour $1 \leq i \leq s$, et l'on sait que chaque ensemble $F^{-1}_{L/Q}(C_{\sigma_i})$ a une densité strictement positive ■

Dans le corollaire suivant, on suppose que $Q = \Phi$ corps des rationnels.

COROLLAIRE 2.- Soit K/Φ une extension abélienne ; désignons par m un entier naturel ≥ 2 tel que $K \subset \Phi^{(m)}$ et par $\overline{G}$ le groupe de Galois de l'extension K/Φ . Pour tout $\overline{\mu} \in \overline{G}$ il existe des entiers r_i , $1 \leq i \leq t(\overline{\mu})$, premiers avec m tel que

$$F^{-1}_{K/\Phi}(\overline{\mu}) \hat{=} \bigcup_{i=1}^{t(\overline{\mu})} P_m(r_i) .$$

Démonstration : Appliquons la proposition I .3.2 avec $L = \Phi^{(m)}$, $G = G_m$, $H = \mathrm{Gal}(\Phi^{(m)}/K)$ et $C = (\overline{\mu})$; on sait alors que $F^{-1}_{K/\Phi}(\overline{\mu})$ est (à une partie finie près) la réunion des ensembles $F^{-1}_{\Phi^{(m)}/\Phi}(\sigma)$ où σ décrit l'ensemble des éléments de G_m tels que $\psi(\sigma) = \overline{\mu}$, et il suffit de remarquer que $F^{-1}_{\Phi^{(m)}/\Phi}(\sigma)$ est un ensemble du type $P_m(r)$ avec $(r,m) = 1$ ■

3.3. Etude de l'intersection de deux ensembles $F^{-1}_{K/Q}(C)$:

On désigne toujours par Q un corps de nombres quelconque.

THEOREME I .3.3.- Soient K_1/Q et K_2/Q deux extensions galoisiennes de corps de nombres. Désignons par L une extension galoisienne de Q contenant $K_1.K_2$, par G (resp. H_1 ,resp. H_2) le groupe de Galois de L/Q (resp. de L/K_1 , resp. de L/K_2) . Soit C_1 (resp. C_2) une classe de conjugaison de G/H_1 (resp. de G/H_2) ; alors

(i) $[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$ est un ensemble infini si et seulement si C_1 et C_2 sont compatibles.

(ii) De manière plus précise on a la relation :

$$[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)] \;\hat{=}\; F^{-1}_{L/Q}[E(C_1,C_2)] \ .$$

Démonstration : Supposons l'ensemble $[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$ infini ; alors il existe $\mathfrak{p} \in \mathfrak{M}_Q$, $\mathfrak{p}$ non ramifié dans L tel que $F_{K_1/Q}(\mathfrak{p}) = C_1$ et $F_{K_2/Q}(\mathfrak{p}) = C_2$. Soit $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P}/\mathfrak{p}$; alors $\sigma_{L/Q}(\mathfrak{P})|K_1 = \sigma_{K_1/Q}(\mathfrak{P} \cap K_1)$, et comme $\mathfrak{P} \cap K_1$ est l'un des idéaux de $\mathfrak{M}_{K_1}$ qui divisent $\mathfrak{p}$, on a $\sigma_{L/Q}(\mathfrak{P})|K_1 \in C_1$; de même $\sigma_{L/Q}(\mathfrak{P})|K_2 \in C_2$; et par suite C_1 et C_2 sont compatibles.

Réciproquement, supposons C_1 et C_2 compatibles ; alors il existe $\sigma \in G$ tel que $\psi_1(\sigma) \in C_1$ et $\psi_2(\sigma) \in C_2$ ou (ce qui est équivalent) $\psi_1(C_\sigma) = C_{\psi_1(\sigma)} = C_1$ et $\psi_2(C_\sigma) = C_{\psi_2(\sigma)} = C_2$. Or il existe une infinité de $\mathfrak{p} \in \mathfrak{M}_Q$ tels que $F_{L/Q}(\mathfrak{p}) = C_\sigma$. Si nous considérons un tel $\mathfrak{p}$ et si $\mathfrak{P} \in \mathfrak{M}_L$ avec $\mathfrak{P}|\mathfrak{p}$, alors $C_{\sigma_{L/Q}(\mathfrak{P})} = C_\sigma$; mais pour $j = 1$ ou 2 :

$$\psi_j[\sigma_{L/Q}(\mathfrak{P})] = \sigma_{L/Q}(\mathfrak{P})|K_j = \sigma_{K_1/Q}(\mathfrak{P} \cap K_j) \ ;$$

or $\mathfrak{P} \cap K_j$ est un idéal de $\mathfrak{M}_{K_j}$ tel que $\mathfrak{P} \cap K_j | \mathfrak{p}$; donc

$$F_{K_j/Q}(\mathfrak{p}) = C_{\sigma_{K_1/Q}(\mathfrak{P} \cap K_j)} = C_{\psi_j[\sigma_{L/Q}(\mathfrak{P})]}$$
$$= \psi_j[C_{\sigma_{L/Q}(\mathfrak{P})}] = \psi_j(C_\sigma) = C_j \ ,$$

et il existe bien une infinité de $\mathfrak{p}$ dans $[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$.

Pour le (ii) : considérons deux classes C_1 et C_2 compatibles, et éliminons les $\mathfrak{p} \in \mathfrak{M}_Q$ qui sont ramifiés dans L. Il est clair que $F_{L/Q}(\mathfrak{p}) \subset E(C_1, C_2)$ implique $F_{K_1/Q}(\mathfrak{p}) = C_1$ et $F_{K_2/Q}(\mathfrak{p}) = C_2$.

Réciproquement, si $\mathfrak{p} \in [F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$, alors $F_{L/Q}(\mathfrak{p})$ est la classe de conjugaison C formée par les $\sigma_{L/Q}(\mathfrak{P})$ pour $\mathfrak{P} \in \mathfrak{M}_L$ et $\mathfrak{P}/\mathfrak{p}$. Mais alors pour $j = 1, 2$:

$$\psi_j(\sigma_{L/Q}(\mathfrak{P})) = \sigma_{L/Q}(\mathfrak{P})|K_j = \sigma_{K_j/Q}(\mathfrak{P} \cap K_j)$$

donc $\psi_j(C) = F_{K_j/Q}(\mathfrak{P} \cap Q) = F_{K_j/Q}(\mathfrak{p}) = C_j$, ce qui équivaut à

$$F_{L/Q}(\mathfrak{p}) = C \subset [\psi_1^{-1}(C_1)] \cap [\psi_2^{-1}(C_2)] = E(C_1, C_2) \text{ , c.q.f.d.}$$

Enfin, si C_1 et C_2 sont non compatibles, il suffit de remarquer que les deux ensembles $[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$ et $F^{-1}_{L/Q}[E(C_1, C_2)]$ sont finis, pour obtenir le résultat désiré ∎

COROLLAIRE.- <u>Si C_1 et C_2 sont compatibles, l'ensemble $[F^{-1}_{K_1/Q}(C_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$ possède une densité analytique $\delta(C_1, C_2)$ et celle-ci est égale à $|E(C_1, C_2)| \cdot |G|^{-1}$; en particulier si $K_1 K_2 = L$ (c'est-à-dire $H_1 \cap H_2 = (1)$) on a</u>

$$\delta(C_1, C_2) \leq |C_1||C_2||G|^{-1} .$$

Démonstration : La première partie résulte du théorème d'Artin-Tchébotarev. Pour la deuxième partie, on peut remarquer que l'homomorphisme Ψ de G dans le produit direct $G/H_1 \times G/H_2$ défini par :

$$\Psi : \sigma \longmapsto (\psi_1(\sigma), \psi_2(\sigma))$$

admet pour noyau $H_1 \cap H_2$ et par suite qu'il est injectif si $L = K_1 K_2$ ∎

3.4. Etude d'un cas particulier : l'une des extensions est abélienne :

On désigne encore par Q un corps de nombres quelconque.

PROPOSITION I .3.4.- Soit K_1/Q (resp. K_2/Q) une extension abélienne (resp. galoisienne) de corps de nombres. Désignons par $\overline{G_1}$ (resp. par $\overline{G_2}$) le groupe de Galois de l'extension K_1/Q (resp. K_2/Q) , par $\bar{\mu}_1$ un élément de $\overline{G_1}$, par C_2 une classe de conjugaison de $\overline{G_2}$, par G le groupe de Galois de l'extension K_1K_2/Q . Si (μ_1) et C_2 sont compatibles, alors :

(i) $E((\bar{\mu}_1),C_2)$ se réduit à une seule classe de conjugaison ;

(ii) $[F^{-1}_{K_1/Q}(\bar{\mu}_1)] \cap [F^{-1}_{K_2/Q}(C_2)]$ admet une densité analytique égale à $|C_2||G|^{-1}$.

Démonstration : Comme (μ_1) et C_2 sont compatibles, il existe une classe de conjugaison C_σ de G telle que $(\bar{\mu}_1) = \psi_1(C_\sigma)$ et $C_2 = \psi_2(C_\sigma)$. L'image par Ψ de C_σ est l'ensemble des couples $(\bar{\mu}_1,\bar{\mu}_2)$, où $\bar{\mu}_2$ décrit C_2 . Comme $L = K_1K_2$, l'application Ψ est injective, par suite $E((\mu_1),C_2) = C_\sigma$ et par conséquent

$$|E((\bar{\mu}_1),C_2| = |C_\sigma| = |C_2| \quad \blacksquare$$

Dans le corollaire suivant, on suppose que $Q = \mathbb{Q}$ le corps des rationnels.

COROLLAIRE 1.- Soit $K/\mathbb{Q}$ une extension galoisienne mais non abélienne ; désignons par $\overline{G}$ son groupe de Galois, par C une classe de conjugaison de $\overline{G}$, par $\overline{G}'$ le groupe des commutateurs de $\overline{G}$; alors

(i) $|C| \leq |\overline{G}'|$;

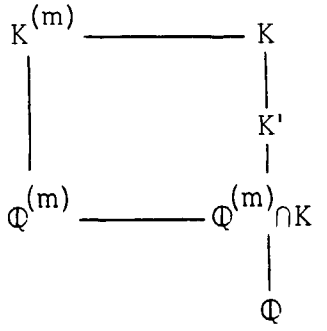
(ii) Si $|C| < |\overline{G}'|$ il n'existe aucun couple d'entiers (m,r) , $m \geq 2$ et $(m,r) = 1$ tel que $P_m(r) \hat{\subset} F^{-1}_{K/Q}(C)$;

(iii) Si au contraire, $|C| = |\overline{G}'|$ il existe un entier $m \geq 2$ et des entiers r_i , $1 \leq i \leq t(C)$, premiers avec m tels que

$$F^{-1}_{K/\Phi}(C) \hat{=} \bigcup_{i=1}^{t(C)} P_m(r_i) .$$

Démonstration : Pour le (i) remarquons que l'image par l'homomorphisme canonique de $\overline{G}$ dans $\overline{G}/\overline{G}'$ de la classe C est une classe de conjugaison C' du groupe $\overline{G}/\overline{G}'$ qui est abélien, par suite $|C'| = 1$ et $|C| \leq |\overline{G}'|$ (Remarque 2, §3.1).

Supposons à présent $|C| < |\overline{G}'|$ pour démontrer le point (ii) il suffit de prouver que quel que soit le couple (m,r) avec $m \geq 2$ et $(m,r) = 1$ l'ensemble $P_m(r) \cap F^{-1}_{K/\Phi}(C)$ a une densité analytique strictement inférieure à celle de $P_m(r)$, c'est-à-dire à $[\varphi(m)]^{-1}$ (où φ désigne la fonction d'Euler). Pour cela considérons un entier $m \geq 3$ (le cas $m = 2$ est trivial) et un entier r tel que $(r,m) = 1$. L'extension $(\Phi^{(m)} \cap K)/\Phi$ est abélienne donc $\Phi^{(m)} \cap K \subset K'$, où K' désigne le corps des invariants de $\overline{G}'$ dans K . Rappelons (voir §2) qu'on désigne par G_m le groupe de Galois de $\Phi^{(m)}/\Phi$, par $K^{(m)}$ le corps $\Phi^{(m)}.K$, par G le groupe de Galois de $K^{(m)}/\Phi$, par ζ_m une racine primitive m-ième de l'unité, par λ_r l'élément de G_m défini par $\lambda_r(\zeta_m) = \zeta_m^r$. Alors l'ensemble $P_m(r) \cap F^{-1}_{K/\Phi}(C)$ est en fait égal à $[F^{-1}_{\Phi^{(m)}/\Phi}(\lambda_r)] \cap [F^{-1}_{K/\Phi}(C)]$ et par suite sa densité est égale à $\delta(C,m,r) = |C||G|^{-1}$;



or $|G| = [K^{(m)}:\Phi^{(m)}].[\Phi^{(m)}:\Phi]$

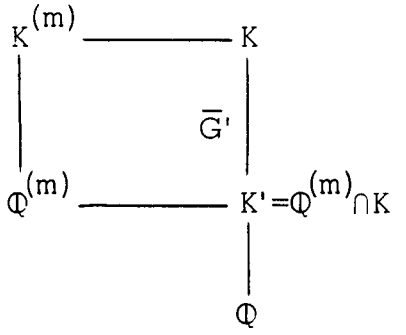
$= [K:\Phi^{(m)} \cap K].\varphi(m)$

$\geq |\overline{G}'|.\varphi(m)$;

donc $\delta(C,m,r) \leq |C|.|\overline{G}'|^{-1}[\varphi(m)]^{-1}$

d'où le résultat.

Pour (iii) : l'extension K'/Φ est abélienne, par suite il existe un entier $m \geq 2$ tel que $K' \subset \Phi^{(m)}$ et par suite $\Phi^{(m)} \cap K = K'$. Alors



l'ensemble $F^{-1}_{K/\Phi}(C)$ est la réunion disjointe des ensembles $P_m(r) \cap F^{-1}_{K/\Phi}(C)$, pour r parcourant un système de représentants de $G(m)$. Eliminons ceux de ces ensembles qui sont finis. Considérons un entier r tel que $P_m(r) \cap F^{-1}_{K/\Phi}(C)$ soit infini. Comme $P_m(r) = F^{-1}_{\Phi^{(m)}/\Phi}(\lambda_r)$, les deux classes (λ_r) et C sont compatibles (théorème I .3.3) et par suite la densité de l'ensemble $P_m(r) \cap F^{-1}_{K/\Phi}(C)$ est égale à

$$|C||G|^{-1} = |C||\bar{G}'|^{-1}[\varphi(m)]^{-1} = [\varphi(m)]^{-1}$$

c'est-à-dire à la densité de $P_m(r)$. Or l'ensemble $[F^{-1}_{\Phi^{(m)}/\Phi}(\lambda_r)] \cap [F^{-1}_{K/\Phi}(C)]$ est d'une part contenu dans $P_m(r)$, d'autre part égal à une partie finie près à $F^{-1}_{K^{(m)}/\Phi}(E((\lambda_r),C)$. Mais $E((\lambda_r),C)$ est réduite à une seule classe de conjugaison C_σ. Par suite, il résulte du corollaire 1 de la proposition I .3.2 que $P_m(r) \cap F^{-1}_{K/\Phi}(C) \hat{=} P_m(r)$, c.q.f.d. ∎

COROLLAIRE 2.- Soit K/Φ une extension galoisienne mais non abélienne ; désignons par G son groupe de Galois. Si C est une classe centrale ($|C| = 1$) de G, alors $F^{-1}_{K/\Phi}(C)$ ne contient aucun ensemble du type $P_m(r)$, avec $(m,r) = 1$ (même à une partie finie près).

En sens inverse :

COROLLAIRE 3.- Soit K/Φ une extension galoisienne. S'il existe $m \geq 2$ et r premier avec m tels que $P_m(r) \hat{\subset} \mathrm{Spl}(K)$, l'extension K/Φ est en fait abélienne.

Remarque 1 : Le corollaire 3 améliore une propriété bien connue ([Wy], p. 576).

Chapitre II

ENSEMBLE DES NOMBRES PREMIERS REPRESENTES PAR UNE FORME QUADRATIQUE BINAIRE

§1 - Généralités sur les formes quadratiques binaires.

1.1. Définitions.

Toutes les formes quadratiques considérées sont à coefficients entiers relatifs.

DEFINITION A.- Une forme quadratique binaire $g(x,y) = ax^2+bxy+cy^2$ est dite primitive si le plus grand commun diviseur de a,b et c est égal à 1 .

DEFINITION B.- Deux formes quadratiques binaires primitives $g_1(x_1,y_1) = a_1x_1^2 + b_1x_1y_1 + c_1y_1^2$ et $g_2(x_2,y_2) = a_2x_2^2+b_2x_2y_2 +c_2y_2^2$, sont dites proprement équivalentes s'il existe un changement de variables :

$$\begin{cases} x_1 = rx_2 + sy_2 \\ y_1 = tx_2 + uy_2 \end{cases} \quad \text{avec} \quad r,s,t,u \in \mathbb{Z} \ , \ ru-st = 1 \quad \text{et} \quad g_1(rx_2+sy_2, tx_2+uy_2) = g_2(x_2,y_2) \ .$$

DEFINITION C.- Si $g(x,y) = ax^2 + bxy+cy^2$ est une forme quadratique binaire, irréductible sur $\mathbb{Q}$, son discriminant $\Delta = b^2 - 4ac$ s'écrit évidemment de manière unique sous la forme $f'^2.d$, où $f' \in \mathbb{N}^*$ et où d désigne un entier relatif sans facteur carré. Le corps quadratique $K = \mathbb{Q}(\sqrt{d})$ est dit corps quadratique associé à g ; l'ordre $\mathfrak{O}$ de K dont le discriminant est Δ est dit ordre associé à g .

De manière plus explicite, désignons par ω l'élément $\sqrt{d}$ (resp. $\frac{1+\sqrt{d}}{2}$) si $d \equiv 2$ ou $3 \pmod 4$ (resp. $d \equiv 1 \pmod 4$) ; on sait que l'anneau des entiers de K est le $\mathbb{Z}$-module $\mathfrak{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$. Remarquons d'autre part que si b est impair, alors $\Delta \equiv 1 \pmod 4$, donc $d \equiv 1 \pmod 4$; et par suite si $d \equiv 2$ ou $3 \pmod 4$, alors b est pair, donc $f' = 2f$, avec $f \in \mathbb{N}^*$. Dès lors il est clair que

si $d \equiv 2$ ou $3 \pmod 4$, $\mathfrak{O}$ est l'ordre de conducteur $\frac{f'}{2}$ donc le $\mathbb{Z}$-module $\mathbb{Z} \oplus \frac{f'}{2}\omega\mathbb{Z}$;

si $d \equiv 1 \pmod 4$, $\mathfrak{O}$ est l'ordre de conducteur f' donc le $\mathbb{Z}$-module $\mathbb{Z} \oplus f'\omega\mathbb{Z}$.

Désormais "forme quadratique" veut dire forme quadratique binaire, primitive, irréductible sur $\mathbb{Q}$, et définie positive si son discriminant est négatif ; d'autre part, chaque fois que la spécification des variables est inutile, nous notons simplement g une telle forme quadratique.

1.2. Correspondance entre formes quadratiques de discriminant Δ et idéaux propres de l'ordre $\mathfrak{O}$ (rappels).

Désignons par $\mathcal{C}_\Delta$ l'ensemble des formes quadratiques (resp. des formes quadratiques définies positives) de discriminant Δ si $\Delta > 0$ (resp. si $\Delta < 0$) et par $\mathcal{F}_\Delta$ le quotient de $\mathcal{C}_\Delta$ par la relation d'équivalence propre. (Si Δ est fixé, toutes les formes de $\mathcal{C}_\Delta$ ont même corps K et même ordre $\mathfrak{O}$ associés). Désignons d'autre part par $\bar{\tau}$ l'automorphisme de K différent de l'identité, et (si ξ et η sont deux éléments de K) par $D(\xi,\eta)$ le nombre réel $\xi\bar{\tau}(\eta) - \bar{\tau}(\xi)\eta$ (resp. $\frac{1}{i}[\xi\bar{\tau}(\eta) - \bar{\tau}(\xi)\eta]$) si $\Delta > 0$ (resp. si $\Delta < 0$).

Si $\mathfrak{a} \in \mathcal{I}_\mathfrak{O}$, considérons une $\mathbb{Z}$-base $\{\alpha,\beta\}$ de $\mathfrak{a}$ et associons à $\{\alpha,\beta\}$ la forme quadratique $g_{\alpha,\beta}(x,y) = \dfrac{N_{K/\mathbb{Q}}(\alpha x+\beta y)}{N(\mathfrak{a})}$. Cette correspondance a l'inconvénient d'associer à $\{\alpha,\beta\}$ qui est une $\mathbb{Z}$-base de $\mathfrak{a}$ et à $\{\bar{\tau}(\alpha),\bar{\tau}(\beta)\}$ qui est une $\mathbb{Z}$-base de $\bar{\tau}\mathfrak{a}$, la même forme quadratique, alors que $\mathfrak{a}$ et $\bar{\tau}\mathfrak{a}$ ne sont en général pas équivalents modulo $\mathcal{P}_\mathfrak{O}^+$. Pour distinguer $\mathfrak{a}$ et $\bar{\tau}\mathfrak{a}$, nous sommes amenés à "orienter" les $\mathbb{Z}$-bases, c'est-à-dire à choisir un signe pour $D(\alpha,\beta)$; nous avons alors la :

PROPOSITION II.1.2.- [B.S] *Si $\mathfrak{a} \in \mathcal{I}_\mathfrak{O}$, considérons une $\mathbb{Z}$-base $\{\alpha,\beta\}$ de $\mathfrak{a}$ telle que $D(\alpha,\beta) > 0$ et associons à $\{\alpha,\beta\}$ la forme quadratique $g_{\alpha,\beta}$; alors l'application*

$$\{\alpha,\beta\} \longmapsto g_{\alpha,\beta}$$

induit une bijection entre le groupe $\mathcal{I}_\mathfrak{O}/\mathcal{P}_\mathfrak{O}^+$ et l'ensemble $\mathcal{F}_\Delta$.

COROLLAIRE.- On peut munir "naturellement" $\mathfrak{F}_\Delta$ d'une structure de groupe.

Remarque : Etant donné la forme quadratique $g(x,y) = ax^2+bxy+cy^2$, il est utile dans la pratique de connaître un idéal $\mathfrak{a}$ entier de l'ordre $\mathfrak{O}$ et une base de $\mathfrak{a}$ dont l'image par l'application de la proposition II.1.2 soit g. Pour cela on peut utiliser la technique suivante :

Désignons par $\psi(t)$ le polynôme at^2+bt+c et par γ le zéro dans $\mathbb{C}$ de $\psi(t)$ dont la partie imaginaire (resp. irrationnelle) est positive si $\Delta < 0$ (resp. si $\Delta > 0$) ; je dis qu'on peut prendre pour $\mathfrak{a}$ le module $a\mathbb{Z}[\gamma]$: on sait en effet que l'ordre associé à $\mathfrak{a}$ est l'ordre de discriminant Δ, c'est-à-dire $\mathfrak{O}$, et que $N(\mathfrak{a}) = a^2.\frac{1}{a} = a$; si on prend pour $\mathfrak{a}$ la base $\{a,-a\gamma\}$, on vérifie sans peine que $D(a,-a\gamma) > 0$; enfin

$$\frac{N_{K/\mathbb{Q}}(ax-a\gamma y)}{N(\mathfrak{a})} = \frac{a^2}{a} N_{K/\mathbb{Q}}(x-\gamma y) = a(x-\gamma y)(x-\bar{\gamma}(\gamma)y) = ax^2+bxy+cy^2 ;$$

d'où notre assertion.

1.3. Définition des ensembles Rep(g).

DEFINITION.- Si $g(x,y) = ax^2+bxy+cy^2$ est une forme quadratique, nous désignons par Rep(g) l'ensemble des nombres premiers p tels qu'il existe $x,y \in \mathbb{Z}$ avec $g(x,y) = p$.

Remarque : Il est clair que si deux formes g_1 et g_2 sont proprement équivalentes, les ensembles $\mathrm{Rep}(g_1)$ et $\mathrm{Rep}(g_2)$ coïncident.

Exemple : Si $g(x,y) = x^2+y^2$,

$$\mathrm{Rep}(g) = [\mathrm{Spl}[\mathbb{Q}(i)] \cup \{2\} = [P_4(1)] \cup \{2\} .$$

Le but de ce chapitre est (rappelons-le) d'une part, de caractériser l'ensemble $Rep(g)$ (en utilisant les théories habituelles des ordres et du corps de classes global) ; d'autre part, de le comparer aux sous-ensembles classiques de P ($Spl_{\mathbb{Q}}(K)$ et $P_m(r)$) et (par exemple) de répondre à la question suivante : "à quelles conditions, $Rep(g)$ est-il (ou n'est-il pas) réunion de "progressions arithmétiques" de nombres premiers ?".

§2 - Première caractérisation des ensembles $Rep(g)$.

2.1. Application de la théorie des ordres.

Soit g une forme quadratique (voir §1, n°1.1). Soit $\mathfrak{C}(g)$ l'élément de $\mathfrak{I}_{\mathfrak{O}}/\mathfrak{P}_{\mathfrak{O}}^{+} = C_{\mathfrak{O}}^{+}$ correspondant (par la bijection de la proposition II.1.2) à la classe de g dans $\mathfrak{F}_{\Delta}$.

PROPOSITION II.2.1.- *Soit* $p \in P$. *Les deux assertions suivantes sont équivalentes* :

(i) $p \in Rep(g)$;

(ii) *il existe dans la classe* $\mathfrak{C}(g)^{-1}$ *un idéal maximal* $\mathfrak{p}$ *propre de* $\mathfrak{O}$ *tel que* $N(\mathfrak{p}) = p$.

Pour une démonstration, voir [B.S].

2.2. Application de la théorie du corps de classes global.

Désignons par f le conducteur de l'ordre $\mathfrak{O}$; nous avons introduit (voir notations) une bijection canonique i entre $\mathfrak{I}_{\mathfrak{O}}^{f}$ et $\mathfrak{I}_{K}^{f}$; on peut montrer (sans difficultés) que le groupe $\mathfrak{H} = i((\mathfrak{P}_{\mathfrak{O}}^{f})^{+})$ est un groupe de congruence modulo f dans $\mathfrak{I}_{K}^{f}$. Désignons par L l'extension abélienne de K associée à $\mathfrak{H}$ par la théorie du corps de classes global, par H le groupe de Galois de l'extension L/K , par S l'ensemble des $p \in P$, qui divisent f , ou qui sont ramifiés dans l'extension

$L/\mathbb{Q}$, par $\mathfrak{B}(g)$ l'image par la bijection i de la classe $\mathfrak{I}_K^f \cap \mathfrak{C}(g)$ et enfin par $\sigma(g)$ l'image dans H de $\mathfrak{B}^{-1}(g)$ par l'application d'Artin $F_{L/K}$. Nous avons alors une première caractérisation de l'ensemble $\mathrm{Rep}(g)$:

PROPOSITION II.2.2.- Soit $p \in P\backslash S$; les deux assertions suivantes sont équivalentes :

(i) $p \in \mathrm{Rep}(g)$;

(ii) $p \in \mathrm{Spl}(K)$ et il existe $q \in \mathfrak{M}_K$ tel que $q \mid p$ et que $F_{L/K}(q) = \sigma(g)$.

Cette proposition n'est qu'une traduction de la proposition II.2.1.

Rappelons qu'on désigne par $h_{\mathfrak{D}}^+$ l'ordre de $\mathcal{C}_{\mathfrak{D}}^+$.

COROLLAIRE.- Soit $\{g_i \; ; \; 1 \leq i \leq h_{\mathfrak{D}}^+\}$ un système complet de représentants des classes de $\mathfrak{F}_\Delta$ alors :

$$\mathrm{Spl}(K) \hat{=} \bigcup_{i=1}^{h_{\mathfrak{D}}^+} \mathrm{Rep}(g_i) \; .$$

Démonstration : Soit $\sigma \in H$; désignons par $R(\sigma)$ l'ensemble des $p \in P\backslash S$ tels que $p \in \mathrm{Spl}(K)$ et qu'il existe $q \in \mathfrak{M}_K$ tel que $q \mid p$ et $F_{L/K}(q) = \sigma$. Il est clair que $\mathrm{Spl}(K) = \bigcup_{\sigma \in H} R(\sigma)$. D'autre part, les groupes $\mathfrak{F}_\Delta$, $\mathcal{C}_{\mathfrak{D}}^+ = \mathfrak{I}_{\mathfrak{D}}^f / (\mathfrak{P}_{\mathfrak{D}}^f)^+$, $\mathfrak{I}_K^f / \mathfrak{H}$ et H étant isomorphes, chaque $R(\sigma)$ est un $\mathrm{Rep}(g_i)$, $1 \leq i \leq h_{\mathfrak{D}}^+$ ■

§3 - Structure de $G = \mathrm{Gal}(L/\mathbb{Q})$.

Remarquons que le groupe $\mathfrak{H}$ est invariant par $\bar{\tau}$: l'extension $L/\mathbb{Q}$ est donc galoisienne ; désignons par G son groupe de Galois.

3.1. Structure du groupe G .

La proposition suivante est apparentée à la théorie des genres ; dans le cas complexe $(d<0)$, elle peut d'ailleurs aussi se démontrer par la théorie de la multiplication complexe.

PROPOSITION II.3.1.- Le groupe G est produit semi-direct d'un sous-groupe d'ordre 2 (engendré par un relèvement τ de $\bar{\tau}$) par le sous-groupe distingué H ; de manière plus précise on a les relations :

(a) $\tau^2 = 1$;

(b) $\tau\sigma\tau^{-1} = \sigma^{-1}$, pour tout $\sigma \in H$.

Démonstration : Soit $\mathfrak{a} \in \mathfrak{I}_K^f$, un idéal non ramifié dans l'extension L/K ; alors l'idéal $\mathfrak{a}.\bar{\tau}(\mathfrak{a})$ est principal et engendré par un nombre rationnel ; ce nombre rationnel ayant dans l'extension $K/\mathbb{Q}$ une norme positive, l'idéal $\mathfrak{a}.\bar{\tau}(\mathfrak{a})$ appartient à $\mathcal{H}$; par suite $F_{L/K}(\mathfrak{a}.\bar{\tau}(\mathfrak{a})) = 1$.

Soit $\sigma \in H$; l'application d'Artin étant surjective, il existe $\mathfrak{a}$ tel que $F_{L/K}(\mathfrak{a}) = \sigma$; la relation (b) résulte alors immédiatement des propriétés de l'application d'Artin. On peut remarquer que le choix du relèvement τ de $\bar{\tau}$ peut être fait de façon arbitraire car le sous-groupe H est abélien.

Pour démontrer (a) , considérons un idéal $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \tau$. Désignons par $\mathfrak{p}$ (resp. par p) l'idéal (resp. le nombre premier) $\mathfrak{P} \cap K$ (resp. tel que $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$) . La classe de conjugaison $F_{K/\mathbb{Q}}(p)$ est réduite à l'élément $\sigma_{K/\mathbb{Q}}(p)$; d'autre part $\sigma_{K/\mathbb{Q}}(p)$ est la restriction à K de $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \tau$, par suite $\sigma_{K/\mathbb{Q}}(p) \neq 1$ et p est inerte dans l'extension $K/\mathbb{Q}$; il en résulte que $f(\mathfrak{p}/p) = 2$ et par suite $\sigma_{L/K}(\mathfrak{p}) = \tau^2$. D'autre part, $\mathfrak{p} = p\mathfrak{O}_K$, donc $\mathfrak{p} \in \mathcal{H}$ et $F_{L/K}(\mathfrak{p}) = 1$ ce qui démontre (a) ∎

Remarque : Il résulte de cette proposition que tout élément de G s'écrit de manière unique $\varepsilon.\sigma$, avec $\varepsilon = 1$ ou τ et $\sigma \in H$.

3.2. Etude de l'extension abélienne maximale de $\mathbb{Q}$ contenue dans L .

Désignons par G' le groupe des commutateurs de G et par L' le corps des invariants dans L de G' , c'est-à-dire l'extension abélienne maximale de $\mathbb{Q}$ contenue dans L .

PROPOSITION II.3.2.- Le groupe G' coïncide avec le groupe H^2 (le groupe des carrés).

COROLLAIRE.- L'extension $L/\mathbb{Q}$ est abélienne si et seulement si le groupe H est d'exposant 2 .

Démonstration de la proposition II.3.2 : G' est le sous-groupe de G engendré par l'ensemble des éléments de G de la forme $\lambda_1^{-1}\lambda_2^{-1}\lambda_1\lambda_2$, avec $\lambda_1 = \varepsilon_1\sigma_1$, $\lambda_2 = \varepsilon_2\sigma_2$, $\varepsilon_1 = 1$ ou τ , $\varepsilon_2 = 1$ ou τ , $\sigma_1 \in H$, $\sigma_2 \in H$.

Si $\varepsilon_1 = \varepsilon_2 = 1$, $\lambda_1^{-1}\lambda_2^{-1}\lambda_1\lambda_2 = 1$ car H est abélien ;

Si $\varepsilon_1 = 1$, $\varepsilon_2 = \tau$, $\lambda_1^{-1}\lambda_2^{-1}\lambda_1\lambda_2 = \sigma_1^{-1}\sigma_2^{-1}\tau\sigma_1\tau\sigma_2 = (\sigma_1^{-1})^2 \in H^2$;

Si $\varepsilon_1 = \tau$, $\varepsilon_2 = 1$, $\lambda_1^{-1}\lambda_2^{-1}\lambda_1\lambda_2 = \sigma_1^{-1}\tau\sigma_2^{-1}\tau\sigma_1\sigma_2 = (\sigma_2)^2 \in H^2$;

Si $\varepsilon_1 = \tau$, $\varepsilon_2 = \tau$, $\lambda_1^{-1}\lambda_2^{-1}\lambda_1\lambda_2 = \sigma_1^{-1}\tau\sigma_2^{-1}\tau\tau\sigma_1\tau\sigma_2 = (\sigma_1^{-1}\sigma_2)^2 \in H^2$.

Réciproquement, tout élément σ^2 de H^2 peut s'écrire sous la forme $\tau\sigma^{-1}\tau\sigma = \tau^{-1}\sigma^{-1}\tau\sigma$, donc est un commutateur ■

§4 - Deuxième caractérisation des ensembles Rep(g) .

Désignons par $C_{\sigma(g)}$, la classe de conjugaison dans G de $\sigma(g)$, nous avons la caractérisation suivante :

4.1. Caractérisation.

PROPOSITION II.4.1.- Si $p \in P\backslash S$, les assertions suivantes sont équivalentes :

(i) $p \in \mathrm{Rep}(g)$

(ii) $F_{L/\mathbb{Q}}(p) = C_{\sigma(g)}$.

COROLLAIRE.- L'ensemble $\mathrm{Rep}(g)$ possède une densité analytique et celle-ci est égale à :

$$[L:\mathbb{Q}]^{-1} \quad \text{si} \quad [\sigma(g)]^2 = 1$$

$$2[L:\mathbb{Q}]^{-1} \quad \text{si} \quad [\sigma(g)]^2 \neq 1 \ .$$

Démonstration de la proposition II.4.1 :Remarquons que $C_{\sigma(g)} = \{\sigma(g), \tau\sigma(g)\tau^{-1}\}$ et que $C_{\sigma(g)}$ se réduit au seul élément $\sigma(g)$ si et seulement si $\tau\sigma(g) = \sigma(g)\tau$ (ce qui ne dépend pas du relèvement τ de $\bar{\tau}$ que l'on a choisit, car H est abélien). Soit $p \in \mathrm{Rep}(g)$; alors $p \in \mathrm{Spl}(K)$ et il existe $\mathfrak{q} \in \mathfrak{M}_K$ tel que $\mathfrak{q} | p$ et $F_{L/K}(\mathfrak{q}) = \sigma(g)$. Soit $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P} | \mathfrak{q}$; alors $\sigma_{L/K}(\mathfrak{P}) = \sigma(g)$. Comme $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \sigma_{L/K}(\mathfrak{P}) = \sigma(g)$ puisque $p \in \mathrm{Spl}(K)$, on a bien $F_{L/\mathbb{Q}}(p) = C_{\sigma(g)}$.

Réciproquement, supposons que $F_{L/\mathbb{Q}}(p) = C_{\sigma(g)} = \{\sigma(g), \tau\sigma(g)\tau^{-1}\}$. Soit $\mathfrak{P} \in \mathfrak{M}_L$ tel que $\mathfrak{P} | p$ et $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \sigma(g)$. Désignons par $\mathfrak{q}$ l'idéal $\mathfrak{P} \cap K$. Alors $\sigma_{K/\mathbb{Q}}(\mathfrak{q})$ est la restriction de $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \sigma(g)$ à K , donc $\sigma_{K/\mathbb{Q}}(\mathfrak{q}) = 1$ (car $\sigma(g) \in H$) , et par suite $p \in \mathrm{Spl}(K)$; comme $f(\mathfrak{q}/p) = 1$, on a $\sigma_{L/\mathbb{Q}}(\mathfrak{P}) = \sigma_{L/K}(\mathfrak{P}) = \sigma(g)$ et donc $F_{L/K}(\mathfrak{q}) = \sigma(g)$ ■

Démonstration du corollaire : C'est une conséquence immédiate du théorème d'Artin-Tchebotarev qui montre que la densité est $[L:\mathbb{Q}]^{-1}$ (resp. $2[L:\mathbb{Q}]^{-1}$) si $\sigma(g)\tau = \tau\sigma(g)$ (resp. si $\sigma(g)\tau \neq \tau\sigma(g)$) ; comme $\tau\sigma(g) = \sigma(g)^{-1}\tau$ nous obtenons bien le résultat désiré ■

4.2. Exemples.

Exemple 1 : Considérons la forme $g_1(x,y) = x^2+16y^2$. Ici $\Delta = -64 = (-1)8^2$; $K = \mathbb{Q}\sqrt{-1} = \mathbb{Q}(i)$, $f = 4$, $\mathfrak{O} = \mathbb{Z} \oplus 4i\mathbb{Z}$; d'autre part, l'équivalence des idéaux au sens restreint coïncide avec l'équivalence simple. On détermine le degré de l'extension L/K :

- soit en calculant le nombre de classes de $\mathfrak{O}$ par la formule $h_{\mathfrak{O}} = h_K . f(\mathfrak{O}_K^* : \mathfrak{O}^*)^{-1} \prod_{p \mid f} (1-(\frac{K}{p})p^{-1})$, ([Co]), ici $h_K = 1$, $f = 4$, $(\mathfrak{O}_K^* : \mathfrak{O}^*) = 2$, $(\frac{K}{2}) = 0$ car 2 est ramifié, par suite $[L:K] = h_{\mathfrak{O}} = 2$;

- soit en déterminant des représentants des classes dans $\mathfrak{I}_{\mathfrak{O}}/\mathfrak{P}_{\mathfrak{O}}$, en utilisant la méthode des idéaux réduits [B.S] : on trouve ici $\mathfrak{a}_1 = \mathfrak{O}$, idéal associé à la forme g_1 , et $\mathfrak{a}_2 = 4\mathbb{Z} \oplus (-2-4i)\mathbb{Z}$ idéal associé à la forme $g_2(x,y) = 4x^2-4xy+5y^2$.

Comme $[L:K]$ est égal à 2 , il est certain que $[\sigma(g)]^2 = 1$ pour tout g . Les densités analytiques de $\mathrm{Rep}(g_1)$ et de $\mathrm{Rep}(g_2)$ sont égales à $\frac{1}{4}$. La somme de ces deux densités est 1/2 , c'est-à-dire à la densité de $\mathrm{Spl}(K)$.

$$H \left\{ \begin{array}{l} L \\ \mid 2 \\ K=\mathbb{Q}(i) \\ \mid \\ \mathbb{Q} \end{array} \right.$$

Désignons par 1 et σ les éléments de H (groupe de Galois de L/K). L'idéal associé à la forme x^2+16y^2 (n°1.2. Remarque) est $\mathfrak{O}$; par suite $\sigma(x^2+16y^2) = 1$ (n°2.2) et $\mathrm{Rep}(x^2+16y^2) \hat{=} \mathrm{Spl}(L)$ (proposition II.4.1). Remarquons que $p = x^2+16y^2$ entraîne $p \equiv 1 \pmod 8$ et par suite $\mathrm{Spl}(L) \hat{\subset} \mathrm{Spl}[\mathbb{Q}^{(8)}]$ d'où il résulte que $\mathbb{Q}^{(8)} \subset L$ (chap.I). Comme $[L:\mathbb{Q}] = [\mathbb{Q}^{(8)}:\mathbb{Q}] = 4$, nous avons en fait $L = \mathbb{Q}^{(8)}$, et par conséquent

$$\mathrm{Rep}(x^2+16y^2) \hat{=} \mathrm{Spl}[\mathbb{Q}^{(8)}] \hat{=} P_8(1) ;$$

$$\mathrm{Rep}(4x^2-4xy+5y^2) \hat{=} \mathrm{Spl}[\mathbb{Q}(i)] \backslash P_8(1) \hat{=} P_8(5) .$$

On peut retrouver également ces résultats, en remarquant que si $p \in \mathrm{Spl}[\mathbb{Q}(i)]$, alors p peut s'écrire sous la forme $p = x^2 + y^2$, avec $x \equiv 1 \pmod 4$

et $y \equiv 0$ ou $2 \pmod 4$, qu'alors $y \equiv 0 \pmod 4$ entraîne $p \equiv 1 \pmod 8$, et $y \equiv 2 \pmod 4$ entraîne $p \equiv 5 \pmod 8$; et qu'enfin $y \equiv 0 \pmod 4$ équivaut à $p \in \mathrm{Rep}(x^2+16y^2)$, et $y \equiv 2 \pmod 4$ équivaut à $p \in \mathrm{Rep}(4x^2-4xy+5y^2)$.

Exemple 2 : Considérons la forme $g_1(x,y) = x^2+32y^2$. Ici $\Delta = -128 = (-2)8^2$; $K = \mathbb{Q}(\sqrt{-2})$; $f = 4$; $\mathfrak{O} = \mathbb{Z} \oplus 4\sqrt{-2}\mathbb{Z}$. Désignons par ω l'élément $\sqrt{-2}$ (c'est-à-dire $i\sqrt{2}$). Nous avons :

$$h_K = 1 \ , \ f = 4 \ , \ (\mathfrak{O}_K^* : \mathfrak{O}^*) = 1 \ , \ \left(\frac{K}{2}\right) = 0 \text{ donc } h_{\mathfrak{O}} = 4 \ .$$

Les représentants des classes sont :

$\mathfrak{a}_1 = \mathfrak{O}$ associé à la forme g_1 ;

$\mathfrak{a}_2 = 3\mathbb{Z} \oplus (1-4\omega)\mathbb{Z}$ " " $g_2(x,y) = 3x^2+2xy+11y^2$;

$\mathfrak{a}_3 = 3\mathbb{Z} \oplus (-1-4\omega)\mathbb{Z}$ " " $g_3(x,y) = 3x^2-2xy+11y^2$;

$\mathfrak{a}_4 = 4\mathbb{Z} \oplus (-2-4\omega)\mathbb{Z}$ " " $g_4(x,y) = 4x^2-4xy+9y^2$;

$\mathfrak{a}_1$ est principal dans l'ordre $\mathfrak{O}$, donc $\sigma(g_1) = 1$ (et par suite $[\sigma(g_1)]^2 = 1$) ; il en résulte que $\mathrm{Rep}(g_1) \hat{=} \mathrm{Spl}(L)$ a pour densité $[L:\mathbb{Q}]^{-1} = 1/8$.

$\mathfrak{a}_4 = 2\,[2\mathbb{Z} \oplus (1+2\omega)\mathbb{Z}]$, $\mathfrak{a}_4^2 = 4\mathfrak{b}$ où $\mathfrak{b}$ est l'idéal engendré par les éléments 4 , $2+4\omega$ et $1+4\omega$; par suite $\mathfrak{b}$ contient 1 et 4ω , donc $\mathfrak{b} = \mathfrak{O}$, $\mathfrak{a}_4^2$ est principal, et $[\sigma(g_4)]^2 = 1$; donc $\delta\,[\mathrm{Rep}(g_4)] = 1/8$.

Comme $\mathrm{Rep}(g_2) = \mathrm{Rep}(g_3)$ et que $\bigcup_{i=1}^{4} \mathrm{Rep}(g_i) \hat{=} \mathrm{Spl}(K)$ on a $\delta(\mathrm{Rep}\ g_2) = 1/4$; par suite $[\sigma(g_2)]^2 \neq 1$ ce qui signifie que le groupe H est cyclique d'ordre 4 et que l'extension $L/\mathbb{Q}$ n'est pas abélienne.

Remarquons qu'il est facile de vérifier "à la main" que $[\sigma(g_2)]^2 \neq 1$: L'idéal $\mathfrak{a}_2^2$ est engendré par les éléments 9 , $3-12\omega$ et $-31-8\omega$. L'élément $2+4\omega = 4.9 - (3-12\omega) - 31 - 8\omega \in \mathfrak{a}_2^2$; d'autre part $3-12\omega$ et $-31-8\omega$ sont combinaisons $\mathbb{Z}$-linéaires de 9 et $2+4\omega$, d'où

$\mathfrak{a}_2^2 = 9\mathbb{Z} \oplus (2+4\omega)\mathbb{Z}$. Supposons $\mathfrak{a}_2^2$ principal : alors il existe $\xi \in K$ tel que $\mathfrak{a}_2^2 = \xi\mathfrak{O}$, donc il existe alors une matrice $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in m_n(\mathbb{Z})$ avec $ru - st = \pm 1$ et

$$\begin{cases} 2+4\omega = r\xi + s\xi 4\omega \\ 9 = t\xi + u\xi 4\omega \end{cases} ;$$

d'où

$$\frac{2+4\omega}{9} = \frac{r+s4\omega}{t+u4\omega} = \frac{(r+s4\omega)(t-u4\omega)}{t^2+32u^2} \quad ; \qquad (1)$$

car $\bar{\tau}(\omega) = -\omega$. La relation (1) équivaut au système

$$\begin{cases} \frac{2}{9} = \frac{rt+32su}{t^2+32u^2} \quad , & (2) \\ \frac{4}{9} = \frac{4(st-ru)}{t^2+32u^2} \quad ; & (3) \end{cases}$$

par suite $st - ru = +1$, $t^2+32u^2 = 9$ et $rt+32su = 2$; ce qui implique

$$\begin{cases} t = \pm 3 \quad \text{et} \quad u = 0 \ , & (4) \\ st - ru = 1 \ , & (5) \\ rt+32su = 2 \ ; & (6) \end{cases}$$

or (4) et (5) sont incompatibles.

Remarque : Avec les méthodes du §5, on peut montrer que l'ensemble $\mathrm{Rep}(x^2+32y^2)$ (resp. $\mathrm{Rep}(3x^2+2xy+11y^2)$) n'est pas (resp. est) réunion de "progressions arithmétiques" de nombres premiers.

Exemple 3 : Lorsque $f = 1$, $\mathfrak{O} = \mathfrak{O}_K$, le groupe $\mathfrak{I}_{\mathfrak{O}}/\mathcal{P}_{\mathfrak{O}}$ coïncide avec le groupe des classes du corps K ; or il existe des tables donnant la structure de ce groupe (par exemple [So]) donc la structure de H .

Exemple 3.1. $H \simeq \mathbb{Z}/4\mathbb{Z}$.

Soit $g_1(x,y) = x^2+14y^2$. Ici $K = \mathbb{Q}(\sqrt{-14})$, $f = 1$, $\mathfrak{O} = \mathfrak{O}_K$. D'après la table, le groupe H est cyclique d'ordre 4 . Il en résulte

- que $L/\mathbb{Q}$ est non abélienne ;

- que l'on a 4 classes de formes avec les densités $1/8$, $1/4$, $1/4$, $1/8$.

On obtient facilement quatre formes représentantes, ce sont outre $g_1(x,y) = x^2+14y^2$, $g_2(x,y) = 3x^2-2xy+5y^2$, $g_3(x,y) = 3x^2+2xy+5y^2$ et $g_4(x,y) = 2x^2+7y^2$.

Exemple 3.2. $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Soit $g_1(x,y) = x^2+21y^2$. Ici $K = \mathbb{Q}(\sqrt{-21})$, $f = 1$, $\mathfrak{O} = \mathfrak{O}_K$. D'après la table, le groupe H est d'ordre 4 , mais c'est un groupe de Klein. Il en résulte

- que $L/\mathbb{Q}$ est abélienne ;

- que l'on a 4 classes de formes avec la densité $1/8$ pour chacune.

On obtient en fait comme formes représentantes outre g_1 , $g_2(x,y) = 3x^2+7y^2$, $g_3(x,y) = 2x^2-2xy+11y^2$, $g_4(x,y) = 5x^2-4xy+5y^2$.

§5 - Comparaison des ensembles Rep(g) et $P_m(r)$.

5.1. Comparaison lorsque l'extension $L/\mathbb{Q}$ est abélienne.

PROPOSITION II.5.1. *Si l'extension $L/\mathbb{Q}$ est abélienne, il existe un entier $m \geq 2$, (ne dépendant que de L) et des entiers r_i , $1 \leq i \leq t$, premiers avec m tels que*

$$\mathrm{Rep}(g) \hat{=} \bigcup_{i=1}^{t} P_m(r_i) .$$

Démonstration : Cette proposition n'est qu'un cas particulier du corollaire de la proposition I .3.2.

5.2. Comparaison lorsque l'extension $L/\mathbb{Q}$ est non abélienne.

PROPOSITION II.5.2.- Si l'extension $L/\mathbb{Q}$ est non abélienne les deux assertions suivantes sont équivalentes :

(i) $[\sigma(g)]^2 \neq 1$ et $|H^2| = 2$;

(ii) il existe un entier $m \geq 2$ et des entiers r_i , $1 \leq i \leq t(g)$, premiers avec m tels que :

$$\mathrm{Rep}(g) \hat{=} \bigcup_{i=1}^{t(g)} P_m(r_i) .$$

Démonstration : Si l'extension $L/\mathbb{Q}$ est non abélienne, le groupe des commutateurs H^2 de G est d'ordre ≥ 2 ; de plus on sait que $C_{\sigma(g)}$ contient 2 éléments si $[\sigma(g)]^2 \neq 1$ et un seul élément si $[\sigma(g)]^2 = 1$. La proposition précédente n'est donc qu'un cas particulier du corollaire 1 de la proposition I .3.4.

§6 - Exemples.

6.1. Exemple 1 : $C_{\mathfrak{O}}^{+} \simeq \mathbb{Z}/4\mathbb{Z}$.

Soit $g(x,y) = x^2+14y^2$. Au §4, n°4.2 nous avons vu que $K = \mathbb{Q}(\sqrt{-14})$, $f = 1$, $\mathfrak{O} = \mathfrak{O}_K$ et que le groupe H était cyclique d'ordre 4 , notons $H = \{1,\sigma,\sigma^2,\sigma^3\}$. On a 4 formes représentantes et 4 idéaux de $\mathfrak{O} = \mathfrak{O}_K$ associés :

$$g_1(x,y) = g(x,y) = x^2+14y^2 \quad , \quad \mathfrak{a}_1 = \mathfrak{O} \ ;$$

$$g_2(x,y) = 2x^2+7y^2 \quad , \quad \mathfrak{a}_2 = 2\mathbb{Z} \oplus (-\sqrt{-14})\mathbb{Z} \ ;$$

$$g_3(x,y) = 3x^2-2xy+5y^2 \quad , \quad \mathfrak{a}_3 = 3\mathbb{Z} \oplus (-1-\sqrt{-14})\mathbb{Z} \ ;$$

$$g_4(x,y) = 3x^2+2xy+5y^2 \quad , \quad \mathfrak{a}_4 = 3\mathbb{Z} \oplus (1-\sqrt{-14})\mathbb{Z} = \bar{\mathfrak{r}}(\mathfrak{a}_3) \ ;$$

Il est clair que $\sigma(g_1) = 1$. D'autre part, $\mathfrak{a}_2^2$ est engendré par 4 , $2\sqrt{-14}$ et -14 , donc par 2 et $2\sqrt{-14}$; donc $\mathfrak{a}_2^2 = 2\mathfrak{O}$, et par suite $\sigma(g_2)$ est d'ordre 2 ; le seul élément d'ordre 2 de H étant σ^2 , on a $\sigma(g_2) = \sigma^2$. Par suite, le couple $(\sigma(g_2),\sigma(g_3))$ est égal au couple (σ,σ^3) qui n'est autre que la classe de conjugaison de σ .

Nous désignons désormais par $P_m(r_1,r_2,\ldots,r_t)$ l'ensemble $\bigcup_{i=1}^{t} P_m(r_i)$.

Déterminons Spl $\mathbb{Q}(\sqrt{-14})$: $p \in \mathrm{Spl}(\mathbb{Q}(\sqrt{-14}))$ équivaut à $(\frac{-14}{p}) = 1$, d'où $(\frac{-1}{p})(\frac{2}{p})(\frac{7}{p}) = 1$, ce qui équivaut à $(-1)^{(p^2-1)/8}(\frac{p}{7}) = 1$ soit

$$\begin{cases} p \equiv \pm 1 \pmod 8 \quad \text{et} \quad p \equiv 1,\ 2 \text{ ou } 4 \pmod 7 \\ \text{ou} \\ p \equiv \pm 3 \pmod 8 \quad \text{et} \quad p \equiv 3,\ 5 \text{ ou } 6 \pmod 7 \end{cases}$$

par suite

(1) $$\mathrm{Spl}(\mathbb{Q}(\sqrt{-14})) = P_{56}(1,3,5,9,13,15,19,23,25,27,39,45) \ .$$

On sait que :

(2) $$\mathrm{Rep}(g_1) \cup \mathrm{Rep}(g_2) \cup \mathrm{Rep}(g_3) \hat{=} \mathrm{Spl}(\mathbb{Q}(\sqrt{-14})) \ ;$$

que $\delta(\mathrm{Rep}(g_1)) = \frac{1}{8}$, $\delta(\mathrm{Rep}(g_2)) = \frac{1}{8}$, $\delta(\mathrm{Rep}(g_3)) = \frac{1}{4}$, puisque $[\sigma(g_1)]^2=1$, $[\sigma(g_2)]^2 = 1$, et $[\sigma(g_3)]^2 = \sigma^2 \neq 1$. Ici, $H = \{1,\sigma,\sigma^2,\sigma^3\}$, $H^2 = \{1,\sigma^2\}$ est d'ordre 2 , la classe de conjugaison de $\sigma(g_3)$ est $\{\sigma,\sigma^3\}$, par suite $\mathrm{Rep}(g_3)$ est "réunion d'ensembles $P_m(r)$" , alors que $\mathrm{Rep}(g_1)$ et $\mathrm{Rep}(g_2)$ ne le sont pas (car les classes de $\sigma(g_1) = 1$ et de $\sigma(g_2) = \sigma^2$ sont réduites à un élément) .

Pour déterminer les $P_{56}(r_i)$ dont la réunion est $\mathrm{Rep}(g_3)$, on peut opérer de la manière suivante : Si $p \in \mathrm{Rep}(g_1)$, alors $p = x^2+14y^2$, d'où il résulte que $(\frac{p}{7}) = 1$, donc $p \equiv 1$, 2 ou 4 (modulo 7), et par suite $\mathrm{Rep}(g_1) \hat{\subset} P_{56}(1,9,15,23,25,39)$; de même si $p \in \mathrm{Rep}(g_2)$, $p = 2x^2+7y^2$ donc $p \equiv 2x^2 \pmod 7$ d'où $p \equiv 1$, 2 ou 4 (modulo 7) ; il en résulte que

(3) $$\mathrm{Rep}(g_1) \cup \mathrm{Rep}(g_2) \hat{\subset} P_{56}(1,9,15,23,25,39) \ .$$

D'autre part $3x^2 - 2xy + 5y^2 = \dfrac{N_{K/\mathbb{Q}}[3x-y(1+\sqrt{-14})]}{N(\mathfrak{a}_3)}$ et $N_{K/\mathbb{Q}}(3x-y-y\sqrt{-14}) = (3x-y)^2+14y^2$; on sait d'autre part que $N(\mathfrak{a}_3) = 3$; par suite si $p \in \mathrm{Rep}(g_3)$ on a $3p = (3x-y)^2+14y^2 \equiv (3x-y)^2$ (modulo 7) , donc $3p \equiv 1$, 2 ou 4 (modulo 7). On vérifie facilement que cette condition n'est remplie par aucun p de $P_{56}(1,9,15,23,25,39)$ et par suite

(4) $$\mathrm{Rep}(g_3) \hat{\subset} P_{56}(3,5,13,19,27,45) \ .$$

Il résulte de (1), (2), (3) et (4) <u>que les inclusions</u> (3) <u>et</u> (4) <u>sont des égalités</u>.

6.2. <u>Exemple 2</u> : $C_{\mathfrak{O}}^{+} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Soit $g(x,y) = g_1(x,y) = x^2+21y^2$. Ici $K = \mathbb{Q}(\sqrt{-21})$, $f = 1$, $\mathfrak{O} = \mathfrak{O}_K$; on a les représentants

$g_1(x,y) = x^2+21y^2$ qui est associée à $\mathfrak{O} = \mathfrak{O}_K$;

$g_2(x,y) = 3x^2+7y^2$ qui est associée à $\mathfrak{a}_2 = 3\mathbb{Z} \oplus (-\sqrt{-21})\mathbb{Z}$;

$g_3(x,y) = 2x^2-2xy+11y^2$ qui est associée à $\mathfrak{a}_3 = 2\mathbb{Z} \oplus (-1-\sqrt{-21})\mathbb{Z}$;

$g_4(x,y) = 5x^2-4xy+5y^2$ qui est associée à $\mathfrak{a}_4 = 5\mathbb{Z} \oplus (-2-\sqrt{-21})\mathbb{Z}$.

On a d'une part

(1) $$\mathrm{Spl}\ \mathbb{Q}(\sqrt{-21}) \hat{=} \bigcup_{i=1}^{4} \mathrm{Rep}(g_i) \ ;$$

d'autre part

(2) $\quad \mathrm{Spl}\ \mathbb{Q}(\sqrt{-21}) \ \hat{=}\ P_{84}(1,5,11,17,19,23,25,31,37,41,55,71)$.

Par ailleurs, si $p \in \mathrm{Rep}(g_1)$, alors $p \equiv x^2 \pmod{21}$, donc $p \equiv 1$, 4 ou 16 (mod 21) , par suite

(3) $\quad \mathrm{Rep}(g_1) \ \hat{\subset}\ P_{84}(1,25,37)$.

Si $p \in \mathrm{Rep}(g_2)$, alors $p = 3x^2+7y^2$, donc $p \equiv 7y^2 \pmod 3$ ou $p \equiv 1 \pmod 3$; d'autre part, $p \equiv 3x^2 \pmod 7$, ou $p \equiv 3$, 5 ou 6 (mod 7) ; par suite

(4) $\quad \mathrm{Rep}(g_2) \ \hat{\subset}\ P_{84}(19,31,55)$.

Si $p \in \mathrm{Rep}(g_3)$, alors $p = 2x^2-2xy+11y^2$, donc $2p = (4x-1)^2+21y^2$, donc $2p \equiv 1,4$ ou 16 (mod 21) , par suite

(5) $\quad \mathrm{Rep}(g_3) \ \hat{\subset}\ P_{84}(11,23,71)$.

Si $p \in \mathrm{Rep}(g_4)$, alors $p = 5x^2-4xy+5y^2$, donc $5p = (5x-2y)^2+21y^2$, donc $5p \equiv 1$, 4 ou 16 (mod 21) , par suite

(6) $\quad \mathrm{Rep}(g_4) \ \hat{\subset}\ P_{84}(5,17,41)$.

Il résulte de (1) , (2) , (3) , (4) , (5) et (6) que les inclusions (3) , (4) , (5) et (6) sont des égalités.

BIBLIOGRAPHIE

[B.S.] - BOREVICH Z.I. SHAFAREVICH I.R. - Number Theory. Academic Press (1966).

[C.F.] - CASSELS J.W.S. FROHLICH F. - Algebraic Number Theory. Academic Press (1967).

[Co] - COHN H. - A second course in Number Theory. Wiley (1962).

[D.D.] - DUBREIL P. DUBREIL-JACOTIN M.L. - Leçons d'algèbre moderne. Dunod (1961).

[Gas] - GASSMANN F. - Bemerkungen zu der vorstehenden Arbeit Von Hurwitz. Math. Zeitschr. 25 (1926) pp. 665-675.

[Gau] - GAUTHIER F. - Décomposition des nombres premiers dans les extensions abéliennes ou résolubles de $\mathbb{Q}$. C.R.A.S. Paris t. 278 pp. 113-115 (14.1.1974).

[Hi] - HILBERT D. - Ueber die Irreducibilität ganzer rationaler Functionen unit ganzzahligen Coefficienten, J. reine angew. Math., 110 (1892), 104-129.

[La] - LANG S. - Elliptic Functions. Addison Weisley.

[Sa] - SAMUEL P. - Theorie algébriques des Nombres. Hermann (1967).

[So] - SOMMER J. - Introduction à la théorie des Nombres algébriques. Hermann. (1911).

[Wy] - WYMAN B.F. - What is reciprocity law ? American Math. Monthly 79 (1972) pp. 571-586.

-:-:-:-